On the logarithm of the identity on connected filtered bialgebras

Darij Grinberg

Version 0.19, 18 June 2021

Contents

***

The purpose of this document is to prove several properties of coalgebras, bialgebras and Hopf algebras. The proofs given here are mostly not new, and often not optimal; however, they are very detailed and don't use Sweedler's notation.

Remark (2017):

This "lab notebook" has been mostly written in 2011–2013 (when I was a graduate student), and collects various results I have encountered while exploring the theory of Hopf algebras (e.g., variants of the Cartier-Milnor-Moore and Leray theorems; properties of the Eulerian idempotent; facts like the invertibility of the antipode in a connected filtered Hopf algebra). I expect few of these results to be new; the best I can claim is that they are stated more explicitly here than in the available literature. Unfortunately, this notebook is rather disorganized, and the results are written down more or less in the order in which I have found them. I have tried to give detailed proofs of all statements (if only to make sure that they are correct); these proofs should be "technically" readable but in practice you might have an easier time skimming them for their main ideas (which are, unfortunately, sometimes hidden well) and reconstructing the rest yourself. Needless to say, the notations used in this notebook are also not the best.

Acknowledgments: Thanks to Philipp Varšo for finding an error in the proof of Proposition 5.13 (the statement of Corollary 5.14 was insufficiently general).

§1. Notations and definitions

In this document, we shall use some standard terminology from the theory of Hopf algebras (see, for example, [Schnei15] or [Mancho06]) along with the following notations:

Convention 1.1. In the following, the symbol $\mathbb{N}$ always denotes the set $\{0, 1, 2, \ldots\}$.

Convention 1.2. A "ring" shall always mean an associative ring with unity.[1]

Definition 1.3. Let k be a field, and U and V be two k-vector spaces. Then, $\mathcal{L}(U, V)$ denotes the vector space of all k-linear maps $U \to V$. (This vector space is commonly denoted by $\mathrm{Hom}_k(U, V)$.)

Convention 1.4. In the following, whenever a commutative ring k exists in the context[2], the $\otimes$ sign will always mean $\otimes_k$.

[1] We will sometimes say "ring with unity" to additionally stress this, but even if we do not say "with unity" we still mean unital rings only.

[2] Most of the time we will be working over a ground field, which will be denoted by k. Occasionally (e.g., in §14), we will be working over a ground ring, but it will also be denoted by k.

Convention 1.5. If Q is any set and n is any nonnegative integer, then we shall denote the Cartesian product $\underbrace{Q \times Q \times \cdots \times Q}_{n \text{ times}}$ by $Q^{\times n}$. This Cartesian product is usually denoted by Q^n in the literature, but we shall instead reserve the notation Q^n for another meaning (which will be introduced in Convention 15.2).

Convention 1.6. Whenever k is a field, A, B, C and D are four k-vector spaces, and $f : A \to B$ and $g : C \to D$ are two k-linear maps, then the notation $f \otimes g$ can mean two different things: On the one hand, it can mean the k-linear map $f \otimes g : A \otimes C \to B \otimes D$ (which maps $a \otimes c$ to $f(a) \otimes g(c)$ for every $a \in A$ and $c \in C$). On the other hand, it can mean the tensor $f \otimes g \in \mathcal{L}(A, B) \otimes \mathcal{L}(C, D)$ (since $f \in \mathcal{L}(A, B)$ and $g \in \mathcal{L}(C, D)$). Let us agree that in the following, whenever a term like $f \otimes g$ (with f and g being two k-linear maps) occurs, it will mean the first thing (i. e., the k-linear map $f \otimes g : A \otimes C \to B \otimes D$) and not the second one (i. e., the tensor $f \otimes g \in \mathcal{L}(A, B) \otimes \mathcal{L}(C, D)$).

Definition 1.7. Let k be a field and A be a k-algebra. Then, μ_A will always denote the multiplication map $A \otimes A \to A$ of the k-algebra A, and η_A will always denote the unity map $k \to A$ of the k-algebra A. When it is clear which algebra we are talking about, we will abbreviate μ_A and η_A as μ and η, respectively.

Definition 1.8. Let k be a field and C be a k-coalgebra. Then, Δ_C will always denote the comultiplication map $C \to C \otimes C$ of the k-coalgebra C, and ε_C will always denote the counit map $C \to k$ of the k-coalgebra C. When it is clear which coalgebra we are talking about, we will abbreviate Δ_C and ε_C as Δ and ε, respectively.

Definition 1.9. Let k be a field, let A be a k-algebra, and let C be a k-coalgebra. Then, the k-vector space $\mathcal{L}(C, A)$ becomes a k-algebra $(\mathcal{L}(C, A), *)$ by setting

$$f * g = \mu_A \circ (f \otimes g) \circ \Delta_C \qquad \text{for any } f \in \mathcal{L}(C, A) \text{ and } g \in \mathcal{L}(C, A). \quad (1)$$

This k-algebra $(\mathcal{L}(C, A), *)$ has unity $\eta_A \circ \varepsilon_C$ and is called the *convolution algebra* of C and A. In the following, we will simply refer to this algebra as $\mathcal{L}(C, A)$.

The binary operation $*$ defined in (1) is called *convolution*. In particular, for any $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$, we will refer to $f * g$ as the *convolution* of the maps f and g.

Convention 1.10. Let k be a field, let A be a k-algebra, and let C be a k-coalgebra. For any $n \in \mathbb{N}$ and any $f \in \mathcal{L}(C, A)$, we will denote by f^{*n} the n-th power of the element f in the convolution algebra $\mathcal{L}(C, A)$.

If an element $f \in \mathcal{L}(C, A)$ has a multiplicative inverse in the k-algebra $\mathcal{L}(C, A)$, then this inverse is denoted by $f^{*(-1)}$ and called the $*$-*inverse* of f.

Definition 1.11. Let k be a field. Let H be a k-Hopf algebra. Then, S_H will always denote the antipode of the k-Hopf algebra S (that is, the $*$-inverse of the identity map $\mathrm{id}_H \in \mathcal{L}(H, H)$).

Definition 1.12. Let k be a field. Let C be a k-coalgebra. Let A be a k-algebra. Then, $e_{C,A}$ shall denote the map $\eta_A \circ \varepsilon_C : C \to A$. This map $e_{C,A}$ is the unity of the convolution algebra $\mathcal{L}(C, A)$.

Next, let us define some concepts related to *filtrations* on vector spaces. Different authors define the words "filtered" and "filtration" in different (often non-equivalent) ways, so some care should be taken when consulting the literature.

Definition 1.13. Let k be a field. A *filtered k-vector space* means a k-vector space V equipped with a family $(V_{\leq \ell})_{\ell \geq 0}$ of k-vector subspaces of V satisfying $V_{\leq 0} \subseteq V_{\leq 1} \subseteq V_{\leq 2} \subseteq \cdots$ and $V = \bigcup_{\ell \geq 0} V_{\leq \ell}$. Such a filtered k-vector space will often be denoted simply by V (that is, the family $(V_{\leq \ell})_{\ell \geq 0}$ will not be explicitly mentioned). The family $(V_{\leq \ell})_{\ell \geq 0}$ is called the *filtration* of this filtered k-vector space. For each $m \in \mathbb{N}$, the k-vector subspace $V_{\leq m}$ of V is called the *m-th part of the filtration* $(V_{\leq \ell})_{\ell \geq 0}$.

Convention 1.14. In the following, whenever V is a filtered vector space, we will denote the filtration on V by $(V_{\leq \ell})_{\ell \geq 0}$. (This is a general convention, so it does not only pertain to filtered vector spaces called V, but pertains to any filtered vector space. For instance, if we have a filtered vector space called C, then this convention yields that the filtration on C is denoted by $(C_{\leq \ell})_{\ell \geq 0}$.)

Furthermore, whenever V is a filtered vector space and ℓ is a negative integer, we define $V_{\leq \ell}$ to mean the k-vector subspace 0 of V. (Thus, $V_{\leq \ell}$ is defined for each $\ell \in \mathbb{Z}$, not only for $\ell \in \mathbb{N}$.)

Definition 1.15. Let k be a field. A *filtered k-coalgebra* means a k-coalgebra C that is simultaneously a filtered k-vector space (i.e., that is equipped with a family $(C_{\leq \ell})_{\ell \geq 0}$ of k-vector subspaces of C satisfying $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$ and $C = \bigcup_{\ell \geq 0} C_{\leq \ell}$) and has the property that

$$\text{each } n \in \mathbb{N} \text{ satisfies } \Delta(C_{\leq n}) \subseteq \sum_{u=0}^{n} C_{\leq u} \otimes C_{\leq n-u}.$$

Definition 1.16. Let k be a field, and let C be a filtered k-coalgebra. We say that the filtered k-coalgebra C is *connected* if and only if the map $\varepsilon_C |_{C_{\leq 0}} : C_{\leq 0} \to k$ is a k-vector space isomorphism[3].

[3]Recall that $(C_{\leq \ell})_{\ell \geq 0}$ denotes the filtration of the filtered k-coalgebra C (according to Convention 1.14).

§2. Unital coalgebras

Next we shall define the notion of a *unital coalgebra*. This notion is an intermediate step between the (rather well-known) notions of a coalgebra and of a bialgebra; it also is an intermediate step between the notions of a coalgebra and of a filtered connected coalgebra. Its definition is very simple:

Definition 2.1. Let k be a field. Let C be a k-coalgebra, and let i be an element of C. Then, (C, i) is said to be a *unital coalgebra*[4] if $\Delta_C(i) = i \otimes i$ and $\varepsilon_C(i) = 1$.

When (C, i) is a unital coalgebra, we will denote the element i by $1_{(C,i)}$ and call it the *unity* of the unital coalgebra (C, i).

When C is a k-coalgebra, there may be several elements $i \in C$ for which (C, i) is a unital coalgebra[5] (but there also may be no such elements). Hence, a unital coalgebra (C, i) is not uniquely determined by the coalgebra C. However, there are many cases where we have some additional structure on C (like a k-bialgebra structure or a connected filtered k-coalgebra structure) which gives rise to one preferred canonical i. First we consider the case when C is a k-bialgebra. In this case, we have:

Proposition 2.2. Let k be a field. Let C be a k-bialgebra. Then, $(C, 1_C)$ is a unital coalgebra. (Here, 1_C denotes the unity of the k-algebra C, as usual.)

Proof of Proposition 2.2. By the axioms of a k-bialgebra, we have $\Delta_C(1_C) = 1_C \otimes 1_C$ and $\varepsilon_C(1_C) = 1$. By the definition of a unital coalgebra, this means that $(C, 1_C)$ is a unital coalgebra. Proposition 2.2 is thus proven. □

Note that Proposition 2.2 really needs the condition that C is a k-bialgebra, and not just some k-vector space with a k-algebra structure and a k-coalgebra structure.

Now we consider the case of connected filtered coalgebras:

Proposition 2.3. Let k be a field. Let C be a connected filtered k-coalgebra. Then, $\left(C, \left(\varepsilon_C|_{C_{\leq 0}}\right)^{-1}(1)\right)$ is a unital coalgebra.

Proof of Proposition 2.3. Since C is connected, the map $\varepsilon_C|_{C_{\leq 0}}: C_{\leq 0} \to k$ is a k-vector space isomorphism. Hence, the map $\left(\varepsilon_C|_{C_{\leq 0}}\right)^{-1}: k \to C_{\leq 0}$ is well-defined.

Let us define an element $i \in C$ by $i = \left(\varepsilon_C|_{C_{\leq 0}}\right)^{-1}(1)$. We are going to show that (C, i) is a unital coalgebra.

Since $\varepsilon_C|_{C_{\leq 0}}: C_{\leq 0} \to k$ is an isomorphism, we have

$$C_{\leq 0} = \left(\varepsilon_C|_{C_{\leq 0}}\right)^{-1}\left(\underbrace{k}_{=k\cdot 1}\right) = \left(\varepsilon_C|_{C_{\leq 0}}\right)^{-1}(k \cdot 1) = k \cdot \underbrace{\left(\varepsilon_C|_{C_{\leq 0}}\right)^{-1}(1)}_{=i} = k \cdot i.$$

[4] To be completely honest, we would have to call this "unital k-coalgebra" to make clear that this notion depends on the field k. However, since we are not going to change the field k anytime soon, we leave the k out of the notation and simply speak of "unital coalgebras".

[5] Such elements are called *grouplike elements* of C. Thus, a unital coalgebra is a pair (C, i) of a coalgebra C and a grouplike element i of C.

Since $i = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$, we have $1 = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)(i) = \underbrace{\varepsilon_C}_{=\varepsilon}(i) = \varepsilon(i)$. Now, $i \in C_{\leq 0}$, so that $\Delta(i) \in \Delta(C_{\leq 0}) \subseteq \sum_{u=0}^{0} C_{\leq u} \otimes C_{\leq 0-u}$ (since C is a filtered coalgebra). Since

$$\sum_{u=0}^{0} C_{\leq u} \otimes C_{\leq 0-u} = C_{\leq 0} \otimes \underbrace{C_{\leq 0-0}}_{=C_{\leq 0}} = C_{\leq 0} \otimes C_{\leq 0} = (k \cdot i) \otimes (k \cdot i) \qquad \text{(since } C_{\leq 0} = k \cdot i\text{)}$$
$$= k \cdot (i \otimes i),$$

this rewrites as $\Delta(i) \in k \cdot (i \otimes i)$. Thus, there exists some $\lambda \in k$ such that $\Delta(i) = \lambda \cdot (i \otimes i)$. Consider this λ.

Let $\mathrm{can} : C \otimes k \to C$ be the canonical k-module isomorphism (sending $c \otimes x$ to cx for all $c \in C$ and $x \in k$). Then, by the axioms of a coalgebra, we have $\mathrm{can} \circ (\mathrm{id} \otimes \varepsilon) \circ \Delta = \mathrm{id}$. But

$$(\mathrm{can} \circ (\mathrm{id} \otimes \varepsilon) \circ \Delta)(i) = \mathrm{can}\left((\mathrm{id} \otimes \varepsilon)\left(\underbrace{\Delta(i)}_{=\lambda \cdot (i \otimes i)}\right)\right) = \mathrm{can}\left(\underbrace{(\mathrm{id} \otimes \varepsilon)(\lambda \cdot (i \otimes i))}_{=\lambda \cdot \mathrm{id}(i) \otimes \varepsilon(i)}\right)$$
$$= \mathrm{can}(\lambda \cdot \mathrm{id}(i) \otimes \varepsilon(i)) = \lambda \cdot \underbrace{\mathrm{id}(i)}_{=i} \cdot \underbrace{\varepsilon(i)}_{=1} \qquad \text{(by the definition of can)}$$
$$= \lambda i,$$

so that

$$\lambda i = \underbrace{(\mathrm{can} \circ (\mathrm{id} \otimes \varepsilon) \circ \Delta)}_{=\mathrm{id}}(i) = \mathrm{id}(i) = i.$$

Now, $\Delta(i) = \lambda \cdot (i \otimes i) = \underbrace{\lambda i}_{=i} \otimes i = i \otimes i$.

So we have $\Delta_C(i) = \Delta(i) = i \otimes i$ and $\varepsilon_C(i) = 1$. By the definition of a unital coalgebra, this shows that (C, i) is a unital coalgebra. Since $i = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$, this means that $\left(C, \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)\right)$ is a unital coalgebra. Proposition 2.3 is proven. □

Proposition 2.2 gives us a unital coalgebra when we start with a k-bialgebra. Proposition 2.3 gives us a unital coalgebra when we start with a connected filtered k-coalgebra. One might wonder what happens if we start with a connected filtered k-bialgebra: In this case, each of Propositions 2.2 and 2.3 gives us a unital coalgebra. Are these two unital coalgebras the same? The answer is yes, as the following proposition shows:

Proposition 2.4. Let k be a field, and let C be a connected filtered[6] k-bialgebra. Then, $1_C = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$ (where 1_C denotes the unity of the k-algebra C). As a consequence, the unital coalgebras $(C, 1_C)$ and $\left(C, \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)\right)$ are identic.

[6]Of course, when we say that the filtered k-bialgebra C is connected, we mean that the filtered k-coalgebra C is connected.

Proof of Proposition 2.4. By the definition of a connected filtered k-coalgebra, the map $\varepsilon_C \mid_{C_{\leq 0}} : C_{\leq 0} \to k$ is a k-vector space isomorphism (since C is connected). Moreover, $\left(\varepsilon_C \mid_{C_{\leq 0}}\right)(1_C) = \varepsilon_C(1_C) = 1$, so that $1_C = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$. This proves Proposition 2.4. $\square$

Since it is cumbersome to explicitly mention the unity every time we are referring to a unital coalgebra, we make the following convention:

Convention 2.5. Let k be a field. Let (C, i) be a unital coalgebra. Then, we will often abbreviate the "unital coalgebra (C, i)" as "unital coalgebra C". This abbreviation is an abuse of notation, since a unital coalgebra (C, i) is not uniquely determined by the coalgebra C; but we will only use this abbreviation when it is clear what i we mean. In particular, we will use this abbreviation when there is a canonical unital coalgebra structure on C obtained from either Definition 2.6 or Definition 2.7 (below), or when the unital coalgebra is just being defined[7].

Definition 2.6. Let k be a field. Let C be a k-bialgebra. Then, according to Proposition 2.2, the unital coalgebra $(C, 1_C)$ is well-defined (where 1_C denotes the unity of the k-algebra C). This unital coalgebra $(C, 1_C)$ is called the *unital coalgebra canonically induced by the k-bialgebra C*. Whenever we just speak of "the unital coalgebra C" (where C is a k-bialgebra), we will always mean this unital coalgebra $(C, 1_C)$.

Definition 2.7. Let k be a field. Let C be a connected filtered k-coalgebra. Then, the unital coalgebra $\left(C, \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)\right)$ (this is well-defined according to Proposition 2.3) is called the *unital coalgebra canonically induced by the connected filtered k-coalgebra C*. Whenever we just speak of "the unital coalgebra C" (where C is a connected filtered k-coalgebra), we will always mean this unital coalgebra $\left(C, \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)\right)$.

Remark 2.8. Let k be a field. Let C be a connected filtered k-bialgebra. Then, the "unital coalgebra C" as understood according to Definition 2.6 is identic with the "unital coalgebra C" as understood according to Definition 2.7. (This is just a rewording of Proposition 2.4.) Thus, the notations introduced in Definitions 2.6 and 2.7 don't conflict with each other.[8]

Remark 2.9. Let k be a field. Let C be a unital coalgebra. Then, the unity of this unital coalgebra C is denoted by 1_C. This is not a new notation we introduce; it is just a consequence of our Definition 2.1 (where we stipulated

[7] For instance, when we write "Let C be a unital coalgebra", we are using this abbreviation; this is okay, because there are no elements i of C defined yet which we can confuse.

[8] This only pertains to the case when C is a connected filtered k-bialgebra. If C would be a vector space with a connected filtered k-coalgebra structure on one hand and a (totally unrelated!) k-bialgebra structure on the other, then, of course, then the "unital coalgebra C" in the sense of Definition 2.6 would not necessarily be identic to the "unital coalgebra C" in the sense of Definition 2.7, so the notations introduced in Definitions 2.6 and 2.7 could conflict. However, in such a case, it would already be a very bad idea to speak of the "coalgebra C", since this could mean any of two different coalgebra structures, so in such a case we would have to be careful with our notations anyway.

that the unity of a unital coalgebra (C, i) will be denoted by $1_{(C,i)}$) because we abbreviate (C, i) by C.

This notation can conflict with the notation 1_A for the unity of a k-algebra A: In fact, if we have a vector space V which happens to be a k-algebra and a unital coalgebra at the same time, then in general it might occur that the unity of the unital coalgebra V is not the same as the unity of the k-algebra V, so the notation 1_V would be ambiguous (it could mean each of these two unities). However, when we have a k-bialgebra C, then the unity of the unital coalgebra C (which is understood according to Definition 2.6) *is* the same as the unity of the k-algebra C [9], so there is no conflict in this case. Fortunately, we are going to have this case all of the time, so we won't have to care about possible conflicts between these notations.

Remark 2.10. Let k be a field, and let C be a connected filtered k-coalgebra. Then, C is a unital coalgebra (according to Definition 2.7) with unity $1_C = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$.

Proof of Remark 2.10. The unital coalgebra C (as defined in Definition 2.7) is $\left(C, \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)\right)$. Hence, the unity of this coalgebra is $\left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$. Since we denote the unity of the unital coalgebra C by 1_C, this means that $1_C = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$. Remark 2.10 is proven. □

Remark 2.11. Let k be a field, and let C be a connected filtered k-coalgebra. Then, $C_{\leq 0} = k \cdot 1_C$. (Here, as usual, 1_C denotes the unity of the unital coalgebra C, which unital coalgebra is defined as in Definition 2.7.)

Proof of Remark 2.11. In the proof of Proposition 2.3, we showed that $C_{\leq 0} = k \cdot i$, where $i = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$. But this i is equal to 1_C (since $i = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1) = 1_C$ by Remark 2.10), so that $C_{\leq 0} = k \cdot i$ rewrites as $C_{\leq 0} = k \cdot 1_C$. Remark 2.11 is now proven. □

Remark 2.12. Let k be a field, and let H be a filtered k-bialgebra. Then, H is connected if and only if $H_{\leq 0} = k \cdot 1_H$ (where 1_H denotes the unity of the k-algebra H).

Proof of Remark 2.12. **a)** Let us prove that if H is connected, then $H_{\leq 0} = k \cdot 1_H$.

Proof. Assume that H is connected. Then, H becomes a unital coalgebra according to Definition 2.7. Thus, the notation 1_H can mean two different things: On the one hand, it can mean the unity of the k-algebra H, but on the other hand, it can mean the unity of the unital coalgebra H (defined by Definition 2.7). Fortunately, this does not yield a conflict because these two things are the same (by Remark 2.9, since H is a k-bialgebra). Remark 2.11 (applied to $C = H$) now yields $H_{\leq 0} = k \cdot 1_H$.

We thus have proven that if H is connected, then $H_{\leq 0} = k \cdot 1_H$.

b) Let us prove that if $H_{\leq 0} = k \cdot 1_H$, then H is connected.

[9] *Proof.* Let C be a k-bialgebra. According to Definition 2.6, the unital coalgebra C is $(C, 1_C)$, where 1_C denotes the unity of the k-algebra C. Hence, the unity of the unital coalgebra C is 1_C, where 1_C denotes the unity of the k-algebra C. In other words, the unity of the unital coalgebra C is the same as the unity of the k-algebra C, qed.

Proof. Assume that $H_{\leq 0} = k \cdot 1_H$. Then, every $\alpha \in H_{\leq 0}$ satisfying $\left(\varepsilon_H \mid_{H_{\leq 0}}\right)(\alpha) = 0$ must satisfy $\alpha = 0$ [10]. Hence, the k-linear map $\varepsilon_H \mid_{H_{\leq 0}}$ must be injective. Since this map is also surjective[11], it thus follows that the map $\varepsilon_H \mid_{H_{\leq 0}}$ is bijective. Hence, $\varepsilon_H \mid_{H_{\leq 0}}$ is an isomorphism. By the definition of "connected", this yields that H is connected.

We have thus proven that if $H_{\leq 0} = k \cdot 1_H$, then H is connected.

Combining the above points **a)** and **b)**, we obtain Remark 2.12. □

Remark: The above Remark 2.12 is often used as an alternative definition of the notion of a connected filtered k-bialgebra. However, we prefer Definition 1.16, since it works for filtered k-coalgebras as well (and not only for filtered k-bialgebras).

Definition 2.13. Let k be a field, and let C be a unital coalgebra. Then, we denote by η_C the map $k \to C$ which sends every $\lambda \in k$ to $\lambda \cdot 1_C \in C$. This map is called the *unity map* of the unital coalgebra C.

This notation could sometimes conflict with the notation η_A for the unity map of a k-algebra A. In fact, such a conflict might emerge when we have a k-vector space H which is both a unital coalgebra and a k-algebra at the same time; in this case, η_H might mean two different things (namely, the unity map of the k-algebra H on the one hand, and the unity map of the unital coalgebra H on the other), just as 1_H might mean two different things. However, when H is a k-bialgebra, both meanings of 1_H are the same, and therefore both meanings of η_H are the same[12]. Thus, no conflict can occur as long as H is a k-bialgebra.

---

[10] *Proof.* Let $\alpha \in H_{\leq 0}$ satisfying $\left(\varepsilon_H \mid_{H_{\leq 0}}\right)(\alpha) = 0$ be arbitrary. Then, $\varepsilon(\alpha) = \left(\varepsilon_H \mid_{H_{\leq 0}}\right)(\alpha) = 0$. On the other hand, $\alpha \in H_{\leq 0} = k \cdot 1_H$, so that there exists some $\lambda \in k$ such that $\alpha = \lambda \cdot 1_H$. Consider this λ. Then, $\varepsilon(\alpha) = \varepsilon(\lambda \cdot 1_H) = \lambda \underbrace{\varepsilon(1_H)}_{=1} = \lambda$. Thus, $\varepsilon(\alpha) = 0$ becomes $\lambda = 0$, so that $\alpha = \underbrace{\lambda}_{=0} \cdot 1_H = 0$, qed.

[11] In fact, every $\beta \in k$ satisfies $\beta \in \left(\varepsilon_H \mid_{H_{\leq 0}}\right)(H_{\leq 0})$ (because $\beta \cdot \underbrace{1_H}_{\in H_{\leq 0}} \in H_{\leq 0}$ and $\left(\varepsilon_H \mid_{H_{\leq 0}}\right)(\beta \cdot 1_H) = \varepsilon(\beta \cdot 1_H) = \beta \underbrace{\varepsilon(1_H)}_{=1} = \beta$, so that $\beta = \left(\varepsilon_H \mid_{H_{\leq 0}}\right)(\beta \cdot 1_H) \in \left(\varepsilon_H \mid_{H_{\leq 0}}\right)(H_{\leq 0})$).

[12] *Proof.* Let H be a k-bialgebra. Then, the notation η_H might mean two different things: namely, the unity map of the k-algebra H on the one hand, and the unity map of the unital coalgebra H on the other. However, these two things are the same, since

(the unity map of the unital coalgebra H)
= (the map $k \to H$ which sends every $\lambda \in k$ to $\lambda \cdot 1_H$, where 1_H denotes the unity of the unital coalgebra H)
(because this is how the unity map of the unital coalgebra H was defined)
= (the map $k \to H$ which sends every $\lambda \in k$ to $\lambda \cdot 1_H$, where 1_H denotes the unity of the k-algebra H)
$\left(\begin{array}{c}\text{since Remark 2.9 (applied to } C = H\text{) says that the unity of the unital coalgebra } H \text{ is the same} \\ \text{as the unity of the } k\text{-algebra } H\end{array}\right)$
= (the unity map of the k-algebra H)
(because this is how the unity map of the k-algebra H was defined).

Hence, both meanings of η_H are the same, qed.

Now that we have defined the notion of unital coalgebras and cleared up some possible and impossible confusions, let us continue introducing notation. First, we observe that if we replace the words "k-algebra" by "unital coalgebra" in the definition of $e_{H,A}$ (Definition 1.12), then this definition still makes sense (because the expression 1_A makes sense not only when A is a k-algebra, but also when A is a unital coalgebra), although of course the map $e_{H,A}$ it defines is no longer the unity of the convolution algebra $\mathcal{L}(H, A)$ (since this convolution algebra does not exist in this situation). Thus, we obtain the following definition:

Definition 2.14. Let k be a field. Let C be a k-coalgebra. Let A be a unital coalgebra. Then, $e_{C,A}$ shall denote the map $\eta_A \circ \varepsilon_C : C \to A$.

Definition 2.14 does not conflict with Definition 1.12 in the case when A is a k-bialgebra (because both interpretations of the expression 1_A mean the same thing in this case); these definitions also do not conflict in the case when A is a connected filtered coalgebra (for the same reason). Of course, if A is simultaneously a k-algebra and a unital coalgebra with two completely unrelated unities, then the two definitions can conflict.

§3. Logarithms and exponentials in convolution algebras

Definition 3.1. Let k be a field, let A be a k-algebra, and let H be a connected filtered k-coalgebra.[13]

(a) We denote by $\mathfrak{g}(H, A)$ the subspace $\{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\}$ of $\mathcal{L}(H, A)$. (Here, 1_H denotes the unity of the unital coalgebra H, which is defined according to Definition 2.7.)

(b) For every $n \in \mathbb{N}$, we denote by $\mathcal{L}^n(H, A)$ the subspace $\left\{f \in \mathcal{L}(H, A) \mid f|_{H_{\leq n-1}} = 0\right\}$ [14]. Then,

$$\mathcal{L}^0(H, A) = \left\{f \in \mathcal{L}(H, A) \mid f|_{H_{\leq 0-1}} = 0\right\} = \mathcal{L}(H, A)$$

(since every $f \in \mathcal{L}(H, A)$ satisfies $f|_{H_{\leq 0-1}} = 0$ (because $H_{\leq 0-1} = H_{\leq -1} =$

[13] We denote this k-coalgebra by H rather than by the (more appropriate) letter C because this is how it is often called in this context in standard literature.

[14] Recall that $(H_{\leq \ell})_{\ell \geq 0}$ denotes the filtration of the filtered k-coalgebra H (according to Convention 1.14).

0)) and

$$\mathcal{L}^1(H,A) = \left\{ f \in \mathcal{L}(H,A) \mid f|_{H_{\leq 1-1}} = 0 \right\} = \left\{ f \in \mathcal{L}(H,A) \mid f|_{\{\lambda \cdot 1_H | \lambda \in k\}} = 0 \right\}$$
$$\left(\begin{array}{c} \text{since } H_{\leq 1-1} = H_{\leq 0} = k \cdot 1_H \text{ (by Remark 2.11, applied to } C = H) \\ \text{and thus } H_{\leq 1-1} = k \cdot 1_H = \{\lambda \cdot 1_H \mid \lambda \in k\} \end{array} \right)$$
$$= \left\{ f \in \mathcal{L}(H,A) \mid \underbrace{f(\lambda \cdot 1_H)}_{=\lambda f(1_H)} = 0 \text{ for every } \lambda \in k \right\}$$
$$= \left\{ f \in \mathcal{L}(H,A) \mid \underbrace{\lambda f(1_H) = 0 \text{ for every } \lambda \in k}_{\text{this is equivalent to } f(1_H)=0} \right\}$$
$$= \{ f \in \mathcal{L}(H,A) \mid f(1_H) = 0 \} = \mathfrak{g}(H,A).$$

(c) Let us denote by $G(H,A)$ the subset $\{ f \in \mathcal{L}(H,A) \mid f(1_H) = 1_A \}$ of $\mathcal{L}(H,A)$. (Here, 1_A denotes the unity of A.)

Definition 3.2. **(a)** In Definition 3.1 **(a)**, we have defined $\mathfrak{g}(H,A)$ when H is a connected filtered k-coalgebra and A is a k-algebra. In the same way (that is, by the formula

$$\mathfrak{g}(H,A) = \{ f \in \mathcal{L}(H,A) \mid f(1_H) = 0 \}$$

), we can define $\mathfrak{g}(H,A)$ when H is a unital coalgebra and A is any k-vector space. In particular, $\mathfrak{g}(H,A)$ is thus defined when H is a k-bialgebra and A is any k-vector space (because according to Definition 2.6, when H is a k-bialgebra, H canonically becomes a unital coalgebra).

(b) In Definition 3.1 **(c)**, we have defined $G(H,A)$ when H is a connected filtered k-coalgebra and A is a k-algebra. In the same way (that is, by the formula

$$G(H,A) = \{ f \in \mathcal{L}(H,A) \mid f(1_H) = 1_A \}$$

), we can define the set $G(H,A)$ when H is a unital coalgebra and A is a k-algebra. Moreover, in the same way (i.e., by the same formula), we can define the set $G(H,A)$ when H is a unital coalgebra and A is a unital coalgebra (because the notation 1_A makes sense whenever A is a unital coalgebra).

Remark 3.3. Let k be a field. Let A be a k-algebra. Let H be a unital coalgebra. Recall (from Definition 1.12) that $e_{H,A}$ denotes the map $\eta_A \circ \varepsilon_H : H \to A$. Recall the sets $\mathfrak{g}(H,A)$ and $G(H,A)$ defined in Definition 3.2.

(a) We have $e_{H,A} \in G(H,A)$.

(b) We have $G(H,A) = e_{H,A} + \mathfrak{g}(H,A)$.

Proof of Remark 3.3. We know that $(H, 1_H)$ is a unital coalgebra. In other words, H is a k-coalgebra and 1_H is an element of H satisfying $\Delta_H(1_H) = 1_H \otimes 1_H$ and $\varepsilon_H(1_H) = 1$ (by the definition of a "unital coalgebra").

We have $e_{H,A} = \eta_A \circ \varepsilon_H$. Thus,

$$\begin{aligned} e_{H,A}(1_H) &= (\eta_A \circ \varepsilon_H)(1_H) = \eta_A\left(\underbrace{\varepsilon_H(1_H)}_{=1}\right) = \eta_A(1) \\ &= 1 \cdot 1_A \qquad \text{(by the definition of the map } \eta_A\text{)} \\ &= 1_A. \end{aligned}$$

Recall that

$$\mathfrak{g}(H,A) = \{f \in \mathcal{L}(H,A) \mid f(1_H) = 0\} \tag{2}$$

and

$$G(H,A) = \{f \in \mathcal{L}(H,A) \mid f(1_H) = 1_A\}. \tag{3}$$

(a) Now, $e_{H,A}$ is an element of $\mathcal{L}(H,A)$ satisfying $e_{H,A}(1_H) = 1_A$. In other words, $e_{H,A}$ is an $f \in \mathcal{L}(H,A)$ satisfying $f(1_H) = 1_A$. In other words, $e_{H,A} \in \{f \in \mathcal{L}(H,A) \mid f(1_H) = 1_A\}$. In view of (3), this rewrites as $e_{H,A} \in G(H,A)$. This proves Remark 3.3 **(a)**.

(b) Let $g \in G(H,A)$. Thus, $g \in G(H,A) = \{f \in \mathcal{L}(H,A) \mid f(1_H) = 1_A\}$. In other words, g is an element $f \in \mathcal{L}(H,A)$ satisfying $f(1_H) = 1_A$. In other words, g is an element of $\mathcal{L}(H,A)$ and satisfies $g(1_H) = 1_A$. Now, $(g - e_{H,A})(1_H) = \underbrace{g(1_H)}_{=1_A} - \underbrace{e_{H,A}(1_H)}_{=1_A} = 1_A - 1_A = 0$. Thus, $g - e_{H,A}$ is an element of $\mathcal{L}(H,A)$ and satisfies $(g - e_{H,A})(1_H) = 0$. In other words, $g - e_{H,A}$ is an $f \in \mathcal{L}(H,A)$ satisfying $f(1_H) = 0$. In other words, $g - e_{H,A} \in \{f \in \mathcal{L}(H,A) \mid f(1_H) = 0\}$. In view of (2), this rewrites as $g - e_{H,A} \in \mathfrak{g}(H,A)$. Thus, $g \in e_{H,A} + \mathfrak{g}(H,A)$.

Now, forget that we fixed g. We thus have shown that $g \in e_{H,A} + \mathfrak{g}(H,A)$ for each $g \in G(H,A)$. In other words,

$$G(H,A) \subseteq e_{H,A} + \mathfrak{g}(H,A). \tag{4}$$

On the other hand, let $h \in e_{H,A} + \mathfrak{g}(H,A)$. Thus, $h \in \mathcal{L}(H,A)$ and $h - e_{H,A} \in \mathfrak{g}(H,A)$. We have $h - e_{H,A} \in \mathfrak{g}(H,A) = \{f \in \mathcal{L}(H,A) \mid f(1_H) = 0\}$. In other words, $h - e_{H,A}$ is an element f of $\mathcal{L}(H,A)$ satisfying $f(1_H) = 0$. In other words, $h - e_{H,A}$ is an element of $\mathcal{L}(H,A)$ and satisfies $(h - e_{H,A})(1_H) = 0$. Comparing $(h - e_{H,A})(1_H) = 0$ with $(h - e_{H,A})(1_H) = h(1_H) - \underbrace{e_{H,A}(1_H)}_{=1_A} = h(1_H) - 1_A$, we obtain $h(1_H) - 1_A = 0$. In other words, $h(1_H) = 1_A$. Now, h is an element of $\mathcal{L}(H,A)$ satisfying $h(1_H) = 1_A$. In other words, h is an $f \in \mathcal{L}(H,A)$ satisfying $f(1_H) = 1_A$. In other words, $h \in \{f \in \mathcal{L}(H,A) \mid f(1_H) = 1_A\}$. In view of (3), this rewrites as $h \in G(H,A)$.

Now, forget that we fixed h. We thus have shown that $h \in G(H,A)$ for each $h \in e_{H,A} + \mathfrak{g}(H,A)$. In other words, $e_{H,A} + \mathfrak{g}(H,A) \subseteq G(H,A)$. Combining this with (4), we obtain $G(H,A) = e_{H,A} + \mathfrak{g}(H,A)$. This proves Remark 3.3 **(b)**. □

Remark 3.4. If we replace the word "k-algebra" by "unital coalgebra" in Remark 3.3, then Remark 3.3 still holds. In fact, the same proof given above still applies in this situation.

Remark 3.5. Let k be a field, let A be a k-algebra, and let H be a connected filtered k-coalgebra. Every $i \in \mathbb{N}$, $n \in \mathbb{N}$ and $f \in \mathfrak{g}(H, A)$ such that $i > n$ satisfy $f^{*i}(H_{\leq n}) = 0$.

Proof of Remark 3.5. We prove Remark 3.5 by induction over i:

Induction base: For $i = 0$, Remark 3.5 is vacuously true (because $i > n$ cannot hold (since $i = 0$ and $n \in \mathbb{N}$)).

Induction step: Let $j \in \mathbb{N}$ be arbitrary. Assume that Remark 3.5 holds for $i = j$. Now, we must prove that Remark 3.5 also holds for $i = j + 1$.

Let $n \in \mathbb{N}$ and $f \in \mathfrak{g}(H, A)$ be such that $j + 1 > n$. Then, $\Delta_H(H_{\leq n}) \subseteq \sum_{u=0}^{n} H_{\leq u} \otimes H_{\leq n-u}$ (since H is a filtered coalgebra) and

$$\begin{aligned}
&\underbrace{f^{*(j+1)}}_{=f^{*j}*f}(H_{\leq n}) \\
&= \left(f^{*j} * f\right)(H_{\leq n}) = \left(\mu_A \circ \left(f^{*j} \otimes f\right) \circ \Delta_H\right)(H_{\leq n}) \\
&= \mu_A\left(\left(f^{*j} \otimes f\right)\left(\underbrace{\Delta_H(H_{\leq n})}_{\subseteq \sum_{u=0}^{n} H_{\leq u} \otimes H_{\leq n-u}}\right)\right) \\
&\subseteq \mu_A\left(\left(f^{*j} \otimes f\right)\left(\sum_{u=0}^{n} H_{\leq u} \otimes H_{\leq n-u}\right)\right) \\
&= \sum_{u=0}^{n} \mu_A\left(\underbrace{\left(f^{*j} \otimes f\right)\left(H_{\leq u} \otimes H_{\leq n-u}\right)}_{\subseteq f^{*j}\left(H_{\leq u}\right) \otimes f\left(H_{\leq n-u}\right)}\right) \\
&\subseteq \sum_{u=0}^{n} \mu_A\left(f^{*j}(H_{\leq u}) \otimes f(H_{\leq n-u})\right) \\
&= \sum_{u=0}^{n-1} \mu_A\left(f^{*j}(H_{\leq u}) \otimes f(H_{\leq n-u})\right) + \mu_A\left(f^{*j}(H_{\leq n}) \otimes f(H_{\leq n-n})\right). \qquad (5)
\end{aligned}$$

Now, every $u \in \{0, 1, \ldots, n-1\}$ satisfies $j > u$ (since $j + 1 > n = \underbrace{(n-1)}_{\geq u} + 1 \geq u + 1$). Thus, for every $u \in \{0, 1, \ldots, n-1\}$, we can apply Remark 3.5 to j and u instead of i and n (since we assumed that Remark 3.5 holds for $i = j$), and obtain $f^{*j}(H_{\leq u}) = 0$. Besides, $f \in \mathfrak{g}(H, A) = \mathcal{L}^1(H, A)$ yields $f|_{H_{\leq 1-1}} = 0$ (by the definition of $\mathcal{L}^1(H, A)$), so that $f(H_{\leq 1-1}) = 0$. Thus, $f(H_{\leq n-n}) = f(H_{\leq 0}) = f(H_{\leq 1-1}) = 0$. Now, (5) becomes

$$\begin{aligned}
f^{*(j+1)}(H_{\leq n}) &\subseteq \sum_{u=0}^{n-1} \mu_A\left(\underbrace{f^{*j}(H_{\leq u})}_{=0} \otimes f(H_{\leq n-u})\right) + \mu_A\left(f^{*j}(H_{\leq n}) \otimes \underbrace{f(H_{\leq n-n})}_{=0}\right) \\
&= \underbrace{\sum_{u=0}^{n-1} \mu_A(0 \otimes f(H_{\leq n-u}))}_{=0} + \underbrace{\mu_A\left(f^{*j}(H_{\leq n}) \otimes 0\right)}_{=0} = 0 + 0 = 0.
\end{aligned}$$

In other words, $f^{*(j+1)}\left(H_{\leq n}\right) = 0$. We have thus proven that Remark 3.5 also holds for $i = j+1$. This completes the induction step.

We thus have completed the induction proof of Remark 3.5. $\square$

Definition 3.6. Let k be a field of characteristic 0, let A be a k-algebra, and let H be a connected filtered k-coalgebra. For every $f \in \mathfrak{g}\left(H, A\right)$, let us define a map $e^{*f} : H \to A$ by the formula

$$\left(e^{*f}\left(x\right) = \sum_{i \geq 0} \frac{f^{*i}\left(x\right)}{i!} \qquad \text{for every } x \in H \right). \tag{6}$$

This map e^{*f} is well-defined, because for every $x \in H$ the infinite sum $\sum_{i \geq 0} \frac{f^{*i}\left(x\right)}{i!}$ converges with respect to the discrete topology[15]. Besides, e^{*f} is a k-linear map[16], so that $e^{*f} \in \mathcal{L}\left(H, A\right)$. More precisely, $e^{*f} \in G\left(H, A\right)$. [17]

Remark. The e in the notation e^{*f} has nothing to do with the e in the notation $e_{H,A}$. The e in the notation e^{*f} is a pure symbol (in particular, e^{*f} is not an "f-th power" of any e (whatever this e would be) with respect to convolution) which has been chosen to suggest similarity with the exponential function known from analysis; despite this

[15] *Proof.* Let $x \in H$. Then, there exists some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$ (since H is filtered). Consider such an n. Then, every integer $i > n$ satisfies $f^{*i}\left(x\right) \in f^{*i}\left(H_{\leq n}\right) = 0$ (by Remark 3.5) and thus $f^{*i}\left(x\right) = 0$. Hence, for every integer $i > n$, the i-th addend of the infinite sum $\sum_{i \geq 0} \frac{f^{*i}\left(x\right)}{i!}$ is zero. Hence, this infinite sum $\sum_{i \geq 0} \frac{f^{*i}\left(x\right)}{i!}$ has only finitely many nonzero addends. Thus, this sum converges with respect to the discrete topology.

[16] *Proof.* Let $\alpha \in k$, $\beta \in k$, $x \in H$ and $y \in H$ be arbitrary. Then, (6) (applied to y instead of x) yields $e^{*f}\left(y\right) = \sum_{i \geq 0} \frac{f^{*i}\left(y\right)}{i!}$. But (6) (applied to $\alpha x + \beta y$ instead of x) yields

$$\begin{aligned} e^{*f}\left(\alpha x + \beta y\right) &= \sum_{i \geq 0} \frac{f^{*i}\left(\alpha x + \beta y\right)}{i!} = \sum_{i \geq 0} \underbrace{\frac{\alpha f^{*i}\left(x\right) + \beta f^{*i}\left(y\right)}{i!}}_{= \alpha \frac{f^{*i}\left(x\right)}{i!} + \beta \frac{f^{*i}\left(y\right)}{i!}} \\ &\qquad \left(\begin{array}{c} \text{since for every } i \in \mathbb{N}, \text{ we have } f^{*i}\left(\alpha x + \beta y\right) = \alpha f^{*i}\left(x\right) + \beta f^{*i}\left(y\right) \\ \text{(because } f^{*i} \text{ is a } k\text{-linear map)} \end{array} \right) \\ &= \alpha \underbrace{\sum_{i \geq 0} \frac{f^{*i}\left(x\right)}{i!}}_{= e^{*f}\left(x\right)} + \beta \underbrace{\sum_{i \geq 0} \frac{f^{*i}\left(y\right)}{i!}}_{= e^{*f}\left(y\right)} = \alpha e^{*f}\left(x\right) + \beta e^{*f}\left(y\right). \end{aligned}$$

Since this holds for all $\alpha \in k$, $\beta \in k$, $x \in H$ and $y \in H$, we thus see that e^{*f} is k-linear, qed.

[17] *Proof.* Every integer $i > 0$ satisfies $f^{*i}\left(H_{\leq 0}\right) = 0$ (by Remark 3.5, applied to $n = 0$) and thus $f^{*i}\left(\underbrace{1_H}_{\in H_{\leq 0}}\right) \in f^{*i}\left(H_{\leq 0}\right) = 0$, so that $f^{*i}\left(1_H\right) = 0$. Hence, every integer $i > 0$ satisfies

$$\frac{f^{*i}\left(1_H\right)}{i!} = \frac{0}{i!} = 0. \tag{7}$$

similarity, there is (in general) no "Euler number" $e \approx 2.718\ldots$ in $\mathcal{L}(H, A)$. The e in the notation $e_{H,A}$ simply stands for "neutral element" (just as the neutral element of a group is often denoted by e).

Definition 3.7. Let k be a field of characteristic 0, let A be a k-algebra, and let H be a connected filtered k-coalgebra. For every $f \in \mathfrak{g}(H, A)$, let us define a map $\operatorname{Log}_1 f : H \to A$ by the formula

$$\left(\left(\operatorname{Log}_1 f\right)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) \qquad \text{for every } x \in H \right). \tag{8}$$

This map $\operatorname{Log}_1 f$ is well-defined, because for every $x \in H$ the infinite sum $\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ converges with respect to the discrete topology[18]. Besides, $\operatorname{Log}_1 f$ is a k-linear map[19], so that $\operatorname{Log}_1 f \in \mathcal{L}(H, A)$. More precisely,

---

But applying (6) to $x = 1_H$, we get

$$e^{*f}(1_H) = \sum_{i \geq 0} \frac{f^{*i}(1_H)}{i!} = \underbrace{\frac{f^{*0}(1_H)}{0!}}_{= \frac{f^{*0}(1_H)}{1} = f^{*0}(1_H)} + \sum_{i>0} \underbrace{\frac{f^{*i}(1_H)}{i!}}_{\substack{=0 \\ \text{(by (7))}}}$$

(here, we have split off the addend for $i = 0$ from the sum)

$$= f^{*0}(1_H) + \underbrace{\sum_{i>0} 0}_{=0} = \underbrace{f^{*0}}_{=e_{H,A}}(1_H) = e_{H,A}(1_H) = 1_A.$$

Thus, $e^{*f} \in G(H, A)$ (by the definition of $G(H, A)$).

[18] *Proof.* Let $x \in H$. Then, there exists some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$ (since H is filtered). Consider this n. Then, every integer $i > n$ satisfies $f^{*i}(x) = 0$ (this is proven just as in Definition 3.6). Therefore, every integer $i > n$ satisfies $\frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{=0} = 0$. In other words, for every integer $i > n$, the i-th addend of the infinite sum $\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ is zero. Hence, this infinite sum $\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ has only finitely many nonzero addends. Thus, this sum converges with respect to the discrete topology, qed.

[19] *Proof.* Let $\alpha \in k$, $\beta \in k$, $x \in H$ and $y \in H$ be arbitrary. Then, (8) (applied to y instead of x) yields $\left(\operatorname{Log}_1 f\right)(y) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(y)$. But (8) (applied to $\alpha x + \beta y$ instead of x) yields

$$\left(\operatorname{Log}_1 f\right)(\alpha x + \beta y) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(\alpha x + \beta y)}_{\substack{= \alpha f^{*i}(x) + \beta f^{*i}(y) \\ \text{(since } f^{*i} \text{ is a } k\text{-linear map)}}} = \sum_{i \geq 1} \underbrace{\frac{(-1)^{i-1}}{i}\left(\alpha f^{*i}(x) + \beta f^{*i}(y)\right)}_{= \alpha \frac{(-1)^{i-1}}{i} f^{*i}(x) + \beta \frac{(-1)^{i-1}}{i} f^{*i}(y)}$$

$$= \alpha \underbrace{\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)}_{= \left(\operatorname{Log}_1 f\right)(x)} + \beta \underbrace{\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(y)}_{= \left(\operatorname{Log}_1 f\right)(y)} = \alpha \left(\operatorname{Log}_1 f\right)(x) + \beta \left(\operatorname{Log}_1 f\right)(y).$$

Since this holds for all $\alpha \in k$, $\beta \in k$, $x \in H$ and $y \in H$, we thus see that $\operatorname{Log}_1 f$ is k-linear, qed.

$\operatorname{Log}_1 f \in \mathfrak{g}(H, A)$. [20]

Definition 3.8. Let k be a field of characteristic 0, let A be a k-algebra, and let H be a connected filtered k-coalgebra. For every $F \in G(H, A)$, let us define an element $\operatorname{Log} F \in \mathfrak{g}(H, A)$ by $\operatorname{Log} F = \operatorname{Log}_1 (F - e_{H,A})$. [21]

§4. $\operatorname{Log}\mathrm{id}$ in a connected filtered cocommutative bialgebra

We are now ready to state a first interesting result:

Theorem 4.1. Let k be a field of characteristic 0, and let H be a connected filtered cocommutative bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. The map $\operatorname{Log}\mathrm{id} \in \mathcal{L}(H, H)$ is a projection from H to the subspace $\operatorname{Prim} H$ of all primitive elements of H.

The map $\operatorname{Log}\mathrm{id} \in \mathcal{L}(H, H)$ defined in Theorem 4.1 is known as the *Eulerian idempotent* of H.

Theorem 4.1 is a classical fact about the Eulerian idempotent in a bialgebra. In particular, it has been used in [PatReu98] (more precisely, in the Example in §2 of [PatReu98]).[22]

§5. Basic properties of Log and e^*

Before we start proving Theorem 4.1, we shall study the concepts of exponentiation and logarithm closer – first, as formal power series, but then as operators on the space $\mathcal{L}(H, A)$ of linear maps from a coalgebra H to an algebra A. (To be precise, they do not act on the full space $\mathcal{L}(H, A)$; but we will make everything precise when we state the results.)

---

[20] *Proof.* Every integer $i > 0$ satisfies $f^{*i}(H_{\leq 0}) = 0$ (by Remark 3.5, applied to $n = 0$) and thus $f^{*i}\left(\underbrace{1_H}_{\in H_{\leq 0}}\right) \in f^{*i}(H_{\leq 0}) = 0$, so that $f^{*i}(1_H) = 0$. But applying (8) to $x = 1_H$, we get

$$(\operatorname{Log}_1 f)(1_H) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(1_H)}_{=0} = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} 0 = 0.$$

Thus, $\operatorname{Log}_1 f \in \mathfrak{g}(H, A)$ (by the definition of $\mathfrak{g}(H, A)$).

[21] This is well-defined since

$$\underbrace{F}_{\in G(H,A) = e_{H,A} + \mathfrak{g}(H,A)} - e_{H,A} \in e_{H,A} + \mathfrak{g}(H, A) - e_{H,A} = \mathfrak{g}(H, A).$$

[22] Actually, our Theorem 4.1 is stronger than the fact used in the Example in §2 of [PatReu98], because [PatReu98] considers only connected *graded* cocommutative bialgebras, whereas our Theorem 4.1 is stated (and proven) for any connected *filtered* cocommutative bialgebra.

Note that the $\mathcal{L}(H, H)$ in our Theorem 4.1 is *not* the $\mathcal{L}(H)$ of [PatReu98] in the case when H is graded. In fact, the $\mathcal{L}(H)$ of [PatReu98] contains only the graded k-linear maps, while our $\mathcal{L}(H, H)$ contains all k-linear maps $H \to H$.

§5.1. log and exp as power series

Let us first study the logarithm and the exponentials as they act on formal power series:

Definition 5.1. Let k be a field of characteristic 0. For every power series $P \in k[[X]]$ whose coefficient before X^0 is 0, let $\exp P$ denote the power series in $k[[X]]$ defined by $\exp P = \sum_{i \geq 0} \frac{P^i}{i!}$. For every power series $Q \in k[[X]]$ whose coefficient before X^0 is 1, let $\log Q$ denote the power series in $k[[X]]$ defined by $\log Q = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} (Q-1)^i$.

Theorem 5.2. Let k be a field of characteristic 0.

(a) Every power series $P \in k[[X]]$ whose coefficient before X^0 is 0 satisfies $\log(\exp P) = P$.

(b) Every power series $Q \in k[[X]]$ whose coefficient before X^0 is 1 satisfies $\exp(\log Q) = Q$.

Theorem 5.2 is an important result in mathematics; in particular, it is frequently applied in combinatorics (e.g., in dealing with generating functions) and in algebra. Often it is derived from the analogous fact from complex analysis (where P and Q, rather than being formal power series, are required to be holomorphic functions). Let us instead give an elementary proof. The proof will be based on some basic properties of derivatives of power series:

Lemma 5.3. Let k be a field of characteristic 0. Let $P \in k[[X]]$ be a power series such that $\frac{d}{dX} P = 0$. Assume furthermore that the coefficient of P before X^0 is 0. Then, $P = 0$.

Proof of Lemma 5.3. Write the power series $P \in k[[X]]$ in the form $P = \sum_{n \in \mathbb{N}} p_n X^n$ for some sequence $(p_0, p_1, p_2, \ldots) \in k^{\mathbb{N}}$ of elements of k. Then,

$$\begin{aligned}
\frac{d}{dX} \underbrace{P}_{= \sum_{n \in \mathbb{N}} p_n X^n} &= \frac{d}{dX} \left(\sum_{n \in \mathbb{N}} p_n X^n \right) \\
&= \sum_{\substack{n \in \mathbb{N}; \\ n \geq 1}} n p_n X^{n-1} \qquad \left(\text{by the definition of the operator } \frac{d}{dX} \right) \\
&= \sum_{n \in \mathbb{N}} (n+1)\, p_{n+1} \underbrace{X^{(n+1)-1}}_{\substack{= X^n \\ (\text{since } (n+1)-1 = n)}} \\
&\qquad \text{(here, we have substituted } n+1 \text{ for } n \text{ in the sum)} \\
&= \sum_{n \in \mathbb{N}} (n+1)\, p_{n+1} X^n.
\end{aligned}$$

Thus, $\sum\limits_{n\in\mathbb{N}} (n+1)\, p_{n+1} X^n = \dfrac{d}{dX} P = 0$. Comparing coefficients on both sides of this equality, we conclude that

$$(n+1)\, p_{n+1} = 0 \qquad \text{for each } n \in \mathbb{N}. \tag{9}$$

On the other hand, the coefficient of P before X^0 is 0. Thus,

$$\begin{aligned} 0 &= \left(\text{the coefficient of } \underbrace{P}_{=\sum\limits_{n\in\mathbb{N}} p_n X^n} \text{ before } X^0 \right) \\ &= \left(\text{the coefficient of } \sum_{n\in\mathbb{N}} p_n X^n \text{ before } X^0 \right) = p_0. \end{aligned}$$

In other words, $p_0 = 0$.

Now, we have

$$p_n = 0 \qquad \text{for each } n \in \mathbb{N} \tag{10}$$

[23]. Thus, $P = \sum\limits_{n\in\mathbb{N}} \underbrace{p_n}_{\substack{=0 \\ \text{(by (10))}}} X^n = \sum\limits_{n\in\mathbb{N}} 0 X^n = 0$. This proves Lemma 5.3. □

Proposition 5.4. Let k be a field of characteristic 0. Let $U \in k\,[[X]]$ and $V \in k\,[[X]]$ be two power series such that $\dfrac{d}{dX} U = \dfrac{d}{dX} V$. Assume furthermore that the coefficient of U before X^0 equals the coefficient of V before X^0. Then, $U = V$.

Proof of Proposition 5.4. We have

$$\begin{aligned} &\big(\text{the coefficient of } U - V \text{ before } X^0\big) \\ &= \underbrace{\big(\text{the coefficient of } U \text{ before } X^0\big)}_{\substack{=\big(\text{the coefficient of } V \text{ before } X^0\big) \\ \text{(since the coefficient of } U \text{ before } X^0 \\ \text{equals the coefficient of } V \text{ before } X^0\text{)}}} - \big(\text{the coefficient of } V \text{ before } X^0\big) \\ &= \big(\text{the coefficient of } V \text{ before } X^0\big) - \big(\text{the coefficient of } V \text{ before } X^0\big) = 0. \end{aligned}$$

In other words, the coefficient of V before X^0 is 0. Moreover, $\dfrac{d}{dX}(U - V) = \dfrac{d}{dX} U - \dfrac{d}{dX} V = 0$ (since $\dfrac{d}{dX} U = \dfrac{d}{dX} V$). Hence, Lemma 5.3 (applied to $P = U - V$) yields $U - V = 0$. In other words, $U = V$. This proves Proposition 5.4. □

[23] *Proof of (10):* Let $n \in \mathbb{N}$. We must prove (10).

If $n = 0$, then clearly $p_n = p_0 = 0$. Hence, (10) is proven in the case when $n = 0$. Thus, for the rest of the proof of (10), we can WLOG assume that we don't have $n = 0$. Assume this.

We have $n \neq 0$ (since we don't have $n = 0$). Combined with $n \in \mathbb{N}$, this yields $n \in \mathbb{N} \setminus \{0\} = \{1, 2, 3, \ldots\}$. Thus, $n - 1 \in \mathbb{N}$. Hence, (9) (applied to $n-1$ instead of n) yields $((n-1)+1)\, p_{(n-1)+1} = 0$. Since $(n-1)+1 = n$, this rewrites as $np_n = 0$. But $n \in \{1, 2, 3, \ldots\}$; thus, n is invertible in k (since k is a field of characteristic 0). Hence, we can cancel n from the equality $np_n = 0$. We thus obtain $p_n = 0$. This proves (10).

Proposition 5.5. Let k be a field. Any two power series $U \in k[[X]]$ and $V \in k[[X]]$ satisfy

$$\frac{d}{dX}(UV) = \left(\frac{d}{dX}U\right) \cdot V + U \cdot \frac{d}{dX}V. \tag{11}$$

Proof of Proposition 5.5. The equality (11) is just the well-known Leibniz identity for the derivation $\frac{d}{dX}$. □

Proposition 5.6. Let k be a field. Let $P \in k[[X]]$ be a power series such that the coefficient of P before X^0 is 1. Then, $\frac{d}{dX}(P^{-1}) = -\frac{1}{P^2} \cdot \frac{d}{dX}P$.

Proof of Proposition 5.6. The multiplicative inverse P^{-1} of the power series P is well-defined, since the coefficient of P before X^0 is 1.

Applying Proposition 5.5 to $U = P^{-1}$ and $V = P$, we obtain

$$\frac{d}{dX}\left(P^{-1}P\right) = \left(\frac{d}{dX}\left(P^{-1}\right)\right) \cdot P + P^{-1} \cdot \frac{d}{dX}P.$$

Comparing this with $\frac{d}{dX}\left(\underbrace{P^{-1}P}_{=1}\right) = \frac{d}{dX}1 = 0$, we obtain

$$\left(\frac{d}{dX}\left(P^{-1}\right)\right) \cdot P + P^{-1} \cdot \frac{d}{dX}P = 0.$$

Hence, $\left(\frac{d}{dX}P^{-1}\right) \cdot P = -P^{-1} \cdot \frac{d}{dX}P$. Multiplying both sides of this equality by P^{-1}, we obtain

$$\left(\frac{d}{dX}\left(P^{-1}\right)\right) \cdot PP^{-1} = -P^{-1} \cdot \left(\frac{d}{dX}P\right) \cdot P^{-1} = -\frac{1}{P^2} \cdot \frac{d}{dX}P.$$

Thus,

$$-\frac{1}{P^2} \cdot \frac{d}{dX}P = \left(\frac{d}{dX}\left(P^{-1}\right)\right) \cdot \underbrace{PP^{-1}}_{=1} = \frac{d}{dX}\left(P^{-1}\right).$$

This proves Proposition 5.6. □

Proposition 5.7. Let k be a field of characteristic 0. Let $U \in k[[X]]$ and $V \in k[[X]]$ be two power series satisfying $V\frac{d}{dX}U = U\frac{d}{dX}V$. Assume that the coefficient of U before X^0 is 1. Assume that the coefficient of V before X^0 is 1. Then, $U = V$.

Proof of Proposition 5.7. The multiplicative inverse V^{-1} of the power series V is well-defined, since the coefficient of V before X^0 is 1.

Let w_0 be the coefficient of the power series UV^{-1} before X^0. Then, we can regard w_0 itself as a constant power series. Of course, the coefficient of this constant power series w_0 before X^0 is w_0 itself. Thus, the coefficient of UV^{-1} before X^0 equals the

coefficient of w_0 before X^0 (since both of these coefficients equal w_0). We have $\frac{d}{dX}w_0 = 0$ (since w_0 is a constant power series).

Proposition 5.5 (applied to V^{-1} instead of V) yields

$$\begin{aligned}
\frac{d}{dX}\left(UV^{-1}\right) &= \left(\frac{d}{dX}U\right)\cdot V^{-1} + U\cdot \underbrace{\frac{d}{dX}\left(V^{-1}\right)}_{\substack{=\frac{-1}{V^2}\cdot\frac{d}{dX}V \\ \text{(by Proposition 5.6} \\ \text{(applied to } P=V\text{))}}} \\
&= \left(\frac{d}{dX}U\right)\cdot V^{-1} + U\cdot\frac{-1}{V^2}\cdot\frac{d}{dX}V = \frac{1}{V}\left(\frac{d}{dX}U\right) - \frac{U}{V^2}\cdot\frac{d}{dX}V \\
&= \frac{1}{V^2}\underbrace{\left(V\left(\frac{d}{dX}U\right) - U\left(\frac{d}{dX}V\right)\right)}_{\substack{=0 \\ \left(\text{since } V\frac{d}{dX}U = U\frac{d}{dX}V\right)}} = \frac{1}{V^2}0 = 0 \\
&= \frac{d}{dX}w_0 \qquad \left(\text{since } \frac{d}{dX}w_0 = 0\right).
\end{aligned}$$

Hence, Proposition 5.4 (applied to UV^{-1} and w_0 instead of U and V) yields $UV^{-1} = w_0$. Thus, $U = w_0V$. Hence,

$$\begin{aligned}
&\left(\text{the coefficient of } \underbrace{U}_{=w_0V} \text{ before } X^0\right) \\
&= \left(\text{the coefficient of } w_0V \text{ before } X^0\right) = w_0 \underbrace{\left(\text{the coefficient of } V \text{ before } X^0\right)}_{\substack{=1 \\ \text{(since the coefficient of } V \text{ before } X^0 \text{ is 1)}}} = w_0,
\end{aligned}$$

so that

$$w_0 = \left(\text{the coefficient of } U \text{ before } X^0\right) = 1$$

(since the coefficient of U before X^0 is 1). Now, $U = \underbrace{w_0}_{=1}V = V$. This proves Proposition 5.7. □

Proposition 5.8. Let k be a field. Let $P \in k[[X]]$ be a power series.

Then, every positive integer n satisfies

$$\frac{d}{dX}\left(P^n\right) = nP^{n-1}\frac{d}{dX}P. \tag{12}$$

Proof of Proposition 5.8. We shall prove (12) by induction over n:

Induction base: We have $1\underbrace{P^{1-1}}_{=P^0=1}\frac{d}{dX}P = 1\frac{d}{dX}P = \frac{d}{dX}P$. Comparing this with $\frac{d}{dX}\left(\underbrace{P^1}_{=P}\right) = \frac{d}{dX}P$, we conclude $\frac{d}{dX}\left(P^1\right) = 1P^{1-1}\frac{d}{dX}P$. In other words, (12) holds for $n = 1$. This completes the induction base.

Induction step: Let N be a positive integer. Assume that (12) holds for $n = N$. We must now show that (12) holds for $n = N + 1$.

We have assumed that (12) holds for $n = N$. In other words, we have

$$\frac{d}{dX}\left(P^N\right) = NP^{N-1}\frac{d}{dX}P.$$

Now,

$$\begin{aligned}
\frac{d}{dX}\left(\underbrace{P^{N+1}}_{=PP^N}\right) &= \frac{d}{dX}\left(PP^N\right) = \underbrace{\left(\frac{d}{dX}P\right)\cdot P^N}_{=P^N\frac{d}{dX}P} + P\cdot \underbrace{\frac{d}{dX}\left(P^N\right)}_{=NP^{N-1}\frac{d}{dX}P} \\
&\qquad \left(\text{by Proposition 5.5 (applied to } U = P \text{ and } V = P^N\right)\text{)} \\
&= P^N\frac{d}{dX}P + \underbrace{P\cdot NP^{N-1}}_{=NP^N}\frac{d}{dX}P = P^N\frac{d}{dX}P + NP^N\frac{d}{dX}P \\
&= \underbrace{(1+N)}_{=N+1}\ \underbrace{P^N}_{\substack{=P^{(N+1)-1} \\ (\text{since } N=(N+1)-1)}}\ \frac{d}{dX}P = (N+1)\,P^{(N+1)-1}\frac{d}{dX}P.
\end{aligned}$$

In other words, (12) holds for $n = N + 1$. This completes the induction step. Thus, the induction proof of (12) is complete.

This proves Proposition 5.8. □

Proposition 5.9. Let k be a field of characteristic 0. Let $P \in k\left[\left[X\right]\right]$ be a power series whose coefficient before X^0 is 0. Then,

$$\frac{d}{dX}\left(\exp P\right) = \left(\frac{d}{dX}P\right)\cdot \exp P.$$

Proof of Proposition 5.9. Every positive integer n satisfies

$$\frac{1}{n!}n = \frac{1}{(n-1)!} \tag{13}$$

[24].

The definition of $\exp P$ yields $\exp P = \sum_{i\geq 0}\frac{P^i}{i!} = \sum_{i\geq 0}\frac{1}{i!}P^i = \sum_{n\geq 0}\frac{1}{n!}P^n$ (here, we have

[24] *Proof of (13):* Let n be a positive integer. The recursive definition of $n!$ yields $n! = n\cdot(n-1)!$. Hence, $\frac{1}{n!}n = \frac{1}{n\cdot(n-1)!}n = \frac{1}{(n-1)!}$. Qed.

renamed the summation index i as n). Hence,

$$\frac{d}{dX}\underbrace{(\exp P)}_{=\sum_{n\geq 0}\frac{1}{n!}P^n} = \frac{d}{dX}\left(\sum_{n\geq 0}\frac{1}{n!}P^n\right) = \sum_{n\geq 0}\frac{1}{n!}\frac{d}{dX}\left(P^n\right)$$

$$= \frac{1}{0!}\frac{d}{dX}\left(\underbrace{P^0}_{=1}\right) + \sum_{n\geq 1}\frac{1}{n!}\underbrace{\frac{d}{dX}\left(P^n\right)}_{\substack{=nP^{n-1}\frac{d}{dX}P \\ \text{(by Proposition 5.8)}}}$$

(here, we have split off the addend for $n = 0$ from the sum)

$$= \frac{1}{0!}\underbrace{\frac{d}{dX}1}_{=0} + \sum_{n\geq 1}\underbrace{\frac{1}{n!}n}_{\substack{=\frac{1}{(n-1)!} \\ \text{(by (13))}}}P^{n-1}\frac{d}{dX}P$$

$$= \underbrace{\frac{1}{0!}0}_{=0} + \sum_{n\geq 1}\frac{1}{(n-1)!}P^{n-1}\frac{d}{dX}P = \sum_{n\geq 1}\frac{1}{(n-1)!}P^{n-1}\frac{d}{dX}P$$

$$= \sum_{n\geq 0}\frac{1}{n!}P^n\frac{d}{dX}P \qquad \left(\begin{array}{c}\text{here, we have substituted } n \text{ for } n-1 \\ \text{in the sum}\end{array}\right).$$

Comparing this with

$$\left(\frac{d}{dX}P\right)\cdot\underbrace{\exp P}_{=\sum_{n\geq 0}\frac{1}{n!}P^n} = \left(\frac{d}{dX}P\right)\cdot\sum_{n\geq 0}\frac{1}{n!}P^n = \sum_{n\geq 0}\underbrace{\left(\frac{d}{dX}P\right)\cdot\frac{1}{n!}P^n}_{=\frac{1}{n!}P^n\frac{d}{dX}P} = \sum_{n\geq 0}\frac{1}{n!}P^n\frac{d}{dX}P,$$

we obtain $\frac{d}{dX}\left(\exp P\right) = \left(\frac{d}{dX}P\right)\cdot\exp P$. This proves Proposition 5.9. □

Proposition 5.10. Let k be a field. Let $Q \in k\left[\left[X\right]\right]$ be a power series whose coefficient before X^0 is 1. Then:

(a) The power series Q has a multiplicative inverse Q^{-1}.

(b) Assume that k is a field of characteristic 0. Then, the multiplicative inverse Q^{-1} of Q satisfies

$$\frac{d}{dX}\left(\log Q\right) = Q^{-1}\cdot\frac{d}{dX}Q.$$

I call Proposition 5.10 **(b)** the *logarithmic derivative theorem*, as it gives the derivative of the logarithm of a power series (provided the logarithm is well-defined).

Proof of Proposition 5.10. Define a power series $R \in k\left[\left[X\right]\right]$ by $R = Q - 1$. Thus,

$$\frac{d}{dX}\underbrace{R}_{=Q-1} = \frac{d}{dX}\left(Q-1\right) = \frac{d}{dX}Q - \underbrace{\frac{d}{dX}1}_{=0} = \frac{d}{dX}Q. \tag{14}$$

Also,

$$\begin{aligned}
&\left(\text{the coefficient of } \underbrace{R}_{=Q-1} \text{ before } X^0\right) \\
&= \left(\text{the coefficient of } Q-1 \text{ before } X^0\right) \\
&= \underbrace{\left(\text{the coefficient of } Q \text{ before } X^0\right)}_{\substack{=1 \\ \text{(since the coefficient of } Q \text{ before } X^0 \text{ is 1)}}} - \underbrace{\left(\text{the coefficient of 1 before } X^0\right)}_{=1} \\
&= 1-1=0.
\end{aligned}$$

In other words, the coefficient of R before X^0 is 0. Hence, the sum $\sum_{n\geq 0}(-1)^n R^n$ converges in $k[[X]]$. The power series $\sum_{n\geq 0}(-1)^n R^n$ is a multiplicative inverse of Q in the commutative ring $k[[X]]$ [25]. Thus, the power series Q has a multiplicative inverse Q^{-1}. This proves Proposition 5.10 **(a)**.

Notice that the multiplicative inverse Q^{-1} of Q must be equal to $\sum_{n\geq 0}(-1)^n R^n$ (since

[25] *Proof.* We have

$$\begin{aligned}
\left(\sum_{n\geq 0}(-1)^n R^n\right) R &= \sum_{n\geq 0}(-1)^n \underbrace{R^n R}_{=R^{n+1}} = \sum_{n\geq 0}(-1)^n R^{n+1} = \sum_{n\geq 1}\underbrace{(-1)^{n-1}}_{=-(-1)^n}\underbrace{R^{(n-1)+1}}_{=R^n} \\
&\qquad \text{(here, we have substituted } n-1 \text{ for } n \text{ in the sum)} \\
&= \sum_{n\geq 1}\left(-(-1)^n\right)R^n = -\sum_{n\geq 1}(-1)^n R^n.
\end{aligned}$$

On the other hand,

$$\begin{aligned}
\sum_{n\geq 0}(-1)^n R^n &= \underbrace{(-1)^0}_{=1}\underbrace{R^0}_{=1} + \sum_{n\geq 1}(-1)^n R^n \qquad \left(\begin{array}{c}\text{here, we have split off the addend} \\ \text{for } n=0 \text{ from the sum}\end{array}\right) \\
&= 1 + \sum_{n\geq 1}(-1)^n R^n.
\end{aligned}$$

Now,

$$\begin{aligned}
&\left(\sum_{n\geq 0}(-1)^n R^n\right) \underbrace{Q}_{\substack{=R+1 \\ \text{(since } R=Q-1\text{)}}} \\
&= \left(\sum_{n\geq 0}(-1)^n R^n\right)(R+1) = \underbrace{\left(\sum_{n\geq 0}(-1)^n R^n\right)}_{=-\sum_{n\geq 1}(-1)^n R^n} R + \underbrace{\sum_{n\geq 0}(-1)^n R^n}_{=1+\sum_{n\geq 1}(-1)^n R^n} \\
&= -\sum_{n\geq 1}(-1)^n R^n + \left(1+\sum_{n\geq 1}(-1)^n R^n\right) = 1.
\end{aligned}$$

Thus, $\sum_{n\geq 0}(-1)^n R^n$ is a multiplicative inverse of Q in the commutative ring $k[[X]]$.

$\sum\limits_{n\geq 0}(-1)^n R^n$ is a multiplicative inverse of Q). In other words,

$$Q^{-1} = \sum_{n\geq 0}(-1)^n R^n. \tag{15}$$

(b) The definition of $\log Q$ yields

$$\log Q = \sum_{i\geq 1}\frac{(-1)^{i-1}}{i}\left(\underbrace{Q-1}_{=R}\right)^i = \sum_{i\geq 1}\frac{(-1)^{i-1}}{i}R^i = \sum_{n\geq 1}\frac{(-1)^{n-1}}{n}R^n$$

(here, we have renamed the summation index i as n). Thus,

$$\begin{aligned}\frac{d}{dX}\underbrace{(\log Q)}_{=\sum\limits_{n\geq 1}\frac{(-1)^{n-1}}{n}R^n} &= \frac{d}{dX}\left(\sum_{n\geq 1}\frac{(-1)^{n-1}}{n}R^n\right) = \sum_{n\geq 1}\frac{(-1)^{n-1}}{n}\cdot \underbrace{\frac{d}{dX}(R^n)}_{\substack{=nR^{n-1}\frac{d}{dX}R \\ \text{(by Proposition 5.8} \\ \text{(applied to } P=R\text{))}}} \\ &= \sum_{n\geq 1}\underbrace{\frac{(-1)^{n-1}}{n}\cdot nR^{n-1}}_{=(-1)^{n-1}R^{n-1}}\frac{d}{dX}R \\ &= \sum_{n\geq 1}(-1)^{n-1}R^{n-1}\frac{d}{dX}R = \sum_{n\geq 0}(-1)^n R^n\frac{d}{dX}R\end{aligned}$$

(here, we have substituted n for $n-1$ in the sum). Comparing this with

$$\underbrace{Q^{-1}}_{\substack{=\sum\limits_{n\geq 0}(-1)^n R^n \\ \text{(by (15))}}}\cdot\underbrace{\frac{d}{dX}Q}_{\substack{=\frac{d}{dX}R \\ \text{(by (14))}}} = \left(\sum_{n\geq 0}(-1)^n R^n\right)\cdot\frac{d}{dX}R = \sum_{n\geq 0}(-1)^n R^n\frac{d}{dX}R,$$

we obtain $\dfrac{d}{dX}(\log Q) = Q^{-1}\cdot\dfrac{d}{dX}Q$. This proves Proposition 5.10 **(b)**. □

Lemma 5.11. Let k be a field. Let $U \in k[[X]]$ and $V \in k[[X]]$ be two power series such that the coefficient of U before X^0 is 0. Then, the coefficient of UV before X^0 is 0.

Proof of Lemma 5.11. We have (the coefficient of U before X^0 is 0) $= 0$ (since the coefficient of U before X^0 is 0). Now, the definition of the product of two power series shows that

$$\begin{aligned}&(\text{the coefficient of } UV \text{ before } X^n) \\ &= \sum_{g=0}^{n}(\text{the coefficient of } U \text{ before } X^g)\cdot\left(\text{the coefficient of } V \text{ before } X^{n-g}\right)\end{aligned}$$

for each $n \in \mathbb{N}$. Applying this to $n = 0$, we find

$$\begin{aligned}
&\left(\text{the coefficient of } UV \text{ before } X^0\right) \\
&= \sum_{g=0}^{0} \left(\text{the coefficient of } U \text{ before } X^g\right) \cdot \left(\text{the coefficient of } V \text{ before } X^{0-g}\right) \\
&= \underbrace{\left(\text{the coefficient of } U \text{ before } X^0\right)}_{=0} \cdot \left(\text{the coefficient of } V \text{ before } X^{0-0}\right) \\
&= 0 \cdot \left(\text{the coefficient of } V \text{ before } X^{0-0}\right) = 0.
\end{aligned}$$

In other words, the coefficient of UV before X^0 is 0. This proves Lemma 5.11. □

Proposition 5.12. Let k be a field of characteristic 0.

(a) If $P \in k\left[[X]\right]$ is a power series whose coefficient before X^0 is 0, then $\exp P$ is a power series whose coefficient before X^0 is 1.

(b) If $Q \in k\left[[X]\right]$ is a power series whose coefficient before X^0 is 1, then $\log Q$ is a power series whose coefficient before X^0 is 0.

Note that Proposition 5.12 shows that the terms $\log\left(\exp P\right)$ and $\exp\left(\log Q\right)$ in Theorem 5.2 make any sense at all.

Proof of Proposition 5.12. Let us first prove a simple fact: If $R \in k\left[[X]\right]$ is a power series whose coefficient before X^0 is 0, and if i is a positive integer, then

$$\left(\text{the coefficient of } R^i \text{ before } X^0\right) = 0 \tag{16}$$

[26].

(a) Let $P \in k\left[[X]\right]$ is a power series whose coefficient before X^0 is 0. The definition

[26] *Proof of (16):* Let $R \in k\left[[X]\right]$ is a power series whose coefficient before X^0 is 0. Let i be a positive integer. Thus, R^{i-1} is well-defined. But Lemma 5.11 (applied to $U = R$ and $V = R^{i-1}$) yields that the coefficient of RR^{i-1} before X^0 is 0. In other words, $\left(\text{the coefficient of } RR^{i-1} \text{ before } X^0\right) = 0$. This rewrites as $\left(\text{the coefficient of } R^i \text{ before } X^0\right) = 0$ (since $RR^{i-1} = R^i$). This proves (16).

of $\exp P$ yields $\exp P = \sum\limits_{i \geq 0} \dfrac{P^i}{i!} = \sum\limits_{i \geq 0} \dfrac{1}{i!} P^i$. Hence,

$$\left(\text{the coefficient of } \underbrace{\exp P}_{= \sum\limits_{i \geq 0} \frac{1}{i!} P^i} \text{ before } X^0 \right)$$

$$= \left(\text{the coefficient of } \sum_{i \geq 0} \frac{1}{i!} P^i \text{ before } X^0 \right)$$

$$= \sum_{i \geq 0} \frac{1}{i!} \left(\text{the coefficient of } P^i \text{ before } X^0 \right)$$

$$= \underbrace{\frac{1}{0!}}_{= \frac{1}{1} = 1} \left(\text{the coefficient of } \underbrace{P^0}_{=1} \text{ before } X^0 \right) + \sum_{i \geq 1} \frac{1}{i!} \underbrace{\left(\text{the coefficient of } P^i \text{ before } X^0 \right)}_{\substack{=0 \\ \text{(by (16) (applied to } R=P\text{))}}}$$

(here, we have split off the addend for $i = 0$ from the sum)

$$= \underbrace{\left(\text{the coefficient of } 1 \text{ before } X^0 \right)}_{=1} + \underbrace{\sum_{i \geq 1} \frac{1}{i!} 0}_{=0} = 1 + 0 = 1.$$

In other words, $\exp P$ is a power series whose coefficient before X^0 is 1. This proves Proposition 5.12 **(a)**.

(b) Let $Q \in k[[X]]$ be a power series whose coefficient before X^0 is 1. Define a power series $R \in k[[X]]$ by $R = Q - 1$. Then, the coefficient of R before X^0 is 0 [27]. Thus, every positive integer i satisfies (16).

Now, the definition of $\log Q$ yields

$$\log Q = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} \left(\underbrace{Q - 1}_{= R} \right)^i = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} R^i.$$

[27] This has already been proven in the proof of Proposition 5.10.

Thus,

$$\begin{aligned}
&\left(\text{the coefficient of } \underbrace{\log Q}_{=\sum\limits_{i\geq 1} \frac{(-1)^{i-1}}{i} R^i} \text{ before } X^0 \right) \\
&= \left(\text{the coefficient of } \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} R^i \text{ before } X^0 \right) \\
&= \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} \underbrace{\left(\text{the coefficient of } R^i \text{ before } X^0 \right)}_{\substack{=0 \\ \text{(by (16))}}} \\
&= \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} 0 = 0.
\end{aligned}$$

In other words, $\log Q$ is a power series whose coefficient before X^0 is 0. This proves Proposition 5.12 **(b)**. □

Now, we can finally come to the proof of Theorem 5.2:

Proof of Theorem 5.2. **(a)** Let $P \in k[[X]]$ is a power series whose coefficient before X^0 is 0. Then, $\exp P$ is a power series whose coefficient before X^0 is 1 (by Proposition 5.12 **(a)**). Hence, $\log(\exp P)$ is a well-defined power series in $k[[X]]$. Furthermore, Proposition 5.12 **(b)** (applied to $Q = \exp P$) shows that $\log(\exp P)$ is a power series whose coefficient before X^0 is 0. Thus, the coefficient of $\log(\exp P)$ before X^0 is 0. On the other hand, the coefficient of P before X^0 is 0 (by the definition of P). Thus, the coefficient of U before $\log(\exp P)$ equals the coefficient of P before X^0 (since both of these coefficients are 0).

Also, Proposition 5.10 **(b)** (applied to $Q = \exp P$) yields

$$\begin{aligned}
\frac{d}{dX}(\log(\exp P)) &= (\exp P)^{-1} \cdot \underbrace{\frac{d}{dX}(\exp P)}_{\substack{=\left(\frac{d}{dX}P\right)\cdot \exp P \\ \text{(by Proposition 5.9)}}} = (\exp P)^{-1} \cdot \left(\frac{d}{dX}P\right) \cdot \exp P \\
&= \frac{d}{dX}P.
\end{aligned}$$

Thus, Proposition 5.4 (applied to $U = \log(\exp P)$ and $V = P$) shows that $\log(\exp P) = P$. This proves Theorem 5.2 **(a)**.

(b) Let $Q \in k[[X]]$ is a power series whose coefficient before X^0 is 1. Then, $\log Q$ is a power series whose coefficient before X^0 is 0 (by Proposition 5.12 **(b)**). Hence, $\exp(\log Q)$ is a well-defined power series in $k[[X]]$. Furthermore, Proposition 5.12 **(a)** (applied to $P = \log Q$) shows that $\exp(\log Q)$ is a power series whose coefficient before X^0 is 1. Thus, the coefficient of $\exp(\log Q)$ before X^0 is 1. On the other hand, the coefficient of Q before X^0 is 1 (by the definition of Q).

Also, Proposition 5.9 (applied to $P = \log Q$) yields

$$\frac{d}{dX}\left(\exp\left(\log Q\right)\right) = \underbrace{\left(\frac{d}{dX}\left(\log Q\right)\right)}_{\substack{=Q^{-1}\cdot\frac{d}{dX}Q \\ \text{(by Proposition 5.10 \textbf{(b)})}}} \cdot \exp\left(\log Q\right)$$
$$= Q^{-1}\cdot\left(\frac{d}{dX}Q\right)\cdot\exp\left(\log Q\right).$$

Multiplying both sides of this equality by Q, we obtain

$$Q\frac{d}{dX}\left(\exp\left(\log Q\right)\right) = \left(\frac{d}{dX}Q\right)\cdot\exp\left(\log Q\right) = \exp\left(\log Q\right)\cdot\frac{d}{dX}Q.$$

Thus, Proposition 5.7 (applied to $U = \exp\left(\log Q\right)$ and $V = Q$) shows that $\exp\left(\log Q\right) = Q$. This proves Theorem 5.2 **(b)**. □

§5.2. $\mathrm{Log} : G(H,A) \to \mathfrak{g}(H,A)$ and $\mathfrak{g}(H,A) \to G(H,A)$

Next, let us prove a basic fact about the map $\mathrm{Log} : G(H,A) \to \mathfrak{g}(H,A)$ and the map $\mathfrak{g}(H,A) \to G(H,A)$ which sends every f to e^{*f} (when H is a connected filtered k-coalgebra and A is a k-algebra, where k is a field of characteristic 0): namely, that these two maps are mutually inverse. Here is how we state this fact:

Proposition 5.13. Let k be a field of characteristic 0, let A be a k-algebra, and let H be a connected filtered k-coalgebra.

(a) Every map $f \in \mathfrak{g}(H,A)$ satisfies $\mathrm{Log}\left(e^{*f}\right) = f$.

(b) Every map $F \in G(H,A)$ satisfies $e^{*(\mathrm{Log}\, F)} = F$.

It is easy to prove Proposition 5.13 using Theorem 5.2 and some topology to make sense of infinite sums like $\sum\limits_{i\geq 0}\dfrac{f^{*i}}{i!}$ and $\sum\limits_{i\geq 1}\dfrac{(-1)^{i-1}}{i}f^{*i}$ in $\mathcal{L}(H,A)$. Here is a more elementary version of this proof:

We start with a "finite version" of Theorem 5.2:

Corollary 5.14. Let k be a field of characteristic 0. Let $n \in \mathbb{N}$.

(a) Let a be an element of a k-algebra such that $a^{n+1} = 0$. Then,

$$\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(\sum_{j=1}^{n}\frac{a^j}{j!}\right)^i = a.$$

(b) Let b be an element of a k-algebra such that $b^{n+1} = 0$. Then,

$$\sum_{j=1}^{n}\frac{\left(\sum\limits_{i=1}^{n}\dfrac{(-1)^{i-1}}{i}b^i\right)^j}{j!} = b.$$

Proof of Corollary 5.14. **(a)** Consider the ring of power series $k[[X]]$. Clearly, X is a power series whose coefficient before X^0 is 0. Thus, applying Theorem 5.2 **(a)** to $P = X$, we obtain $\log(\exp X) = X$. Now, in the ring $k[[X]]$, we have

$$\underbrace{\exp X}_{=\sum\limits_{j=0}^{\infty}\frac{X^j}{j!}=\frac{X^0}{0!}+\sum\limits_{j=1}^{\infty}\frac{X^j}{j!}} - 1 = \underbrace{\frac{X^0}{0!}}_{=1} + \sum_{j=1}^{\infty}\frac{X^j}{j!} - 1 = \sum_{j=1}^{\infty}\frac{X^j}{j!} = \sum_{j=1}^{n}\frac{X^j}{j!} + \sum_{j=n+1}^{\infty}\underbrace{\frac{X^j}{j!}}_{\substack{\equiv 0 \bmod X^{n+1}k[[X]] \\ \text{(since } j\geq n+1 \text{ leads to} \\ X^j \equiv 0 \bmod X^{n+1}k[[X]]\text{)}}}$$

$$\equiv \sum_{j=1}^{n}\frac{X^j}{j!} + \underbrace{\sum_{j=n+1}^{\infty} 0}_{=0} = \sum_{j=1}^{n}\frac{X^j}{j!} \bmod X^{n+1}k[[X]].$$

Thus,

$$\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(\underbrace{\sum_{j=1}^{n}\frac{X^j}{j!}}_{\equiv \exp X - 1 \bmod X^{n+1}k[[X]]}\right)^i \equiv \sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}(\exp X - 1)^i \bmod X^{n+1}k[[X]].$$

On the other hand, $X \mid \exp X - 1$ in $k[[X]]$ (since $\exp X - 1 = \sum\limits_{j=1}^{\infty}\frac{X^j}{j!} = \sum\limits_{j=1}^{\infty}\frac{XX^{j-1}}{j!} = X\sum\limits_{j=1}^{\infty}\frac{X^{j-1}}{j!}$ is divisible by X), and thus $X^i \mid (\exp X - 1)^i$ in $k[[X]]$ for every $i \in \mathbb{N}$. Thus,

$$(\exp X - 1)^i \equiv 0 \bmod X^{n+1}k[[X]] \tag{17}$$

for every $i \in \mathbb{N}$ satisfying $i \geq n+1$ (because $i \geq n+1$ leads to $X^{n+1} \mid X^i \mid (\exp X - 1)^i$). Now,

$$X = \log(\exp X) = \sum_{i\geq 1}\frac{(-1)^{i-1}}{i}(\exp X - 1)^i \qquad \text{(by the definition of log)}$$

$$= \sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(\underbrace{\exp X - 1}_{\equiv \sum\limits_{j=1}^{n}\frac{X^j}{j!} \bmod X^{n+1}k[[X]]}\right)^i + \sum_{i=n+1}^{\infty}\frac{(-1)^{i-1}}{i}\underbrace{(\exp X - 1)^i}_{\substack{\equiv 0 \bmod X^{n+1}k[[X]] \\ \text{(by (17))}}}$$

$$\equiv \sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(\sum_{j=1}^{n}\frac{X^j}{j!}\right)^i + \underbrace{\sum_{i=n+1}^{\infty}\frac{(-1)^{i-1}}{i}0}_{=0}$$

$$= \sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(\sum_{j=1}^{n}\frac{X^j}{j!}\right)^i \bmod X^{n+1}k[[X]].$$

Thus, $X^{n+1} \mid X - \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{X^j}{j!} \right)^i$ in $k\left[\left[X\right]\right]$. This means that the coefficient of the power series $X - \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{X^j}{j!} \right)^i$ before X^λ is 0 for every $\lambda \in \{0, 1, \ldots, n\}$. But the power series $X - \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{X^j}{j!} \right)^i$ is actually a polynomial, so this rewrites as follows: The coefficient of the polynomial $X - \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{X^j}{j!} \right)^i$ before X^λ is 0 for every $\lambda \in \{0, 1, \ldots, n\}$. In other words, $X^{n+1} \mid X - \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{X^j}{j!} \right)^i$ in $k\left[X\right]$. Hence, there exists a polynomial $\mathbf{P} \in k\left[X\right]$ such that $X - \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{X^j}{j!} \right)^i = X^{n+1}\mathbf{P}$. Consider this polynomial $\mathbf{P}$.

Applying the polynomial identity $X - \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{X^j}{j!} \right)^i = X^{n+1}\mathbf{P}$ to a instead of X, we get

$$a - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{a^j}{j!} \right)^i = \underbrace{a^{n+1}}_{=0} \mathbf{P}\left(a\right) = 0,$$

so that $\sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} \left(\sum\limits_{j=1}^{n} \dfrac{a^j}{j!} \right)^i = a$. This proves Corollary 5.14 **(a)**.

(b) Consider the ring of power series $k\left[\left[X\right]\right]$. Clearly, $1 + X$ is a power series whose coefficient before X^0 is 1. Thus, applying Theorem 5.2 **(b)** to $P = 1 + X$, we obtain $\exp\left(\log\left(1 + X\right)\right) = 1 + X$. Now, in the ring $k\left[\left[X\right]\right]$, we have

$$\begin{aligned}
\log\left(1 + X\right) &= \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} \left(\underbrace{(1 + X) - 1}_{=X} \right)^i \qquad \text{(by the definition of log)} \\
&= \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} X^i = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} X^i + \sum_{i=n+1}^{\infty} \underbrace{\frac{(-1)^{i-1}}{i} X^i}_{\substack{\equiv 0 \bmod X^{n+1}k[[X]] \\ \text{(since } i \geq n+1 \text{ leads to} \\ X^i \equiv 0 \bmod X^{n+1}k[[X]]\text{)}}} \\
&\equiv \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} X^i + \underbrace{\sum_{i=n+1}^{\infty} 0}_{=0} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} X^i \bmod X^{n+1} k\left[\left[X\right]\right].
\end{aligned}$$

On the other hand,

$$1+X = \exp\left(\log\left(1+X\right)\right) = \sum_{j=0}^{\infty} \frac{\left(\log\left(1+X\right)\right)^j}{j!} \qquad \text{(by the definition of exp)}$$

$$= \underbrace{\frac{\left(\log\left(1+X\right)\right)^0}{0!}}_{=\frac{1}{1}=1} + \sum_{j=1}^{\infty} \frac{\left(\log\left(1+X\right)\right)^j}{j!} = 1 + \sum_{j=1}^{\infty} \frac{\left(\log\left(1+X\right)\right)^j}{j!}.$$

Subtracting 1 from this yields

$$X = \sum_{j=1}^{\infty} \frac{\left(\log\left(1+X\right)\right)^j}{j!}.$$

Since $X \mid \log\left(1+X\right)$ in $k\left[\left[X\right]\right]$ (because $\log\left(1+X\right) = \sum\limits_{i\geq 1} \frac{\left(-1\right)^{i-1}}{i} \underbrace{X^i}_{=XX^{i-1}} = X \sum\limits_{i\geq 1} \frac{\left(-1\right)^{i-1}}{i} X^{i-1}$ is divisible by X), we have $X^j \mid \left(\log\left(1+X\right)\right)^j$ for every $j \in \mathbb{N}$. Thus every $j \in \mathbb{N}$ such that $j \geq n+1$ satisfies

$$\left(\log\left(1+X\right)\right)^j \equiv 0 \bmod X^{n+1} k\left[\left[X\right]\right] \tag{18}$$

(since $j \geq n+1$ leads to $X^{n+1} \mid X^j \mid \left(\log\left(1+X\right)\right)^j$). Now,

$$X = \sum_{j=1}^{\infty} \frac{\left(\log\left(1+X\right)\right)^j}{j!} = \sum_{j=1}^{n} \frac{\left(\log\left(1+X\right)\right)^j}{j!} + \sum_{j=n+1}^{\infty} \underbrace{\frac{\left(\log\left(1+X\right)\right)^j}{j!}}_{\substack{\equiv 0 \bmod X^{n+1} k\left[\left[X\right]\right] \\ \text{(since } j \geq n+1 \text{ and thus} \\ \left(\log(1+X)\right)^j \equiv 0 \bmod X^{n+1} k\left[\left[X\right]\right] \\ \text{(by (18)))}}}$$

$$\equiv \sum_{j=1}^{n} \frac{\left(\log\left(1+X\right)\right)^j}{j!} + \underbrace{\sum_{j=n+1}^{\infty} 0}_{=0} = \sum_{j=1}^{n} \frac{\left(\log\left(1+X\right)\right)^j}{j!}$$

$$\equiv \sum_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i\right)^j}{j!} \bmod X^{n+1} k\left[\left[X\right]\right]$$

(since $\log\left(1+X\right) \equiv \sum\limits_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i \bmod X^{n+1} k\left[\left[X\right]\right]$). Thus, $X^{n+1} \mid X - \sum\limits_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i\right)^j}{j!}$ in $k\left[\left[X\right]\right]$. This means that the coefficient of the power series $X - \sum\limits_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i\right)^j}{j!}$ before X^λ is 0 for every $\lambda \in \{0, 1, \ldots, n\}$. But the power series $X - \sum\limits_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i\right)^j}{j!}$

is actually a polynomial, so this rewrites as follows: The coefficient of the polynomial $X - \sum_{j=1}^{n} \dfrac{\left(\sum_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!}$ before X^λ is 0 for every $\lambda \in \{0, 1, \ldots, n\}$. In other words, $X^{n+1} \mid X - \sum_{j=1}^{n} \dfrac{\left(\sum_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!}$ in $k[X]$. Hence, there exists a polynomial $\mathbf{Q} \in k[X]$ such that $X - \sum_{j=1}^{n} \dfrac{\left(\sum_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!} = X^{n+1}\mathbf{Q}$. Consider this polynomial $\mathbf{Q}$.

Applying the polynomial identity $X - \sum_{j=1}^{n} \dfrac{\left(\sum_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!} = X^{n+1}\mathbf{Q}$ to b instead of X, we get

$$b - \sum_{j=1}^{n} \frac{\left(\sum_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} b^i\right)^j}{j!} = \underbrace{b^{n+1}}_{=0} \mathbf{Q}(b) = 0,$$

so that $\sum_{j=1}^{n} \dfrac{\left(\sum_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} b^i\right)^j}{j!} = b$. This proves Corollary 5.14 **(b)**. □

Next, we shall show a very easy fact:

Proposition 5.15. Let k be a field. Let H be a filtered k-coalgebra. Then, $H_{\leq n}$ is a subcoalgebra of H for every $n \in \mathbb{N}$.

Proof of Proposition 5.15. Let $n \in \mathbb{N}$. Then, since H is a filtered k-coalgebra, we have

$$\Delta_H(H_{\leq n}) \subseteq \sum_{u=0}^{n} \underbrace{H_{\leq u}}_{\substack{\subseteq H_{\leq n} \\ (\text{since } u \leq n)}} \otimes \underbrace{H_{\leq n-u}}_{\substack{\subseteq H_{\leq n} \\ (\text{since } n-u \leq n)}} \subseteq \sum_{u=0}^{n} H_{\leq n} \otimes H_{\leq n} \subseteq H_{\leq n} \otimes H_{\leq n}$$

(since $H_{\leq n} \otimes H_{\leq n}$ is a k-vector space). Thus, $H_{\leq n}$ is a subcoalgebra of H. This proves Proposition 5.15. □

Now some triviality:

Proposition 5.16. Let k be a field. Let H be a k-coalgebra. Let J be a subcoalgebra of H. Let A be a k-algebra.

(a) Then, any $f \in \mathcal{L}(H, A)$ and any $g \in \mathcal{L}(H, A)$ satisfy $(f\mid_J) * (g\mid_J) = (f * g)\mid_J$.

(b) Also, any $f \in \mathcal{L}(H, A)$ and any $i \in \mathbb{N}$ satisfy $(f\mid_J)^{*i} = f^{*i}\mid_J$.

Proof of Proposition 5.16. **(a)** Any $f \in \mathcal{L}(H, A)$ and any $g \in \mathcal{L}(H, A)$ satisfy

$$(f \mid_J) * (g \mid_J) = \mu_A \circ \underbrace{((f \mid_J) \otimes (g \mid_J))}_{=(f \otimes g)|_{J \otimes J}} \circ \underbrace{\Delta_J}_{=\Delta_H|_J} \qquad \text{(by the definition of convolution)}$$
$$= \mu_A \circ ((f \otimes g) \mid_{J \otimes J}) \circ (\Delta_H \mid_J) = \underbrace{(\mu_A \circ (f \otimes g) \circ \Delta_H)}_{=f*g} \mid_J = (f * g) \mid_J .$$

This proves Proposition 5.16 **(a)**.

(b) Proposition 5.16 **(b)** easily follows from Proposition 5.16 **(a)** by induction over i.

This completes the proof of Proposition 5.16. □

Now let us give a proof of Proposition 5.13. (We will give another proof of Proposition 5.13 (and even of a more general fact: Proposition 14.3) in §14; it will avoid the use of Propositions 5.15 and 5.16.)

Proof of Proposition 5.13. **(a)** Let $f \in \mathfrak{g}(H, A)$. Let $n \in \mathbb{N}$. Proposition 5.15 yields that $H_{\leq n}$ is a subcoalgebra of H.

Let $g = e^{*f} - e_{H,A}$. Then, $g \in \mathfrak{g}(H, A)$ (since $e^{*f} \in G(H, A) = e_{H,A} + \mathfrak{g}(H, A)$, so that $e^{*f} - e_{H,A} \in \mathfrak{g}(H, A)$). Hence, Remark 3.5 (applied to g instead of f) yields $g^{*i}(H_{\leq n}) = 0$ for every $i > n$. Also, Remark 3.5 yields $f^{*i}(H_{\leq n}) = 0$ for every $i > n$.

We have

$$\operatorname{Log}\left(e^{*f}\right) = \operatorname{Log}_1 \underbrace{\left(e^{*f} - e_{H,A}\right)}_{=g} \qquad \text{(by the definition of Log)}$$
$$= \operatorname{Log}_1 g.$$

Thus, every $x \in H_{\leq n}$ satisfies

$$\left(\operatorname{Log}\left(e^{*f}\right)\right)(x) = \left(\operatorname{Log}_1 g\right)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} g^{*i}(x) \qquad \text{(by the definition of Log}_1\text{)}$$
$$= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} \underbrace{g^{*i}(x)}_{\substack{=0 \text{ (since} \\ x \in H_{\leq n} \text{ and thus} \\ g^{*i}(x) \in g^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{))}}}$$
$$= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \underbrace{\sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} 0}_{=0} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x).$$

In other words,

$$\operatorname{Log}\left(e^{*f}\right) \mid_{H_{\leq n}} = \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right) \mid_{H_{\leq n}} .$$

Since

$$\left(\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}g^{*i}\right)|_{H_{\leq n}}=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\underbrace{\left(g^{*i}|_{H_{\leq n}}\right)}_{=\left(g|_{H_{\leq n}}\right)^{*i}}=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(g|_{H_{\leq n}}\right)^{*i},$$

(because Proposition 5.16 **(b)** (applied to $H_{\leq n}$ and g instead of J and f) yields $\left(g|_{H_{\leq n}}\right)^{*i}=g^{*i}|_{H_{\leq n}}$)

this rewrites as

$$\operatorname{Log}\left(e^{*f}\right)|_{H_{\leq n}}=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(g|_{H_{\leq n}}\right)^{*i}.$$

But every $x\in H_{\leq n}$ satisfies

$$e^{*f}(x)=\sum_{i\geq 0}\frac{f^{*i}(x)}{i!}=\sum_{i=0}^{n}\frac{f^{*i}(x)}{i!}+\sum_{i=n+1}^{\infty}\underbrace{\frac{f^{*i}(x)}{i!}}_{\substack{=0 \text{ (since } x\in H_{\leq n} \text{ and thus} \\ f^{*i}(x)\in f^{*i}\left(H_{\leq n}\right)=0 \\ \text{(since } i>n\text{), so that} \\ f^{*i}(x)=0)}}=\sum_{i=0}^{n}\frac{f^{*i}(x)}{i!}+\underbrace{\sum_{i=n+1}^{\infty}0}_{=0}$$

$$=\sum_{i=0}^{n}\frac{f^{*i}(x)}{i!}=\underbrace{\frac{f^{*0}(x)}{0!}}_{=\frac{e_{H,A}(x)}{1}=e_{H,A}(x)}+\sum_{i=1}^{n}\frac{f^{*i}(x)}{i!}=e_{H,A}(x)+\sum_{i=1}^{n}\frac{f^{*i}(x)}{i!}$$

and thus

$$\underbrace{g}_{=e^{*f}-e_{H,A}}(x)=\left(e^{*f}-e_{H,A}\right)(x)=\underbrace{e^{*f}(x)}_{=e_{H,A}(x)+\sum_{i=1}^{n}\frac{f^{*i}(x)}{i!}}-e_{H,A}(x)=\sum_{i=1}^{n}\frac{f^{*i}(x)}{i!}=\sum_{i=1}^{n}\frac{f^{*i}}{i!}(x)$$

$$=\sum_{j=1}^{n}\frac{f^{*j}}{j!}(x)\qquad\text{(here, we substituted } j \text{ for } i \text{ in the sum)}.$$

In other words,

$$g|_{H_{\leq n}}=\left(\sum_{j=1}^{n}\frac{f^{*j}}{j!}\right)|_{H_{\leq n}}=\sum_{j=1}^{n}\frac{f^{*j}|_{H_{\leq n}}}{j!}$$

$$=\sum_{j=1}^{n}\frac{\left(f|_{H_{\leq n}}\right)^{*j}}{j!}$$

$$\left(\begin{array}{c}\text{since Proposition 5.16 } \mathbf{(b)} \text{ (applied to } H_{\leq n} \text{ and } j \text{ instead of } J \text{ and } i) \\ \text{yields } \left(f|_{H_{\leq n}}\right)^{*j}=f^{*j}|_{H_{\leq n}}\text{, so that } f^{*j}|_{H_{\leq n}}=\left(f|_{H_{\leq n}}\right)^{*j}\end{array}\right).$$

Now,

$$\operatorname{Log}\left(e^{*f}\right)|_{H_{\leq n}} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\underbrace{g|_{H_{\leq n}}}_{= \sum_{j=1}^{n} \frac{\left(f|_{H_{\leq n}}\right)^{*j}}{j!}} \right)^{*i} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{\left(f|_{H_{\leq n}}\right)^{*j}}{j!} \right)^{*i}. \tag{19}$$

But $n+1 > n$. Hence, Remark 3.5 (applied to $i = n+1$) yields $f^{*(n+1)}(H_{\leq n}) = 0$. Since

$$\begin{aligned} \left(f|_{H_{\leq n}}\right)^{*(n+1)} &= f^{*(n+1)}|_{H_{\leq n}} \qquad \left(\begin{array}{c} \text{by Proposition 5.16 } \mathbf{(b)} \\ \text{(applied to } H_{\leq n} \text{ and } n+1 \text{ instead of } J \text{ and } i) \end{array} \right) \\ &= 0 \qquad \left(\text{since } f^{*(n+1)}(H_{\leq n}) = 0\right), \end{aligned}$$

we can apply Corollary 5.14 **(a)** to $a = f|_{H_{\leq n}}$ and obtain $\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{\left(f|_{H_{\leq n}}\right)^{*j}}{j!} \right)^{*i} = f|_{H_{\leq n}}$. Thus, (19) becomes

$$\operatorname{Log}\left(e^{*f}\right)|_{H_{\leq n}} = f|_{H_{\leq n}}.$$

We have thus proven this for every $n \in \mathbb{N}$.

Now, let $x \in H$ be arbitrary. Since H is filtered, there must exist some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$. Consider this n. From $x \in H_{\leq n}$, we obtain

$$\left(\operatorname{Log}\left(e^{*f}\right)\right)(x) = \underbrace{\left(\operatorname{Log}\left(e^{*f}\right)|_{H_{\leq n}}\right)}_{= f|_{H_{\leq n}}}(x) = \left(f|_{H_{\leq n}}\right)(x) = f(x).$$

Since this holds for every $x \in H$, we can now conclude that $\operatorname{Log}\left(e^{*f}\right) = f$.

This proves Proposition 5.13 **(a)**.

(b) Let $F \in G(H, A)$. Let $n \in \mathbb{N}$. Proposition 5.15 yields that $H_{\leq n}$ is a subcoalgebra of H.

Let $g = F - e_{H,A}$. Then, $g \in \mathfrak{g}(H, A)$ (since $F \in G(H, A) = e_{H,A} + \mathfrak{g}(H, A)$, so that $F - e_{H,A} \in \mathfrak{g}(H, A)$). Hence, Remark 3.5 (applied to g instead of f) yields $g^{*i}(H_{\leq n}) = 0$ for every $i > n$.

Let $\varphi = \operatorname{Log} F$. Then, $\varphi \in \mathfrak{g}(H, A)$, so that Remark 3.5 (applied to φ instead of f) yields $\varphi^{*i}(H_{\leq n}) = 0$ for every $i > n$.

By the definition of Log, we have $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{H,A})}_{=g} = \operatorname{Log}_1 g$. Hence, $\varphi = \operatorname{Log} f = \operatorname{Log}_1 g$.

Thus, every $x \in H_{\leq n}$ satisfies

$$\begin{aligned}
\varphi(x) &= (\operatorname{Log}_1 g)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} g^{*i}(x) \qquad \text{(by the definition of } \operatorname{Log}_1\text{)} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} \underbrace{g^{*i}(x)}_{\substack{=0 \text{ (since} \\ x \in H_{\leq n} \text{ and thus} \\ g^{*i}(x) \in g^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{))}}} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \underbrace{\sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} 0}_{=0} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x).
\end{aligned}$$

In other words,

$$\varphi\,|_{H_{\leq n}} = \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}}.$$

Since

$$\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \underbrace{\left(g^{*i}\,|_{H_{\leq n}}\right)}_{\substack{= \left(g|_{H_{\leq n}}\right)^{*i} \text{ (because Proposition 5.16 } \mathbf{(b)} \\ \text{(applied to } H_{\leq n} \text{ and } g \text{ instead of} \\ J \text{ and } f\text{) yields } \left(g|_{H_{\leq n}}\right)^{*i} = g^{*i}|_{H_{\leq n}}\text{)}}} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(g\,|_{H_{\leq n}}\right)^{*i},$$

this rewrites as

$$\varphi\,|_{H_{\leq n}} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(g\,|_{H_{\leq n}}\right)^{*i}.$$

But every $x \in H_{\leq n}$ satisfies

$$\begin{aligned}
e^{*\varphi}(x) &= \sum_{i \geq 0} \frac{\varphi^{*i}(x)}{i!} = \sum_{i=0}^{n} \frac{\varphi^{*i}(x)}{i!} + \sum_{i=n+1}^{\infty} \underbrace{\frac{\varphi^{*i}(x)}{i!}}_{\substack{=0 \text{ (since} \\ x \in H_{\leq n} \text{ and thus} \\ \varphi^{*i}(x) \in \varphi^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{), so that} \\ \varphi^{*i}(x) = 0\text{)}}} = \sum_{i=0}^{n} \frac{\varphi^{*i}(x)}{i!} + \underbrace{\sum_{i=n+1}^{\infty} 0}_{=0} = \sum_{i=0}^{n} \frac{\varphi^{*i}(x)}{i!} \\
&= \underbrace{\frac{\varphi^{*0}(x)}{0!}}_{= \frac{e_{H,A}(x)}{1} = e_{H,A}(x)} + \sum_{i=1}^{n} \frac{\varphi^{*i}(x)}{i!} = e_{H,A}(x) + \sum_{i=1}^{n} \frac{\varphi^{*i}(x)}{i!}
\end{aligned}$$

and thus

$$(e^{*\varphi} - e_{H,A})(x) = \underbrace{e^{*\varphi}(x)}_{=e_{H,A}(x)+\sum_{i=1}^{n}\frac{\varphi^{*i}(x)}{i!}} - e_{H,A}(x) = \sum_{i=1}^{n}\frac{\varphi^{*i}(x)}{i!} = \sum_{i=1}^{n}\frac{\varphi^{*i}}{i!}(x)$$

$$= \sum_{j=1}^{n}\frac{\varphi^{*j}}{j!}(x) \qquad \text{(here, we substituted } j \text{ for } i \text{ in the sum)}.$$

In other words,

$$\begin{aligned}
&(e^{*\varphi} - e_{H,A})\mid_{H_{\leq n}} \\
&= \left(\sum_{j=1}^{n}\frac{\varphi^{*j}}{j!}\right)\mid_{H_{\leq n}} = \sum_{j=1}^{n}\frac{\varphi^{*j}\mid_{H_{\leq n}}}{j!} \\
&= \sum_{j=1}^{n}\frac{\left(\varphi\mid_{H_{\leq n}}\right)^{*j}}{j!} \\
&\qquad \left(\begin{array}{c}\text{since Proposition 5.16 } \mathbf{(b)} \text{ (applied to } \varphi, H_{\leq n} \text{ and } j \text{ instead of } f, J \text{ and } i)\\ \text{yields } \left(\varphi\mid_{H_{\leq n}}\right)^{*j} = \varphi^{*j}\mid_{H_{\leq n}}, \text{ so that } \varphi^{*j}\mid_{H_{\leq n}} = \left(\varphi\mid_{H_{\leq n}}\right)^{*j}\end{array}\right) \\
&= \sum_{j=1}^{n}\frac{\left(\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(g\mid_{H_{\leq n}}\right)^{*i}\right)^{*j}}{j!} \qquad \left(\text{since } \varphi\mid_{H_{\leq n}} = \sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(g\mid_{H_{\leq n}}\right)^{*i}\right).
\end{aligned} \tag{20}$$

But Remark 3.5 (applied to $n+1$ and g instead of i and f) yields $g^{*(n+1)}(H_{\leq n}) = 0$ (since $n+1 > n$). Since

$$\begin{aligned}
&\left(g\mid_{H_{\leq n}}\right)^{*(n+1)} \\
&= g^{*(n+1)}\mid_{H_{\leq n}} \qquad \left(\begin{array}{c}\text{by Proposition 5.16 } \mathbf{(b)}\\ \text{(applied to } g, H_{\leq n} \text{ and } n+1 \text{ instead of } f, J \text{ and } i)\end{array}\right) \\
&= 0 \qquad \left(\text{since } g^{*(n+1)}(H_{\leq n}) = 0\right),
\end{aligned}$$

we can apply Corollary 5.14 **(b)** to $b = g\mid_{H_{\leq n}}$ and obtain $\sum_{j=1}^{n}\frac{\left(\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}\left(g\mid_{H_{\leq n}}\right)^{*i}\right)^{*j}}{j!} = g\mid_{H_{\leq n}}$. Thus, (20) becomes

$$\begin{aligned}
(e^{*\varphi} - e_{H,A})\mid_{H_{\leq n}} &= g\mid_{H_{\leq n}} = (F - e_{H,A})\mid_{H_{\leq n}} \qquad (\text{since } g = F - e_{H,A}) \\
&= F\mid_{H_{\leq n}} - e_{H,A}\mid_{H_{\leq n}}.
\end{aligned}$$

Since $(e^{*\varphi} - e_{H,A})\mid_{H_{\leq n}} = e^{*\varphi}\mid_{H_{\leq n}} - e_{H,A}\mid_{H_{\leq n}}$, this rewrites as $e^{*\varphi}\mid_{H_{\leq n}} - e_{H,A}\mid_{H_{\leq n}} = F\mid_{H_{\leq n}} - e_{H,A}\mid_{H_{\leq n}}$. Thus, $e^{*\varphi}\mid_{H_{\leq n}} = F\mid_{H_{\leq n}}$. Since $\varphi = \operatorname{Log} F$, this becomes $e^{*(\operatorname{Log} F)}\mid_{H_{\leq n}} = F\mid_{H_{\leq n}}$. We have thus proven this for every $n \in \mathbb{N}$.

Now, let $x \in H$ be arbitrary. Since H is filtered, there must exist some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$. Consider this n. From $x \in H_{\leq n}$, we obtain

$$e^{*(\operatorname{Log} F)}(x) = \underbrace{\left(e^{*(\operatorname{Log} F)} \mid_{H_{\leq n}}\right)}_{=F\mid_{H_{\leq n}}}(x) = \left(F \mid_{H_{\leq n}}\right)(x) = F(x).$$

Since this holds for every $x \in H$, we can now conclude that $e^{*(\operatorname{Log} F)} = F$.

This proves Proposition 5.13 **(b)**. □

§6. Some properties of primitive elements

Next let us recall the definition of a primitive element:

Definition 6.1. Let k be a field. Let H be a unital coalgebra. Let $x \in H$ be an element. The element x is said to be *primitive* if $\Delta(x) = x \otimes 1_H + 1_H \otimes x$. Here, $1_H \in H$ denotes the unity of the unital coalgebra H (as defined in Definition 2.1).

Remark. Some authors define the notion of primitivity slightly differently: they define an element $x \in H$ to be *primitive* if $\Delta(x) = x \otimes 1_H + 1_H \otimes x$ and $\varepsilon(x) = 0$. However, this definition of "primitive" turns out to be equivalent to our Definition 6.1. This is because every element $x \in H$ which is primitive in the sense of Definition 6.1 satisfies $\Delta(x) = x \otimes 1_H + 1_H \otimes x$ and $\varepsilon(x) = 0$ (by Remark 6.3), and conversely, every element $x \in H$ satisfying $\Delta(x) = x \otimes 1_H + 1_H \otimes x$ and $\varepsilon(x) = 0$ is clearly primitive in the sense of Definition 6.1.

Next we show:

Proposition 6.2. Let k be a field, let A be a k-algebra, and let H be a unital coalgebra. Let $\operatorname{Prim} H$ denote the set of all primitive elements of H.

(a) Any $f \in \mathfrak{g}(H, A)$ and any $g \in \mathfrak{g}(H, A)$ satisfy $f * g \in \mathfrak{g}(H, A)$ and $(f * g)(\operatorname{Prim} H) = 0$.

(b) Every $f \in \mathfrak{g}(H, A)$ satisfies $f^{*i} \in \mathfrak{g}(H, A)$ and $f^{*i}(\operatorname{Prim} H) = 0$ for every integer $i > 1$.

(c) Assume that the field k has characteristic 0, and that H is a connected filtered k-coalgebra. Then, every $F \in G(H, A)$ satisfies $(\operatorname{Log} F) \mid_{\operatorname{Prim} H} = F \mid_{\operatorname{Prim} H}$.

Before we prove this, let us show a very easy (and classical) observation about primitive elements:

Remark 6.3. Let k be a field. Let H be a unital coalgebra. Then, $\varepsilon(x) = 0$ for every $x \in \operatorname{Prim} H$.

Proof of Remark 6.3. Recall that the unity of the unital coalgebra H is denoted by 1_H. Thus, $(H, 1_H)$ is a unital coalgebra. Hence, by the definition of a unital coalgebra, we have $\Delta_H(1_H) = 1_H \otimes 1_H$ and $\varepsilon_H(1_H) = 1$. Since we abbreviate ε_H as ε, we have $\varepsilon(1_H) = \varepsilon_H(1_H) = 1$.

Let $x \in \operatorname{Prim} H$. Then, x is primitive (by the definition of $\operatorname{Prim} H$). In other words, $\Delta(x) = x \otimes 1_H + 1_H \otimes x$.

Now, let $\operatorname{can} : H \otimes k \to H$ be the canonical k-module isomorphism (sending $c \otimes x$ to cx for all $c \in H$ and $x \in k$). Then, by the axioms of a coalgebra, we have $\operatorname{can} \circ (\operatorname{id} \otimes \varepsilon) \circ \Delta = \operatorname{id}$. But

$$\begin{aligned}
(\operatorname{can} \circ (\operatorname{id} \otimes \varepsilon) \circ \Delta)(x) &= \operatorname{can}\left((\operatorname{id} \otimes \varepsilon)\left(\underbrace{\Delta(x)}_{=x\otimes 1_H + 1_H \otimes x}\right)\right) = \operatorname{can}\left(\underbrace{(\operatorname{id} \otimes \varepsilon)(x \otimes 1_H + 1_H \otimes x)}_{=\operatorname{id}(x)\otimes\varepsilon(1_H)+\operatorname{id}(1_H)\otimes\varepsilon(x)}\right) \\
&= \operatorname{can}(\operatorname{id}(x) \otimes \varepsilon(1_H) + \operatorname{id}(1_H) \otimes \varepsilon(x)) \\
&= \underbrace{\operatorname{id}(x)}_{=x} \cdot \underbrace{\varepsilon(1_H)}_{=1} + \underbrace{\operatorname{id}(1_H)}_{=1_H} \cdot \varepsilon(x) \qquad \text{(by the definition of can)} \\
&= x + 1_H \cdot \varepsilon(x).
\end{aligned}$$

Comparing this with $\left(\underbrace{\operatorname{can} \circ (\operatorname{id} \otimes \varepsilon) \circ \Delta}_{=\operatorname{id}}\right)(x) = \operatorname{id}(x) = x$, we obtain $x + 1_H \cdot \varepsilon(x) = x$. Thus, $1_H \cdot \varepsilon(x) = 0$. Hence, $\varepsilon(1_H \cdot \varepsilon(x)) = 0$. Since $\varepsilon(1_H \cdot \varepsilon(x)) = \underbrace{\varepsilon(1_H)}_{=1} \cdot \varepsilon(x) = \varepsilon(x)$, this rewrites as $\varepsilon(x) = 0$. This proves Remark 6.3. $\square$

Proof of Proposition 6.2. Recall that the unity of the unital coalgebra H is denoted by 1_H. Thus, $(H, 1_H)$ is a unital coalgebra. Hence, by the definition of a unital coalgebra, we have $\Delta_H(1_H) = 1_H \otimes 1_H$ and $\varepsilon_H(1_H) = 1$. Since we abbreviate Δ_H by Δ, we have $\Delta(1_H) = \Delta_H(1_H) = 1_H \otimes 1_H$.

(a) Let $x \in \operatorname{Prim} H$. Then, x is a primitive element of H (since $\operatorname{Prim} H$ is the set of all primitive elements of H). In other words, $\Delta(x) = x \otimes 1_H + 1_H \otimes x$. But by the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta$. Thus,

$$\begin{aligned}
(f * g)(x) &= (\mu_A \circ (f \otimes g) \circ \Delta)(x) = \mu_A\left((f \otimes g)\ \underbrace{(\Delta(x))}_{=x\otimes 1_H + 1_H \otimes x}\right) \\
&= \mu_A\left(\underbrace{(f \otimes g)(x \otimes 1_H + 1_H \otimes x)}_{=f(x)\otimes g(1_H)+f(1_H)\otimes g(x)}\right) \\
&= \mu_A\left(f(x) \otimes \underbrace{g(1_H)}_{\substack{=0 \\ (\text{since } g\in\mathfrak{g}(H,A))}} + \underbrace{f(1_H)}_{\substack{=0 \\ (\text{since } f\in\mathfrak{g}(H,A))}} \otimes g(x)\right) \\
&= \mu_A\left(\underbrace{f(x) \otimes 0 + 0 \otimes g(x)}_{=0}\right) = 0.
\end{aligned}$$

Since this holds for every $x \in \operatorname{Prim} H$, we thus get $(f * g)(\operatorname{Prim} H) = 0$.

Besides, $f * g = \mu_A \circ (f \otimes g) \circ \Delta$ leads to

$$(f*g)(1_H) = (\mu_A \circ (f \otimes g) \circ \Delta)(1_H) = \mu_A\left((f \otimes g)\underbrace{(\Delta(1_H))}_{=1_H \otimes 1_H}\right) = \mu_A\left(\underbrace{(f \otimes g)(1_H \otimes 1_H)}_{=f(1_H)\otimes g(1_H)}\right)$$

$$= \mu_A\left(\underbrace{f(1_H)}_{\substack{=0 \\ (\text{since } f \in \mathfrak{g}(H,A))}} \otimes \underbrace{g(1_H)}_{\substack{=0 \\ (\text{since } g \in \mathfrak{g}(H,A))}}\right) = \mu_A(0 \otimes 0) = 0.$$

Thus, $f * g \in \mathfrak{g}(H,A)$ (by the definition of $\mathfrak{g}(H,A)$).

This proves Proposition 6.2 **(a)**.

(b) We will prove Proposition 6.2 **(b)** by induction over i:

Induction base: Proposition 6.2 **(a)** (applied to $g = f$) yields $f * f \in \mathfrak{g}(H,A)$ and $(f*f)(\operatorname{Prim} H) = 0$. Since $f*f = f^{*2}$, this rewrites as follows: We have $f^{*2} \in \mathfrak{g}(H,A)$ and $f^{*2}(\operatorname{Prim} H) = 0$. This proves Proposition 6.2 **(b)** for $i = 2$. The induction base is thus complete.

Induction step: Let $j > 1$ be an integer. Assume that Proposition 6.2 **(b)** holds for $i = j$. We must then prove Proposition 6.2 **(b)** for $i = j + 1$.

Since Proposition 6.2 **(b)** holds for $i = j$, we have $f^{*j} \in \mathfrak{g}(H,A)$ and $f^{*j}(\operatorname{Prim} H) = 0$. Now, Proposition 6.2 **(a)** (applied to $g = f^{*j}$) yields $f * f^{*j} \in \mathfrak{g}(H,A)$ and $(f * f^{*j})(\operatorname{Prim} H) = 0$. Since $f * f^{*j} = f^{*(j+1)}$, this rewrites as follows: We have $f^{*(j+1)} \in \mathfrak{g}(H,A)$ and $f^{*(j+1)}(\operatorname{Prim} H) = 0$. In other words, Proposition 6.2 **(b)** holds for $i = j + 1$. The induction step is thus complete.

This completes the induction proof of Proposition 6.2 **(b)**.

(c) Let $F \in G(H,A)$.

Let $f = F - e_{H,A}$. Then, $f \in \mathfrak{g}(H,A)$ (since $F \in G(H,A) = e_{H,A} + \mathfrak{g}(H,A)$, so that $F - e_{H,A} \in \mathfrak{g}(H,A)$). Proposition 6.2 **(b)** thus yields $f^{*i}(\operatorname{Prim} H) = 0$ for every integer $i > 1$.

Now, the definition of Log says that $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{H,A})}_{=f} = \operatorname{Log}_1 f$.

Let $x \in \operatorname{Prim} H$. Then, $f^{*i}(x) \in f^{*i}(\operatorname{Prim} H) = 0$ for every integer $i > 1$. In other words, $f^{*i}(x) = 0$ for every integer $i > 1$. On the other hand, $\varepsilon(x) = 0$ (by Remark 6.3), so that $\underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_H}(x) = (\eta_A \circ \varepsilon_H)(x) = \eta_A\left(\underbrace{\varepsilon_H(x)}_{=\varepsilon(x)=0}\right) = 0$. Thus, $F(x) - e_{H,A}(x) = F(x)$. Since $F(x) - e_{H,A}(x) = \underbrace{(F - e_{H,A})}_{=f}(x) = f(x)$, this rewrites as $f(x) = F(x)$. Now,

$$\underbrace{(\operatorname{Log} F)}_{=\operatorname{Log}_1 f}(x) = (\operatorname{Log}_1 f)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) = \underbrace{\frac{(-1)^{1-1}}{1}}_{=1} f^{*1}(x) + \sum_{i>1} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{=0}$$

$$= \underbrace{1 f^{*1}(x)}_{=f^{*1}(x)=f(x)} + \underbrace{\sum_{i>1} \frac{(-1)^{i-1}}{i} 0}_{=0} = f(x) = F(x).$$

Since this holds for every $x \in \operatorname{Prim} H$, we thus conclude that $(\operatorname{Log} F)\mid_{\operatorname{Prim} H} = F\mid_{\operatorname{Prim} H}$. This proves Proposition 6.2 **(c)**. $\square$

§7. $(\varepsilon, \varepsilon)$-coderivations

We now introduce the notion of an $(\varepsilon, \varepsilon)$-*coderivation*. This notion can be defined in two ways; we are going to take the one that is more similar to the notion of an $(\varepsilon, \varepsilon)$-derivation[28] as definition, and then prove the equivalence to the other one as a theorem (Theorem 7.2).

Definition 7.1. Let k be a field. Let C be a k-coalgebra. Let H be a unital coalgebra. Let $f : C \to H$ be a k-linear map. Then, f is said to be an $(\varepsilon, \varepsilon)$-*coderivation* if and only if $\Delta_H \circ f = (f \otimes e_{C,H} + e_{C,H} \otimes f) \circ \Delta_C$. Here, the map $e_{C,H}$ is defined to be the map $\eta_H \circ \varepsilon_C : C \to H$ (this definition of the map $e_{C,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 2.14).

The following theorem shows how we can actually think of coderivations:

Theorem 7.2. Let k be a field. Let C be a k-coalgebra. Let H be a unital coalgebra. We denote by $\operatorname{Prim} H$ the set of all primitive elements of H. Let $f : C \to H$ be a k-linear map. Then, f is an $(\varepsilon, \varepsilon)$-coderivation if and only if $f(C) \subseteq \operatorname{Prim} H$.

Before we prove this, we recall a familiar fact from basic algebra:

$$\left(\begin{array}{c} \text{Any six } k\text{-vector spaces } U,\ V,\ W,\ U',\ V' \text{ and } W' \\ \text{and any four } k\text{-linear maps } \alpha : U \to V,\ \beta : V \to W,\ \alpha' : U' \to V' \\ \text{and } \beta' : V' \to W' \text{ satisfy } (\beta \circ \alpha) \otimes (\beta' \circ \alpha') = (\beta \otimes \beta') \circ (\alpha \otimes \alpha') . \end{array} \right) \tag{21}$$

Proof of Theorem 7.2. **a)** First, let us show that every $x \in C$ satisfies

$$((f \otimes e_{C,H} + e_{C,H} \otimes f) \circ \Delta_C)(x) = f(x) \otimes 1_H + 1_H \otimes f(x) . \tag{22}$$

(This holds no matter whether f is an $(\varepsilon, \varepsilon)$-coderivation or not, and whether $f(C) \subseteq \operatorname{Prim} H$ or not.)

Proof. First it is clear that every $x \in C$ satisfies $(\varepsilon_C \otimes \mathrm{id})(\Delta_C(x)) = 1 \otimes x$ [29]. Since $e_{C,H} = \eta_H \circ \varepsilon_C$ and $f = f \circ \mathrm{id}$, we have

$$e_{C,H} \otimes f = (\eta_H \circ \varepsilon_C) \otimes (f \circ \mathrm{id}) = (\eta_H \otimes f) \circ (\varepsilon_C \otimes \mathrm{id}) \\ (\text{by an application of (21)}) ,$$

[28] The notion of an $(\varepsilon, \varepsilon)$-derivation is a known one; we recall its definition in §15 (Definitions 15.6 and 15.7). Note that we speak of "$(\varepsilon_H, \varepsilon_H)$-derivations" instead of "$(\varepsilon, \varepsilon)$-derivations" for reasons of pedantry.

[29] *Proof.* Let $x \in C$. Let $\mathrm{kan} : C \to k \otimes C$ be the canonical isomorphism which sends every $y \in C$ to $1 \otimes y$. Then, by the axioms of a coalgebra, we have $(\varepsilon_C \otimes \mathrm{id}) \circ \Delta_C = \mathrm{kan}$ (since C is a coalgebra), and $(\varepsilon_C \otimes \mathrm{id})(\Delta_C(x)) = \underbrace{((\varepsilon_C \otimes \mathrm{id}) \circ \Delta_C)}_{=\mathrm{kan}}(x) = \mathrm{kan}(x) = 1 \otimes x$ (by the definition of kan), qed.

so that every $x \in C$ satisfies

$$\begin{aligned}\left(e_{C,H} \otimes f\right)\left(\Delta_C\left(x\right)\right) &= \left(\left(\eta_H \otimes f\right) \circ \left(\varepsilon_C \otimes \mathrm{id}\right)\right)\left(\Delta_C\left(x\right)\right) = \left(\eta_H \otimes f\right)\left(\underbrace{\left(\varepsilon_C \otimes \mathrm{id}\right)\left(\Delta_C\left(x\right)\right)}_{=1\otimes x}\right) \\ &= \left(\eta_H \otimes f\right)\left(1 \otimes x\right) = \underbrace{\eta_H\left(1\right)}_{\substack{=1\cdot 1_H \\ \text{(by the definition of } \eta_H\text{)}}} \otimes f\left(x\right) = \underbrace{1 \cdot 1_H}_{=1_H} \otimes f\left(x\right) = 1_H \otimes f\left(x\right).\end{aligned}$$

The same argument (but with permuted tensorands) shows that every $x \in C$ satisfies

$$\left(f \otimes e_{C,H}\right)\left(\Delta_C\left(x\right)\right) = f\left(x\right) \otimes 1_H.$$

Now, every $x \in C$ satisfies

$$\begin{aligned}\left(\left(f \otimes e_{C,H} + e_{C,H} \otimes f\right) \circ \Delta_C\right)\left(x\right) &= \left(f \otimes e_{C,H} + e_{C,H} \otimes f\right)\left(\Delta_C\left(x\right)\right) \\ &= \underbrace{\left(f \otimes e_{C,H}\right)\left(\Delta_C\left(x\right)\right)}_{=f(x)\otimes 1_H} + \underbrace{\left(e_{C,H} \otimes f\right)\left(\Delta_C\left(x\right)\right)}_{=1_H\otimes f(x)} \\ &= f\left(x\right) \otimes 1_H + 1_H \otimes f\left(x\right).\end{aligned}$$

This proves (22). Thus, **a)** is proven.

b) Now, let us prove that if f is an $(\varepsilon, \varepsilon)$-coderivation, then $f\left(C\right) \subseteq \operatorname{Prim} H$.

Proof. Assume that f is an $(\varepsilon, \varepsilon)$-coderivation. Then, $\Delta_H \circ f = \left(f \otimes e_{C,H} + e_{C,H} \otimes f\right) \circ \Delta_C$ (by the definition of an $(\varepsilon, \varepsilon)$-coderivation, since f is an $(\varepsilon, \varepsilon)$-coderivation).

Using (22), it is easy to see that every $y \in f\left(C\right)$ satisfies $y \in \operatorname{Prim} H$. [30] In other words, $f\left(C\right) \subseteq \operatorname{Prim} H$. This proves **b)**.

c) Now, let us prove that if $f\left(C\right) \subseteq \operatorname{Prim} H$, then f is an $(\varepsilon, \varepsilon)$-coderivation.

Proof. Assume that $f\left(C\right) \subseteq \operatorname{Prim} H$. Then, for every $x \in C$, the element $f\left(x\right) \in H$ is primitive (since $x \in C$ and thus $f\left(x\right) \in f\left(C\right) \subseteq \operatorname{Prim} H =$ (the set of all primitive elements of H)). Now, for every $x \in C$, we have

$$\begin{aligned}&\left(\Delta_H \circ f\right)\left(x\right) \\ &= \Delta_H\left(f\left(x\right)\right) = f\left(x\right) \otimes 1_H + 1_H \otimes f\left(x\right) \\ &\qquad \left(\begin{array}{c}\text{since } f\left(x\right) \text{ is primitive, and since a primitive element of } H \text{ was defined} \\ \text{as an element } z \in H \text{ satisfying } \Delta_H\left(z\right) = z \otimes 1_H + 1_H \otimes z\end{array}\right) \\ &= \left(\left(f \otimes e_{C,H} + e_{C,H} \otimes f\right) \circ \Delta_C\right)\left(x\right) \qquad \text{(by (22))}.\end{aligned}$$

[30] *Proof.* Let $y \in f\left(C\right)$. Then, there exists some $x \in C$ such that $y = f\left(x\right)$. Consider this x. Then,

$$\begin{aligned}\Delta_H\left(y\right) = \Delta_H\left(f\left(x\right)\right) &= \underbrace{\left(\Delta_H \circ f\right)}_{=\left(f\otimes e_{C,H} + e_{C,H}\otimes f\right)\circ\Delta_C}\left(x\right) = \left(\left(f \otimes e_{C,H} + e_{C,H} \otimes f\right) \circ \Delta_C\right)\left(x\right) \\ &= \underbrace{f\left(x\right)}_{=y} \otimes 1_H + 1_H \otimes \underbrace{f\left(x\right)}_{=y} \qquad \text{(by (22))} \\ &= y \otimes 1_H + 1_H \otimes y.\end{aligned}$$

But this yields that y is primitive (because a primitive element of H was defined as an element $z \in H$ satisfying $\Delta_H\left(z\right) = z \otimes 1_H + 1_H \otimes z$). In other words, $y \in \operatorname{Prim} H$ (since $\operatorname{Prim} H$ is the set of all primitive elements of H), qed.

Thus, $\Delta_H \circ f = (f \otimes e_{C,H} + e_{C,H} \otimes f) \circ \Delta_C$. In other words, f is an $(\varepsilon, \varepsilon)$-coderivation (because this is how $(\varepsilon, \varepsilon)$-coderivations were defined). This proves **c)**.

d) Combining the results of **b)** and **c)**, we see that f is an $(\varepsilon, \varepsilon)$-coderivation if and only if $f(C) \subseteq \operatorname{Prim} H$. Theorem 7.2 is thus proven. $\square$

§8. The exponent-logarithm bijection between $(\varepsilon, \varepsilon)$-coderivations and coalgebra homomorphisms

We are now ready to formulate a fact which will give us a major part of Theorem 4.1, and is of significant interest in its own:

Theorem 8.1. Let k be a field of characteristic 0. Let C be a connected filtered cocommutative k-coalgebra. Let H be a k-bialgebra. Let $f \in \mathfrak{g}(C, H)$. Then, f is an $(\varepsilon, \varepsilon)$-coderivation if and only if e^{*f} is a k-coalgebra homomorphism.

Being an "if and only if" statement, the assertion of this theorem splits into two parts, which we will now formulate as two independent lemmas:

Lemma 8.2. Let k be a field of characteristic 0. Let C be a connected filtered cocommutative k-coalgebra. Let H be a k-bialgebra. Let $f \in \mathfrak{g}(C, H)$. If f is an $(\varepsilon, \varepsilon)$-coderivation, then e^{*f} is a k-coalgebra homomorphism.

Lemma 8.3. Let k be a field of characteristic 0. Let C be a connected filtered cocommutative k-coalgebra. Let H be a k-bialgebra. Let $f \in \mathfrak{g}(C, H)$. If e^{*f} is a k-coalgebra homomorphism, then f is an $(\varepsilon, \varepsilon)$-coderivation.

Of these two lemmas, only one will be used in the proof of Theorem 4.1 - namely, Lemma 8.3. However, both of them are interesting and we will prove both for the sake of completeness.

§9. The "$(\varepsilon, \varepsilon)$-coderivation $\Longrightarrow$ coalgebra homomorphism" direction

First let us prepare some auxiliary results for proving Lemma 8.2. We start with a triviality:

Lemma 9.1. Let k be a field. Let C and D be k-coalgebras. Let A and B be k-algebras. Let $p : C \to A$, $q : C \to A$, $r : D \to B$ and $s : D \to B$ be four k-linear maps. Then,

$$(\mu_A \otimes \mu_B) \circ (p \otimes q \otimes r \otimes s) \circ (\Delta_C \otimes \Delta_D) = (p * q) \otimes (r * s)$$

(this is an equality between two maps $C \otimes D \to A \otimes B$).

Proof of Lemma 9.1. By (21) (applied to $U = C$, $V = C \otimes C$, $W = A \otimes A$, $U' = D$, $V' = D \otimes D$, $W' = B \otimes B$, $\alpha = \Delta_C$, $\beta = p \otimes q$, $\alpha' = \Delta_D$ and $\beta' = r \otimes s$), we have

$$((p \otimes q) \circ \Delta_C) \otimes ((r \otimes s) \circ \Delta_D) = (p \otimes q \otimes r \otimes s) \circ (\Delta_C \otimes \Delta_D) .$$

By (21) (applied to $U = C$, $V = A \otimes A$, $W = A$, $U' = D$, $V' = B \otimes B$, $W' = B$, $\alpha = (p \otimes q) \circ \Delta_C$, $\beta = \mu_A$, $\alpha' = (r \otimes s) \circ \Delta_D$ and $\beta' = \mu_B$), we have

$$\begin{aligned}
&(\mu_A \circ (p \otimes q) \circ \Delta_C) \otimes (\mu_B \circ (r \otimes s) \circ \Delta_D) \\
&= (\mu_A \otimes \mu_B) \circ \underbrace{(((p \otimes q) \circ \Delta_C) \otimes ((r \otimes s) \circ \Delta_D))}_{= (p \otimes q \otimes r \otimes s) \circ (\Delta_C \otimes \Delta_D)} \\
&= (\mu_A \otimes \mu_B) \circ (p \otimes q \otimes r \otimes s) \circ (\Delta_C \otimes \Delta_D) .
\end{aligned}$$

Now,

$$\begin{aligned}
&\underbrace{(p * q)}_{\substack{= \mu_A \circ (p \otimes q) \circ \Delta_C \\ \text{(by the definition of convolution)}}} \otimes \underbrace{(r * s)}_{\substack{= \mu_B \circ (r \otimes s) \circ \Delta_D \\ \text{(by the definition of convolution)}}} \\
&= (\mu_A \circ (p \otimes q) \circ \Delta_C) \otimes (\mu_B \circ (r \otimes s) \circ \Delta_D) \\
&= (\mu_A \otimes \mu_B) \circ (p \otimes q \otimes r \otimes s) \circ (\Delta_C \otimes \Delta_D) ,
\end{aligned}$$

so that Lemma 9.1 is proven. □

Next, a definition:

Definition 9.2. Let k be a field. Let V and W be two k-vector spaces. Then, $\tau_{V,W}$ will denote the (V, W)-*flip*; this is the k-linear map $V \otimes W \to W \otimes V$ which, for every $v \in V$ and $w \in W$, sends the element $v \otimes w \in V \otimes W$ to the element $w \otimes v \in W \otimes V$.

First let us show a trivial property of these flips:

Proposition 9.3. Let k be a field.

(a) Let V, W, V' and W' be four k-vector spaces, and $f : V \to V'$ and $g : W \to W'$ be two k-linear maps. Then, $(g \otimes f) \circ \tau_{V,W} = \tau_{V',W'} \circ (f \otimes g)$.

(b) Let U, V, W, T, U', V', W' and T' be eight k-vector spaces, and $e : U \to U'$, $f : V \to V'$, $g : W \to W'$ and $h : T \to T'$ be four k-linear maps. Then,

$$(\mathrm{id}_{U'} \otimes \tau_{V',W'} \otimes \mathrm{id}_{T'}) \circ (e \otimes f \otimes g \otimes h) = (e \otimes g \otimes f \otimes h) \circ (\mathrm{id}_U \otimes \tau_{V,W} \otimes \mathrm{id}_T)$$

(this is an equality between k-linear maps from $U \otimes V \otimes W \otimes T$ to $U' \otimes W' \otimes V' \otimes T'$).

Proof of Proposition 9.3. **(a)** Every $v \in V$ and $w \in W$ satisfy

$$\begin{aligned}
((g \otimes f) \circ \tau_{V,W}) (v \otimes w) &= (g \otimes f) \left(\underbrace{\tau_{V,W} (v \otimes w)}_{\substack{= w \otimes v \\ \text{(by the definition of } \tau_{V,W}\text{)}}} \right) \\
&= (g \otimes f) (w \otimes v) = g(w) \otimes f(v)
\end{aligned}$$

and

$$(\tau_{V',W'} \circ (f \otimes g))(v \otimes w) = \tau_{V',W'}\left(\underbrace{(f \otimes g)(v \otimes w)}_{=f(v)\otimes g(w)}\right) = \tau_{V',W'}(f(v) \otimes g(w))$$
$$= g(w) \otimes f(v) \qquad \text{(by the definition of } \tau_{V',W'}\text{)}.$$

Hence, every $v \in V$ and $w \in W$ satisfy

$$((g \otimes f) \circ \tau_{V,W})(v \otimes w) = g(w) \otimes f(v) = (\tau_{V',W'} \circ (f \otimes g))(v \otimes w).$$

In other words, the two maps $(g \otimes f) \circ \tau_{V,W}$ and $\tau_{V',W'} \circ (f \otimes g)$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $(g \otimes f) \circ \tau_{V,W} = \tau_{V',W'} \circ (f \otimes g)$. This proves Proposition 9.3 **(a)**.

(b) Applying (21) to $V \otimes W$, $W \otimes V$, $W' \otimes V'$, T, T, T', $\tau_{V,W}$, $g \otimes f$, id_T and h instead of U, V, W, U', V', W', α, β, α' and β', we obtain

$$((g \otimes f) \circ \tau_{V,W}) \otimes (h \circ \mathrm{id}_T) = (g \otimes f \otimes h) \circ (\tau_{V,W} \otimes \mathrm{id}_T).$$

Applying (21) to U, U, U', $V \otimes W \otimes T$, $W \otimes V \otimes T$, $W' \otimes V' \otimes T'$, id_U, e, $\tau_{V,W} \otimes \mathrm{id}_T$ and $g \otimes f \otimes h$ instead of U, V, W, U', V', W', α, β, α' and β', we obtain

$$(e \circ \mathrm{id}_U) \otimes ((g \otimes f \otimes h) \circ (\tau_{V,W} \otimes \mathrm{id}_T)) = (e \otimes g \otimes f \otimes h) \circ (\mathrm{id}_U \otimes \tau_{V,W} \otimes \mathrm{id}_T).$$

Thus,

$$(e \otimes g \otimes f \otimes h) \circ (\mathrm{id}_U \otimes \tau_{V,W} \otimes \mathrm{id}_T) = \underbrace{(e \circ \mathrm{id}_U)}_{=e} \otimes \underbrace{((g \otimes f \otimes h) \circ (\tau_{V,W} \otimes \mathrm{id}_T))}_{=((g\otimes f)\circ\tau_{V,W})\otimes(h\circ\mathrm{id}_T)}$$
$$= e \otimes \underbrace{((g \otimes f) \circ \tau_{V,W})}_{\substack{=\tau_{V',W'}\circ(f\otimes g) \\ \text{(by Proposition 9.3 (a))}}} \otimes \underbrace{(h \circ \mathrm{id}_T)}_{=h}$$
$$= e \otimes (\tau_{V',W'} \circ (f \otimes g)) \otimes h. \tag{23}$$

On the other hand, applying (21) to $V \otimes W$, $V' \otimes W'$, $W' \otimes V'$, T, T', T', $f \otimes g$, $\tau_{V',W'}$, h and $\mathrm{id}_{T'}$ instead of U, V, W, U', V', W', α, β, α' and β', we obtain

$$(\tau_{V',W'} \circ (f \otimes g)) \otimes (\mathrm{id}_{T'} \circ h) = (\tau_{V',W'} \otimes \mathrm{id}_{T'}) \circ (f \otimes g \otimes h).$$

Applying (21) to U, U', U', $V \otimes W \otimes T$, $V' \otimes W' \otimes T'$, $W' \otimes V' \otimes T'$, e, $\mathrm{id}_{U'}$, $f \otimes g \otimes h$ and $\tau_{V',W'} \otimes \mathrm{id}_{T'}$ instead of U, V, W, U', V', W', α, β, α' and β', we obtain

$$(\mathrm{id}_{U'} \circ e) \otimes ((\tau_{V',W'} \otimes \mathrm{id}_{T'}) \circ (f \otimes g \otimes h)) = (\mathrm{id}_{U'} \otimes \tau_{V',W'} \otimes \mathrm{id}_{T'}) \circ (e \otimes f \otimes g \otimes h).$$

Thus,

$$(\mathrm{id}_{U'} \otimes \tau_{V',W'} \otimes \mathrm{id}_{T'}) \circ (e \otimes f \otimes g \otimes h) = \underbrace{(\mathrm{id}_{U'} \circ e)}_{=e} \otimes \underbrace{((\tau_{V',W'} \otimes \mathrm{id}_{T'}) \circ (f \otimes g \otimes h))}_{=(\tau_{V',W'}\circ(f\otimes g))\otimes(\mathrm{id}_{T'}\circ h)}$$
$$= e \otimes (\tau_{V',W'} \circ (f \otimes g)) \otimes \underbrace{(\mathrm{id}_{T'} \circ h)}_{=h}$$
$$= e \otimes (\tau_{V',W'} \circ (f \otimes g)) \otimes h.$$

Compared with (23), this yields

$$(e \otimes g \otimes f \otimes h) \circ (\mathrm{id}_U \otimes \tau_{V,W} \otimes \mathrm{id}_T) = (\mathrm{id}_{U'} \otimes \tau_{V',W'} \otimes \mathrm{id}_{T'}) \circ (e \otimes f \otimes g \otimes h)\,.$$

This proves Proposition 9.3 **(b)**. □

Next, we shall show a general property of coalgebras:

Lemma 9.4. Let k be a field. Let C be a k-coalgebra. Then,

$$(\Delta_C \otimes \Delta_C) \circ \Delta_C = (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C.$$

Proof of Lemma 9.4. By the axioms of a coalgebra, we have

$$(\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C = (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C$$

(since C is a coalgebra).

On the other hand,

$$\underbrace{\Delta_C}_{=\Delta_C \circ \mathrm{id}_C} \otimes \underbrace{\Delta_C}_{=\mathrm{id}_{C\otimes C} \circ \Delta_C} = (\Delta_C \circ \mathrm{id}_C) \otimes (\mathrm{id}_{C\otimes C} \circ \Delta_C) = (\Delta_C \otimes \mathrm{id}_{C\otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C)$$

(by (21) (applied to $U = C$, $V = C$, $W = C \otimes C$, $U' = C$, $V' = C \otimes C$, $W' = C \otimes C$, $\alpha = \mathrm{id}_C$, $\beta = \Delta_C$, $\alpha' = \Delta_C$ and $\beta' = \mathrm{id}_{C\otimes C}$)), and thus

$$\begin{aligned}\underbrace{(\Delta_C \otimes \Delta_C)}_{=(\Delta_C \otimes \mathrm{id}_{C\otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C)} \circ \Delta_C &= \left(\Delta_C \otimes \underbrace{\mathrm{id}_{C\otimes C}}_{=\mathrm{id}_C \otimes \mathrm{id}_C}\right) \circ \underbrace{(\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C}_{=(\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C} \\ &= (\Delta_C \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C. \end{aligned} \tag{24}$$

But (21) (applied to $U = C$, $V = C \otimes C$, $W = C \otimes C \otimes C$, $U' = C$, $V' = C$, $W' = C$, $\alpha = \Delta_C$, $\beta = \Delta_C \otimes \mathrm{id}_C$, $\alpha' = \mathrm{id}_C$ and $\beta' = \mathrm{id}_C$) yields

$$((\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) = (\Delta_C \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C)\,,$$

so that

$$\begin{aligned}(\Delta_C \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) &= \underbrace{((\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C)}_{=(\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C} \otimes (\mathrm{id}_C \circ \mathrm{id}_C) \\ &= ((\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) \\ &= (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C)\end{aligned}$$

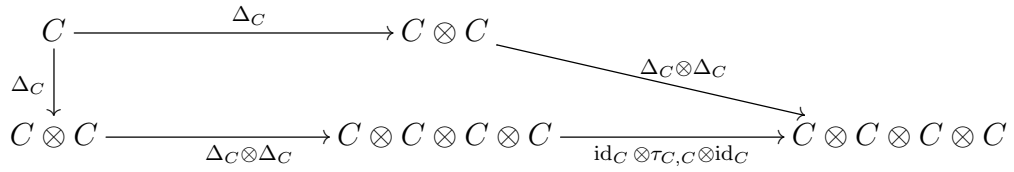
(by (21), applied to $U = C$, $V = C \otimes C$, $W = C \otimes C \otimes C$, $U' = C$, $V' = C$, $W' = C$, $\alpha = \Delta_C$, $\beta = \mathrm{id}_C \otimes \Delta_C$, $\alpha' = \mathrm{id}_C$ and $\beta' = \mathrm{id}_C$). Thus, (24) becomes

$$\begin{aligned}(\Delta_C \otimes \Delta_C) \circ \Delta_C &= \underbrace{(\Delta_C \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C)}_{=(\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C)} \circ \Delta_C \\ &= (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C.\end{aligned}$$

This proves Lemma 9.4. □

Now, we turn to a basic property of cocommutative coalgebras:

Lemma 9.5. Let k be a field. Let C be a cocommutative k-coalgebra. Then, the diagram



(25)

commutes. In other words,

$$(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C = (\Delta_C \otimes \Delta_C) \circ \Delta_C. \tag{26}$$

Proof of Lemma 9.5. Lemma 9.4 yields

$$(\Delta_C \otimes \Delta_C) \circ \Delta_C = (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C. \tag{27}$$

The equality (21) (applied to $U = C$, $V = C$, $W = C$, $U' = C \otimes C$, $V' = C \otimes C \otimes C$, $W' = C \otimes C \otimes C$, $\alpha = \mathrm{id}_C$, $\beta = \mathrm{id}_C$, $\alpha' = \Delta_C \otimes \mathrm{id}_C$ and $\beta' = \tau_{C,C} \otimes \mathrm{id}_C$) yields

$$(\mathrm{id}_C \circ \mathrm{id}_C) \otimes ((\tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C)) = (\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C). \tag{28}$$

But (21) (applied to $U = C$, $V = C \otimes C$, $W = C \otimes C$, $U' = C$, $V' = C$, $W' = C$, $\alpha = \Delta_C$, $\beta = \tau_{C,C}$, $\alpha' = \mathrm{id}_C$ and $\beta' = \mathrm{id}_C$) yields $(\tau_{C,C} \circ \Delta_C) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) = (\tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C)$, so that

$$\begin{aligned}(\tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) &= (\tau_{C,C} \circ \Delta_C) \otimes \underbrace{(\mathrm{id}_C \circ \mathrm{id}_C)}_{=\mathrm{id}_C} = \underbrace{(\tau_{C,C} \circ \Delta_C)}_{\substack{=\Delta_C \\ \text{(since } C \text{ is cocommutative)}}} \otimes \mathrm{id}_C \\ &= \Delta_C \otimes \mathrm{id}_C. \end{aligned} \tag{29}$$

Now, (28) becomes

$$\begin{aligned}&(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \\ &= \underbrace{(\mathrm{id}_C \circ \mathrm{id}_C)}_{=\mathrm{id}_C} \otimes \underbrace{((\tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C))}_{\substack{=\Delta_C \otimes \mathrm{id}_C \\ \text{(by (29))}}} = \mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C. \end{aligned} \tag{30}$$

Now,

$$\begin{aligned}&(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ \underbrace{(\Delta_C \otimes \Delta_C) \circ \Delta_C}_{\substack{=(\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C \\ \text{(by (27))}}} \\ &= \underbrace{(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C)}_{=\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C} \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C \\ &= (\mathrm{id}_C \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C = (\Delta_C \otimes \Delta_C) \circ \Delta_C \end{aligned}$$

(by (27)). Hence, (26) holds. In other words, the diagram (25) is commutative. This proves Lemma 9.5. □

Remark: Actually, many elementary properties of coalgebras (in fact, all purely diagrammatic properties) are "duals" of analogous properties of algebras. For instance, Lemma 9.5 is a "dual" of the fact that for any four elements a, b, c, d of a commutative k-algebra, we have $(ac) \cdot (bd) = (ab) \cdot (cd)$. This fact is, of course, trivial. This gives us two ways to prove Lemma 9.5:

- Either invoke the theorem that the "dual" of a true purely diagrammatic property of k-algebras must be a true property of k-coalgebras. However, this would require us to prove this theorem.
- Or reformulate the property of k-algebras (that for any four elements a, b, c, d of a commutative k-algebra, we have $(ac) \cdot (bd) = (ab) \cdot (cd)$) in a purely diagrammatic form (i. e., in form of a commutative diagram with no concrete elements occurring) and *prove it purely by diagram chasing* (again, without using elements), and then reverse all the arrows in this proof. As a result you get a proof of Lemma 9.5. This is how I constructed the above proof of Lemma 9.5.[31]

So when Lemma 9.5 is just a "dual" of a fact about k-algebras, then why is the fact about k-algebras trivial while Lemma 9.5 took us so long to prove? This is an example of how working with coalgebras is a lot more cumbersome than working with algebras, because working with algebras is easily done elementwise, while working with coalgebras usually requires transforming equations into commutative diagrams and chasing diagrams. There *is* a second way to efficiently work with coalgebras: namely, by using Sweedler's notation; however, this would require us to introduce Sweedler's notation[32], which I don't want to do here. Using Sweedler's notation, we could give a proof of Lemma 9.5 shorter than the one given above, but still not as short as the obvious proof of the fact about k-algebras (that for any four elements a, b, c, d of a commutative k-algebra, we have $(ac) \cdot (bd) = (ab) \cdot (cd)$).

Next, let us show another simple property of arbitrary coalgebras:

Lemma 9.6. Let k be a field. Let C be a k-coalgebra.

(a) Every $x \in C$ satisfies $((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x) = \varepsilon_C(x)\, 1 \otimes 1$.

(b) Consider the obvious canonical k-coalgebra structure on k (with Δ_k being the canonical isomorphism $k \to k \otimes k$, and ε_k being the identity map). The map ε_C is a k-coalgebra homomorphism from C to k.

Proof of Lemma 9.6. **(a)** Let kan be the canonical isomorphism $C \to C \otimes k$ which maps every $c \in C$ to $c \otimes 1$. Since C is a coalgebra, we have $(\mathrm{id} \otimes \varepsilon_C) \circ \Delta_C = \mathrm{kan}$ (by the axioms of a coalgebra).

We have $\underbrace{\varepsilon_C}_{=\varepsilon_C \circ \mathrm{id}} \otimes \underbrace{\varepsilon_C}_{=\mathrm{id} \circ \varepsilon_C} = (\varepsilon_C \circ \mathrm{id}) \otimes (\mathrm{id} \circ \varepsilon_C) = (\varepsilon_C \otimes \mathrm{id}) \circ (\mathrm{id} \otimes \varepsilon_C)$ (by an application of (21)), so that

$$(\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C = (\varepsilon_C \otimes \mathrm{id}) \circ \underbrace{(\mathrm{id} \otimes \varepsilon_C) \circ \Delta_C}_{=\mathrm{kan}} = (\varepsilon_C \otimes \mathrm{id}) \circ \mathrm{kan}\,.$$

[31] Of course, if you are comparing different proofs, you need to count the proof of Lemma 9.4 as a part of the above proof of Lemma 9.5.

[32] To my knowledge, there is not a single book about Hopf algebras that cares to formally and correctly introduce Sweedler's notation. However, I have not read too many books, so this needs not say much.

Hence, for every $x \in C$, we have

$$((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x) = ((\varepsilon_C \otimes \mathrm{id}) \circ \mathrm{kan})(x) = (\varepsilon_C \otimes \mathrm{id}) \underbrace{(\mathrm{kan}\, x)}_{\substack{=x\otimes 1 \\ \text{(by the definition of kan)}}} = (\varepsilon_C \otimes \mathrm{id})(x \otimes 1)$$

$$= \varepsilon_C(x) \otimes \underbrace{\mathrm{id}(1)}_{=1} = \varepsilon_C(x) \otimes 1 = \varepsilon_C(x)\, 1 \otimes 1.$$

This proves Lemma 9.6 **(a)**.

(b) Let $\mathrm{kan}_k : k \to k \otimes k$ be the canonical isomorphism which sends every $\lambda \in k$ to $\lambda 1 \otimes 1 = \lambda \otimes 1 = 1 \otimes \lambda \in k \otimes k$. Then, $\Delta_k = \mathrm{kan}_k$ (by the definition of the coalgebra structure on k). Also, $\varepsilon_k = \mathrm{id}$ (by the definition of the coalgebra structure on k).

Now, every $x \in C$ satisfies

$$\begin{aligned}
&((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x) \\
&= \varepsilon_C(x)\, 1 \otimes 1 \qquad \text{(by Lemma 9.6 \textbf{(a)})} \\
&= \mathrm{kan}_k(\varepsilon_C(x)) \qquad \text{(because } \mathrm{kan}_k(\varepsilon_C(x)) = \varepsilon_C(x)\, 1 \otimes 1 \text{ (by the definition of } \mathrm{kan}_k)) \\
&= (\mathrm{kan}_k \circ \varepsilon_C)(x).
\end{aligned}$$

Thus, $(\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C = \underbrace{\mathrm{kan}_k}_{=\Delta_k} \circ \varepsilon_C = \Delta_k \circ \varepsilon_C$. Combined with $\underbrace{\varepsilon_k}_{=\mathrm{id}} \circ \varepsilon_C = \varepsilon_C$, this yields that ε_C is a k-coalgebra homomorphism from C to k. This proves Lemma 9.6 **(b)**. $\square$

Now we will show a less trivial fact, much closer to Lemma 8.2:

Lemma 9.7. Let k be a field. Let C be a cocommutative k-coalgebra. Let H be a k-bialgebra. Let $f \in \mathcal{L}(C, H)$ be an $(\varepsilon, \varepsilon)$-coderivation. Then, for every $n \in \mathbb{N}$, we have

$$\Delta_H \circ f^{*n} = \sum_{i=0}^{n} \binom{n}{i} \left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C. \tag{31}$$

Proof of Lemma 9.7. We are going to prove Lemma 9.7 by induction over n.

Induction base: Recall that H is a bialgebra, so that $\Delta_H(1_H) = 1_H \otimes 1_H$ by the axioms of a bialgebra.

We have $f^{*0} = e_{C,H}$ and

$$\begin{aligned}
\sum_{i=0}^{0} \binom{0}{i} \left(f^{*i} \otimes f^{*(0-i)}\right) \circ \Delta_C &= \underbrace{\binom{0}{0}}_{=1} \left(\underbrace{f^{*0}}_{=e_{C,H}} \otimes \underbrace{f^{*0}}_{=e_{C,H}}\right) \circ \Delta_C \\
&= (e_{C,H} \otimes e_{C,H}) \circ \Delta_C.
\end{aligned} \tag{32}$$

Since $e_{C,H} = \eta_H \circ \varepsilon_C$, we have

$$e_{C,H} \otimes e_{C,H} = (\eta_H \circ \varepsilon_C) \otimes (\eta_H \circ \varepsilon_C) = (\eta_H \otimes \eta_H) \circ (\varepsilon_C \otimes \varepsilon_C)$$

(by an application of (21)). Hence, every $x \in C$ satisfies

$$\begin{aligned}
\left(\underbrace{\left(e_{C,H} \otimes e_{C,H}\right)}_{=(\eta_H \otimes \eta_H) \circ (\varepsilon_C \otimes \varepsilon_C)} \circ \Delta_C \right)(x) &= \left((\eta_H \otimes \eta_H) \circ (\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C\right)(x) \\
&= (\eta_H \otimes \eta_H) \left(\underbrace{\left((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C\right)(x)}_{\substack{=\varepsilon_C(x) 1 \otimes 1 \\ \text{(by Lemma 9.6 \textbf{(a)})}}} \right) \\
&= (\eta_H \otimes \eta_H)\left(\varepsilon_C(x)\, 1 \otimes 1\right) = \varepsilon_C(x)\, \eta_H(1) \otimes \eta_H(1) \\
&= \varepsilon_C(x)\, \underbrace{1_H \otimes 1_H}_{=\Delta_H(1_H)} \\
&\qquad \text{(since the definition of } \eta_H \text{ yields } \eta_H(1) = 1 \cdot 1_H = 1_H)
\end{aligned}$$

and

$$\begin{aligned}
\left(\Delta_H \circ \underbrace{e_{C,H}}_{=\eta_H \circ \varepsilon_C} \right)(x) &= \left(\Delta_H \circ \eta_H \circ \varepsilon_C\right)(x) = \Delta_H \left(\underbrace{\eta_H\left(\varepsilon_C(x)\right)}_{\substack{=\varepsilon_C(x) 1_H \\ \text{(by the definition of } \eta_H\text{)}}} \right) \\
&= \Delta_H\left(\varepsilon_C(x)\, 1_H\right) = \varepsilon_C(x)\, \underbrace{\Delta_H(1_H)}_{=1_H \otimes 1_H} = \varepsilon_C(x)\, 1_H \otimes 1_H.
\end{aligned}$$

Hence, every $x \in C$ satisfies

$$\left((e_{C,H} \otimes e_{C,H}) \circ \Delta_C\right)(x) = \left(\Delta_H \circ e_{C,H}\right)(x).$$

In other words, $(e_{C,H} \otimes e_{C,H}) \circ \Delta_C = \Delta_H \circ e_{C,H}$. Now,

$$\Delta_H \circ \underbrace{f^{*0}}_{=e_{C,H}} = \Delta_H \circ e_{C,H} = (e_{C,H} \otimes e_{C,H}) \circ \Delta_C = \sum_{i=0}^{0} \binom{0}{i} \left(f^{*i} \otimes f^{*(0-i)}\right) \circ \Delta_C$$

(by (32)). In other words, Lemma 9.7 holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that Lemma 9.7 holds for $n = N$. To complete the induction, we must show that Lemma 9.7 also holds for $n = N + 1$.

Since Lemma 9.7 holds for $n = N$, we have

$$\Delta_H \circ f^{*N} = \sum_{i=0}^{N} \binom{N}{i} \left(f^{*i} \otimes f^{*(N-i)}\right) \circ \Delta_C. \tag{33}$$

Denote the k-linear map $\sum_{i=0}^{N} \binom{N}{i} \left(f^{*i} \otimes f^{*(N-i)}\right) : C \otimes C \to H \otimes H$ by Φ. Then, (33)

becomes

$$\Delta_H \circ f^{*N} = \sum_{i=0}^{N} \binom{N}{i} \left(f^{*i} \otimes f^{*(N-i)}\right) \circ \Delta_C = \underbrace{\left(\sum_{i=0}^{N} \binom{N}{i} \left(f^{*i} \otimes f^{*(N-i)}\right)\right)}_{=\Phi} \circ \Delta_C$$

$$\text{(since composition of } k\text{-linear maps is distributive)}$$

$$= \Phi \circ \Delta_C. \tag{34}$$

Now,

$$f^{*(N+1)} = f * f^{*N} = \mu_H \circ \left(f \otimes f^{*N}\right) \circ \Delta_C \qquad \text{(by the definition of convolution)},$$

so that

$$\Delta_H \circ f^{*(N+1)} = \underbrace{\Delta_H \circ \mu_H}_{\substack{=(\mu_H \otimes \mu_H) \circ \left(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H\right) \circ (\Delta_H \otimes \Delta_H) \\ \text{(by the axioms of a bialgebra, since } H \text{ is a bialgebra)}}} \circ \left(f \otimes f^{*N}\right) \circ \Delta_C$$

$$= (\mu_H \otimes \mu_H) \circ (\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ (\Delta_H \otimes \Delta_H) \circ \left(f \otimes f^{*N}\right) \circ \Delta_C. \tag{35}$$

But an application of (21) yields $(\Delta_H \circ f) \otimes \left(\Delta_H \circ f^{*N}\right) = (\Delta_H \otimes \Delta_H) \circ \left(f \otimes f^{*N}\right)$, so that

$$\begin{aligned}
&(\Delta_H \otimes \Delta_H) \circ \left(f \otimes f^{*N}\right) \\
&= \underbrace{(\Delta_H \circ f)}_{\substack{=\left(f \otimes e_{C,H} + e_{C,H} \otimes f\right) \circ \Delta_C \\ \text{(since } f \text{ is an } (\varepsilon,\varepsilon)\text{-coderivation)}}} \otimes \underbrace{\left(\Delta_H \circ f^{*N}\right)}_{\substack{=\Phi \circ \Delta_C \\ \text{(by (34))}}} \\
&= \left((f \otimes e_{C,H} + e_{C,H} \otimes f) \circ \Delta_C\right) \otimes (\Phi \circ \Delta_C) \\
&= \left((f \otimes e_{C,H} + e_{C,H} \otimes f) \otimes \Phi\right) \circ (\Delta_C \otimes \Delta_C) \\
&\qquad \left(\begin{array}{c} \text{by (21), applied to } U = C,\ V = C \otimes C,\ W = H \otimes H,\ U' = C,\ V' = C \otimes C, \\ W' = H \otimes H,\ \alpha = \Delta_C,\ \beta = \left(f \otimes e_{C,H} + e_{C,H} \otimes f\right),\ \alpha' = \Delta_C \text{ and } \beta' = \Phi \end{array} \right).
\end{aligned}$$

Hence, (35) becomes

$$\begin{aligned}
&\Delta_H \circ f^{*(N+1)} \\
&= (\mu_H \otimes \mu_H) \circ (\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \underbrace{(\Delta_H \otimes \Delta_H) \circ \left(f \otimes f^{*N}\right)}_{=\left(\left(f \otimes e_{C,H} + e_{C,H} \otimes f\right) \otimes \Phi\right) \circ (\Delta_C \otimes \Delta_C)} \circ \Delta_C \\
&= (\mu_H \otimes \mu_H) \circ (\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \left((f \otimes e_{C,H} + e_{C,H} \otimes f) \otimes \Phi\right) \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C.
\end{aligned} \tag{36}$$

But since tensoring of k-linear maps is distributive, we have

$$
\begin{aligned}
&(f \otimes e_{C,H} + e_{C,H} \otimes f) \otimes \Phi \\
&= (f \otimes e_{C,H}) \otimes \Phi + (e_{C,H} \otimes f) \otimes \Phi \\
&= \underbrace{(f \otimes e_{C,H}) \otimes \left(\sum_{i=0}^{N} \binom{N}{i} \left(f^{*i} \otimes f^{*(N-i)} \right) \right)}_{= \sum_{i=0}^{N} \binom{N}{i} \left(f \otimes e_{C,H}\right) \otimes \left(f^{*i} \otimes f^{*(N-i)}\right)} + \underbrace{(e_{C,H} \otimes f) \otimes \left(\sum_{i=0}^{N} \binom{N}{i} \left(f^{*i} \otimes f^{*(N-i)} \right) \right)}_{= \sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f\right) \otimes \left(f^{*i} \otimes f^{*(N-i)}\right)} \\
&\qquad \text{(since tensoring of } k\text{-linear maps is } k\text{-bilinear)} \qquad \text{(since tensoring of } k\text{-linear maps is } k\text{-bilinear)} \\
&\qquad \text{(since tensoring of } k\text{-linear maps is distributive)} \\
&= \sum_{i=0}^{N} \binom{N}{i} \underbrace{(f \otimes e_{C,H}) \otimes \left(f^{*i} \otimes f^{*(N-i)} \right)}_{= f \otimes e_{C,H} \otimes f^{*i} \otimes f^{*(N-i)}} + \sum_{i=0}^{N} \binom{N}{i} \underbrace{(e_{C,H} \otimes f) \otimes \left(f^{*i} \otimes f^{*(N-i)} \right)}_{= e_{C,H} \otimes f \otimes f^{*i} \otimes f^{*(N-i)}} \\
&= \sum_{i=0}^{N} \binom{N}{i} f \otimes e_{C,H} \otimes f^{*i} \otimes f^{*(N-i)} + \sum_{i=0}^{N} \binom{N}{i} e_{C,H} \otimes f \otimes f^{*i} \otimes f^{*(N-i)},
\end{aligned}
$$

and thus

$$
\begin{aligned}
&(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ ((f \otimes e_{C,H} + e_{C,H} \otimes f) \otimes \Phi) \\
&= (\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \left(\sum_{i=0}^{N} \binom{N}{i} f \otimes e_{C,H} \otimes f^{*i} \otimes f^{*(N-i)} + \sum_{i=0}^{N} \binom{N}{i} e_{C,H} \otimes f \otimes f^{*i} \otimes f^{*(N-i)} \right) \\
&= \underbrace{(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \left(\sum_{i=0}^{N} \binom{N}{i} f \otimes e_{C,H} \otimes f^{*i} \otimes f^{*(N-i)} \right)}_{= \sum_{i=0}^{N} \binom{N}{i} \left(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H\right) \circ \left(f \otimes e_{C,H} \otimes f^{*i} \otimes f^{*(N-i)}\right)} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&\qquad + \underbrace{(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \left(\sum_{i=0}^{N} \binom{N}{i} e_{C,H} \otimes f \otimes f^{*i} \otimes f^{*(N-i)} \right)}_{= \sum_{i=0}^{N} \binom{N}{i} \left(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H\right) \circ \left(e_{C,H} \otimes f \otimes f^{*i} \otimes f^{*(N-i)}\right)} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&\qquad \text{(since composition of } k\text{-linear maps is distributive)} \\
&= \sum_{i=0}^{N} \binom{N}{i} \underbrace{(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \left(f \otimes e_{C,H} \otimes f^{*i} \otimes f^{*(N-i)}\right)}_{= \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)}\right) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)} \\
&\qquad \text{(by Proposition 9.3 \textbf{(b)}, applied to } C, C, C, C, \\
&\qquad H, H, H, H, f, e_{C,H}, f^{*i}, f^{*(N-i)} \text{ instead of} \\
&\qquad U, V, W, T, U', V', W', T', e, f, g, h) \\
&\qquad + \sum_{i=0}^{N} \binom{N}{i} \underbrace{(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \left(e_{C,H} \otimes f \otimes f^{*i} \otimes f^{*(N-i)}\right)}_{= \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)}\right) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)} \\
&\qquad \text{(by Proposition 9.3 \textbf{(b)}, applied to } C, C, C, C, \\
&\qquad H, H, H, H, e_{C,H}, f, f^{*i}, f^{*(N-i)} \text{ instead of} \\
&\qquad U, V, W, T, U', V', W', T', e, f, g, h) \\
&= \underbrace{\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)}\right) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)}_{= \left(\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)}\right) \right) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&\qquad + \underbrace{\sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)}\right) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)}_{= \left(\sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)}\right) \right) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)}
\end{aligned}
$$

$$
\begin{aligned}
&= \left(\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \right) \circ (\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \\
&\qquad + \left(\sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \right) \circ (\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \\
&= \left(\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) + \sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \right) \circ (\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)}\,. \qquad (37)
\end{aligned}
$$

Let us denote by Ψ the k-linear map

$$
\begin{aligned}
&\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) + \sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \\
&: C \otimes C \otimes C \otimes C \to H \otimes H \otimes H \otimes H.
\end{aligned}
$$

Then, (37) becomes

$$
\begin{aligned}
&(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ ((f \otimes e_{C,H} + e_{C,H} \otimes f) \otimes \Phi) \\
&= \underbrace{\left(\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) + \sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \right)}_{=\Psi} \circ (\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \\
&= \Psi \circ (\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C)\,. \qquad (38)
\end{aligned}
$$

Hence, (36) becomes

$$
\begin{aligned}
&\Delta_H \circ f^{*(N+1)} \\
&= (\mu_H \otimes \mu_H) \circ \underbrace{(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ ((f \otimes e_{C,H} + e_{C,H} \otimes f) \otimes \Phi)}_{=\Psi \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C \right)} \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C \\
&= (\mu_H \otimes \mu_H) \circ \Psi \circ \underbrace{(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C}_{\substack{=(\Delta_C \otimes \Delta_C) \circ \Delta_C \\ \text{(by (26))}}} \\
&= (\mu_H \otimes \mu_H) \circ \Psi \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C. \qquad (39)
\end{aligned}
$$

But since

$$
\Psi = \sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) + \sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right),
$$

we have

$$
\begin{aligned}
&(\mu_H \otimes \mu_H) \circ \Psi \\
&= (\mu_H \otimes \mu_H) \circ \left(\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) + \sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \right) \\
&= \underbrace{(\mu_H \otimes \mu_H) \circ \left(\sum_{i=0}^{N} \binom{N}{i} \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \right)}_{\substack{= \sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \\ \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)}}} \\
&\qquad + \underbrace{(\mu_H \otimes \mu_H) \circ \left(\sum_{i=0}^{N} \binom{N}{i} \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \right)}_{\substack{= \sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \\ \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)}}} \\
&\qquad \text{(since composition of } k\text{-linear maps is distributive)} \\
&= \sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \\
&\qquad + \sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right),
\end{aligned}
$$

so that

$$
\begin{aligned}
&(\mu_H \otimes \mu_H) \circ \Psi \circ (\Delta_C \otimes \Delta_C) \\
&= \left(\sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \right. \\
&\qquad \left. + \sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \right) \\
&\qquad \circ (\Delta_C \otimes \Delta_C) \\
&= \underbrace{\left(\sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \right) \circ (\Delta_C \otimes \Delta_C)}_{= \sum\limits_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \circ (\Delta_C \otimes \Delta_C)} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&\qquad + \underbrace{\left(\sum_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \right) \circ (\Delta_C \otimes \Delta_C)}_{= \sum\limits_{i=0}^{N} \binom{N}{i} (\mu_H \otimes \mu_H) \circ \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \circ (\Delta_C \otimes \Delta_C)} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&\qquad \text{(since composition of } k\text{-linear maps is distributive)} \\
&= \sum_{i=0}^{N} \binom{N}{i} \qquad \underbrace{(\mu_H \otimes \mu_H) \circ \left(f \otimes f^{*i} \otimes e_{C,H} \otimes f^{*(N-i)} \right) \circ (\Delta_C \otimes \Delta_C)}_{= \left(f * f^{*i} \right) \otimes \left(e_{C,H} * f^{*(N-i)} \right)} \\
&\qquad \text{(by Lemma 9.1, applied to } A{=}H,\ B{=}H,\ D{=}C,\ p{=}f,\ q{=}f^{*i},\ r{=}e_{C,H} \text{ and } s{=}f^{*(N-i)}) \\
&\qquad + \sum_{i=0}^{N} \binom{N}{i} \qquad \underbrace{(\mu_H \otimes \mu_H) \circ \left(e_{C,H} \otimes f^{*i} \otimes f \otimes f^{*(N-i)} \right) \circ (\Delta_C \otimes \Delta_C)}_{= \left(e_{C,H} * f^{*i} \right) \otimes \left(f * f^{*(N-i)} \right)} \\
&\qquad \text{(by Lemma 9.1, applied to } A{=}H,\ B{=}H,\ D{=}C,\ p{=}e_{C,H},\ q{=}f^{*i},\ r{=}f \text{ and } s{=}f^{*(N-i)}) \\
&= \sum_{i=0}^{N} \binom{N}{i} \underbrace{\left(f * f^{*i} \right)}_{= f^{*(i+1)}} \otimes \underbrace{\left(e_{C,H} * f^{*(N-i)} \right)}_{= f^{*(N-i)}} + \sum_{i=0}^{N} \binom{N}{i} \underbrace{\left(e_{C,H} * f^{*i} \right)}_{= f^{*i}} \otimes \underbrace{\left(f * f^{*(N-i)} \right)}_{= f^{*((N-i)+1)} = f^{*(N+1-i)}} \\
&= \sum_{i=0}^{N} \binom{N}{i} f^{*(i+1)} \otimes f^{*(N-i)} + \sum_{i=0}^{N} \binom{N}{i} f^{*i} \otimes f^{*(N+1-i)}.
\end{aligned}
$$

Compared with

$$\sum_{i=0}^{N+1}\binom{N+1}{i}f^{*i}\otimes f^{*(N+1-i)}$$
$$=\sum_{i=0}^{N+1}\left(\binom{N}{i-1}+\binom{N}{i}\right)f^{*i}\otimes f^{*(N+1-i)}$$
$$\left(\text{since }\binom{N+1}{i}=\binom{N}{i-1}+\binom{N}{i}\text{ by the recursion of the binomial coefficients}\right)$$
$$=\underbrace{\sum_{i=0}^{N+1}\binom{N}{i-1}f^{*i}\otimes f^{*(N+1-i)}}_{=\binom{N}{0-1}f^{*0}\otimes f^{*(N+1-0)}+\sum_{i=1}^{N+1}\binom{N}{i-1}f^{*i}\otimes f^{*(N+1-i)}}+\underbrace{\sum_{i=0}^{N+1}\binom{N}{i}f^{*i}\otimes f^{*(N+1-i)}}_{=\sum_{i=0}^{N}\binom{N}{i}f^{*i}\otimes f^{*(N+1-i)}+\binom{N}{N+1}f^{*(N+1)}\otimes f^{*(N+1-(N+1))}}$$
$$=\underbrace{\binom{N}{0-1}}_{=0}f^{*0}\otimes f^{*(N+1-0)}+\underbrace{\sum_{i=1}^{N+1}\binom{N}{i-1}f^{*i}\otimes f^{*(N+1-i)}}_{=\sum_{i=0}^{N}\binom{N}{i+1-1}f^{*(i+1)}\otimes f^{*(N+1-(i+1))}}$$
(here, we substituted i+1 for i in the sum)
$$+\sum_{i=0}^{N}\binom{N}{i}f^{*i}\otimes f^{*(N+1-i)}+\underbrace{\binom{N}{N+1}}_{=0}f^{*(N+1)}\otimes f^{*(N+1-(N+1))}$$
$$=\underbrace{0f^{*0}\otimes f^{*(N+1-0)}}_{=0}+\sum_{i=0}^{N}\underbrace{\binom{N}{i+1-1}}_{=\binom{N}{i}}f^{*(i+1)}\otimes\underbrace{f^{*(N+1-(i+1))}}_{=f^{*(N-i)}}$$
$$+\sum_{i=0}^{N}\binom{N}{i}f^{*i}\otimes f^{*(N+1-i)}+\underbrace{0f^{*(N+1)}\otimes f^{*(N+1-(N+1))}}_{=0}$$
$$=\sum_{i=0}^{N}\binom{N}{i}f^{*(i+1)}\otimes f^{*(N-i)}+\sum_{i=0}^{N}\binom{N}{i}f^{*i}\otimes f^{*(N+1-i)},$$

this yields

$$(\mu_H\otimes\mu_H)\circ\Psi\circ(\Delta_C\otimes\Delta_C)=\sum_{i=0}^{N+1}\binom{N+1}{i}f^{*i}\otimes f^{*(N+1-i)}.$$

Hence, (39) becomes

$$\begin{aligned}\Delta_H \circ f^{*(N+1)} &= \underbrace{\left(\mu_H \otimes \mu_H\right) \circ \Psi \circ \left(\Delta_C \otimes \Delta_C\right)}_{=\sum_{i=0}^{N+1} \binom{N+1}{i} f^{*i} \otimes f^{*(N+1-i)}} \circ \Delta_C \\ &= \sum_{i=0}^{N+1} \binom{N+1}{i} \left(f^{*i} \otimes f^{*(N+1-i)}\right) \circ \Delta_C.\end{aligned}$$

In other words, Lemma 9.7 holds for $n = N+1$. This completes the induction step. The induction proof of Lemma 9.7 is thus complete. $\square$

Here is a little brother of Lemma 9.7 (a similar property of ε_C, much easier to prove):

Lemma 9.8. Let k be a field. Let C be a k-coalgebra. Let H be a k-bialgebra. Let $f \in \mathcal{L}(C, H)$ be an $(\varepsilon, \varepsilon)$-coderivation. Then, for every positive $n \in \mathbb{N}$, we have $\varepsilon_H \circ f^{*n} = 0$.

Proof of Lemma 9.8. Since n is positive, we have $f^{*n} = f * f^{*(n-1)} = \mu_H \circ \left(f \otimes f^{*(n-1)}\right) \circ \Delta_C$ (by the definition of convolution). Since H is a k-bialgebra, we have $\varepsilon_H \circ \mu_H = \mu_k \circ (\varepsilon_H \otimes \varepsilon_H)$ (by the axioms of a bialgebra), where μ_k is the canonical k-module isomorphism $k \otimes k \to k$.

Since f is an $(\varepsilon, \varepsilon)$-coderivation, we have $f(C) \subseteq \operatorname{Prim} H$ (since by Theorem 7.2, we know that f is an $(\varepsilon, \varepsilon)$-coderivation if and only if $f(C) \subseteq \operatorname{Prim} H$). Thus, every $x \in C$ satisfies $f(x) \in f(C) \subseteq \operatorname{Prim} H$, so that $\varepsilon(f(x)) = 0$ (by Remark 6.3, applied to $f(x)$ instead of x) and therefore

$$(\varepsilon_H \circ f)(x) = \varepsilon_H(f(x)) = \varepsilon(f(x)) = 0.$$

Since this holds for every $x \in C$, we thus conclude that $\varepsilon_H \circ f = 0$.

Now, for every positive $n \in \mathbb{N}$, we have

$$\begin{aligned}\varepsilon_H \circ \underbrace{f^{*n}}_{=\mu_H \circ \left(f \otimes f^{*(n-1)}\right) \circ \Delta_C} &= \underbrace{\varepsilon_H \circ \mu_H}_{=\mu_k \circ (\varepsilon_H \otimes \varepsilon_H)} \circ \left(f \otimes f^{*(n-1)}\right) \circ \Delta_C \\ &= \mu_k \circ (\varepsilon_H \otimes \varepsilon_H) \circ \left(f \otimes f^{*(n-1)}\right) \circ \Delta_C.\end{aligned}$$

Since an application of (21) yields $(\varepsilon_H \circ f) \otimes \left(\varepsilon_H \circ f^{*(n-1)}\right) = (\varepsilon_H \otimes \varepsilon_H) \circ \left(f \otimes f^{*(n-1)}\right)$, this becomes

$$\begin{aligned}\varepsilon_H \circ f^{*n} &= \mu_k \circ \underbrace{(\varepsilon_H \otimes \varepsilon_H) \circ \left(f \otimes f^{*(n-1)}\right)}_{=(\varepsilon_H \circ f) \otimes \left(\varepsilon_H \circ f^{*(n-1)}\right)} \circ \Delta_C \\ &= \mu_k \circ \left(\underbrace{(\varepsilon_H \circ f)}_{=0} \otimes \left(\varepsilon_H \circ f^{*(n-1)}\right)\right) \circ \Delta_C = \mu_k \circ \underbrace{\left(0 \otimes \left(\varepsilon_H \circ f^{*(n-1)}\right)\right)}_{=0} \circ \Delta_C \\ &= \mu_k \circ 0 \circ \Delta_C = 0 \qquad \left(\text{since } \mu_k \text{ is } k\text{-linear}\right).\end{aligned}$$

This proves Lemma 9.8. $\square$

We can now move on to the proof of Lemma 8.2:

Proof of Lemma 8.2. Assume that f is an $(\varepsilon, \varepsilon)$-coderivation. Let $x \in C$.

Since $\Delta_C(x)$ is a tensor in $C \otimes C$, we can write $\Delta_C(x)$ as $\Delta_C(x) = \sum_{j=1}^{m} \lambda_j a_j \otimes b_j$ for some $m \in \mathbb{N}$, some elements a_1, a_2, ..., a_m of C, and some elements b_1, b_2, ..., b_m of C. Consider this m, these a_1, a_2, ..., a_m, and these b_1, b_2, ..., b_m.

Every $n \in \mathbb{N}$ and every $i \in \{0, 1, \ldots, n\}$ satisfy

$$\frac{1}{n!}\binom{n}{i} \underbrace{\left(\left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C\right)(x)}_{=\left(f^{*i} \otimes f^{*(n-i)}\right)(\Delta_C(x))}$$

$$= \frac{1}{n!} \underbrace{\binom{n}{i}}_{=\frac{n!}{i!\,(n-i)!}} \left(f^{*i} \otimes f^{*(n-i)}\right) \left(\underbrace{\Delta_C(x)}_{=\sum_{j=1}^{m} \lambda_j a_j \otimes b_j}\right)$$

$$= \underbrace{\frac{1}{n!} \cdot \frac{n!}{i!\,(n-i)!}}_{=\frac{1}{i!} \cdot \frac{1}{(n-i)!}} \underbrace{\left(f^{*i} \otimes f^{*(n-i)}\right) \left(\sum_{j=1}^{m} \lambda_j a_j \otimes b_j\right)}_{=\sum_{j=1}^{m} \lambda_j f^{*i}(a_j) \otimes f^{*(n-i)}(b_j)}$$

$$= \frac{1}{i!} \cdot \frac{1}{(n-i)!} \cdot \sum_{j=1}^{m} \lambda_j f^{*i}(a_j) \otimes f^{*(n-i)}(b_j) = \sum_{j=1}^{m} \lambda_j \frac{f^{*i}(a_j)}{i!} \otimes \frac{f^{*(n-i)}(b_j)}{(n-i)!}. \tag{40}$$

We have

$$\left(\Delta_H \circ e^{*f}\right)(x)$$

$$= \Delta_H\left(e^{*f}(x)\right) = \Delta_H\left(\sum_{i \geq 0} \underbrace{\frac{f^{*i}(x)}{i!}}_{=\frac{1}{i!} f^{*i}(x)}\right) \qquad \text{(by (6))}$$

$$= \Delta_H\left(\sum_{i \geq 0} \frac{1}{i!} f^{*i}(x)\right) = \sum_{i \geq 0} \frac{1}{i!} \underbrace{\Delta_H\left(f^{*i}(x)\right)}_{=(\Delta_H \circ f^{*i})(x)} \qquad \text{(since } \Delta_H \text{ is } k\text{-linear)}$$

$$= \sum_{i \geq 0} \frac{1}{i!} \left(\Delta_H \circ f^{*i}\right)(x) = \sum_{n \geq 0} \frac{1}{n!} \underbrace{\left(\Delta_H \circ f^{*n}\right)}_{=\sum_{i=0}^{n} \binom{n}{i} \left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C \text{ (by Lemma 9.7)}} (x)$$

(here, we renamed the index i as n in the sum)

$$= \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C\right)(x).$$

Compared to[33]

$$\left(\left(e^{*f}\otimes e^{*f}\right)\circ\Delta_C\right)(x)$$

$$=\left(e^{*f}\otimes e^{*f}\right)\left(\underbrace{\Delta_C(x)}_{=\sum\limits_{j=1}^{m}\lambda_j a_j\otimes b_j}\right)=\left(e^{*f}\otimes e^{*f}\right)\left(\sum_{j=1}^{m}\lambda_j a_j\otimes b_j\right)$$

$$=\sum_{j=1}^{m}\lambda_j\quad\underbrace{e^{*f}(a_j)}_{\substack{=\sum\limits_{i\geq 0}\frac{f^{*i}(a_j)}{i!}\\ \text{(by (6), applied to } a_j \\ \text{instead of } x)}}\quad\otimes\quad\underbrace{e^{*f}(b_j)}_{\substack{=\sum\limits_{i\geq 0}\frac{f^{*i}(b_j)}{i!}\\ \text{(by (6), applied to } b_j \\ \text{instead of } x)}}$$

$$=\sum_{j=1}^{m}\lambda_j\left(\sum_{i\geq 0}\frac{f^{*i}(a_j)}{i!}\right)\otimes\left(\sum_{i\geq 0}\frac{f^{*i}(b_j)}{i!}\right)=\sum_{j=1}^{m}\lambda_j\left(\sum_{i\geq 0}\frac{f^{*i}(a_j)}{i!}\right)\otimes\left(\sum_{\ell\geq 0}\frac{f^{*\ell}(b_j)}{\ell!}\right)$$

(here, we renamed the index i as ℓ in the third sum)

$$=\sum_{j=1}^{m}\lambda_j\sum_{i\geq 0}\sum_{\ell\geq 0}\frac{f^{*i}(a_j)}{i!}\otimes\frac{f^{*\ell}(b_j)}{\ell!}=\sum_{j=1}^{m}\lambda_j\underbrace{\sum_{i\geq 0}\sum_{\substack{n\geq 0;\\ i\leq n}}}_{=\sum\limits_{n\geq 0}\sum\limits_{\substack{i\geq 0;\\ i\leq n}}}\frac{f^{*i}(a_j)}{i!}\otimes\frac{f^{*(n-i)}(b_j)}{(n-i)!}$$

(here, we substituted n for $i+\ell$ in the third sum)

[33]The following computation is a manipulation with infinite sums. Such manipulations may be dangerous, since infinite sums (even when they converge) may fail to satisfy some of the rules one would expect infinite sums to satisfy: For example, switching two summation signs might not always preserve the sum. However, the specific computation that we are going to do is safe from such troubles, for the following reasons:

- Whenever a sum appears in the computation, it has the property that all but finitely many of its addends are zero.
- Whenever two summation signs get switched in the computation, they have the property that all but finitely many addends of the resulting **double sum** are zero. (For example, we can transform the "$\sum\limits_{j=1}^{m}\sum\limits_{n\geq 0}\sum\limits_{\substack{i\geq 0;\\ i\leq n}}$" into "$\sum\limits_{n\geq 0}\sum\limits_{\substack{i\geq 0;\\ i\leq n}}\sum\limits_{j=1}^{m}$" in the triple sum $\sum\limits_{j=1}^{m}\sum\limits_{n\geq 0}\sum\limits_{\substack{i\geq 0;\\ i\leq n}}\lambda_j\frac{f^{*i}(a_j)}{i!}\otimes\frac{f^{*(n-i)}(b_j)}{(n-i)!}$, because all but finitely many **triples** $(j,n,i)\in\{1,2,\ldots,m\}\times\mathbb{N}\times\mathbb{N}$ satisfying $i\leq n$ satisfy $\lambda_j\frac{f^{*i}(a_j)}{i!}\otimes\frac{f^{*(n-i)}(b_j)}{(n-i)!}=0$.)

$$= \sum_{j=1}^{m} \lambda_j \sum_{n\geq 0} \sum_{\substack{i\geq 0;\\ i\leq n}} \frac{f^{*i}(a_j)}{i!} \otimes \frac{f^{*(n-i)}(b_j)}{(n-i)!} = \sum_{j=1}^{m} \sum_{n\geq 0} \sum_{\substack{i\geq 0;\\ i\leq n}} \lambda_j \frac{f^{*i}(a_j)}{i!} \otimes \frac{f^{*(n-i)}(b_j)}{(n-i)!}$$

$$= \sum_{n\geq 0} \underbrace{\sum_{\substack{i\geq 0;\\ i\leq n}}}_{=\sum_{i=0}^{n}} \underbrace{\sum_{j=1}^{m} \lambda_j \frac{f^{*i}(a_j)}{i!} \otimes \frac{f^{*(n-i)}(b_j)}{(n-i)!}}_{=\frac{1}{n!}\binom{n}{i}\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)} \quad \text{(by (40))}$$

$$= \sum_{n\geq 0} \sum_{i=0}^{n} \frac{1}{n!}\binom{n}{i}\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x) = \sum_{n\geq 0}\frac{1}{n!}\sum_{i=0}^{n}\binom{n}{i}\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)$$

$$= \sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x),$$

this yields

$$\left(\Delta_H \circ e^{*f}\right)(x) = \left(\left(e^{*f}\otimes e^{*f}\right)\circ\Delta_C\right)(x).$$

Since this holds for every $x \in C$, we thus conclude that $\Delta_H \circ e^{*f} = \left(e^{*f}\otimes e^{*f}\right)\circ\Delta_C$.

On the other hand, every $x \in C$ satisfies

$$\left(\varepsilon_H \circ e^{*f}\right)(x) = \varepsilon_H\left(e^{*f}(x)\right) = \varepsilon_H\left(\sum_{i\geq 0}\underbrace{\frac{f^{*i}(x)}{i!}}_{=\frac{1}{i!}f^{*i}(x)}\right) \qquad \text{(by (6))}$$

$$= \varepsilon_H\left(\sum_{i\geq 0}\frac{1}{i!}f^{*i}(x)\right) = \sum_{i\geq 0}\frac{1}{i!}\varepsilon_H\left(f^{*i}(x)\right) \qquad \text{(since } \varepsilon_H \text{ is } k\text{-linear)}$$

$$= \underbrace{\frac{1}{0!}}_{=\frac{1}{1}=1}\varepsilon_H\left(\underbrace{f^{*0}}_{=e_{C,H}=\eta_H\circ\varepsilon_C}(x)\right) + \sum_{i\geq 1}\frac{1}{i!}\underbrace{\varepsilon_H\left(f^{*i}(x)\right)}_{=(\varepsilon_H\circ f^{*i})(x)}$$

$$= \underbrace{\varepsilon_H\left(\left(\eta_H\circ\varepsilon_C\right)(x)\right)}_{=(\varepsilon_H\circ\eta_H\circ\varepsilon_C)(x)} + \sum_{i\geq 1}\frac{1}{i!}\underbrace{\left(\varepsilon_H\circ f^{*i}\right)}_{\substack{=0\\ \text{(by Lemma 9.8,}\\ \text{applied to } n=i\text{)}}}(x)$$

$$= \left(\underbrace{\varepsilon_H\circ\eta_H}_{\substack{=\mathrm{id}\\ \text{(by the axioms of a bialgebra,}\\ \text{since } H \text{ is a bialgebra)}}}\circ\varepsilon_C\right)(x) + \sum_{i\geq 1}\frac{1}{i!}\underbrace{0(x)}_{=0} = \varepsilon_C(x) + \underbrace{\sum_{i\geq 1}\frac{1}{i!}0}_{=0} = \varepsilon_C(x).$$

Thus, $\varepsilon_H \circ e^{*f} = \varepsilon_C$. Combined with $\Delta_H \circ e^{*f} = \left(e^{*f}\otimes e^{*f}\right)\circ\Delta_C$, this yields that e^{*f} is a k-coalgebra homomorphism. This proves Lemma 8.2. $\square$

Now that we have proved Lemma 8.2, let us formulate three easy corollaries of Lemma 9.1 and Proposition 9.3 **(b)**. We will not use them in this paper until §22, but they are commonly used elsewhere:

Corollary 9.9. Let k be a field. Let C and D be k-coalgebras. Let A and B be k-algebras. Let $p : C \to A$, $q : C \to A$, $r : D \to B$ and $s : D \to B$ be four k-linear maps. Then,

$$(p \otimes r) * (q \otimes s) = (p * q) \otimes (r * s)$$

(this is an equality between two maps $C \otimes D \to A \otimes B$). Here, $(p \otimes r) * (q \otimes s)$ denotes the convolution of the two k-linear maps $p \otimes r : C \otimes D \to A \otimes B$ and $q \otimes s : C \otimes D \to A \otimes B$. (This convolution is well-defined, since $C \otimes D$ is a k-coalgebra and $A \otimes B$ is a k-algebra.)

Corollary 9.10. Let k be a field. Let C and D be k-coalgebras. Let A and B be k-algebras. Let $f : C \to A$ and $g : D \to B$ be two k-linear maps. Let maps $e_{C,A} : C \to A$ and $e_{D,B} : D \to B$ be defined as in Definition 1.12. Then,

$$(f \otimes e_{D,B}) * (e_{C,A} \otimes g) = f \otimes g = (e_{C,A} \otimes g) * (f \otimes e_{D,B})$$

(this is an equality between two maps $C \otimes D \to A \otimes B$). Here, $*$ denotes the convolution of the k-linear maps $C \otimes D \to A \otimes B$. (This convolution is well-defined, since $C \otimes D$ is a k-coalgebra and $A \otimes B$ is a k-algebra.)

Corollary 9.11. Let k be a field. Let C and D be k-coalgebras. Let A and B be k-algebras. Let a map $e_{D,B} : D \to B$ be defined as in Definition 1.12. Recall that $C \otimes D$ is a k-coalgebra and $A \otimes B$ is a k-algebra; hence, $\mathcal{L}(C \otimes D, A \otimes B)$ becomes a k-algebra with respect to convolution.

(a) For any two k-linear maps $f : C \to A$ and $g : C \to A$, we have

$$(f \otimes e_{D,B}) * (g \otimes e_{D,B}) = (f * g) \otimes e_{D,B}$$

(this is an equality between two maps $C \otimes D \to A \otimes B$).

(b) We have $e_{C,A} \otimes e_{D,B} = e_{C \otimes D, A \otimes B}$.

(c) For any k-linear map $f : C \to A$ and any $i \in \mathbb{N}$, we have $(f \otimes e_{D,B})^{*i} = f^{*i} \otimes e_{D,B}$.

Proof of Corollary 9.9. By the definition of the k-algebra $A \otimes B$, we have $\mu_{A \otimes B} = (\mu_A \otimes \mu_B) \circ (\mathrm{id}_A \otimes \tau_{B,A} \otimes \mathrm{id}_B)$, where $\tau_{B,A}$ is defined according to Definition 9.2.

By the definition of the k-coalgebra $C \otimes D$, we have $\Delta_{C \otimes D} = (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D)$, where $\tau_{C,D}$ is defined according to Definition 9.2.

Now, by the definition of convolution,

$$\begin{aligned}
&(p \otimes r) * (q \otimes s) \\
&= \underbrace{\mu_{A \otimes B}}_{= (\mu_A \otimes \mu_B) \circ \left(\mathrm{id}_A \otimes \tau_{B,A} \otimes \mathrm{id}_B\right)} \circ \underbrace{((p \otimes r) \otimes (q \otimes s))}_{= p \otimes r \otimes q \otimes s} \circ \underbrace{\Delta_{C \otimes D}}_{= \left(\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D\right) \circ (\Delta_C \otimes \Delta_D)} \\
&= (\mu_A \otimes \mu_B) \circ \underbrace{(\mathrm{id}_A \otimes \tau_{B,A} \otimes \mathrm{id}_B) \circ (p \otimes r \otimes q \otimes s)}_{\substack{= (p \otimes q \otimes r \otimes s) \circ \left(\mathrm{id}_C \otimes \tau_{D,C} \otimes \mathrm{id}_D\right) \\ \text{(by Proposition 9.3 \textbf{(b)}, applied to} \\ U=C,\ V=D,\ W=C,\ T=D,\ U'=A,\ V'=B,\ W'=A,\ T'=B, \\ e=p,\ f=r,\ g=q \text{ and } h=s)}} \circ (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D) \\
&= (\mu_A \otimes \mu_B) \circ (p \otimes q \otimes r \otimes s) \circ (\mathrm{id}_C \otimes \tau_{D,C} \otimes \mathrm{id}_D) \circ (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D) \,.
\end{aligned} \tag{41}$$

Recall that any two k-vector spaces V and W satisfy $\tau_{V,W} \circ \tau_{W,V} = \mathrm{id}_{W \otimes V}$. Applied to $V = D$ and $W = C$, this yields $\tau_{D,C} \circ \tau_{C,D} = \mathrm{id}_{C \otimes D}$. Hence, $\underbrace{(\tau_{D,C} \circ \tau_{C,D})}_{= \mathrm{id}_{C \otimes D}} \otimes \mathrm{id}_D =$ $\mathrm{id}_{C \otimes D} \otimes \mathrm{id}_D = \mathrm{id}_{C \otimes D \otimes D}$. But since

$$(\tau_{D,C} \circ \tau_{C,D}) \otimes \underbrace{\mathrm{id}_D}_{= \mathrm{id}_D \circ \mathrm{id}_D} = (\tau_{D,C} \circ \tau_{C,D}) \otimes (\mathrm{id}_D \circ \mathrm{id}_D) = (\tau_{D,C} \otimes \mathrm{id}_D) \circ (\tau_{C,D} \otimes \mathrm{id}_D)$$

(by (21), applied to $U = C \otimes D$, $V = D \otimes C$, $W = C \otimes D$, $U' = D$, $V' = D$, $W' = D$, $\alpha = \tau_{C,D}$, $\beta = \tau_{D,C}$, $\alpha' = \mathrm{id}_D$, $\beta' = \mathrm{id}_D$), this becomes

$$(\tau_{D,C} \otimes \mathrm{id}_D) \circ (\tau_{C,D} \otimes \mathrm{id}_D) = \mathrm{id}_{C \otimes D \otimes D} \,.$$

Hence,

$$\mathrm{id}_C \otimes \underbrace{((\tau_{D,C} \otimes \mathrm{id}_D) \circ (\tau_{C,D} \otimes \mathrm{id}_D))}_{= \mathrm{id}_{C \otimes D \otimes D}} = \mathrm{id}_C \otimes \mathrm{id}_{C \otimes D \otimes D} = \mathrm{id}_{C \otimes C \otimes D \otimes D} \,.$$

But since

$$\begin{aligned}
\underbrace{\mathrm{id}_C}_{= \mathrm{id}_C \circ \mathrm{id}_C} \otimes ((\tau_{D,C} \otimes \mathrm{id}_D) \circ (\tau_{C,D} \otimes \mathrm{id}_D)) &= (\mathrm{id}_C \circ \mathrm{id}_C) \otimes ((\tau_{D,C} \otimes \mathrm{id}_D) \circ (\tau_{C,D} \otimes \mathrm{id}_D)) \\
&= (\mathrm{id}_C \otimes \tau_{D,C} \otimes \mathrm{id}_D) \circ (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D)
\end{aligned}$$

(by (21), applied to $U = C$, $V = C$, $W = C$, $U' = C \otimes D \otimes D$, $V' = D \otimes C \otimes D$, $W' = C \otimes D \otimes D$, $\alpha = \mathrm{id}_C$, $\beta = \mathrm{id}_C$, $\alpha' = \tau_{C,D} \otimes \mathrm{id}_D$, $\beta' = \tau_{D,C} \otimes \mathrm{id}_D$), this becomes

$$(\mathrm{id}_C \otimes \tau_{D,C} \otimes \mathrm{id}_D) \circ (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D) = \mathrm{id}_{C \otimes C \otimes D \otimes D} \,.$$

Hence, (41) becomes

$$\begin{aligned}
&(p \otimes r) * (q \otimes s) \\
&= (\mu_A \otimes \mu_B) \circ (p \otimes q \otimes r \otimes s) \circ \underbrace{(\mathrm{id}_C \otimes \tau_{D,C} \otimes \mathrm{id}_D) \circ (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D)}_{= \mathrm{id}_{C \otimes C \otimes D \otimes D}} \circ (\Delta_C \otimes \Delta_D) \\
&= (\mu_A \otimes \mu_B) \circ (p \otimes q \otimes r \otimes s) \circ (\Delta_C \otimes \Delta_D) = (p * q) \otimes (r * s)
\end{aligned}$$

(by Lemma 9.1). This proves Corollary 9.9. $\square$

Proof of Corollary 9.10. Applying Corollary 9.9 to $p = f$, $q = e_{C,A}$, $r = e_{D,B}$ and $s = g$, we obtain

$$(f \otimes e_{D,B}) * (e_{C,A} \otimes g) = \underbrace{(f * e_{C,A})}_{=f} \otimes \underbrace{(e_{D,B} * g)}_{=g} = f * g.$$

Applying Corollary 9.9 to $p = e_{C,A}$, $q = f$, $r = g$ and $s = e_{D,B}$, we obtain

$$(e_{C,A} \otimes g) * (f \otimes e_{D,B}) = \underbrace{(e_{C,A} * f)}_{=f} \otimes \underbrace{(g * e_{D,B})}_{=g} = f * g.$$

Thus, we have shown that $(f \otimes e_{D,B}) * (e_{C,A} \otimes g) = f * g = (e_{C,A} \otimes g) * (f \otimes e_{D,B})$. This proves Corollary 9.10. □

Proof of Corollary 9.11. **(a)** Let $f : C \to A$ and $g : C \to A$ be two k-linear maps. Applying Corollary 9.9 to $p = f$, $q = g$, $r = e_{D,B}$ and $s = e_{D,B}$, we obtain

$$(f \otimes e_{D,B}) * (g \otimes e_{D,B}) = (f * g) \otimes \underbrace{(e_{D,B} * e_{D,B})}_{=e_{D,B}} = (f * g) \otimes e_{D,B}.$$

This proves Corollary 9.11 **(a)**.

(b) We have

$$e_{C\otimes D, A\otimes B} = \underbrace{\eta_{A\otimes B}}_{\substack{=\eta_A\otimes\eta_B \\ \text{(by the definition of} \\ \text{the } k\text{-algebra } A\otimes B)}} \circ \underbrace{\varepsilon_{C\otimes D}}_{\substack{=\varepsilon_C\otimes\varepsilon_D \\ \text{(by the definition of} \\ \text{the } k\text{-coalgebra } C\otimes D)}} \qquad \text{(by the definition of } e_{C\otimes D, A\otimes B})$$
$$= (\eta_A \otimes \eta_B) \circ (\varepsilon_C \otimes \varepsilon_D)$$

and

$$\underbrace{e_{C,A}}_{\substack{=\eta_A\circ\varepsilon_C \\ \text{(by the definition of } e_{C,A})}} \otimes \underbrace{e_{D,B}}_{\substack{=\eta_B\circ\varepsilon_D \\ \text{(by the definition of } e_{D,B})}} = (\eta_A \circ \varepsilon_C)\otimes(\eta_B \circ \varepsilon_D) = (\eta_A \otimes \eta_B)\circ(\varepsilon_C \otimes \varepsilon_D)$$

(by (21), applied to $U = C$, $V = k$, $W = A$, $U' = D$, $V' = k$, $W' = B$, $\alpha = \varepsilon_C$, $\beta = \eta_A$, $\alpha' = \varepsilon_D$ and $\beta' = \eta_B$). Thus, $e_{C\otimes D, A\otimes B} = (\eta_A \otimes \eta_B) \circ (\varepsilon_C \otimes \varepsilon_D) = e_{C,A} \otimes e_{D,B}$. This proves Corollary 9.11 **(b)**.

(c) We are going to prove Corollary 9.11 **(c)** by induction over i:

Induction base: For every k-linear map $f : C \to A$, we have

$$(f \otimes e_{D,B})^{*0} = e_{C\otimes D, A\otimes B} = \underbrace{e_{C,A}}_{=f^{*0}} \otimes e_{D,B} \qquad \text{(by Corollary 9.11 } \textbf{(b)}\text{)}$$
$$= f^{*0} \otimes e_{D,B}.$$

In other words, Corollary 9.11 **(c)** holds for $i = 0$. This completes the induction base.

Induction step: Let $n \in \mathbb{N}$. Assume that Corollary 9.11 **(c)** holds for $i = n$. Now we will prove that Corollary 9.11 **(c)** also holds for $i = n + 1$.

Let $f : C \to A$ be a k-linear map. Then, $(f \otimes e_{D,B})^{*n} = f^{*n} \otimes e_{D,B}$ (since Corollary 9.11 **(c)** holds for $i = n$). Now,

$$\begin{aligned}(f \otimes e_{D,B})^{*(n+1)} &= (f \otimes e_{D,B}) * \underbrace{(f \otimes e_{D,B})^{*n}}_{=f^{*n} \otimes e_{D,B}} = (f \otimes e_{D,B}) * (f^{*n} \otimes e_{D,B}) \\ &= \underbrace{(f * f^{*n})}_{=f^{*(n+1)}} \otimes e_{D,B} \qquad \text{(by Corollary 9.11 \textbf{(a)}, applied to } g = f^{*n}) \\ &= f^{*(n+1)} \otimes e_{D,B}.\end{aligned}$$

Thus, Corollary 9.11 **(c)** holds for $i = n + 1$. We thus have completed the induction step. The induction proof of Corollary 9.11 **(c)** is thus complete. □

§10. The product of coalgebra homomorphisms

The next result will be used in our proof of Lemma 8.3, but is actually much more fundamental and important than Lemma 8.3:

Proposition 10.1. Let k be a field. Let C be a cocommutative k-coalgebra. Let H be a k-bialgebra. Let $f : C \to H$ and $g : C \to H$ be two k-coalgebra homomorphisms. Then, $f*g : C \to H$ is also a k-coalgebra homomorphism.

The proof of this proposition is similar to (but much simpler than!) the induction step in the proof of Lemma 9.7 above. (It is simpler because we don't have to work with sums, so we do not need distributivity and k-bilinearity of tensoring and composition.) Here are the details that any reader should be able to see on his own anyway:

Proof of Proposition 10.1. Since f is a k-coalgebra homomorphism, we have $\Delta_H \circ f = (f \otimes f) \circ \Delta_C$ and $\varepsilon_H \circ f = \varepsilon_C$. Since g is a k-coalgebra homomorphism, we have $\Delta_H \circ g = (g \otimes g) \circ \Delta_C$ and $\varepsilon_H \circ g = \varepsilon_C$.

By the definition of convolution, $f * g = \mu_H \circ (f \otimes g) \circ \Delta_C$, so that

$$\begin{aligned}\Delta_H \circ (f * g) &= \underbrace{\Delta_H \circ \mu_H}_{\substack{=(\mu_H \otimes \mu_H) \circ \left(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H\right) \circ (\Delta_H \otimes \Delta_H) \\ \text{(by the axioms of a bialgebra, since } H \text{ is a bialgebra)}}} \circ (f \otimes g) \circ \Delta_C \\ &= (\mu_H \otimes \mu_H) \circ (\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ (\Delta_H \otimes \Delta_H) \circ (f \otimes g) \circ \Delta_C. \qquad (42)\end{aligned}$$

But an application of (21) yields $(\Delta_H \circ f) \otimes (\Delta_H \circ g) = (\Delta_H \otimes \Delta_H) \circ (f \otimes g)$, so that

$$\begin{aligned}&(\Delta_H \otimes \Delta_H) \circ (f \otimes g) \\ &= \underbrace{(\Delta_H \circ f)}_{=(f \otimes f) \circ \Delta_C} \otimes \underbrace{(\Delta_H \circ g)}_{=(g \otimes g) \circ \Delta_C} \\ &= ((f \otimes f) \circ \Delta_C) \otimes ((g \otimes g) \circ \Delta_C) \\ &= (f \otimes f \otimes g \otimes g) \circ (\Delta_C \otimes \Delta_C) \\ &\qquad \left(\begin{array}{c} \text{by (21), applied to } U = C,\ V = C \otimes C,\ W = H \otimes H,\ U' = C,\ V' = C \otimes C, \\ W' = H \otimes H,\ \alpha = \Delta_C,\ \beta = f \otimes f,\ \alpha' = \Delta_C \text{ and } \beta' = g \otimes g \end{array} \right).\end{aligned}$$

Hence, (42) becomes

$$\begin{aligned}
&\Delta_H \circ (f * g) \\
&= (\mu_H \otimes \mu_H) \circ (\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ \underbrace{(\Delta_H \otimes \Delta_H) \circ (f \otimes g)}_{=(f \otimes f \otimes g \otimes g) \circ (\Delta_C \otimes \Delta_C)} \circ \Delta_C \\
&= (\mu_H \otimes \mu_H) \circ \underbrace{(\mathrm{id}_H \otimes \tau_{H,H} \otimes \mathrm{id}_H) \circ (f \otimes f \otimes g \otimes g)}_{=(f \otimes g \otimes f \otimes g) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)} \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C \\
&\qquad \begin{array}{c}\text{(by Proposition 9.3 \textbf{(b)}, applied to } C,\ C,\ C,\ C, \\ H,\ H,\ H,\ H,\ f,\ f,\ g,\ g \text{ instead of} \\ U,\ V,\ W,\ T,\ U',\ V',\ W',\ T',\ e,\ f,\ g,\ h)\end{array} \\
&= (\mu_H \otimes \mu_H) \circ (f \otimes g \otimes f \otimes g) \circ \underbrace{(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C}_{\substack{=(\Delta_C \otimes \Delta_C) \circ \Delta_C \\ \text{(by (26))}}} \\
&= \underbrace{(\mu_H \otimes \mu_H) \circ (f \otimes g \otimes f \otimes g) \circ (\Delta_C \otimes \Delta_C)}_{\substack{=(f*g) \otimes (f*g) \\ \text{(by Lemma 9.1, applied to } A=H,\ B=H,\ D=C,\ p=f,\ q=g,\ r=f \text{ and } s=g)}} \circ \Delta_C \\
&= ((f * g) \otimes (f * g)) \circ \Delta_C.
\end{aligned}$$

Also, let us denote by μ_k the canonical isomorphism $k \otimes k \to k$. Then, μ_k is the multiplication map of the k-algebra k. By the axioms of a bialgebra, ε_H is a k-algebra homomorphism (since H is a bialgebra); thus, $\varepsilon_H \circ \mu_H = \mu_k \circ (\varepsilon_H \otimes \varepsilon_H)$. On the other hand, $(\varepsilon_H \circ f) \otimes (\varepsilon_H \circ g) = (\varepsilon_H \otimes \varepsilon_H) \circ (f \otimes g)$ (by an application of (21)). Using these equalities, we have

$$\begin{aligned}
\varepsilon_H \circ \underbrace{(f * g)}_{=\mu_H \circ (f \otimes g) \circ \Delta_C} &= \underbrace{\varepsilon_H \circ \mu_H}_{=\mu_k \circ (\varepsilon_H \otimes \varepsilon_H)} \circ (f \otimes g) \circ \Delta_C = \mu_k \circ \underbrace{(\varepsilon_H \otimes \varepsilon_H) \circ (f \otimes g)}_{=(\varepsilon_H \circ f) \otimes (\varepsilon_H \circ g)} \circ \Delta_C \\
&= \mu_k \circ \left(\underbrace{(\varepsilon_H \circ f)}_{=\varepsilon_C} \otimes \underbrace{(\varepsilon_H \circ g)}_{=\varepsilon_C} \right) \circ \Delta_C = \mu_k \circ (\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C.
\end{aligned}$$

But from the axioms of a coalgebra, it is easy to see that $\mu_k \circ (\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C = \varepsilon_C$ [34]. Altogether, we thus have

$$\varepsilon_H \circ (f * g) = \mu_k \circ (\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C = \varepsilon_C.$$

Combined with $\Delta_H \circ (f * g) = ((f * g) \otimes (f * g)) \circ \Delta_C$, this yields that $f * g$ is a k-coalgebra homomorphism. This proves Proposition 10.1. □

As a consequence, we have:

[34] *Proof.* Every $x \in C$ satisfies $((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x) = \varepsilon_C(x)\, 1 \otimes 1$ (by Lemma 9.6 **(a)**) and thus

$$\begin{aligned}
(\mu_k \circ (\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x) &= \mu_k \left(\underbrace{((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x)}_{=\varepsilon_C(x) 1 \otimes 1} \right) = \mu_k (\varepsilon_C(x)\, 1 \otimes 1) \\
&= \varepsilon_C(x) \qquad \text{(by the definition of } \mu_k).
\end{aligned}$$

Hence, $\mu_k \circ (\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C = \varepsilon_C$, qed.

Corollary 10.2. Let k be a field. Let C be a cocommutative k-coalgebra. Let H be a k-bialgebra. Let $f : C \to H$ be a k-coalgebra homomorphism. Let $n \in \mathbb{N}$. Then, $f^{*n} : C \to H$ is also a k-coalgebra homomorphism.

Proof of Corollary 10.2. We are going to prove Corollary 10.2 by induction over n.

Induction base: Consider the obvious canonical k-coalgebra structure on k (with Δ_k being the canonical isomorphism $k \to k \otimes k$, and ε_k being the identity map). Lemma 9.6 **(b)** shows that $\varepsilon_C : C \to k$ is a k-coalgebra homomorphism. Combined with the fact that $\eta_H : k \to H$ is a k-coalgebra homomorphism (because H is a k-bialgebra), this yields that $\eta_H \circ \varepsilon_C$ is a k-coalgebra homomorphism (since the composition of two k-coalgebra homomorphisms is a k-coalgebra homomorphism). Since $f^{*0} = e_{C,H} = \eta_H \circ \varepsilon_C$ (by the definition of $e_{C,H}$), this yields that f^{*0} is a k-coalgebra homomorphism. In other words, Corollary 10.2 holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that Corollary 10.2 holds for $n = N$. We must now prove that Corollary 10.2 also holds for $n = N + 1$.

Since Corollary 10.2 holds for $n = N$, we know that f^{*N} is a k-coalgebra homomorphism. Proposition 10.1 (applied to $g = f^{*N}$) now yields that $f * f^{*N}$ is a k-coalgebra homomorphism. Since $f * f^{*N} = f^{*(N+1)}$, this yields that $f^{*(N+1)}$ is a k-coalgebra homomorphism. In other words, Corollary 10.2 holds for $n = N + 1$. This completes the induction step. The induction proof of Corollary 10.2 is thus complete. □

§11. The addition-to-multiplication property of the exponent

One more thing we need about exponentiation (the map $\mathfrak{g}(C, H) \to G(C, H)$, $f \mapsto e^{*f}$) is the following property (which gives us the moral claim to call it exponentiation!):

Proposition 11.1. Let k be a field of characteristic 0. Let C be a connected filtered k-coalgebra. Let H be a k-algebra. Let $f \in \mathfrak{g}(C, H)$ and $g \in \mathfrak{g}(C, H)$ be such that $f * g = g * f$. Then, $e^{*(f+g)} = e^{*f} * e^{*g}$.

Note that the condition $f * g = g * f$ in this proposition can be replaced by the stronger condition that C be cocommutative and H be commutative: In fact, whenever C is cocommutative and H is commutative, it is easy to see that any two k-linear maps $f : C \to H$ and $g : C \to H$ satisfy $f * g = g * f$. We are not going to use and prove this, though.

Before we prove Proposition 11.1, let us state a basic fact in noncommutative algebra:

Proposition 11.2. Let k be a field. Let A be a k-algebra. Let S be a subset of A such that the k-algebra A is generated by S. Assume that any two elements of S commute. Then, the k-algebra A is commutative.

Proposition 11.2 is usually stated in the form "a k-algebra generated by pairwise commuting generators must be commutative".

Proof of Proposition 11.2. For every $a \in A$, let $Z(a)$ denote the subset

$$\{b \in A \mid ab = ba\}$$

of A. Then, for every $a \in A$, the subset $Z(a)$ of A is a k-subalgebra of A [35].

The k-algebra A is generated by S. In other words, the k-subalgebra of A generated by S is A. In other words, A is the k-subalgebra of A generated by S. In other words, A is the smallest k-subalgebra of A which contains S as a subset (because the k-subalgebra of A generated by S is the smallest k-subalgebra of A which contains S as a subset). Hence,

$$\left(\begin{array}{c} \text{whenever } U \text{ is a } k\text{-subalgebra of } A \text{ which contains } S \text{ as} \\ \text{a subset, we must necessarily have } A \subseteq U \end{array} \right). \tag{43}$$

Now, fix an $s \in S$. We know that for every $a \in A$, the subset $Z(a)$ of A is a k-subalgebra of A. Applying this to $a = s$, we obtain the following: The subset $Z(s)$ of A is a k-subalgebra of A (since we know that for every $a \in A$, the subset $Z(a)$ of A is a k-subalgebra of A). But we have $S \subseteq Z(s)$ [36]. Hence, $Z(s)$ contains S as a subset.

Now, we know that $Z(s)$ is a k-subalgebra of A which contains S as a subset. Hence, (43) (applied to $U = Z(s)$) yields $Z(s) = A$. Thus, $A = Z(s) = \{b \in A \mid sb = bs\}$ (by the definition of $Z(s)$).

Now, forget that we fixed $s \in S$. We thus have shown that every $s \in S$ satisfies $A = \{b \in A \mid sb = bs\}$.

Now, fix some $a \in A$. Recall that the subset $Z(a)$ of A is a k-subalgebra of A. Moreover, $S \subseteq Z(a)$. [37] In other words, $Z(a)$ contains S as a subset.

---

[35] *Proof.* Let $a \in A$. The definition of $Z(a)$ yields $Z(a) = \{b \in A \mid ab = ba\}$.

We know that 0 is an element of A and satisfies $a \cdot 0 = 0 \cdot a$ (since $a \cdot 0 = 0 = 0 \cdot a$). In other words, $0 \in \{b \in A \mid ab = ba\} = Z(a)$.

We know that 1 is an element of A and satisfies $a \cdot 1 = 1 \cdot a$ (since $a \cdot 1 = a = 1 \cdot a$). In other words, $1 \in \{b \in A \mid ab = ba\} = Z(a)$.

Let $c \in Z(a)$ and $d \in Z(a)$. Then, $c \in Z(a) = \{b \in A \mid ab = ba\}$. In other words, c is an element of A and satisfies $ac = ca$. Also, $d \in Z(a) = \{b \in A \mid ab = ba\}$. In other words, d is an element of A and satisfies $ad = da$. Now, $a(c+d) = \underbrace{ac}_{=ca} + \underbrace{ad}_{=da} = ca + da = (c+d)a$ and $\underbrace{ac}_{=ca} d = c \underbrace{ad}_{=da} = cda$.

So we know that $c + d$ is an element of A and satisfies $a(c+d) = (c+d)a$. In other words, $c + d \in \{b \in A \mid ab = ba\} = Z(a)$. Also, cd is an element of A and satisfies $acd = cda$. In other words, $cd \in \{b \in A \mid ab = ba\} = Z(a)$.

Now, forget that we fixed c and d. We thus have shown that every $c \in Z(a)$ and $d \in Z(a)$ satisfy $c + d \in Z(a)$ and $cd \in Z(a)$.

Next, let $\lambda \in k$ and $c \in Z(a)$. Then, $c \in Z(a) = \{b \in A \mid ab = ba\}$. In other words, c is an element of A and satisfies $ac = ca$. Now, λc is an element of A and satisfies $a(\lambda c) = (\lambda c)a$ (since $a(\lambda c) = \lambda \underbrace{ac}_{=ca} = \lambda ca = (\lambda c)a$). In other words, $\lambda c \in \{b \in A \mid ab = ba\} = Z(a)$. So we know that λc is an element of A and satisfies $\lambda c \in Z(a)$. Combined with the fact that every $c \in Z(a)$ and $d \in Z(a)$ satisfy $c + d \in Z(a)$, and combined with the fact that $0 \in Z(a)$, this yields that $Z(a)$ is a k-vector subspace of A. Combined with the fact that $1 \in Z(a)$, and combined with the fact that $c \in Z(a)$ and $d \in Z(a)$ satisfy $cd \in Z(a)$, this yields that $Z(a)$ is a k-subalgebra of A, qed.

[36] *Proof.* Let $t \in S$. Then, t is an element of S. Also, the elements s and t of S commute (since any two elements of S commute). Thus, $st = ts$. Now, the definition of $Z(s)$ yields $Z(s) = \{b \in A \mid sb = bs\}$. But t is an element of A and satisfying $st = ts$. In other words, $t \in \{b \in A \mid sb = bs\} = Z(s)$.

Now, forget that we fixed t. We thus have proven that every $t \in S$ satisfies $t \in Z(s)$. In other words, $S \subseteq Z(s)$, qed.

[37] *Proof.* Let $s \in S$. We have $a \in A = \{b \in A \mid sb = bs\}$. In other words, a is an element of A and satisfies $sa = as$. Thus, $as = sa$.

Now, we know that $Z(a)$ is a k-subalgebra of A which contains A as a subset. Hence, (43) (applied to $U = Z(a)$) yields $Z(a) = A$. Hence, $A = Z(a)$.

Now let $c \in A$ be arbitrary. Then, $c \in A = Z(a) = \{b \in A \mid ab = ba\}$ (by the definition of $Z(a)$). In other words, c is an element of A and satisfies $ac = ca$.

Now, forget that we fixed a and c. We thus have proven that every $a \in A$ and $c \in A$ satisfy $ac = ca$. In other words, the k-algebra A is commutative. Proposition 11.2 is proven. □

We record a corollary of Proposition 11.2 for easy reference:

Corollary 11.3. Let k be a field. Let A be a k-algebra. Let f and g be two elements of A. Assume that f and g commute. Let $\mathfrak{H}$ be the k-subalgebra of A generated by f and g. Then, the k-algebra $\mathfrak{H}$ is commutative.

Proof of Corollary 11.3. Let $S = \{f, g\}$. Recall that $\mathfrak{H}$ is the k-subalgebra of A generated by f and g. In other words,

$$\begin{aligned}\mathfrak{H} &= (\text{the } k\text{-subalgebra of } A \text{ generated by } f \text{ and } g) \\ &= \left(\text{the } k\text{-subalgebra of } A \text{ generated by } \underbrace{\{f, g\}}_{=S}\right) \\ &= (\text{the } k\text{-subalgebra of } A \text{ generated by } S) \supseteq S.\end{aligned}$$

Thus, S is a subset of $\mathfrak{H}$. Moreover, the k-algebra $\mathfrak{H}$ is generated by S (because $\mathfrak{H} =$ (the k-subalgebra of A generated by S)). Finally, any two elements of S commute.[38] Hence, Proposition 11.2 (applied to $\mathfrak{H}$ instead of A) yields that the k-algebra $\mathfrak{H}$ is commutative. This proves Corollary 11.3. □

But recall that the definition of $Z(a)$ yields $Z(a) = \{b \in A \mid ab = ba\}$. Now, s is an element of a and satisfies $as = sa$. In other words, $s \in \{b \in A \mid ab = ba\} = Z(a)$.

Now, forget that we fixed s. We thus have proven that every $s \in S$ satisfies $s \in Z(a)$. In other words, $S \subseteq Z(a)$, qed.

[38] *Proof.* Let u and v be two elements of S. We are going to prove that $uv = vu$.

We have $u \in S = \{f, g\}$. Hence, we must be in one of the following two cases:

Case 1: We have $u = f$.

Case 2: We have $u = g$.

Let us consider Case 1 first. In this case, we have $u = f$.

We have $v \in S = \{f, g\}$. Hence, we must be in one of the following two subcases:

Subcase 1.1: We have $v = f$.

Subcase 1.2: We have $v = g$.

Let us first consider Subcase 1.1. In this subcase, we have $v = f$. Now, $\underbrace{u}_{=f}\underbrace{v}_{=f} = ff$ and $\underbrace{v}_{=f}\underbrace{u}_{=f} = ff$. Hence, $uv = ff = vu$. Thus, $uv = vu$ is proven in Subcase 1.1.

Let us next consider Subcase 1.2. In this subcase, we have $v = g$. Now, $\underbrace{u}_{=f}\underbrace{v}_{=g} = fg$ and $\underbrace{v}_{=g}\underbrace{u}_{=f} = gf$. Hence, $uv = fg = gf = vu$. Thus, $uv = vu$ is proven in Subcase 1.2.

We now have proven $uv = vu$ in each of the two Subcases 1.1 and 1.2. Since these two Subcases cover the whole Case 1, this yields that $uv = vu$ always holds in Case 1.

Let us now consider Case 2. In this case, we must have $u = g$.

We have $v \in S = \{f, g\}$. Hence, we must be in one of the following two subcases:

Subcase 2.1: We have $v = f$.

Subcase 2.2: We have $v = g$.

Proof of Proposition 11.1. Let $x \in C$. By (6) (applied to $f * g$ instead of f), we have

$$e^{*(f+g)}(x) = \sum_{i \geq 0} \frac{(f+g)^{*i}(x)}{i!}. \tag{44}$$

We have $f * g = g * f$. In other words, f and g commute (as elements of $\mathcal{L}(C, H)$). Now, let $\mathfrak{H}$ be the k-subalgebra of $\mathcal{L}(C, H)$ generated by f and g. Then, the k-algebra $\mathfrak{H}$ is commutative (by Corollary 11.3, applied to $A = \mathcal{L}(C, H)$).

Thus, $\mathfrak{H}$ is a commutative k-algebra. Hence, we can calculate inside $\mathfrak{H}$ as in any commutative algebra; in particular, we thus obtain $(f+g)^{*i} = \sum_{j=0}^{i} \binom{i}{j} f^{*j} * g^{*(i-j)}$ (by the binomial formula) for every $i \in \mathbb{N}$. Hence, (44) becomes

$$\begin{aligned}
e^{*(f+g)}(x) &= \sum_{i \geq 0} \frac{\left(\sum_{j=0}^{i} \binom{i}{j} f^{*j} * g^{*(i-j)} \right)(x)}{i!} = \sum_{i \geq 0} \frac{\sum_{j=0}^{i} \binom{i}{j} \left(f^{*j} * g^{*(i-j)} \right)(x)}{i!} \\
&= \sum_{i \geq 0} \frac{1}{i!} \sum_{j=0}^{i} \binom{i}{j} \left(f^{*j} * g^{*(i-j)} \right)(x) \\
&= \sum_{i \geq 0} \underbrace{\sum_{j=0}^{i}}_{= \sum\limits_{\substack{j \geq 0; \\ j \leq i}}} \underbrace{\frac{1}{i!} \binom{i}{j}}_{= \frac{1}{j!\,(i-j)!}} \left(f^{*j} * g^{*(i-j)} \right)(x) \\
&\qquad \left(\text{since } \binom{i}{j} = \frac{i!}{j!\,(i-j)!} \right) \\
&= \sum_{i \geq 0} \sum_{\substack{j \geq 0; \\ j \leq i}} \frac{1}{j!\,(i-j)!} \left(f^{*j} * g^{*(i-j)} \right)(x). \qquad (45)
\end{aligned}$$

Since $\Delta_C(x)$ is a tensor in $C \otimes C$, we can write $\Delta_C(x)$ as $\Delta_C(x) = \sum_{\ell=1}^{m} \lambda_\ell a_\ell \otimes b_\ell$ for some $m \in \mathbb{N}$, some elements a_1, a_2, ..., a_m of C, and some elements b_1, b_2, ..., b_m of C. Consider this m, these a_1, a_2, ..., a_m, and these b_1, b_2, ..., b_m. Then, every $i \in \mathbb{N}$

Let us first consider Subcase 2.1. In this subcase, we have $v = f$. Now, $\underbrace{u}_{=g} \underbrace{v}_{=f} = gf$ and $\underbrace{v}_{=f} \underbrace{u}_{=g} = fg = gf$. Hence, $uv = gf = vu$. Thus, $uv = vu$ is proven in Subcase 2.1.

Let us next consider Subcase 2.2. In this subcase, we have $v = g$. Now, $\underbrace{u}_{=g} \underbrace{v}_{=g} = gg$ and $\underbrace{v}_{=g} \underbrace{u}_{=g} = gg$. Hence, $uv = gg = vu$. Thus, $uv = vu$ is proven in Subcase 2.2.

We now have proven $uv = vu$ in each of the two Subcases 2.1 and 2.2. Since these two Subcases cover the whole Case 2, this yields that $uv = vu$ always holds in Case 2.

We now have proven $uv = vu$ in each of the two Cases 1 and 2. Since these two Cases cover all possibilities, this yields that $uv = vu$ always holds. In other words, u and v commute.

Now, forget that we fixed u and v. We thus have shown that u and v commute for any two elements u and v of S. In other words, any two elements of S commute, qed.

and $j \in \mathbb{N}$ satisfy

$$\underbrace{\left(f^{*j} * g^{*i}\right)}_{=\mu_H \circ \left(f^{*j} \otimes g^{*i}\right) \circ \Delta_C \text{ (by the definition of convolution)}} (x)$$

$$= \left(\mu_H \circ \left(f^{*j} \otimes g^{*i}\right) \circ \Delta_C\right)(x) = \mu_H \left(\left(f^{*j} \otimes g^{*i}\right) \left(\underbrace{\Delta_C(x)}_{=\sum_{\ell=1}^{m} \lambda_\ell a_\ell \otimes b_\ell}\right)\right)$$

$$= \mu_H \left(\underbrace{\left(f^{*j} \otimes g^{*i}\right)\left(\sum_{\ell=1}^{m} \lambda_\ell a_\ell \otimes b_\ell\right)}_{=\sum_{\ell=1}^{m} \lambda_\ell f^{*j}(a_\ell) \otimes g^{*i}(b_\ell)}\right) = \mu_H \left(\sum_{\ell=1}^{m} \lambda_\ell f^{*j}(a_\ell) \otimes g^{*i}(b_\ell)\right)$$

$$= \sum_{\ell=1}^{m} \lambda_\ell f^{*j}(a_\ell)\, g^{*i}(b_\ell) \qquad \text{(since } \mu_H \text{ is the multiplication map)}. \tag{46}$$

On the other hand,[39]

$$\underbrace{\left(e^{*f} * e^{*g}\right)}_{\substack{=\mu_H \circ \left(e^{*f} \otimes e^{*g}\right) \circ \Delta_C \\ \text{(by the definition of convolution)}}} (x)$$

$$= \left(\mu_H \circ \left(e^{*f} \otimes e^{*g}\right) \circ \Delta_C\right)(x) = \mu_H \left(\left(e^{*f} \otimes e^{*g}\right) \left(\underbrace{\Delta_C(x)}_{=\sum_{\ell=1}^{m} \lambda_\ell a_\ell \otimes b_\ell}\right)\right)$$

$$= \mu_H \left(\underbrace{\left(e^{*f} \otimes e^{*g}\right)\left(\sum_{\ell=1}^{m} \lambda_\ell a_\ell \otimes b_\ell\right)}_{=\sum_{\ell=1}^{m} \lambda_\ell e^{*f}(a_\ell) \otimes e^{*g}(b_\ell)}\right)$$

$$= \mu_H \left(\sum_{\ell=1}^{m} \lambda_\ell e^{*f}(a_\ell) \otimes e^{*g}(b_\ell)\right) = \sum_{\ell=1}^{m} \lambda_\ell \quad \underbrace{e^{*f}(a_\ell)}_{\substack{=\sum_{i \geq 0} \frac{f^{*i}(a_\ell)}{i!} \\ \text{(by (6), applied} \\ \text{to } a_\ell \text{ instead of } x)}} \quad \underbrace{e^{*g}(b_\ell)}_{\substack{=\sum_{i \geq 0} \frac{g^{*i}(b_\ell)}{i!} \\ \text{(by (6), applied} \\ \text{to } b_\ell \text{ and } g \text{ instead of } x \text{ and } f)}}$$

(because μ_H is the multiplication map)

[39]The following computation is a manipulation with infinite sums. Such manipulations may be dangerous, since infinite sums (even when they converge) may fail to satisfy some of the rules one would expect infinite sums to satisfy: For example, switching two summation signs might not always preserve the sum. However, the specific computation that we are going to do is safe from such troubles, for the following reasons:

- Whenever a sum appears in the computation, it has the property that all but finitely many of its addends are zero.
- Whenever two summation signs get switched in the computation, they have the property that all but finitely many addends of the resulting **double sum** are zero. (For example, we can transform the "$\sum\limits_{j \geq 0} \sum\limits_{\substack{i \geq 0; \\ j \leq i}}$" into "$\sum\limits_{i \geq 0} \sum\limits_{\substack{j \geq 0; \\ j \leq i}}$" in the double sum $\sum\limits_{j \geq 0} \sum\limits_{\substack{i \geq 0; \\ j \leq i}} \dfrac{1}{j!\,(i-j)!} \left(f^{*j} * g^{*(i-j)}\right)(x)$, because all but finitely many **pairs** $(i, j) \in \mathbb{N}^{\times 2}$ satisfying $j \leq i$ satisfy $\dfrac{1}{j!\,(i-j)!} \left(f^{*j} * g^{*(i-j)}\right)(x) = 0$.)

$$= \sum_{\ell=1}^{m} \lambda_\ell \left(\sum_{i \geq 0} \frac{f^{*i}(a_\ell)}{i!} \right) \left(\sum_{i \geq 0} \frac{g^{*i}(b_\ell)}{i!} \right) = \sum_{\ell=1}^{m} \lambda_\ell \left(\sum_{j \geq 0} \frac{f^{*j}(a_\ell)}{j!} \right) \left(\sum_{i \geq 0} \frac{g^{*i}(b_\ell)}{i!} \right)$$

(here, we renamed the index i as j in the second sum)

$$= \sum_{\ell=1}^{m} \lambda_\ell \sum_{j \geq 0} \sum_{i \geq 0} \underbrace{\frac{f^{*j}(a_\ell)}{j!} \frac{g^{*i}(b_\ell)}{i!}}_{= \frac{1}{j!i!} f^{*j}(a_\ell) g^{*i}(b_\ell)} = \sum_{\ell=1}^{m} \lambda_\ell \sum_{j \geq 0} \sum_{i \geq 0} \frac{1}{j!i!} f^{*j}(a_\ell) g^{*i}(b_\ell)$$

$$= \sum_{j \geq 0} \sum_{i \geq 0} \frac{1}{j!i!} \underbrace{\sum_{\ell=1}^{m} \lambda_\ell f^{*j}(a_\ell) g^{*i}(b_\ell)}_{= \left(f^{*j} * g^{*i}\right)(x) \text{ (by (46))}} = \sum_{j \geq 0} \sum_{i \geq 0} \frac{1}{j!i!} \left(f^{*j} * g^{*i}\right)(x)$$

$$= \sum_{j \geq 0} \underbrace{\sum_{i \geq j}}_{= \sum\limits_{\substack{i \geq 0; \\ i \geq j}} = \sum\limits_{\substack{i \geq 0; \\ j \leq i}}} \frac{1}{j!(i-j)!} \left(f^{*j} * g^{*(i-j)}\right)(x)$$

(here, we substituted $i-j$ for i in the second sum)

$$= \underbrace{\sum_{j \geq 0} \sum_{\substack{i \geq 0; \\ j \leq i}}}_{= \sum\limits_{i \geq 0} \sum\limits_{\substack{j \geq 0; \\ j \leq i}}} \frac{1}{j!(i-j)!} \left(f^{*j} * g^{*(i-j)}\right)(x) = \sum_{i \geq 0} \sum_{\substack{j \geq 0; \\ j \leq i}} \frac{1}{j!(i-j)!} \left(f^{*j} * g^{*(i-j)}\right)(x).$$

Compared to (45), this yields $\left(e^{*f} * e^{*g}\right)(x) = e^{*(f+g)}(x)$. Since this is proven for all $x \in C$, we can conclude that $e^{*f} * e^{*g} = e^{*(f+g)}$. Proposition 11.1 is thus proven. □

As a consequence, we can describe the natural powers of exponentials:

Corollary 11.4. Let k be a field of characteristic 0. Let C be a connected filtered k-coalgebra. Let H be a k-algebra. Let $f \in \mathfrak{g}(C, H)$ and $n \in \mathbb{N}$. Then, $e^{*(nf)} = \left(e^{*f}\right)^{*n}$.

We could extend this corollary to hold for all $n \in \mathbb{Z}$ (it is not a priori clear that e^{*f} is invertible as an element of $\mathcal{L}(C, H)$, but it is true), but we won't need this extension, so we don't prove it.

Proof of Corollary 11.4. We are going to prove Corollary 11.4 by induction over n:

Induction base: We have $e^{*0} = e_{C,H}$ [40]. Thus, $e^{*(0f)} = e^{*0} = e_{C,H} = \left(e^{*f}\right)^{*0}$. In other words, Corollary 11.4 holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$ be arbitrary. Assume that Corollary 11.4 holds for $n = N$. We now must prove that Corollary 11.4 also holds for $n = N + 1$.

Since Corollary 11.4 holds for $n = N$, we have $e^{*(Nf)} = \left(e^{*f}\right)^{*N}$. Since $f * (Nf) = N(f * f) = (Nf) * f$, we can apply Proposition 11.1 to $g = Nf$, and conclude that $e^{*(f+Nf)} = e^{*f} * e^{*(Nf)}$. Since $(N+1) f = f + Nf$, we now have

$$e^{*((N+1)f)} = e^{*(f+Nf)} = e^{*f} * \underbrace{e^{*(Nf)}}_{=\left(e^{*f}\right)^{*N}} = e^{*f} * \left(e^{*f}\right)^{*N} = \left(e^{*f}\right)^{*(N+1)}.$$

In other words, Corollary 11.4 holds for $n = N+1$. This completes the induction step. Thus, the induction proof of Corollary 11.4 is done. □

§12. The "coalgebra homomorphism $\Longrightarrow$ $(\varepsilon, \varepsilon)$-coderivation" direction

Our proof of Lemma 8.3 will further need the following, purely linear-algebraic fact about filtered vector spaces over a field of characteristic 0.

Proposition 12.1. Let k be a field of characteristic 0. Let V be a filtered k-vector space. Let W be a k-vector space. For every $n \in \mathbb{N}$, let $h_n : V \to W$ be a k-linear map such that $h_n(V_{\leq n-1}) = 0$.

(a) Then, for every $x \in V$ and every $t \in \mathbb{Z}$, the element $\sum_{i \geq 0} t^i h_i(x) \in W$ is well-defined, i. e., the infinite sum $\sum_{i \geq 0} t^i h_i(x)$ converges with respect to the discrete topology.

(b) Assume that every $x \in V$ and every $t \in \mathbb{N}$ satisfy $\sum_{i \geq 0} t^i h_i(x) = 0$. Then, $h_n = 0$ for every $n \in \mathbb{N}$.

To get an intuition for this proposition, we should note that part **(a)** is more or less trivial (we have to use that every $x \in V$ lies in V_n for some high enough n), and

[40] *Proof.* Every $x \in C$ satisfies

$$\begin{aligned} e^{*0}(x) &= \sum_{i \geq 0} \frac{0^{*i}(x)}{i!} \qquad \text{(by (6), applied to 0 instead of } f\text{)} \\ &= \underbrace{\frac{0^{*0}(x)}{0!}}_{= \frac{0^{*0}(x)}{1} = 0^{*0}(x)} + \sum_{i \geq 1} \underbrace{\frac{0^{*i}(x)}{i!}}_{\substack{=0 \text{ (since } 0^{*i}(x) = 0 \\ \text{(due to } i \geq 1\text{))}}} \\ &= \underbrace{0^{*0}}_{= e_{C,H}}(x) + \underbrace{\sum_{i \geq 1} 0}_{=0} = e_{C,H}(x). \end{aligned}$$

Thus, $e^{*0} = e_{C,H}$, qed.

part **(b)** is an assertion of the kind "if a polynomial in one variable vanishes on every $t \in \mathbb{N}$, then it must be the zero polynomial". Note that part **(b)** is the only part which uses the condition that k be of characteristic 0. There are two easy ways to prove part **(b)**: one is by using Vandermonde determinants, the other by finite differences. We are going to follow the second way here. The proof will need the following theorem as an auxiliary result:

Theorem 12.2. Let k be a commutative ring with unity. Let $N \in \mathbb{N}$. Then, the equalities

$$\sum_{t=0}^{N} (-1)^t \binom{N}{t} t^\ell = 0 \qquad \text{for every } \ell \in \{0, 1, \ldots, N-1\} \tag{47}$$

and

$$\sum_{t=0}^{N} (-1)^t \binom{N}{t} t^N = (-1)^N N! \tag{48}$$

are satisfied in k.

Proof of Theorem 12.2. Theorem 12.2 is identical with Theorem 1 of [QEDMO09], with the only difference that the R and the k from Theorem 1 of [QEDMO09] have been renamed as k and t in Theorem 12.2. Since Theorem 1 of [QEDMO09] is proven in [QEDMO09], we thus don't need to prove Theorem 12.2 here. □

Proof of Proposition 12.1. First we notice that

$$h_n(V_{\leq i}) = 0 \qquad \text{for any } n \in \mathbb{N} \text{ and } i \in \mathbb{N} \text{ satisfying } i < n \tag{49}$$

[41].

(a) Let $x \in V$ and $t \in \mathbb{Z}$. Since V is filtered, there exists some $n \in \mathbb{N}$ such that $x \in V_{\leq n}$. Consider such an n.

Every integer $i > n$ satisfies $h_i(V_{\leq n}) = 0$ (by (49), applied to i and n instead of n and i) and thus $h_i(x) = 0$ (since $x \in V_{\leq n}$ and therefore $h_i(x) \in h_i(V_{\leq n}) = 0$, so that $h_i(x) = 0$), so that $t^i h_i(x) = 0$. Hence, for every integer $i > n$, the i-th addend of the infinite sum $\sum_{i \geq 0} t^i h_i(x)$ is zero. Hence, this infinite sum $\sum_{i \geq 0} t^i h_i(x)$ has only finitely many nonzero addends. Thus, this sum converges with respect to the discrete topology. Proposition 12.1 **(a)** is thus proven.

(b) Assume that every $x \in V$ and every $t \in \mathbb{N}$ satisfy $\sum_{i \geq 0} t^i h_i(x) = 0$. We are now going to show that

$$\text{every } x \in V \text{ and every } n \in \mathbb{N} \text{ satisfy } h_n(x) = 0. \tag{50}$$

Proof of (50). Fix some $x \in V$. We then must prove that $h_n(x) = 0$ for every $n \in \mathbb{N}$.

Since V is filtered, there exists some $j \in \mathbb{N}$ such that $x \in V_{\leq j}$. Consider such a j.

[41] *Proof.* Let $n \in \mathbb{N}$ and $i \in \mathbb{N}$ satisfy $i < n$. Then, $i \leq n-1$ (since i and n are integers) and thus $V_{\leq i} \subseteq V_{\leq n-1}$ (since $(V_{\leq \ell})_{\ell \geq 0}$ is a filtration). Hence, $h_n(V_{\leq i}) \subseteq h_n(V_{\leq n-1}) = 0$. In other words, $h_n(V_{\leq i}) = 0$. This proves (49).

Every integer $n > j$ satisfies $h_n(x) \in h_n(V_{\leq j})$ (since $x \in V_{\leq j}$) and $h_n(V_{\leq j}) = 0$ (by (49), applied to j instead of i). Hence, every integer $n > j$ satisfies $h_n(x) \in h_n(V_{\leq j}) = 0$. In other words, every integer $n > j$ satisfies $h_n(x) = 0$.

Now we are going to prove that

$$\text{for every } \ell \in \{0, 1, \ldots, j+1\}, \text{ every integer } n > j - \ell \text{ satisfies } h_n(x) = 0. \tag{51}$$

[42]

Proof of (51). We are going to prove (51) by induction over ℓ:

Induction base: For $\ell = 0$, every integer $n > j - \ell$ satisfies $h_n(x) = 0$. [43] In other words, (51) holds for $\ell = 0$. This completes the induction base.

Induction step: Let $L \in \{0, 1, \ldots, j\}$. Assume that (51) holds for $\ell = L$. In order to complete the induction step, we must then prove that (51) also holds for $\ell = L + 1$.

We know that

$$\text{every integer } n > j - L \text{ satisfies } h_n(x) = 0 \tag{52}$$

(because (51) holds for $\ell = L$). Now, let n be an integer such that $n > j - (L+1)$. We are going to prove that $h_n(x) = 0$.

Proof of $h_n(x) = 0$: First we notice that $n > j - (L+1) = j - L - 1$. Since n and $j - L$ are integers, this yields $n \geq (j - L - 1) + 1 = j - L$. Hence, two cases are possible:

Case 1: We have $n > j - L$.

Case 2: We have $n = j - L$.

In Case 1, we trivially have $h_n(x) = 0$ (by (52)).

Now consider Case 2. In this case, $n = j - L$. Notice that $n = j - L \in \mathbb{N}$ (since $L \in \{0, 1, \ldots, j\}$). For every $t \in \mathbb{N}$, we have

$$\begin{aligned} 0 &= \sum_{i \geq 0} t^i h_i(x) \qquad \text{(by our assumption)} \\ &= \sum_{i=0}^{j-L} t^i h_i(x) + \sum_{i > j-L} t^i \underbrace{h_i(x)}_{\substack{=0 \\ \text{(by (52), applied to } i \text{ instead of } n\text{)}}} = \sum_{i=0}^{j-L} t^i h_i(x) + \underbrace{\sum_{i > j-L} t^i 0}_{=0} = \sum_{i=0}^{j-L} t^i h_i(x). \end{aligned} \tag{53}$$

Clearly,

$$\sum_{t=0}^{N} (-1)^t \binom{j-L}{t} \underbrace{\left(\sum_{i=0}^{j-L} t^i h_i(x) \right)}_{=0 \text{ (by (53))}} = \sum_{t=0}^{N} (-1)^t \binom{j-L}{t} 0 = 0.$$

[42] Note that for $\ell = 0$, this is pretty much obvious, whereas for $\ell = j + 1$, this is our goal.

[43] *Proof.* Let $\ell = 0$. We know that every integer $n > j$ satisfies $h_n(x) = 0$. Since $j = j - \underbrace{0}_{=\ell} = j - \ell$, this rewrites as follows: Every integer $n > j - \ell$ satisfies $h_n(x) = 0$, qed.

Compared to

$$\sum_{t=0}^{j-L}(-1)^t\binom{j-L}{t}\left(\sum_{i=0}^{j-L}t^i h_i(x)\right)$$
$$=\sum_{i=0}^{j-L}\left(\sum_{t=0}^{j-L}(-1)^t\binom{j-L}{t}t^i\right)h_i(x)$$
$$=\sum_{i=0}^{j-L-1}\underbrace{\left(\sum_{t=0}^{j-L}(-1)^t\binom{j-L}{t}t^i\right)}_{\substack{=0\\ \text{(by (47), applied to } N=j-L \text{ and } \ell=i)}}h_i(x)+\underbrace{\left(\sum_{t=0}^{j-L}(-1)^t\binom{j-L}{t}t^{j-L}\right)}_{\substack{=(-1)^{j-L}(j-L)!\\ \text{(by (48), applied to } N=j-L)}}h_{j-L}(x)$$
$$=\underbrace{\sum_{i=0}^{j-L-1}0h_i(x)}_{=0}+(-1)^{j-L}(j-L)!h_{j-L}(x)=(-1)^{j-L}(j-L)!h_{j-L}(x),$$

this yields

$$(-1)^{j-L}(j-L)!h_{j-L}(x)=0.$$

Since $(-1)^{j-L}(j-L)!$ is invertible in k (because k has characteristic 0), this simplifies to $h_{j-L}(x)=0$. Since $j-L=n$, this becomes $h_n(x)=0$. We thus have proven $h_n(x)=0$ in Case 2.

Hence, $h_n(x)=0$ is proven in both possible cases 1 and 2. This completes the proof of $h_n(x)=0$.

We have thus shown that

$$\text{every integer } n>j-(L+1) \text{ satisfies } h_n(x)=0.$$

In other words, we have shown that (51) holds for $\ell=L+1$. This completes the induction step (of the proof of (51)). Hence, the induction proof of (51) is complete.

Now we can apply (51) to $\ell=j+1$, and conclude that

$$\text{every integer } n>j-(j+1) \text{ satisfies } h_n(x)=0. \tag{54}$$

Thus, every $n\in\mathbb{N}$ satisfies $h_n(x)=0$ (because $n\in\mathbb{N}$ yields $n>-1=j-(j+1)$, and thus $h_n(x)=0$ by (54)).

So we have proven that for every $n\in\mathbb{N}$, every $x\in V$ satisfies $h_n(x)=0$. Thus, for every $n\in\mathbb{N}$, we have $h_n=0$ (because $h_n(x)=0$ for every $x\in V$). This proves Proposition 12.1 **(b)**. □

Our next result is a distillate of the proof of Lemma 8.2:

Lemma 12.3. Let k be a field of characteristic 0. Let C be a connected filtered k-coalgebra. Let H be a k-bialgebra. Let $f\in\mathfrak{g}(C,H)$. Let $x\in C$. Then,

$$\left(\Delta_H\circ e^{*f}\right)(x)=\sum_{n\geq 0}\frac{1}{n!}\left(\Delta_H\circ f^{*n}\right)(x) \tag{55}$$

and

$$\left(\left(e^{*f} \otimes e^{*f}\right) \circ \Delta_C\right)(x) = \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C \right)(x). \tag{56}$$

(In particular, the infinite sums $\sum_{n \geq 0} \frac{1}{n!} \left(\Delta_H \circ f^{*n}\right)(x)$ and $\sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C \right)(x)$ converge with respect to the discrete topology, i. e., each of these sums has only finitely many nonzero addends.)

Proof of Lemma 12.3. The equalities (55) and (56) have been proven during our proof of Lemma 8.2, *without using the assumptions that C be cocommutative and f be an $(\varepsilon, \varepsilon)$-coderivation.* Hence, these equalities are true. Lemma 12.3 is thus true. □

We now proceed to proving Lemma 8.3:

Proof of Lemma 8.3. Assume that e^{*f} is a k-coalgebra homomorphism.

For every $n \in \mathbb{N}$, define a k-linear map $h_n : C \to H$ by

$$h_n = \frac{1}{n!} \Delta_H \circ f^{*n} - \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} \left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C. \tag{57}$$

a) We now will prove that every $n \in \mathbb{N}$ satisfies $h_n\left(C_{\leq n-1}\right) = 0$.

Proof. Fix some $n \in \mathbb{N}$. If $n = 0$, then $h_n\left(C_{\leq n-1}\right) = 0$ is obviously true (since if $n = 0$, then $C_{\leq n-1} = C_{\leq 0-1} = 0$, so that $h\left(C_{\leq n-1}\right) = h\left(0\right) = 0$). Hence, we can WLOG assume (for the rest of the proof of **a)**) that $n \neq 0$. Then, $n \geq 1$. Thus, $n - 1 \in \mathbb{N}$.

We have $f^{*n}\left(C_{\leq n-1}\right) = 0$ (by Remark 3.5, applied to C, H, n and $n-1$ instead of H, A, i and n). On the other hand, since C is a filtered coalgebra, every $m \in \mathbb{N}$ satisfies $\Delta_C\left(C_{\leq m}\right) \subseteq \sum_{u=0}^{m} C_{\leq u} \otimes C_{\leq m-u}$. Applied to $m = n-1$, this yields $\Delta_C\left(C_{\leq n-1}\right) \subseteq$

$\sum\limits_{u=0}^{n-1} C_{\leq u} \otimes C_{\leq n-1-u}$. Thus, for every $i \in \{0,1,\ldots,n\}$, we have

$$\begin{aligned}
&\left(f^{*i} \otimes f^{*(n-i)}\right)\left(\Delta_C\left(C_{\leq n-1}\right)\right) \\
&\subseteq \left(f^{*i} \otimes f^{*(n-i)}\right)\left(\sum_{u=0}^{n-1} C_{\leq u} \otimes C_{\leq n-1-u}\right) \\
&= \sum_{u=0}^{n-1} \underbrace{\left(f^{*i} \otimes f^{*(n-i)}\right)\left(C_{\leq u} \otimes C_{\leq n-1-u}\right)}_{\subseteq f^{*i}\left(C_{\leq u}\right) \otimes f^{*(n-i)}\left(C_{\leq n-1-u}\right)} \subseteq \sum_{u=0}^{n-1} f^{*i}\left(C_{\leq u}\right) \otimes f^{*(n-i)}\left(C_{\leq n-1-u}\right) \\
&= \sum_{u=0}^{i-1} \underbrace{f^{*i}\left(C_{\leq u}\right)}_{\substack{=0 \text{ (by Remark 3.5} \\ \text{(applied to } C, H, i \text{ and } u \\ \text{instead of } H, A, i \text{ and } n), \\ \text{since } i>u)}} \otimes f^{*(n-i)}\left(C_{\leq n-1-u}\right) + \sum_{u=i}^{n-1} f^{*i}\left(C_{\leq u}\right) \otimes \underbrace{f^{*(n-i)}\left(C_{\leq n-1-u}\right)}_{\substack{=0 \text{ (by Remark 3.5} \\ \text{(applied to } C, H, n-i \text{ and } n-1-u \\ \text{instead of } H, A, i \text{ and } n), \\ \text{since } n-i>n-1-u \text{ (because} \\ i\leq u, \text{ so that } n-i\geq n-u>n-1-u))}} \\
&= \sum_{u=0}^{i-1} \underbrace{0 \otimes f^{*(n-i)}\left(C_{\leq n-1-u}\right)}_{=0} + \sum_{u=i}^{n-1} \underbrace{f^{*i}\left(C_{\leq u}\right) \otimes 0}_{=0} = \underbrace{\sum_{u=0}^{i-1} 0}_{=0} + \underbrace{\sum_{u=i}^{n-1} 0}_{=0} = 0+0=0. \qquad (58)
\end{aligned}$$

Now, (57) yields

$$\begin{aligned}
h_n\left(C_{\leq n-1}\right) &= \left(\frac{1}{n!}\Delta_H \circ f^{*n} - \frac{1}{n!}\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C\right)\left(C_{\leq n-1}\right) \\
&\subseteq \underbrace{\left(\frac{1}{n!}\Delta_H \circ f^{*n}\right)\left(C_{\leq n-1}\right)}_{=\frac{1}{n!}\left(\Delta_H \circ f^{*n}\right)\left(C_{\leq n-1}\right)} - \underbrace{\left(\frac{1}{n!}\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C\right)\left(C_{\leq n-1}\right)}_{=\frac{1}{n!}\left(\sum\limits_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)\left(C_{\leq n-1}\right)} \\
&= \frac{1}{n!}\underbrace{\left(\Delta_H \circ f^{*n}\right)\left(C_{\leq n-1}\right)}_{=\Delta_H\left(f^{*n}\left(C_{\leq n-1}\right)\right)} - \frac{1}{n!}\underbrace{\left(\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C\right)\left(C_{\leq n-1}\right)}_{\subseteq \sum\limits_{i=0}^{n}\binom{n}{i}\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)\left(C_{\leq n-1}\right)} \\
&= \frac{1}{n!}\Delta_H\left(\underbrace{f^{*n}\left(C_{\leq n-1}\right)}_{=0}\right) - \frac{1}{n!}\sum_{i=0}^{n}\binom{n}{i}\underbrace{\left(\left(f^{*i} \otimes f^{*(n-i)}\right) \circ \Delta_C\right)\left(C_{\leq n-1}\right)}_{=\left(f^{*i}\otimes f^{*(n-i)}\right)\left(\Delta_C\left(C_{\leq n-1}\right)\right)=0 \text{ (by (58))}} \\
&= \frac{1}{n!}\underbrace{\Delta_H\left(0\right)}_{=0} - \frac{1}{n!}\underbrace{\sum_{i=0}^{n}\binom{n}{i}0}_{=0} = \frac{1}{n!}0 - \frac{1}{n!}0 = 0-0=0.
\end{aligned}$$

Thus we have proven that every $n \in \mathbb{N}$ satisfies $h_n\left(C_{\leq n-1}\right) = 0$. In other words, **a)** is proven.

b) Now, we will show that every $x \in C$ and every $t \in \mathbb{N}$ satisfy $\sum_{i \geq 0} t^i h_i(x) = 0$. [44]

Proof. Let $x \in C$ and $t \in \mathbb{N}$ be arbitrary. By Corollary 10.2 (applied to t and e^{*f} instead of n and f), we see that $\left(e^{*f}\right)^{*t}$ is a k-coalgebra homomorphism. Since $e^{*(tf)} = \left(e^{*f}\right)^{*t}$ (by Corollary 11.4, applied to t instead of n), this rewrites as follows: The map $e^{*(tf)}$ is a k-coalgebra homomorphism. In other words,

$$\Delta_H \circ e^{*(tf)} = \left(e^{*(tf)} \otimes e^{*(tf)}\right) \circ \Delta_C \tag{59}$$

(by the definition of a k-coalgebra homomorphism).

But applying Lemma 12.3 to tf instead of f (this is allowed since $f \in \mathfrak{g}(C, H)$ yields $tf \in \mathfrak{g}(C, H)$), we obtain

$$\left(\Delta_H \circ e^{*(tf)}\right)(x) = \sum_{n \geq 0} \frac{1}{n!} \left(\Delta_H \circ (tf)^{*n}\right)(x) \tag{60}$$

and

$$\left(\left(e^{*(tf)} \otimes e^{*(tf)}\right) \circ \Delta_C\right)(x) = \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \left((tf)^{*i} \otimes (tf)^{*(n-i)}\right) \circ \Delta_C\right)(x). \tag{61}$$

We are now going to rewrite these two equalities by taking t out of the brackets.

Since

$$\sum_{n \geq 0} \frac{1}{n!} \left(\Delta_H \circ \underbrace{(tf)^{*n}}_{=t^n f^{*n}}\right)(x) = \sum_{n \geq 0} \frac{1}{n!} \left(\underbrace{\Delta_H \circ \left(t^n f^{*n}\right)}_{\substack{=t^n \cdot (\Delta_H \circ f^{*n}) \\ \text{(since composition of} \\ k\text{-linear maps is } k\text{-bilinear)}}}\right)(x) = \sum_{n \geq 0} \frac{1}{n!} \underbrace{\left(t^n \cdot (\Delta_H \circ f^{*n})\right)(x)}_{=t^n \cdot (\Delta_H \circ f^{*n})(x)}$$

$$= \sum_{n \geq 0} \frac{1}{n!} t^n \cdot \left(\Delta_H \circ f^{*n}\right)(x) = \sum_{n \geq 0} t^n \frac{1}{n!} \left(\Delta_H \circ f^{*n}\right)(x),$$

the equality (60) rewrites as

$$\left(\Delta_H \circ e^{*(tf)}\right)(x) = \sum_{n \geq 0} t^n \frac{1}{n!} \left(\Delta_H \circ f^{*n}\right)(x). \tag{62}$$

[44] Note that the element $\sum_{i \geq 0} t^i h_i(x)$ is well-defined due to Proposition 12.1 **(a)** (applied to $V = C$ and $W = H$).

Since

$$\sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(\underbrace{(tf)^{*i}}_{=t^i f^{*i}}\otimes\underbrace{(tf)^{*(n-i)}}_{=t^{n-i}f^{*(n-i)}}\right)\circ\Delta_C\right)(x)$$

$$=\sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(\underbrace{t^i f^{*i}\otimes t^{n-i}f^{*(n-i)}}_{\substack{=t^i t^{n-i}\cdot\left(f^{*i}\otimes f^{*(n-i)}\right)\\ \text{(since tensoring of } k\text{-linear maps}\\ \text{is } k\text{-bilinear)}}}\right)\circ\Delta_C\right)(x)$$

$$=\sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(\underbrace{t^i t^{n-i}}_{=t^n}\cdot\left(f^{*i}\otimes f^{*(n-i)}\right)\right)\circ\Delta_C\right)(x)$$

$$=\sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\underbrace{\left(t^n\cdot\left(f^{*i}\otimes f^{*(n-i)}\right)\right)\circ\Delta_C}_{\substack{=t^n\cdot\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)\\ \text{(since composition of } k\text{-linear}\\ \text{maps is } k\text{-bilinear)}}}\right)(x)$$

$$=\sum_{n\geq 0}\frac{1}{n!}\underbrace{\left(\sum_{i=0}^{n}\binom{n}{i}t^n\cdot\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)\right)(x)}_{=\sum\limits_{i=0}^{n}\binom{n}{i}t^n\cdot\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)}$$

$$=\sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}t^n\cdot\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)\right)=\sum_{n\geq 0}t^n\frac{1}{n!}\underbrace{\left(\sum_{i=0}^{n}\binom{n}{i}\left(\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)\right)}_{=\left(\sum\limits_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)}$$

$$=\sum_{n\geq 0}t^n\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)\,,$$

the equality (61) rewrites as

$$\left(\left(e^{*(tf)}\otimes e^{*(tf)}\right)\circ\Delta_C\right)(x)=\sum_{n\geq 0}t^n\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)\,.\qquad(63)$$

Now,

$$\begin{aligned}
\sum_{i\geq 0} t^i h_i(x) &= \sum_{n\geq 0} t^n h_n(x) \qquad \text{(here, we renamed the index } i \text{ as } n \text{ in the sum)} \\
&= \sum_{n\geq 0} t^n \underbrace{\left(\frac{1}{n!}\Delta_H \circ f^{*n} - \frac{1}{n!}\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)}_{=\frac{1}{n!}(\Delta_H\circ f^{*n})(x) - \frac{1}{n!}\left(\sum\limits_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)} \qquad \text{(by (57))} \\
&= \sum_{n\geq 0} t^n \left(\frac{1}{n!}\left(\Delta_H\circ f^{*n}\right)(x) - \frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)\right) \\
&= \underbrace{\sum_{n\geq 0} t^n \frac{1}{n!}\left(\Delta_H\circ f^{*n}\right)(x)}_{=\left(\Delta_H\circ e^{*(tf)}\right)(x) \text{ (by (62))}} - \underbrace{\sum_{n\geq 0} t^n \frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}\left(f^{*i}\otimes f^{*(n-i)}\right)\circ\Delta_C\right)(x)}_{=\left(\left(e^{*(tf)}\otimes e^{*(tf)}\right)\circ\Delta_C\right)(x) \text{ (by (63))}} \\
&= \underbrace{\left(\Delta_H\circ e^{*(tf)}\right)}_{=\left(e^{*(tf)}\otimes e^{*(tf)}\right)\circ\Delta_C \text{ (by (59))}}(x) - \left(\left(e^{*(tf)}\otimes e^{*(tf)}\right)\circ\Delta_C\right)(x) \\
&= \left(\left(e^{*(tf)}\otimes e^{*(tf)}\right)\circ\Delta_C\right)(x) - \left(\left(e^{*(tf)}\otimes e^{*(tf)}\right)\circ\Delta_C\right)(x) = 0.
\end{aligned}$$

We thus have proven that every $x \in C$ and every $t \in \mathbb{N}$ satisfy $\sum\limits_{i\geq 0} t^i h_i(x) = 0$. In other words, part **b)** of the proof is done.

c) We know that every $n \in \mathbb{N}$ satisfies $h_n\left(C_{\leq n-1}\right) = 0$ (by part **a)**), and that every $x \in C$ and every $t \in \mathbb{N}$ satisfy $\sum\limits_{i\geq 0} t^i h_i(x) = 0$ (by part **b)**). Hence, Proposition 12.1 **(b)** (applied to C and H instead of V and W) yields that $h_n = 0$ for every $n \in \mathbb{N}$. Applied to $n = 1$, this yields $h_1 = 0$. But (57) (applied to $n = 1$) yields

$$\begin{aligned}
h_1 &= \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1}\Delta_H \circ \underbrace{f^{*1}}_{=f} - \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1}\underbrace{\sum_{i=0}^{1}\binom{1}{i}\left(f^{*i}\otimes f^{*(1-i)}\right)\circ\Delta_C}_{=\binom{1}{0}\left(f^{*0}\otimes f^{*(1-0)}\right)\circ\Delta_C + \binom{1}{1}\left(f^{*1}\otimes f^{*(1-1)}\right)\circ\Delta_C} \\
&= \Delta_H\circ f - \left(\underbrace{\binom{1}{0}}_{=1}\left(\underbrace{f^{*0}}_{=e_{C,H}}\otimes\underbrace{f^{*(1-0)}}_{=f^{*1}=f}\right)\circ\Delta_C + \underbrace{\binom{1}{1}}_{=1}\left(\underbrace{f^{*1}}_{=f}\otimes\underbrace{f^{*(1-1)}}_{=f^{*0}=e_{C,H}}\right)\circ\Delta_C\right) \\
&= \Delta_H\circ f - \left(\left(e_{C,H}\otimes f\right)\circ\Delta_C + \left(f\otimes e_{C,H}\right)\circ\Delta_C\right).
\end{aligned}$$

Since $h_1 = 0$, this rewrites as

$$0 = \Delta_H\circ f - \left(\left(e_{C,H}\otimes f\right)\circ\Delta_C + \left(f\otimes e_{C,H}\right)\circ\Delta_C\right),$$

so that

$$\begin{aligned}\Delta_H \circ f &= (e_{C,H} \otimes f) \circ \Delta_C + (f \otimes e_{C,H}) \circ \Delta_C = (f \otimes e_{C,H}) \circ \Delta_C + (e_{C,H} \otimes f) \circ \Delta_C \\ &= (f \otimes e_{C,H} + e_{C,H} \otimes f) \circ \Delta_C \\ &\qquad \text{(since composition of } k\text{-linear maps is distributive)}.\end{aligned}$$

By the definition of "$(\varepsilon, \varepsilon)$-coderivation", this means that f is an $(\varepsilon, \varepsilon)$-coderivation.

We thus have proven that, under the assumption that e^{*f} is a k-coalgebra homomorphism, the map f is an $(\varepsilon, \varepsilon)$-coderivation. Thus, Lemma 8.3 is proven. □

Proof of Theorem 8.1. The assertion of Theorem 8.1 is an "if and only if" assertion. Its "if" part was proven in Lemma 8.3, and its "only if" part was proven in Lemma 8.2. Hence, both parts of the assertion of Theorem 8.1 are proven. This finally completes the proof of Theorem 8.1. □

§13. Proof of Theorem 4.1

Theorem 4.1 will now be merely a trivial consequence of the facts proven above.

Proof of Theorem 4.1. Let f be the map $\operatorname{Log} \mathrm{id} \in \mathcal{L}(H, H)$. Then, $f = \operatorname{Log} \mathrm{id} \in \mathfrak{g}(H, H)$ (because $\operatorname{Log} F \in \mathfrak{g}(H, H)$ for every $F \in G(H, H)$). Besides, $f = \operatorname{Log} \mathrm{id}$ yields $e^{*f} = e^{*(\operatorname{Log} \mathrm{id})} = \mathrm{id}$ (by Proposition 5.13 **(b)**, applied to $F = \mathrm{id}$ and $A = H$). Hence, e^{*f} is a k-coalgebra homomorphism. By Lemma 8.3 (applied to $C = H$), this yields that f is an $(\varepsilon, \varepsilon)$-coderivation.

But Theorem 7.2 (applied to $C = H$) tells us that f is an $(\varepsilon, \varepsilon)$-coderivation if and only if $f(H) \subseteq \operatorname{Prim} H$. Hence, $f(H) \subseteq \operatorname{Prim} H$ (since we know that f is an $(\varepsilon, \varepsilon)$-coderivation).

Proposition 6.2 **(c)** (applied to $F = \mathrm{id}$ and $A = H$) yields $(\operatorname{Log} \mathrm{id}) \mid_{\operatorname{Prim} H} = \mathrm{id} \mid_{\operatorname{Prim} H} = \mathrm{id}_{\operatorname{Prim} H}$. Since $\operatorname{Log} \mathrm{id} = f$, this rewrites as $f \mid_{\operatorname{Prim} H} = \mathrm{id}_{\operatorname{Prim} H}$.

So we know that f is a k-linear map satisfying $f(H) \subseteq \operatorname{Prim} H$ and $f \mid_{\operatorname{Prim} H} = \mathrm{id}_{\operatorname{Prim} H}$. In other words, f is a projection from H to the subspace $\operatorname{Prim} H$. Since $f = \operatorname{Log} \mathrm{id}$, this rewrites as follows: The map $\operatorname{Log} \mathrm{id}$ is a projection from H to the subspace $\operatorname{Prim} H$. Theorem 4.1 is therefore proven. □

§14. On the case of k being a ring

The above results have been formulated for k being a field (except of Theorem 12.2). However, all of them, apart from Propositions 5.15 and 5.16, still hold if k is just a commutative ring with unity, as long as the following replacements are made:

- Any occurrence of "k-vector space" must be replaced by "k-module".
- Any requirement that k be a field of characteristic 0 must be replaced by a requirement that k be a commutative $\mathbb{Q}$-algebra.
- The definition of the notion of a "filtered k-coalgebra" has to be replaced by the following Definition 14.1 (which is adjusted to the case of k being a commutative ring with unity):

Definition 14.1. Let k be a commutative ring with unity. Let C be a k-coalgebra and, at the same time, a filtered k-vector space. Then, C is said to be a *filtered k-coalgebra* if and only if every $n \in \mathbb{N}$ satisfies

$$\Delta_C\left(C_{\leq n}\right) \subseteq \sum_{u=0}^{n} \left(\iota_u \otimes \iota_{n-u}\right)\left(C_{\leq u} \otimes C_{\leq n-u}\right).$$

Here, for every $v \in \mathbb{N}$, we denote by ι_v the canonical inclusion $C_{\leq v} \to C$.

Note that this Definition 14.1 is not the only possible way to define a "filtered k-coalgebra" in the case of k being a commutative ring with unity. There might be the other definitions around, and possibly even non-equivalent ones. However, Definition 14.1 makes all of our results (except of Propositions 5.15 and 5.16) valid in the case of k being a commutative ring with unity. (I suspect that the other possible definitions also make them valid, but I am not sure, since there might always be some definition I haven't thought of.)

Here is the reason why Propositions 5.15 and 5.16 do not hold when k is a commutative ring with unity: If k is just a commutative ring with unity, then tensor products might behave strangely; in particular, if U, V, U', V' are k-modules such that $U \subseteq U'$ and $V \subseteq V'$, then we cannot in general identify $U \otimes V$ with a k-submodule of $U' \otimes V'$. (We still have a canonical map $U \otimes V \to U' \otimes V'$ obtained by tensoring the inclusion maps $U \to U'$ and $V \to V'$, but this map can fail to be injective.) Hence, the notion of a "subcoalgebra" becomes ambiguous: If we define a subcoalgebra of a coalgebra C to be a k-submodule D of C satisfying $\Delta_C\left(D\right) \subseteq \left(\iota \otimes \iota\right)\left(D \otimes D\right)$ (with ι being the inclusion map $D \to C$), then it is not true in general that a subcoalgebra D of a coalgebra C is a coalgebra, so that Proposition 5.16 makes no sense anymore! On the other hand, if we define a subcoalgebra of a coalgebra C to be a coalgebra D equipped with an injective coalgebra homomorphism $D \to C$, then Proposition 5.16 remains true, but I am not sure whether Proposition 5.15 still holds (at least our proof becomes hopelessly wrong).

While all of our results except of Propositions 5.15 and 5.16 still hold if k is just a commutative ring with unity, the same cannot be said about the proofs. Instead, we must take some more care. What is true is that all of our above proofs, except of the proofs of Propositions 5.13, 5.15 and 5.16, still hold if k is just a commutative ring with unity, as long as we make the following replacements:

- Any occurrence of "k-vector space" must be replaced by "k-module".
- Any requirement that k be a field of characteristic 0 must be replaced by a requirement that k be a commutative $\mathbb{Q}$-algebra.
- The definition of the notion of a "filtered k-coalgebra" has to be replaced by Definition 14.1.
- In some situations, inclusion maps have to be made more explicit. This means the following: Whenever we have four k-modules U, V, U', V' (they need not actually be called U, V, U', V') such that $U \subseteq U'$ and $V \subseteq V'$, then the assumption that k be a field allows us to identify $U \otimes V$ with a k-submodule of $U' \otimes V'$ (by abuse of notation). This identification has been done several times in our above proofs

(because we worked with the assumption that k be a field), in order to save space. In order to adjust the proofs to the case of k being just a commutative ring with unity, we have to get rid of this identification (because we can no longer identify $U \otimes V$ with a k-submodule of $U' \otimes V'$ when k is just a commutative ring with unity). This means that every time the notation $U \otimes V$ is used to mean a k-submodule of $U' \otimes V'$, we have to replace it by $\left(\iota_U \otimes \iota_V\right)(U \otimes V)$, where ι_U is the canonical inclusion $U' \to U$ and ι_V is the canonical inclusion $V' \to V$. (But when the notation $U \otimes V$ is used to mean just the k-module $U \otimes V$ itself, then it should stay a $U \otimes V$.) These replacements are straightforward and we are not going to perform them en detail. (Note that Definition 14.1 is exactly what comes out if we take the standard definition of a filtered k-coalgebra over a field k, and perform these replacements on that definition!)

However, even these replacement do not salvage our proof of Proposition 5.13 in the case when k is just a commutative ring with unity. In fact, this proof made use of Propositions 5.15 and 5.16, which both require k to be a field and are not valid otherwise (at least not in general). Hence, in the case when k is just a commutative ring with unity, we need a new proof of Proposition 5.13. We are going to provide one such proof. First, let us show an auxiliary result:

Proposition 14.2. Let k be a commutative ring with unity, let A be a k-algebra, and let H be a filtered k-coalgebra. For every $n \in \mathbb{N}$, the subset $\mathcal{L}^n(H, A)$ of $\mathcal{L}(H, A)$ is an ideal of the k-algebra $\mathcal{L}(H, A)$. (For the definition of $\mathcal{L}^n(H, A)$, see Definition 3.1 **(b)**.)

Proof of Proposition 14.2. In Definition 3.1 **(b)**, we defined $\mathcal{L}^n(H, A)$ by

$$\mathcal{L}^n(H, A) = \left\{ f \in \mathcal{L}(H, A) \mid f|_{H_{\leq n-1}} = 0 \right\}.$$

Thus it is easy to see that $\mathcal{L}^n(H, A)$ is a k-submodule of $\mathcal{L}(H, A)$. [45] Besides, $\mathcal{L}^n(H, A)$ is a left ideal of $\mathcal{L}(H, A)$ [46] and a right ideal of $\mathcal{L}(H, A)$ (similarly). Hence, $\mathcal{L}^n(H, A)$ is an ideal of $\mathcal{L}(H, A)$. Proposition 14.2 is thus proven. $\square$

[45] *Proof.* Let $\alpha \in k$, $\beta \in k$, $g \in \mathcal{L}^n(H, A)$ and $h \in \mathcal{L}^n(H, A)$ be arbitrary. Since $g \in \mathcal{L}^n(H, A) = \left\{ f \in \mathcal{L}(H, A) \mid f|_{H_{\leq n-1}} = 0 \right\}$, we have $g|_{H_{\leq n-1}} = 0$. Similarly, $h|_{H_{\leq n-1}} = 0$. Now,

$$(\alpha g + \beta h)|_{H_{\leq n-1}} = \alpha \underbrace{g|_{H_{\leq n-1}}}_{=0} + \beta \underbrace{h|_{H_{\leq n-1}}}_{=0} = \alpha 0 + \beta 0 = 0,$$

so that $\alpha g + \beta h \in \left\{ f \in \mathcal{L}(H, A) \mid f|_{H_{\leq n-1}} = 0 \right\} = \mathcal{L}^n(H, A)$.

Hence, we have proven that for every $\alpha \in k$, $\beta \in k$, $g \in \mathcal{L}^n(H, A)$ and $h \in \mathcal{L}^n(H, A)$, we have $\alpha g + \beta h \in \mathcal{L}^n(H, A)$. In other words, $\mathcal{L}^n(H, A)$ is a k-submodule of $\mathcal{L}(H, A)$.

[46] *Proof.* Let $g \in \mathcal{L}(H, A)$ and $h \in \mathcal{L}^n(H, A)$. Then, we are going to prove that $g * h \in \mathcal{L}^n(H, A)$.

If $n = 0$, then this is obvious (because $\mathcal{L}^0(H, A)$ is the whole k-module $\mathcal{L}(H, A)$), so let us now WLOG assume that $n \neq 0$. Then, $n \geq 1$, so that $n - 1 \in \mathbb{N}$.

We have $h \in \mathcal{L}^n(H, A) = \left\{ f \in \mathcal{L}(H, A) \mid f|_{H_{\leq n-1}} = 0 \right\}$, so that $h|_{H_{\leq n-1}} = 0$. We now get $h(H_{\leq n-1}) = \underbrace{\left(h|_{H_{\leq n-1}}\right)}_{=0}(H_{\leq n-1}) = 0(H_{\leq n-1}) = 0$.

Now, for every $v \in \mathbb{N}$, let ι_v denote the canonical inclusion map $H_{\leq v} \to H$. Then, by the definition of a filtered k-coalgebra (Definition 14.1), we have

$$\Delta_H(H_{\leq m}) \subseteq \sum_{u=0}^{m} \left(\iota_u \otimes \iota_{m-u}\right)(H_{\leq u} \otimes H_{\leq m-u}) \qquad \text{for every } m \in \mathbb{N}$$

Now we can finally prove the generalization of Proposition 5.13 to the case of k being a commutative ring with unity. Our proof will be similar to the one we gave above in the case of k being a field, but instead of restricting maps to $H_{\leq n}$ we will now consider their equivalence classes modulo the ideal $\mathcal{L}^{n+1}(H, A)$.

First we formulate the generalization of Proposition 5.13 to the case of k being a commutative ring with unity:

Proposition 14.3. Let k be a commutative $\mathbb{Q}$-algebra. Let A be a k-algebra, and let H be a connected filtered k-coalgebra.

(a) Every map $f \in \mathfrak{g}(H, A)$ satisfies $\operatorname{Log}\left(e^{*f}\right) = f$.

(b) Every map $F \in G(H, A)$ satisfies $e^{*(\operatorname{Log} F)} = F$.

Note that the following proof of Proposition 14.3 automatically gives us a second proof of Proposition 5.13, since Proposition 14.3 generalizes Proposition 5.13.

Proof of Proposition 14.3. Due to how we defined $\mathcal{L}^{n+1}(H, A)$ (in Definition 3.1 **(b)**), we have

$$\mathcal{L}^{n+1}(H, A) = \left\{ f \in \mathcal{L}(H, A) \mid \underbrace{f|_{H_{\leq n+1-1}}}_{=f|_{H_{\leq n}}} = 0 \right\} = \left\{ f \in \mathcal{L}(H, A) \mid f|_{H_{\leq n}} = 0 \right\}$$
$$= \left\{ h \in \mathcal{L}(H, A) \mid h|_{H_{\leq n}} = 0 \right\} \qquad \text{(here, we renamed } f \text{ as } h\text{)} \quad (65)$$

for every $n \in \mathbb{N}$.

(a) Let $f \in \mathfrak{g}(H, A)$. Let $n \in \mathbb{N}$.

According to Proposition 14.2 (applied to $n+1$ instead of n), the subset $\mathcal{L}^{n+1}(H, A)$ of $\mathcal{L}(H, A)$ is an ideal of $\mathcal{L}(H, A)$. Thus, there is a factor algebra $\mathcal{L}(H, A) / \mathcal{L}^{n+1}(H, A)$.

(since H is a filtered k-coalgebra). Applied to $m = n-1$, this yields

$$\Delta_H(H_{\leq n-1}) \subseteq \sum_{u=0}^{n-1} (\iota_u \otimes \iota_{n-1-u})(H_{\leq u} \otimes H_{\leq n-1-u}).$$

On the other hand, for every $u \in \{0, 1, \ldots, n-1\}$, we have $h \circ \iota_{n-1-u} = 0$ (because every $x \in H_{\leq n-1-u}$ satisfies

$$(h \circ \iota_{n-1-u})(x) = h\left(\underbrace{\iota_{n-1-u}(x)}_{=x \text{ (since } \iota_{n-1-u} \text{ is just an inclusion map)}}\right) = h\left(\underbrace{x}_{\in H_{\leq n-1-u}}\right) \in h(H_{\leq n-1-u}) \subseteq h(H_{\leq n-1})$$
$$\left(\text{since } (H_{\leq \ell})_{\ell \geq 0} \text{ is a filtration, and thus } H_{\leq n-1-u} \subseteq H_{\leq n-1} \text{ (since } n-1-u \leq n-1)\right)$$
$$= 0$$

and thus $(h \circ \iota_{n-1-u})(x) = 0$) and

$$(g \otimes h) \circ (\iota_u \otimes \iota_{n-1-u}) = (g \circ \iota_u) \otimes (h \circ \iota_{n-1-u})$$
$$\left(\begin{array}{c} \text{because an application of (21) yields} \\ (g \circ \iota_u) \otimes (h \circ \iota_{n-1-u}) = ((g \otimes h) \circ (\iota_u \otimes \iota_{n-1-u})) \end{array} \right)$$
$$= (g \circ \iota_u) \otimes \underbrace{(h \circ \iota_{n-1-u})}_{=0} = (g \circ \iota_u) \otimes 0 = 0. \qquad (64)$$

For every $p \in \mathcal{L}(H, A)$, we are going to denote by $\overline{p}$ the projection of p to this factor algebra (i. e., the residue class of p modulo the ideal $\mathcal{L}^{n+1}(H, A)$). We are going to denote the multiplication in the factor algebra $\mathcal{L}(H, A) / \mathcal{L}^{n+1}(H, A)$ by the $*$ sign, and we are going to write q^{*i} for the i-th power of q (in the factor algebra $\mathcal{L}(H, A) / \mathcal{L}^{n+1}(H, A)$) whenever $q \in \mathcal{L}(H, A) / \mathcal{L}^{n+1}(H, A)$ and $i \in \mathbb{N}$.

Let $g = e^{*f} - e_{H,A}$. Then, $g \in \mathfrak{g}(H, A)$ (since $e^{*f} \in G(H, A) = e_{H,A} + \mathfrak{g}(H, A)$, so that $e^{*f} - e_{H,A} \in \mathfrak{g}(H, A)$). Hence, Remark 3.5 (applied to g instead of f) yields $g^{*i}(H_{\leq n}) = 0$ for every $i > n$. Also, Remark 3.5 yields $f^{*i}(H_{\leq n}) = 0$ for every $i > n$.

We have

$$\begin{aligned} \operatorname{Log}\left(e^{*f}\right) &= \operatorname{Log}_1 \underbrace{\left(e^{*f} - e_{H,A}\right)}_{=g} \qquad \text{(by the definition of Log)} \\ &= \operatorname{Log}_1 g. \end{aligned}$$

By the definition of convolution, $g * h = \mu_H \circ (g \otimes h) \circ \Delta_H$, so that

$$(g * h)(H_{\leq n-1}) = (\mu_H \circ (g \otimes h) \circ \Delta_H)(H_{\leq n-1}) = \mu_H \left((g \otimes h) \underbrace{(\Delta_H(H_{\leq n-1}))}_{\subseteq \sum_{u=0}^{n-1} (\iota_u \otimes \iota_{n-1-u})\left(H_{\leq u} \otimes H_{\leq n-1-u}\right)} \right)$$

$$\subseteq \mu_H \left(\underbrace{(g \otimes h)\left(\sum_{u=0}^{n-1} (\iota_u \otimes \iota_{n-1-u})(H_{\leq u} \otimes H_{\leq n-1-u})\right)}_{\substack{\subseteq \sum_{u=0}^{n-1} (g \otimes h)\left((\iota_u \otimes \iota_{n-1-u})\left(H_{\leq u} \otimes H_{\leq n-1-u}\right)\right) \\ \text{(since } g \otimes h \text{ is } k\text{-linear)}}} \right)$$

$$= \mu_H \left(\sum_{u=0}^{n-1} \underbrace{(g \otimes h)((\iota_u \otimes \iota_{n-1-u})(H_{\leq u} \otimes H_{\leq n-1-u}))}_{=((g \otimes h) \circ (\iota_u \otimes \iota_{n-1-u}))\left(H_{\leq u} \otimes H_{\leq n-1-u}\right)} \right)$$

$$= \mu_H \left(\sum_{u=0}^{n-1} \underbrace{((g \otimes h) \circ (\iota_u \otimes \iota_{n-1-u}))}_{\substack{=0 \\ \text{(by (64))}}} (H_{\leq u} \otimes H_{\leq n-1-u}) \right)$$

$$= \mu_H \left(\sum_{u=0}^{n-1} \underbrace{0\,(H_{\leq u} \otimes H_{\leq n-1-u})}_{=0} \right) = \mu_H \left(\underbrace{\sum_{u=0}^{n-1} 0}_{=0} \right) = \mu_H(0) = 0$$

and therefore $g * h \in \left\{ f \in \mathcal{L}(H, A) \mid f|_{H_{\leq n-1}} = 0 \right\} \subseteq \mathcal{L}^n(H, A)$.

We thus have shown that every $g \in \mathcal{L}(H, A)$ and $h \in \mathcal{L}^n(H, A)$ satisfy $g * h \in \mathcal{L}^n(H, A)$. In other words, $\mathcal{L}^n(H, A)$ is a left ideal of $\mathcal{L}(H, A)$, qed.

Thus, every $x \in H_{\leq n}$ satisfies

$$\begin{aligned}
\left(\operatorname{Log}\left(e^{*f}\right)\right)(x) &= \left(\operatorname{Log}_1 g\right)(x) = \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} g^{*i}(x) \qquad \text{(by the definition of } \operatorname{Log}_1\text{)} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} \underbrace{g^{*i}(x)}_{\substack{=0 \text{ (since } x\in H_{\leq n} \text{ and thus} \\ g^{*i}(x)\in g^{*i}\left(H_{\leq n}\right)=0 \\ \text{(since } i>n\text{))}}} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \underbrace{\sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} 0}_{=0} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x).
\end{aligned}$$

In other words,

$$\operatorname{Log}\left(e^{*f}\right)|_{H_{\leq n}} = \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)|_{H_{\leq n}},$$

so that

$$\begin{aligned}
\left(\operatorname{Log}\left(e^{*f}\right) - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)|_{H_{\leq n}} &= \underbrace{\operatorname{Log}\left(e^{*f}\right)|_{H_{\leq n}}}_{=\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)|_{H_{\leq n}}} - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}|_{H_{\leq n}} \\
&= \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)|_{H_{\leq n}} - \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)|_{H_{\leq n}} = 0
\end{aligned}$$

and thus

$$\operatorname{Log}\left(e^{*f}\right) - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \in \left\{h \in \mathcal{L}(H,A) \mid h|_{H_{\leq n}} = 0\right\} = \mathcal{L}^{n+1}(H,A)$$

(by (65)). In other words,

$$\operatorname{Log}\left(e^{*f}\right) \equiv \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \bmod \mathcal{L}^{n+1}(H,A). \tag{66}$$

But every $x \in H_{\leq n}$ satisfies

$$e^{*f}(x) = \sum_{i \geq 0} \frac{f^{*i}(x)}{i!} = \sum_{i=0}^{n} \frac{f^{*i}(x)}{i!} + \sum_{i=n+1}^{\infty} \underbrace{\frac{f^{*i}(x)}{i!}}_{\substack{=0 \text{ (since } x \in H_{\leq n} \text{ and thus} \\ f^{*i}(x) \in f^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{), so that} \\ f^{*i}(x) = 0)}} = \sum_{i=0}^{n} \frac{f^{*i}(x)}{i!} + \underbrace{\sum_{i=n+1}^{\infty} 0}_{=0} = \sum_{i=0}^{n} \frac{f^{*i}(x)}{i!}$$

$$= \underbrace{\frac{f^{*0}(x)}{0!}}_{= \frac{e_{H,A}(x)}{1} = e_{H,A}(x)} + \sum_{i=1}^{n} \frac{f^{*i}(x)}{i!} = e_{H,A}(x) + \sum_{i=1}^{n} \frac{f^{*i}(x)}{i!}$$

and thus

$$\underbrace{g}_{= e^{*f} - e_{H,A}}(x) = \left(e^{*f} - e_{H,A}\right)(x) = \underbrace{e^{*f}(x)}_{= e_{H,A}(x) + \sum\limits_{i=1}^{n} \frac{f^{*i}(x)}{i!}} - e_{H,A}(x) = \sum_{i=1}^{n} \frac{f^{*i}(x)}{i!} = \sum_{i=1}^{n} \frac{f^{*i}}{i!}(x)$$

$$= \sum_{j=1}^{n} \frac{f^{*j}}{j!}(x) \qquad \text{(here, we substituted } j \text{ for } i \text{ in the sum)}.$$

In other words,

$$g\,|_{H_{\leq n}} = \left(\sum_{j=1}^{n} \frac{f^{*j}}{j!}\right)|_{H_{\leq n}}.$$

Hence,

$$\left(g - \sum_{j=1}^{n} \frac{f^{*j}}{j!}\right)|_{H_{\leq n}} = \underbrace{g\,|_{H_{\leq n}}}_{= \left(\sum\limits_{j=1}^{n} \frac{f^{*j}}{j!}\right)|_{H_{\leq n}}} - \left(\sum_{j=1}^{n} \frac{f^{*j}}{j!}\right)|_{H_{\leq n}}$$

$$= \left(\sum_{j=1}^{n} \frac{f^{*j}}{j!}\right)|_{H_{\leq n}} - \left(\sum_{j=1}^{n} \frac{f^{*j}}{j!}\right)|_{H_{\leq n}} = 0.$$

This yields

$$g - \sum_{j=1}^{n} \frac{f^{*j}}{j!} \in \left\{h \in \mathcal{L}(H, A) \mid h\,|_{H_{\leq n}} = 0\right\} = \mathcal{L}^{n+1}(H, A)$$

(by (65)). In other words,

$$g \equiv \sum_{j=1}^{n} \frac{f^{*j}}{j!} \bmod \mathcal{L}^{n+1}(H, A).$$

Thus, (66) becomes

$$\operatorname{Log}\left(e^{*f}\right) \equiv \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\underbrace{}_{\equiv \sum_{j=1}^{n} \frac{f^{*j}}{j!} \bmod \mathcal{L}^{n+1}(H,A)} \right)^{*i}$$
$$\equiv \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{f^{*j}}{j!} \right)^{*i} \bmod \mathcal{L}^{n+1}(H,A). \tag{67}$$

But since $f^{*(n+1)} |_{H_{\leq n}} = 0$ (since Remark 3.5 (applied to $i = n+1$) yields $f^{*(n+1)}(H_{\leq n}) = 0$), we have $f^{*(n+1)} \in \left\{ h \in \mathcal{L}(H,A) \mid h |_{H_{\leq n}} = 0 \right\} = \mathcal{L}^{n+1}(H,A)$ (by (65)). In other words, $f^{*(n+1)} \equiv 0 \bmod \mathcal{L}^{n+1}(H,A)$. In other words, $\overline{f^{*(n+1)}} = 0$. Thus, $\overline{f}^{*(n+1)} = \overline{f^{*(n+1)}} = 0$. Hence, we can apply Corollary 5.14 **(a)** to $a = \overline{f}$ and obtain $\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{\overline{f}^{*j}}{j!} \right)^{*i} = \overline{f}$. Hence,

$$\overline{\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{f^{*j}}{j!} \right)^{*i}} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{\overline{f}^{*j}}{j!} \right)^{*i} = \overline{f}.$$

In other words,

$$\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \left(\sum_{j=1}^{n} \frac{f^{*j}}{j!} \right)^{*i} \equiv f \bmod \mathcal{L}^{n+1}(H,A).$$

Combined with (67), this yields $\operatorname{Log}\left(e^{*f}\right) \equiv f \bmod \mathcal{L}^{n+1}(H,A)$. In other words,

$$\operatorname{Log}\left(e^{*f}\right) - f \in \mathcal{L}^{n+1}(H,A) = \left\{ h \in \mathcal{L}(H,A) \mid h |_{H_{\leq n}} = 0 \right\}$$

(by (65)). In other words, $\left(\operatorname{Log}\left(e^{*f}\right) - f\right) |_{H_{\leq n}} = 0$. Hence,

$$0 = \left(\operatorname{Log}\left(e^{*f}\right) - f\right) |_{H_{\leq n}} = \left(\operatorname{Log}\left(e^{*f}\right)\right) |_{H_{\leq n}} - f |_{H_{\leq n}}.$$

Hence,

$$\left(\operatorname{Log}\left(e^{*f}\right)\right) |_{H_{\leq n}} = f |_{H_{\leq n}}. \tag{68}$$

We have thus proven this for every $n \in \mathbb{N}$.

Now, let $x \in H$ be arbitrary. Since H is filtered, there must exist some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$. Consider this n. From $x \in H_{\leq n}$, we obtain

$$\left(\operatorname{Log}\left(e^{*f}\right)\right)(x) = \underbrace{\left(\operatorname{Log}\left(e^{*f}\right) |_{H_{\leq n}}\right)}_{\substack{= f|_{H_{\leq n}} \\ \text{(by (68))}}} (x) = \left(f |_{H_{\leq n}}\right)(x) = f(x).$$

Since this holds for every $x \in H$, we can now conclude that $\operatorname{Log}\left(e^{*f}\right) = f$.

This proves Proposition 14.3 **(a)**.

(b) Let $F \in G(H,A)$. Let $n \in \mathbb{N}$.

According to Proposition 14.2 (applied to $n+1$ instead of n), the subset $\mathcal{L}^{n+1}(H,A)$ of $\mathcal{L}(H,A)$ is an ideal of $\mathcal{L}(H,A)$. Thus, there is a factor algebra $\mathcal{L}(H,A)/\mathcal{L}^{n+1}(H,A)$. For every $p \in \mathcal{L}(H,A)$, we are going to denote by $\overline{p}$ the projection of p to this factor algebra (i. e., the residue class of p modulo the ideal $\mathcal{L}^{n+1}(H,A)$). We are going to denote the multiplication in the factor algebra $\mathcal{L}(H,A)/\mathcal{L}^{n+1}(H,A)$ by the $*$ sign, and we are going to write q^{*i} for the i-th power of q (in the factor algebra $\mathcal{L}(H,A)/\mathcal{L}^{n+1}(H,A)$) whenever $q \in \mathcal{L}(H,A)/\mathcal{L}^{n+1}(H,A)$ and $i \in \mathbb{N}$.

Let $g = F - e_{H,A}$. Then, $g \in \mathfrak{g}(H,A)$ (since $F \in G(H,A) = e_{H,A} + \mathfrak{g}(H,A)$, so that $F - e_{H,A} \in \mathfrak{g}(H,A)$). Hence, Remark 3.5 (applied to g instead of f) yields $g^{*i}(H_{\leq n}) = 0$ for every $i > n$.

Let $\varphi = \operatorname{Log} F$. Then, $\varphi \in \mathfrak{g}(H,A)$, so that Remark 3.5 (applied to φ instead of f) yields $\varphi^{*i}(H_{\leq n}) = 0$ for every $i > n$.

By the definition of Log, we have $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{H,A})}_{=g} = \operatorname{Log}_1 g$. Hence, $\varphi = \operatorname{Log} f = \operatorname{Log}_1 g$.

Thus, every $x \in H_{\leq n}$ satisfies

$$\begin{aligned}
\varphi(x) &= (\operatorname{Log}_1 g)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} g^{*i}(x) \qquad \text{(by the definition of } \operatorname{Log}_1\text{)} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} \underbrace{g^{*i}(x)}_{\substack{=0 \text{ (since} \\ x \in H_{\leq n} \text{ and thus} \\ g^{*i}(x) \in g^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{))}}} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \underbrace{\sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} 0}_{=0} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x).
\end{aligned}$$

In other words,

$$\varphi\,|_{H_{\leq n}} = \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}}.$$

Now,

$$\begin{aligned}
\left(\varphi - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} &= \underbrace{\varphi\,|_{H_{\leq n}}}_{= \left(\sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}}} - \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} \\
&= \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} - \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} = 0.
\end{aligned}$$

In other words,

$$\varphi - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \in \left\{ h \in \mathcal{L}(H,A) \mid h\,|_{H_{\leq n}} = 0 \right\} = \mathcal{L}^{n+1}(H,A)$$

(by (65)). This rewrites as

$$\varphi \equiv \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \bmod \mathcal{L}^{n+1}(H,A). \tag{69}$$

But every $x \in H_{\leq n}$ satisfies

$$e^{*\varphi}(x) = \sum_{i\geq 0} \frac{\varphi^{*i}(x)}{i!} = \sum_{i=0}^{n} \frac{\varphi^{*i}(x)}{i!} + \sum_{i=n+1}^{\infty} \underbrace{\frac{\varphi^{*i}(x)}{i!}}_{\substack{=0 \text{ (since } x\in H_{\leq n} \text{ and thus} \\ \varphi^{*i}(x)\in\varphi^{*i}\left(H_{\leq n}\right)=0 \\ \text{(since } i>n\text{), so that} \\ \varphi^{*i}(x)=0)}} = \sum_{i=0}^{n} \frac{\varphi^{*i}(x)}{i!} + \underbrace{\sum_{i=n+1}^{\infty} 0}_{=0} = \sum_{i=0}^{n} \frac{\varphi^{*i}(x)}{i!}$$

$$= \underbrace{\frac{\varphi^{*0}(x)}{0!}}_{\substack{=\frac{e_{H,A}(x)}{1} \\ =e_{H,A}(x)}} + \sum_{i=1}^{n} \frac{\varphi^{*i}(x)}{i!} = e_{H,A}(x) + \sum_{i=1}^{n} \frac{\varphi^{*i}(x)}{i!}$$

and thus

$$\left(e^{*\varphi} - e_{H,A}\right)(x) = \underbrace{e^{*\varphi}(x)}_{=e_{H,A}(x)+\sum\limits_{i=1}^{n} \frac{\varphi^{*i}(x)}{i!}} - e_{H,A}(x) = \sum_{i=1}^{n} \frac{\varphi^{*i}(x)}{i!} = \sum_{i=1}^{n} \frac{\varphi^{*i}}{i!}(x)$$

$$= \sum_{j=1}^{n} \frac{\varphi^{*j}}{j!}(x) \qquad \text{(here, we substituted } j \text{ for } i \text{ in the sum)}.$$

In other words,

$$\left(e^{*\varphi} - e_{H,A}\right)|_{H_{\leq n}} = \left(\sum_{j=1}^{n} \frac{\varphi^{*j}}{j!}\right)|_{H_{\leq n}}.$$

But now,

$$\left(\left(e^{*\varphi} - e_{H,A}\right) - \sum_{j=1}^{n} \frac{\varphi^{*j}}{j!}\right)|_{H_{\leq n}}$$

$$= \underbrace{\left(e^{*\varphi} - e_{H,A}\right)|_{H_{\leq n}}}_{=\left(\sum\limits_{j=1}^{n} \frac{\varphi^{*j}}{j!}\right)|_{H_{\leq n}}} - \left(\sum_{j=1}^{n} \frac{\varphi^{*j}}{j!}\right)|_{H_{\leq n}}$$

$$= \left(\sum_{j=1}^{n} \frac{\varphi^{*j}}{j!}\right)|_{H_{\leq n}} - \left(\sum_{j=1}^{n} \frac{\varphi^{*j}}{j!}\right)|_{H_{\leq n}} = 0.$$

In other words,

$$\left(e^{*\varphi} - e_{H,A}\right) - \sum_{j=1}^{n} \frac{\varphi^{*j}}{j!} \in \left\{h \in \mathcal{L}(H,A) \mid h|_{H_{\leq n}} = 0\right\} = \mathcal{L}^{n+1}(H,A)$$

(by (65)). This rewrites as

$$e^{*\varphi} - e_{H,A} \equiv \sum_{j=1}^{n} \frac{\varphi^{*j}}{j!} \bmod \mathcal{L}^{n+1}(H,A).$$

Substituting (69) into the right hand side of this congruence, we get

$$e^{*\varphi} - e_{H,A} \equiv \sum_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)^{*j}}{j!} \bmod \mathcal{L}^{n+1}(H,A). \tag{70}$$

But since $g^{*(n+1)} \mid_{H_{\leq n}} = 0$ (since Remark 3.5 (applied to $n+1$ and g instead of i and f) yields $g^{*(n+1)}(H_{\leq n}) = 0$), we have $g^{*(n+1)} \in \left\{h \in \mathcal{L}(H,A) \mid h \mid_{H_{\leq n}} = 0\right\} = \mathcal{L}^{n+1}(H,A)$ (by (65)). In other words, $g^{*(n+1)} \equiv 0 \bmod \mathcal{L}^{n+1}(H,A)$, so that $\overline{g^{*(n+1)}} = 0$. Thus, $\overline{g}^{*(n+1)} = \overline{g^{*(n+1)}} = 0$. Hence, we can apply Corollary 5.14 **(b)** to $b = \overline{g}$ and obtain $\sum\limits_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} \overline{g}^{*i}\right)^{*j}}{j!} = \overline{g}$. Thus,

$$\overline{\sum_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)^{*j}}{j!}} = \sum_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} \overline{g}^{*i}\right)^{*j}}{j!} = \overline{g}.$$

In other words,

$$\sum_{j=1}^{n} \frac{\left(\sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)^{*j}}{j!} \equiv g \bmod \mathcal{L}^{n+1}(H,A).$$

Combined with (70), this yields $e^{*\varphi} - e_{H,A} \equiv g \bmod \mathcal{L}^{n+1}(H,A)$. Since $g = F - e_{H,A}$, this rewrites as $e^{*\varphi} - e_{H,A} \equiv F - e_{H,A} \bmod \mathcal{L}^{n+1}(H,A)$. This simplifies to $e^{*\varphi} \equiv F \bmod \mathcal{L}^{n+1}(H,A)$. In other words,

$$e^{*\varphi} - F \in \mathcal{L}^{n+1}(H,A) = \left\{h \in \mathcal{L}(H,A) \mid h \mid_{H_{\leq n}} = 0\right\}$$

(by (65)). In other words, $(e^{*\varphi} - F) \mid_{H_{\leq n}} = 0$. Thus,

$$0 = (e^{*\varphi} - F) \mid_{H_{\leq n}} = e^{*\varphi} \mid_{H_{\leq n}} - F \mid_{H_{\leq n}},$$

so that $e^{*\varphi} \mid_{H_{\leq n}} = F \mid_{H_{\leq n}}$. Since $\varphi = \operatorname{Log} F$, this becomes

$$e^{*(\operatorname{Log} F)} \mid_{H_{\leq n}} = F \mid_{H_{\leq n}}. \tag{71}$$

We have thus proven this for every $n \in \mathbb{N}$.

Now, let $x \in H$ be arbitrary. Since H is filtered, there must exist some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$. Consider this n. From $x \in H_{\leq n}$, we obtain

$$e^{*(\operatorname{Log} F)}(x) = \underbrace{\left(e^{*(\operatorname{Log} F)} \mid_{H_{\leq n}}\right)}_{\substack{=F|_{H_{\leq n}} \\ \text{(by (71))}}}(x) = \left(F \mid_{H_{\leq n}}\right)(x) = F(x).$$

Since this holds for every $x \in H$, we can now conclude that $e^{*(\operatorname{Log} F)} = F$.

This proves Proposition 14.3 **(b)**.

We are thus done proving Proposition 14.3. □

§15. The dual theorem

Before we proceed, let us introduce two pieces of notation:

Convention 15.1. Let k be a field. Let V be a k-vector space. Let S be a subset of V. Then, $\langle S \rangle$ will denote the k-vector subspace of V generated by the subset S. Note that $\langle S \rangle$ is the set of all k-linear combinations of elements of S. We have $S \subseteq \langle S \rangle$.

Convention 15.2. Let k be a field. Let A be a k-algebra.

If U and V are two k-vector subspaces of A, then we let UV denote the k-vector subspace

$$\langle uv \mid (u, v) \in U \times V \rangle$$

of A. This subspace is called the *product* of the subspaces U and V of A; we will also denote it by $U \cdot V$. (Note that it depends on the base field k.)

This definition makes the set of all k-vector subspaces of A into a multiplicative monoid, with neutral element $k \cdot 1_A$ (the subspace of all scalar multiples of the unity 1_A). Any k-vector subspace V of A satisfies $(k \cdot 1_A) \cdot V = V \cdot (k \cdot 1_A) = V$. Any three k-vector subspaces U, V and W of A satisfy $(UV) W = U (VW)$. We will use the standard notations that are used in multiplicative monoids (such as writing UVW for the product $(UV) W = U (VW)$). In particular, if V is a k-vector subspace of A and n is a nonnegative integer, then V^n will denote the n-th power of V in the multiplicative monoid of all k-vector subspaces of A (that is, the subspace $\underbrace{VV \cdots V}_{n \text{ times}}$ of A).

Three remarks about this are in order. Firstly, the notation V^n cannot be misunderstood for the Cartesian product $\underbrace{V \times V \times \cdots \times V}_{n \text{ times}}$, because we are denoting the latter Cartesian product by $V^{\times n}$ and not by V^n (see Convention 1.5).

Secondly, it is obvious that standard power rules that hold in monoids hold in the multiplicative monoid of all k-vector subspaces of A. For instance, $V^n V^m = V^{n+m}$ for any k-vector subspace V of A and every $n \in \mathbb{N}$ and $m \in \mathbb{N}$.

Furthermore, if n is a nonnegative integer, and V_1, V_2, ..., V_n are n arbitrary k-vector subspaces of a k-algebra A, then

$$V_1 V_2 \cdots V_n = \langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in V_1 \times V_2 \times \cdots \times V_n \rangle . \quad (72)$$

In particular, if n is a nonnegative integer, and V is a k-vector subspace of a k-algebra A, then

$$V^n = \left\langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle . \quad (73)$$

Thirdly, some authors define the notion of an n-th power of an ideal of a ring. When the ring is A, their definition of the n-th power of an ideal I of A differs from our definition of I^n in that they define it as an A-linear span whereas we define it as a k-linear span. This difference is insubstantial if $n > 0$ (that is, the reader can easily check that the two definitions are equivalent if $n > 0$). But if $n = 0$, then their definition gives a different result than ours. Namely, their definition leads to $I^0 = A$ while ours leads to $I^0 = k \cdot 1_A$. While their definition is more suitable for studying ideals (in particular, it ensures that $I^0 \supseteq I^1 \supseteq I^2 \supseteq \cdots$ for any ideal I, whereas our definition only ensures that ideals I satisfy $I^1 \supseteq I^2 \supseteq I^3 \supseteq \cdots$ but usually not $I^0 \supseteq I^1$), our definition is more useful for arbitrary k-vector subspaces.

Now we are going to state and prove a result which is, in some sense, dual to Theorem 4.1:

Theorem 15.3. Let k be a field of characteristic 0, and let H be a connected filtered commutative bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. The map $\operatorname{Log} \mathrm{id} \in \mathcal{L}(H, H)$ is a projection such that $\operatorname{Ker}(\operatorname{Log} \mathrm{id}) = (\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H$. [47]

Theorem 15.3 is not directly obtainable from Theorem 4.1 by dualization: First of all, the dual of a bialgebra is not necessarily a bialgebra (the dual of a coalgebra is always an algebra, but the dual of an algebra needs not be a coalgebra unless the algebra is finite-dimensional), but even this technical hurdle aside, the dual of a coalgebra filtration is not a filtration but something reasonably called a "cofiltration" (a decreasing filtration with intersection 0). Given these difficulties, one might be surprised that Theorem 15.3 is correct at all. Fortunately, the filtration is not really an important part of Theorems 4.1 and 15.3 - its main purpose is to make $\operatorname{Log} \mathrm{id}$ (and, more generally, $\operatorname{Log} f$ for $f \in \mathfrak{g}(H, H)$) well-defined. The main core of Theorem 15.3 *is* dual to that of Theorem 4.1. We will make this clear by giving a proof of Theorem 15.3 which mirrors the above proof of Theorem 4.1 - at least it will have the same large-scale structure, using lemmas which are duals of respective lemmas used to prove Theorem 4.1 (though some of the lemmas will not have to be modified at all). As far as the details of the proof are concerned (the proofs of these lemmas), they will be simpler than those in the proof of Theorem 4.1, since we will be able to replace many complicated computations with maps by simpler computations with elements.

First let us formulate a proposition, which is in some sense a dual of Proposition 6.2:

[47] Recall that $(\operatorname{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Thus, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

Proposition 15.4. Let k be a field of characteristic 0. Let A be a k-algebra, and let H be a connected filtered k-coalgebra. Let $\varepsilon_A : A \to k$ be a k-algebra homomorphism. Then:

(a) Any $f \in \mathcal{L}(H, A)$ and any $g \in \mathcal{L}(H, A)$ such that $\varepsilon_A \circ f = 0$ and $\varepsilon_A \circ g = 0$ satisfy $\varepsilon_A \circ (f * g) = 0$ and $(f * g)(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$. [48]

(b) Every $f \in \mathcal{L}(H, A)$ such that $\varepsilon_A \circ f = 0$ and every integer $i > 1$ satisfy $\varepsilon_A \circ f^{*i} = 0$ and $f^{*i}(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$.

(c) Every $F \in G(H, A)$ satisfying $\varepsilon_A \circ F = \varepsilon_H$ satisfies $(\operatorname{Log} F - F)(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2 + k \cdot 1_A$.

Note that the duality between Proposition 6.2 and Proposition 15.4 is not perfect. The condition $\varepsilon_A \circ F = \varepsilon_H$ of Proposition 15.4 **(c)** is dual to the condition $F(1_H) = 1_A$ (which is implicit in the condition $F \in G(H, A)$) of Proposition 6.2 **(c)**, but the condition $F \in G(H, A)$ of Proposition 15.4 **(c)** is not dual to anything required in Proposition 6.2 **(c)** - it just is there to make sure that $\operatorname{Log} F$ is well-defined.

Before we start proving Proposition 15.4, let us show a simple lemma:

Lemma 15.5. Let k be a field. Let A be a k-algebra. Then,

$$\text{any two } k\text{-vector subspaces } U \text{ and } V \text{ of } A \text{ satisfy } \mu_A(U \otimes V) = UV \quad (74)$$

(where we consider $U \otimes V$ as a k-vector subspace of $A \otimes A$ by tensoring the inclusion maps $U \to A$ and $V \to A$).

Proof of Lemma 15.5. Let U and V be two k-vector subspaces of A. Let tensor : $U \times V \to U \otimes V$ be the map defined by

$$(\operatorname{tensor}(u, v) = u \otimes v \text{ for every } (u, v) \in U \times V).$$

Recall that for every k-vector space M and every subset S of M, we denote by $\langle S \rangle$ the k-vector subspace of M generated by the elements of S.

For every k-vector space M, every set Φ and every map $P : \Phi \to M$, let us denote by $\langle P(v) \mid v \in \Phi \rangle$ the subspace $\langle \{P(v) \mid v \in \Phi\} \rangle$ of M (this is the k-vector subspace of M generated by all the elements $P(v)$ with $v \in \Phi$).

It is a known fact that any two k-vector spaces M and R, any k-linear map $\phi : M \to R$ and every subset S of M satisfy $\phi(\langle S \rangle) = \langle \phi(S) \rangle$. Applied to $M = A \otimes A$, $R = A$, $\phi = \mu_A$ and $S = \{\operatorname{tensor}(u, v) \mid (u, v) \in U \times V\}$, this yields

$$\mu_A(\langle \{\operatorname{tensor}(u, v) \mid (u, v) \in U \times V\} \rangle) = \langle \mu_A(\{\operatorname{tensor}(u, v) \mid (u, v) \in U \times V\}) \rangle.$$

Since $\operatorname{tensor}(u, v) = u \otimes v$, this rewrites as

$$\mu_A(\langle \{u \otimes v \mid (u, v) \in U \times V\} \rangle) = \langle \mu_A(\{u \otimes v \mid (u, v) \in U \times V\}) \rangle.$$

Now, since the tensor product $U \otimes V$ is generated by pure tensors, we have

$$U \otimes V = \langle u \otimes v \mid (u, v) \in U \times V \rangle = \langle \{u \otimes v \mid (u, v) \in U \times V\} \rangle,$$

[48] Recall that $(\operatorname{Ker}(\varepsilon_A))^2$ is defined according to Convention 15.2. Hence, $(\operatorname{Ker}(\varepsilon_A))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_A)) \cdot (\operatorname{Ker}(\varepsilon_A))$ of A.

so that

$$\mu_A(U \otimes V) = \mu_A(\langle \{u \otimes v \mid (u,v) \in U \times V\} \rangle) = \left\langle \underbrace{\mu_A(\{u \otimes v \mid (u,v) \in U \times V\})}_{=\{\mu_A(u \otimes v) \mid (u,v) \in U \times V\}} \right\rangle$$

$$= \left\langle \left\{ \underbrace{\mu_A(u \otimes v)}_{\substack{=uv \\ \text{(since } \mu_A \text{ is the multiplication map)}}} \mid (u,v) \in U \times V \right\} \right\rangle$$

$$= \langle \{uv \mid (u,v) \in U \times V\} \rangle = \langle uv \mid (u,v) \in U \times V \rangle = UV.$$

This proves Lemma 15.5. □

Proof of Proposition 15.4. **(a)** We have $\varepsilon_A(f(H)) = \underbrace{(\varepsilon_A \circ f)}_{=0}(H) = 0(H) = 0$ and thus $f(H) \subseteq \operatorname{Ker}(\varepsilon_A)$. Similarly, $g(H) \subseteq \operatorname{Ker}(\varepsilon_A)$.

By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_H$. Thus,

$$(f * g)(H) = (\mu_A \circ (f \otimes g) \circ \Delta_H)(H) = \mu_A\left((f \otimes g)\underbrace{(\Delta_H(H))}_{\subseteq H \otimes H}\right) \subseteq \mu_A\left(\underbrace{(f \otimes g)(H \otimes H)}_{=f(H) \otimes g(H)}\right)$$

$$= \mu_A\left(\underbrace{f(H)}_{\subseteq \operatorname{Ker}(\varepsilon_A)} \otimes \underbrace{g(H)}_{\subseteq \operatorname{Ker}(\varepsilon_A)}\right) \subseteq \mu_A((\operatorname{Ker}(\varepsilon_A)) \otimes (\operatorname{Ker}(\varepsilon_A))).$$

But (74) (applied to $U = \operatorname{Ker}(\varepsilon_A)$ and $V = \operatorname{Ker}(\varepsilon_A)$) yields $\mu_A((\operatorname{Ker}(\varepsilon_A)) \otimes (\operatorname{Ker}(\varepsilon_A))) = (\operatorname{Ker}(\varepsilon_A))(\operatorname{Ker}(\varepsilon_A)) = (\operatorname{Ker}(\varepsilon_A))^2$. Thus, $(f * g)(H) \subseteq \mu_A((\operatorname{Ker}(\varepsilon_A)) \otimes (\operatorname{Ker}(\varepsilon_A)))$ rewrites as $(f * g)(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$. Hence,

$$\varepsilon_A((f * g)(H)) \subseteq \varepsilon_A\left((\operatorname{Ker}(\varepsilon_A))^2\right) \subseteq \left(\underbrace{\varepsilon_A(\operatorname{Ker}(\varepsilon_A))}_{=0}\right)^2$$

(since ε_A is a k-algebra homomorphism)

$$= 0^2 = 0,$$

so that $(\varepsilon_A \circ (f * g))(H) = \varepsilon_A((f * g)(H)) = 0$. In other words, $\varepsilon_A \circ (f * g) = 0$. This completes the proof of Proposition 15.4 **(a)**.

(b) We will prove Proposition 15.4 **(b)** by induction over i:

Induction base: Proposition 15.4 **(a)** (applied to $g = f$) yields $\varepsilon_A \circ (f * f) = 0$ and $(f * f)(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$. Since $f * f = f^{*2}$, this rewrites as follows: We have $\varepsilon_A \circ f^{*2} = 0$ and $f^{*2}(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$. This proves Proposition 15.4 **(b)** for $i = 2$. The induction base is thus complete.

Induction step: Let $j > 1$ be an integer. Assume that Proposition 15.4 **(b)** holds for $i = j$. We must then prove Proposition 15.4 **(b)** for $i = j + 1$.

Since Proposition 15.4 **(b)** holds for $i = j$, we have $\varepsilon_A \circ f^{*j} = 0$ and $f^{*j}(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$. Now, Proposition 15.4 **(a)** (applied to $g = f^{*j}$) yields $\varepsilon_A \circ (f * f^{*j}) = 0$ and $(f * f^{*j})(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$. Since $f * f^{*j} = f^{*(j+1)}$, this rewrites as follows: We

have $\varepsilon_A \circ f^{*(j+1)} = 0$ and $f^{*(j+1)}(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$. In other words, Proposition 15.4 **(b)** holds for $i = j+1$. The induction step is thus complete.

This completes the induction proof of Proposition 15.4 **(b)**.

(c) Let $F \in G(H, A)$ satisfy $\varepsilon_A \circ F = \varepsilon_H$.

Since ε_A is a k-algebra homomorphism, we have $\varepsilon_A \circ \eta_A = \eta_k = \mathrm{id}_k$.

Let $f = F - e_{H,A}$. Then,

$$\varepsilon_A \circ f = \varepsilon_A \circ (F - e_{H,A}) = \underbrace{\varepsilon_A \circ F}_{=\varepsilon_H} - \varepsilon_A \circ \underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_H} = \varepsilon_H - \underbrace{\varepsilon_A \circ \eta_A}_{=\mathrm{id}_k} \circ \varepsilon_H$$
$$= \varepsilon_H - \varepsilon_H = 0$$

and $f \in \mathfrak{g}(H, A)$ (since $F \in G(H, A) = e_{H,A} + \mathfrak{g}(H, A)$, so that $F - e_{H,A} \in \mathfrak{g}(H, A)$).

Now, the definition of Log says that $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{H,A})}_{=f} = \operatorname{Log}_1 f$.

Let $x \in H$. Then,

$$\underbrace{(\operatorname{Log} F)}_{=\operatorname{Log}_1 f}(x) = (\operatorname{Log}_1 f)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) = \underbrace{\frac{(-1)^{1-1}}{1}}_{=1} f^{*1}(x) + \sum_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$$
$$= \underbrace{1 f^{*1}(x)}_{=f^{*1}(x)=f(x)} + \sum_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x) = f(x) + \sum_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x).$$

On the other hand, $f = F - e_{H,A}$ yields

$$f(x) = (F - e_{H,A})(x) = F(x) - \underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_E}(x) = F(x) - (\eta_A \circ \varepsilon_H)(x)$$
$$= F(x) - \underbrace{\eta_A(\varepsilon_H(x))}_{\substack{=\varepsilon_H(x) \cdot 1_A \\ \text{(by the definition of } \eta_A\text{)}}} = F(x) - \varepsilon_H(x) \cdot 1_A,$$

so that $F(x) = f(x) + \varepsilon_H(x) \cdot 1_A$. Thus,

$$(\operatorname{Log} F - F)(x) = \underbrace{(\operatorname{Log} F)(x)}_{\substack{= f(x) + \sum\limits_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x)}} - \underbrace{F(x)}_{=f(x)+\varepsilon_H(x)\cdot 1_A}$$
$$= \left(f(x) + \sum_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x) \right) - (f(x) + \varepsilon_H(x) \cdot 1_A)$$
$$= \sum_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x) + \varepsilon_H(x) \cdot 1_A. \tag{75}$$

But every integer $i > 1$ satisfies $f^{*i}(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2$ (by Proposition 15.4 **(b)**) and thus $f^{*i}(x) \in (\operatorname{Ker}(\varepsilon_A))^2$ (since $x \in H$ and thus $f^{*i}(x) \in f^{*i}(H)$). Hence, $\sum\limits_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ is a finite k-linear combination of elements of $(\operatorname{Ker}(\varepsilon_A))^2$ (it is finite because we know that only finitely many addends of the infinite sum $\sum\limits_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$

are nonzero). Therefore, $\sum_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ is an element of $(\operatorname{Ker}(\varepsilon_A))^2$ (because $(\operatorname{Ker}(\varepsilon_A))^2$ is a k-vector space, so that every finite k-linear combination of elements of $(\operatorname{Ker}(\varepsilon_A))^2$ must be an element of $(\operatorname{Ker}(\varepsilon_A))^2$ itself). Thus, (75) becomes

$$(\operatorname{Log} F - F)(x) = \underbrace{\sum_{i>1} \frac{(-1)^{i-1}}{i} f^{*i}(x)}_{\in (\operatorname{Ker}(\varepsilon_A))^2} + \underbrace{\varepsilon_H(x) \cdot 1_A}_{\in k \cdot 1_A} \in (\operatorname{Ker}(\varepsilon_A))^2 + k \cdot 1_A.$$

Since this holds for every $x \in H$, we thus have proven that $(\operatorname{Log} F - F)(H) \subseteq (\operatorname{Ker}(\varepsilon_A))^2 + k \cdot 1_A$. This proves Proposition 15.4 **(c)**. □

Next, just as we defined the notion of $(\varepsilon, \varepsilon)$-coderivations in Definition 7.1, let us define $(\varepsilon, \varepsilon)$-derivations (which is, in fact, a well-known notion, after which the notion of $(\varepsilon, \varepsilon)$-coderivations was modelled after):

Definition 15.6. Let k be a field. Let H be a k-algebra, and let $\varepsilon_H : H \to k$ be a k-algebra homomorphism. Let A be a k-algebra. Let $f : H \to A$ be a k-linear map. Then, f is said to be an $(\varepsilon_H, \varepsilon_H)$-*derivation* if and only if $f \circ \mu_H = \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f)$. Here, the map $e_{H,A}$ is defined to be the map $\eta_A \circ \varepsilon_H : H \to A$ (this definition of the map $e_{H,A}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

This definition can be very easily equivalently rewritten as follows:

Definition 15.7. Let k be a field. Let H be a k-algebra, and let $\varepsilon_H : H \to k$ be a k-algebra homomorphism. Let A be a k-algebra. Let $f : H \to A$ be a k-linear map. Then, f is said to be an $(\varepsilon_H, \varepsilon_H)$-*derivation* if and only if every $(a, b) \in H \times H$ satisfies $f(ab) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\,f(b)$.

We will be able to use both Definitions 15.6 and 15.7 in parallel as soon as we have shown the following proposition:

Proposition 15.8. Definition 15.6 and Definition 15.7 are equivalent.

Proof of Proposition 15.8. Let k be a field. Let H be a k-algebra, and let $\varepsilon_H : H \to k$ be a k-algebra homomorphism. Let A be a k-algebra. Let $f : H \to A$ be a k-linear map.

It is well-known that two k-linear maps from a tensor product are equal if and only if they are equal on each pure tensor. Applying this fact to the two k-linear maps $f \circ \mu_H : H \otimes H \to A$ and $\mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f) : H \otimes H \to A$, we conclude that we have the following equivalence:

$$\begin{aligned} &(\text{the two maps } f \circ \mu_H \text{ and } \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f) \text{ are equal}) \\ &\iff (\text{the two maps } f \circ \mu_H \text{ and } \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f) \text{ are equal on each pure tensor}). \end{aligned} \tag{76}$$

Since pure tensors in $H \otimes H$ are tensors of the form $a \otimes b$ with $(a, b) \in H \times H$, we have the equivalence

$$\begin{aligned}
&\left(\text{the two maps } f \circ \mu_H \text{ and } \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f) \text{ are equal on each pure tensor}\right) \\
&\iff \left(\text{the two maps } f \circ \mu_H \text{ and } \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f) \text{ are}\right. \\
&\qquad\qquad \left.\text{equal on } a \otimes b \text{ for each } (a, b) \in H \times H\right) \\
&\iff \left((f \circ \mu_H)(a \otimes b) = (\mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f))(a \otimes b) \text{ for each } (a, b) \in H \times H\right).
\end{aligned} \tag{77}$$

But every $(a, b) \in H \times H$ satisfies

$$(f \circ \mu_H)(a \otimes b) = f\left(\underbrace{\mu_H(a \otimes b)}_{\substack{=ab \\ (\text{since } \mu_H \text{ is the multiplication map})}}\right) = f(ab)$$

and

$$\begin{aligned}
&(\mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f))(a \otimes b) \\
&= \mu_A\left(\underbrace{(f \otimes e_{H,A} + e_{H,A} \otimes f)(a \otimes b)}_{=\left(f \otimes e_{H,A}\right)(a \otimes b) + \left(e_{H,A} \otimes f\right)(a \otimes b)}\right) \\
&= \mu_A\left(\underbrace{(f \otimes e_{H,A})(a \otimes b)}_{=f(a) \otimes e_{H,A}(b)} + \underbrace{(e_{H,A} \otimes f)(a \otimes b)}_{=e_{H,A}(a) \otimes f(b)}\right) \\
&= \mu_A(f(a) \otimes e_{H,A}(b) + e_{H,A}(a) \otimes f(b)) \\
&= f(a) \underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_H}(b) + \underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_H}(a) f(b) \qquad \left(\text{since } \mu_A \text{ is the multiplication map}\right) \\
&= f(a) \underbrace{(\eta_A \circ \varepsilon_H)(b)}_{\substack{=\eta_A(\varepsilon_H(b)) = \varepsilon_H(b) \cdot 1_A \\ (\text{by the definition of } \eta_A)}} + \underbrace{(\eta_A \circ \varepsilon_H)(a)}_{\substack{=\eta_A(\varepsilon_H(a)) = \varepsilon_H(a) \cdot 1_A \\ (\text{by the definition of } \eta_A)}} f(b) \\
&= f(a) \varepsilon_H(b) \cdot 1_A + \varepsilon_H(a) \cdot 1_A f(b) = f(a) \varepsilon_H(b) + \varepsilon_H(a) f(b).
\end{aligned}$$

Now, we have the following chain of equivalences:

$$
\begin{aligned}
&\text{(the map } f \text{ is an } (\varepsilon_H, \varepsilon_H)\text{-derivation in the sense of Definition 15.6)} \\
&\iff (f \circ \mu_H = \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f)) \qquad \text{(by Definition 15.6)} \\
&\iff \text{(the two maps } f \circ \mu_H \text{ and } \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f) \text{ are equal)} \\
&\iff \text{(the two maps } f \circ \mu_H \text{ and } \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f) \text{ are equal on each pure tensor)} \\
&\qquad \text{(by (76))} \\
&\iff \left(\underbrace{(f \circ \mu_H)(a \otimes b)}_{=f(ab)} = \underbrace{(\mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f))(a \otimes b)}_{=f(a)\varepsilon_H(b)+\varepsilon_H(a)f(b)} \text{ for each } (a,b) \in H \times H \right) \\
&\qquad \text{(by (77))} \\
&\iff (f(ab) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\,f(b) \text{ for each } (a,b) \in H \times H) \\
&\iff \text{(the map } f \text{ is an } (\varepsilon_H, \varepsilon_H)\text{-derivation in the sense of Definition 15.7)} \\
&\qquad \text{(by Definition 15.7)}.
\end{aligned}
$$

In other words, Definition 15.6 and Definition 15.7 are equivalent. This proves Proposition 15.8. □

There is another way of thinking about $(\varepsilon_H, \varepsilon_H)$-derivations. It is given by a result (in some way) dual to Theorem 7.2:

Theorem 15.9. Let k be a field. Let H be a k-algebra, and let $\varepsilon_H : H \to k$ be a k-algebra homomorphism. Let A be a k-algebra. Let $f : H \to A$ be a k-linear map. Then, f is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $f\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$. [49]

Proof of Theorem 15.9. **a)** Let us prove that if f is an $(\varepsilon_H, \varepsilon_H)$-derivation, then $f\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$.

Proof. Assume that f is an $(\varepsilon_H, \varepsilon_H)$-derivation. By Definition 15.7, this means that

$$\text{every } (a,b) \in H \times H \text{ satisfies } f(ab) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\,f(b). \tag{78}$$

Applying (78) to $(a,b) = (1_H, 1_H)$, we get

$$
\begin{aligned}
f(1_H 1_H) &= f(1_H)\,\varepsilon_H(1_H) + \varepsilon_H(1_H)\,f(1_H) = f(1_H)\,1 + 1 f(1_H) \\
&\qquad \text{(since } \varepsilon_H \text{ is a } k\text{-algebra homomorphism, and thus } \varepsilon_H(1_H) = 1) \\
&= f(1_H) + f(1_H).
\end{aligned}
$$

Since $1_H 1_H = 1_H$, this rewrites as $f(1_H) = f(1_H) + f(1_H)$. This simplifies to $f(1_H) = 0$.

On the other hand,

$$\text{every } (a,b) \in (\operatorname{Ker}(\varepsilon_H)) \times (\operatorname{Ker}(\varepsilon_H)) \text{ satisfies } f(ab) = 0. \tag{79}$$

[49] Recall that $(\operatorname{Ker}(\varepsilon_H))^2$ is defined according to Convention 15.2; thus, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

[50]

Now it is easy to see that $f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2\right) = 0$. [51]

But f is k-linear, so that

$$f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H\right) = \underbrace{f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2\right)}_{=0} + k \cdot \underbrace{f\left(1_H\right)}_{=0} = 0 + k \cdot 0 = 0.$$

So we have shown that $f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H\right) = 0$. This proves **a)**.

b) Now let us prove that if $f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H\right) = 0$, then f is an $(\varepsilon_H, \varepsilon_H)$-derivation.

Proof. Assume that $f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H\right) = 0$.

Let $(a, b) \in H \times H$ be arbitrary. Since

$$\begin{aligned}\varepsilon_H\left(a - \varepsilon_H\left(a\right) \cdot 1_H\right) &= \varepsilon_H\left(a\right) - \varepsilon_H\left(a\right) \cdot 1 \qquad \text{(since } \varepsilon_H \text{ is a } k\text{-algebra homomorphism)} \\ &= \varepsilon_H\left(a\right) - \varepsilon_H\left(a\right) = 0,\end{aligned}$$

we have $a - \varepsilon_H\left(a\right) \cdot 1_H \in \operatorname{Ker}\left(\varepsilon_H\right)$ and similarly $b - \varepsilon_H\left(b\right) \cdot 1_H \in \operatorname{Ker}\left(\varepsilon_H\right)$. Hence, $\underbrace{\left(a - \varepsilon_H\left(a\right) \cdot 1_H\right)}_{\in \operatorname{Ker}\left(\varepsilon_H\right)} \underbrace{\left(b - \varepsilon_H\left(b\right) \cdot 1_H\right)}_{\in \operatorname{Ker}\left(\varepsilon_H\right)} \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) = \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. Thus,

$$\underbrace{\left(a - \varepsilon_H\left(a\right) \cdot 1_H\right)\left(b - \varepsilon_H\left(b\right) \cdot 1_H\right)}_{\in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2} + \left(\underbrace{-\varepsilon_H\left(a\right)\varepsilon_H\left(b\right)}_{\in k} \cdot 1_H\right) \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H,$$

so that

$$f\left(\left(a - \varepsilon_H\left(a\right) \cdot 1_H\right)\left(b - \varepsilon_H\left(b\right) \cdot 1_H\right) + \left(-\varepsilon_H\left(a\right)\varepsilon_H\left(b\right) \cdot 1_H\right)\right) \in f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H\right) = 0.$$

---

[50] *Proof.* Let $(a, b) \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \times \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)$. Then, $a \in \operatorname{Ker}\left(\varepsilon_H\right)$, so that $\varepsilon_H\left(a\right) = 0$ and similarly $\varepsilon_H\left(b\right) = 0$. Now, (78) yields $f\left(ab\right) = f\left(a\right)\underbrace{\varepsilon_H\left(b\right)}_{=0} + \underbrace{\varepsilon_H\left(a\right)}_{=0} f\left(b\right) = f\left(a\right)0 + 0f\left(b\right) = 0$, and thus (79) is proven.

[51] *Proof.* Let $x \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. Then,

$$\begin{aligned}x \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 &= \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \\ &= (\text{the } k\text{-vector subspace of } H \text{ generated by the terms } ab \text{ with } (a, b) \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \times \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)) \\ &= (\text{the set of all } k\text{-linear combinations of terms of the form } ab \text{ with } (a, b) \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \times \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)).\end{aligned}$$

Hence, x is a k-linear combination of terms of the form ab with $(a, b) \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \times \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)$. In other words, there exists some $n \in \mathbb{N}$, some elements λ_1, λ_2, ..., λ_n of k, some elements a_1, a_2, ..., a_n of $\operatorname{Ker}\left(\varepsilon_H\right)$, and some elements b_1, b_2, ..., b_n of $\operatorname{Ker}\left(\varepsilon_H\right)$ such that $x = \sum_{i=1}^{n} \lambda_i a_i b_i$. Consider this n, these λ_1, λ_2, ..., λ_n, these a_1, a_2, ..., a_n, and these b_1, b_2, ..., b_n. Then, $x = \sum_{i=1}^{n} \lambda_i a_i b_i$ leads to

$$\begin{aligned}f\left(x\right) &= f\left(\sum_{i=1}^{n} \lambda_i a_i b_i\right) = \sum_{i=1}^{n} \lambda_i \underbrace{f\left(a_i b_i\right)}_{\substack{=0 \\ \text{(by (79), applied to } (a,b)=(a_i,b_i))}} \qquad \text{(since } f \text{ is } k\text{-linear)} \\ &= \sum_{i=1}^{n} \lambda_i 0 = 0.\end{aligned}$$

Since this is proven for every $x \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$, we thus have $f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2\right) = 0$, qed.

In other words,

$$f\left(\left(a-\varepsilon_H\left(a\right)\cdot 1_H\right)\left(b-\varepsilon_H\left(b\right)\cdot 1_H\right)+\left(-\varepsilon_H\left(a\right)\varepsilon_H\left(b\right)\cdot 1_H\right)\right)=0.$$

Thus,

$$\begin{aligned}
0 &= f\left(\underbrace{\left(a-\varepsilon_H\left(a\right)\cdot 1_H\right)\left(b-\varepsilon_H\left(b\right)\cdot 1_H\right)}_{=ab-a\varepsilon_H(b)-\varepsilon_H(a)b+\varepsilon_H(a)\varepsilon_H(b)1_H}+\left(-\varepsilon_H\left(a\right)\varepsilon_H\left(b\right)\cdot 1_H\right)\right) \\
&= f\left(ab-a\varepsilon_H\left(b\right)-\varepsilon_H\left(a\right)b+\underbrace{\varepsilon_H\left(a\right)\varepsilon_H\left(b\right)1_H-\varepsilon_H\left(a\right)\varepsilon_H\left(b\right)\cdot 1_H}_{=0}\right) \\
&= f\left(ab-a\varepsilon_H\left(b\right)-\varepsilon_H\left(a\right)b\right)=f\left(ab\right)-f\left(a\right)\varepsilon_H\left(b\right)-\varepsilon_H\left(a\right)f\left(b\right) \qquad \left(\text{since } f \text{ is } k\text{-linear}\right).
\end{aligned}$$

This rewrites as

$$f\left(ab\right)=f\left(a\right)\varepsilon_H\left(b\right)+\varepsilon_H\left(a\right)f\left(b\right).$$

Forget that we fixed (a,b). We have proven that every $(a,b)\in H\times H$ satisfies $f\left(ab\right)=f\left(a\right)\varepsilon_H\left(b\right)+\varepsilon_H\left(a\right)f\left(b\right)$. By Definition 15.7, this means that f is an $(\varepsilon_H,\varepsilon_H)$-derivation. This proves **b)**.

c) Combining the results of **a)** and **b)**, we see that f is an $(\varepsilon_H,\varepsilon_H)$-derivation if and only if $f\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2+k\cdot 1_H\right)=0$. This proves Theorem 15.9. □

Our main thrust on Theorem 15.3 will come from the next theorem, which is (in some ways, but not completely) a dual version of Theorem 8.1:

Theorem 15.10. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a commutative k-algebra. Let $f\in\mathfrak{g}\left(H,A\right)$. Then, f is an $(\varepsilon_H,\varepsilon_H)$-derivation if and only if e^{*f} is a k-algebra homomorphism.

Being an "if and only if" statement, the assertion of this theorem splits into two parts, which we will now formulate as two independent lemmas:

Lemma 15.11. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a commutative k-algebra. Let $f\in\mathfrak{g}\left(H,A\right)$. If f is an $(\varepsilon_H,\varepsilon_H)$-derivation, then e^{*f} is a k-algebra homomorphism.

Lemma 15.12. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a commutative k-algebra. Let $f\in\mathfrak{g}\left(H,A\right)$. If e^{*f} is a k-algebra homomorphism, then f is an $(\varepsilon_H,\varepsilon_H)$-derivation.

In order to prove Lemma 15.11, we first show an auxiliary result:

Lemma 15.13. Let k be a field. Let H be a k-bialgebra. Let A be a commutative k-algebra. Let $f \in \mathcal{L}(H, A)$ be an $(\varepsilon_H, \varepsilon_H)$-derivation. Then, for every $n \in \mathbb{N}$, we have

$$f^{*n}(ab) = \sum_{i=0}^{n} \binom{n}{i} f^{*i}(a) f^{*(n-i)}(b) \qquad \text{for any } a \in H \text{ and } b \in H. \quad (80)$$

Note that this Lemma 15.13 is the dual of Lemma 9.7 - as you can see if you rewrite the equation (80) as

$$f^{*n} \circ \mu_H = \sum_{i=0}^{n} \binom{n}{i} \mu_A \circ \left(f^{*i} \otimes f^{*(n-i)}\right).$$

This time, it is a true duality, without any filtrations that could prevent us from dualizing things. As a consequence, one could obtain a proof of Lemma 15.13 by "reversing all arrows" in our above proof of Lemma 9.7 (but first, one would have to rewrite our above proof of Lemma 9.7 in a purely categorical form). Let us here take a somewhat different route towards proving Lemma 15.13 - namely, by direct computation with elements. It will turn out to be faster and easier (although still requiring a lot of computation since we are not using Sweedler notation).

Proof of Lemma 15.13. We are going to prove Lemma 15.13 by induction over n.

Induction base: We have $f^{*0} = e_{H,A} = \eta_A \circ \varepsilon_H$. Hence, every $x \in H$ satisfies

$$f^{*0}(x) = (\eta_A \circ \varepsilon_H)(x) = \eta_A(\varepsilon_H(x)) = \varepsilon_H(x) 1_A \qquad \text{(by the definition of } \eta_A). \quad (81)$$

Applying (81) to $x = a$, we obtain $f^{*0}(a) = \varepsilon_H(a) 1_A$. Applying (81) to $x = b$, we obtain $f^{*0}(b) = \varepsilon_H(b) 1_A$. Applying (81) to $x = ab$, we obtain $f^{*0}(ab) = \varepsilon_H(ab) 1_A$. Since H is a bialgebra, we have $\varepsilon_H(ab) = \varepsilon_H(a) \varepsilon_H(b)$ (by the axioms of a bialgebra). Now, comparing

$$f^{*0}(ab) = \underbrace{\varepsilon_H(ab)}_{=\varepsilon_H(a)\varepsilon_H(b)} 1_A = \varepsilon_H(a) \varepsilon_H(b) 1_A$$

with

$$\sum_{i=0}^{0} \binom{0}{i} f^{*i}(a) f^{*(0-i)}(b) = \underbrace{\binom{0}{0}}_{=1} f^{*0}(a) \underbrace{f^{*(0-0)}}_{=f^{*0}}(b) = \underbrace{f^{*0}(a)}_{=\varepsilon_H(a)1_A} \underbrace{f^{*0}(b)}_{=\varepsilon_H(b)1_A} = \varepsilon_H(a) 1_A \cdot \varepsilon_H(b) 1_A$$
$$= \varepsilon_H(a) \varepsilon_H(b) 1_A,$$

we obtain $f^{*0}(ab) = \sum_{i=0}^{0} \binom{0}{i} f^{*i}(a) f^{*(0-i)}(b)$. In other words, Lemma 15.13 holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that Lemma 15.13 holds for $n = N$. To complete the induction, we must show that Lemma 15.13 also holds for $n = N + 1$.

Since Lemma 15.13 holds for $n = N$, we have

$$f^{*N}(ab) = \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a) f^{*(N-i)}(b) \qquad \text{for any } a \in H \text{ and } b \in H. \quad (82)$$

On the other hand, f is an $(\varepsilon_H, \varepsilon_H)$-derivation. By Definition 15.7, this means that

$$f(ab) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\,f(b) \qquad \text{for any } (a,b) \in H \times H. \tag{83}$$

Now let $a \in H$ and $b \in H$ be arbitrary.

Since $\Delta_H(a) \in H \otimes H$, we can write $\Delta_H(a)$ in the form $\Delta_H(a) = \sum_{j=1}^{M} \lambda_j a_j \otimes a'_j$ for some $M \in \mathbb{N}$, some elements λ_1, λ_2, ..., λ_M of k, some elements a_1, a_2, ..., a_M of H, and some elements a'_1, a'_2, ..., a'_M of H. Consider this M, these λ_1, λ_2, ..., λ_M, these a_1, a_2, ..., a_M, and these a'_1, a'_2, ..., a'_M.

Since $\Delta_H(b) \in H \otimes H$, we can write $\Delta_H(b)$ in the form $\Delta_H(b) = \sum_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell$ for some $K \in \mathbb{N}$, some elements μ_1, μ_2, ..., μ_K of k, some elements b_1, b_2, ..., b_K of H, and some elements b'_1, b'_2, ..., b'_K of H. Consider this K, these μ_1, μ_2, ..., μ_K, these b_1, b_2, ..., b_K, and these b'_1, b'_2, ..., b'_K.

Since H is a bialgebra,

$$\begin{aligned}
\Delta_H(ab) &= \underbrace{\Delta_H(a)}_{=\sum_{j=1}^{M} \lambda_j a_j \otimes a'_j} \cdot \underbrace{\Delta_H(b)}_{=\sum_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell} \qquad \text{(by the axioms of a bialgebra)} \\
&= \left(\sum_{j=1}^{M} \lambda_j a_j \otimes a'_j\right) \cdot \left(\sum_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell\right) = \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell \underbrace{\left(a_j \otimes a'_j\right)\left(b_\ell \otimes b'_\ell\right)}_{=a_j b_\ell \otimes a'_j b'_\ell} \\
&= \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell a_j b_\ell \otimes a'_j b'_\ell.
\end{aligned}$$

Now, $f^{*(N+1)} = f * f^{*N} = \mu_A \circ \left(f \otimes f^{*N}\right) \circ \Delta_H$ (by the definition of convolution),

so that

$$f^{*(N+1)}(ab) = \left(\mu_A \circ \left(f \otimes f^{*N}\right) \circ \Delta_H\right)(ab)$$

$$= \mu_A\left(\left(f \otimes f^{*N}\right) \underbrace{\left(\Delta_H(ab)\right)}_{=\sum_{j=1}^{M}\sum_{\ell=1}^{K}\lambda_j\mu_\ell a_j b_\ell \otimes a'_j b'_\ell}\right) = \mu_A\left(\underbrace{\left(f \otimes f^{*N}\right)\left(\sum_{j=1}^{M}\sum_{\ell=1}^{K}\lambda_j\mu_\ell a_j b_\ell \otimes a'_j b'_\ell\right)}_{\substack{=\sum_{j=1}^{M}\sum_{\ell=1}^{K}\lambda_j\mu_\ell f(a_j b_\ell)\otimes f^{*N}\left(a'_j b'_\ell\right) \\ \text{(by the definition of } f\otimes f^{*N}\text{)}}}\right)$$

$$= \mu_A\left(\sum_{j=1}^{M}\sum_{\ell=1}^{K}\lambda_j\mu_\ell f(a_j b_\ell) \otimes f^{*N}\left(a'_j b'_\ell\right)\right) = \sum_{j=1}^{M}\sum_{\ell=1}^{K}\lambda_j\mu_\ell \underbrace{f(a_j b_\ell)}_{\substack{=f(a_j)\varepsilon_H(b_\ell)+\varepsilon_H(a_j)f(b_\ell) \\ \text{(by (83), applied to} \\ (a_j, b_\ell) \text{ instead of } (a,b)\text{)}}} \cdot f^{*N}\left(a'_j b'_\ell\right)$$

(since μ_A is the multiplication map)

$$= \sum_{j=1}^{M}\sum_{\ell=1}^{K}\underbrace{\lambda_j\mu_\ell\left(f(a_j)\varepsilon_H(b_\ell) + \varepsilon_H(a_j) f(b_\ell)\right)\cdot f^{*N}\left(a'_j b'_\ell\right)}_{=\lambda_j\mu_\ell f(a_j)\varepsilon_H(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right)+\lambda_j\mu_\ell\varepsilon_H(a_j)f(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right)}$$

$$= \sum_{j=1}^{M}\sum_{\ell=1}^{K}\left(\lambda_j\mu_\ell f(a_j)\varepsilon_H(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right) + \lambda_j\mu_\ell\varepsilon_H(a_j) f(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right)\right)$$

$$= \underbrace{\sum_{j=1}^{M}\sum_{\ell=1}^{K}\lambda_j\mu_\ell f(a_j)\varepsilon_H(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right)}_{=\sum_{j=1}^{M}\lambda_j f(a_j)\sum_{\ell=1}^{K}\mu_\ell\varepsilon_H(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right)} + \underbrace{\sum_{j=1}^{M}\sum_{\ell=1}^{K}\lambda_j\mu_\ell\varepsilon_H(a_j) f(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right)}_{=\sum_{\ell=1}^{K}\mu_\ell f(b_\ell)\sum_{j=1}^{M}\lambda_j\varepsilon_H(a_j)\cdot f^{*N}\left(a'_j b'_\ell\right)}$$

$$= \sum_{j=1}^{M}\lambda_j f(a_j)\underbrace{\sum_{\ell=1}^{K}\mu_\ell\varepsilon_H(b_\ell)\cdot f^{*N}\left(a'_j b'_\ell\right)}_{\substack{=f^{*N}\left(\sum_{\ell=1}^{K}\mu_\ell\varepsilon_H(b_\ell)a'_j b'_\ell\right) \\ \text{(since } f^{*N} \text{ is } k\text{-linear)}}} + \sum_{\ell=1}^{K}\mu_\ell f(b_\ell)\underbrace{\sum_{j=1}^{M}\lambda_j\varepsilon_H(a_j)\cdot f^{*N}\left(a'_j b'_\ell\right)}_{\substack{=f^{*N}\left(\sum_{j=1}^{M}\lambda_j\varepsilon_H(a_j)\cdot a'_j b'_\ell\right) \\ \text{(since } f^{*N} \text{ is } k\text{-linear)}}}$$

$$= \sum_{j=1}^{M}\lambda_j f(a_j) f^{*N}\left(\sum_{\ell=1}^{K}\mu_\ell\varepsilon_H(b_\ell) a'_j b'_\ell\right) + \sum_{\ell=1}^{K}\mu_\ell f(b_\ell) f^{*N}\left(\sum_{j=1}^{M}\lambda_j\varepsilon_H(a_j)\cdot a'_j b'_\ell\right). \tag{84}$$

Now, it is easy to see (using the axioms of a coalgebra and the fact that $\Delta_H(b) =$

$\sum\limits_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell$) that $\sum\limits_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell)\, b'_\ell = b$ [52], and thus every $j \in \{1,2,\ldots,M\}$ satisfies

$$\sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell)\, a'_j b'_\ell = a'_j \cdot \underbrace{\sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell)\, b'_\ell}_{=b} = a'_j b,$$

so that

$$f^{*N}\left(\sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell)\, a'_j b'_\ell\right) = f^{*N}\left(a'_j b\right) = \sum_{i=0}^{N} \binom{N}{i} f^{*i}\left(a'_j\right) f^{*(N-i)}(b)$$
$$\left(\text{by (82), applied to } a'_j \text{ instead of } a\right).$$

Hence,

$$\sum_{j=1}^{M} \lambda_j f(a_j) \underbrace{f^{*N}\left(\sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell)\, a'_j b'_\ell\right)}_{=\sum\limits_{i=0}^{N}\binom{N}{i} f^{*i}\left(a'_j\right) f^{*(N-i)}(b)}$$
$$= \sum_{j=1}^{M} \lambda_j f(a_j) \sum_{i=0}^{N} \binom{N}{i} f^{*i}\left(a'_j\right) f^{*(N-i)}(b)$$
$$= \sum_{i=0}^{N} \binom{N}{i} \left(\sum_{j=1}^{M} \lambda_j f(a_j)\, f^{*i}\left(a'_j\right)\right) f^{*(N-i)}(b). \tag{85}$$

Also, it is easy to see (using the axioms of a coalgebra and the fact that $\Delta_H(a) =$

[52] *Proof.* Let $\mathrm{kan} : k \otimes H \to H$ be the canonical isomorphism (which maps $1 \otimes x$ to x for every $x \in H$). Then, by the axioms of a coalgebra, $\mathrm{kan} \circ (\varepsilon_H \otimes \mathrm{id}_H) \circ \Delta_H = \mathrm{id}_H$ (since H is a coalgebra). Thus, $(\mathrm{kan} \circ (\varepsilon_H \otimes \mathrm{id}_H) \circ \Delta_H)(b) = \mathrm{id}_H(b)$. Since

$$(\mathrm{kan} \circ (\varepsilon_H \otimes \mathrm{id}_H) \circ \Delta_H)(b) = \mathrm{kan}\left((\varepsilon_H \otimes \mathrm{id}_H)\ \underbrace{(\Delta_H(b))}_{=\sum\limits_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell}\right) = \mathrm{kan}\left(\underbrace{(\varepsilon_H \otimes \mathrm{id}_H)\left(\sum_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell\right)}_{\substack{=\sum\limits_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell) \otimes \mathrm{id}_H\left(b'_\ell\right) \\ \text{(by the definition of } \varepsilon_H \otimes \mathrm{id}_H \text{)}}}\right)$$
$$= \mathrm{kan}\left(\sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell) \otimes \mathrm{id}_H\left(b'_\ell\right)\right) = \sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell) \underbrace{\mathrm{id}_H\left(b'_\ell\right)}_{=b'_\ell} \qquad \text{(by the definition of kan)}$$
$$= \sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell)\, b'_\ell$$

and $\mathrm{id}_H(b) = b$, this rewrites as $\sum\limits_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell)\, b'_\ell = b$, qed.

$\sum\limits_{j=1}^{M} \lambda_j a_j \otimes a'_j$) that $\sum\limits_{j=1}^{M} \lambda_j \varepsilon_H(a_j)\, a'_j = a$ [53], and thus every $\ell \in \{1,2,\ldots,M\}$ satisfies

$$\sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j) \cdot a'_j b'_\ell = \underbrace{\sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j)\, a'_j}_{=a} \cdot b'_\ell = a b'_\ell,$$

so that

$$f^{*N}\left(\sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j) \cdot a'_j b'_\ell\right) = f^{*N}(a b'_\ell) = \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a)\, f^{*(N-i)}(b'_\ell)$$
$$\text{(by (82), applied to } b'_\ell \text{ instead of } b).$$

Hence,

$$\sum_{\ell=1}^{K} \mu_\ell f(b_\ell) \underbrace{f^{*N}\left(\sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j) \cdot a'_j b'_\ell\right)}_{=\sum\limits_{i=0}^{N} \binom{N}{i} f^{*i}(a) f^{*(N-i)}\left(b'_\ell\right)}$$
$$= \sum_{\ell=1}^{K} \mu_\ell f(b_\ell) \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a)\, f^{*(N-i)}(b'_\ell) = \sum_{i=0}^{N} \binom{N}{i} \sum_{\ell=1}^{K} \mu_\ell \underbrace{f(b_\ell)\, f^{*i}(a)}_{\substack{=f^{*i}(a) f(b_\ell) \\ \text{(since } A \text{ is commutative)}}} f^{*(N-i)}(b'_\ell)$$
$$= \sum_{i=0}^{N} \binom{N}{i} \sum_{\ell=1}^{K} \mu_\ell f^{*i}(a)\, f(b_\ell)\, f^{*(N-i)}(b'_\ell) = \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a) \left(\sum_{\ell=1}^{K} \mu_\ell f(b_\ell)\, f^{*(N-i)}(b'_\ell)\right). \tag{86}$$

---

[53] *Proof.* Let $\mathrm{kan} : k \otimes H \to H$ be the canonical isomorphism (which maps $1 \otimes x$ to x for every $x \in H$). Then, by the axioms of a coalgebra, $\mathrm{kan} \circ (\varepsilon_H \otimes \mathrm{id}_H) \circ \Delta_H = \mathrm{id}_H$ (since H is a coalgebra). Thus, $(\mathrm{kan} \circ (\varepsilon_H \otimes \mathrm{id}_H) \circ \Delta_H)(a) = \mathrm{id}_H(a)$. Since

$$(\mathrm{kan} \circ (\varepsilon_H \otimes \mathrm{id}_H) \circ \Delta_H)(a)$$
$$= \mathrm{kan}\left((\varepsilon_H \otimes \mathrm{id}_H) \underbrace{(\Delta_H(a))}_{=\sum\limits_{j=1}^{M} \lambda_j a_j \otimes a'_j}\right) = \mathrm{kan}\left(\underbrace{(\varepsilon_H \otimes \mathrm{id}_H)\left(\sum_{j=1}^{M} \lambda_j a_j \otimes a'_j\right)}_{\substack{=\sum\limits_{j=1}^{M} \lambda_j \varepsilon_H(a_j) \otimes \mathrm{id}_H\left(a'_j\right) \\ \text{(by the definition of } \varepsilon_H \otimes \mathrm{id}_H \text{)}}}\right)$$
$$= \mathrm{kan}\left(\sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j) \otimes \mathrm{id}_H\left(a'_j\right)\right) = \sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j) \underbrace{\mathrm{id}_H\left(a'_j\right)}_{=a'_j} \qquad \text{(by the definition of kan)}$$
$$= \sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j)\, a'_j$$

and $\mathrm{id}_H(a) = a$, this rewrites as $\sum\limits_{j=1}^{M} \lambda_j \varepsilon_H(a_j)\, a'_j = a$, qed.

Now, (84) becomes

$$f^{*(N+1)}(ab) = \underbrace{\sum_{j=1}^{M} \lambda_j f(a_j) f^{*N}\left(\sum_{\ell=1}^{K} \mu_\ell \varepsilon_H(b_\ell) a'_j b'_\ell\right)}_{=\sum_{i=0}^{N}\binom{N}{i}\left(\sum_{j=1}^{M}\lambda_j f(a_j) f^{*i}\left(a'_j\right)\right) f^{*(N-i)}(b) \text{ (by (85))}} + \underbrace{\sum_{\ell=1}^{K} \mu_\ell f(b_\ell) f^{*N}\left(\sum_{j=1}^{M} \lambda_j \varepsilon_H(a_j) \cdot a'_j b'_\ell\right)}_{=\sum_{i=0}^{N}\binom{N}{i} f^{*i}(a)\left(\sum_{\ell=1}^{K}\mu_\ell f(b_\ell) f^{*(N-i)}\left(b'_\ell\right)\right) \text{ (by (86))}}$$

$$= \sum_{i=0}^{N}\binom{N}{i}\left(\sum_{j=1}^{M}\lambda_j f(a_j) f^{*i}\left(a'_j\right)\right) f^{*(N-i)}(b) + \sum_{i=0}^{N}\binom{N}{i} f^{*i}(a)\left(\sum_{\ell=1}^{K}\mu_\ell f(b_\ell) f^{*(N-i)}\left(b'_\ell\right)\right). \tag{87}$$

But now, we notice that every $i \in \{0, 1, \ldots, N\}$ satisfies

$$f^{*(i+1)}(a) = \left(\mu_A \circ \left(f \otimes f^{*i}\right) \circ \Delta_H\right)(a)$$

$$\left(\text{since } f^{*(i+1)} = f * f^{*i} = \mu_A \circ \left(f \otimes f^{*i}\right) \circ \Delta_H \text{ by the definition of convolution}\right)$$

$$= \mu_A\left(\left(f \otimes f^{*i}\right)\left(\underbrace{\Delta_H(a)}_{=\sum_{j=1}^{M}\lambda_j a_j \otimes a'_j}\right)\right) = \mu_A\left(\underbrace{\left(f \otimes f^{*i}\right)\left(\sum_{j=1}^{M}\lambda_j a_j \otimes a'_j\right)}_{=\sum_{j=1}^{M}\lambda_j f(a_j)\otimes f^{*i}\left(a'_j\right) \text{ (by the definition of } f\otimes f^{*i})}\right)$$

$$= \mu_A\left(\sum_{j=1}^{M}\lambda_j f(a_j) \otimes f^{*i}\left(a'_j\right)\right) = \sum_{j=1}^{M}\lambda_j f(a_j) f^{*i}\left(a'_j\right) \tag{88}$$

(since μ_A is the multiplication map) and

$$f^{*(N-i+1)}(b)$$

$$= \left(\mu_A \circ \left(f \otimes f^{*(N-i)}\right) \circ \Delta_H\right)(b)$$

$$\left(\text{since } f^{*(N-i+1)} = f * f^{*(N-i)} = \mu_A \circ \left(f \otimes f^{*(N-i)}\right) \circ \Delta_H \text{ by the definition of convolution}\right)$$

$$= \mu_A\left(\left(f \otimes f^{*(N-i)}\right)\left(\underbrace{\Delta_H(b)}_{=\sum_{\ell=1}^{K}\mu_\ell b_\ell \otimes b'_\ell}\right)\right) = \mu_A\left(\underbrace{\left(f \otimes f^{*(N-i)}\right)\left(\sum_{\ell=1}^{K}\mu_\ell b_\ell \otimes b'_\ell\right)}_{=\sum_{\ell=1}^{K}\mu_\ell f(b_\ell)\otimes f^{*(N-i)}\left(b'_\ell\right) \text{ (by the definition of } f\otimes f^{*(N-i)})}\right)$$

$$= \mu_A\left(\sum_{\ell=1}^{K}\mu_\ell f(b_\ell) \otimes f^{*(N-i)}\left(b'_\ell\right)\right) = \sum_{\ell=1}^{K}\mu_\ell f(b_\ell) f^{*(N-i)}\left(b'_\ell\right) \tag{89}$$

(since μ_A is the multiplication map).

With the help of these identities, (87) becomes

$$
\begin{aligned}
f^{*(N+1)}(ab) &= \sum_{i=0}^{N} \binom{N}{i} \underbrace{\left(\sum_{j=1}^{M} \lambda_j f(a_j) f^{*i}(a'_j) \right)}_{\substack{= f^{*(i+1)}(a) \\ \text{(by (88))}}} f^{*(N-i)}(b) \\
&\qquad + \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a) \underbrace{\left(\sum_{\ell=1}^{K} \mu_\ell f(b_\ell) f^{*(N-i)}(b'_\ell) \right)}_{\substack{= f^{*(N-i+1)}(b) \\ \text{(by (89))}}} \\
&= \sum_{i=0}^{N} \binom{N}{i} f^{*(i+1)}(a) f^{*(N-i)}(b) + \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a) f^{*(N-i+1)}(b) \\
&= \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a) f^{*(N-i+1)}(b) + \sum_{i=0}^{N} \binom{N}{i} f^{*(i+1)}(a) f^{*(N-i)}(b) \\
&= \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a) \underbrace{f^{*(N-i+1)}}_{= f^{*(N+1-i)}}(b) + \sum_{i=1}^{N+1} \binom{N}{i-1} \underbrace{f^{*((i-1)+1)}}_{= f^{*i}}(a) \underbrace{f^{*(N-(i-1))}}_{= f^{*(N+1-i)}}(b) \\
&\qquad \text{(here, we substituted } i-1 \text{ for } i \text{ in the second sum)} \\
&= \sum_{i=0}^{N} \binom{N}{i} f^{*i}(a) f^{*(N+1-i)}(b) + \sum_{i=1}^{N+1} \binom{N}{i-1} f^{*i}(a) f^{*(N+1-i)}(b) .
\end{aligned}
$$

Compared to

$$\sum_{i=0}^{N+1}\binom{N+1}{i}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)$$

$$=\sum_{i=0}^{N+1}\left(\binom{N}{i}+\binom{N}{i-1}\right)f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)$$

$$\left(\text{since }\binom{N+1}{i}=\binom{N}{i}+\binom{N}{i-1}\text{ by the recurrence of the binomial coefficients}\right)$$

$$=\underbrace{\sum_{i=0}^{N+1}\binom{N}{i}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)}_{=\sum_{i=0}^{N}\binom{N}{i}f^{*i}(a)f^{*(N+1-i)}(b)+\binom{N}{N+1}f^{*(N+1)}(a)f^{*(N+1-(N+1))}(b)}$$

$$+\underbrace{\sum_{i=0}^{N+1}\binom{N}{i-1}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)}_{=\binom{N}{0-1}f^{*0}(a)f^{*(N+1-0)}(b)+\sum_{i=1}^{N+1}\binom{N}{i-1}f^{*i}(a)f^{*(N+1-i)}(b)}$$

$$=\left(\sum_{i=0}^{N}\binom{N}{i}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)+\underbrace{\binom{N}{N+1}}_{=0\text{ (since }N+1>N)}f^{*(N+1)}\left(a\right)f^{*\left(N+1-(N+1)\right)}\left(b\right)\right)$$

$$+\left(\underbrace{\binom{N}{0-1}}_{=0\text{ (since }0-1<0)}f^{*0}\left(a\right)f^{*\left(N+1-0\right)}\left(b\right)+\sum_{i=1}^{N+1}\binom{N}{i-1}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)\right)$$

$$=\left(\sum_{i=0}^{N}\binom{N}{i}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)+\underbrace{0f^{*(N+1)}\left(a\right)f^{*\left(N+1-(N+1)\right)}\left(b\right)}_{=0}\right)$$

$$+\left(\underbrace{0f^{*0}\left(a\right)f^{*\left(N+1-0\right)}\left(b\right)}_{=0}+\sum_{i=1}^{N+1}\binom{N}{i-1}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)\right)$$

$$=\sum_{i=0}^{N}\binom{N}{i}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right)+\sum_{i=1}^{N+1}\binom{N}{i-1}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right),$$

this yields

$$f^{*(N+1)}\left(ab\right)=\sum_{i=0}^{N+1}\binom{N+1}{i}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right).$$

Now forget that we fixed a and b. We thus have shown that every $a\in H$ and $b\in H$ satisfy

$$f^{*(N+1)}\left(ab\right)=\sum_{i=0}^{N+1}\binom{N+1}{i}f^{*i}\left(a\right)f^{*\left(N+1-i\right)}\left(b\right).$$

In other words, Lemma 15.13 holds for $n = N + 1$. This completes the induction step. The induction proof of Lemma 15.13 is thus complete. $\square$

Here is a little brother of Lemma 15.13 and, unsurprisingly, the dual of Lemma 9.8:

Lemma 15.14. Let k be a field. Let H be a k-bialgebra. Let A be a commutative k-algebra. Let $f \in \mathcal{L}(H, A)$ be an $(\varepsilon_H, \varepsilon_H)$-derivation. Then, for every positive $n \in \mathbb{N}$, we have $f^{*n}(1_H) = 0$.

Proof of Lemma 15.14. Since H is a k-bialgebra, we have $\Delta_H(1_H) = 1_H \otimes 1_H$ (by the axioms of a bialgebra).

Just as in part **a)** of the proof of Theorem 15.9, we can find that $f(1_H) = 0$ (because H is a k-bialgebra, and thus ε_H is a k-algebra homomorphism (by the axioms of a bialgebra)).

Since n is positive, we have $f^{*n} = f * f^{*(n-1)} = \mu_A \circ \left(f \otimes f^{*(n-1)}\right) \circ \Delta_H$ (by the definition of convolution), and thus

$$\begin{aligned} f^{*n}(1_H) &= \left(\mu_A \circ \left(f \otimes f^{*(n-1)}\right) \circ \Delta_H\right)(1_H) = \mu_A\left(\left(f \otimes f^{*(n-1)}\right) \underbrace{\left(\Delta_H(1_H)\right)}_{=1_H \otimes 1_H}\right) \\ &= \mu_A\left(\underbrace{\left(f \otimes f^{*(n-1)}\right)(1_H \otimes 1_H)}_{=f(1_H) \otimes f^{*(n-1)}(1_H)}\right) = \mu_A\left(\underbrace{f(1_H)}_{=0} \otimes f^{*(n-1)}(1_H)\right) \\ &= \mu_A \underbrace{\left(0 \otimes f^{*(n-1)}(1_H)\right)}_{=0} = \mu_A(0) = 0. \end{aligned}$$

This proves Lemma 15.14. $\square$

Now, in analogy to our above proof of Lemma 8.2 (but, again, slightly simpler), we can prove Lemma 15.11:

Proof of Lemma 15.11. Assume that f is an $(\varepsilon_H, \varepsilon_H)$-derivation.

Let $a \in H$ and $b \in H$. Then, (6) (applied to $x = a$) yields $e^{*f}(a) = \sum_{i \geq 0} \dfrac{f^{*i}(a)}{i!}$. Also, (6) (applied to $x = b$) yields $e^{*f}(b) = \sum_{i \geq 0} \dfrac{f^{*i}(b)}{i!} = \sum_{j \geq 0} \dfrac{f^{*j}(b)}{j!}$ (here, we renamed

the index i as j in the sum). Hence,

$$\begin{aligned}
e^{*f}(a)\cdot e^{*f}(b) &= \left(\sum_{i\geq 0}\frac{f^{*i}(a)}{i!}\right)\cdot\left(\sum_{j\geq 0}\frac{f^{*j}(b)}{j!}\right) = \sum_{i\geq 0}\sum_{j\geq 0}\frac{f^{*i}(a)}{i!}\cdot\frac{f^{*j}(b)}{j!} \\
&= \underbrace{\sum_{i\geq 0}\sum_{\substack{n\geq 0;\\ n\geq i}}}_{=\sum_{n\geq 0}\sum_{\substack{i\geq 0;\\ n\geq i}}}\frac{f^{*i}(a)}{i!}\cdot\frac{f^{*(n-i)}(b)}{(n-i)!} \\
&\qquad \text{(here, we substituted } n-i \text{ for } j \text{ in the second sum)} \\
&= \sum_{n\geq 0}\underbrace{\sum_{\substack{i\geq 0;\\ n\geq i}}}_{=\sum_{i=0}^{n}}\underbrace{\frac{f^{*i}(a)}{i!}\cdot\frac{f^{*(n-i)}(b)}{(n-i)!}}_{=\frac{1}{i!(n-i)!}f^{*i}(a)f^{*(n-i)}(b)} \\
&= \sum_{n\geq 0}\sum_{i=0}^{n}\underbrace{\frac{1}{i!(n-i)!}}_{=\frac{1}{n!}\binom{n}{i}\ \left(\text{since } \frac{n!}{i!(n-i)!}=\binom{n}{i}\right)} f^{*i}(a)\, f^{*(n-i)}(b) \\
&= \sum_{n\geq 0}\sum_{i=0}^{n}\frac{1}{n!}\binom{n}{i}f^{*i}(a)\, f^{*(n-i)}(b) = \sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}f^{*i}(a)\, f^{*(n-i)}(b)\right).
\end{aligned}$$

Compared with

$$\begin{aligned}
e^{*f}(ab) &= \sum_{i\geq 0}\frac{f^{*i}(ab)}{i!} \qquad \text{(by (6), applied to } x=ab) \\
&= \sum_{n\geq 0}\frac{f^{*n}(ab)}{n!} \qquad \text{(here, we renamed the index } i \text{ as } n \text{ in the sum)} \\
&= \sum_{n\geq 0}\frac{1}{n!}f^{*n}(ab) = \sum_{n\geq 0}\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}f^{*i}(a)\, f^{*(n-i)}(b)\right) \qquad \text{(by (80))},
\end{aligned}$$

this yields $e^{*f}(a)\cdot e^{*f}(b) = e^{*f}(ab)$.

Now forget that we fixed a and b. We thus have proven that all $a\in H$ and $b\in H$

satisfy $e^{*f}(a) \cdot e^{*f}(b) = e^{*f}(ab)$. Combined with the fact that

$$e^{*f}(1_H) = \sum_{i \geq 0} \frac{f^{*i}(1_H)}{i!} \qquad \text{(by (6), applied to } x = 1_H\text{)}$$

$$= \frac{f^{*0}(1_H)}{1!} + \sum_{i>0} \underbrace{\frac{f^{*i}(1_H)}{i!}}_{\substack{=0 \\ \text{(because Lemma 15.14 (applied to } n=i\text{) yields } f^{*i}(1_H)=0\text{)}}} = \frac{f^{*0}(1_H)}{1!} + \underbrace{\sum_{i>0} 0}_{=0} = \frac{f^{*0}(1_H)}{1!} = \frac{f^{*0}(1_H)}{1}$$

$$= \underbrace{f^{*0}}_{=e_{H,A}=\eta_A \circ \varepsilon_H} (1_H) = (\eta_A \circ \varepsilon_H)(1_H) = \eta_A(\varepsilon_H(1_H)) = \underbrace{\varepsilon_H(1_H)}_{\substack{=1 \\ \text{(by the axioms of a bialgebra, since } H \text{ is a bialgebra)}}} 1_A$$

(by the definition of η_A)

$$= 1 \cdot 1_A = 1_A,$$

this shows that e^{*f} is a k-algebra homomorphism. This proves Lemma 15.11. $\square$

Next let us prepare for the proof of Lemma 15.12. We are not going to need a "dual" Corollary 11.4, since Corollary 11.4 is already fine (it is as self-dual as a statement about filtered coalgebras can get), but we need a dual of Corollary 10.2, and for this we first need a dual of Proposition 10.1:

Proposition 15.15. Let k be a field. Let H be a k-bialgebra. Let A be a commutative k-algebra. Let $f : H \to A$ and $g : H \to A$ be two k-algebra homomorphisms. Then, $f * g : H \to A$ is also a k-algebra homomorphism.

One possible proof of this proposition would be obtained by reversing the arrows in the proof of Proposition 10.1 (though, of course, we would need to do the same with Lemma 9.5). But let us (like in the proof of Lemma 15.13) work elementwise:

Proof of Proposition 15.15. First we notice that $\Delta_H(1_H) = 1_H \otimes 1_H$ (by the axioms of a bialgebra, since H is a bialgebra). Since $f * g = \mu_A \circ (f \otimes g) \circ \Delta_H$ (by the definition of convolution), we have

$$(f * g)(1_H) = (\mu_A \circ (f \otimes g) \circ \Delta_H)(1_H) = \mu_A\left((f \otimes g)\underbrace{(\Delta_H(1_H))}_{=1_H \otimes 1_H}\right) = \mu_A\left(\underbrace{(f \otimes g)(1_H \otimes 1_H)}_{=f(1_H) \otimes g(1_H)}\right)$$

$$= \mu_A(f(1_H) \otimes g(1_H)) = \underbrace{f(1_H)}_{\substack{=1_A \\ \text{(since } f \text{ is a } k\text{-algebra homomorphism)}}} \underbrace{g(1_H)}_{\substack{=1_A \\ \text{(since } g \text{ is a } k\text{-algebra homomorphism)}}}$$

(since μ_A is the multiplication map)

$$= 1_A \cdot 1_A = 1_A.$$

Now, let $a \in H$ and $b \in H$ be arbitrary.

Since $\Delta_H(a) \in H \otimes H$, we can write $\Delta_H(a)$ in the form $\Delta_H(a) = \sum_{j=1}^{M} \lambda_j a_j \otimes a'_j$ for some $M \in \mathbb{N}$, some elements λ_1, λ_2, ..., λ_M of k, some elements a_1, a_2, ..., a_M of H,

and some elements a'_1, a'_2, ..., a'_M of H. Consider this M, these λ_1, λ_2, ..., λ_M, these a_1, a_2, ..., a_M, and these a'_1, a'_2, ..., a'_M.

Since $\Delta_H(b) \in H \otimes H$, we can write $\Delta_H(b)$ in the form $\Delta_H(b) = \sum_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell$ for some $K \in \mathbb{N}$, some elements μ_1, μ_2, ..., μ_K of k, some elements b_1, b_2, ..., b_K of H, and some elements b'_1, b'_2, ..., b'_K of H. Consider this K, these μ_1, μ_2, ..., μ_K, these b_1, b_2, ..., b_K, and these b'_1, b'_2, ..., b'_K.

Since H is a bialgebra,

$$\begin{aligned}
\Delta_H(ab) &= \underbrace{\Delta_H(a)}_{=\sum_{j=1}^{M} \lambda_j a_j \otimes a'_j} \cdot \underbrace{\Delta_H(b)}_{=\sum_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell} \qquad \text{(by the axioms of a bialgebra)} \\
&= \left(\sum_{j=1}^{M} \lambda_j a_j \otimes a'_j \right) \cdot \left(\sum_{\ell=1}^{K} \mu_\ell b_\ell \otimes b'_\ell \right) = \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell \underbrace{\left(a_j \otimes a'_j\right)\left(b_\ell \otimes b'_\ell\right)}_{=a_j b_\ell \otimes a'_j b'_\ell} \\
&= \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell a_j b_\ell \otimes a'_j b'_\ell.
\end{aligned}$$

Since $f * g = \mu_A \circ (f \otimes g) \circ \Delta_H$, we now have

$$(f * g)(ab) = (\mu_A \circ (f \otimes g) \circ \Delta_H)(ab) = \mu_A \left((f \otimes g) \underbrace{(\Delta_H (ab))}_{= \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell a_j b_\ell \otimes a'_j b'_\ell} \right)$$

$$= \mu_A \left(\underbrace{(f \otimes g) \left(\sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell a_j b_\ell \otimes a'_j b'_\ell \right)}_{= \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell f(a_j b_\ell) \otimes g\left(a'_j b'_\ell\right) \text{ (by the definition of } f \otimes g)} \right)$$

$$= \mu_A \left(\sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell f(a_j b_\ell) \otimes g\left(a'_j b'_\ell\right) \right)$$

$$= \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell \underbrace{f(a_j b_\ell)}_{\substack{= f(a_j) f(b_\ell) \\ \text{(since } f \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} \underbrace{g\left(a'_j b'_\ell\right)}_{\substack{= g\left(a'_j\right) g\left(b'_\ell\right) \\ \text{(since } g \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}}$$

(since μ_A is the multiplication map)

$$= \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell f(a_j) \underbrace{f(b_\ell) g\left(a'_j\right)}_{\substack{= g\left(a'_j\right) f(b_\ell) \\ \text{(since } A \text{ is commutative)}}} g\left(b'_\ell\right)$$

$$= \sum_{j=1}^{M} \sum_{\ell=1}^{K} \lambda_j \mu_\ell f(a_j) g\left(a'_j\right) f(b_\ell) g\left(b'_\ell\right)$$

$$= \left(\sum_{j=1}^{M} \lambda_j f(a_j) g\left(a'_j\right) \right) \left(\sum_{\ell=1}^{K} \mu_\ell f(b_\ell) g\left(b'_\ell\right) \right). \tag{90}$$

Since

$$(f*g)(a) = (\mu_A \circ (f\otimes g)\circ \Delta_H)(a) \qquad \text{(because } f*g = \mu_A\circ(f\otimes g)\circ\Delta_H\text{)}$$

$$= \mu_A\left((f\otimes g)\underbrace{(\Delta_H(a))}_{=\sum_{j=1}^{M}\lambda_j a_j\otimes a'_j}\right) = \mu_A\left(\underbrace{(f\otimes g)\left(\sum_{j=1}^{M}\lambda_j a_j\otimes a'_j\right)}_{\substack{=\sum_{j=1}^{M}\lambda_j f(a_j)\otimes g\left(a'_j\right)\\ \text{(by the definition of } f\otimes g\text{)}}}\right)$$

$$= \mu_A\left(\sum_{j=1}^{M}\lambda_j f(a_j)\otimes g\left(a'_j\right)\right)$$

$$= \sum_{j=1}^{M}\lambda_j f(a_j)\, g\left(a'_j\right) \qquad \text{(since } \mu_A \text{ is the multiplication map)}$$

and

$$(f*g)(b) = \sum_{\ell=1}^{K}\mu_\ell f(b_\ell)\, g(b'_\ell) \qquad \text{(by the same argument, done for } b \text{ instead of } a\text{)},$$

the equality (90) becomes

$$(f*g)(ab) = \underbrace{\left(\sum_{j=1}^{M}\lambda_j f(a_j)\, g\left(a'_j\right)\right)}_{=(f*g)(a)}\underbrace{\left(\sum_{\ell=1}^{K}\mu_\ell f(b_\ell)\, g(b'_\ell)\right)}_{=(f*g)(b)}$$
$$= (f*g)(a)\cdot(f*g)(b).$$

Now forget that we fixed a and b. We have now shown that any $a\in H$ and $b\in H$ satisfy $(f*g)(ab) = (f*g)(a)\cdot(f*g)(b)$. Combined with $(f*g)(1_H) = 1_A$, this yields that $f*g$ is a k-algebra homomorphism. Proposition 15.15 is proven. □

As a consequence, we have:

Corollary 15.16. Let k be a field. Let H be a k-bialgebra. Let A be a commutative k-algebra. Let $f: H\to A$ be a k-algebra homomorphism. Let $n\in\mathbb{N}$. Then, $f^{*n}: H\to A$ is also a k-algebra homomorphism.

Proof of Corollary 15.16. We are going to prove Corollary 15.16 by induction over n.

Induction base: Consider the obvious canonical k-algebra structure on k (with μ_k being the canonical isomorphism $k\otimes k\to k$, and η_k being the identity map). Since A is a k-algebra, it is clear that $\eta_A: k\to A$ is a k-algebra homomorphism.[54] Combined with

[54] *Proof.* Any two $\lambda\in k$ and $\mu\in k$ satisfy

$$\underbrace{\eta_A(\lambda)}_{\substack{=\lambda\cdot 1_A\\ \text{(by the definition of } \eta_A\text{)}}}\cdot\underbrace{\eta_A(\mu)}_{\substack{=\mu\cdot 1_A\\ \text{(by the definition of } \eta_A\text{)}}} = (\lambda\cdot 1_A)\cdot(\mu\cdot 1_A) = \lambda\mu\cdot 1_A = \eta_A(\lambda\mu)$$

(since $\eta_A(\lambda\mu) = \lambda\mu\cdot 1_A$ by the definition of η_A). Combined with the fact that (again, as the definition of η_A shows) $\eta_A(1) = 1\cdot 1_A = 1_A$, this yields that η_A is a k-algebra homomorphism, qed.

the fact that $\varepsilon_H : H \to k$ is a k-algebra homomorphism (because H is a k-bialgebra), this yields that $\eta_A \circ \varepsilon_H$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is a k-algebra homomorphism). Since $f^{*0} = e_{H,A} = \eta_A \circ \varepsilon_H$ (by the definition of $e_{H,A}$), this yields that f^{*0} is a k-algebra homomorphism. In other words, Corollary 15.16 holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that Corollary 15.16 holds for $n = N$. We must now prove that Corollary 15.16 also holds for $n = N + 1$.

Since Corollary 15.16 holds for $n = N$, we know that f^{*N} is a k-algebra homomorphism. Proposition 15.15 (applied to $g = f^{*N}$) now yields that $f * f^{*N}$ is a k-algebra homomorphism. Since $f * f^{*N} = f^{*(N+1)}$, this yields that $f^{*(N+1)}$ is a k-algebra homomorphism. In other words, Corollary 15.16 holds for $n = N + 1$. This completes the induction step. The induction proof of Corollary 15.16 is thus complete. □

Next, we dualize Lemma 12.3:

Lemma 15.17. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a k-algebra. Let $f \in \mathfrak{g}(H, A)$. Let $a \in H$ and $b \in H$. Then,

$$e^{*f}(ab) = \sum_{n \geq 0} \frac{1}{n!} f^{*n}(ab) \tag{91}$$

and

$$e^{*f}(a) \cdot e^{*f}(b) = \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} f^{*i}(a) f^{*(n-i)}(b) \right). \tag{92}$$

(In particular, the infinite sums $\sum_{n \geq 0} \frac{1}{n!} f^{*n}(ab)$ and $\sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} f^{*i}(a) f^{*(n-i)}(b) \right)$ converge with respect to the discrete topology, i. e., each of these sums has only finitely many nonzero addends.)

Proof of Lemma 15.17. The equalities (91) and (92) have been proven during our proof of Lemma 15.11, *without using the assumptions that A be commutative and f be an $(\varepsilon_H, \varepsilon_H)$-derivation*. Hence, these equalities are true. Lemma 15.17 is thus true. □

We can now prove Lemma 15.12:

Proof of Lemma 15.12. Assume that e^{*f} is a k-algebra homomorphism.

Fix some $(a, b) \in H \times H$. Thus, $a \in H$ and $b \in H$.

We want to prove that $f(ab) = f(a) \varepsilon_H(b) + \varepsilon_H(a) f(b)$.

Since H is filtered, there exists some $N \in \mathbb{N}$ such that $a \in H_{\leq N}$. Consider this N.

Since H is filtered, there exists some $M \in \mathbb{N}$ such that $b \in H_{\leq M}$. Consider this M.

Since H is filtered, there exists some $K \in \mathbb{N}$ such that $ab \in H_{\leq K}$. Consider this K.

We define a filtration $(k_{\leq \ell})_{\ell \geq 0}$ on the k-vector space k by

$$\left(k_{\leq \ell} = \begin{cases} 0, \text{ if } \ell \leq N + M + K; \\ k, \text{ if } \ell > N + M + K \end{cases} \qquad \text{for every } \ell \in \mathbb{N} \right).$$

For every $n \in \mathbb{N}$, define a k-linear map $h_n : k \to A$ by

$$h_n = \frac{1}{n!} f^{*n}(ab)\,\eta_A - \frac{1}{n!}\left(\sum_{i=0}^{n} \binom{n}{i} f^{*i}(a)\, f^{*(n-i)}(b)\right)\eta_A. \tag{93}$$

a) We now will prove that every $n \in \mathbb{N}$ satisfies $h_n(k_{\leq n-1}) = 0$.

Proof. Fix some $n \in \mathbb{N}$. We distinguish between two cases:

Case 1: We have $n \leq N + M + K + 1$.

Case 2: We have $n > N + M + K + 1$.

First let us consider Case 1. In this case, $n \leq N + M + K + 1$, so that $n - 1 \leq N + M + K$, and thus

$$\begin{aligned} k_{\leq n-1} &= \begin{cases} 0, \text{ if } n-1 \leq N+M+K; \\ k, \text{ if } n-1 > N+M+K \end{cases} \qquad \text{(by the definition of } k_{\leq n-1}) \\ &= 0 \qquad \text{(since } n-1 \leq N+M+K), \end{aligned}$$

so that $h_n(k_{\leq n-1}) = h_n(0) = 0$. Hence, $h_n(k_{\leq n-1}) = 0$ is proven in Case 1.

Now let us consider Case 2. In this case, $n > N+M+K+1 > K$. Thus, Remark 3.5 (applied to n and K instead of i and n) yields $f^{*n}(H_{\leq K}) = 0$. Since $ab \in H_{\leq K}$, this yields $f^{*n}(ab) = 0$. On the other hand,

$$\text{every } i \in \{0, 1, \ldots, N\} \text{ satisfies } f^{*(n-i)}(b) = 0. \tag{94}$$

[55]

Also,

$$\text{every } i \in \{N+1, N+2, \ldots, n\} \text{ satisfies } f^{*i}(a) = 0. \tag{95}$$

[56]

Keeping these facts in mind, we have

$$\begin{aligned} \sum_{i=0}^{n} \binom{n}{i} f^{*i}(a)\, f^{*(n-i)}(b) &= \sum_{i=0}^{N} \binom{n}{i} f^{*i}(a) \underbrace{f^{*(n-i)}(b)}_{\substack{=0 \\ \text{(by (94))}}} + \sum_{i=N+1}^{n} \binom{n}{i} \underbrace{f^{*i}(a)}_{\substack{=0 \\ \text{(by (95))}}} f^{*(n-i)}(b) \\ &= \underbrace{\sum_{i=0}^{N} \binom{n}{i} f^{*i}(a)\, 0}_{=0} + \underbrace{\sum_{i=N+1}^{n} \binom{n}{i} 0 f^{*(n-i)}(b)}_{=0} = 0 + 0 = 0. \end{aligned}$$

Now, by the definition of h_n, we have

$$h_n = \frac{1}{n!} \underbrace{f^{*n}(ab)}_{=0} \eta_A - \frac{1}{n!} \underbrace{\left(\sum_{i=0}^{n} \binom{n}{i} f^{*i}(a)\, f^{*(n-i)}(b)\right)}_{=0} \eta_A = \frac{1}{n!} 0 \eta_A - \frac{1}{n!} 0 \eta_A = 0$$

[55] *Proof.* Let $i \in \{0, 1, \ldots, N\}$. Then, $i \leq N$, so that $\underbrace{n}_{>N+M+K+1>N+M} - \underbrace{i}_{\leq N} > N + M - N = M$. Thus, Remark 3.5 (applied to $n - i$ and M instead of i and n) yields $f^{*(n-i)}(H_{\leq M}) = 0$. Since $b \in H_{\leq M}$, this yields $f^{*(n-i)}(b) = 0$, and thus (94) is proven.

[56] *Proof.* Let $i \in \{N+1, N+2, \ldots, n\}$. Then, $i > N$. Hence, Remark 3.5 (applied to N instead of n) yields $f^{*i}(H_{\leq N}) = 0$. Since $a \in H_{\leq N}$, this yields $f^{*i}(a) = 0$, and thus (95) is proven.

and thus $h_n(k_{\leq n-1}) = 0$. Hence, $h_n(k_{\leq n-1}) = 0$ is proven in Case 2.

Hence, in both possible cases, we have shown that $h_n(k_{\leq n-1}) = 0$. This proves that $h_n(k_{\leq n-1}) = 0$ always holds. In other words, part **a)** is proven.

b) Now, we will show that every $x \in k$ and every $t \in \mathbb{N}$ satisfy $\sum_{i \geq 0} t^i h_i(x) = 0$. [57]

Proof. Let $x \in k$ and $t \in \mathbb{N}$ be arbitrary. By Corollary 15.16 (applied to t and e^{*f} instead of n and f), we see that $\left(e^{*f}\right)^{*t}$ is a k-algebra homomorphism. Since $e^{*(tf)} = \left(e^{*f}\right)^{*t}$ (by Corollary 11.4, applied to H, A and t instead of C, H and n), this rewrites as follows: The map $e^{*(tf)}$ is a k-algebra homomorphism. Thus,

$$e^{*(tf)}(ab) = e^{*(tf)}(a) \cdot e^{*(tf)}(b). \tag{96}$$

But applying Lemma 15.17 to tf instead of f (this is allowed since $f \in \mathfrak{g}(H, A)$ yields $tf \in \mathfrak{g}(H, A)$), we obtain

$$e^{*(tf)}(ab) = \sum_{n \geq 0} \frac{1}{n!} (tf)^{*n}(ab) \tag{97}$$

and

$$e^{*(tf)}(a) \cdot e^{*(tf)}(b) = \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} (tf)^{*i}(a) (tf)^{*(n-i)}(b) \right). \tag{98}$$

We are now going to rewrite these two equalities by taking t out of the brackets.

Since

$$\sum_{n \geq 0} \frac{1}{n!} \underbrace{(tf)^{*n}}_{=t^n f^{*n}}(ab) = \sum_{n \geq 0} \frac{1}{n!} \underbrace{\left(t^n f^{*n}\right)(ab)}_{=t^n f^{*n}(ab)} = \sum_{n \geq 0} \frac{1}{n!} t^n f^{*n}(ab) = \sum_{n \geq 0} t^n \frac{1}{n!} f^{*n}(ab),$$

the equality (96) rewrites as

$$e^{*(tf)}(ab) = \sum_{n \geq 0} t^n \frac{1}{n!} f^{*n}(ab). \tag{99}$$

Since

$$\begin{aligned}
&\sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \underbrace{(tf)^{*i}}_{=t^i f^{*i}}(a) \underbrace{(tf)^{*(n-i)}}_{=t^{n-i} f^{*(n-i)}}(b) \right) \\
&= \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \underbrace{\left(t^i f^{*i}\right)(a)}_{=t^i f^{*i}(a)} \underbrace{\left(t^{n-i} f^{*(n-i)}\right)(b)}_{=t^{n-i} f^{*(n-i)}(b)} \right) = \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \underbrace{t^i f^{*i}(a)\, t^{n-i} f^{*(n-i)}(b)}_{=t^i t^{n-i} f^{*i}(a) f^{*(n-i)}(b)} \right) \\
&= \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} \underbrace{t^i t^{n-i}}_{=t^n} f^{*i}(a)\, f^{*(n-i)}(b) \right) = \sum_{n \geq 0} \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} t^n f^{*i}(a)\, f^{*(n-i)}(b) \right) \\
&= \sum_{n \geq 0} t^n \frac{1}{n!} \left(\sum_{i=0}^{n} \binom{n}{i} f^{*i}(a)\, f^{*(n-i)}(b) \right),
\end{aligned}$$

[57] Note that the element $\sum_{i \geq 0} t^i h_i(x)$ is well-defined due to Proposition 12.1 **(a)** (applied to $V = k$ and $W = A$), but in our case even the element $\sum_{i \geq 0} t^i h_i$ itself is well-defined (we can see that, for instance, by following the proof of **b)**).

the equality (98) rewrites as

$$e^{*(tf)}(a)\cdot e^{*(tf)}(b)=\sum_{n\geq 0}t^n\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}f^{*i}(a)\,f^{*(n-i)}(b)\right). \tag{100}$$

Now,

$$\begin{aligned}
\sum_{i\geq 0}t^i h_i &= \sum_{n\geq 0}t^n h_n \qquad \text{(here, we renamed the index } i \text{ as } n \text{ in the sum)}\\
&= \sum_{n\geq 0}t^n\left(\frac{1}{n!}f^{*n}(ab)\,\eta_A-\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}f^{*i}(a)\,f^{*(n-i)}(b)\right)\eta_A\right) \qquad \text{(by (93))}\\
&= \underbrace{\sum_{n\geq 0}t^n\frac{1}{n!}f^{*n}(ab)\,\eta_A}_{=\left(\sum_{n\geq 0}t^n\frac{1}{n!}f^{*n}(ab)\right)\eta_A}-\underbrace{\sum_{n\geq 0}t^n\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}f^{*i}(a)\,f^{*(n-i)}(b)\right)\eta_A}_{=\left(\sum_{n\geq 0}t^n\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}f^{*i}(a)f^{*(n-i)}(b)\right)\right)\eta_A}\\
&= \underbrace{\left(\sum_{n\geq 0}t^n\frac{1}{n!}f^{*n}(ab)\right)}_{\substack{=e^{*(tf)}(ab)\\ \text{(by (99))}}}\eta_A-\underbrace{\left(\sum_{n\geq 0}t^n\frac{1}{n!}\left(\sum_{i=0}^{n}\binom{n}{i}f^{*i}(a)\,f^{*(n-i)}(b)\right)\right)}_{\substack{=e^{*(tf)}(a)\cdot e^{*(tf)}(b)\\ \text{(by (100))}}}\eta_A\\
&= \underbrace{e^{*(tf)}(ab)}_{\substack{=e^{*(tf)}(a)\cdot e^{*(tf)}(b)\\ \text{(by (96))}}}\eta_A-e^{*(tf)}(a)\cdot e^{*(tf)}(b)\,\eta_A\\
&= e^{*(tf)}(a)\cdot e^{*(tf)}(b)\,\eta_A-e^{*(tf)}(a)\cdot e^{*(tf)}(b)\,\eta_A=0,
\end{aligned}$$

so that

$$\sum_{i\geq 0}t^i h_i(x)=\underbrace{\left(\sum_{i\geq 0}t^i h_i\right)}_{=0}(x)=0(x)=0.$$

We thus have proven that every $x\in k$ and every $t\in\mathbb{N}$ satisfy $\sum_{i\geq 0}t^i h_i(x)=0$. In other words, part **b)** of the proof is done.

c) We know that every $n\in\mathbb{N}$ satisfies $h_n(k_{\leq n-1})=0$ (by part **a)**), and that every $x\in k$ and every $t\in\mathbb{N}$ satisfy $\sum_{i\geq 0}t^i h_i(x)=0$ (by part **b)**). Hence, Proposition 12.1 **(b)** (applied to k and A instead of V and W) yields that $h_n=0$ for every $n\in\mathbb{N}$. Applied

to $n=1$, this yields $h_1 = 0$. But (93) (applied to $n=1$) yields

$$h_1 = \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1} \underbrace{f^{*1}}_{=f}(ab)\,\eta_A - \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1} \underbrace{\left(\sum_{i=0}^{1}\binom{1}{i} f^{*i}(a)\, f^{*(1-i)}(b)\right)}_{=\binom{1}{0} f^{*0}(a) f^{*(1-0)}(b) + \binom{1}{1} f^{*1}(a) f^{*(1-1)}(b)} \eta_A$$

$$= f(ab)\,\eta_A - \left(\underbrace{\binom{1}{0}}_{=1} \underbrace{f^{*0}}_{=e_{H,A}}(a)\,\underbrace{f^{*(1-0)}}_{=f^{*1}=f}(b) + \underbrace{\binom{1}{1}}_{=1}\underbrace{f^{*1}}_{=f}(a)\,\underbrace{f^{*(1-1)}}_{=e_{H,A}}(b)\right)\eta_A$$

$$= f(ab)\,\eta_A - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right)\eta_A = \left(f(ab) - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right)\right)\eta_A.$$

Since $h_1 = 0$, this rewrites as

$$0 = \left(f(ab) - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right)\right)\eta_A.$$

Hence,

$$\begin{aligned} 0(1) &= \left(\left(f(ab) - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right)\right)\eta_A\right)(1) \\ &= \left(f(ab) - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right)\right) \underbrace{\left(\eta_A(1)\right)}_{\substack{=1\cdot 1_A \\ \text{(by the definition of the map } \eta_A\text{)}}} \\ &= \left(f(ab) - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right)\right) 1 \cdot 1_A \\ &= f(ab) - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right). \end{aligned}$$

So we have

$$0 = 0(1) = f(ab) - \left(e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b)\right),$$

thus

$$f(ab) = e_{H,A}(a)\, f(b) + f(a)\, e_{H,A}(b).$$

Since

$$\underbrace{e_{H,A}}_{=\eta_A\circ\varepsilon_H}(a) = \left(\eta_A \circ \varepsilon_H\right)(a) = \eta_A\left(\varepsilon_H(a)\right) = \varepsilon_H(a)\cdot 1_A \qquad \text{(by the definition of } \eta_A\text{)}$$

and

$$e_{H,A}(b) = \varepsilon_H(b)\cdot 1_A \qquad \text{(for similar reasons)},$$

this becomes

$$\begin{aligned} f(ab) &= \underbrace{e_{H,A}(a)}_{=\varepsilon_H(a)\cdot 1_A} f(b) + f(a) \underbrace{e_{H,A}(b)}_{=\varepsilon_H(b)\cdot 1_A} = \varepsilon_H(a)\cdot 1_A f(b) + f(a)\,\varepsilon_H(b)\cdot 1_A \\ &= \varepsilon_H(a)\, f(b) + f(a)\,\varepsilon_H(b) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\, f(b). \end{aligned}$$

d) Now forget that we fixed (a,b). What we have shown is that every $(a,b) \in H \times H$ satisfies $f(ab) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\, f(b)$. According to Definition 15.7, this means that f is an $(\varepsilon_H, \varepsilon_H)$-derivation.

We have thus proven that, under the assumption that e^{*f} is a k-algebra homomorphism, the map f is an $(\varepsilon_H, \varepsilon_H)$-derivation. Thus, Lemma 15.12 is proven. □

Proof of Theorem 15.10. The assertion of Theorem 15.10 is an "if and only if" assertion. Its "if" part was proven in Lemma 15.12, and its "only if" part was proven in Lemma 15.11. Hence, both parts of the assertion of Theorem 15.10 are proven. This finally completes the proof of Theorem 15.10. □

Now we can finally deal with Theorem 15.3:

Proof of Theorem 15.3. Recall that $\mathrm{id} \in G(H,H)$. Thus, $\operatorname{Log}\mathrm{id} \in \mathfrak{g}(H,H)$ (because $\operatorname{Log} F \in \mathfrak{g}(H,H)$ for every $F \in G(H,H)$).

Let f be the map $\operatorname{Log}\mathrm{id} \in \mathcal{L}(H,H)$. Then, $f = \operatorname{Log}\mathrm{id} \in \mathfrak{g}(H,H)$. Besides, $f = \operatorname{Log}\mathrm{id}$ yields $e^{*f} = e^{*(\operatorname{Log}\mathrm{id})} = \mathrm{id}$ (by Proposition 5.13 **(b)**, applied to $F = \mathrm{id}$ and $A = H$). Hence, e^{*f} is a k-algebra homomorphism (since id is a k-algebra homomorphism). By Lemma 15.12 (applied to $A = H$), this yields that f is an $(\varepsilon_H, \varepsilon_H)$-derivation.

Since H is a bialgebra, ε_H is a k-algebra homomorphism (by the axioms of a bialgebra). Hence, we can apply Theorem 15.9 and Proposition 15.4 to $A = H$.

Theorem 15.9 (applied to $A = H$) tells us that f is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $f\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$. Hence, $f\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$ (since we know that f is an $(\varepsilon_H, \varepsilon_H)$-derivation).

We have $\varepsilon_H \circ \mathrm{id} = \varepsilon_H$. Thus, Proposition 15.4 **(c)** (applied to $F = \mathrm{id}$ and $A = H$) yields $(\operatorname{Log}\mathrm{id} - \mathrm{id})(H) \subseteq \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$. Since $\operatorname{Log}\mathrm{id} = f$, this rewrites as $(f - \mathrm{id})(H) \subseteq \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$. Now,

$$\underbrace{\left(f^2 - f\right)}_{=f\circ(f-\mathrm{id})}(H) = (f \circ (f - \mathrm{id}))(H) = f\left(\underbrace{(f - \mathrm{id})(H)}_{\subseteq(\operatorname{Ker}(\varepsilon_H))^2 + k\cdot 1_H}\right) \subseteq f\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0,$$

so that $\left(f^2 - f\right)(H) = 0$. Thus, $f^2 - f = 0$, so that $f^2 = f$. In other words, f is a projection. Since $f = \operatorname{Log}\mathrm{id}$, this rewrites as follows: The map $\operatorname{Log}\mathrm{id}$ is a projection.

Also, $f\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$ yields $\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H \subseteq \operatorname{Ker} f$. On the other hand, $\operatorname{Ker} f \subseteq (f - \mathrm{id})(H)$ [58] combined with $(f - \mathrm{id})(H) \subseteq \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$ yields $\operatorname{Ker} f \subseteq \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$. Combined with $\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H \subseteq \operatorname{Ker} f$, this results in $\operatorname{Ker} f = \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$. Since $f = \operatorname{Log}\mathrm{id}$, this rewrites as $\operatorname{Ker}(\operatorname{Log}\mathrm{id}) = \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$.

This completes the proof of Theorem 15.3. □

§16. Consequences for graded bialgebras

We have hitherto been considering filtered bialgebras (and general bialgebras), but not graded bialgebras. The reason for this is that we had no reason for considering graded bialgebras: As long as the same statement holds for graded and for filtered bialgebras,

[58] *Proof.* Let $x \in \operatorname{Ker} f$ be arbitrary. Then, $f(x) = 0$, so that $(f - \mathrm{id})(x) = \underbrace{f(x)}_{=0} - \underbrace{\mathrm{id}(x)}_{=x} = -x$. Thus, $x = -(f - \mathrm{id})(x) = (f - \mathrm{id})(-x)$ (since $f - \mathrm{id}$ is linear). Hence, $x \in (f - \mathrm{id})(H)$ (since $-x \in H$).

We have thus shown that every $x \in \operatorname{Ker} f$ satisfies $x \in (f - \mathrm{id})(H)$. In other words, $\operatorname{Ker} f \subseteq (f - \mathrm{id})(H)$, qed.

it is clearly enough to prove it for filtered ones only, since graded bialgebras can always be seen as filtered bialgebras (by Proposition 16.8 below), but not the other way round. In this section §16, we are going to formulate the relation between graded and filtered bialgebras, and show some additional properties special to graded bialgebras.

Convention 16.1. In the following, whenever V is a graded vector space[59], we will denote the grading on V by $(V_\ell)_{\ell \geq 0}$. (This is a general convention, so it does not only pertain to graded vector spaces called V, but pertains to any graded vector space. For instance, if we have a graded vector space called C, then this convention yields that the grading on C is denoted by $(C_\ell)_{\ell \geq 0}$.)

Proposition 16.2. Let k be a field. Let V be a graded vector space. For every $n \in \mathbb{N}$, define a k-vector subspace $V_{\leq n}$ of V by $V_{\leq n} = \bigoplus_{\ell=0}^{n} V_\ell$ [60]. Then, $\left(V, (V_{\leq n})_{n \geq 0}\right)$ is a filtered k-vector space.

Convention 16.3. Let k be a field. Let V be a graded vector space. Then, whenever we speak of "the filtered k-vector space V", we are going to mean the filtered k-vector space $\left(V, (V_{\leq n})_{n \geq 0}\right)$ defined in Proposition 16.2. In particular, whenever we mention some $V_{\leq n}$ (for some $n \in \mathbb{N}$), we are going to mean the $V_{\leq n}$ defined in Proposition 16.2.

Proof of Proposition 16.2. **a)** We have $V_{\leq n} \subseteq V_{\leq n+1}$ for every $n \in \mathbb{N}$.

Proof. Let $n \in \mathbb{N}$. By the definition of $V_{\leq n}$, we have $V_{\leq n} = \bigoplus_{\ell=0}^{n} V_\ell$. By the definition of $V_{\leq n+1}$, we have

$$V_{\leq n+1} = \bigoplus_{\ell=0}^{n+1} V_\ell = \underbrace{\bigoplus_{\ell=0}^{n} V_\ell}_{=V_{\leq n}} \oplus V_{n+1} = V_{\leq n} \oplus V_{n+1} \supseteq V_{\leq n},$$

so that $V_{\leq n} \subseteq V_{\leq n+1}$. This proves **a)**.

b) We have

$$V_{\leq a} \subseteq V_{\leq b} \text{ for every } a \in \mathbb{N} \text{ and } b \in \mathbb{N} \text{ satisfying } a \leq b. \tag{101}$$

Proof. From part **a)**, we see that the sequence $(V_{\leq n})_{n \geq 0}$ of k-vector subspaces of V is monotonically increasing with respect to inclusion. This yields (101). Thus, **b)** is proven.

[59] Note that a *graded vector space* is defined as a vector space V along with a family $(V_\ell)_{\ell \geq 0}$ of subspaces of V such that $V = \bigoplus_{\ell \in \mathbb{N}} V_\ell$. There are some more general definitions of the word "graded" in literature, but we need this one. (In particular, if you are used to the notion of a "G-graded vector space" where G is a monoid, then you should notice that our notion of "graded vector space" means an $\mathbb{N}$-graded vector space.)

[60] This is well-defined, because the sum $\sum_{\ell=0}^{n} V_\ell$ is a direct sum (in fact, since V is a graded vector space, we have $V = \bigoplus_{\ell \in \mathbb{N}} V_\ell$; now, the sum $\sum_{\ell=0}^{n} V_\ell$ is a partial sum of the direct sum $\bigoplus_{\ell \in \mathbb{N}} V_\ell$, and thus a direct sum itself).

c) We have $V = \bigcup\limits_{n \in \mathbb{N}} V_{\leq n}$.

Proof. Let $v \in V$. Then, $v \in V = \bigoplus\limits_{\ell \in \mathbb{N}} V_\ell$ (since V is a graded vector space), so there exists some family $(a_\ell)_{\ell \geq 0} \in \prod\limits_{\ell \in \mathbb{N}} V_\ell$ such that (all but finitely many $\ell \in \mathbb{N}$ satisfy $a_\ell = 0$) and $v = \sum\limits_{\ell \in \mathbb{N}} a_\ell$. Consider this family $(a_\ell)_{\ell \geq 0}$.

Notice that $a_\ell \in V_\ell$ for each $\ell \in \mathbb{N}$ (since $(a_\ell)_{\ell \geq 0} \in \prod\limits_{\ell \in \mathbb{N}} V_\ell$).

There exists a finite subset S of $\mathbb{N}$ such that

$$(\text{all } \ell \in \mathbb{N} \setminus S \text{ satisfy } a_\ell = 0) \tag{102}$$

(because all but finitely many $\ell \in \mathbb{N}$ satisfy $a_\ell = 0$). Consider this S. Then, S is a finite set, and thus has a supremum in $\mathbb{N}$ (this supremum is actually a maximum unless $S = \varnothing$). Let N be this supremum. Then, every $m \in S$ satisfies

$$a_m \in V_{\leq N} \tag{103}$$

[61]. Now we have

$$\begin{aligned} v &= \sum_{\ell \in \mathbb{N}} a_\ell = \sum_{\ell \in S} \underbrace{a_\ell}_{\substack{\in V_{\leq N} \\ \text{(by (103) (applied to } m=\ell))}} + \sum_{\ell \in \mathbb{N} \setminus S} \underbrace{a_\ell}_{\substack{=0 \\ \text{(by (102))}}} \\ &\in \sum_{\ell \in S} V_{\leq N} + \underbrace{\sum_{\ell \in \mathbb{N} \setminus S} 0}_{=0} = \sum_{\ell \in S} V_{\leq N} \subseteq V_{\leq N} \qquad \text{(since } V_{\leq N} \text{ is a } k\text{-vector subspace)} \\ &\subseteq \bigcup_{n \in \mathbb{N}} V_{\leq n} \qquad \left(\text{since } V_{\leq N} \text{ is a term of the union } \bigcup_{n \in \mathbb{N}} V_{\leq n} \right). \end{aligned}$$

Now forget that we fixed v. We have thus shown that for every $v \in V$, we have $v \in \bigcup\limits_{n \in \mathbb{N}} V_{\leq n}$. In other words, $V \subseteq \bigcup\limits_{n \in \mathbb{N}} V_{\leq n}$. Combined with the triviality $\bigcup\limits_{n \in \mathbb{N}} V_{\leq n} \subseteq V$, this yields $V = \bigcup\limits_{n \in \mathbb{N}} V_{\leq n}$. This proves **c)**.

d) Combining the statements of parts **a)** and **c)**, we conclude that $\left(V, (V_{\leq n})_{n \geq 0}\right)$ is a filtered k-vector space. This proves Proposition 16.2. ☐

Proposition 16.4. Let k be a field. Let A be a graded k-algebra. Then, $\left(A, (A_{\leq n})_{n \geq 0}\right)$ is a filtered k-algebra.[62]

[61] *Proof of (103):* Let $m \in S$. Recall that N is the supremum of the set S in $\mathbb{N}$. Hence, $N \geq s$ for each $s \in S$. Applying this to $s = m$, we obtain $N \geq m$. Thus, $m \leq N$. Hence, $m \in \{0, 1, \ldots, N\}$.

The definition of $V_{\leq N}$ yields $V_{\leq N} = \bigoplus\limits_{\ell=0}^{N} V_\ell$. But V_m is an addend of the direct sum $\bigoplus\limits_{\ell=0}^{N} V_\ell$ (since $m \in \{0, 1, \ldots, N\}$). Hence, $V_m \subseteq \bigoplus\limits_{\ell=0}^{N} V_\ell$. But recall that $a_\ell \in V_\ell$ for each $\ell \in \mathbb{N}$. Applying this to $\ell = m$, we obtain $a_m \in V_m \subseteq \bigoplus\limits_{\ell=0}^{N} V_\ell = V_{\leq N}$. This proves (103).

[62] Of course, the notation $A_{\leq n}$ has to be understood here as according to Convention 16.3; that is, $A_{\leq n}$ is defined by $A_{\leq n} = \bigoplus\limits_{\ell=0}^{n} A_\ell$.

Convention 16.5. Let k be a field. Let A be a graded k-algebra. Then, whenever we speak of "the filtered k-algebra A", we are going to mean the filtered k-algebra $\left(A, \left(A_{\leq n}\right)_{n \geq 0}\right)$ defined in Proposition 16.4.

Proof of Proposition 16.4. **a)** By Proposition 16.2 (applied to $V = A$), we know that $\left(A, \left(A_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-vector space.

b) We have $1 \in A_{\leq 0}$.

Proof. By the definition of $A_{\leq 0}$, we have $A_{\leq 0} = \bigoplus_{\ell=0}^{0} A_\ell = A_0$. Since A is a graded k-algebra, we have $1 \in A_0 = A_{\leq 0}$. This proves **b)**.

c) We have

$$A_u \subseteq A_{\leq v} \qquad \text{for any } u \in \mathbb{N} \text{ and } v \in \mathbb{N} \text{ satisfying } u \leq v. \tag{104}$$

Proof. Let $u \in \mathbb{N}$ and $v \in \mathbb{N}$ satisfy $u \leq v$. Then, the definition of $A_{\leq v}$ says that $A_{\leq v} = \bigoplus_{\ell=0}^{v} A_\ell$. Since A_u is a summand in the direct sum $\bigoplus_{\ell=0}^{v} A_\ell$ (because $u \in \mathbb{N}$ and $u \leq v$), this yields $A_{\leq v} \supseteq A_u$, so that $A_u \subseteq A_{\leq v}$. This proves **c)**.

d) We have $A_{\leq i} A_{\leq j} \subseteq A_{\leq i+j}$ for every $i \in \mathbb{N}$ and $j \in \mathbb{N}$.

Proof. Since A is a graded k-algebra, we have

$$A_\ell A_m \subseteq A_{\ell+m} \qquad \text{for any } \ell \in \mathbb{N} \text{ and } m \in \mathbb{N}. \tag{105}$$

Now, let $i \in \mathbb{N}$ and $j \in \mathbb{N}$ be arbitrary. Then, by the definition of $A_{\leq i}$, we have $A_{\leq i} = \bigoplus_{\ell=0}^{i} A_\ell = \sum_{\ell=0}^{i} A_\ell$ (since direct sums are sums). Also, by the definition of $A_{\leq j}$, we have

$$\begin{aligned} A_{\leq j} &= \bigoplus_{\ell=0}^{j} A_\ell = \bigoplus_{m=0}^{j} A_m \qquad \text{(here, we renamed the index } \ell \text{ as } m\text{)} \\ &= \sum_{m=0}^{j} A_m \qquad \text{(since direct sums are sums)}. \end{aligned}$$

Thus,

$$\underbrace{A_{\leq i}}_{= \sum_{\ell=0}^{i} A_\ell} \underbrace{A_{\leq j}}_{= \sum_{m=0}^{j} A_m} = \left(\sum_{\ell=0}^{i} A_\ell\right)\left(\sum_{m=0}^{j} A_m\right) = \sum_{\ell=0}^{i}\sum_{m=0}^{j} \underbrace{A_\ell A_m}_{\substack{\subseteq A_{\ell+m} \\ \text{(by (105))}}} \subseteq \sum_{\ell=0}^{i}\sum_{m=0}^{j} A_{\ell+m}.$$

Since every $\ell \in \{0, 1, \ldots, i\}$ and $m \in \{0, 1, \ldots, j\}$ satisfy $A_{\ell+m} \subseteq A_{\leq i+j}$ [63], this becomes

$$A_{\leq i} A_{\leq j} \subseteq \sum_{\ell=0}^{i}\sum_{m=0}^{j} \underbrace{A_{\ell+m}}_{\subseteq A_{\leq i+j}} \subseteq \sum_{\ell=0}^{i}\sum_{m=0}^{j} A_{\leq i+j} \subseteq A_{\leq i+j} \qquad \text{(since } A_{\leq i+j} \text{ is a } k\text{-vector space)}.$$

[63] *Proof.* Let $\ell \in \{0, 1, \ldots, i\}$ and $m \in \{0, 1, \ldots, j\}$ be arbitrary. Then, $0 \leq \ell \leq i$ and $0 \leq m \leq j$. Hence, $0 \leq \ell + m \leq i + j$, so that $A_{\ell+m} \subseteq A_{\leq i+j}$ (by (104), applied to $u = \ell + m$ and $v = i + j$),

This proves **d)**.

e) By combining the results of parts **b)** and **d)**, we see that $\left(A, \left(A_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-algebra. This proves Proposition 16.4. $\square$

Proposition 16.6. Let k be a field. Let C be a graded k-coalgebra. Then, $\left(C, \left(C_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-coalgebra.[64]

Convention 16.7. Let k be a field. Let C be a graded k-coalgebra. Then, whenever we speak of "the filtered k-coalgebra C", we are going to mean the filtered k-coalgebra $\left(C, \left(C_{\leq n}\right)_{n \geq 0}\right)$ defined in Proposition 16.6.

Proof of Proposition 16.6. **a)** By Proposition 16.2 (applied to $V = C$), we know that $\left(C, \left(C_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-vector space.

Since C is a graded k-coalgebra, we have

$$\Delta_C\left(C_\ell\right) \subseteq \bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=\ell}} C_i \otimes C_j \qquad \text{for every } \ell \in \mathbb{N}. \tag{106}$$

Here, the sum $\bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=\ell}} C_i \otimes C_j$ is considered as a partial sum of the infinite direct sum

$$\bigoplus_{(i,j) \in \mathbb{N}^{\times 2}} C_i \otimes C_j = \underbrace{\left(\bigoplus_{i \in \mathbb{N}} C_i\right)}_{=C} \otimes \underbrace{\left(\bigoplus_{j \in \mathbb{N}} C_j\right)}_{=C} = C \otimes C.$$

We can rewrite the right hand side of (106). In fact, for every $\ell \in \mathbb{N}$, the map $\{0, 1, \ldots, \ell\} \to \{(i,j) \in \mathbb{N}^{\times 2} \mid i + j = \ell\}$ which sends every $i \in \{0, 1, \ldots, \ell\}$ to $(i, \ell - i)$ is a bijection (according to elementary combinatorics). Hence, for every $\ell \in \mathbb{N}$, we have

$$\begin{aligned} \bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=\ell}} C_i \otimes C_j &= \underbrace{\bigoplus_{i \in \{0,1,\ldots,\ell\}}}_{=\bigoplus_{i=0}^{\ell}} C_i \otimes C_{\ell - i} \\ &\qquad \left(\begin{array}{c} \text{here, we substituted } (i, \ell - i) \text{ for } (i,j) \text{ in the direct sum,} \\ \text{because the map } \{0, 1, \ldots, \ell\} \to \{(i,j) \in \mathbb{N}^{\times 2} \mid i + j = \ell\} \\ \text{which sends every } i \in \{0, 1, \ldots, \ell\} \text{ to } (i, \ell - i) \text{ is a bijection} \end{array} \right) \\ &= \bigoplus_{i=0}^{\ell} C_i \otimes C_{\ell - i}. \end{aligned}$$

Now, (106) becomes

$$\Delta_C\left(C_\ell\right) \subseteq \bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=\ell}} C_i \otimes C_j = \bigoplus_{i=0}^{\ell} C_i \otimes C_{\ell - i} = \sum_{i=0}^{\ell} C_i \otimes C_{\ell - i} \tag{107}$$

[64] Of course, the notation $C_{\leq n}$ has to be understood here as according to Convention 16.3; that is, $C_{\leq n}$ is defined by $C_{\leq n} = \bigoplus_{\ell=0}^{n} C_\ell$.

(since direct sums are sums) for every $\ell \in \mathbb{N}$.

b) We have

$$C_u \subseteq C_{\leq v} \text{ for any } u \in \mathbb{N} \text{ and } v \in \mathbb{N} \text{ satisfying } u \leq v. \tag{108}$$

Proof. Let $u \in \mathbb{N}$ and $v \in \mathbb{N}$ satisfy $u \leq v$. Then, the definition of $C_{\leq v}$ says that $C_{\leq v} = \bigoplus_{\ell=0}^{v} C_\ell$. Since C_u is a summand in the direct sum $\bigoplus_{\ell=0}^{v} C_\ell$ (because $u \in \mathbb{N}$ and $u \leq v$), this yields that C_u is a direct addend of $\bigoplus_{\ell=0}^{v} C_\ell = C_{\leq v}$. Thus, $C_u \subseteq C_{\leq v}$. This proves **b)**.

c) For every $n \in \mathbb{N}$, we have

$$\Delta_C\left(C_{\leq n}\right) \subseteq \sum_{u=0}^{n} C_{\leq u} \otimes C_{\leq n-u}.$$

Proof. Let $n \in \mathbb{N}$. Then, $C_{\leq n} = \bigoplus_{\ell=0}^{n} C_\ell = \sum_{\ell=0}^{n} C_\ell$ (since direct sums are sums), so that

$$\begin{aligned}
\Delta_C\left(C_{\leq n}\right) &= \Delta_C\left(\sum_{\ell=0}^{n} C_\ell\right) = \sum_{\ell=0}^{n} \underbrace{\Delta_C\left(C_\ell\right)}_{\substack{\subseteq \sum_{i=0}^{\ell} C_i \otimes C_{\ell-i} \\ \text{(by (107))}}} \qquad \text{(since } \Delta_C \text{ is } k\text{-linear)} \\
&= \sum_{\ell=0}^{n} \sum_{i=0}^{\ell} \underbrace{C_i}_{\substack{\subseteq C_{\leq i} \\ \text{(by (108) (applied to} \\ u=i \text{ and } v=i\text{), since } i \leq i)}} \otimes \underbrace{C_{\ell-i}}_{\substack{\subseteq C_{\leq n-i} \\ \text{(by (108) (applied to } u=\ell-i \text{ and } v=n-i\text{),} \\ \text{since } \ell-i \leq n-i \text{ (because } \ell \leq n\text{))}}} \\
&\subseteq \sum_{\ell=0}^{n} \underbrace{\sum_{i=0}^{\ell} C_{\leq i} \otimes C_{\leq n-i}}_{\substack{\subseteq \sum_{i=0}^{n} C_{\leq i} \otimes C_{\leq n-i} \\ \text{(because } \ell \leq n\text{, and thus the sum } \sum_{i=0}^{\ell} C_{\leq i} \otimes C_{\leq n-i} \\ \text{is a partial sum of the sum } \sum_{i=0}^{n} C_{\leq i} \otimes C_{\leq n-i}\text{)}}} \subseteq \sum_{\ell=0}^{n} \sum_{i=0}^{n} C_{\leq i} \otimes C_{\leq n-i} \\
&\subseteq \sum_{i=0}^{n} C_{\leq i} \otimes C_{\leq n-i} \\
&\qquad \left(\text{since } \sum_{i=0}^{n} C_{\leq i} \otimes C_{\leq n-i} \text{ is a } k\text{-vector space}\right) \\
&= \sum_{u=0}^{n} C_{\leq u} \otimes C_{\leq n-u} \qquad \text{(here, we renamed } i \text{ as } u \text{ in the sum)}.
\end{aligned}$$

This proves **c)**.

d) From part **c)**, we immediately see that $\left(C, \left(C_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-coalgebra. This proves Proposition 16.6. $\square$

Proposition 16.8. Let k be a field. Let H be a graded k-bialgebra. Then, $\left(H, \left(H_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-bialgebra.[65]

Convention 16.9. Let k be a field. Let H be a graded k-bialgebra. Then, whenever we speak of "the filtered k-bialgebra H", we are going to mean the filtered k-bialgebra $\left(H, \left(H_{\leq n}\right)_{n \geq 0}\right)$ defined in Proposition 16.8.

Proof of Proposition 16.8. Since $\left(H, \left(H_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-algebra (by Proposition 16.4, applied to $A = H$) and a filtered k-coalgebra (by Proposition 16.6, applied to $C = H$), we see that $\left(H, \left(H_{\leq n}\right)_{n \geq 0}\right)$ is a filtered k-bialgebra. This proves Proposition 16.8. □

Next we define the notion of a connected graded k-coalgebra:

Definition 16.10. Let k be a field. Let C be a graded k-coalgebra. We say that the graded k-coalgebra C is *connected* if and only if the map $\varepsilon_C \mid_{C_0} : C_0 \to k$ is a k-vector space isomorphism.

Note that such a definition of a connected graded k-coalgebra might bring us into trouble: In fact, if C is a filtered k-coalgebra, then when we just say that "C is connected" it is not immediately clear whether we mean that the *graded* k-coalgebra C is connected, or whether we mean that the *filtered* k-coalgebra C (defined in Convention 16.7) is connected. Fortunately, these two meanings are the same, because we have the following fact:

Remark 16.11. Let k be a field. Let C be a graded k-coalgebra. The graded k-coalgebra C is connected if and only if the filtered k-coalgebra C (defined in Convention 16.7) is connected.

Proof of Remark 16.11. Consider the filtered k-coalgebra C (defined in Convention 16.7). Then, by the definition of $C_{\leq 0}$, we have $C_{\leq 0} = \bigoplus_{\ell=0}^{0} C_\ell = C_0$. Now, by Definition 16.10, we have the following equivalence of assertions:

$$\begin{aligned}
&\text{(the graded } k\text{-coalgebra } C \text{ is connected)} \\
&\iff \text{(the map } \varepsilon_C \mid_{C_0} : C_0 \to k \text{ is a } k\text{-vector space isomorphism)} \\
&\iff \left(\text{the map } \varepsilon_C \mid_{C_{\leq 0}} : C_{\leq 0} \to k \text{ is a } k\text{-vector space isomorphism}\right) \\
&\qquad \text{(since } C_0 = C_{\leq 0}\text{)} \\
&\iff \text{(the filtered } k\text{-coalgebra } C \text{ is connected)} \qquad \text{(by Definition 1.16)}.
\end{aligned}$$

This proves Remark 16.11. □

Remark 16.11 was a triviality to prove, but it shows us an important thing: It shows us that all properties of connected filtered bialgebras that we showed above automatically yield properties of connected graded bialgebras. Since connected graded

[65] Of course, the notation $H_{\leq n}$ has to be understood here as according to Convention 16.3; that is, $H_{\leq n}$ is defined by $H_{\leq n} = \bigoplus_{\ell=0}^{n} H_\ell$.

bialgebras have more structure than connected filtered bialgebras, we can expect connected graded bialgebras to also have some additional properties that don't hold (or don't even make sense) for connected filtered bialgebras. This Section §16 is devoted to some such properties.

Here is a simple consequence of Definition 16.10:

Remark 16.12. Let k be a field. Let C be a graded k-coalgebra. Let $\lambda \in C_0$ be such that $C_0 = k \cdot \lambda$ and $\varepsilon_C(\lambda) = 1$. Then, the graded k-coalgebra C is connected.

Proof of Remark 16.12. Since the map ε_C is k-linear, we have $\varepsilon_C(k \cdot \lambda) = k \cdot \underbrace{\varepsilon_C(\lambda)}_{=1} = k \cdot 1 = k$. Now,

$$(\varepsilon_C|_{C_0})(C_0) = \varepsilon_C\left(\underbrace{C_0}_{=k\cdot\lambda}\right) = \varepsilon_C(k \cdot \lambda) = k.$$

In other words, the map $\varepsilon_C|_{C_0}: C_0 \to k$ is surjective.

Let $x \in \operatorname{Ker}(\varepsilon_C|_{C_0})$. Then, $x \in C_0$ satisfies $(\varepsilon_C|_{C_0})(x) = 0$. Since $x \in C_0 = k \cdot \lambda$, there exists a $\tau \in k$ such that $x = \tau\lambda$. Consider this τ. Since

$$0 = (\varepsilon_C|_{C_0})(x) = \varepsilon_C\left(\underbrace{x}_{=\tau\lambda}\right) = \varepsilon_C(\tau\lambda) = \tau\underbrace{\varepsilon_C(\lambda)}_{=1} \qquad \text{(since } \varepsilon_C \text{ is } k\text{-linear)}$$

$$= \tau,$$

we have $x = \underbrace{\tau}_{=0}\lambda = 0$. Now, forget that we fixed x. We thus have shown that every $x \in \operatorname{Ker}(\varepsilon_C|_{C_0})$ satisfies $x = 0$. In other words, $\operatorname{Ker}(\varepsilon_C|_{C_0}) = 0$. Hence, the map $\varepsilon_C|_{C_0}$ is injective. Combined with the fact that the map $\varepsilon_C|_{C_0}$ is surjective, this yields that the map $\varepsilon_C|_{C_0}$ is bijective.

So $\varepsilon_C|_{C_0}: C_0 \to k$ is a bijective k-linear map. Hence, $\varepsilon_C|_{C_0}: C_0 \to k$ is a k-vector space isomorphism.

But Definition 16.10 yields that the graded k-coalgebra C is connected if and only if the map $\varepsilon_C|_{C_0}: C_0 \to k$ is a k-vector space isomorphism. Thus, the graded k-coalgebra C is connected (because the map $\varepsilon_C|_{C_0}: C_0 \to k$ is a k-vector space isomorphism). Remark 16.12 is thus proven. □

An analogue of Remark 16.12 holds for filtered k-coalgebras:

Remark 16.13. Let k be a field. Let C be a filtered k-coalgebra. Let $\lambda \in C_{\leq 0}$ be such that $C_{\leq 0} = k \cdot \lambda$ and $\varepsilon_C(\lambda) = 1$. Then, the filtered k-coalgebra C is connected.

Proof of Remark 16.13. A proof of Remark 16.13 can be obtained by making the following replacements to the proof of Remark 16.12:

- Any occurrence of "C_0" should be replaced by "$C_{\leq 0}$".
- Any occurrence of "graded" should be replaced by "filtered".

- The reference to Definition 16.10 should be replaced by a reference to Definition 1.16.

Thus, Remark 16.13 is proven. □

We next repeat some basics related to graded vector spaces:

Definition 16.14. Let k be a field. Let V and W be graded k-vector spaces. Let $f : V \to W$ be a k-linear map. Then, the map f is said to be *graded* if every $n \in \mathbb{N}$ satisfies $f(V_n) \subseteq W_n$.

Remark 16.15. Let k be a field. Let V be a graded k-vector space. Then, $V = \bigoplus_{\ell \in \mathbb{N}} V_\ell$. For every $n \in \mathbb{N}$, let $\pi_n : \bigoplus_{\ell \in \mathbb{N}} V_\ell \to V_n$ be the canonical projection from the direct sum to its n-th addend, and let $\iota_n : V_n \to \bigoplus_{\ell \in \mathbb{N}} V_\ell$ be the canonical injection of the n-th addend into the direct sum. Since $\bigoplus_{\ell \in \mathbb{N}} V_\ell = V$, the map $\pi_n : \bigoplus_{\ell \in \mathbb{N}} V_\ell \to V_n$ is actually a map $V \to V_n$, and the map $\iota_n : V_n \to \bigoplus_{\ell \in \mathbb{N}} V_\ell$ is actually a map $V_n \to V$. Thus, the composition $\iota_n \circ \pi_n$ is a map $V \to V$. This map $\iota_n \circ \pi_n$ maps every element $v \in V$ to the n-th graded component of v, seen as an element of V.

Definition 16.16. Let k be a field. Let V be a graded k-vector space. For every $n \in \mathbb{N}$, we denote the k-linear map $\iota_n \circ \pi_n$ defined in Remark 16.15 as the *n-th grade identity* of V, and we denote it by $p_{n,V}$. As we mentioned in Remark 16.15, this map $p_{n,V}$ (which we denoted by $\iota_n \circ \pi_n$ in Remark 16.15) maps every element $v \in V$ to the n-th graded component of v, seen as an element of V.

Let us recall some well-known properties of these maps $p_{n,V}$:

For every $n \in \mathbb{N}$, the map $p_{n,V}$ is idempotent, i. e., it satisfies

$$p_{n,V} \circ p_{n,V} = p_{n,V} \tag{109}$$

[66]. It is known that

$$p_{n,V} \mid_{V_n} = \mathrm{id}_V \mid_{V_n} \qquad \text{for every } n \in \mathbb{N} \tag{110}$$

[66] *Proof of (109).* Let $n \in \mathbb{N}$. Let us use the notations of Remark 16.15. Then, $p_{n,V} = \iota_n \circ \pi_n$. Since $\pi_n : \bigoplus_{\ell \in \mathbb{N}} V_\ell \to V_n$ the canonical projection from the direct sum to its n-th addend, whereas $\iota_n : V_n \to \bigoplus_{\ell \in \mathbb{N}} V_\ell$ is the canonical injection of the n-th addend into the direct sum, it is clear that $\pi_n \circ \iota_n = \mathrm{id}$. Now, $p_{n,V} = \iota_n \circ \pi_n$ yields

$$p_{n,V} \circ p_{n,V} = \iota_n \circ \underbrace{\pi_n \circ \iota_n}_{=\mathrm{id}} \circ \pi_n = \iota_n \circ \mathrm{id} \circ \pi_n = \iota_n \circ \pi_n = p_{n,V},$$

thus proving (109).

[67], and that

$$p_{n,V} \mid_{V_m} = 0 \qquad \text{for any } n \in \mathbb{N} \text{ and } m \in \mathbb{N} \text{ satisfying } n \neq m \tag{111}$$

[68]. Also,

$$p_{n,V}(V) = V_n \qquad \text{for every } n \in \mathbb{N} \tag{112}$$

[69]. Also,

$$\text{the map } p_{n,V} \text{ is graded for every } n \in \mathbb{N} \tag{113}$$

[70].

---

[67] *Proof of (110).* Let $n \in \mathbb{N}$. Let us use the notations of Remark 16.15. Then, $p_{n,V} = \iota_n \circ \pi_n$. Since $\pi_n : \bigoplus_{\ell \in \mathbb{N}} V_\ell \to V_n$ the canonical projection from the direct sum to its n-th addend, it is clear that $\pi_n \mid_{V_n} = \mathrm{id}$. Now, $p_{n,V} = \iota_n \circ \pi_n$ yields

$$p_{n,V} \mid_{V_n} = (\iota_n \circ \pi_n) \mid_{V_n} = \iota_n \circ \underbrace{(\pi_n \mid_{V_n})}_{=\mathrm{id}} = \iota_n \circ \mathrm{id} = \iota_n = \mathrm{id}_V \mid_{V_n}$$

(since $\iota_n : V_n \to \bigoplus_{\ell \in \mathbb{N}} V_\ell$ is the canonical injection of the n-th addend into the direct sum). This proves (110).

[68] *Proof of (111).* Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$ satisfy $n \neq m$. Let us use the notations of Remark 16.15. Then, $p_{n,V} = \iota_n \circ \pi_n$. Since $\pi_n : \bigoplus_{\ell \in \mathbb{N}} V_\ell \to V_n$ the canonical projection from the direct sum to its n-th addend, it is clear that $\pi_n \mid_{V_\ell} = 0$ for every $\ell \in \mathbb{N}$ such that $\ell \neq n$. Applied to $\ell = m$, this yields that $\pi_n \mid_{V_m} = 0$. Now, $p_{n,V} = \iota_n \circ \pi_n$ yields

$$p_{n,V} \mid_{V_m} = (\iota_n \circ \pi_n) \mid_{V_m} = \iota_n \circ \underbrace{(\pi_n \mid_{V_m})}_{=0} = \iota_n \circ 0 = 0.$$

This proves (111).

[69] *Proof of (112).* Let $n \in \mathbb{N}$. Let us use the notations of Remark 16.15. Then, $p_{n,V} = \iota_n \circ \pi_n$. Since π_n is the canonical projection $\bigoplus_{\ell \in \mathbb{N}} V_\ell \to V_n$, it is clear that $\pi_n(V) = V_n$. Since ι_n is the canonical injection $V_n \to \bigoplus_{\ell \in \mathbb{N}} V_\ell$, we have $\iota_n(V_n) = V_n$. Thus,

$$\underbrace{p_{n,V}}_{=\iota_n \circ \pi_n}(V) = (\iota_n \circ \pi_n)(V) = \iota_n\left(\underbrace{\pi_n(V)}_{=V_n}\right) = \iota_n(V_n) = V_n,$$

so that (112) is proven.

[70] *Proof of (113).* Let $n \in \mathbb{N}$. Let $m \in \mathbb{N}$. We are going to prove that $p_{n,V}(V_m) \subseteq V_m$.

In fact, let us distinguish between two cases:

Case 1: We have $m = n$.

Case 2: We have $m \neq n$.

First let us consider Case 1. In this case, $m = n$, so that $V_m = V_n$. Now, $V_m \subseteq V$, so that $p_{n,V}(V_m) \subseteq p_{n,V}(V) = V_n$ (by (112)), so that $p_{n,V}(V_m) \subseteq V_n = V_m$.

We thus have proven $p_{n,V}(V_m) \subseteq V_m$ in Case 1.

Now let us consider Case 2. In this case, $m \neq n$, so that $p_{n,V} \mid_{V_m} = 0$ (by (111)). But now, $p_{n,V}(V_m) = \underbrace{(p_{n,V} \mid_{V_m})}_{=0}(V_m) = 0(V_m) = 0 \subseteq V_m$.

We thus have proven $p_{n,V}(V_m) \subseteq V_m$ in Case 2.

Now, $p_{n,V}(V_m) \subseteq V_m$ is proven in both cases 1 and 2. Since these cases are the only possible cases, this means that $p_{n,V}(V_m) \subseteq V_m$ always holds.

Now forget that we fixed m. We have proved that $p_{n,V}(V_m) \subseteq V_m$ for every $m \in \mathbb{N}$. In other words, $p_{n,V}$ is graded. This proves (113).

It is also known that every $v \in V$ satisfies

$$v = \sum_{\ell \in \mathbb{N}} p_{\ell,V}(v) \tag{114}$$

(where the sum $\sum_{\ell \in \mathbb{N}} p_{\ell,V}(v)$ is well-defined since it has only finitely many nonzero terms)[71].

Proposition 16.17. Let k be a field. Let V and W be graded k-vector spaces. Let $f : V \to W$ be a graded k-linear map. Then, $f \circ p_{n,V} = p_{n,W} \circ f = p_{n,W} \circ f \circ p_{n,V}$ (where $p_{n,V}$ and $p_{n,W}$ are the n-th grade identities of V and W, as defined in Definition 16.16) for every $n \in \mathbb{N}$.

Proof of Proposition 16.17. Let $n \in \mathbb{N}$.

a) Every $m \in \mathbb{N}$ satisfies $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$.

Proof. Let $m \in \mathbb{N}$. We distinguish between two cases:

Case 1: We have $m = n$.

[71] *Proof of (114).* Let $v \in V$.

Since $v \in V = \bigoplus_{\ell \in \mathbb{N}} V_\ell$, we can write v in the form $\sum_{\ell \in \mathbb{N}} v_\ell$, where ($v_\ell \in V_\ell$ for every $\ell \in \mathbb{N}$) and ($v_\ell = 0$ for all but finitely many $\ell \in \mathbb{N}$). So let us write v in this form.

For every $n \in \mathbb{N}$, we have

$$\begin{aligned}
p_{n,V}(v) &= p_{n,V}\left(\sum_{\ell \in \mathbb{N}} v_\ell\right) && \left(\text{since } v = \sum_{\ell \in \mathbb{N}} v_\ell\right) \\
&= \sum_{\ell \in \mathbb{N}} \underbrace{p_{n,V}(v_\ell)}_{\substack{=(p_{n,V}|_{V_\ell})(v_\ell) \\ (\text{since } v_\ell \in V_\ell)}} && (\text{since } p_{n,V} \text{ is } k\text{-linear}) \\
&= \sum_{\ell \in \mathbb{N}} (p_{n,V}|_{V_\ell})(v_\ell) = \underbrace{\sum_{\substack{\ell \in \mathbb{N}; \\ n=\ell}} (p_{n,V}|_{V_\ell})(v_\ell)}_{=(p_{n,V}|_{V_n})(v_n)} + \sum_{\substack{\ell \in \mathbb{N}; \\ n \neq \ell}} (p_{n,V}|_{V_\ell})(v_\ell) \\
&= \underbrace{(p_{n,V}|_{V_n})}_{\substack{=\mathrm{id}_V|_{V_n} \\ (\text{by (110)})}}(v_n) + \sum_{\substack{\ell \in \mathbb{N}; \\ n \neq \ell}} \underbrace{(p_{n,V}|_{V_\ell})}_{\substack{=0 \text{ (by (111) (applied to } m=\ell), \\ \text{since } n \neq \ell)}} (v_\ell) \\
&= \underbrace{(\mathrm{id}_V|_{V_n})(v_n)}_{=\mathrm{id}_V(v_n)=v_n} + \underbrace{\sum_{\substack{\ell \in \mathbb{N}; \\ n \neq \ell}} 0\,(v_\ell)}_{=0} = v_n.
\end{aligned}$$

Thus,

$$\begin{aligned}
\sum_{n \in \mathbb{N}} p_{n,V}(v) &= \sum_{n \in \mathbb{N}} v_n = \sum_{\ell \in \mathbb{N}} v_\ell && (\text{here, we renamed the index } n \text{ as } \ell \text{ in the sum}) \\
&= v,
\end{aligned}$$

so that

$$v = \sum_{n \in \mathbb{N}} p_{n,V}(v) = \sum_{\ell \in \mathbb{N}} p_{\ell,V}(v) \qquad (\text{here, we renamed the index } n \text{ as } \ell \text{ in the sum}).$$

This proves (114).

Case 2: We have $m \neq n$.

First, let us consider Case 1. In this case, $m = n$. Thus,

$$(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = (f \circ p_{n,V} - p_{n,W} \circ f)(V_n). \tag{115}$$

Now, let $x \in V_n$ be arbitrary. Then, $p_{n,V}(x) = \underbrace{(p_{n,V} \mid_{V_n})}_{\substack{=\mathrm{id}_V \mid_{V_n} \\ \text{(by (110))}}}(x) = (\mathrm{id}_V \mid_{V_n})(x) = \mathrm{id}_V(x) = x$. On the other hand, since $x \in V_n$, we have $f(x) \in f(V_n) \subseteq W_n$ (since f is graded), so that $p_{n,W}(f(x)) = \underbrace{(p_{n,W} \mid_{W_n})}_{\substack{=\mathrm{id}_W \mid_{W_n} \\ \text{(by (110), applied} \\ \text{to } W \text{ instead of } V)}}(f(x)) = (\mathrm{id}_W \mid_{W_n})(f(x)) = \mathrm{id}_W(f(x)) = f(x)$. But clearly,

$$\begin{aligned}(f \circ p_{n,V} - p_{n,W} \circ f)(x) &= (f \circ p_{n,V})(x) - (p_{n,W} \circ f)(x) \\ &= f\left(\underbrace{p_{n,V}(x)}_{=x}\right) - \underbrace{p_{n,W}(f(x))}_{=f(x)} = f(x) - f(x) = 0.\end{aligned}$$

Forget that we fixed x. We have thus proven that $(f \circ p_{n,V} - p_{n,W} \circ f)(x) = 0$ for every $x \in V_n$. In other words, $(f \circ p_{n,V} - p_{n,W} \circ f)(V_n) = 0$. Combined with (115), this becomes $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$.

We thus have proven that $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$ in Case 1.

Now let us treat Case 2. In this case, $m \neq n$. Now, $f(V_m) \subseteq W_m$ (since f is graded). We have

$$\begin{aligned}(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) &\subseteq \underbrace{(f \circ p_{n,V})(V_m)}_{=f\left(p_{n,V}(V_m)\right)} - \underbrace{(p_{n,W} \circ f)(V_m)}_{=p_{n,W}(f(V_m))} \\ &= f(p_{n,V}(V_m)) - p_{n,W}\left(\underbrace{f(V_m)}_{\subseteq W_m}\right) \subseteq f\left(\underbrace{p_{n,V}(V_m)}_{\substack{=0 \\ \text{(by (111))}}}\right) - \underbrace{p_{n,W}(W_m)}_{\substack{=0 \\ \text{(by (111), applied} \\ \text{to } W \text{ instead of } V)}} \\ &= \underbrace{f(0)}_{=0} - 0 = 0 - 0 = 0.\end{aligned}$$

Hence, $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$. This proves $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$ in Case 2.

Hence, we have proven $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$ in each of the cases 1 and 2. Since these two cases are all cases that can occur, this means that we have proven $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$ in every case. This completes the proof of **a)**.

b) We have $f \circ p_{n,V} = p_{n,W} \circ f$.

Proof. Every $m \in \mathbb{N}$ satisfies $(f \circ p_{n,V} - p_{n,W} \circ f)(V_m) = 0$ (according to part **a)**). In other words, every $m \in \mathbb{N}$ satisfies $V_m \subseteq \mathrm{Ker}(f \circ p_{n,V} - p_{n,W} \circ f)$. Thus,

$$\sum_{m \in \mathbb{N}} V_m \subseteq \sum_{m \in \mathbb{N}} \mathrm{Ker}(f \circ p_{n,V} - p_{n,W} \circ f) \subseteq \mathrm{Ker}(f \circ p_{n,V} - p_{n,W} \circ f)$$

$$\left(\begin{array}{c} \text{since } \mathrm{Ker}(f \circ p_{n,V} - p_{n,W} \circ f) \text{ is a } k\text{-vector subspace of } V \\ \text{(because } f \circ p_{n,V} - p_{n,W} \circ f \text{ is a } k\text{-linear map)} \end{array} \right).$$

But since V is graded, we have $V = \bigoplus_{m \in \mathbb{N}} V_m = \sum_{m \in \mathbb{N}} V_m$ (since direct sums are sums). Thus,

$$V = \sum_{m \in \mathbb{N}} V_m \subseteq \operatorname{Ker}\left(f \circ p_{n,V} - p_{n,W} \circ f\right),$$

so that $f \circ p_{n,V} - p_{n,W} \circ f = 0$. In other words, $f \circ p_{n,V} = p_{n,W} \circ f$. This proves part **b)**.

c) By part **b)**, we know that $f \circ p_{n,V} = p_{n,W} \circ f$. Thus, $\underbrace{p_{n,W} \circ f}_{= f \circ p_{n,V}} \circ p_{n,V} = f \circ \underbrace{p_{n,V} \circ p_{n,V}}_{\substack{= p_{n,V} \\ \text{(by (109))}}} = f \circ p_{n,V}$. Combined with $f \circ p_{n,V} = p_{n,W} \circ f$, this yields $f \circ p_{n,V} = p_{n,W} \circ f = p_{n,W} \circ f \circ p_{n,V}$. This proves Proposition 16.17. □

We now prove that gradedness is compatible with convolution:

Proposition 16.18. Let k be a field. Let C be a graded k-coalgebra. Let A be a graded k-algebra.

(a) If $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$ are two graded maps, then $f * g \in \mathcal{L}(C, A)$ is graded as well.

(b) The map $e_{C,A} : C \to A$ is graded.

(c) If $f \in \mathcal{L}(C, A)$ is a graded map and $n \in \mathbb{N}$, then $f^{*n} \in \mathcal{L}(C, A)$ is graded as well.

(d) Assume that C is a connected filtered k-coalgebra, and that the field k has characteristic 0. If $f \in \mathfrak{g}(C, A)$ is a graded map, then e^{*f} is a graded map.

(e) Assume that C is a connected filtered k-coalgebra, and that the field k has characteristic 0. If $F \in G(C, A)$ is a graded map, then $\operatorname{Log} F$ is a graded map.

Proof of Proposition 16.18. **(a)** Let $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$ be two graded maps.

By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$. Now, since A is a graded k-algebra, its multiplication map μ_A is graded (where the grading on $A \otimes A$ is the usual one that is given to the tensor product of two graded k-vector spaces). Since C is a graded k-coalgebra, its comultiplication map Δ_C is graded (where the grading on $C \otimes C$ is the usual one that is given to the tensor product of two graded k-vector spaces). Also, the map $f \otimes g$ is graded (since f and g are graded, and since the tensor product of two graded maps is graded). Now recall that the composition of graded maps is graded. Thus, the map $\mu_A \circ (f \otimes g) \circ \Delta_C$ is graded (since μ_A, $f \otimes g$ and Δ_C are graded). Since $\mu_A \circ (f \otimes g) \circ \Delta_C = f * g$, this means that the map $f * g$ is graded. This proves Proposition 16.18 **(a)**.

(b) Let us give k the usual grading (the one where $k_0 = k$ and $k_n = 0$ for all positive $n \in \mathbb{N}$). Since A is a graded k-algebra, its unity map $\eta_A : k \to A$ is graded. Since C is a graded k-coalgebra, its counity map $\varepsilon_C : C \to k$ is graded. Now, the map $e_{C,A} = \eta_A \circ \varepsilon_C$ is graded (since η_A and ε_C are graded, and since the composition of graded maps is graded). This proves Proposition 16.18 **(b)**.

(c) Let us prove Proposition 16.18 **(c)** by induction over n:

Induction base: The map f^{*0} is graded for every $f \in \mathcal{L}(C, A)$ (because for every $f \in \mathcal{L}(C, A)$, the map f^{*0} equals $e_{C,A}$ and thus is graded by Proposition 16.18 **(b)**). Thus, Proposition 16.18 **(c)** holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that Proposition 16.18 **(c)** holds for $n = N$. We must show that Proposition 16.18 **(c)** also holds for $n = N + 1$.

Let $f \in \mathcal{L}(C, A)$ be graded. Then, f^{*N} is graded as well (since we assumed that Proposition 16.18 **(c)** holds for $n = N$). Now, Proposition 16.18 **(a)** (applied to $g = f^{*N}$) yields that $f * f^{*N}$ is graded. Since $f * f^{*N} = f^{*(N+1)}$, this means that $f^{*(N+1)}$ is graded.

Thus we have shown that for every graded $f \in \mathcal{L}(C, A)$, the map $f^{*(N+1)} \in \mathcal{L}(C, A)$ is graded as well. In other words, we have proven that Proposition 16.18 **(c)** holds for $n = N + 1$. This completes the induction step.

Thus, the induction proof of Proposition 16.18 **(c)** is complete.

(e) Let $F \in G(C, A)$ be a graded map.

The map $e_{C,A}$ is graded (by Proposition 16.18 **(b)**).

By Definition 3.8, we have $\operatorname{Log} F = \operatorname{Log}_1 (F - e_{C,A})$. Let $f = F - e_{C,A}$. Then, $f = F - e_{C,A}$ is graded (because F and $e_{C,A}$ are graded, and because the difference of graded maps is graded). Hence, for every integer $i \geq 1$, the map f^{*i} is graded (by Proposition 16.18 **(c)**, applied to $n = i$). Also, $f = F - e_{C,A} \in \mathfrak{g}(C, A)$ (since $F \in G(C, A) = e_{C,A} + \mathfrak{g}(C, A)$). Thus, every $i \in \mathbb{N}$ and $n \in \mathbb{N}$ such that $i > n$ satisfy $f^{*i}(C_{\leq n}) = 0$ (by Remark 3.5, applied to $H = C$).

Now let $n \in \mathbb{N}$. The definition of $C_{\leq n}$ says that $C_{\leq n} = \bigoplus_{\ell=0}^{n} C_\ell = C_n \oplus \bigoplus_{\ell=0}^{n-1} C_\ell \supseteq C_n$. Hence, $C_n \subseteq C_{\leq n}$.

Let $x \in C_n$. Then, every $i \in \mathbb{N}$ and $n \in \mathbb{N}$ such that $i > n$ satisfy $f^{*i}(x) = 0$ (since $f^{*i}\left(\underbrace{x}_{\in C_n \subseteq C_{\leq n}}\right) \in f^{*i}(C_{\leq n}) = 0$). Thus, $\sum\limits_{\substack{i \geq 1; \\ i > n}} \dfrac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{=0 \text{ (since } i>n)} = \sum\limits_{\substack{i \geq 1; \\ i > n}} \dfrac{(-1)^{i-1}}{i} 0 = 0$.

For every integer $i \geq 1$, we have $f^{*i}(C_n) \subseteq A_n$ (since f^{*i} is graded). Thus, for every integer $i \geq 1$, we have $f^{*i}(x) \in A_n$ (because $x \in C_n$ and thus $f^{*i}(x) \in f^{*i}(C_n) \subseteq A_n$). But

$$\begin{aligned}
(\operatorname{Log}_1 f)(x) &= \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) \qquad \text{(by (8))} \\
&= \sum_{\substack{i \geq 1; \\ i \leq n}} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{\in A_n} + \underbrace{\sum_{\substack{i \geq 1; \\ i > n}} \frac{(-1)^{i-1}}{i} f^{*i}(x)}_{=0} \in \sum_{\substack{i \geq 1; \\ i \leq n}} \frac{(-1)^{i-1}}{i} A_n \subseteq A_n
\end{aligned}$$

(since A_n is a k-vector space).

Now forget that we fixed x. We thus have proven that $(\operatorname{Log}_1 f)(x) \in A_n$ for every $x \in C_n$. In other words, $(\operatorname{Log}_1 f)(C_n) \subseteq A_n$.

Now forget that we fixed n. We have thus proven that $(\operatorname{Log}_1 f)(C_n) \subseteq A_n$ for every $n \in \mathbb{N}$. In other words, the map $\operatorname{Log}_1 f$ is graded.

The map $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{C,A})}_{=f} = \operatorname{Log}_1 f$ is graded (as we just have shown).

This proves Proposition 16.18 **(e)**.

(d) The proof of Proposition 16.18 **(d)** is very similar to that of Proposition 16.18 **(e)** (and even easier since we do not have two maps F and f but only one map f). We will leave it at that and let the reader fill in the details. (We won't need Proposition 16.18 **(d)** anyway.) $\square$

We now need a notation:

Convention 16.19. Let k be a field, let A be a k-algebra, and let S be a subset of A. Then, *the k-subalgebra of A generated by S* can be defined in several ways. Here are four ways to define it:

- It is the smallest k-subalgebra of A which contains S as a subset. ("Smallest" means that it is contained in every such k-subalgebra. Of course, it is not immediately trivial that the smallest k-subalgebra of A which contains S exists at all.)
- It is the intersection of all k-subalgebras of A which contain S as a subset.
- It is the subset of A formed by all elements that can be obtained by repeated addition, multiplication and scaling with elements of k [72] from elements of S. Here, "multiplication" doesn't only mean multiplication of two elements, but can also mean multiplication of n elements for any $n \in \mathbb{N}$. (In particular, it can mean multiplication of 0 elements; this gives the unity 1_A as the result.)
- It is the k-vector subspace $\langle S \rangle^0 + \langle S \rangle^1 + \langle S \rangle^2 + \cdots = \sum_{\ell \in \mathbb{N}} \langle S \rangle^\ell$ of A (where $\langle S \rangle$ denotes the k-vector subspace of A generated by the subset S).

It is rather well-known that all of these definitions of the k-subalgebra of A generated by S are equivalent, and that the k-subalgebra of A generated by S is really a k-subalgebra of A. We denote by $\operatorname{AlgGen}_k S$ the k-subalgebra of A generated by S.

Some rather obvious properties of this notation will be used without explicit mention. For example, if S and T are two subsets of a k-subalgebra A satisfying $S \subseteq T$, then $\operatorname{AlgGen}_k S \subseteq \operatorname{AlgGen}_k T$. (This can easily be derived from any of the definitions of $\operatorname{AlgGen}_k S$.)

Here is another, even more obvious fact:

Lemma 16.20. Let k be a field. Let A be a k-algebra. Let S be any subset of A. Then,

$$S \subseteq \operatorname{AlgGen}_k S. \tag{116}$$

Proof of Lemma 16.20. Recall that $\operatorname{AlgGen}_k S$ is the k-subalgebra of A generated by S; this k-subalgebra clearly contains S as a subset. In other words, $\operatorname{AlgGen}_k S$ contains S as a subset. In other words, $S \subseteq \operatorname{AlgGen}_k S$. This proves Lemma 16.20. $\square$

[72] By "scaling with an element $\lambda \in k$ ", we mean the map $A \to A$ which sends every $a \in A$ to λa.

Our next goal is the following theorem:

Theorem 16.21. Let k be a field of characteristic 0, and let H be a connected graded k-bialgebra. Let ζ be the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$.

(a) The map ζ is graded.

(b) For every $n \in \mathbb{N}$, let p_n denote the map $p_{n,H}$ (defined according to Definition 16.16), and let ζ_n denote the map $\zeta \circ p_n$. Then,

$$\zeta_n = \zeta \circ p_n = p_n \circ \zeta = p_n \circ \zeta \circ p_n \qquad \text{for every } n \in \mathbb{N}. \tag{117}$$

Besides,

$$\operatorname{AlgGen}_k \{\zeta_1, \zeta_2, \zeta_3, \ldots\} = \operatorname{AlgGen}_k \{p_1, p_2, p_3, \ldots\}. \tag{118}$$

Remark. In Theorem 16.21 and in the following Proposition 16.22, we are considering the algebra $\mathcal{L}(H, H)$ whose multiplication is convolution, *not* the algebra $\operatorname{End} H$ whose multiplication is composition of mappings. Thus, for example, $\operatorname{AlgGen}_k \{\zeta_1, \zeta_2, \zeta_3, \ldots\}$ denotes the k-subalgebra of $\mathcal{L}(H, H)$ (not of $\operatorname{End} H$) generated by the subset $\{\zeta_1, \zeta_2, \zeta_3, \ldots\}$.

Before we begin proving Theorem 16.21, let us notice that its part **(a)** is a trivial consequence of Proposition 16.18 **(e)**, and the equation (117) in part **(b)** follows immediately from part **(a)** due to Proposition 16.17. The main part of Theorem 16.21 is the equality (118). This equality was mentioned in the Example in §2 of [PatReu98][73].

First let us prove the easy part of Theorem 16.21:

Proof of Theorem 16.21, first part. **(a)** Applying Proposition 16.18 **(e)** to $C = H$, $A = H$ and $f = \operatorname{id}$, we conclude that $\operatorname{Log} \operatorname{id}$ is graded (since $\operatorname{id} \in G(H, H)$ is graded). Since $\zeta = \operatorname{Log} \operatorname{id}$, this rewrites as follows: The map ζ is graded. This proves Theorem 16.21 **(a)**.

(b) Let $n \in \mathbb{N}$. Since the map ζ is graded (by Theorem 16.21 **(a)**), we have

$$\zeta \circ p_{n,H} = p_{n,H} \circ \zeta = p_{n,H} \circ \zeta \circ p_{n,H}$$

(by Proposition 16.17, applied to $V = H$, $W = H$ and $f = \zeta$). Since $p_{n,H} = p_n$, this rewrites as $\zeta \circ p_n = p_n \circ \zeta = p_n \circ \zeta \circ p_n$. Combined with $\zeta_n = \zeta \circ p_n$, this yields (117).

We thus have proven (117). We are going to prove (118) later. For the time being, we leave the proof of Theorem 16.21. ☐

Here is an assertion which will turn out to be somewhat stronger than (118) (we are later going to derive (118) from it):

[73] More precisely, the notations F, A, e, e_n, $\mathcal{D}(A)$ and $\mathcal{D}_e$ of [PatReu98] correspond to the notations k, H, ζ, ζ_n, $\operatorname{AlgGen}_k \{p_1, p_2, p_3, \ldots\}$ and $\operatorname{AlgGen}_k \{\zeta_1, \zeta_2, \zeta_3, \ldots\}$ in our text (but we do not require H to be cocommutative here). Hence, our equation (118) rewrites as $\mathcal{D}(A) = \mathcal{D}_e$ using the notations of [PatReu98]. This is mentioned in the Example in §2 of [PatReu98], and used afterwards in the proof of Theorem 5.1 of [PatReu98].

Proposition 16.22. Let k be a field of characteristic 0, and let H be a connected graded k-bialgebra. Let ζ be the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$. We are going to use the notations of Theorem 16.21 **(b)**.

For every $n \in \mathbb{N}$, we have

$$p_n - \zeta_n \in \operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_{n-1}\}.$$

And here is a "finite" version of (118):

Proposition 16.23. Let k be a field of characteristic 0, and let H be a connected graded k-bialgebra. Let ζ be the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$. We are going to use the notations of Theorem 16.21 **(b)**.

For every $n \in \mathbb{N}$, we have

$$\operatorname{AlgGen}_k \{\zeta_1, \zeta_2, \ldots, \zeta_n\} = \operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_n\}.$$

We will prove these two propositions before showing Theorem 16.21. But first, we introduce another notation, and show some of its properties. First, the notation:

Definition 16.24. Let k be a field. Let H be a graded k-vector space. Let $f \in \mathcal{L}(H, H)$ be a graded map. Let $n \in \mathbb{N}$. Just as in Theorem 16.21 **(b)**, let p_n denote the map $p_{n,H}$ (defined according to Definition 16.16). Then, we say that f is *concentrated in degree n* if and only if $f = p_n \circ f$.

It is easily seen that (in the context of Definition 16.24) we have the following chain of equivalences:

$$\begin{aligned}
&(f \text{ is concentrated in degree } n) \\
&\iff (f = p_n \circ f) \iff (f = f \circ p_n) \iff (f = p_n \circ f \circ p_n) \\
&\iff (f(H) \subseteq H_n) \iff (f(H_m) = 0 \text{ for all } m \in \mathbb{N} \text{ satisfying } m \neq n).
\end{aligned}$$

However, we are not going to use these equivalences (at least not explicitly).

The following properties of being concentrated in degree n will be used:

Proposition 16.25. Let k be a field. Let H be a graded k-bialgebra.

(a) The map $e_{H,H}$ is graded and concentrated in degree 0.

(b) Let $a \in \mathbb{N}$, $b \in \mathbb{N}$, $f \in \mathcal{L}(H, H)$ and $g \in \mathcal{L}(H, H)$. Assume that f is graded and concentrated in degree a. Assume that g is graded and concentrated in degree b. Then, $f * g$ is graded and concentrated in degree $a + b$.

(c) Let $\ell \in \mathbb{N}$. Let a_i be a nonnegative integer for every $i \in \{1, 2, \ldots, \ell\}$. Let f_i be an element of $\mathcal{L}(H, H)$ for every $i \in \{1, 2, \ldots, \ell\}$. Assume that for every $i \in \{1, 2, \ldots, \ell\}$, the map f_i is graded and concentrated in degree a_i. Then, $f_1 * f_2 * \cdots * f_\ell$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_\ell$.

(d) For every $n \in \mathbb{N}$, the map p_n (defined in Theorem 16.21 **(b)**) is graded and concentrated in degree n.

(e) If the graded k-bialgebra H is connected, then $e_{H,H} = p_0$ (where the map p_0 is defined as $p_{0,H}$, just as in Theorem 16.21 **(b)**).

Proof of Proposition 16.25. Just as in Theorem 16.21 **(b)**, let p_n denote the map $p_{n,H}$ for every $n \in \mathbb{N}$ (defined according to Definition 16.16).

(a) We have $e_{H,H} = \eta_H \circ \varepsilon_H$. But since H is a graded k-bialgebra, we have $1_H \in H_0$.

By the definition of p_0, we have $p_0 = p_{0,H}$. Thus, $p_0 \mid_{H_0} = p_{0,H} \mid_{H_0} = \mathrm{id}_H \mid_{H_0}$ (by (110), applied to $V = H$ and $n = 0$).

Every $x \in H$ satisfies

$$\underbrace{e_{H,H}}_{=\eta_H \circ \varepsilon_H}(x) = (\eta_H \circ \varepsilon_H)(x) = \eta_H(\varepsilon_H(x)) = \varepsilon_H(x) \cdot 1_H \qquad \text{(by the definition of } \eta_H\text{)}$$

and now

$$\begin{aligned}
&(p_0 \circ e_{H,H})(x) \\
&= p_0\left(\underbrace{e_{H,H}(x)}_{=\varepsilon_H(x)\cdot 1_H}\right) = p_0(\varepsilon_H(x) \cdot 1_H) \\
&= \underbrace{(p_0 \mid_{H_0})}_{=\mathrm{id}_H \mid_{H_0}}(\varepsilon_H(x) \cdot 1_H) \qquad \left(\text{since } \varepsilon_H(x) \cdot \underbrace{1_H}_{\in H_0} \in H_0 \text{ (since } H_0 \text{ is a } k\text{-vector space)}\right) \\
&= (\mathrm{id}_H \mid_{H_0})(\varepsilon_H(x) \cdot 1_H) = \varepsilon_H(x) \cdot 1_H = e_{H,H}(x).
\end{aligned}$$

Thus, $p_0 \circ e_{H,H} = e_{H,H}$. In other words, $e_{H,H} = p_0 \circ e_{H,H}$. Combined with the fact that $e_{H,H}$ is graded (by Proposition 16.18 **(b)**, applied to $C = H$ and $A = H$), this yields that $e_{H,H}$ is concentrated in degree 0 (by Definition 16.24). This proves Proposition 16.25 **(a)**.

(b) Since f is graded and concentrated in degree a, we have $f = p_a \circ f$ (by Definition 16.24). Thus,

$$\begin{aligned}
f(H) = (p_a \circ f)(H) &= \underbrace{p_a}_{\substack{=p_{a,H} \\ \text{(by the definition of } p_a\text{)}}}\left(\underbrace{f(H)}_{\subseteq H}\right) \subseteq p_{a,H}(H) \\
&= H_a \qquad \text{(by (112), applied to } n = a \text{ and } V = H\text{)}.
\end{aligned}$$

Similarly, $g(H) \subseteq H_b$.

Since H is a graded k-bialgebra, its multiplication map $\mu_H : H \otimes H \to H$ is graded, where the grading on $H \otimes H$ is the usual grading on the tensor product of two graded k-vector spaces. Now, this grading is defined by $(H \otimes H)_n = \sum_{\ell=0}^{n} H_\ell \otimes H_{n-\ell}$ for every

$n \in \mathbb{N}$. Hence, for every $a \in \mathbb{N}$ and $b \in \mathbb{N}$, we have

$$\begin{aligned}
(H \otimes H)_{a+b} &= \sum_{\ell=0}^{a+b} H_\ell \otimes H_{a+b-\ell} \\
&\qquad \left(\text{due to } (H \otimes H)_n = \sum_{\ell=0}^{n} H_\ell \otimes H_{n-\ell}, \text{ applied to } n = a+b \right) \\
&\supseteq H_a \otimes \underbrace{H_{a+b-a}}_{=H_b} \\
&\qquad \left(\begin{array}{c} \text{since } H_a \otimes H_{a+b-a} \text{ is an addend in the sum } \sum_{\ell=0}^{a+b} H_\ell \otimes H_{a+b-\ell} \\ \text{(namely, the addend for } \ell = a) \end{array} \right) \\
&= H_a \otimes H_b.
\end{aligned}$$

Thus, for every $a \in \mathbb{N}$ and $b \in \mathbb{N}$, we have $H_a \otimes H_b \subseteq (H \otimes H)_{a+b}$, so that

$$\mu_H (H_a \otimes H_b) \subseteq \mu_H \left((H \otimes H)_{a+b} \right) \subseteq H_{a+b} \qquad \text{(since } \mu_H \text{ is graded)}.$$

Now, by the definition of convolution, $f * g = \mu_H \circ (f \otimes g) \circ \Delta_H$, so that

$$\begin{aligned}
(f * g)(H) &= (\mu_H \circ (f \otimes g) \circ \Delta_H)(H) = \mu_H \left((f \otimes g) \underbrace{(\Delta_H (H))}_{\subseteq H \otimes H} \right) \subseteq \mu_H \left(\underbrace{(f \otimes g)(H \otimes H)}_{=f(H) \otimes g(H)} \right) \\
&= \mu_H \left(\underbrace{f(H)}_{\subseteq H_a} \otimes \underbrace{g(H)}_{\subseteq H_b} \right) \subseteq \mu_H (H_a \otimes H_b) \subseteq H_{a+b}.
\end{aligned}$$

Thus, every $x \in H$ satisfies $(f * g)(x) \in H_{a+b}$. Hence, every $x \in H$ satisfies

$$\begin{aligned}
(p_{a+b} \circ (f * g))(x) &= p_{a+b}((f * g)(x)) = \left(\underbrace{p_{a+b}}_{\substack{=p_{a+b,H} \\ \text{(by the definition of } p_{a+b}\text{)}}} |_{H_{a+b}} \right) ((f * g)(x)) \\
&\qquad \text{(since } (f * g)(x) \in H_{a+b}\text{)} \\
&= \underbrace{\left(p_{a+b,H} |_{H_{a+b}} \right)}_{\substack{=\mathrm{id}_H |_{H_{a+b}} \\ \text{(by (110), applied to} \\ V=H \text{ and } n=a+b\text{)}}} ((f * g)(x)) = \left(\mathrm{id}_H |_{H_{a+b}} \right) ((f * g)(x)) \\
&= (f * g)(x).
\end{aligned}$$

In other words, $p_{a+b} \circ (f * g) = f * g$.

Hence, $f * g = p_{a+b} \circ (f * g)$. Combined with the fact that $f * g$ is graded (by Proposition 16.18 **(a)**, applied to $C = H$ and $A = H$), this yields that $f * g$ is concentrated in degree $a + b$ (by Definition 16.24). This proves Proposition 16.25 **(b)**.

(c) We are going to prove that for every $j \in \{0, 1, \ldots, \ell\}$,

$$\text{the map } f_1 * f_2 * \cdots * f_j \text{ is graded and concentrated in degree } a_1 + a_2 + \cdots + a_j. \quad (119)$$

Proof of (119). We will prove (119) by induction over j:

Induction base: The map $f_1 * f_2 * \cdots * f_0 = e_{H,H}$ is graded and concentrated in degree 0 (by Proposition 16.25 **(a)**). Since $0 = a_1 + a_2 + \cdots + a_0$, we thus have shown that the map $f_1 * f_2 * \cdots * f_0$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_0$. In other words, we have shown that (119) holds for $j = 0$. This completes the induction base.

Induction step: Let $J \in \{0, 1, \ldots, \ell - 1\}$. Assume that (119) holds for $j = J$. We now must prove that (119) holds for $j = J + 1$.

We know that for every $i \in \{1, 2, \ldots, \ell\}$, the map f_i is graded and concentrated in degree a_i. Hence, the map f_{J+1} is graded and concentrated in degree a_{J+1}.

Since (119) holds for $j = J$, the map $f_1 * f_2 * \cdots * f_J$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_J$. Applying Proposition 16.25 **(b)** to $a = a_1 + a_2 + \cdots + a_J$, $b = a_{J+1}$, $f = f_1 * f_2 * \cdots * f_J$ and $g = f_{J+1}$, we now see that the map $(f_1 * f_2 * \cdots * f_J) * f_{J+1}$ is graded and concentrated in degree $(a_1 + a_2 + \cdots + a_J) + a_{J+1}$. Since $(f_1 * f_2 * \cdots * f_J) * f_{J+1} = f_1 * f_2 * \cdots * f_{J+1}$ and $(a_1 + a_2 + \cdots + a_J) + a_{J+1} = a_1 + a_2 + \cdots + a_{J+1}$, this rewrites as follows: The map $f_1 * f_2 * \cdots * f_{J+1}$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_{J+1}$. In other words, (119) holds for $j = J + 1$. This completes the induction step.

Thus, the induction proof of (119) is complete.

Now we can apply (119) to $j = \ell$, and conclude that the map $f_1 * f_2 * \cdots * f_\ell$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_\ell$. This proves Proposition 16.25 **(c)**.

(d) Let $n \in \mathbb{N}$. Since p_n was defined as $p_{n,H}$, we can rewrite the identity $p_{n,H} \circ p_{n,H} = p_{n,H}$ (which follows from (109), applied to $V = H$) as $p_n \circ p_n = p_n$.

Also, $p_n = p_{n,H}$ is graded (by (113), applied to $V = H$). Thus, p_n is a graded map satisfying $p_n = p_n \circ p_n$. By Definition 16.24, this yields that p_n is concentrated in degree n. This proves Proposition 16.25 **(d)**.

(e) Assume that the graded k-bialgebra H is connected. Then, $\varepsilon_H \mid_{H_0} : H_0 \to k$ is a k-vector space isomorphism (because this is how a connected graded k-bialgebra was defined in Definition 16.10).

Let us give k the usual grading (the one where $k_0 = k$ and $k_n = 0$ for all positive $n \in \mathbb{N}$). Since H is a graded k-coalgebra, its counity map $\varepsilon_H : H \to k$ is graded. Thus, Proposition 16.17 (applied to $V = H$, $W = k$, $f = \varepsilon_H$ and $n = 0$) yields $\varepsilon_H \circ p_{0,H} = p_{0,k} \circ \varepsilon_H = p_{0,k} \circ \varepsilon_H \circ p_{0,H}$. But since $k_0 = k$, we have

$$\begin{aligned} p_{0,k} &= p_{0,k} \mid_{k_0} = \mathrm{id}_k \mid_{k_0} \qquad \text{(by (110), applied to } V = k \text{ and } n = 0) \\ &= \mathrm{id}_k \qquad (\text{since } k_0 = k), \end{aligned}$$

so that $\varepsilon_H \circ p_{0,H} = p_{0,k} \circ \varepsilon_H$ simplifies to $\varepsilon_H \circ p_{0,H} = \varepsilon_H$. Since $p_{0,H} = p_0$, this further rewrites as $\varepsilon_H \circ p_0 = \varepsilon_H$.

Since H is a bialgebra, we have $\varepsilon_H \circ \eta_H = \mathrm{id}_k$ (by the axioms of a bialgebra). But $e_{H,H} = \eta_H \circ \varepsilon_H$ (by the definition of $e_{H,H}$). Thus, $\varepsilon_H \circ e_{H,H} = \underbrace{\varepsilon_H \circ \eta_H}_{=\mathrm{id}_k} \circ \varepsilon_H = \varepsilon_H$.

Now let $x \in H$. Then,

$$\underbrace{p_0}_{=p_{0,H}}(x) = p_{0,H}(x) \in p_{0,H}(H) = H_0 \qquad \text{(by (112), applied to } V = H \text{ and } n = 0),$$

so that $(\varepsilon_H \mid_{H_0})(p_0(x))$ is well-defined. Also,

$$\underbrace{e_{H,H}}_{=\eta_H \circ \varepsilon_H}(x) = (\eta_H \circ \varepsilon_H)(x) = \eta_H(\varepsilon_H(x)) = \varepsilon_H(x) \cdot 1_H \qquad \text{(by the definition of } \eta_H\text{)}$$

$$\in H_0 \qquad \left(\begin{array}{c} \text{since } 1_H \in H_0 \text{ (because } H \text{ is a graded } k\text{-algebra),} \\ \text{and since } H_0 \text{ is a } k\text{-vector space} \end{array} \right),$$

so that $(\varepsilon_H \mid_{H_0})(e_{H,H}(x))$ is well-defined. Since

$$(\varepsilon_H \mid_{H_0})(p_0(x)) = \varepsilon_H(p_0(x)) = \underbrace{(\varepsilon_H \circ p_0)}_{=\varepsilon_H = \varepsilon_H \circ e_{H,H}}(x) = (\varepsilon_H \circ e_{H,H})(x)$$
$$= \varepsilon_H(e_{H,H}(x)) = (\varepsilon_H \mid_{H_0})(e_{H,H}(x)),$$

we conclude that $p_0(x) = e_{H,H}(x)$ (since $\varepsilon_H \mid_{H_0}$ is an isomorphism). Since we have proven this for every $x \in H$, we conclude that $p_0 = e_{H,H}$. This proves Proposition 16.25 **(e)**. □

Proposition 16.25 has a very easy corollary:

Corollary 16.26. Let k be a field. Let H be a graded k-bialgebra. For every $n \in \mathbb{N}$, let p_n denote the map $p_{n,H}$ (defined according to Definition 16.16).

Let $n \in \mathbb{N}$ and $\ell \in \mathbb{N}$. Let a_i be a nonnegative integer for every $i \in \{1, 2, \ldots, \ell\}$.

(a) We have $p_n \circ (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) = 0$ if $n \neq a_1 + a_2 + \cdots + a_\ell$.

(b) We have $p_n \circ (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) = p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}$ if $n = a_1 + a_2 + \cdots + a_\ell$.

Proof of Corollary 16.26. For every $i \in \{1, 2, \ldots, \ell\}$, the map p_{a_i} is graded and concentrated in degree a_i (by Proposition 16.25 **(d)**, applied to a_i instead of n). Thus, Proposition 16.25 **(c)** (applied to $f_i = p_{a_i}$) yields that $p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_\ell$. According to Definition 16.24, this means that

$$p_{a_1+a_2+\cdots+a_\ell} \circ (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) = p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}. \tag{120}$$

(a) Assume that $n \neq a_1 + a_2 + \cdots + a_\ell$. Then, $p_{n,H} \mid_{H_{a_1+a_2+\cdots+a_\ell}} = 0$ (by (111), applied to $m = a_1 + a_2 + \cdots + a_\ell$ and $V = H$).

But

$$\underbrace{(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell})}_{\substack{=p_{a_1+a_2+\cdots+a_\ell} \circ (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) \\ \text{(by (120))}}}(H)$$
$$= (p_{a_1+a_2+\cdots+a_\ell} \circ (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}))(H)$$
$$= \underbrace{p_{a_1+a_2+\cdots+a_\ell}}_{\substack{=p_{a_1+a_2+\cdots+a_\ell,H} \\ \text{(by the definition of } p_{a_1+a_2+\cdots+a_\ell}\text{)}}} \left(\underbrace{(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell})(H)}_{\subseteq H} \right)$$
$$\subseteq p_{a_1+a_2+\cdots+a_\ell,H}(H) = H_{a_1+a_2+\cdots+a_\ell} \qquad \left(\begin{array}{c} \text{by (112), applied to } H \text{ and } a_1 + a_2 + \cdots + a_\ell \\ \text{instead of } V \text{ and } n \end{array} \right)$$

and thus

$$p_n\left(\left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(H)\right) \subseteq \underbrace{p_n}_{\substack{=p_{n,H} \\ \text{(by the definition of } p_n\text{)}}}\left(H_{a_1+a_2+\cdots+a_\ell}\right) = p_{n,H}\left(H_{a_1+a_2+\cdots+a_\ell}\right)$$
$$= \underbrace{\left(p_{n,H}\mid_{H_{a_1+a_2+\cdots+a_\ell}}\right)}_{=0}\left(H_{a_1+a_2+\cdots+a_\ell}\right) = 0\left(H_{a_1+a_2+\cdots+a_\ell}\right) = 0.$$

Since $p_n\left(\left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(H)\right) = \left(p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)\right)(H)$, this rewrites as $\left(p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)\right)(H) = 0$. Thus, $p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right) = 0$. This proves Corollary 16.26 **(a)**.

(b) Now assume that $n = a_1 + a_2 + \cdots + a_\ell$. Then,

$$p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right) = p_{a_1+a_2+\cdots+a_\ell} \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right) = p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}$$

(by (120)). This proves Corollary 16.26 **(b)**. □

Proof of Proposition 16.22. Let $n \in \mathbb{N}$.

Let h denote the map $\mathrm{id} - e_{H,H}$ (where id means id_H). Then, since $\mathrm{id} \in G(H,H) = e_{H,H} + \mathfrak{g}(H,H)$, we have $\mathrm{id} - e_{H,H} \in \mathfrak{g}(H,H)$, so that $h = \mathrm{id} - e_{H,H} \in \mathfrak{g}(H,H)$.

We will now prove Proposition 16.22 in several steps:

a) Every $x \in H_{\leq n}$ satisfies

$$h(x) = \left(p_1 + p_2 + \cdots + p_n\right)(x). \tag{121}$$

Proof of (121). Let $x \in H_{\leq n}$. By (114) (applied to $V = H$ and $v = x$), we have $x = \sum_{\ell \in \mathbb{N}} p_{\ell,H}(x)$. Since $p_\ell = p_{\ell,H}$ for all $\ell \in \mathbb{N}$ (by the definition of p_ℓ), this becomes

$$x = \sum_{\ell \in \mathbb{N}} \underbrace{p_{\ell,H}}_{=p_\ell}(x) = \sum_{\ell \in \mathbb{N}} p_\ell(x) = \sum_{\substack{\ell \in \mathbb{N}; \\ \ell \leq n}} p_\ell(x) + \sum_{\substack{\ell \in \mathbb{N}; \\ \ell > n}} p_\ell(x). \tag{122}$$

But for every $\ell \in \mathbb{N}$ satisfying $\ell > n$, we have $p_\ell\left(H_{\leq n}\right) = 0$. [74] Thus, for every $\ell \in \mathbb{N}$ satisfying $\ell > n$, we have $p_\ell(x) = 0$ (since $x \in H_{\leq n}$, and thus, for every $\ell \in \mathbb{N}$ satisfying $\ell > n$, we obtain $p_\ell(x) \in p_\ell\left(H_{\leq n}\right) = 0$, so that $p_\ell(x) = 0$). Thus, (122) becomes

$$x = \sum_{\substack{\ell \in \mathbb{N}; \\ \ell \leq n}} p_\ell(x) + \sum_{\substack{\ell \in \mathbb{N}; \\ \ell > n}} \underbrace{p_\ell(x)}_{=0} = \sum_{\substack{\ell \in \mathbb{N}; \\ \ell \leq n}} p_\ell(x) + \underbrace{\sum_{\substack{\ell \in \mathbb{N}; \\ \ell > n}} 0}_{=0} = \sum_{\substack{\ell \in \mathbb{N}; \\ \ell \leq n}} p_\ell(x) = p_0(x) + p_1(x) + \cdots + p_n(x) \tag{123}$$

$$= \underbrace{p_0}_{\substack{=e_{H,H} \\ \text{(by Proposition 16.25 (e),} \\ \text{since } H \text{ is connected)}}}(x) + \underbrace{\left(p_1(x) + p_2(x) + \cdots + p_n(x)\right)}_{=(p_1+p_2+\cdots+p_n)(x)} = e_{H,H}(x) + \left(p_1 + p_2 + \cdots + p_n\right)(x). \tag{124}$$

[74] *Proof.* By the definition of $H_{\leq n}$, we have

$$H_{\leq n} = \bigoplus_{\ell=0}^{n} H_\ell = \bigoplus_{m=0}^{n} H_m \qquad \text{(here, we renamed the summation index } \ell \text{ as } m\text{)}$$
$$= \sum_{m=0}^{n} H_m \qquad \text{(since direct sums are sums)}.$$

Thus,

$$(p_1+p_2+\cdots+p_n)(x) = \underbrace{x}_{=\mathrm{id}(x)} - e_{H,H}(x) = \mathrm{id}(x) - e_{H,H}(x) = \underbrace{(\mathrm{id} - e_{H,H})}_{=h}(x) = h(x).$$

This proves (121) for every $x \in H_{\leq n}$. Step **a)** is thus done.

b) Every $x \in H_{\leq n}$ and every $\ell \in \mathbb{N}$ satisfy

$$h^{*\ell}(x) = (p_1+p_2+\cdots+p_n)^{*\ell}(x). \tag{125}$$

Proof of (125). There are several ways to derive (125) from (121). Here is one of them:

Let $\ell \in \mathbb{N}$.

We are going to use the notation $\mathcal{L}^n(H,A)$ introduced in Definition 3.1 **(b)**.

By the definition of $\mathcal{L}^{n+1}(H,H)$, we have

$$\mathcal{L}^{n+1}(H,H) = \left\{ f \in \mathcal{L}(H,H) \ \mid \ \underbrace{f|_{H_{\leq n+1-1}}}_{=f|_{H_{\leq n}}} = 0 \right\} = \left\{ f \in \mathcal{L}(H,H) \ \mid \ f|_{H_{\leq n}} = 0 \right\}.$$

By Proposition 14.2 (applied to $n+1$ and H instead of n and A), the set $\mathcal{L}^{n+1}(H,H)$ is an ideal of the k-algebra $\mathcal{L}(H,H)$.

Every $x \in H_{\leq n}$ satisfies

$$\begin{aligned}(h-(p_1+p_2+\cdots+p_n))(x) &= \underbrace{h(x)}_{\substack{=(p_1+p_2+\cdots+p_n)(x) \\ \text{(by (121))}}} - (p_1+p_2+\cdots+p_n)(x) \\ &= (p_1+p_2+\cdots+p_n)(x) - (p_1+p_2+\cdots+p_n)(x) = 0.\end{aligned}$$

In other words, $(h-(p_1+p_2+\cdots+p_n))|_{H_{\leq n}} = 0$. Thus,

$$h-(p_1+p_2+\cdots+p_n) \in \left\{ f \in \mathcal{L}(H,H) \ \mid \ f|_{H_{\leq n}} = 0 \right\} = \mathcal{L}^{n+1}(H,H).$$

In other words, $h \equiv p_1+p_2+\cdots+p_n \bmod \mathcal{L}^{n+1}(H,H)$. Thus,

$$h^{*\ell} \equiv (p_1+p_2+\cdots+p_n)^{*\ell} \bmod \mathcal{L}^{n+1}(H,H)$$

Hence, for every $\ell \in \mathbb{N}$ satisfying $\ell > n$, we have

$$\begin{aligned}p_\ell(H_{\leq n}) &= p_\ell\left(\sum_{m=0}^{n} H_m\right) = \sum_{m=0}^{n} \underbrace{p_\ell(H_m)}_{=(p_\ell|_{H_m})(H_m)} \qquad \text{(since } p_\ell \text{ is } k\text{-linear)} \\ &= \sum_{m=0}^{n} \left(\underbrace{p_\ell}_{\substack{=p_{\ell,H} \\ \text{(by the definition of } H\text{)}}} |_{H_m} \right)(H_m) = \sum_{m=0}^{n} \underbrace{(p_{\ell,H}|_{H_m})}_{\substack{=0 \text{ (by (111) (applied} \\ \text{to } \ell \text{ and } H \text{ instead of } n \text{ and } V\text{)}, \\ \text{since } \ell \neq m \text{ (since } \ell > n \geq m\text{))}}} (H_m) \\ &= \sum_{m=0}^{n} 0(H_m) = 0,\end{aligned}$$

qed.

(because $\mathcal{L}^{n+1}(H,H)$ is an ideal of the k-algebra $\mathcal{L}(H,H)$, and hence we can multiply congruences modulo $\mathcal{L}^{n+1}(H,H)$). In other words,

$$h^{*\ell} - (p_1 + p_2 + \cdots + p_n)^{*\ell} \in \mathcal{L}^{n+1}(H,H) = \left\{ f \in \mathcal{L}(H,H) \mid f|_{H_{\leq n}} = 0 \right\},$$

so that $\left(h^{*\ell} - (p_1 + p_2 + \cdots + p_n)^{*\ell}\right)|_{H_{\leq n}} = 0$. Hence, every $x \in H_{\leq n}$ satisfies $\left(h^{*\ell} - (p_1 + p_2 + \cdots + p_n)^{*\ell}\right)(x) = 0$. As a consequence, every $x \in H_{\leq n}$ satisfies $h^{*\ell}(x) = (p_1 + p_2 + \cdots + p_n)^{*\ell}(x)$ (because

$$h^{*\ell}(x) - (p_1 + p_2 + \cdots + p_n)^{*\ell}(x) = \left(h^{*\ell} - (p_1 + p_2 + \cdots + p_n)^{*\ell}\right)(x) = 0$$

). In other words, (125) is proven for every $x \in H_{\leq n}$ and every $\ell \in \mathbb{N}$. This completes step **b)**.

c) Every $x \in H_{\leq n}$ satisfies

$$\zeta(x) = \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} h^{*\ell}(x). \tag{126}$$

Proof of (126). Since

$$\begin{aligned} \zeta &= \operatorname{Log} \mathrm{id} = \operatorname{Log}_1 \underbrace{(\mathrm{id} - e_{H,H})}_{=h} \qquad \text{(by the definition of Log)} \\ &= \operatorname{Log}_1 h, \end{aligned}$$

every $x \in H_{\leq n}$ satisfies

$$\begin{aligned} \zeta(x) &= (\operatorname{Log}_1 h)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} h^{*i}(x) \qquad \text{(by (8), applied to } f = h) \\ &= \sum_{\substack{i \geq 1; \\ i \leq n}} \frac{(-1)^{i-1}}{i} h^{*i}(x) + \sum_{\substack{i \geq 1; \\ i > n}} \frac{(-1)^{i-1}}{i} \underbrace{h^{*i}(x)}_{\substack{=0 \text{ (since } x \in H_{\leq n} \text{ and thus} \\ h^{*i}(x) \in h^{*i}\left(H_{\leq n}\right) = 0 \text{ (by Remark 3.5} \\ \text{(applied to } f=h\text{), since } i>n\text{),} \\ \text{so that } h^{*i}(x)=0\text{)}}} \\ &= \underbrace{\sum_{\substack{i \geq 1; \\ i \leq n}}}_{= \sum_{i=1}^{n}} \frac{(-1)^{i-1}}{i} h^{*i}(x) + \underbrace{\sum_{\substack{i \geq 1; \\ i > n}} \frac{(-1)^{i-1}}{i} 0}_{=0} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} h^{*i}(x) \\ &= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} h^{*\ell}(x) \qquad \text{(here, we renamed the summation index } i \text{ as } \ell). \end{aligned}$$

This proves (126), and thus our step **c)** is complete.

d) Every $x \in H_{\leq n}$ satisfies

$$\zeta(x) = \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{(a_1, a_2, \ldots, a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell})(x). \tag{127}$$

Proof of (127). Let $x \in H^n$. Then, for every $\ell \in \mathbb{N}$, we have

$$h^{*\ell}(x) = \underbrace{(p_1 + p_2 + \cdots + p_n)^{*\ell}}_{\substack{= \sum\limits_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} p_{a_1} * p_{a_2} * \cdots * p_{a_\ell} \\ \text{(by the product rule)}}} (x) \qquad \text{(by (125))}$$

$$= \left(\sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} p_{a_1} * p_{a_2} * \cdots * p_{a_\ell} \right)(x) = \sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x).$$

Now, (126) becomes

$$\zeta(x) = \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \underbrace{h^{*\ell}(x)}_{= \sum\limits_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x)}$$

$$= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x).$$

This proves (127).

e) Every $x \in H_n$ satisfies[75]

$$\zeta(x) = \left(\sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right) \right)(x). \tag{128}$$

Proof of (128). Let $x \in H_n$. Then, $\zeta(x) \in \zeta(H_n) \subseteq H_n$ (since ζ is graded (by Theorem 16.21 **(a)**)). Thus,

$$p_n(\zeta(x)) = \left(\underbrace{p_n}_{\substack{= p_{n,H} \\ \text{(by the definition of } p_n\text{)}}} |_{H_n} \right)(\zeta(x)) = \underbrace{\left(p_{n,H} \mid_{H_n}\right)}_{\substack{= \mathrm{id}_H|_{H_n} \\ \text{(by (110), applied to } V=H\text{)}}} (\zeta(x))$$

$$= \left(\mathrm{id}_H \mid_{H_n}\right)(\zeta(x)) = \mathrm{id}_H(\zeta(x)) = \zeta(x). \tag{129}$$

Since $H_{\leq n} = \bigoplus_{\ell=0}^{n} H_\ell$ by the definition of $H_{\leq n}$, we have $H_n \subseteq H_{\leq n}$ (since H_n is one addend of the direct sum $\bigoplus_{\ell=0}^{n} H_\ell$, and thus $H_n \subseteq \bigoplus_{\ell=0}^{n} H_\ell = H_{\leq n}$).

Now, (129) yields

$$\zeta(x) = p_n(\zeta(x)) = p_n\left(\sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x) \right)$$

(by (127), since $x \in H_n \subseteq H_{\leq n}$)

$$= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} p_n\left(\left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x)\right) \qquad \text{(since } p_n \text{ is } k\text{-linear)}.$$

[75] Note that here we require $x \in H_n$ rather than $x \in H_{\leq n}$.

Since every $\ell \in \{1,2,\ldots,n\}$ satisfies

$$\begin{aligned}
&\sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \underbrace{p_n\left(\left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x)\right)}_{=\left(p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)\right)(x)} \\
&= \sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \left(p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)\right)(x) \\
&= \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \underbrace{\left(p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)\right)}_{\substack{=p_{a_1} * p_{a_2} * \cdots * p_{a_\ell} \\ \text{(by Corollary 16.26 \textbf{(b)}, since} \\ n=a_1+a_2+\cdots+a_\ell)}}(x) \\
&\quad + \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n\neq a_1+a_2+\cdots+a_\ell}} \underbrace{\left(p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)\right)}_{\substack{=0 \\ \text{(by Corollary 16.26 \textbf{(a)}, since} \\ n\neq a_1+a_2+\cdots+a_\ell)}}(x) \\
&= \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x) + \underbrace{\sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n\neq a_1+a_2+\cdots+a_\ell}} 0\,(x)}_{=0} \\
&= \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x),
\end{aligned}$$

this rewrites as

$$\begin{aligned}
\zeta(x) &= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \underbrace{\sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} p_n\left(\left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x)\right)}_{= \sum\limits_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x)} \\
&= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)(x) \\
&= \left(\sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right) \right)(x).
\end{aligned}$$

This proves (128).

f) Now an auxiliary result:

$$\left(\begin{array}{c} \text{Whenever } f : H \to H \text{ and } g : H \to H \text{ are two graded maps} \\ \text{satisfying } \left(f(x) = g(x) \text{ for all } x \in H_n\right), \text{ then } p_n \circ f = p_n \circ g \end{array} \right). \tag{130}$$

Proof of (130). Let $f : H \to H$ and $g : H \to H$ be two graded maps satisfying $\left(f(x) = g(x) \text{ for all } x \in H_n\right)$.

Since f is graded, Proposition 16.17 (applied to $V = H$ and $W = H$) yields that $p_{n,H} \circ f = f \circ p_{n,H} = p_{n,H} \circ f \circ p_{n,H}$. Since $p_{n,H} = p_n$, this rewrites as $p_n \circ f = f \circ p_n = p_n \circ f \circ p_n$. The same argument done for g instead of f shows that $p_n \circ g = g \circ p_n = p_n \circ g \circ p_n$.

Since $p_n = p_{n,H}$, we have $p_n(H) = p_{n,H}(H) = H_n$ (by (112), applied to $V = H$).

For every $y \in H$, we have

$$(f \circ p_n)(y) = f(p_n(y)) = g(p_n(y))$$
$$\left(\begin{array}{c} \text{this follows from the assumption that } (f(x) = g(x) \text{ for all } x \in H_n), \\ \text{applied to } x = p_n(y) \text{ (because } p_n(y) \in p_n(H) = H_n) \end{array} \right)$$
$$= (g \circ p_n)(y).$$

Thus, $f \circ p_n = g \circ p_n$, so that $p_n \circ f = f \circ p_n = g \circ p_n = p_n \circ g$. This proves (130).

g) We have

$$\zeta_n = \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}). \tag{131}$$

Proof of (131). For every $\ell \in \{1, 2, \ldots, n\}$ and every $(a_1, a_2, \ldots, a_\ell) \in \{1, 2, \ldots, n\}^{\times \ell}$, the map $p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}$ is graded[76]. Hence, the map

$$\sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell})$$

is graded (since a k-linear combination of graded maps is always graded). Also, ζ is graded (by Theorem 16.21 **(a)**). The two latter facts, along with the fact that

$$\zeta(x) = \left(\sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) \right)(x)$$

for all $x \in H_n$ (by (128)), show that we can apply (130) to $f = \zeta$ and $g = \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell})$. As a result, we conclude that

$$p_n \circ \zeta = p_n \circ \left(\sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) \right).$$

[76] *Proof.* Let $\ell \in \{1, 2, \ldots, n\}$ and $(a_1, a_2, \ldots, a_\ell) \in \{1, 2, \ldots, n\}^{\times \ell}$. Then, for every $i \in \{1, 2, \ldots, \ell\}$, the map p_{a_i} is graded and concentrated in degree a_i (by Proposition 16.25 **(d)**, applied to a_i instead of n). Hence, by Proposition 16.25 **(c)** (applied to $f_i = p_{a_i}$), the map $p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_\ell$, qed.

Using this identity, we have

$$\begin{aligned}
\zeta_n &= p_n \circ \zeta \qquad \text{(by (117))} \\
&= p_n \circ \left(\sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right) \right) \\
&= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \underbrace{\left(p_n \circ \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right)\right)}_{\substack{=p_{a_1}*p_{a_2}*\cdots*p_{a_\ell} \\ \text{(by Corollary 16.26 \textbf{(b)}, since} \\ n=a_1+a_2+\cdots+a_\ell)}} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right).
\end{aligned}$$

This proves (131).

h) Now let us finally prove the claim of Proposition 16.22; this claims states that $p_n - \zeta_n \in \operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_{n-1}\}$.

In fact, first we assume that $n \neq 0$, because in the case $n = 0$ this is very easy[77].

Now, it is very easy to see that

$$\left(\begin{array}{c} \text{for every } \ell \in \{2,3,\ldots,n\} \text{ and every } (a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times\ell} \\ \text{satisfying } n = a_1 + a_2 + \cdots + a_\ell, \text{ we have} \\ p_{a_1} * p_{a_2} * \cdots * p_{a_\ell} \in \operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_{n-1}\} \end{array} \right). \tag{132}$$

[77] *Proof.* Assume that $n = 0$. Then, $p_n = p_0 = e_{H,H}$ (by Proposition 16.25 **(e)**, since H is connected). Also, by (131), we have

$$\begin{aligned}
\zeta_n &= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}\right) = (\text{empty sum}) \qquad (\text{since } n = 0) \\
&= 0.
\end{aligned}$$

Thus,

$$\underbrace{p_n}_{=e_{H,H}} - \underbrace{\zeta_n}_{=0} = e_{H,H} = (\text{unity of the } k\text{-algebra } \mathcal{L}(H,H)) \in \operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_{n-1}\}.$$

Thus, the claim of Proposition 16.22 is proven in the case $n = 0$.

[78] *Proof of (132).* Let $\ell \in \{2,3,\ldots,n\}$ and $(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times\ell}$ satisfy $n = a_1 + a_2 + \cdots + a_\ell$. Then, a_1, a_2, ..., a_ℓ are elements of the set $\{1,2,\ldots,n\}$ and therefore positive integers. In other words, a_i is a positive integer for every $i \in \{1,2,\ldots,\ell\}$. Also, $\ell \in \{2,3,\ldots,n\}$, so that $\ell \geq 2$. Hence, for every $i \in \{1,2,\ldots,\ell\}$, the set $\{j \in \{1,2,\ldots,\ell\};\ j \neq i\}$ is nonempty. Thus, for every $i \in \{1,2,\ldots,\ell\}$, the sum $\sum_{\substack{j\in\{1,2,\ldots,\ell\}; \\ j\neq i}} a_j$ is nonempty. Since all addends of this sum are positive (because a_1, a_2, ..., a_ℓ are positive), this sum $\sum_{\substack{j\in\{1,2,\ldots,\ell\}; \\ j\neq i}} a_j$ is therefore > 0. Now, for every

Now that we have assumed that $n \neq 0$, we have

$$\begin{aligned}
\zeta_n &= \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) \qquad \text{(by (131))} \\
&= \underbrace{\frac{(-1)^{1-1}}{1}}_{=\frac{1}{1}=1} \underbrace{\sum_{\substack{(a_1,a_2,\ldots,a_1)\in\{1,2,\ldots,n\}^{\times 1}; \\ n=a_1+a_2+\cdots+a_1}} (p_{a_1} * p_{a_2} * \cdots * p_{a_1})}_{= \sum\limits_{\substack{(a_1)\in\{1,2,\ldots,n\}^{\times 1}; \\ n=a_1}} p_{a_1} = \sum\limits_{\substack{a_1\in\{1,2,\ldots,n\}; \\ n=a_1}} p_{a_1} = p_n} \\
&\qquad + \sum_{\ell=2}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \underbrace{(p_{a_1} * p_{a_2} * \cdots * p_{a_\ell})}_{\in \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\} \text{ (by (132))}} \\
&\in p_n + \underbrace{\sum_{\ell=2}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}}_{\subseteq \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\} \text{ (since } \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\} \text{ is a } k\text{-vector space)}} \\
&\subseteq p_n + \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\},
\end{aligned}$$

so that

$$\zeta_n - p_n \in \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}.$$

Hence,

$$p_n - \zeta_n = -\underbrace{(\zeta_n - p_n)}_{\in \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}} \in -\operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\} \subseteq \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}$$

(since $\operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}$ is a k-vector space). This proves Proposition 16.22. □

The step from Proposition 16.22 to Proposition 16.23 and Theorem 16.21 is a purely formal one, and formalized in the following lemma:

Lemma 16.27. Let k be a field. Let A be a k-algebra. Let $(x_1, x_2, x_3, \ldots)$ and $(y_1, y_2, y_3, \ldots)$ be two sequences of elements of A. Assume that

$$x_n - y_n \in \operatorname{AlgGen}_k\{x_1, x_2, \ldots, x_{n-1}\} \tag{133}$$

$i \in \{1,2,\ldots,\ell\}$, we have

$$n = a_1 + a_2 + \cdots + a_\ell = \sum_{j\in\{1,2,\ldots,\ell\}} a_j = \underbrace{\sum_{\substack{j\in\{1,2,\ldots,\ell\}; \\ j\neq i}} a_j}_{>0} + a_i > a_i.$$

Thus, for every $i \in \{1,2,\ldots,\ell\}$, we have $a_i \in \{1,2,\ldots,n-1\}$ (since a_i is a positive integer satisfying $a_i < n$) and thus $p_{a_i} \in \{p_1,p_2,\ldots,p_{n-1}\} \subseteq \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}$. Hence, $p_{a_1} * p_{a_2} * \cdots * p_{a_\ell} \in \operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}$ (because the product of elements of $\operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}$ always lies in $\operatorname{AlgGen}_k\{p_1,p_2,\ldots,p_{n-1}\}$). This proves (132).

for every positive integer n.

(a) Then, every $n \in \mathbb{N}$ satisfies

$$\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_n\} = \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_n\}.$$

(b) Besides,

$$\operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\} = \operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}.$$

Proof of Lemma 16.27. **(a)** Let us prove Lemma 16.27 **(a)** by induction over n:

Induction base: For $n = 0$, both sets $\{x_1, x_2, \ldots, x_n\}$ and $\{y_1, y_2, \ldots, y_n\}$ are empty, and thus $\{x_1, x_2, \ldots, x_n\} = \{y_1, y_2, \ldots, y_n\}$, so that $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_n\} = \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_n\}$. Thus, Lemma 16.27 **(a)** is true if $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$ be positive. Assume that Lemma 16.27 **(a)** holds for $n = N - 1$. We now must prove that Lemma 16.27 **(a)** also holds for $n = N$.

The assumption (133) (applied to $n = N$) yields

$$x_N - y_N \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_{N-1}\}. \tag{134}$$

Since Lemma 16.27 **(a)** holds for $n = N-1$, we have $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_{N-1}\} = \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_{N-1}\}$. Thus, (134) becomes $x_N - y_N \in \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_{N-1}\}$. Hence,

$$\begin{aligned} y_N - x_N &= - \underbrace{(x_N - y_N)}_{\in \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_{N-1}\}} \in - \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_{N-1}\} \\ &= \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_{N-1}\} \end{aligned} \tag{135}$$

(since $\operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_{N-1}\}$ is a k-vector space).

From (134), we have

$$\begin{aligned} y_N &\in \underbrace{x_N}_{\in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}} - \operatorname{AlgGen}_k \underbrace{\{x_1, x_2, \ldots, x_{N-1}\}}_{\subseteq \{x_1, x_2, \ldots, x_N\}} \\ &\subseteq \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\} - \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\} \subseteq \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\} \end{aligned}$$

(since $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ is a k-vector space).

Now, it is easy to see that every $i \in \{1, 2, \ldots, N\}$ satisfies $y_i \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ [79]. Thus, $\{y_1, y_2, \ldots, y_N\} \subseteq \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$. In other words, $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$

[79] *Proof.* Let $i \in \{1, 2, \ldots, N\}$. Then, only two cases are possible:

Case 1: We have $i \neq N$.

Case 2: We have $i = N$.

First let us consider Case 1. In this case, $i \in \{1, 2, \ldots, N\}$ but $i \neq N$; thus, $i \in \{1, 2, \ldots, N-1\}$, so that

$$\begin{aligned} y_i &\in \{y_1, y_2, \ldots, y_{N-1}\} \subseteq \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_{N-1}\} = \operatorname{AlgGen}_k \underbrace{\{x_1, x_2, \ldots, x_{N-1}\}}_{\subseteq \{x_1, x_2, \ldots, x_N\}} \\ &\subseteq \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}. \end{aligned}$$

Thus, $y_i \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ is proven in Case 1.

In Case 2, we have $i = N$ and thus $y_i = y_N \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$. Thus, $y_i \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ is also proven in Case 2.

Hence, $y_i \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ is proven in both cases 1 and 2. Since these two cases are the only ones possible, this yields that $y_i \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ always holds, qed.

contains $\{y_1, y_2, \ldots, y_N\}$ as a subset. Hence, $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ is a k-subalgebra of A containing $\{y_1, y_2, \ldots, y_N\}$ as a subset[80].

But we know that $\operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\}$ is the smallest k-subalgebra of A containing $\{y_1, y_2, \ldots, y_N\}$ as a subset. This means that whenever U is a k-subalgebra of A containing $\{y_1, y_2, \ldots, y_N\}$ as a subset, we must necessarily have $\operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\} \subseteq U$. Applied to $U = \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$, this yields that $\operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\} \subseteq \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$.

So we have proven $\operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\} \subseteq \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$. But the same argument, with the sequences $(x_1, x_2, x_3, \ldots)$ and $(y_1, y_2, y_3, \ldots)$ interchanged (and using the equality (135) instead of (134)), shows that $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\} \subseteq \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\}$.

Combining $\operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\} \subseteq \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ and $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\} \subseteq \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\}$, we obtain $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\} = \operatorname{AlgGen}_k \{y_1, y_2, \ldots, y_N\}$. In other words, Lemma 16.27 **(a)** holds for $n = N$. This completes the induction step.

Thus, the induction proof of Lemma 16.27 **(a)** is complete.

(b) For every positive integer n, we have

$$x_n \in \operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_n\} = \operatorname{AlgGen}_k \underbrace{\{y_1, y_2, \ldots, y_n\}}_{\subseteq \{y_1, y_2, y_3, \ldots\}} \qquad \text{(by Lemma 16.27 (a))}$$

$$\subseteq \operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}.$$

In other words, $\{x_1, x_2, x_3, \ldots\} \subseteq \operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$. In other words, $\operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$ contains $\{x_1, x_2, x_3, \ldots\}$ as a subset. Thus, $\operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$ is a k-subalgebra of A containing $\{x_1, x_2, x_3, \ldots\}$ as a subset[81].

But we know that $\operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\}$ is the smallest k-subalgebra of A containing $\{x_1, x_2, x_3, \ldots\}$ as a subset. This means that whenever U is a k-subalgebra of A containing $\{x_1, x_2, x_3, \ldots\}$ as a subset, we must necessarily have $\operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\} \subseteq U$. Applied to $U = \operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$, this yields that $\operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\} \subseteq \operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$. The same argument, but with the sequences $(x_1, x_2, x_3, \ldots)$ and $(y_1, y_2, y_3, \ldots)$ interchanged, shows that $\operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\} \subseteq \operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\}$.

Combining $\operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\} \subseteq \operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$ with $\operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\} \subseteq \operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\}$, we obtain $\operatorname{AlgGen}_k \{x_1, x_2, x_3, \ldots\} = \operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$. This proves Lemma 16.27 **(b)**. □

Proof of Proposition 16.23. We have

$$p_n - \zeta_n \in \operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_{n-1}\}$$

for every $n \in \mathbb{N}$ (by Proposition 16.22). Thus, Lemma 16.27 **(a)** (applied to $A = \mathcal{L}(H, H)$, $(x_1, x_2, x_3, \ldots) = (p_1, p_2, p_3, \ldots)$ and $(y_1, y_2, y_3, \ldots) = (\zeta_1, \zeta_2, \zeta_3, \ldots)$) yields that every $n \in \mathbb{N}$ satisfies $\operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_n\} = \operatorname{AlgGen}_k \{\zeta_1, \zeta_2, \ldots, \zeta_n\}$. This proves Proposition 16.23. □

Proof of Theorem 16.21, second part. We have already proven Theorem 16.21 **(a)** and (117). Thus, the only thing we still need to do is proving (118).

[80] because $\operatorname{AlgGen}_k \{x_1, x_2, \ldots, x_N\}$ is clearly a k-subalgebra of A

[81] since $\operatorname{AlgGen}_k \{y_1, y_2, y_3, \ldots\}$ clearly is a k-subalgebra of A

We have

$$p_n - \zeta_n \in \operatorname{AlgGen}_k \{p_1, p_2, \ldots, p_{n-1}\}$$

for every $n \in \mathbb{N}$ (by Proposition 16.22). Thus, Lemma 16.27 **(b)** (applied to $A = \mathcal{L}(H, H)$, $(x_1, x_2, x_3, \ldots) = (p_1, p_2, p_3, \ldots)$ and $(y_1, y_2, y_3, \ldots) = (\zeta_1, \zeta_2, \zeta_3, \ldots)$) yields that $\operatorname{AlgGen}_k \{p_1, p_2, p_3, \ldots\} = \operatorname{AlgGen}_k \{\zeta_1, \zeta_2, \zeta_3, \ldots\}$. This proves (118). This completes the proof of Theorem 16.21. □

§17. The surjectivity part of Cartier-Milnor-Moore

In this Section §17, we are going to continue what we began this paper with: namely, studying cocommutative connected filtered bialgebras and the properties of $\operatorname{Log} \mathrm{id}$ therein. Our first goal in §17 is to derive the following corollary from Theorem 4.1:

Theorem 17.1. Let k be a field of characteristic 0, and let H be a connected filtered cocommutative bialgebra over k. Then, $H = \operatorname{AlgGen}_k (\operatorname{Prim} H)$, where $\operatorname{Prim} H$ denotes the set of all primitive elements of H.

Note that this theorem is often worded as follows: A connected filtered cocommutative bialgebra over a field of characteristic 0 is always primitively generated.

Note also that Theorem 17.1 can be seen as one part of the so-called *Cartier-Milnor-Moore theorem*, which we are going to prove later (in §34):

Theorem 17.2 (the Cartier-Milnor-Moore theorem)**.** Let k be a field of characteristic 0, and let H be a connected filtered cocommutative bialgebra over k. Let $\operatorname{Prim} H$ denote the set of all primitive elements of H. For every Lie algebra $\mathfrak{g}$, let $U(\mathfrak{g})$ denote the universal enveloping algebra of $\mathfrak{g}$. Then, the canonical k-algebra homomorphism $U(\operatorname{Prim} H) \to H$ (which is obtained from the inclusion map $\operatorname{Prim} H \to H$ via the universal property of the universal enveloping algebra) is an isomorphism of k-bialgebras.

Theorem 17.1 shows that the canonical k-algebra homomorphism $U(\operatorname{Prim} H) \to H$ in Theorem 17.2 is surjective. Injectivity (and being a homomorphism of k-bialgebras) will be proven in §34.

We are going to show something stronger than Theorem 17.1:

Proposition 17.3. Let k be a field of characteristic 0, and let H be a connected filtered cocommutative bialgebra over k. Then,

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} (\operatorname{Prim} H)^i \qquad \text{for every } \ell \in \mathbb{N}.$$

82

Actually, we shall show a somewhat more general fact:

[82] Recall that $(\operatorname{Prim} H)^i$ means the i-th power of the subspace $\operatorname{Prim} H$ of the k-algebra H as explained in Convention 15.2.

Proposition 17.4. Let k be a field of characteristic 0, and let H be a connected filtered bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. Let $\mathfrak{e}$ denote the map $\operatorname{Log} \mathrm{id} \in \mathcal{L}(H, H)$. Let $\mathfrak{E}$ be the k-vector subspace $\mathfrak{e}(H)$ of H. Then,

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} \mathfrak{E}^i \qquad \text{for every } \ell \in \mathbb{N}.$$

[83]

This will be proven by induction over ℓ, but before we start this proof, we need a very basic concept:

Definition 17.5. Let k be a field. Let V and W be two filtered k-vector spaces. Let $f : V \to W$ be a k-linear map. We say that the map f *respects the filtration* if and only if $(f(V_{\leq n}) \subseteq W_{\leq n}$ for every $n \in \mathbb{N})$.

First some very basic properties of this notion:

Remark 17.6. Let k be a field. Let V and W be two filtered k-vector spaces.

(a) The map $0 : V \to W$ (which sends every $v \in V$ to 0) respects the filtration.

(b) If a k-linear map $f : V \to W$ respects the filtration, and if λ is an element of k, then λf respects the filtration as well.

(c) If $f : V \to W$ and $g : V \to W$ are two k-linear maps respecting the filtration, then $f + g$ also respects the filtration.

(d) The set of all k-linear maps $V \to W$ respecting the filtration is a k-vector subspace of $\mathcal{L}(V, W)$.

This remark is a well-known fact from basic algebra and has not much to do with Hopf algebras. Purely for the sake of completeness, we prove part of it:

Proof of Remark 17.6. **(a)** For every $n \in \mathbb{N}$, the map $0 : V \to W$ satisfies $0(V_{\leq n}) = 0 \subseteq W_{\leq n}$. Thus, the map $0 : V \to W$ respects the filtration. This proves Remark 17.6 **(a)**.

(b) Let $f : V \to W$ be a k-linear map respecting the filtration. Let $\lambda \in k$. Then, $f(V_{\leq n}) \subseteq W_{\leq n}$ for every $n \in \mathbb{N}$ (since f respects the filtration). Now, $(\lambda f)(V_{\leq n}) = \lambda \underbrace{f(V_{\leq n})}_{\subseteq W_{\leq n}} \subseteq \lambda W_{\leq n} \subseteq W_{\leq n}$ (since $W_{\leq n}$ is a k-vector space) for every $n \in \mathbb{N}$. In other words, λf respects the filtration. This proves Remark 17.6 **(b)**.

(c) Let $f : V \to W$ and $g : V \to W$ be two k-linear maps respecting the filtration. Then, $f(V_{\leq n}) \subseteq W_{\leq n}$ for every $n \in \mathbb{N}$ (since f respects the filtration). Also, $g(V_{\leq n}) \subseteq W_{\leq n}$ for every $n \in \mathbb{N}$ (since g respects the filtration). Now,

$$(f+g)(V_{\leq n}) \subseteq \underbrace{f(V_{\leq n})}_{\subseteq W_{\leq n}} + \underbrace{g(V_{\leq n})}_{\subseteq W_{\leq n}} \subseteq W_{\leq n} + W_{\leq n} \subseteq W_{\leq n}$$

[83] Recall that $\mathfrak{E}^i$ means the i-th power of the subspace $\mathfrak{E}$ of the k-algebra H as explained in Convention 15.2.

(since $W_{\leq n}$ is a k-vector space) for every $n \in \mathbb{N}$. In other words, $f+g$ respects the filtration. This proves Remark 17.6 **(c)**.

(d) The set of all k-linear maps $V \to W$ respecting the filtration is obviously a subset of $\mathcal{L}(V,W)$. But we also know that this subset contains 0 (by Remark 17.6 **(a)**), is closed under multiplication with every $\lambda \in k$ (by Remark 17.6 **(b)**), and is closed under addition (by Remark 17.6 **(c)**). Hence, this subset is a k-vector subspace of $\mathcal{L}(V,W)$. This proves Remark 17.6 **(d)**. □

Proposition 17.7. Let k be a field. Let C be a connected filtered k-coalgebra. Let A be a k-algebra. If $f \in \mathfrak{g}(C,A)$ and $g \in \mathfrak{g}(C,A)$ are two k-linear maps, then

$$(f*g)(C_{\leq \ell}) \subseteq \sum_{u=1}^{\ell-1} f(C_{\leq u})\, g(C_{\leq \ell-u}) \qquad \text{for every positive } \ell \in \mathbb{N}.$$

Proof of Proposition 17.7. Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$.

By the definition of $\mathfrak{g}(C,A)$, we have

$$\mathfrak{g}(C,A) = \{f \in \mathcal{L}(C,A) \mid f(1_C) = 0\} = \{h \in \mathcal{L}(C,A) \mid h(1_C) = 0\}$$

(here we renamed f as h).

Let $f \in \mathfrak{g}(C,A)$ and $g \in \mathfrak{g}(C,A)$ be two k-linear maps. Let $\ell \in \mathbb{N}$ be positive.

Since $f \in \mathfrak{g}(C,A) = \{h \in \mathcal{L}(C,A) \mid h(1_C) = 0\}$, we have $f(1_C) = 0$. But Remark 2.11 gives $C_{\leq 0} = k \cdot 1_C$, so that

$$\begin{aligned} f(C_{\leq 0}) &= f(k \cdot 1_C) = k \cdot \underbrace{f(1_C)}_{=0} \qquad \text{(since } f \text{ is } k\text{-linear)} \\ &= k \cdot 0 = 0. \end{aligned}$$

The same argument (applied to g instead of f) shows that $g(C_{\leq 0}) = 0$.

Now,

$$\begin{aligned} &\Delta_C(C_{\leq \ell}) \\ &\subseteq \sum_{u=0}^{\ell} C_{\leq u} \otimes C_{\leq \ell-u} \qquad \text{(since } C \text{ is a filtered coalgebra)} \\ &= C_{\leq 0} \otimes \underbrace{C_{\leq \ell-0}}_{=C_{\leq \ell}} + \sum_{u=1}^{\ell-1} C_{\leq u} \otimes C_{\leq \ell-u} + C_{\leq \ell} \otimes \underbrace{C_{\leq \ell-\ell}}_{=C_{\leq 0}} \\ &\qquad \left(\begin{array}{c} \text{here, we have split off the addend for } u=0 \text{ and the} \\ \text{addend for } u=\ell \text{ from the sum (since } \ell > 0) \end{array} \right) \\ &= C_{\leq 0} \otimes C_{\leq \ell} + \sum_{u=1}^{\ell-1} C_{\leq u} \otimes C_{\leq \ell-u} + C_{\leq \ell} \otimes C_{\leq 0}. \end{aligned}$$

Applying the map $f \otimes g$ to both sides of this relation, we obtain

$$\begin{aligned}
&(f \otimes g)\left(\Delta_C\left(C_{\leq \ell}\right)\right) \\
&\subseteq (f \otimes g)\left(C_{\leq 0} \otimes C_{\leq \ell} + \sum_{u=1}^{\ell-1} C_{\leq u} \otimes C_{\leq \ell-u} + C_{\leq \ell} \otimes C_{\leq 0}\right) \\
&\subseteq \underbrace{(f \otimes g)\left(C_{\leq 0} \otimes C_{\leq \ell}\right)}_{\subseteq f\left(C_{\leq 0}\right) \otimes g\left(C_{\leq \ell}\right)} + \sum_{u=1}^{\ell-1} \underbrace{(f \otimes g)\left(C_{\leq u} \otimes C_{\leq \ell-u}\right)}_{\subseteq f\left(C_{\leq u}\right) \otimes g\left(C_{\leq \ell-u}\right)} + \underbrace{(f \otimes g)\left(C_{\leq \ell} \otimes C_{\leq 0}\right)}_{\subseteq f\left(C_{\leq \ell}\right) \otimes g\left(C_{\leq 0}\right)} \\
&\qquad \text{(since } f \otimes g \text{ is } k\text{-linear)} \\
&\subseteq \underbrace{f\left(C_{\leq 0}\right)}_{=0} \otimes g\left(C_{\leq \ell}\right) + \sum_{u=1}^{\ell-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq \ell-u}\right) + f\left(C_{\leq \ell}\right) \otimes \underbrace{g\left(C_{\leq 0}\right)}_{=0} \\
&\subseteq \underbrace{0 \otimes g\left(C_{\leq \ell}\right)}_{=0} + \sum_{u=1}^{\ell-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq \ell-u}\right) + \underbrace{f\left(C_{\leq \ell}\right) \otimes 0}_{=0} = \sum_{u=1}^{\ell-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq \ell-u}\right).
\end{aligned}$$

Now, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$, so that

$$\begin{aligned}
(f * g)\left(C_{\leq \ell}\right) &= \left(\mu_A \circ (f \otimes g) \circ \Delta_C\right)\left(C_{\leq \ell}\right) = \mu_A\left(\underbrace{(f \otimes g)\left(\Delta_C\left(C_{\leq \ell}\right)\right)}_{\subseteq \sum_{u=1}^{\ell-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq \ell-u}\right)}\right) \\
&\subseteq \mu_A\left(\sum_{u=1}^{\ell-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq \ell-u}\right)\right) \\
&\subseteq \sum_{u=1}^{\ell-1} \underbrace{\mu_A\left(f\left(C_{\leq u}\right) \otimes g\left(C_{\leq \ell-u}\right)\right)}_{\substack{= f\left(C_{\leq u}\right) g\left(C_{\leq \ell-u}\right) \\ \text{(by (74), applied to} \\ U = f\left(C_{\leq u}\right) \text{ and } V = g\left(C_{\leq \ell-u}\right))}} \qquad \text{(since } \mu_A \text{ is } k\text{-linear)} \\
&= \sum_{u=1}^{\ell-1} f\left(C_{\leq u}\right) g\left(C_{\leq \ell-u}\right).
\end{aligned}$$

This proves Proposition 17.7. □

Now we shall show some facts about maps respecting the filtration:

Proposition 17.8. Let k be a field. Let C be a filtered k-coalgebra. Let A be a filtered k-algebra.

(a) The map $e_{C,A} : C \to A$ respects the filtration.

(b) If $f : C \to A$ and $g : C \to A$ are two k-linear maps respecting the filtration, then $f * g$ also respects the filtration.

(c) If $f : C \to A$ is a k-linear map respecting the filtration, and if n is a nonnegative integer, then f^{*n} also respects the filtration.

(d) If the filtered k-coalgebra C is connected, and if $f \in \mathfrak{g}(C, A)$ and $g \in \mathfrak{g}(C, A)$ are two k-linear maps respecting the filtration, then

$$(f * g)(C_{\leq \ell}) \subseteq \sum_{u=1}^{\ell-1} A_{\leq u} A_{\leq \ell - u} \qquad \text{for every positive } \ell \in \mathbb{N}. \tag{136}$$

Proof of Proposition 17.8. Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$.

Since A is filtered, we have $A_{\leq 0} \subseteq A_{\leq 1} \subseteq A_{\leq 2} \subseteq \cdots$. Since A is a filtered k-algebra, we also have $1_A \in A_{\leq 0}$ and

$$A_{\leq a} A_{\leq b} \subseteq A_{\leq a+b} \qquad \text{for any } a \in \mathbb{N} \text{ and } b \in \mathbb{N}. \tag{137}$$

(a) Now, for every $x \in C$, we have

$$\underbrace{e_{C,A}}_{=\eta_A \circ \varepsilon_C}(x) = (\eta_A \circ \varepsilon_C)(x) = \eta_A(\varepsilon_C(x)) = \varepsilon_C(x) \cdot \underbrace{1_A}_{\in A_{\leq 0}} \qquad \text{(by the definition of } \eta_A\text{)}$$
$$\in \varepsilon_C(x) \cdot A_{\leq 0} \subseteq A_{\leq 0} \qquad \text{(since } A_{\leq 0} \text{ is a } k\text{-vector space)}.$$

In other words, $e_{C,A}(C) \subseteq A_{\leq 0}$. Hence, for every $n \in \mathbb{N}$, we have $e_{C,A}\left(\underbrace{C_{\leq n}}_{\subseteq C}\right) \subseteq e_{C,A}(C) \subseteq A_{\leq 0} \subseteq A_{\leq n}$ (since $0 \leq n$ and $A_{\leq 0} \subseteq A_{\leq 1} \subseteq A_{\leq 2} \subseteq \cdots$). In other words, $e_{C,A}$ respects the filtration. This proves Proposition 17.8 **(a)**.

(b) Let $f : C \to A$ and $g : C \to A$ be two k-linear maps respecting the filtration. Then,

$$f(C_{\leq n}) \subseteq A_{\leq n} \qquad \text{for every } n \in \mathbb{N} \tag{138}$$

(since f respects the filtration), and

$$g(C_{\leq n}) \subseteq A_{\leq n} \qquad \text{for every } n \in \mathbb{N} \tag{139}$$

(since g respects the filtration).

Let $n \in \mathbb{N}$. Let $x \in C_{\leq n}$ be arbitrary. Then,

$$\Delta(x) \in \Delta(C_{\leq n}) \subseteq \sum_{u=0}^{n} C_{\leq u} \otimes C_{\leq n-u} \qquad \text{(since } C \text{ is a filtered coalgebra)},$$

so that

$$(f \otimes g)(\Delta(x)) \in (f \otimes g)\left(\sum_{u=0}^{n} C_{\leq u} \otimes C_{\leq n-u}\right) \subseteq \sum_{u=0}^{n} \underbrace{(f \otimes g)(C_{\leq u} \otimes C_{\leq n-u})}_{\subseteq f\left(C_{\leq u}\right) \otimes g\left(C_{\leq n-u}\right)}$$
$$\text{(since } f \otimes g \text{ is } k\text{-linear)}$$
$$\subseteq \sum_{u=0}^{n} \underbrace{f(C_{\leq u})}_{\substack{\subseteq A_{\leq u} \\ \text{(by (138), applied to } u \\ \text{instead of } n\text{)}}} \otimes \underbrace{g(C_{\leq n-u})}_{\substack{\subseteq A_{\leq n-u} \\ \text{(by (139), applied to } n-u \\ \text{instead of } n\text{)}}} \subseteq \sum_{u=0}^{n} A_{\leq u} \otimes A_{\leq n-u}.$$

Now, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$ (by the definition of convolution), so that

$$(f * g)(x) = (\mu_A \circ (f \otimes g) \circ \Delta_C)(x) = \mu_A \left((f \otimes g) \underbrace{(\Delta_C(x))}_{=\Delta(x)} \right)$$

$$= \mu_A \left(\underbrace{(f \otimes g)(\Delta(x))}_{\in \sum_{u=0}^{n} A_{\leq u} \otimes A_{\leq n-u}} \right) \in \mu_A \left(\sum_{u=0}^{n} A_{\leq u} \otimes A_{\leq n-u} \right) \subseteq \sum_{u=0}^{n} \underbrace{\mu_A (A_{\leq u} \otimes A_{\leq n-u})}_{\substack{=A_{\leq u} A_{\leq n-u} \\ \text{(by (74), applied to} \\ U = A_{\leq u} \text{ and } V = A_{\leq n-u})}}$$

(since μ_A is k-linear)

$$= \sum_{u=0}^{n} \underbrace{A_{\leq u} A_{\leq n-u}}_{\substack{\subseteq A_{\leq u+(n-u)} \\ \text{(by (137), applied to } a=u \text{ and } b=n-u)}} \subseteq \sum_{u=0}^{n} \underbrace{A_{\leq u+(n-u)}}_{=A_{\leq n}} = \sum_{u=0}^{n} A_{\leq n} \subseteq A_{\leq n}$$

(since $A_{\leq n}$ is a k-vector space).

Now forget that we fixed x. We thus have proven that $(f * g)(x) \in A_{\leq n}$ for every $x \in C_{\leq n}$. In other words, $(f * g)(C_{\leq n}) \subseteq A_{\leq n}$.

Now forget that we fixed n. We thus have proven that $(f * g)(C_{\leq n}) \subseteq A_{\leq n}$ for every $n \in \mathbb{N}$. In other words, $f * g$ respects the filtration. This proves Proposition 17.8 **(b)**.

(c) We are going to prove Proposition 17.8 **(c)** by induction over n:

Induction base: For any k-linear map $f : C \to A$, the map f^{*0} respects the filtration (since $f^{*0} = e_{C,A}$, and since $e_{C,A}$ respects the filtration by Proposition 17.8 **(a)**). In other words, Proposition 17.8 **(c)** holds for $n = 0$. This completes the induction base.

Induction base: Let $N \in \mathbb{N}$. Assume that Proposition 17.8 **(c)** holds for $n = N$. We now must prove that Proposition 17.8 **(c)** holds for $n = N + 1$.

Let $f : C \to A$ be a k-linear map respecting the filtration. Then, f^{*N} respects the filtration (by Proposition 17.8 **(c)**). Hence, $f * f^{*N}$ respects the filtration (by Proposition 17.8 **(b)**, applied to $g = f^{*N}$). Since $f * f^{*N} = f^{*(N+1)}$, this rewrites as follows: The map $f^{*(N+1)}$ respects the filtration. In other words, Proposition 17.8 **(c)** holds for $n = N + 1$. This completes the induction step.

The induction proof of Proposition 17.8 **(c)** is thus complete.

(d) Assume that the filtered k-coalgebra C is connected. Let $f \in \mathfrak{g}(C, A)$ and $g \in \mathfrak{g}(C, A)$ be two k-linear maps respecting the filtration. Let $\ell \in \mathbb{N}$ be positive.

Note that we have (138) (since f respects the filtration) and (139) (since g respects the filtration).

Proposition 17.7 yields

$$(f * g)(C_{\leq \ell}) \subseteq \sum_{u=1}^{\ell-1} \underbrace{f(C_{\leq u})}_{\substack{\subseteq A_{\leq u} \\ \text{(by (138), applied to } u \\ \text{instead of } n)}} \underbrace{g(C_{\leq \ell-u})}_{\substack{\subseteq A_{\leq \ell-u} \\ \text{(by (139), applied to } \ell-u \\ \text{instead of } n)}} \subseteq \sum_{u=1}^{\ell-1} A_{\leq u} A_{\leq \ell-u}.$$

This proves Proposition 17.8 **(d)**. □

On a sidenote, in the above proof of Proposition 17.7, we saw that

$$\Delta_C\left(C_{\leq \ell}\right) \subseteq C_{\leq 0} \otimes C_{\leq \ell} + \sum_{u=1}^{\ell-1} C_{\leq u} \otimes C_{\leq \ell-u} + C_{\leq \ell} \otimes C_{\leq 0} \qquad \text{for every positive } \ell \in \mathbb{N}$$

when C is a connected filtered k-coalgebra. This is a useful fact, but more useful is its following strengthening:

Proposition 17.9. Let k be a field. Let C be a connected filtered k-coalgebra. Let $\ell \in \mathbb{N}$ be positive. Then,

$$\Delta_C(x) \in x \otimes 1_C + 1_C \otimes x + \sum_{u=1}^{\ell-1} C_{\leq u} \otimes C_{\leq \ell-u} \qquad \text{for every } x \in C_{\leq \ell} \cap \operatorname{Ker} \varepsilon.$$

This proposition is often used (e. g., it is Proposition II.2.1 in [Mancho06]; however, the statement given in [Mancho06] is slightly wrong, and the proof is not a "Straightforward adaptation of proof of proposition II.1.1" as asserted in [Mancho06]). Let us give a proof of this proposition here, although we are not going to use it until much further in this paper.

Proof of Proposition 17.9. Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$.

By Remark 2.11, we have $C_{\leq 0} = k \cdot 1_C$. In particular, $1_C \in k \cdot 1_C = C_{\leq 0}$. Also, since 1_C was defined as $\left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$, we have $1 = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)(1_C) = \varepsilon_C(1_C) = \varepsilon(1_C)$.

For every $n \in \mathbb{N}$, let $C_{\leq n+}$ denote the k-vector subspace $C_{\leq n} \cap \operatorname{Ker} \varepsilon$ of $C_{\leq n}$. Then, every $n \in \mathbb{N}$ satisfies

$$C_{\leq n} = C_{\leq n+} + C_{\leq 0} \tag{140}$$

[84].

[84] *Proof of (140).* Let $n \in \mathbb{N}$. Then, $0 \leq n$, so that $C_{\leq 0} \subseteq C_{\leq n}$ (since $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$). Hence, $\underbrace{C_{\leq n+}}_{\subseteq C_{\leq n}} + \underbrace{C_{\leq 0}}_{\subseteq C_{\leq n}} \subseteq C_{\leq n} + C_{\leq n} \subseteq C_{\leq n}$ (since $C_{\leq n}$ is a k-vector space).

On the other hand, every $x \in C_{\leq n}$ satisfies $\underbrace{x}_{\in C_{\leq n}} - \varepsilon(x) \cdot \underbrace{1_C}_{\in k \cdot 1_C = C_{\leq 0} \subseteq C_{\leq n}} \in C_{\leq n} - \varepsilon(x) \cdot C_{\leq n} \subseteq C_{\leq n}$ (since $C_{\leq n}$ is a k-vector space) and $x - \varepsilon(x) \cdot 1_C \in \operatorname{Ker} \varepsilon$ (since

$$\begin{aligned} \varepsilon\left(x - \varepsilon(x) \cdot 1_C\right) &= \varepsilon(x) - \varepsilon(x) \cdot \underbrace{\varepsilon(1_C)}_{=1} \qquad \text{(since } \varepsilon \text{ is } k\text{-linear)} \\ &= \varepsilon(x) - \varepsilon(x) = 0 \end{aligned}$$

). Hence, every $x \in C_{\leq n}$ satisfies

$$\begin{aligned} x - \varepsilon(x) \cdot 1_C &\in C_{\leq n} \cap \operatorname{Ker} \varepsilon \qquad \text{(since } x - \varepsilon(x) \cdot 1_C \in C_{\leq n} \text{ and } x - \varepsilon(x) \cdot 1_C \in \operatorname{Ker} \varepsilon\text{)} \\ &= C_{\leq n+}. \end{aligned}$$

Thus, every $x \in C_{\leq n}$ satisfies

$$x = \underbrace{\varepsilon(x) \cdot 1_C}_{\in k \cdot 1_C = C_{\leq 0}} + \underbrace{\left(x - \varepsilon(x) \cdot 1_C\right)}_{\in C_{\leq n+}} \in C_{\leq 0} + C_{\leq n+} = C_{\leq n+} + C_{\leq 0}.$$

In other words, $C_{\leq n} \subseteq C_{\leq n+} + C_{\leq 0}$. Combined with $C_{\leq n+} + C_{\leq 0} \subseteq C_{\leq n}$, this yields $C_{\leq n} = C_{\leq n+} + C_{\leq 0}$, qed.

For each $u \in \{1, 2, \ldots, \ell - 1\}$, we have

$$\begin{aligned}
&\underbrace{C_{\leq u}}_{\substack{=C_{\leq u+}+C_{\leq 0} \\ \text{(by (140), applied to } n=u\text{)}}} \otimes \underbrace{C_{\leq \ell-u}}_{\substack{=C_{\leq(\ell-u)+}+C_{\leq 0} \\ \text{(by (140), applied to } n=\ell-u\text{)}}} \\
&= \left(C_{\leq u+} + C_{\leq 0}\right) \otimes \left(C_{\leq(\ell-u)+} + C_{\leq 0}\right) \\
&= C_{\leq u+} \otimes \left(\underbrace{C_{\leq(\ell-u)+} + C_{\leq 0}}_{=C_{\leq 0}+C_{\leq(\ell-u)+}} \right) + C_{\leq 0} \otimes \left(C_{\leq(\ell-u)+} + C_{\leq 0}\right) \\
&= \underbrace{C_{\leq u+} \otimes \left(C_{\leq 0} + C_{\leq(\ell-u)+}\right)}_{\substack{=C_{\leq u+}\otimes C_{\leq 0}+C_{\leq u+}\otimes C_{\leq(\ell-u)+} \\ \text{(since the tensor product is distributive)}}} + \underbrace{C_{\leq 0} \otimes \left(C_{\leq(\ell-u)+} + C_{\leq 0}\right)}_{\substack{=C_{\leq 0}\otimes C_{\leq(\ell-u)+}+C_{\leq 0}\otimes C_{\leq 0} \\ \text{(since the tensor product is distributive)}}} \\
&\qquad \text{(since the tensor product is distributive)} \\
&= \underbrace{C_{\leq u+}}_{\substack{\subseteq C_{\leq u}\subseteq C_{\leq \ell} \\ \text{(since } u\leq\ell \\ \text{and } C_{\leq 0}\subseteq C_{\leq 1}\subseteq C_{\leq 2}\subseteq\cdots\text{)}}} \otimes C_{\leq 0} + C_{\leq u+} \otimes C_{\leq(\ell-u)+} \\
&\qquad + C_{\leq 0} \otimes \underbrace{C_{\leq(\ell-u)+}}_{\substack{\subseteq C_{\leq \ell-u}\subseteq C_{\leq \ell} \\ \text{(since } \ell-u\leq\ell \\ \text{and } C_{\leq 0}\subseteq C_{\leq 1}\subseteq C_{\leq 2}\subseteq\cdots\text{)}}} + C_{\leq 0} \otimes \underbrace{C_{\leq 0}}_{\substack{\subseteq C_{\leq \ell} \\ \text{(since } 0\leq\ell \\ \text{and } C_{\leq 0}\subseteq C_{\leq 1}\subseteq C_{\leq 2}\subseteq\cdots\text{)}}} \\
&\subseteq C_{\leq \ell} \otimes C_{\leq 0} + C_{\leq u+} \otimes C_{\leq(\ell-u)+} + \underbrace{C_{\leq 0} \otimes C_{\leq \ell} + C_{\leq 0} \otimes C_{\leq \ell}}_{\substack{\subseteq C_{\leq 0}\otimes C_{\leq \ell} \\ \text{(since } C_{\leq 0}\otimes C_{\leq \ell} \text{ is a } k\text{-vector space)}}} \\
&\subseteq C_{\leq \ell} \otimes C_{\leq 0} + C_{\leq u+} \otimes C_{\leq(\ell-u)+} + C_{\leq 0} \otimes C_{\leq \ell}. \qquad (141)
\end{aligned}$$

Now, since C is a filtered coalgebra, we have

$$\begin{aligned}
&\Delta\left(C_{\leq \ell}\right) \\
&\subseteq \sum_{u=0}^{\ell} C_{\leq u} \otimes C_{\leq \ell-u} = C_{\leq 0} \otimes C_{\leq \ell-0} + \sum_{u=1}^{\ell-1} C_{\leq u} \otimes C_{\leq \ell-u} + C_{\leq \ell} \otimes C_{\leq \ell-\ell} \qquad \left(\text{since } \ell > 0\right) \\
&= C_{\leq 0} \otimes \underbrace{C_{\leq \ell-0}}_{=C_{\leq \ell}} + C_{\leq \ell} \otimes \underbrace{C_{\leq \ell-\ell}}_{=C_{\leq 0}} + \sum_{u=1}^{\ell-1} \underbrace{C_{\leq u} \otimes C_{\leq \ell-u}}_{\substack{\subseteq C_{\leq \ell} \otimes C_{\leq 0} + C_{\leq u+} \otimes C_{\leq (\ell-u)+} + C_{\leq 0} \otimes C_{\leq \ell} \\ \text{(by (141))}}} \\
&\subseteq C_{\leq 0} \otimes C_{\leq \ell} + C_{\leq \ell} \otimes C_{\leq 0} + \underbrace{\sum_{u=1}^{\ell-1} \left(C_{\leq \ell} \otimes C_{\leq 0} + C_{\leq u+} \otimes C_{\leq (\ell-u)+} + C_{\leq 0} \otimes C_{\leq \ell}\right)}_{= \sum\limits_{u=1}^{\ell-1} C_{\leq \ell} \otimes C_{\leq 0} + \sum\limits_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+} + \sum\limits_{u=1}^{\ell-1} C_{\leq 0} \otimes C_{\leq \ell}} \\
&= C_{\leq 0} \otimes C_{\leq \ell} + C_{\leq \ell} \otimes C_{\leq 0} + \sum_{u=1}^{\ell-1} C_{\leq \ell} \otimes C_{\leq 0} + \sum_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+} + \sum_{u=1}^{\ell-1} C_{\leq 0} \otimes C_{\leq \ell} \\
&= \underbrace{C_{\leq 0} \otimes C_{\leq \ell} + \sum_{u=1}^{\ell-1} C_{\leq 0} \otimes C_{\leq \ell}}_{\substack{\subseteq C_{\leq 0} \otimes C_{\leq \ell} \\ \text{(since } C_{\leq 0} \otimes C_{\leq \ell} \text{ is a } k\text{-vector space)}}} + \underbrace{C_{\leq \ell} \otimes C_{\leq 0} + \sum_{u=1}^{\ell-1} C_{\leq \ell} \otimes C_{\leq 0}}_{\substack{\subseteq C_{\leq \ell} \otimes C_{\leq 0} \\ \text{(since } C_{\leq \ell} \otimes C_{\leq 0} \text{ is a } k\text{-vector space)}}} + \sum_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+} \\
&\subseteq C_{\leq 0} \otimes C_{\leq \ell} + C_{\leq \ell} \otimes C_{\leq 0} + \sum_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+}.
\end{aligned}$$

It is easy to see that

for every $U \in C_{\leq 0} \otimes C_{\leq \ell}$, there exists some $u \in C_{\leq \ell}$ such that $U = 1_C \otimes u$. (142)

[85] *Proof of (142).* Let $\xi : C_{\leq \ell} \to C_{\leq 0} \otimes C_{\leq \ell}$ be the map which sends every $t \in C_{\leq \ell}$ to $1_C \otimes t \in C_{\leq 0} \otimes C_{\leq \ell}$ (this is well-defined since every $t \in C_{\leq \ell}$ satisfies $\underbrace{1_C}_{\in C_{\leq 0}} \otimes \underbrace{t}_{\in C_{\leq \ell}} \in C_{\leq 0} \otimes C_{\leq \ell}$). Let $\operatorname{kan} : C_{\leq \ell} \to k \otimes C_{\leq \ell}$ be the canonical isomorphism which sends every $t \in C_{\leq \ell}$ to $1 \otimes t$.

Since C is a connected coalgebra, $\varepsilon_C \mid_{C_{\leq 0}} : C_{\leq 0} \to k$ is an isomorphism. Hence, $\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \mathrm{id}_{C_{\leq \ell}} : C_{\leq 0} \otimes C_{\leq \ell} \to k \otimes C_{\leq \ell}$ is an isomorphism as well.

Now, every $t \in C_{\leq \ell}$ satisfies

$$\begin{aligned}
\left(\left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \mathrm{id}_{C_{\leq \ell}}\right) \circ \xi\right)(t) &= \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \mathrm{id}_{C_{\leq \ell}}\right) \underbrace{\left(\xi\left(t\right)\right)}_{\substack{=1_C \otimes t \\ \text{(by the definition of } \xi\text{)}}} = \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \mathrm{id}_{C_{\leq \ell}}\right)\left(1_C \otimes t\right) \\
&= \underbrace{\left(\varepsilon_C \mid_{C_{\leq 0}}\right)\left(1_C\right)}_{=1} \otimes \underbrace{\mathrm{id}_{C_{\leq \ell}}\left(t\right)}_{=t} = 1 \otimes t = \operatorname{kan} t \\
&\qquad \left(\text{since } \operatorname{kan} t = 1 \otimes t \text{ by the definition of kan}\right).
\end{aligned}$$

Hence, $\left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \mathrm{id}_{C_{\leq \ell}}\right) \circ \xi = \operatorname{kan}$. Since $\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \mathrm{id}_{C_{\leq \ell}}$ and kan are isomorphisms, this yields that ξ is an isomorphism. Thus, the map ξ^{-1} is well-defined.

Now, for every $U \in C_{\leq 0} \otimes C_{\leq \ell}$, we have

$$U = \xi\left(\xi^{-1}\left(U\right)\right) = 1_C \otimes \xi^{-1}\left(U\right) \qquad \left(\text{by the definition of } \xi\right).$$

The same argument, but with the two tensorands transposed, shows that

$$\text{for every } V \in C_{\leq \ell} \otimes C_{\leq 0}, \text{ there exists some } v \in C_{\leq \ell} \text{ such that } V = v \otimes 1_C. \tag{143}$$

Now, let $x \in C_{\leq \ell} \cap \operatorname{Ker} \varepsilon$. Then, $x \in C_{\leq \ell} \cap \operatorname{Ker} \varepsilon \subseteq C_{\leq \ell}$ and $x \in C_{\leq \ell} \cap \operatorname{Ker} \varepsilon \subseteq \operatorname{Ker} \varepsilon$. From $x \in \operatorname{Ker} \varepsilon$, we conclude that $\varepsilon(x) = 0$.

Since $x \in C_{\leq \ell}$, we have

$$\Delta(x) \in \Delta\left(C_{\leq \ell}\right) \subseteq C_{\leq 0} \otimes C_{\leq \ell} + C_{\leq \ell} \otimes C_{\leq 0} + \sum_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+}.$$

Thus, there exist some $U \in C_{\leq 0} \otimes C_{\leq \ell}$, some $V \in C_{\leq \ell} \otimes C_{\leq 0}$ and some $W \in \sum_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+}$ such that $\Delta(x) = U + V + W$. Consider these U, V and W.

According to (142), there exists some $u \in C_{\leq \ell}$ such that $U = 1_C \otimes u$. Consider this u.

According to (143), there exists some $v \in C_{\leq \ell}$ such that $V = v \otimes 1_C$. Consider this v.

Now,

$$\Delta(x) = \underbrace{U}_{=1_C \otimes u} + \underbrace{V}_{=v \otimes 1_C} + W = 1_C \otimes u + v \otimes 1_C + W. \tag{144}$$

But

$$\text{every } n \in \mathbb{N} \text{ satisfies } \varepsilon\left(C_{\leq n+}\right) = 0 \tag{145}$$

(since $C_{\leq n+} = C_{\leq n} \cap \operatorname{Ker} \varepsilon \subseteq \operatorname{Ker} \varepsilon$).

Let kan_1 be the canonical isomorphism $C \otimes k \to C$ which maps $c \otimes \lambda$ to λc for every $(c, \lambda) \in C \times k$. By the axioms of a coalgebra, $\operatorname{kan}_1 \circ (\operatorname{id} \otimes \varepsilon) \circ \Delta = \operatorname{id}_C$.

Let kan_2 be the canonical isomorphism $k \otimes C \to C$ which maps $\lambda \otimes c$ to λc for every $(c, \lambda) \in C \times k$. By the axioms of a coalgebra, $\operatorname{kan}_2 \circ (\varepsilon \otimes \operatorname{id}) \circ \Delta = \operatorname{id}_C$.

Now,

$$\begin{aligned}
(\operatorname{id} \otimes \varepsilon)(W) &\in (\operatorname{id} \otimes \varepsilon)\left(\sum_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+}\right) \qquad \left(\text{since } W \in \sum_{u=1}^{\ell-1} C_{\leq u+} \otimes C_{\leq (\ell-u)+}\right) \\
&\in \sum_{u=1}^{\ell-1} \underbrace{(\operatorname{id} \otimes \varepsilon)\left(C_{\leq u+} \otimes C_{\leq (\ell-u)+}\right)}_{\subseteq \operatorname{id}\left(C_{\leq u+}\right) \otimes \varepsilon\left(C_{\leq (\ell-u)+}\right)} \qquad (\text{since } \operatorname{id} \otimes \varepsilon \text{ is } k\text{-linear}) \\
&\subseteq \sum_{u=1}^{\ell-1} \operatorname{id}\left(C_{\leq u+}\right) \otimes \underbrace{\varepsilon\left(C_{\leq (\ell-u)+}\right)}_{=0 \text{ (by (145), applied to } n=\ell-u)} = \sum_{u=1}^{\ell-1} \underbrace{\operatorname{id}\left(C_{\leq u+}\right) \otimes 0}_{=0} = \sum_{u=1}^{\ell-1} 0 = 0,
\end{aligned}$$

Hence, for every $U \in C_{\leq 0} \otimes C_{\leq \ell}$, there exists some $u \in C_{\leq \ell}$ such that $U = 1_C \otimes u$ (namely, $u = \xi^{-1}(U)$). This proves (142).

so that $(\mathrm{id}\otimes\varepsilon)(W)=0$. Now,

$$\begin{aligned}(\mathrm{id}\otimes\varepsilon)(\Delta(x)) &= (\mathrm{id}\otimes\varepsilon)(1_C\otimes u+v\otimes 1_C+W) \qquad \text{(by (144))}\\ &= \underbrace{(\mathrm{id}\otimes\varepsilon)(1_C\otimes u)}_{=\mathrm{id}(1_C)\otimes\varepsilon(u)}+\underbrace{(\mathrm{id}\otimes\varepsilon)(v\otimes 1_C)}_{=\mathrm{id}(v)\otimes\varepsilon(1_C)}+\underbrace{(\mathrm{id}\otimes\varepsilon)(W)}_{=0}\\ &\qquad \text{(since } \mathrm{id}\otimes\varepsilon \text{ is } k\text{-linear)}\\ &= \underbrace{\mathrm{id}(1_C)}_{=1_C}\otimes\underbrace{\varepsilon(u)}_{=\varepsilon(u)1}+\underbrace{\mathrm{id}(v)}_{=v}\otimes\underbrace{\varepsilon(1_C)}_{=1} = \underbrace{1_C\otimes\varepsilon(u)1}_{=\varepsilon(u)1_C\otimes 1}+v\otimes 1\\ &= \varepsilon(u)1_C\otimes 1+v\otimes 1=(\varepsilon(u)1_C+v)\otimes 1.\end{aligned}$$

Now,

$$\begin{aligned}x &= \underbrace{\mathrm{id}_C}_{=\mathrm{kan}_1\circ(\mathrm{id}\otimes\varepsilon)\circ\Delta}(x) = (\mathrm{kan}_1\circ(\mathrm{id}\otimes\varepsilon)\circ\Delta)(x) = \mathrm{kan}_1\underbrace{((\mathrm{id}\otimes\varepsilon)(\Delta(x)))}_{=(\varepsilon(u)1_C+v)\otimes 1}\\ &= \mathrm{kan}_1((\varepsilon(u)1_C+v)\otimes 1)=1\cdot(\varepsilon(u)1_C+v) \qquad \text{(by the definition of } \mathrm{kan}_1)\\ &= \varepsilon(u)1_C+v.\end{aligned}$$

Thus,

$$v=x-\varepsilon(u)1_C. \tag{146}$$

On the other hand,

$$\begin{aligned}(\varepsilon\otimes\mathrm{id})(W) &\in (\varepsilon\otimes\mathrm{id})\left(\sum_{u=1}^{\ell-1}C_{\leq u+}\otimes C_{\leq(\ell-u)+}\right) \qquad \left(\text{since } W\in\sum_{u=1}^{\ell-1}C_{\leq u+}\otimes C_{\leq(\ell-u)+}\right)\\ &\in \sum_{u=1}^{\ell-1}\underbrace{(\varepsilon\otimes\mathrm{id})\left(C_{\leq u+}\otimes C_{\leq(\ell-u)+}\right)}_{\subseteq\varepsilon\left(C_{\leq u+}\right)\otimes\mathrm{id}\left(C_{\leq(\ell-u)+}\right)} \qquad \text{(since } \varepsilon\otimes\mathrm{id} \text{ is } k\text{-linear)}\\ &\subseteq \sum_{u=1}^{\ell-1}\underbrace{\varepsilon\left(C_{\leq u+}\right)}_{\substack{=0\\ \text{(by (145), applied to } n=u)}}\otimes\mathrm{id}\left(C_{\leq(\ell-u)+}\right)=\sum_{u=1}^{\ell-1}\underbrace{0\otimes\mathrm{id}\left(C_{\leq(\ell-u)+}\right)}_{=0}=\sum_{u=1}^{\ell-1}0=0,\end{aligned}$$

so that $(\varepsilon\otimes\mathrm{id})(W)=0$. Now,

$$\begin{aligned}(\varepsilon\otimes\mathrm{id})(\Delta(x)) &= (\varepsilon\otimes\mathrm{id})(1_C\otimes u+v\otimes 1_C+W) \qquad \text{(by (144))}\\ &= \underbrace{(\varepsilon\otimes\mathrm{id})(1_C\otimes u)}_{=\varepsilon(1_C)\otimes\mathrm{id}(u)}+\underbrace{(\varepsilon\otimes\mathrm{id})(v\otimes 1_C)}_{=\varepsilon(v)\otimes\mathrm{id}(1_C)}+\underbrace{(\varepsilon\otimes\mathrm{id})(W)}_{=0}\\ &\qquad \text{(since } \varepsilon\otimes\mathrm{id} \text{ is } k\text{-linear)}\\ &= \underbrace{\varepsilon(1_C)}_{=1}\otimes\underbrace{\mathrm{id}(u)}_{=u}+\underbrace{\varepsilon(v)}_{=\varepsilon(v)1}\otimes\underbrace{\mathrm{id}(1_C)}_{=1_C}=1\otimes u+\underbrace{\varepsilon(v)1\otimes 1_C}_{=1\otimes\varepsilon(v)1_C}\\ &= 1\otimes u+1\otimes\varepsilon(v)1_C=1\otimes(u+\varepsilon(v)1_C).\end{aligned}$$

Now,

$$\begin{aligned} x &= \underbrace{\mathrm{id}_C}_{=\mathrm{kan}_2\circ(\varepsilon\otimes\mathrm{id})\circ\Delta}(x) = \left(\mathrm{kan}_2\circ(\varepsilon\otimes\mathrm{id})\circ\Delta\right)(x) = \mathrm{kan}_2\underbrace{\left((\varepsilon\otimes\mathrm{id})(\Delta(x))\right)}_{=1\otimes(u+\varepsilon(v)1_C)} \\ &= \mathrm{kan}_2\left(1\otimes(u+\varepsilon(v)1_C)\right) \\ &= 1\cdot(u+\varepsilon(v)1_C) \qquad \text{(by the definition of } \mathrm{kan}_2) \\ &= u+\varepsilon(v)1_C. \end{aligned}$$

Thus,

$$u = x-\varepsilon(v)1_C. \tag{147}$$

Hence,

$$\begin{aligned} \varepsilon(u) &= \varepsilon(x-\varepsilon(v)1_C) = \underbrace{\varepsilon(x)}_{=0} - \varepsilon(v)\underbrace{\varepsilon(1_C)}_{=1} \qquad \text{(since } \varepsilon \text{ is } k\text{-linear)} \\ &= -\varepsilon(v), \end{aligned}$$

so that

$$\varepsilon(u)+\varepsilon(v) = 0. \tag{148}$$

Now, (144) becomes

$$\begin{aligned} \Delta(x) &= 1_C\otimes \underbrace{u}_{\substack{=x-\varepsilon(v)1_C \\ \text{(by (147))}}} + \underbrace{v}_{\substack{=x-\varepsilon(u)1_C \\ \text{(by (146))}}} \otimes 1_C + W \\ &= \underbrace{1_C\otimes(x-\varepsilon(v)1_C)}_{=1_C\otimes x-\varepsilon(v)1_C\otimes 1_C} + \underbrace{(x-\varepsilon(u)1_C)\otimes 1_C}_{=x\otimes 1_C-\varepsilon(u)1_C\otimes 1_C} + W \\ &= 1_C\otimes x-\varepsilon(v)1_C\otimes 1_C + x\otimes 1_C-\varepsilon(u)1_C\otimes 1_C + W \\ &= x\otimes 1_C + 1_C\otimes x - \underbrace{(\varepsilon(u)1_C\otimes 1_C+\varepsilon(v)1_C\otimes 1_C)}_{\substack{=(\varepsilon(u)+\varepsilon(v))1_C\otimes 1_C=0 \\ \text{(since } \varepsilon(u)+\varepsilon(v)=0 \text{ by (148))}}} + W \\ &= x\otimes 1_C + 1_C\otimes x + W \in x\otimes 1_C + 1_C\otimes x + \sum_{u=1}^{\ell-1} \underbrace{C_{\leq u+}}_{\subseteq C_{\leq u}} \otimes \underbrace{C_{\leq(\ell-u)+}}_{\subseteq C_{\leq \ell-u}} \\ &\qquad \left(\text{since } W\in\sum_{u=1}^{\ell-1} C_{\leq u+}\otimes C_{\leq(\ell-u)+}\right) \\ &\subseteq x\otimes 1_C + 1_C\otimes x + \sum_{u=1}^{\ell-1} C_{\leq u}\otimes C_{\leq \ell-u}. \end{aligned}$$

This proves Proposition 17.9. □

The next lemma is essentially obvious:

Lemma 17.10. Let k be a field, let A be a k-algebra, and let H be a connected filtered k-coalgebra. Every positive $i\in\mathbb{N}$ and every $h\in\mathfrak{g}(H,A)$ satisfy $h^{*i}\in\mathfrak{g}(H,A)$.

Proof of Lemma 17.10. Let $i \in \mathbb{N}$ be positive. Let $h \in \mathfrak{g}(H, A)$. Since $i > 0$, we can apply Remark 3.5 to $n = 0$ and $f = h$, and obtain $h^{*i}(H_{\leq 0}) = 0$. Since $1_H \in H_{\leq 0}$ (because H is a filtered k-algebra), this yields $h^{*i}(1_H) = 0$. Thus, $h^{*i} \in \{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\} = \mathfrak{g}(H, A)$. This proves Lemma 17.10. $\square$

We can now prove Proposition 17.4:

Proof of Proposition 17.4. We will prove Proposition 17.4 by strong induction over ℓ:

Induction step: Let $L \in \mathbb{N}$ be a nonnegative integer. Assume that Proposition 17.4 has already been proven whenever $\ell < L$. Now our aim is to prove Proposition 17.4 for $\ell = L$.

First of all, Proposition 17.4 obviously holds for $\ell = L$ if $L = 0$ (in fact,

$$\begin{aligned} H_{\leq 0} &= k \cdot 1_H \qquad \text{(by Remark 2.11, applied to } C = H\text{)} \\ &= \mathfrak{E}^0 \qquad \left(\text{since } \mathfrak{E}^0 = k \cdot 1_H\right) \\ &= \sum_{i=0}^{0} \mathfrak{E}^i, \end{aligned}$$

so that Proposition 17.4 holds for $\ell = 0$; in other words, Proposition 17.4 holds for $\ell = L$ if $L = 0$). Hence, in the following, we can WLOG assume that $L \neq 0$. Thus, L is positive, so that $L \geq 1$.

Since Proposition 17.4 has already been proven whenever $\ell < L$, we have

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} \mathfrak{E}^i \qquad \text{for every nonnegative integer } \ell < L. \tag{149}$$

Let $f = \mathrm{id} - e_{H,H}$, where id denotes the identity map $\mathrm{id}_H : H \to H$. Then, $f \in \mathfrak{g}(H, H)$ [86].

Let $g : H \to H$ be the map $\sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} f^{*(i-1)}$.

For every $i \in \{2, 3, \ldots, L\}$, we have $f^{*(i-1)} \in \mathfrak{g}(H, H)$ [87]. Thus,

$$g = \sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} \underbrace{f^{*(i-1)}}_{\in \mathfrak{g}(H,H)} \in \sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} \mathfrak{g}(H, H) \subseteq \mathfrak{g}(H, H)$$

(since $\mathfrak{g}(H, H)$ is a k-vector space).

By Remark 17.6 **(d)** (applied to $V = H$ and $W = H$), the set of all k-linear maps $H \to H$ respecting the filtration is a k-vector subspace of $\mathcal{L}(H, H)$.

Since the map id respects the filtration (obviously) and the map $e_{H,H}$ respects the filtration (by Proposition 17.8 **(a)**, applied to $C = H$ and $A = H$), the map $\mathrm{id} - e_{H,H}$ also respects the filtration (since the set of all k-linear maps $H \to H$ respecting the

[86] *Proof.* We have $\mathrm{id} \in G(H, H) = e_{H,H} + \mathfrak{g}(H, H)$, and thus $\mathrm{id} - e_{H,H} \in \mathfrak{g}(H, H)$, so that $f = \mathrm{id} - e_{H,H} \in \mathfrak{g}(H, H)$.

[87] *Proof.* Let $i \in \{2, 3, \ldots, L\}$. Then, $i - 1 \in \{1, 2, \ldots, L - 1\}$, so that $i - 1$ is a positive element of $\mathbb{N}$. Hence, Lemma 17.10 (applied to H, f and $i - 1$ instead of A, h and i) shows that $f^{*(i-1)} \in \mathfrak{g}(H, H)$. Qed.

filtration is a k-vector subspace of $\mathcal{L}(H,H)$). Since $\mathrm{id} - e_{H,H} = f$, this means that the map f respects the filtration.

Thus, for every $i \in \{2,3,\ldots,L\}$, the map $f^{*(i-1)}$ respects the filtration (by Proposition 17.8 **(c)**, applied to $C = H$, $A = H$ and $n = i-1$). Hence, the map $\sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} f^{*(i-1)}$ also respects the filtration (since the set of all k-linear maps $H \to H$ respecting the filtration is a k-vector subspace of $\mathcal{L}(H,H)$). Since $\sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} f^{*(i-1)} = g$, this means that the map g respects the filtration.

By the definition of Log, we have $\operatorname{Log} \mathrm{id} = \operatorname{Log}_1 \underbrace{(\mathrm{id} - e_{H,H})}_{=f} = \operatorname{Log}_1 f$. Thus, $\mathfrak{e} = \operatorname{Log} \mathrm{id} = \operatorname{Log}_1 f$.

Now let $x \in H_{\leq L}$ be arbitrary. Then,

$$f^{*i}(x) = 0 \qquad \text{for every integer } i > L \tag{150}$$

[88]. Now, $\mathfrak{e} = \operatorname{Log}_1 f$ leads to

$$\begin{aligned}
\mathfrak{e}(x) &= (\operatorname{Log}_1 f)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) \qquad \text{(by (8))} \\
&= \sum_{\substack{i \geq 1; \\ i \leq L}} \frac{(-1)^{i-1}}{i} f^{*i}(x) + \sum_{\substack{i \geq 1; \\ i > L}} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{\substack{=0 \\ \text{(by (150))}}} \\
&= \underbrace{\sum_{\substack{i \geq 1; \\ i \leq L}}}_{=\sum_{i=1}^{L}} \frac{(-1)^{i-1}}{i} f^{*i}(x) + \underbrace{\sum_{\substack{i \geq 1; \\ i > L}} \frac{(-1)^{i-1}}{i} 0}_{=0} = \sum_{i=1}^{L} \frac{(-1)^{i-1}}{i} f^{*i}(x) \\
&= \underbrace{\frac{(-1)^{1-1}}{1}}_{=\frac{1}{1}=1} \underbrace{f^{*1}}_{=f}(x) + \sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}}_{=f*f^{*(i-1)}}(x) \\
&\qquad \left(\begin{array}{c} \text{here, we have split off the addend for } i = 1 \\ \text{from the sum, because } L \geq 1 \end{array} \right) \\
&= f(x) + \sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} \left(f * f^{*(i-1)}\right)(x),
\end{aligned}$$

[88] *Proof of (150):* Let $i > L$ be an integer. Then, $i > L \geq 0$, so that $i \in \mathbb{N}$. Now, Remark 3.5 (applied to $n = L$ and $A = H$) yields $f^{*i}(H_{\leq L}) = 0$ (since $i > L$). But $x \in H_{\leq L}$ yields $f^{*i}(x) \in f^{*i}(H_{\leq L}) = 0$, thus $f^{*i}(x) = 0$. This proves (150).

so that

$$\mathfrak{e}(x) - f(x) = \sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} \left(f * f^{*(i-1)}\right)(x) = \underbrace{\left(\sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} f * f^{*(i-1)}\right)}_{\substack{= f * \left(\sum\limits_{i=2}^{L} \frac{(-1)^{i-1}}{i} f^{*(i-1)}\right) \\ \text{(since convolution of } k\text{-linear maps} \\ \text{is } k\text{-bilinear)}}} (x)$$

$$= \left(f * \underbrace{\left(\sum_{i=2}^{L} \frac{(-1)^{i-1}}{i} f^{*(i-1)}\right)}_{=g} \right)(x) = (f * g)(x).$$

This rewrites as

$$f(x) = \mathfrak{e}(x) - (f * g)(x).$$

Since

$$\underbrace{f}_{=\mathrm{id} - e_{H,H}}(x) = (\mathrm{id} - e_{H,H})(x) = \underbrace{\mathrm{id}(x)}_{=x} - \underbrace{e_{H,H}}_{=\eta_H \circ \varepsilon_H}(x)$$
$$= x - \underbrace{(\eta_H \circ \varepsilon_H)(x)}_{\substack{= \eta_H(\varepsilon_H(x)) = \varepsilon_H(x) \cdot 1_H \\ \text{(by the definition of } \eta_H)}} = x - \varepsilon_H(x) \cdot 1_H,$$

this becomes $x - \varepsilon_H(x) \cdot 1_H = \mathfrak{e}(x) - (f * g)(x)$. In other words,

$$x = \varepsilon_H(x) \cdot 1_H + \mathfrak{e}(x) - (f * g)(x). \tag{151}$$

But since $f \in \mathfrak{g}(H, H)$ and $g \in \mathfrak{g}(H, H)$, and since the maps f and g respect the filtration, Proposition 17.8 **(d)** (applied to $\ell = L$, $C = H$ and $A = H$) yields

$$(f * g)(H_{\leq L}) \subseteq \sum_{u=1}^{L-1} H_{\leq u} H_{\leq L-u}. \tag{152}$$

But using (149), it is easy to see that every $u \in \{1, 2, \ldots, L-1\}$ satisfies $H_{\leq u} H_{\leq L-u} \subseteq \sum\limits_{i=0}^{L} \mathfrak{E}^i$ [89]. Hence, (152) becomes

$$(f * g)(H_{\leq L}) \subseteq \sum_{u=1}^{L-1} \underbrace{H_{\leq u} H_{\leq L-u}}_{\subseteq \sum\limits_{i=0}^{L} \mathfrak{E}^i} \subseteq \sum_{u=1}^{L-1} \sum_{i=0}^{L} \mathfrak{E}^i \subseteq \sum_{i=0}^{L} \mathfrak{E}^i$$

[89] *Proof.* Let $u \in \{1, 2, \ldots, L-1\}$. Then, $u \geq 1$ and $u \leq L-1$.

Since $u \leq L - 1 < L$, we have $H_{\leq u} \subseteq \sum\limits_{i=0}^{u} \mathfrak{E}^i$ (by (149) (applied to $\ell = u$)).

(since $\sum_{i=0}^{L} \mathfrak{E}^i$ is a k-vector space). Hence, $x \in H_{\leq L}$ yields

$$(f * g)(x) \in (f * g)(H_{\leq L}) \subseteq \sum_{i=0}^{L} \mathfrak{E}^i.$$

On the other hand,

$$\mathfrak{e}\left(\underbrace{x}_{\in H}\right) \in \mathfrak{e}(H) = \mathfrak{E} \qquad \text{(since } \mathfrak{E} \text{ was defined to be } \mathfrak{e}(H)\text{)}$$

$$= \mathfrak{E}^1 \subseteq \sum_{i=0}^{L} \mathfrak{E}^i$$

$$\left(\begin{array}{c} \text{since } L \geq 1, \text{ so that } 1 \in \{0,1,\ldots,L\}, \text{ and thus} \\ \mathfrak{E}^1 \text{ is an addend of the sum } \sum_{i=0}^{L} \mathfrak{E}^i \end{array} \right).$$

Also,

$$1_H \in \mathfrak{E}^0 \subseteq \sum_{i=0}^{L} \mathfrak{E}^i \qquad \left(\begin{array}{c} \text{since } 0 \in \{0,1,\ldots,L\}, \text{ and thus} \\ \mathfrak{E}^0 \text{ is an addend of the sum } \sum_{i=0}^{L} \mathfrak{E}^i \end{array} \right).$$

Since $L - \underbrace{u}_{\geq 1} \leq L - 1 < L$, we have

$$H_{\leq L-u} \subseteq \sum_{i=0}^{L-u} \mathfrak{E}^i \qquad \text{(by (149) (applied to } \ell = L-u\text{))}$$

$$= \sum_{j=0}^{L-u} \mathfrak{E}^j \qquad \text{(here, we renamed the index } i \text{ as } j \text{ in the sum)}.$$

Multiplying $H_{\leq u} \subseteq \sum_{i=0}^{u} \mathfrak{E}^i$ and $H_{\leq L-u} \subseteq \sum_{j=0}^{L-u} \mathfrak{E}^j$, we obtain

$$H_{\leq u} H_{\leq L-u} \subseteq \left(\sum_{i=0}^{u} \mathfrak{E}^i\right)\left(\sum_{j=0}^{L-u} \mathfrak{E}^j\right) = \sum_{i=0}^{u}\sum_{j=0}^{L-u} \underbrace{\mathfrak{E}^i \mathfrak{E}^j}_{=\mathfrak{E}^{i+j} \subseteq \sum_{\nu=0}^{L} \mathfrak{E}^\nu}$$

(because $i \leq u$ and $j \leq L-u$, so that $i+j \leq u+(L-u)=L$, so that $i+j \in \{0,1,\ldots,L\}$, so that $\mathfrak{E}^{i+j}$ is an addend in the sum $\sum_{\nu=0}^{L} \mathfrak{E}^\nu$)

$$\subseteq \sum_{i=0}^{u}\sum_{j=0}^{L-u}\sum_{\nu=0}^{L} \mathfrak{E}^\nu \subseteq \sum_{\nu=0}^{L} \mathfrak{E}^v \qquad \left(\text{since } \sum_{\nu=0}^{L} \mathfrak{E}^\nu \text{ is a } k\text{-vector space}\right)$$

$$= \sum_{i=0}^{L} \mathfrak{E}^i \qquad \text{(here, we renamed the summation index } \nu \text{ as } i\text{)},$$

qed.

Using these all facts, (151) becomes

$$\begin{aligned} x &= \varepsilon_H(x) \cdot \underbrace{1_H}_{\in \sum_{i=0}^{L} \mathfrak{E}^i} + \underbrace{\mathfrak{e}(x)}_{\in \sum_{i=0}^{L} \mathfrak{E}^i} - \underbrace{(f * g)(x)}_{\in \sum_{i=0}^{L} \mathfrak{E}^i} \\ &\in \varepsilon_H(x) \cdot \left(\sum_{i=0}^{L} \mathfrak{E}^i \right) + \sum_{i=0}^{L} \mathfrak{E}^i - \sum_{i=0}^{L} \mathfrak{E}^i \\ &\subseteq \sum_{i=0}^{L} \mathfrak{E}^i \qquad \left(\text{since } \sum_{i=0}^{L} \mathfrak{E}^i \text{ is a } k\text{-vector space} \right). \end{aligned}$$

Now forget that we fixed x. We thus have shown that every $x \in H_{\leq L}$ satisfies $x \in \sum_{i=0}^{L} \mathfrak{E}^i$. In other words, $H_{\leq L} \subseteq \sum_{i=0}^{L} \mathfrak{E}^i$. In other words, we have proven Proposition 17.4 for $\ell = L$. This completes the induction step.

Thus, the induction proof of Proposition 17.4 is complete. □

Proof of Proposition 17.3. Consider the convolution algebra $\mathcal{L}(H, H)$. Let $\mathfrak{e}$ denote the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$. Let $\mathfrak{E}$ be the k-vector subspace $\mathfrak{e}(H)$ of H.

Theorem 4.1 yields that $\operatorname{Log} \operatorname{id}$ is a projection to $\operatorname{Prim} H$. In other words, $\mathfrak{e}$ is a projection to $\operatorname{Prim} H$ (since $\mathfrak{e} = \operatorname{Log} \operatorname{id}$). Hence, $\mathfrak{e}(H) = \operatorname{Prim} H$. Thus, $\mathfrak{E} = \mathfrak{e}(H) = \operatorname{Prim} H$.

Now, fix $\ell \in \mathbb{N}$. Proposition 17.4 yields

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} \underbrace{\mathfrak{E}^i}_{\substack{= (\operatorname{Prim} H)^i \\ (\text{since } \mathfrak{E} = \operatorname{Prim} H)}} = \sum_{i=0}^{\ell} (\operatorname{Prim} H)^i .$$

This proves Proposition 17.3. □

Proof of Theorem 17.1. For every $\ell \in \mathbb{N}$, Proposition 17.3 yields

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} \underbrace{(\operatorname{Prim} H)^i}_{\subseteq \operatorname{AlgGen}_k(\operatorname{Prim} H)} \subseteq \sum_{i=0}^{\ell} \operatorname{AlgGen}_k(\operatorname{Prim} H) \subseteq \operatorname{AlgGen}_k(\operatorname{Prim} H)$$

(since $\operatorname{AlgGen}_k(\operatorname{Prim} H)$ is a k-vector space). Since H is filtered, we have

$$H = \bigcup_{\ell \in \mathbb{N}} \underbrace{H_{\leq \ell}}_{\subseteq \operatorname{AlgGen}_k(\operatorname{Prim} H)} \subseteq \bigcup_{\ell \in \mathbb{N}} \operatorname{AlgGen}_k(\operatorname{Prim} H) = \operatorname{AlgGen}_k(\operatorname{Prim} H).$$

Combined with $\operatorname{AlgGen}_k(\operatorname{Prim} H) \subseteq H$ (which is trivial), this yields $H = \operatorname{AlgGen}_k(\operatorname{Prim} H)$. This proves Theorem 17.1. □

We will next prove a kind of strengthening of Theorem 17.1 and Proposition 17.3. First a notation:

Definition 17.11. Let k be a field.

(a) For every k-vector space M and every subset S of M, let us denote by $\langle S \rangle$ the k-vector subspace of M generated by the elements of S. (This is precisely Convention 15.1; we just have repeated it for the sake of convenience.)

(b) For every k-vector space M, every set Φ and every map $P : \Phi \to M$, let us denote by $\langle P(v) \mid v \in \Phi \rangle$ the subspace $\langle \{P(v) \mid v \in \Phi\} \rangle$ of M (this is the k-vector subspace of M generated by all the elements $P(v)$ with $v \in \Phi$).

(c) Assume that the field k has characteristic 0. For every k-algebra A, every k-vector subspace V of A, and every $n \in \mathbb{N}$, we denote by $\operatorname{symp}_n V$ the k-vector subspace

$$\left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle$$

of A (where S_n denotes the n-th symmetric group). Note that this definition yields that $\operatorname{symp}_0 V = k \cdot 1_A$ [90] and $\operatorname{symp}_1 V = V$ (this is also immediate to see).

Now, the strengthening of Theorem 17.1:

Theorem 17.12. Let k be a field of characteristic 0, and let H be a connected filtered cocommutative bialgebra over k. Then,

$$H = \sum_{i \in \mathbb{N}} \operatorname{symp}_i (\operatorname{Prim} H).$$

And here the (more concrete) strengthening of Proposition 17.3:

Proposition 17.13. Let k be a field of characteristic 0, and let H be a connected filtered cocommutative bialgebra over k. Then,

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} \operatorname{symp}_i (\operatorname{Prim} H) \qquad \text{for every } \ell \in \mathbb{N}.$$

[90] *Proof.* Let pt denote the 0-tuple of elements of V (i. e., the only element of $V^{\times 0}$), and let id_0 denote the identity map $\varnothing \to \varnothing$. Then, $V^{\times 0} = \{\mathrm{pt}\}$ and $S_0 = \{\mathrm{id}_0\}$.

Since $S_0 = \{\mathrm{id}_0\}$, we have $\sum_{\sigma \in S_0} 1_A = 1_A$.

But by the definition of $\operatorname{symp}_0 V$, we have

$$\begin{aligned}
\operatorname{symp}_0 V &= \left\langle \underbrace{\frac{1}{0!}}_{=\frac{1}{1}=1} \sum_{\sigma \in S_0} \underbrace{v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(0)}}_{=(\text{empty product})=1_A} \mid (v_1, v_2, \ldots, v_0) \in \underbrace{V^{\times 0}}_{=\{\mathrm{pt}\}} \right\rangle \\
&= \left\langle \underbrace{\sum_{\sigma \in S_0} 1_A}_{=1_A} \mid (v_1, v_2, \ldots, v_0) \in \{\mathrm{pt}\} \right\rangle \\
&= \langle 1_A \mid (v_1, v_2, \ldots, v_0) \in \{\mathrm{pt}\} \rangle = k \cdot 1_A,
\end{aligned}$$

qed.

The path from Proposition 17.3 to Proposition 17.13 consists of two parts: one (very easy) Hopf-algebraic computation, and one elementary algebraic (i. e., using no coalgebra structure) argument. First, the Hopf-algebraic computation:

Proposition 17.14. Let k be a field. Let H be a k-bialgebra. Then, $xy - yx \in \operatorname{Prim} H$ for any $x \in \operatorname{Prim} H$ and $y \in \operatorname{Prim} H$.

This Proposition 17.14 is very easy (a straightforward computation, which we will do in a moment) but immensely important: It shows that $\operatorname{Prim} H$ is a Lie subalgebra of the Lie algebra H (with the Lie bracket being given by the commutator).

Next, we shall need a basic fact about sums, known as the *telescope principle*:

Lemma 17.15. Let k be a field. Let A be a k-vector space. Let $m \in \mathbb{N}$. Let $a_0, a_1, \ldots, a_m$ be $m+1$ elements of A.

(a) Then,

$$\sum_{j=1}^{m} \left(a_{j-1} - a_j\right) = a_0 - a_m.$$

(b) Let M be a k-vector subspace of A. Assume that $a_{j-1} - a_j \in M$ for each $j \in \{1, 2, \ldots, m\}$. Then, $a_0 \equiv a_m \bmod M$.

Less easy (but completely elementary – it could be an exercise in basic algebra) is the following proposition:

Proposition 17.16. Let k be a field. Let A be a k-algebra. Let V be a k-vector subspace of A. Assume that

$$xy - yx \in V \qquad \text{for any } x \in V \text{ and } y \in V. \tag{153}$$

(a) For any positive $n \in \mathbb{N}$, any $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ and any $\sigma \in S_n$, we have

$$v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \equiv v_1 v_2 \cdots v_n \bmod V^{n-1}.$$

(b) Assume that the field k has characteristic 0. For any $\ell \in \mathbb{N}$, we have

$$\sum_{i=0}^{\ell} V^i = \sum_{i=0}^{\ell} \operatorname{symp}_i V.$$

91

Let us now step to the proofs of these facts. We begin with the straightforward proof of Proposition 17.14:

Proof of Proposition 17.14. Let $x \in \operatorname{Prim} H$ and $y \in \operatorname{Prim} H$.

Since $x \in \operatorname{Prim} H =$ (the set of all primitive elements of H), the element x of H is primitive. In other words, $\Delta(x) = x \otimes 1_H + 1_H \otimes x$ (by the definition of "primitive"). Similarly, $\Delta(y) = y \otimes 1_H + 1_H \otimes y$.

[91] Recall that V^i is to be understood as in Convention 15.2. Hence, V^i means the i-th power of the subspace V of the k-algebra A.

Since H is a bialgebra,

$$\begin{aligned}
\Delta(xy) &= \underbrace{\Delta(x)}_{=x\otimes 1_H+1_H\otimes x} \cdot \underbrace{\Delta(y)}_{=y\otimes 1_H+1_H\otimes y} \qquad \text{(by the axioms of a bialgebra)} \\
&= (x\otimes 1_H + 1_H\otimes x)\cdot(y\otimes 1_H + 1_H\otimes y) \\
&= \underbrace{(x\otimes 1_H)\cdot(y\otimes 1_H)}_{=xy\otimes 1_H 1_H} + \underbrace{(x\otimes 1_H)\cdot(1_H\otimes y)}_{=x1_H\otimes 1_H y} + \underbrace{(1_H\otimes x)\cdot(y\otimes 1_H)}_{=1_H y\otimes x1_H} + \underbrace{(1_H\otimes x)\cdot(1_H\otimes y)}_{=1_H 1_H\otimes xy} \\
&= xy\otimes \underbrace{1_H 1_H}_{=1_H} + \underbrace{x1_H}_{=x}\otimes\underbrace{1_H y}_{=y} + \underbrace{1_H y}_{=y}\otimes\underbrace{x1_H}_{=x} + \underbrace{1_H 1_H}_{=1_H}\otimes xy \\
&= xy\otimes 1_H + x\otimes y + y\otimes x + 1_H\otimes xy.
\end{aligned}$$

The same argument, but with x and y transposed, yields

$$\Delta(yx) = yx\otimes 1_H + y\otimes x + x\otimes y + 1_H\otimes yx.$$

Now, since Δ is k-linear, we have

$$\begin{aligned}
\Delta(xy-yx) &= \underbrace{\Delta(xy)}_{=xy\otimes 1_H+x\otimes y+y\otimes x+1_H\otimes xy} - \underbrace{\Delta(yx)}_{=yx\otimes 1_H+y\otimes x+x\otimes y+1_H\otimes yx} \\
&= (xy\otimes 1_H + x\otimes y + y\otimes x + 1_H\otimes xy) - (yx\otimes 1_H + y\otimes x + x\otimes y + 1_H\otimes yx) \\
&= \underbrace{xy\otimes 1_H - yx\otimes 1_H}_{=(xy-yx)\otimes 1_H} + \underbrace{1_H\otimes xy - 1_H\otimes yx}_{=1_H\otimes(xy-yx)} \\
&= (xy-yx)\otimes 1_H + 1_H\otimes(xy-yx).
\end{aligned}$$

In other words, $xy-yx$ is primitive (by the definition of "primitive"). Thus, $xy-yx \in$ (the set of all primitive elements of H) $= \operatorname{Prim} H$. This proves Proposition 17.14. $\square$

Next, let us prove Lemma 17.15.

Proof of Lemma 17.15. **(a)** If $m=0$, then Lemma 17.15 **(a)** holds[92]. Hence, for the rest of our proof of Lemma 17.15 **(a)**, we can WLOG assume that we don't have $m=0$. Assume this.

[92] *Proof.* Assume that $m=0$. We must show that Lemma 17.15 **(a)** holds.

We have $m=0$ and thus $\sum_{j=1}^{m}(a_{j-1}-a_j) = \sum_{j=1}^{0}(a_{j-1}-a_j) =$ (empty sum) $= 0$. Comparing this with $a_0 - \underbrace{a_m}_{\substack{=a_0 \\ (\text{since } m=0)}} = a_0 - a_0 = 0$, we obtain $\sum_{j=1}^{m}(a_{j-1}-a_j) = a_0 - a_m$. Thus, Lemma 17.15 **(a)** holds. Qed.

We have $m \neq 0$ (since we don't have $m = 0$). Thus, $m \geq 1$ (since $m \in \mathbb{N}$). Now,

$$\begin{aligned}
&\sum_{j=1}^{m} (a_{j-1} - a_j) \\
&= \sum_{j=1}^{m} a_{j-1} - \sum_{j=1}^{m} a_j \\
&= \underbrace{\sum_{j=0}^{m-1} a_j}_{\substack{= a_0 + \sum_{j=1}^{m-1} a_j \\ \text{(here, we have split off the addend for } j=0 \\ \text{from the sum, because } m \geq 1)}} - \underbrace{\sum_{j=1}^{m} a_j}_{\substack{= \sum_{j=1}^{m-1} a_j + a_m \\ \text{(here, we have split off the addend for } j=m \\ \text{from the sum, because } m \geq 1)}} \\
&\qquad \text{(here, we substituted } j \text{ for } j-1 \text{ in the first sum)} \\
&= \left(a_0 + \sum_{j=1}^{m-1} a_j \right) - \left(\sum_{j=1}^{m-1} a_j + a_m \right) = a_0 - a_m.
\end{aligned}$$

This proves Lemma 17.15 **(a)**.

(b) We assumed that $a_{j-1} - a_j \in M$ for each $j \in \{1, 2, \ldots, m\}$. Thus, $\sum_{j=1}^{m} \underbrace{(a_{j-1} - a_j)}_{\in M} \in \sum_{j=1}^{m} M \subseteq M$ (since M is a k-vector space). Now, Lemma 17.15 **(a)** yields

$$a_0 - a_m = \sum_{j=1}^{m} (a_{j-1} - a_j) \in M.$$

In other words, $a_0 \equiv a_m \bmod M$. This proves Lemma 17.15 **(b)**. □

Before we step to the proof of Proposition 17.16, let us recall a known fact from linear algebra:

$$\left(\begin{array}{c} \text{if } M \text{ is a } k\text{-vector space, if } S \text{ is a subset of } M, \text{ and if } Q \text{ is a} \\ k\text{-vector subspace of } M \text{ such that } S \subseteq Q, \text{ then } \langle S \rangle \subseteq Q \end{array} \right). \tag{154}$$

Now, let us show Proposition 17.16:

Proof of Proposition 17.16. **(a)** Let $n \in \mathbb{N}$, $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ and $\sigma \in S_n$ be arbitrary.

For every $i \in \{1, 2, \ldots, n-1\}$, let τ_i denote the transposition $(i, i+1) \in S_n$.

Now, it is known that every element of the symmetric group S_n can be written as a product of some transpositions from the set $\{\tau_1, \tau_2, \ldots, \tau_{n-1}\}$ [93]. Applying this to the element $\sigma \in S_n$, we conclude that σ can be written as a product of some transpositions from the set $\{\tau_1, \tau_2, \ldots, \tau_{n-1}\}$. In other words, there exists a natural number $m \in \mathbb{N}$ and a sequence $(i_1, i_2, \ldots, i_m) \in \{1, 2, \ldots, n-1\}^{\times m}$

[93] Indeed, this is precisely the claim of [Grinbe17, Exercise 5.1 **(b)**] (since the transpositions that we denote by $\tau_1, \tau_2, \ldots, \tau_{n-1}$ have been denoted by $s_1, s_2, \ldots, s_{n-1}$ in [Grinbe17]).

such that $\sigma = \tau_{i_1}\tau_{i_2}\cdots\tau_{i_m}$. Consider this m and this $(i_1, i_2, \ldots, i_m)$. For every $j \in \{0, 1, \ldots, m\}$, let σ_j denote the permutation $\tau_{i_1}\tau_{i_2}\cdots\tau_{i_j} \in S_n$. Then, $\sigma_0 = \tau_{i_1}\tau_{i_2}\cdots\tau_{i_0} =$ (empty product) $=$ id and $\sigma_m = \tau_{i_1}\tau_{i_2}\cdots\tau_{i_m} = \sigma$. Moreover, every $j \in \{1, 2, \ldots, m\}$ satisfies $v_{\sigma_{j-1}(1)}v_{\sigma_{j-1}(2)}\cdots v_{\sigma_{j-1}(n)} - v_{\sigma_j(1)}v_{\sigma_j(2)}\cdots v_{\sigma_j(n)} \in V^{n-1}$. [94] Thus, Lemma 17.15 **(b)** (applied to $M = V^{n-1}$ and $a_j = v_{\sigma_j(1)}v_{\sigma_j(2)}\cdots v_{\sigma_j(n)}$) yields

$$v_{\sigma_0(1)}v_{\sigma_0(2)}\cdots v_{\sigma_0(n)} \equiv v_{\sigma_m(1)}v_{\sigma_m(2)}\cdots v_{\sigma_m(n)} \bmod V^{n-1}$$

(since V^{n-1} is a k-vector subspace of A). But from $\sigma_0 = \mathrm{id}$, we obtain

$$v_{\sigma_0(1)}v_{\sigma_0(2)}\cdots v_{\sigma_0(n)} = v_{\mathrm{id}(1)}v_{\mathrm{id}(2)}\cdots v_{\mathrm{id}(n)} = v_1v_2\cdots v_n,$$

[94] *Proof.* Let $j \in \{1, 2, \ldots, m\}$ be arbitrary. Then,

$$\underbrace{\sigma_{j-1}}_{\substack{=\tau_{i_1}\tau_{i_2}\cdots\tau_{i_{j-1}} \\ \text{(by the formula } \sigma_j=\tau_{i_1}\tau_{i_2}\cdots\tau_{i_j}\text{,} \\ \text{applied to } j-1 \text{ instead of } j)}} \tau_{i_j} = \tau_{i_1}\tau_{i_2}\cdots\tau_{i_{j-1}}\tau_{i_j} = \tau_{i_1}\tau_{i_2}\cdots\tau_{i_j} = \sigma_j,$$

so that $\sigma_j = \sigma_{j-1}\tau_{i_j}$. Denote i_j by $\mathbf{I}$. Then, $\sigma_j = \sigma_{j-1}\tau_{i_j}$ rewrites as $\sigma_j = \sigma_{j-1}\tau_{\mathbf{I}}$.

Since $\tau_{\mathbf{I}} = (\mathbf{I}, \mathbf{I}+1)$, every $\ell \in \{1, 2, \ldots, \mathbf{I}-1\}$ satisfies

$$\tau_{\mathbf{I}}(\ell) = (\mathbf{I}, \mathbf{I}+1)(\ell) = \ell \qquad (\text{since } \ell \in \{1, 2, \ldots, \mathbf{I}-1\}, \text{ so that } \ell \notin \{\mathbf{I}, \mathbf{I}+1\})$$

and thus

$$\begin{aligned} v_{\sigma_j(\ell)} &= v_{\sigma_{j-1}(\tau_{\mathbf{I}}(\ell))} \qquad (\text{since } \sigma_j = \sigma_{j-1}\tau_{\mathbf{I}} \text{ and thus } \sigma_j(\ell) = (\sigma_{j-1}\tau_{\mathbf{I}})(\ell) = \sigma_{j-1}(\tau_{\mathbf{I}}(\ell))) \\ &= v_{\sigma_{j-1}(\ell)} \qquad (\text{since } \tau_{\mathbf{I}}(\ell) = \ell). \end{aligned}$$

In other words, $v_{\sigma_j(1)} = v_{\sigma_{j-1}(1)}$, $v_{\sigma_j(2)} = v_{\sigma_{j-1}(2)}$, …, $v_{\sigma_j(\mathbf{I}-1)} = v_{\sigma_{j-1}(\mathbf{I}-1)}$. Multiplying these $\mathbf{I}-1$ equations, we obtain $v_{\sigma_j(1)}v_{\sigma_j(2)}\cdots v_{\sigma_j(\mathbf{I}-1)} = v_{\sigma_{j-1}(1)}v_{\sigma_{j-1}(2)}\cdots v_{\sigma_{j-1}(\mathbf{I}-1)}$.

Since $\tau_{\mathbf{I}} = (\mathbf{I}, \mathbf{I}+1)$, every $\ell \in \{\mathbf{I}+2, \mathbf{I}+3, \ldots, n\}$ satisfies

$$\tau_{\mathbf{I}}(\ell) = (\mathbf{I}, \mathbf{I}+1)(\ell) = \ell \qquad (\text{since } \ell \in \{\mathbf{I}+2, \mathbf{I}+3, \ldots, n\}, \text{ so that } \ell \notin \{\mathbf{I}, \mathbf{I}+1\})$$

and thus

$$\begin{aligned} v_{\sigma_j(\ell)} &= v_{\sigma_{j-1}(\tau_{\mathbf{I}}(\ell))} \qquad (\text{since } \sigma_j = \sigma_{j-1}\tau_{\mathbf{I}} \text{ and thus } \sigma_j(\ell) = (\sigma_{j-1}\tau_{\mathbf{I}})(\ell) = \sigma_{j-1}(\tau_{\mathbf{I}}(\ell))) \\ &= v_{\sigma_{j-1}(\ell)} \qquad (\text{since } \tau_{\mathbf{I}}(\ell) = \ell). \end{aligned}$$

In other words, $v_{\sigma_j(\mathbf{I}+2)} = v_{\sigma_{j-1}(\mathbf{I}+2)}$, $v_{\sigma_j(\mathbf{I}+3)} = v_{\sigma_{j-1}(\mathbf{I}+3)}$, …, $v_{\sigma_j(n)} = v_{\sigma_{j-1}(n)}$. Multiplying these $n-(\mathbf{I}+1)$ equations, we obtain $v_{\sigma_j(\mathbf{I}+2)}v_{\sigma_j(\mathbf{I}+3)}\cdots v_{\sigma_j(n)} = v_{\sigma_{j-1}(\mathbf{I}+2)}v_{\sigma_{j-1}(\mathbf{I}+3)}\cdots v_{\sigma_{j-1}(n)}$.

Since $\tau_{\mathbf{I}} = (\mathbf{I}, \mathbf{I}+1)$, we have $\tau_{\mathbf{I}}(\mathbf{I}) = \mathbf{I}+1$ and

$$\begin{aligned} v_{\sigma_j(\mathbf{I})} &= v_{\sigma_{j-1}(\tau_{\mathbf{I}}(\mathbf{I}))} \qquad (\text{since } \sigma_j = \sigma_{j-1}\tau_{\mathbf{I}} \text{ and thus } \sigma_j(\mathbf{I}) = (\sigma_{j-1}\tau_{\mathbf{I}})(\mathbf{I}) = \sigma_{j-1}(\tau_{\mathbf{I}}(\mathbf{I}))) \\ &= v_{\sigma_{j-1}(\mathbf{I}+1)} \qquad (\text{since } \tau_{\mathbf{I}}(\mathbf{I}) = \mathbf{I}+1). \end{aligned}$$

Since $\tau_{\mathbf{I}} = (\mathbf{I}, \mathbf{I}+1)$, we have $\tau_{\mathbf{I}}(\mathbf{I}+1) = \mathbf{I}$ and

$$\begin{aligned} v_{\sigma_j(\mathbf{I}+1)} &= v_{\sigma_{j-1}(\tau_{\mathbf{I}}(\mathbf{I}+1))} \qquad (\text{since } \sigma_j = \sigma_{j-1}\tau_{\mathbf{I}} \text{ and thus } \sigma_j(\mathbf{I}+1) = (\sigma_{j-1}\tau_{\mathbf{I}})(\mathbf{I}+1) = \sigma_{j-1}(\tau_{\mathbf{I}}(\mathbf{I}+1))) \\ &= v_{\sigma_{j-1}(\mathbf{I})} \qquad (\text{since } \tau_{\mathbf{I}}(\mathbf{I}+1) = \mathbf{I}). \end{aligned}$$

Since $(v_1, v_2, \ldots, v_n) \in V^{\times n}$, we have $v_{\sigma_{j-1}(\mathbf{I})} \in V$ and $v_{\sigma_{j-1}(\mathbf{I}+1)} \in V$. Thus, (153) (applied to $x = v_{\sigma_{j-1}(\mathbf{I})}$ and $y = v_{\sigma_{j-1}(\mathbf{I}+1)}$) yields that $v_{\sigma_{j-1}(\mathbf{I})}v_{\sigma_{j-1}(\mathbf{I}+1)} - v_{\sigma_{j-1}(\mathbf{I}+1)}v_{\sigma_{j-1}(\mathbf{I})} \in V$.

so that

$$\begin{aligned} v_1 v_2 \cdots v_n &= v_{\sigma_0(1)} v_{\sigma_0(2)} \cdots v_{\sigma_0(n)} \equiv v_{\sigma_m(1)} v_{\sigma_m(2)} \cdots v_{\sigma_m(n)} \\ &= v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \bmod V^{n-1} \qquad (\text{since } \sigma_m = \sigma). \end{aligned}$$

This proves Proposition 17.16 **(a)**.

(b) Let us prove Proposition 17.16 **(b)** by induction over ℓ:

Induction base: We have

$$\sum_{i=0}^{0} V^i = V^0 = k \cdot 1_A$$

and

$$\sum_{i=0}^{0} \operatorname{symp}_i V = \operatorname{symp}_0 V = k \cdot 1_A,$$

so that $\sum\limits_{i=0}^{0} V^i = \sum\limits_{i=0}^{0} \operatorname{symp}_i V$. In other words, Proposition 17.16 **(b)** holds for $\ell = 0$. This completes the induction base.

Induction step: Let $n \in \mathbb{N}$ be positive. Assume that Proposition 17.16 **(b)** holds for $\ell = n-1$. We now must prove that Proposition 17.16 **(b)** holds for $\ell = n$ as well.

Since Proposition 17.16 **(b)** holds for $\ell = n-1$, we have

$$\sum_{i=0}^{n-1} V^i = \sum_{i=0}^{n-1} \operatorname{symp}_i V. \tag{155}$$

Now,

$$\begin{aligned}
&\underbrace{v_{\sigma_{j-1}(1)} v_{\sigma_{j-1}(2)} \cdots v_{\sigma_{j-1}(n)}}_{= \left(v_{\sigma_{j-1}(1)} v_{\sigma_{j-1}(2)} \cdots v_{\sigma_{j-1}(\mathbf{I}-1)}\right) v_{\sigma_{j-1}(\mathbf{I})} v_{\sigma_{j-1}(\mathbf{I}+1)} \left(v_{\sigma_{j-1}(\mathbf{I}+2)} v_{\sigma_{j-1}(\mathbf{I}+3)} \cdots v_{\sigma_{j-1}(n)}\right)} \\
&\quad - \underbrace{v_{\sigma_j(1)} v_{\sigma_j(2)} \cdots v_{\sigma_j(n)}}_{= \left(v_{\sigma_j(1)} v_{\sigma_j(2)} \cdots v_{\sigma_j(\mathbf{I}-1)}\right) v_{\sigma_j(\mathbf{I})} v_{\sigma_j(\mathbf{I}+1)} \left(v_{\sigma_j(\mathbf{I}+2)} v_{\sigma_j(\mathbf{I}+3)} \cdots v_{\sigma_j(n)}\right)} \\
&= \left(v_{\sigma_{j-1}(1)} v_{\sigma_{j-1}(2)} \cdots v_{\sigma_{j-1}(\mathbf{I}-1)}\right) v_{\sigma_{j-1}(\mathbf{I})} v_{\sigma_{j-1}(\mathbf{I}+1)} \left(v_{\sigma_{j-1}(\mathbf{I}+2)} v_{\sigma_{j-1}(\mathbf{I}+3)} \cdots v_{\sigma_{j-1}(n)}\right) \\
&\quad - \underbrace{\left(v_{\sigma_j(1)} v_{\sigma_j(2)} \cdots v_{\sigma_j(\mathbf{I}-1)}\right)}_{= v_{\sigma_{j-1}(1)} v_{\sigma_{j-1}(2)} \cdots v_{\sigma_{j-1}(\mathbf{I}-1)}} \underbrace{v_{\sigma_j(\mathbf{I})}}_{= v_{\sigma_{j-1}(\mathbf{I}+1)}} \underbrace{v_{\sigma_j(\mathbf{I}+1)}}_{= v_{\sigma_{j-1}(\mathbf{I})}} \underbrace{\left(v_{\sigma_j(\mathbf{I}+2)} v_{\sigma_j(\mathbf{I}+3)} \cdots v_{\sigma_j(n)}\right)}_{= v_{\sigma_{j-1}(\mathbf{I}+2)} v_{\sigma_{j-1}(\mathbf{I}+3)} \cdots v_{\sigma_{j-1}(n)}} \\
&= \left(v_{\sigma_{j-1}(1)} v_{\sigma_{j-1}(2)} \cdots v_{\sigma_{j-1}(\mathbf{I}-1)}\right) v_{\sigma_{j-1}(\mathbf{I})} v_{\sigma_{j-1}(\mathbf{I}+1)} \left(v_{\sigma_{j-1}(\mathbf{I}+2)} v_{\sigma_{j-1}(\mathbf{I}+3)} \cdots v_{\sigma_{j-1}(n)}\right) \\
&\quad - \left(v_{\sigma_{j-1}(1)} v_{\sigma_{j-1}(2)} \cdots v_{\sigma_{j-1}(\mathbf{I}-1)}\right) v_{\sigma_{j-1}(\mathbf{I}+1)} v_{\sigma_{j-1}(\mathbf{I})} \left(v_{\sigma_{j-1}(\mathbf{I}+2)} v_{\sigma_{j-1}(\mathbf{I}+3)} \cdots v_{\sigma_{j-1}(n)}\right) \\
&= \underbrace{\left(v_{\sigma_{j-1}(1)} v_{\sigma_{j-1}(2)} \cdots v_{\sigma_{j-1}(\mathbf{I}-1)}\right)}_{\substack{\in V^{\mathbf{I}-1} \\ (\text{since } (v_1, v_2, \ldots, v_n) \in V^{\times n}, \text{ so that} \\ v_{\sigma_{j-1}(1)}, v_{\sigma_{j-1}(2)}, \ldots, v_{\sigma_{j-1}(\mathbf{I}-1)} \\ \text{all lie in } V)}} \underbrace{\left(v_{\sigma_{j-1}(\mathbf{I})} v_{\sigma_{j-1}(\mathbf{I}+1)} - v_{\sigma_{j-1}(\mathbf{I}+1)} v_{\sigma_{j-1}(\mathbf{I})}\right)}_{\in V = V^1} \underbrace{\left(v_{\sigma_{j-1}(\mathbf{I}+2)} v_{\sigma_{j-1}(\mathbf{I}+3)} \cdots v_{\sigma_{j-1}(n)}\right)}_{\substack{\in V^{n-(\mathbf{I}+1)} \\ (\text{since } (v_1, v_2, \ldots, v_n) \in V^{\times n}, \text{ so that} \\ v_{\sigma_{j-1}(\mathbf{I}+2)}, v_{\sigma_{j-1}(\mathbf{I}+3)}, \ldots, v_{\sigma_{j-1}(n)} \\ \text{all lie in } V)}} \\
&\in V^{\mathbf{I}-1} \cdot V^1 \cdot V^{n-(\mathbf{I}+1)} = V^{(\mathbf{I}-1)+1+(n-(\mathbf{I}+1))} = V^{n-1},
\end{aligned}$$

qed.

Next, we notice that

$$\begin{aligned}
&\left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \\
&\subseteq \left\langle \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle \\
&= \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle = \operatorname{symp}_n V.
\end{aligned}$$

Thus,

$$\text{every } (v_1, v_2, \ldots, v_n) \in V^{\times n} \text{ satisfies } \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \in \operatorname{symp}_n V. \tag{156}$$

On the other hand, every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies

$$\begin{aligned}
\frac{1}{n!} \sum_{\sigma \in S_n} \underbrace{v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}}_{\substack{\equiv v_1 v_2 \cdots v_n \bmod V^{n-1} \\ \text{(by Proposition 17.16 \textbf{(a)})}}} &\equiv \frac{1}{n!} \underbrace{\sum_{\sigma \in S_n} v_1 v_2 \cdots v_n}_{= |S_n| \cdot v_1 v_2 \cdots v_n} = \frac{1}{n!} \underbrace{|S_n|}_{=n!} \cdot v_1 v_2 \cdots v_n \\
&= \frac{1}{n!} n! \cdot v_1 v_2 \cdots v_n = v_1 v_2 \cdots v_n \bmod V^{n-1},
\end{aligned}$$

so that $v_1 v_2 \cdots v_n \equiv \dfrac{1}{n!} \sum\limits_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \bmod V^{n-1}$, and thus

$$\begin{aligned}
v_1 v_2 \cdots v_n &\in \underbrace{\frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}}_{\substack{\in \operatorname{symp}_n V \\ \text{(by (156))}}} + \underbrace{V^{n-1}}_{\substack{\subseteq \sum_{i=0}^{n-2} V^i + V^{n-1} = \sum_{i=0}^{n-1} V^i \\ = \sum_{i=0}^{n-1} \operatorname{symp}_i V \\ \text{(by (155))}}} \\
&\subseteq \operatorname{symp}_n V + \sum_{i=0}^{n-1} \operatorname{symp}_i V = \sum_{i=0}^{n} \operatorname{symp}_i V.
\end{aligned}$$

In other words,

$$\left\{ v_1 v_2 \cdots v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \subseteq \sum_{i=0}^{n} \operatorname{symp}_i V.$$

Hence, (154) (applied to $M = A$, $S = \left\{ v_1 v_2 \cdots v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}$ and $Q = \sum\limits_{i=0}^{n} \operatorname{symp}_i V$) yields

$$\left\langle \left\{ v_1 v_2 \cdots v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle \subseteq \sum_{i=0}^{n} \operatorname{symp}_i V.$$

Since

$$\left\langle \left\{ v_1 v_2 \cdots v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle = \left\langle v_1 v_2 \cdots v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle$$
$$= V^n \qquad \text{(by (73))},$$

this becomes $V^n \subseteq \sum_{i=0}^{n} \operatorname{symp}_i V$. Thus,

$$\sum_{i=0}^{n} V^i = \underbrace{\sum_{i=0}^{n-1} V^i}_{\substack{= \sum_{i=0}^{n-1} \operatorname{symp}_i V \\ \text{(by (155))}}} + \underbrace{V^n}_{\subseteq \sum_{i=0}^{n} \operatorname{symp}_i V} \subseteq \underbrace{\sum_{i=0}^{n-1} \operatorname{symp}_i V}_{\substack{\subseteq \sum_{i=0}^{n} \operatorname{symp}_i V \\ \text{(since } n-1 \leq n\text{)}}} + \sum_{i=0}^{n} \operatorname{symp}_i V$$
$$\subseteq \sum_{i=0}^{n} \operatorname{symp}_i V + \sum_{i=0}^{n} \operatorname{symp}_i V \subseteq \sum_{i=0}^{n} \operatorname{symp}_i V \tag{157}$$

(since $\sum_{i=0}^{n} \operatorname{symp}_i V$ is a k-vector space).

On the other hand, every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies

$$\frac{1}{n!} \sum_{\sigma \in S_n} \underbrace{v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}}_{\substack{\in V^n \\ \text{(since } v_{\sigma(1)}, v_{\sigma(2)}, \ldots, v_{\sigma(n)} \text{ all lie in } V\text{)}}} \in \frac{1}{n!} \sum_{\sigma \in S_n} V^n \subseteq V^n$$

(since V^n is a k-vector space). In other words,

$$\left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \subseteq V^n.$$

Hence, (154) (applied to $M = A$, $S = \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}$ and $Q = V^n$) yields

$$\left\langle \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle \subseteq V^n.$$

Since

$$\left\langle \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle$$
$$= \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle = \operatorname{symp}_n V,$$

this rewrites as $\operatorname{symp}_n V \subseteq V^n$. Thus,

$$\sum_{i=0}^{n} \operatorname{symp}_i V = \underbrace{\sum_{i=0}^{n-1} \operatorname{symp}_i V}_{\substack{= \sum_{i=0}^{n-1} V^i \\ \text{(by (155))}}} + \underbrace{\operatorname{symp}_n V}_{\subseteq V^n} \subseteq \sum_{i=0}^{n-1} V^i + V^n = \sum_{i=0}^{n} V^i.$$

Combined with (157), this yields

$$\sum_{i=0}^{n} V^i = \sum_{i=0}^{n} \operatorname{symp}_i V.$$

In other words, Proposition 17.16 **(b)** is proven for $\ell = n$. This completes the induction step. Thus, the induction proof of Proposition 17.16 **(b)** is complete. □

Proof of Proposition 17.13. Let $\ell \in \mathbb{N}$.

Let $A = H$ and $V = \operatorname{Prim} H$. Then, the condition (153) of Proposition 17.16 is satisfied (because Proposition 17.14 tells us that $xy - yx \in \operatorname{Prim} H$ for any $x \in \operatorname{Prim} H$ and $y \in \operatorname{Prim} H$). Thus, we can apply Proposition 17.16 **(b)** and conclude that $\sum_{i=0}^{\ell} V^i = \sum_{i=0}^{\ell} \operatorname{symp}_i V$. Since $V = \operatorname{Prim} H$, this becomes $\sum_{i=0}^{\ell} (\operatorname{Prim} H)^i = \sum_{i=0}^{\ell} \operatorname{symp}_i (\operatorname{Prim} H)$. But Proposition 17.3 yields

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} (\operatorname{Prim} H)^i = \sum_{i=0}^{\ell} \operatorname{symp}_i (\operatorname{Prim} H).$$

This proves Proposition 17.13. □

Proof of Theorem 17.12. For every $\ell \in \mathbb{N}$, Proposition 17.13 yields

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} \operatorname{symp}_i (\operatorname{Prim} H) \subseteq \sum_{i \in \mathbb{N}} \operatorname{symp}_i (\operatorname{Prim} H).$$

Since H is filtered, we have

$$H = \bigcup_{\ell \in \mathbb{N}} \underbrace{H_{\leq \ell}}_{\subseteq \sum_{i \in \mathbb{N}} \operatorname{symp}_i (\operatorname{Prim} H)} \subseteq \bigcup_{\ell \in \mathbb{N}} \sum_{i \in \mathbb{N}} \operatorname{symp}_i (\operatorname{Prim} H) = \sum_{i \in \mathbb{N}} \operatorname{symp}_i (\operatorname{Prim} H).$$

Combined with $\sum_{i \in \mathbb{N}} \operatorname{symp}_i (\operatorname{Prim} H) \subseteq H$ (which is trivial), this yields $H = \sum_{i \in \mathbb{N}} \operatorname{symp}_i (\operatorname{Prim} H)$. This proves Theorem 17.12. □

§18. Intermezzo on homogeneous subspaces

As often happens with properties of filtered bialgebras, the particular case of Theorem 17.12 for a *graded* bialgebra H can be somewhat extended using the grading. Before we formulate this extension, we introduce an auxiliary notion. This is the notion of *homogeneous subspaces* of graded vector spaces. There are several equivalent definitions of this notion; here, we will use the following one:

Definition 18.1. Let k be a field. Let V be a graded k-vector space. Let W be a k-vector subspace of V.

We say that W is a *homogeneous subspace* of V if $W = \bigoplus_{n \in \mathbb{N}} (W \cap V_n)$.

Note that the internal direct sum $\bigoplus_{n\in\mathbb{N}} (W \cap V_n)$ is always well-defined[95], and thus always is a k-vector subspace of W [96]. But it is not always the whole W.

A basic fact from linear algebra:

Remark 18.2. Let k be a field. Let U and V be two graded k-vector spaces. Let $f : V \to U$ be a graded k-linear map. Then, $\operatorname{Ker} f$ is a homogeneous subspace of V.

Proof of Remark 18.2. Let $W = \operatorname{Ker} f$. By Definition 18.1, we know that the internal direct sum $\bigoplus_{n\in\mathbb{N}} (W \cap V_n)$ is well-defined and a k-vector subspace of W. We are now going to show that $W = \bigoplus_{n\in\mathbb{N}} (W \cap V_n)$.

Let $w \in W$. Then, $w \in W = \operatorname{Ker} f \subseteq V$ and $f(w) = 0$ (since $w \in \operatorname{Ker} f$). Now, for every $n \in \mathbb{N}$, we have

$$f(p_{n,V}(w)) = \underbrace{(f \circ p_{n,V})}_{\substack{=p_{n,U}\circ f \\ \text{(by Proposition 16.17,} \\ \text{applied to } U \text{ instead of } W)}} (w) = (p_{n,U} \circ f)(w) = p_{n,U}\left(\underbrace{f(w)}_{=0}\right) = p_{n,U}(0) = 0$$

and thus $p_{n,V}(w) \in \operatorname{Ker} f$. But for every $n \in \mathbb{N}$, we also have $p_{n,V}\left(\underbrace{w}_{\in V}\right) \in p_{n,V}(V) = V_n$ (by (112)). Thus, for every $n \in \mathbb{N}$, we have $p_{n,V}(w) \in W \cap V_n$ (this results from combining $p_{n,V}(w) \in \operatorname{Ker} f = W$ and $p_{n,V}(w) \in V_n$). But (114) (applied to $v = w$) yields

$$w = \sum_{\ell\in\mathbb{N}} p_{\ell,V}(w) = \sum_{n\in\mathbb{N}} \underbrace{p_{n,V}(w)}_{\in W\cap V_n} \qquad \text{(here, we renamed the index } \ell \text{ as } n \text{ in the sum)}$$
$$\in \sum_{n\in\mathbb{N}} (W \cap V_n) = \bigoplus_{n\in\mathbb{N}} (W \cap V_n).$$

[95] *Proof.* Since V is a graded k-vector space, we have $V = \bigoplus_{n\in\mathbb{N}} V_n$. Thus, $\sum_{n\in\mathbb{N}} V_n$ is a direct sum. Hence,

$$\left(\begin{array}{c}\text{every family } (v_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} V_n \text{ satisfying } \sum_{n\in\mathbb{N}} v_n = 0 \text{ and} \\ (v_n = 0 \text{ for all but finitely many } n \in \mathbb{N}) \text{ must satisfy } (v_n)_{n\in\mathbb{N}} = (0)_{n\in\mathbb{N}}\end{array}\right). \tag{158}$$

Now, it follows that every family $(v_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} (W \cap V_n)$ satisfying $\sum_{n\in\mathbb{N}} v_n = 0$ and ($v_n = 0$ for all but finitely many $n \in \mathbb{N}$) must satisfy $(v_n)_{n\in\mathbb{N}} = (0)_{n\in\mathbb{N}}$ (by (158), since $(v_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} (W \cap V_n)$ yields $(v_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} V_n$). In other words, $\sum_{n\in\mathbb{N}} (W \cap V_n)$ is a direct sum. Hence, the internal direct sum $\bigoplus_{n\in\mathbb{N}} (W \cap V_n)$ is well-defined, qed.

[96] *Proof.* Since direct sums are sums, we have $\bigoplus_{n\in\mathbb{N}} (W \cap V_n) = \sum_{n\in\mathbb{N}} \underbrace{(W \cap V_n)}_{\subseteq W} \subseteq \sum_{n\in\mathbb{N}} W \subseteq W$ (W is a k-vector space), qed.

Now forget that we fixed w. We thus have proven that every $w \in W$ satisfies $w \in \bigoplus_{n \in \mathbb{N}} (W \cap V_n)$. Thus, $W \subseteq \bigoplus_{n \in \mathbb{N}} (W \cap V_n)$. Combined with the (already known) relation $\bigoplus_{n \in \mathbb{N}} (W \cap V_n) \subseteq W$, this yields $W = \bigoplus_{n \in \mathbb{N}} (W \cap V_n)$. Thus, W is a homogeneous subspace of V (by the definition of "homogeneous subspace"). Since $W = \operatorname{Ker} f$, this yields that $\operatorname{Ker} f$ is a homogeneous subspace of V. This proves Remark 18.2. $\square$

Now we can see the following fundamental fact:

Proposition 18.3. Let k be a field. Let H be a graded k-bialgebra. Then, $\operatorname{Prim} H$ (this is the set of all primitive elements of H) is a homogeneous subspace of H.

Proof of Proposition 18.3. Define a map $f : H \to H$ by

$$(f(x) = \Delta(x) - x \otimes 1_H - 1_H \otimes x \qquad \text{for every } x \in H). \tag{159}$$

Then, this map f is k-linear (because Δ is k-linear, so that the term $\Delta(x) - x \otimes 1_H - 1_H \otimes x$ depends k-linearly on x). We are now going to prove that $\operatorname{Prim} H = \operatorname{Ker} f$ and that f is a graded map. Then, an application of Remark 18.2 will do the rest. Here are the details:

a) We have $\operatorname{Prim} H = \operatorname{Ker} f$.

Proof. We have

$$\begin{aligned}
\operatorname{Prim} H &= (\text{the set of all primitive elements of } H) \\
&= \left\{ x \in H \mid \underbrace{x \text{ is primitive}}_{\substack{\text{this is equivalent to } \Delta(x) = x \otimes 1_H + 1_H \otimes x \\ \text{(by the definition of "primitive")}}} \right\} \\
&= \left\{ x \in H \mid \underbrace{\Delta(x) = x \otimes 1_H + 1_H \otimes x}_{\substack{\text{this is equivalent to} \\ \Delta(x) - x \otimes 1_H - 1_H \otimes x = 0}} \right\} \\
&= \left\{ x \in H \mid \underbrace{\Delta(x) - x \otimes 1_H - 1_H \otimes x}_{= f(x) \text{ (by (159))}} = 0 \right\} \\
&= \{ x \in H \mid f(x) = 0 \} = \operatorname{Ker} f.
\end{aligned}$$

This proves part **a)**.

b) The map f is graded.

Proof. Let $n \in \mathbb{N}$. Since Δ is graded (because H is a graded k-coalgebra), we have $\Delta(H_n) \subseteq (H \otimes H)_n$. But by the definition of the tensor product of two graded k-vector spaces, we have $(H \otimes H)_n = \sum_{\ell=0}^{n} H_\ell \otimes H_{n-\ell}$. Hence,

$$(H \otimes H)_n = \sum_{\ell=0}^{n} H_\ell \otimes H_{n-\ell} = \sum_{\ell=0}^{n-1} H_\ell \otimes H_{n-\ell} + H_n \otimes H_{n-n} \supseteq H_n \otimes \underbrace{H_{n-n}}_{=H_0} = H_n \otimes H_0$$

and

$$(H \otimes H)_n = \sum_{\ell=0}^{n} H_\ell \otimes H_{n-\ell} = H_0 \otimes H_{n-0} + \sum_{\ell=1}^{n} H_\ell \otimes H_{n-\ell} \supseteq H_0 \otimes \underbrace{H_{n-0}}_{=H_n} = H_0 \otimes H_n.$$

Also, $1_H \in H_0$ (since H is a graded k-algebra).

Now, every $x \in H_n$ satisfies

$$\begin{aligned} f(x) &= \Delta\left(\underbrace{x}_{\in H_n}\right) - \underbrace{x}_{\in H_n} \otimes \underbrace{1_H}_{\in H_0} - \underbrace{1_H}_{\in H_0} \otimes \underbrace{x}_{\in H_n} \\ &\in \underbrace{\Delta(H_n)}_{\subseteq (H\otimes H)_n} - \underbrace{H_n \otimes H_0}_{\subseteq (H\otimes H)_n} - \underbrace{H_0 \otimes H_n}_{\subseteq (H\otimes H)_n} \\ &\subseteq (H \otimes H)_n - (H \otimes H)_n - (H \otimes H)_n \subseteq (H \otimes H)_n \end{aligned}$$

(since $(H \otimes H)_n$ is a k-vector space). In other words, $f(H_n) \subseteq (H \otimes H)_n$.

Now forget that we fixed n. Thus, we have proven that every $n \in \mathbb{N}$ satisfies $f(H_n) \subseteq (H \otimes H)_n$. In other words, the map f is graded. This proves part **b)**.

c) Since f is graded (by part **b)**), we can apply Remark 18.2 to $U = H$ and $V = H$, and conclude that $\operatorname{Ker} f$ is a homogeneous subspace of H. Since $\operatorname{Ker} f = \operatorname{Prim} H$ (by part **a)**), this yields that $\operatorname{Prim} H$ is a homogeneous subspace of H. This proves Proposition 18.3. □

§19. A graded Theorem 17.12

Now, to formulate the graded strengthening of Theorem 17.12, we define a notion:

Definition 19.1. Let k be a field of characteristic 0. Let A be a graded k-algebra. Let V be a k-vector subspace of A. Let $n \in \mathbb{N}$. Let μ be an n-tuple of nonnegative integers. Then, we define a k-vector subspace $\operatorname{symp}^\mu V$ of A as follows: Let V_i denote $V \cap A_i$ for every $i \in \mathbb{N}$. Write the n-tuple μ in the form $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$. Then, we define $\operatorname{symp}^\mu V$ as the k-vector subspace

$$\left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\rangle$$

of A (where S_n denotes the n-th symmetric group).

Definition 19.2. A *partition* will mean a nonincreasing finite sequence[97] of positive integers.

[97] A *finite sequence*, of course, means the same as a *tuple* (i. e., an object which, for a suitable n, is an n-tuple). The word "nonincreasing" means the same as "weakly decreasing": i.e., a sequence $(a_1, a_2, \ldots, a_n)$ is said to be *nonincreasing* if and only if $a_1 \geq a_2 \geq \cdots \geq a_n$. (The concept of "nonincreasing" is defined similarly for infinite sequences.)

Note that Definition 19.2 is not the only definition of a partition. There is a different definition, which defines a partition as a nonincreasing *infinite but essentially finite*[98] sequence of nonnegative integers. This definition of a partition is, of course, not directly equivalent to Definition 19.2, but it is essentially the same, since there exists a canonical bijection

(the set of nonincreasing finite sequences of positive integers)
$\to$ (the set of nonincreasing infinite but essentially finite sequences of nonnegative integers) .

[99]. We will not care about this here (we are not really studying partitions here) and just define a partition by Definition 19.2.

We now claim:

Theorem 19.3. Let k be a field of characteristic 0, and let H be a connected graded cocommutative bialgebra over k. Then,

$$H = \sum_{\lambda \text{ is a partition}} \operatorname{symp}^{\lambda} (\operatorname{Prim} H) .$$

Note that for every partition λ, the k-vector subspace $\operatorname{symp}^{\lambda} (\operatorname{Prim} H)$ of H is well-defined (due to Definition 19.1, since λ is an n-tuple for an appropriate n).

Note that Theorem 19.3 can be strengthened to:

Theorem 19.4. Let k be a field of characteristic 0, and let H be a connected graded cocommutative bialgebra over k. Then,

$$H = \bigoplus_{\lambda \text{ is a partition}} \operatorname{symp}^{\lambda} (\operatorname{Prim} H) .$$

Note that for every partition λ, the k-vector subspace $\operatorname{symp}^{\lambda} (\operatorname{Prim} H)$ of H is well-defined (due to Definition 19.1, since λ is an n-tuple for an appropriate n).

This is, however, a significantly harder result, requiring the Poincaré-Birkhoff-Witt and Cartier-Milnor-Moore theorems to prove; we will not prove this here.

We notice that [PatReu98] makes use of Theorem 19.4 in the proof of Theorem 4.3 in [PatReu98].[100] *However*, the proof of Theorem 4.3 in [PatReu98] does not need the

[98] A sequence of integers is said to be *essentially finite* if all but finitely many of its entries are 0.

[99] This bijection sends every nonincreasing finite sequence $(\lambda_1, \lambda_2, \ldots, \lambda_n)$ of positive integers to the infinite sequence $(\lambda_1, \lambda_2, \ldots, \lambda_n, 0, 0, \ldots)$. (The inverse of this bijection trims an infinite sequence after its last nonzero entry.)

[100] Namely, if we work with the notations of Section 4 of [PatReu98], then applying our Theorem 19.4 to $H = A$ yields $A = \bigoplus_{\lambda \text{ is a partition}} \operatorname{symp}^{\lambda} (\operatorname{Prim} A)$. But $\operatorname{symp}^{\lambda} (\operatorname{Prim} A)$ is exactly what was denoted by A^{λ} in [PatReu98]. Thus, we get $A = \bigoplus_{\lambda \text{ is a partition}} A^{\lambda}$ (still working with the notations of [PatReu98]). This fact is used in the proof of Theorem 4.3 in [PatReu98] (where it is proven using the Cartier-Milnor-Moore theorem and the Poincaré-Birkhoff-Witt theorem).

whole strength of Theorem 19.4; in fact it only uses Theorem 19.3.[101] Hence, our proof of Theorem 19.3 further below will relieve the proof of Theorem 4.3 in [PatReu98] from having to use the Cartier-Milnor-Moore and Poincaré-Birkhoff-Witt theorems.[102]

We will derive Theorem 19.3 from a rather elementary fact once again:

Proposition 19.5. Let k be a field of characteristic 0. Let A be a graded k-algebra. Let V be a homogeneous subspace of A such that $V \cap A_0 = 0$. Assume that

$$xy - yx \in V \qquad \text{for any } x \in V \text{ and } y \in V. \tag{160}$$

Then,

$$\sum_{i \in \mathbb{N}} V^i = \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V.$$

103

To prove this, we begin with a trivial consequence of Proposition 17.16:

Proposition 19.6. Let k be a field of characteristic 0. Let A be a k-algebra. Let V be a k-vector subspace of A. Assume that

$$xy - yx \in V \qquad \text{for any } x \in V \text{ and } y \in V.$$

Then,

$$\sum_{i \in \mathbb{N}} V^i = \sum_{i \in \mathbb{N}} \operatorname{symp}_i V.$$

(Here, V^i is to be understood as in Proposition 19.5.)

Proof of Proposition 19.6. Every $\ell \in \mathbb{N}$ satisfies

$$\begin{aligned} V^\ell &\subseteq V^\ell + \sum_{i=0}^{\ell-1} V^i = \sum_{i=0}^{\ell} V^i = \sum_{i=0}^{\ell} \operatorname{symp}_i V \qquad \text{(by Proposition 17.16 } \mathbf{(b)}\text{)} \\ &\subseteq \sum_{i \in \mathbb{N}} \operatorname{symp}_i V \end{aligned} \tag{161}$$

[101] In fact, if we work with the notations of Section 4 of [PatReu98], then applying our Theorem 19.3 to $H = A$ yields $A = \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda (\operatorname{Prim} A)$. But $\operatorname{symp}^\lambda (\operatorname{Prim} A)$ is exactly what was denoted by A^λ in [PatReu98]. Thus, we get $A = \sum_{\lambda \text{ is a partition}} A^\lambda$ (still working with the notations of [PatReu98]). This is already enough to prove that, if the restriction of E^ι_λ to A^λ is the identity for every partition λ, then $\sum_{|\mu|=n} \operatorname{Im}\left(E^\iota_\mu\right) = A_n$.

[102] Note that the proof of Corollary 4.4 in [PatReu98] may still require these two theorems - I don't know (I don't understand how Corollary 4.4 in [PatReu98] is proven).

[103] Recall that V^i is to be understood according to Convention 15.2. Hence, V^i means the i-th power of the subspace V of the k-algebra A.

and

$$\begin{aligned}\operatorname{symp}_\ell V &\subseteq \operatorname{symp}_\ell V + \sum_{i=0}^{\ell-1} \operatorname{symp}_i V = \sum_{i=0}^{\ell} \operatorname{symp}_i V \\ &= \sum_{i=0}^{\ell} V^i \qquad \text{(by Proposition 17.16 } \mathbf{(b)}\text{)} \\ &\subseteq \sum_{i\in\mathbb{N}} V^i. \end{aligned} \tag{162}$$

Now,

$$\sum_{i\in\mathbb{N}} V^i = \sum_{\ell\in\mathbb{N}} \underbrace{V^\ell}_{\subseteq \sum_{i\in\mathbb{N}} \operatorname{symp}_i V \text{ (by (161))}} \qquad \text{(here, we renamed the index } i \text{ as } \ell \text{ in the sum)}$$

$$\subseteq \sum_{\ell\in\mathbb{N}} \sum_{i\in\mathbb{N}} \operatorname{symp}_i V \subseteq \sum_{i\in\mathbb{N}} \operatorname{symp}_i V \qquad \left(\text{since } \sum_{i\in\mathbb{N}} \operatorname{symp}_i V \text{ is a } k\text{-vector space}\right),$$

combined with

$$\sum_{i\in\mathbb{N}} \operatorname{symp}_i V = \sum_{\ell\in\mathbb{N}} \underbrace{\operatorname{symp}_\ell V}_{\subseteq \sum_{i\in\mathbb{N}} V^i \text{ (by (162))}} \qquad \text{(here, we renamed the index } i \text{ as } \ell \text{ in the sum)}$$

$$\subseteq \sum_{\ell\in\mathbb{N}} \sum_{i\in\mathbb{N}} V^i \subseteq \sum_{i\in\mathbb{N}} V^i \qquad \left(\text{since } \sum_{i\in\mathbb{N}} V^i \text{ is a } k\text{-vector space}\right),$$

yields $\sum_{i\in\mathbb{N}} V^i = \sum_{i\in\mathbb{N}} \operatorname{symp}_i V$. This proves Proposition 19.6. □

The next step is less obvious, but still not a large step:

Proposition 19.7. Let k be a field of characteristic 0. Let A be a graded k-algebra. Let V be a homogeneous subspace of A such that $V \cap A_0 = 0$. Then,

$$\operatorname{symp}_n V = \sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V \qquad \text{for every } n \in \mathbb{N}.$$

Note that we are not summing over all partitions μ, but over all n-tuples of positive integers.

To prove this, we need the following purely linear-algebraic fact (which is an analogue of the product rule for tensor products, and is proven in the same way as the product rule):

Remark 19.8. Let k be a field. Let $(W_i)_{i\in I}$ be a family of k-vector spaces (where I is some index set). Let $m \in \mathbb{N}$. For every m-tuple $\mu \in I^{\times m}$, let us write the m-tuple μ in the form $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$. [104]. Then,

$$\left(\bigoplus_{i\in I} W_i\right)^{\otimes m} = \bigoplus_{\mu\in I^{\times m}} \left(W_{\mu_1} \otimes W_{\mu_2} \otimes \cdots \otimes W_{\mu_m}\right)$$

[104]This means that, for every $s \in \{1, 2, \ldots, m\}$, we denote by μ_s the s-th element of the m-tuple μ.

(where W_j is considered a subspace of $\bigoplus_{i \in I} W_i$ for every $j \in I$, and thus $W_{\mu_1} \otimes W_{\mu_2} \otimes \cdots \otimes W_{\mu_m}$ is considered a subspace of $\left(\bigoplus_{i \in I} W_i \right)^{\otimes m}$ for every $\mu \in I^{\times m}$).

Remark 19.8 is a particular case of the following, even more general fact:

Remark 19.9. Let k be a field. Let $m \in \mathbb{N}$. Let I_1, I_2, ..., I_m be m sets. For every $j \in \{1, 2, \ldots, m\}$, let $(W_{j,i})_{i \in I_j}$ be a family of k-vector spaces. For every m-tuple $\mu \in I_1 \times I_2 \times \cdots \times I_m$, let us write the m-tuple μ in the form $\mu = (\mu_1, \mu_2, \ldots, \mu_m)$. [105]. Then,

$$\left(\bigoplus_{i \in I_1} W_{1,i} \right) \otimes \left(\bigoplus_{i \in I_2} W_{2,i} \right) \otimes \cdots \otimes \left(\bigoplus_{i \in I_m} W_{m,i} \right) = \bigoplus_{\mu \in I_1 \times I_2 \times \cdots \times I_m} \left(W_{1,\mu_1} \otimes W_{2,\mu_2} \otimes \cdots \otimes W_{m,\mu_m} \right)$$

(where $W_{j,\ell}$ is considered a subspace of $\bigoplus_{i \in I_j} W_{j,i}$ for every $j \in \{1, 2, \ldots, m\}$ and $\ell \in I_j$, and thus $W_{1,\mu_1} \otimes W_{2,\mu_2} \otimes \cdots \otimes W_{m,\mu_m}$ is considered a subspace of $\left(\bigoplus_{i \in I_1} W_{1,i} \right) \otimes \left(\bigoplus_{i \in I_2} W_{2,i} \right) \otimes \cdots \otimes \left(\bigoplus_{i \in I_m} W_{m,i} \right)$ for every $\mu \in I_1 \times I_2 \times \cdots \times I_m$).

Remark 19.9 can be proven by induction on m (just as the product rule). Remark 19.8 follows from Remark 19.9 (applied to $I_1 = I$, $I_2 = I$, ..., $I_m = I$ and $W_{j,i} = W_i$).

Proof of Proposition 19.7. For every n-tuple $\mu \in I^{\times n}$, let us write the n-tuple μ in the form $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$. [106]

Let V_i denote $V \cap A_i$ for every $i \in \mathbb{N}$. Since V is a homogeneous subspace of A, we have

$$\begin{aligned} V &= \bigoplus_{n \in \mathbb{N}} (V \cap A_n) \qquad \text{(by the definition of "homogeneous subspace")} \\ &= \underbrace{V \cap A_0}_{=0} \oplus \underbrace{\bigoplus_{\substack{n \in \mathbb{N}; \\ n \geq 1}}}_{= \bigoplus_{n \in \{1,2,3,\ldots\}}} \underbrace{(V \cap A_n)}_{\substack{=V_n \\ \text{(since } V_n \text{ was defined as } V \cap A_n\text{)}}} = \bigoplus_{n \in \{1,2,3,\ldots\}} V_n \\ &= \bigoplus_{i \in \{1,2,3,\ldots\}} V_i \qquad \text{(here, we renamed the index } n \text{ as } i\text{)}. \end{aligned}$$

[105] This means that, for every $s \in \{1, 2, \ldots, m\}$, we denote by μ_s the s-th element of the m-tuple μ.

[106] This means that, for every $s \in \{1, 2, \ldots, n\}$, we denote by μ_s the s-th element of the n-tuple μ.

Now, let $n \in \mathbb{N}$ be arbitrary. Then, $V = \bigoplus_{i \in \{1,2,3,\ldots\}} V_i$ leads to

$$\begin{aligned} V^{\otimes n} &= \left(\bigoplus_{i \in \{1,2,3,\ldots\}} V_i \right)^{\otimes n} = \bigoplus_{\mu \in \{1,2,3,\ldots\}^{\times n}} \left(V_{\mu_1} \otimes V_{\mu_2} \otimes \cdots \otimes V_{\mu_n} \right) \\ &\qquad \text{(by Remark 19.8, applied to } I = \{1,2,3,\ldots\},\ m = n \text{ and } W_i = V_i) \\ &= \sum_{\mu \in \{1,2,3,\ldots\}^{\times n}} \left(V_{\mu_1} \otimes V_{\mu_2} \otimes \cdots \otimes V_{\mu_n} \right) \qquad \text{(since direct sums are sums)}. \end{aligned} \tag{163}$$

Let $\operatorname{tensor}_n : V^{\times n} \to V^{\otimes n}$ be the map defined by

$$\left(\operatorname{tensor}_n (v_1, v_2, \ldots, v_n) = v_1 \otimes v_2 \otimes \cdots \otimes v_n \qquad \text{for every } (v_1, v_2, \ldots, v_n) \in V^{\times n} \right).$$

Then, by the universal property of the n-th tensor power, every n-multilinear map from $V^{\times n}$ factors through tensor_n.

Now let us define a map $\varphi_n : V^{\times n} \to A$ by

$$\left(\varphi_n (v_1, v_2, \ldots, v_n) = \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \qquad \text{for every } (v_1, v_2, \ldots, v_n) \in V^{\times n} \right).$$

Then, this map φ_n is clearly n-multilinear. Thus, φ_n factors through tensor_n (since every n-multilinear map from $V^{\times n}$ factors through tensor_n). This means that there exists a k-linear map $\psi_n : V^{\otimes n} \to A$ such that $\varphi_n = \psi_n \circ \operatorname{tensor}_n$. Consider this ψ_n. Every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies

$$\begin{aligned} \psi_n \underbrace{(v_1 \otimes v_2 \otimes \cdots \otimes v_n)}_{= \operatorname{tensor}_n (v_1, v_2, \ldots, v_n)} &= \psi_n (\operatorname{tensor}_n (v_1, v_2, \ldots, v_n)) = \underbrace{(\psi_n \circ \operatorname{tensor}_n)}_{= \varphi_n} (v_1, v_2, \ldots, v_n) \\ &= \varphi_n (v_1, v_2, \ldots, v_n) \\ &= \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}. \end{aligned} \tag{164}$$

Now, we recall the basic linear-algebraic fact that

$$\left(\begin{array}{c} \text{for any two } k\text{-vector spaces } M \text{ and } R, \text{ any } k\text{-linear map } \phi : M \to R \\ \text{and every subset } S \text{ of } M \text{ satisfy } \phi (\langle S \rangle) = \langle \phi (S) \rangle \end{array} \right). \tag{165}$$

Since the tensor power $V^{\otimes n}$ is generated by pure tensors, we have

$$\begin{aligned} V^{\otimes n} &= \left\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\ &= \left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle, \end{aligned}$$

so that

$$\begin{aligned}
\psi_n\left(V^{\otimes n}\right) &= \psi_n\left(\left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle\right) \\
&= \left\langle \underbrace{\psi_n\left(\left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}\right)}_{= \left\{ \psi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n) \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}} \right\rangle \\
&\qquad \left(\begin{array}{c} \text{by (165), applied to } M = V^{\otimes n},\ R = A,\ \phi = \psi_n \text{ and} \\ S = \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \end{array} \right) \\
&= \left\langle \left\{ \psi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle \\
&= \left\langle \underbrace{\psi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right)}_{= \frac{1}{n!} \sum\limits_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \text{ (by (164))}} \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\
&= \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle = \operatorname{symp}_n V. \qquad (166)
\end{aligned}$$

On the other hand, for every $\mu \in \{1, 2, 3, \ldots\}^{\times n}$, the tensor product $V_{\mu_1} \otimes V_{\mu_2} \otimes \cdots \otimes V_{\mu_n}$ is generated by pure tensors, so that

$$\begin{aligned}
V_{\mu_1} \otimes V_{\mu_2} \otimes \cdots \otimes V_{\mu_n} &= \left\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\rangle \\
&= \left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\} \right\rangle,
\end{aligned}$$

so that

$$\begin{aligned}
&\psi_n\left(V_{\mu_1} \otimes V_{\mu_2} \otimes \cdots \otimes V_{\mu_n}\right) \\
&= \psi_n\left(\left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\} \right\rangle\right) \\
&= \left\langle \underbrace{\psi_n\left(\left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\}\right)}_{= \left\{ \psi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n) \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\}} \right\rangle \\
&\qquad \left(\begin{array}{c} \text{by (165), applied to } M = V_{\mu_1} \otimes V_{\mu_2} \otimes \cdots \otimes V_{\mu_n},\ R = A,\ \phi = \psi_n \text{ and} \\ S = \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\} \end{array} \right) \\
&= \left\langle \left\{ \psi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\} \right\rangle \\
&= \left\langle \underbrace{\psi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right)}_{= \frac{1}{n!} \sum\limits_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \text{ (by (164))}} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\rangle \\
&= \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\rangle = \operatorname{symp}^{\mu} V. \qquad (167)
\end{aligned}$$

Now, (166) yields

$$\begin{aligned}
\operatorname{symp}_n V &= \psi_n\left(V^{\otimes n}\right) = \psi_n\left(\sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \left(V_{\mu_1}\otimes V_{\mu_2}\otimes\cdots\otimes V_{\mu_n}\right)\right) && \text{(by (163))}\\
&= \sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \underbrace{\psi_n\left(V_{\mu_1}\otimes V_{\mu_2}\otimes\cdots\otimes V_{\mu_n}\right)}_{\substack{=\operatorname{symp}^{\mu} V\\ \text{(by (167))}}} && \text{(since } \psi_n \text{ is } k\text{-linear)}\\
&= \sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^{\mu} V.
\end{aligned}$$

This proves Proposition 19.7. □

The next easy step is to prove the following fact:

Proposition 19.10. Let k be a field of characteristic 0. Let A be a graded k-algebra. Let $n\in\mathbb{N}$. Let $\mu\in\{1,2,3,\ldots\}^{\times n}$ be arbitrary. Then,

$$\operatorname{symp}^{\mu} V \subseteq \sum_{\lambda \text{ is a partition}} \operatorname{symp}^{\lambda} V.$$

Proof of Proposition 19.10. Let us write the n-tuple μ in the form $\mu=(\mu_1,\mu_2,\ldots,\mu_n)$.[107]

Every finite sequence of integers can be sorted into nonincreasing order by a permutation. Applying this to the sequence $(\mu_1,\mu_2,\ldots,\mu_n)$, we see that there exists a permutation $\tau\in S_n$ such that $\mu_{\tau(1)}\geq\mu_{\tau(2)}\geq\cdots\geq\mu_{\tau(n)}$. Consider such a τ.

The numbers $\mu_{\tau(1)}$, $\mu_{\tau(2)}$, …, $\mu_{\tau(n)}$ are positive integers (since $\mu\in\{1,2,3,\ldots\}^{\times n}$) and satisfy $\mu_{\tau(1)}\geq\mu_{\tau(2)}\geq\cdots\geq\mu_{\tau(n)}$. Hence, $\left(\mu_{\tau(1)},\mu_{\tau(2)},\ldots,\mu_{\tau(n)}\right)$ is a nonincreasing finite sequence of positive integers. In other words, $\left(\mu_{\tau(1)},\mu_{\tau(2)},\ldots,\mu_{\tau(n)}\right)$ is a partition (by Definition 19.2). Denote this partition by ρ. Thus, $\rho=\left(\mu_{\tau(1)},\mu_{\tau(2)},\ldots,\mu_{\tau(n)}\right)$.

Let us write the n-tuple ρ in the form $\rho=(\rho_1,\rho_2,\ldots,\rho_n)$. Since we already know that $\rho=\left(\mu_{\tau(1)},\mu_{\tau(2)},\ldots,\mu_{\tau(n)}\right)$, we obtain $(\rho_1,\rho_2,\ldots,\rho_n)=\rho=\left(\mu_{\tau(1)},\mu_{\tau(2)},\ldots,\mu_{\tau(n)}\right)$. Hence,

$$\rho_j=\mu_{\tau(j)} \qquad \text{for every } j\in\{1,2,\ldots,n\}. \tag{168}$$

Now, by the definition of $\operatorname{symp}^{\rho} V$, we have

$$\operatorname{symp}^{\rho} V = \left\langle \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \;\mid\; (v_1,v_2,\ldots,v_n)\in V_{\rho_1}\times V_{\rho_2}\times\cdots\times V_{\rho_n}\right\rangle,$$

[107] This means that, for every $s\in\{1,2,\ldots,n\}$, we denote by μ_s the s-th element of the n-tuple μ.

so that

$$\begin{aligned}
&\left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\rho_1} \times V_{\rho_2} \times \cdots \times V_{\rho_n} \right\} \\
&\subseteq \left\langle \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\rho_1} \times V_{\rho_2} \times \cdots \times V_{\rho_n} \right\} \right\rangle \\
&= \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\rho_1} \times V_{\rho_2} \times \cdots \times V_{\rho_n} \right\rangle \\
&= \operatorname{symp}^{\rho} V.
\end{aligned}$$

In other words,

$$\frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \in \operatorname{symp}^{\rho} V \qquad \text{for every } (v_1, v_2, \ldots, v_n) \in V_{\rho_1} \times V_{\rho_2} \times \cdots \times V_{\rho_n}. \tag{169}$$

Now, let us prove that

$$\frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \in \operatorname{symp}^{\rho} V \qquad \text{for every } (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n}. \tag{170}$$

Proof of (170). Since S_n is a group, the map

$$S_n \to S_n, \qquad \sigma \mapsto \tau \circ \sigma$$

is a bijection.

Let $(v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n}$ be arbitrary. Then, for every $i \in \{1, 2, \ldots, n\}$, we have $v_i \in V_{\mu_i}$. Hence, for every $j \in \{1, 2, \ldots, n\}$, we have

$$\begin{aligned}
v_{\tau(j)} &\in V_{\mu_{\tau(j)}} \qquad \left(\text{by the formula } v_i \in V_{\mu_i}, \text{ applied to } i = \tau(j)\right) \\
&= V_{\rho_j} \qquad \left(\text{since } \mu_{\tau(j)} = \rho_j \text{ (by (168))}\right).
\end{aligned}$$

In other words, $\left(v_{\tau(1)}, v_{\tau(2)}, \ldots, v_{\tau(n)}\right) \in V_{\rho_1} \times V_{\rho_2} \times \cdots \times V_{\rho_n}$. Thus, (169) (applied to $\left(v_{\tau(1)}, v_{\tau(2)}, \ldots, v_{\tau(n)}\right)$ instead of $(v_1, v_2, \ldots, v_n)$) yields

$$\frac{1}{n!} \sum_{\sigma \in S_n} v_{\tau(\sigma(1))} v_{\tau(\sigma(2))} \cdots v_{\tau(\sigma(n))} \in \operatorname{symp}^{\rho} V.$$

But since

$$\begin{aligned}
&\sum_{\sigma \in S_n} \underbrace{v_{\tau(\sigma(1))} v_{\tau(\sigma(2))} \cdots v_{\tau(\sigma(n))}}_{= v_{(\tau \circ \sigma)(1)} v_{(\tau \circ \sigma)(2)} \cdots v_{(\tau \circ \sigma)(n)}} \\
&\qquad \left(\text{since } \tau(\sigma(1)) = (\tau \circ \sigma)(1),\ \tau(\sigma(2)) = (\tau \circ \sigma)(2),\ \ldots,\ \tau(\sigma(n)) = (\tau \circ \sigma)(n)\right) \\
&= \sum_{\sigma \in S_n} v_{(\tau \circ \sigma)(1)} v_{(\tau \circ \sigma)(2)} \cdots v_{(\tau \circ \sigma)(n)} \\
&= \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \qquad \left(\begin{array}{c} \text{here, we substituted } \sigma \text{ for } \tau \circ \sigma \text{ in the sum, since the map} \\ S_n \to S_n, \qquad \sigma \mapsto \tau \circ \sigma \\ \text{is a bijection} \end{array} \right),
\end{aligned}$$

this rewrites as $\frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \in \operatorname{symp}^\rho V$. This proves (170).

Now that (170) is proven, we can rewrite (170) as follows:

$$\left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\} \subseteq \operatorname{symp}^\rho V.$$

Thus, (154) (applied to $M = A$, $S = \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\}$ and $Q = \operatorname{symp}^\rho V$) yields

$$\left\langle \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\} \right\rangle \subseteq \operatorname{symp}^\rho V.$$

Thus,

$$\begin{aligned} &\operatorname{symp}^\mu V \\ &= \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\rangle \\ &= \left\langle \left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \ \mid \ (v_1, v_2, \ldots, v_n) \in V_{\mu_1} \times V_{\mu_2} \times \cdots \times V_{\mu_n} \right\} \right\rangle \\ &\subseteq \operatorname{symp}^\rho V \subseteq \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V \end{aligned}$$

(since ρ is a partition, and thus $\operatorname{symp}^\rho V$ is an addend of the sum $\sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V$). This proves Proposition 19.10. $\square$

Now, finally, we prove Proposition 19.5 and Theorem 19.3:

Proof of Proposition 19.5. Proposition 19.6 yields

$$\begin{aligned} \sum_{i \in \mathbb{N}} V^i &= \sum_{i \in \mathbb{N}} \underbrace{\operatorname{symp}_i V}_{= \sum_{\mu \in \{1,2,3,\ldots\}^{\times i}} \operatorname{symp}^\mu V \text{ (by Proposition 19.7, applied to } n=i)} = \sum_{i \in \mathbb{N}} \sum_{\mu \in \{1,2,3,\ldots\}^{\times i}} \underbrace{\operatorname{symp}^\mu V}_{\subseteq \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V \text{ (by Proposition 19.10, applied to } n=i)} \\ &\subseteq \sum_{i \in \mathbb{N}} \sum_{\mu \in \{1,2,3,\ldots\}^{\times i}} \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V \subseteq \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V \qquad (171) \end{aligned}$$

$$\left(\text{since } \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V \text{ is a } k\text{-vector space} \right).$$

On the other hand, for every partition λ, we have $\operatorname{symp}^\lambda V \subseteq \sum\limits_{n\in\mathbb{N}} \sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V$. [108] Thus,

$$\sum_{\lambda \text{ is a partition}} \underbrace{\operatorname{symp}^\lambda V}_{\subseteq \sum\limits_{n\in\mathbb{N}} \sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V}$$

$$\subseteq \sum_{\lambda \text{ is a partition}} \sum_{n\in\mathbb{N}} \sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V$$

$$\subseteq \sum_{n\in\mathbb{N}} \underbrace{\sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V}_{=\operatorname{symp}_n V \text{ (by Proposition 19.7)}} \qquad \left(\text{since } \sum_{n\in\mathbb{N}} \sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V \text{ is a } k\text{-vector space}\right)$$

$$= \sum_{n\in\mathbb{N}} \operatorname{symp}_n V = \sum_{i\in\mathbb{N}} \operatorname{symp}_i V \qquad \text{(here, we renamed the index } n \text{ as } i \text{ in the sum)}$$

$$= \sum_{i\in\mathbb{N}} V^i \qquad \text{(by Proposition 19.6)}.$$

Combined with (171), this yields $\sum\limits_{i\in\mathbb{N}} V^i = \sum\limits_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda V$. This proves Proposition 19.5. □

Proof of Theorem 19.3. First, $\operatorname{Prim} H$ is a homogeneous subspace of H (by Proposition 18.3).

Second, it is easy to see $(\operatorname{Prim} H) \cap H_0 = 0$ [109].

---

[108] *Proof.* Let λ be a partition. Then, λ is a tuple of positive integers. In other words, there exists an $m \in \mathbb{N}$ such that λ is an m-tuple of positive integers. Consider this m. Then, λ is an m-tuple of positive integers, so that $\lambda \in \{1,2,3,\ldots\}^{\times m}$. Hence, $\operatorname{symp}^\lambda V$ is an addend of the sum $\sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times m}} \operatorname{symp}^\mu V$. Thus, $\operatorname{symp}^\lambda V \subseteq \sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times m}} \operatorname{symp}^\mu V$. But $\sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times m}} \operatorname{symp}^\mu V$ is an addend of the sum $\sum\limits_{n\in\mathbb{N}} \sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V$. Thus, $\sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times m}} \operatorname{symp}^\mu V \subseteq \sum\limits_{n\in\mathbb{N}} \sum\limits_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V$. Hence,

$$\operatorname{symp}^\lambda V \subseteq \sum_{\mu\in\{1,2,3,\ldots\}^{\times m}} \operatorname{symp}^\mu V \subseteq \sum_{n\in\mathbb{N}} \sum_{\mu\in\{1,2,3,\ldots\}^{\times n}} \operatorname{symp}^\mu V,$$

qed.

[109] *Proof.* Let $x \in (\operatorname{Prim} H) \cap H_0$. Then, $x \in (\operatorname{Prim} H) \cap H_0 \subseteq H_0 = H_{\leq 0}$ (because the definition of $H_{\leq 0}$ yields $H_{\leq 0} = \bigoplus\limits_{\ell=0}^{0} H_\ell = H_0$). Since $H_{\leq 0} = k \cdot 1_H$ (by Remark 2.11, applied to $C = H$), this rewrites as $x \in k \cdot 1_H$. Hence, there exists some $\lambda \in k$ such that $x = \lambda \cdot 1_H$. Consider such a λ.

On the other hand, $x \in (\operatorname{Prim} H) \cap H_0 \subseteq \operatorname{Prim} H$. Since H is a unital coalgebra (by Proposition 2.3, applied to $C = H$), this yields $\varepsilon(x) = 0$ (by Remark 6.3). Since $x = \lambda \cdot 1_H$, this becomes $\varepsilon(\lambda \cdot 1_H) = 0$. But since

$$\varepsilon(\lambda \cdot 1_H) = \lambda \cdot \underbrace{\varepsilon(1_H)}_{\substack{=1 \\ \text{(by the axioms of a bialgebra,} \\ \text{since } H \text{ is a bialgebra)}}} \qquad \text{(since } \varepsilon \text{ is } k\text{-linear)}$$

$$= \lambda,$$

this means that $\lambda = 0$, so that $x = \underbrace{\lambda}_{=0} \cdot 1_H = 0$.

Third, we know from Proposition 17.14 that $xy - yx \in \operatorname{Prim} H$ for any $x \in \operatorname{Prim} H$ and $y \in \operatorname{Prim} H$.

Thus, we can apply Proposition 19.5 to $A = H$ and $V = \operatorname{Prim} H$. We conclude that

$$\sum_{i \in \mathbb{N}} (\operatorname{Prim} H)^i = \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda (\operatorname{Prim} H) .$$

But since H is filtered, we know that

$$\begin{aligned} H &= \bigcup_{\ell \in \mathbb{N}} \underbrace{H_{\leq \ell}}_{\substack{\subseteq \sum_{i=0}^{\ell} (\operatorname{Prim} H)^i \\ \text{(by Proposition 17.3)}}} \subseteq \bigcup_{\ell \in \mathbb{N}} \left(\underbrace{\sum_{i=0}^{\ell} (\operatorname{Prim} H)^i}_{\subseteq \sum_{i \in \mathbb{N}} (\operatorname{Prim} H)^i} \right) \subseteq \bigcup_{\ell \in \mathbb{N}} \left(\sum_{i \in \mathbb{N}} (\operatorname{Prim} H)^i \right) \\ &= \sum_{i \in \mathbb{N}} (\operatorname{Prim} H)^i = \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda (\operatorname{Prim} H) . \end{aligned}$$

Combined with the obvious relation $\sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda (\operatorname{Prim} H) \subseteq H$, this yields $H = \sum_{\lambda \text{ is a partition}} \operatorname{symp}^\lambda (\operatorname{Prim} H)$. This proves Theorem 19.3. □

§20. Writing p_n as a sum of convolutions of ζ_m's

We continue to study connected graded bialgebras. First let us make explicit one result that we proved during the proof of Proposition 16.22:

Theorem 20.1. Let k be a field of characteristic 0, and let H be a connected graded k-bialgebra. Let ζ be the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$. For every $n \in \mathbb{N}$, let p_n denote the map $p_{n,H}$ (defined according to Definition 16.16), and let ζ_n denote the map $\zeta \circ p_n$. Then,

$$\zeta_n = \sum_{\ell=1}^{n} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1, a_2, \ldots, a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell})$$

for every $n \in \mathbb{N}$.

Proof of Theorem 20.1. Theorem 20.1 directly follows from (131). □

Theorem 20.1 gives us a formula for writing ζ_n in terms of convolutions of p_m's. We can also get a formula for writing p_n in terms of convolutions of ζ_m's:

Theorem 20.2. Let k be a field of characteristic 0, and let H be a connected graded k-bialgebra. Let ζ be the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$. For every

Now forget that we fixed x. We thus have shown that every $x \in (\operatorname{Prim} H) \cap H_0$ satisfies $x = 0$. In other words, $(\operatorname{Prim} H) \cap H_0 = 0$, qed.

$n \in \mathbb{N}$, let p_n denote the map $p_{n,H}$ (defined according to Definition 16.16), and let ζ_n denote the map $\zeta \circ p_n$. Then,

$$p_n = \sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})$$

for every $n \in \mathbb{N}$.

We are going to prove Theorem 20.2 now. As we could expect, the proof will be similar to the proof of Theorem 20.1 which we did in §16. We begin with a few lemmata:

Lemma 20.3. Let k be a field of characteristic 0, and let H be a connected graded k-bialgebra. Let ζ be the map $\operatorname{Log} \mathrm{id} \in \mathcal{L}(H, H)$. For every $n \in \mathbb{N}$, let p_n denote the map $p_{n,H}$ (defined according to Definition 16.16), and let ζ_n denote the map $\zeta \circ p_n$. Then, $\zeta_0 = 0$.

Proof of Lemma 20.3. Theorem 20.1 (applied to $n = 0$) yields

$$\zeta_0 = \sum_{\ell=1}^{0} \frac{(-1)^{\ell-1}}{\ell} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,0\}^{\times \ell}; \\ 0 = a_1 + a_2 + \cdots + a_\ell}} (p_{a_1} * p_{a_2} * \cdots * p_{a_\ell}) = (\text{empty sum}) = 0.$$

This proves Lemma 20.3. □

(Of course, we could have proven Lemma 20.3 much more easily.)

The following proposition is reminiscent of Proposition 16.25 **(d)**:

Proposition 20.4. Let k be a field of characteristic 0, and let H be a connected graded k-bialgebra. Then, for every $n \in \mathbb{N}$, the map ζ_n (defined in Theorem 20.2) is graded and concentrated in degree n.

Proof of Proposition 20.4. Let $n \in \mathbb{N}$. Then, $\zeta_n = \zeta \circ p_n$ is the composition of two graded maps (since ζ is graded (by Theorem 16.21) and since p_n is graded (by Proposition 16.25 **(d)**)). Since the composition of two graded maps must always be graded, this yields that ζ_n is graded.

We have $\zeta_n = \zeta \circ p_n = p_n \circ \zeta \circ p_n$ (by (117)), thus $\zeta_n = p_n \circ \underbrace{\zeta \circ p_n}_{=\zeta_n} = p_n \circ \zeta_n$. Since ζ_n is graded, this yields that ζ_n is concentrated in degree n. This proves Proposition 20.4. □

Next, here is an analogue of Corollary 16.26:

Corollary 20.5. Let k be a field. Let H be a graded k-bialgebra. Let ζ be the map $\operatorname{Log} \mathrm{id} \in \mathcal{L}(H, H)$. For every $n \in \mathbb{N}$, let p_n denote the map $p_{n,H}$ (defined according to Definition 16.16), and let ζ_n denote the map $\zeta \circ p_n$.

Let $n \in \mathbb{N}$ and $\ell \in \mathbb{N}$. Let a_i be a nonnegative integer for every $i \in \{1, 2, \ldots, \ell\}$.

(a) We have $p_n \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}) = 0$ if $n \neq a_1 + a_2 + \cdots + a_\ell$.

(b) We have $p_n \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}) = \zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}$ if $n = a_1 + a_2 + \cdots + a_\ell$.

Proof of Corollary 20.5. For every $i \in \{1, 2, \ldots, \ell\}$, the map ζ_{a_i} is graded and concentrated in degree a_i (by Proposition 20.4, applied to a_i instead of n). Thus, Proposition 16.25 **(c)** (applied to $f_i = \zeta_{a_i}$) yields that $\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_\ell$. According to Definition 16.24, this means that

$$p_{a_1+a_2+\cdots+a_\ell} \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}) = \zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}. \tag{172}$$

(a) Assume that $n \neq a_1 + a_2 + \cdots + a_\ell$. Then, $p_{n,H} \mid_{H_{a_1+a_2+\cdots+a_\ell}} = 0$ (by (111), applied to $m = a_1 + a_2 + \cdots + a_\ell$ and $V = H$).

But

$$\underbrace{(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})}_{\substack{= p_{a_1+a_2+\cdots+a_\ell} \circ \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right) \\ \text{(by (172))}}} (H)$$

$$= \left(p_{a_1+a_2+\cdots+a_\ell} \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})\right)(H) = \underbrace{p_{a_1+a_2+\cdots+a_\ell}}_{\substack{= p_{a_1+a_2+\cdots+a_\ell, H} \\ \text{(by the definition of } p_{a_1+a_2+\cdots+a_\ell})}} \left(\underbrace{(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})(H)}_{\subseteq H}\right)$$

$$\subseteq p_{a_1+a_2+\cdots+a_\ell, H}(H) = H_{a_1+a_2+\cdots+a_\ell} \qquad \left(\begin{array}{c} \text{by (112), applied to } H \text{ and } a_1 + a_2 + \cdots + a_\ell \\ \text{instead of } V \text{ and } n \end{array}\right)$$

and thus

$$p_n\left((\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})(H)\right) \subseteq \underbrace{p_n}_{\substack{= p_{n,H} \\ \text{(by the definition of } p_n)}} (H_{a_1+a_2+\cdots+a_\ell}) = p_{n,H}(H_{a_1+a_2+\cdots+a_\ell})$$

$$= \underbrace{\left(p_{n,H} \mid_{H_{a_1+a_2+\cdots+a_\ell}}\right)}_{=0} (H_{a_1+a_2+\cdots+a_\ell}) = 0\,(H_{a_1+a_2+\cdots+a_\ell}) = 0.$$

Since $p_n\left((\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})(H)\right) = \left(p_n \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})\right)(H)$, this rewrites as $\left(p_n \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell})\right)(H) = 0$. Thus, $p_n \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}) = 0$. This proves Corollary 20.5 **(a)**.

(b) Now assume that $n = a_1 + a_2 + \cdots + a_\ell$. Then,

$$p_n \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}) = p_{a_1+a_2+\cdots+a_\ell} \circ (\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}) = \zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}$$

(by (172)). This proves Corollary 20.5 **(b)**. □

The next proof of Theorem 20.2 proceeds in analogy to (and occasional use of) the proof of Proposition 16.22 above.

Proof of Theorem 20.2. Let $n \in \mathbb{N}$.

Notice that $\zeta = \operatorname{Log} \mathrm{id} \in \mathfrak{g}(H, H)$ (by the definition of Log).

We will now prove Theorem 20.2 in several steps:

a) Every $x \in H_{\leq n}$ satisfies

$$\zeta(x) = (\zeta_1 + \zeta_2 + \cdots + \zeta_n)(x). \tag{173}$$

Proof of (173). Let $x \in H_{\leq n}$. We know that $x = p_0(x) + p_1(x) + \cdots + p_n(x)$ (this is the equality (123) which we proved during the proof of (121), while we were proving Proposition 16.22). Thus,

$$\zeta(x) = \zeta\underbrace{(p_0(x) + p_1(x) + \cdots + p_n(x))}_{=\sum_{i=0}^{n} p_i(x)} = \zeta\left(\sum_{i=0}^{n} p_i(x)\right) = \sum_{i=0}^{n} \underbrace{\zeta(p_i(x))}_{=(\zeta \circ p_i)(x)}$$

(since ζ is k-linear)

$$= \sum_{i=0}^{n} \underbrace{(\zeta \circ p_i)}_{\substack{=\zeta_i \\ \text{(since } \zeta_i \text{ was defined as } \zeta \circ p_i\text{)}}}(x) = \sum_{i=0}^{n} \zeta_i(x) = \underbrace{\zeta_0}_{\substack{=0 \\ \text{(by Lemma 20.3)}}}(x) + \sum_{i=1}^{n} \zeta_i(x)$$

$$= \underbrace{0(x)}_{=0} + \underbrace{\sum_{i=1}^{n} \zeta_i(x)}_{=\zeta_1(x)+\zeta_2(x)+\cdots+\zeta_n(x)} = \zeta_1(x) + \zeta_2(x) + \cdots + \zeta_n(x) = (\zeta_1 + \zeta_2 + \cdots + \zeta_n)(x).$$

This proves (173). Step **a)** is thus done.

b) Every $x \in H_{\leq n}$ and every $\ell \in \mathbb{N}$ satisfy

$$\zeta^{*\ell}(x) = (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell}(x). \tag{174}$$

Proof of (174). There are several ways to derive (174) from (173) (just as there were several ways to derive (125) from (121)). Here is one of them:

Let $\ell \in \mathbb{N}$.

We are going to use the notation $\mathcal{L}^n(H, A)$ introduced in Definition 3.1 **(b)**.

By the definition of $\mathcal{L}^{n+1}(H, H)$, we have

$$\mathcal{L}^{n+1}(H,H) = \left\{ f \in \mathcal{L}(H,H) \mid \underbrace{f|_{H_{\leq n+1-1}}}_{=f|_{H_{\leq n}}} = 0 \right\} = \left\{ f \in \mathcal{L}(H,H) \mid f|_{H_{\leq n}} = 0 \right\}.$$

By Proposition 14.2 (applied to $n+1$ and H instead of n and A), the set $\mathcal{L}^{n+1}(H, H)$ is an ideal of the k-algebra $\mathcal{L}(H, H)$.

Every $x \in H_{\leq n}$ satisfies

$$(\zeta - (\zeta_1 + \zeta_2 + \cdots + \zeta_n))(x) = \underbrace{\zeta(x)}_{\substack{=(\zeta_1+\zeta_2+\cdots+\zeta_n)(x) \\ \text{(by (173))}}} - (\zeta_1 + \zeta_2 + \cdots + \zeta_n)(x)$$

$$= (\zeta_1 + \zeta_2 + \cdots + \zeta_n)(x) - (\zeta_1 + \zeta_2 + \cdots + \zeta_n)(x) = 0.$$

In other words, $(\zeta - (\zeta_1 + \zeta_2 + \cdots + \zeta_n))|_{H_{\leq n}} = 0$. Thus,

$$\zeta - (\zeta_1 + \zeta_2 + \cdots + \zeta_n) \in \left\{ f \in \mathcal{L}(H,H) \mid f|_{H_{\leq n}} = 0 \right\} = \mathcal{L}^{n+1}(H,H).$$

In other words, $\zeta \equiv \zeta_1 + \zeta_2 + \cdots + \zeta_n \bmod \mathcal{L}^{n+1}(H, H)$. Thus,

$$\zeta^{*\ell} \equiv (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell} \bmod \mathcal{L}^{n+1}(H,H)$$

(because $\mathcal{L}^{n+1}(H,H)$ is an ideal of the k-algebra $\mathcal{L}(H,H)$, and hence we can multiply congruences modulo $\mathcal{L}^{n+1}(H,H)$). In other words,

$$\zeta^{*\ell} - (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell} \in \mathcal{L}^{n+1}(H,H) = \left\{ f \in \mathcal{L}(H,H) \ \mid \ f\mid_{H_{\leq n}} = 0 \right\},$$

so that $\left(\zeta^{*\ell} - (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell}\right)\mid_{H_{\leq n}} = 0$. Hence, every $x \in H_{\leq n}$ satisfies $\left(\zeta^{*\ell} - (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell}\right)(x) = 0$. As a consequence, every $x \in H_{\leq n}$ satisfies $\zeta^{*\ell}(x) = (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell}(x)$ (because

$$\zeta^{*\ell}(x) - (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell}(x) = \left(\zeta^{*\ell} - (\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell}\right)(x) = 0$$

). In other words, (174) is proven for every $x \in H_{\leq n}$ and every $\ell \in \mathbb{N}$. This completes step **b)**.

c) Every $x \in H_{\leq n}$ satisfies

$$x = \sum_{\ell=0}^{n} \frac{1}{\ell!} \zeta^{*\ell}(x). \tag{175}$$

Proof of (175). Since $\zeta = \operatorname{Log} \mathrm{id}$, we have $e^{*\zeta} = e^{*(\operatorname{Log}\mathrm{id})} = \mathrm{id}$ (by Proposition 5.13 **(b)**, applied to $A = H$ and $F = \mathrm{id}$). Thus, every $x \in H_{\leq n}$ satisfies

$$\begin{aligned}
x &= \underbrace{\mathrm{id}}_{=e^{*\zeta}}(x) = e^{*\zeta}(x) = \sum_{i \geq 0} \underbrace{\frac{\zeta^{*i}(x)}{i!}}_{=\frac{1}{i!}\zeta^{*i}(x)} \qquad \text{(by (6), applied to } f = \zeta\text{)} \\
&= \sum_{i \geq 0} \frac{1}{i!} \zeta^{*i}(x) = \sum_{\substack{i \geq 0; \\ i \leq n}} \frac{1}{i!} \zeta^{*i}(x) + \sum_{\substack{i \geq 0; \\ i > n}} \frac{1}{i!} \underbrace{\zeta^{*i}(x)}_{\substack{=0 \text{ (since } x \in H_{\leq n} \text{ and thus} \\ \zeta^{*i}(x) \in \zeta^{*i}\left(H_{\leq n}\right) = 0 \text{ (by Remark 3.5} \\ \text{(applied to } f = \zeta\text{), since } i > n\text{)}, \\ \text{so that } \zeta^{*i}(x) = 0\text{)}}} \\
&= \underbrace{\sum_{\substack{i \geq 0; \\ i \leq n}}}_{=\sum_{i=0}^{n}} \frac{1}{i!} \zeta^{*i}(x) + \underbrace{\sum_{\substack{i \geq 0; \\ i > n}} \frac{1}{i!} 0}_{=0} = \sum_{i=0}^{n} \frac{1}{i!} \zeta^{*i}(x) = \sum_{\ell=0}^{n} \frac{1}{\ell!} \zeta^{*\ell}(x)
\end{aligned}$$

(here, we renamed the summation index i as ℓ).

This proves (175), and thus our step **c)** is complete.

d) Every $x \in H_{\leq n}$ satisfies

$$x = \sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{(a_1, a_2, \ldots, a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x). \tag{176}$$

Proof of (176). Let $x \in H_{\leq n}$. Then, for every $\ell \in \mathbb{N}$, we have

$$\zeta^{*\ell}(x) = \underbrace{(\zeta_1 + \zeta_2 + \cdots + \zeta_n)^{*\ell}}_{= \sum\limits_{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} \zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell} \text{ (by the product rule)}} (x) \qquad \text{(by (174))}$$

$$= \left(\sum_{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} \zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell} \right)(x) = \sum_{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x).$$

Now, (175) becomes

$$x = \sum_{\ell=0}^{n} \frac{1}{\ell!} \underbrace{\zeta^{*\ell}(x)}_{= \sum\limits_{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x)}$$

$$= \sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x).$$

This proves (176).

e) Every $x \in H_n$ satisfies[110]

$$x = \left(\sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right) \right)(x). \tag{177}$$

Proof of (177). Let $x \in H_n$.

Since $H_{\leq n} = \bigoplus\limits_{\ell=0}^{n} H_\ell$ by the definition of $H_{\leq n}$, we have $H_n \subseteq H_{\leq n}$ (since H_n is one addend of the direct sum $\bigoplus\limits_{\ell=0}^{n} H_\ell$, and thus $H_n \subseteq \bigoplus\limits_{\ell=0}^{n} H_\ell = H_{\leq n}$).

Now, $p_{n,H} \mid_{H_n} = \mathrm{id}_H \mid_{H_n}$ (by (110), applied to $V = H$). Since $p_n = p_{n,H}$ (by the definition of p_n), this rewrites as $p_n \mid_{H_n} = \mathrm{id}_H \mid_{H_n}$. Since $x \in H_n$, we have

$$p_n(x) = \underbrace{(p_n \mid_{H_n})}_{= \mathrm{id}_H \mid_{H_n}}(x) = (\mathrm{id}_H \mid_{H_n})(x) = \mathrm{id}_H(x) = x.$$

Thus,

$$x = p_n(x) = p_n \left(\sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x) \right)$$

(by (176), since $x \in H_n \subseteq H_{\leq n}$)

$$= \sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}} p_n\left(\left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x)\right) \qquad \text{(since } p_n \text{ is } k\text{-linear)}.$$

[110] Note that here we require $x \in H_n$ rather than $x \in H_{\leq n}$.

Since every $\ell \in \{0, 1, \ldots, n\}$ satisfies

$$\begin{aligned}
&\sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \underbrace{p_n\left(\left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x)\right)}_{=\left(p_n \circ \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)\right)(x)} \\
&= \sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} \left(p_n \circ \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)\right)(x) \\
&= \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \underbrace{\left(p_n \circ \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)\right)}_{\substack{=\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell} \\ \text{(by Corollary 20.5 \textbf{(b)}, since} \\ n=a_1+a_2+\cdots+a_\ell)}}(x) \\
&\quad + \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n\neq a_1+a_2+\cdots+a_\ell}} \underbrace{\left(p_n \circ \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)\right)}_{\substack{=0 \\ \text{(by Corollary 20.5 \textbf{(a)}, since} \\ n\neq a_1+a_2+\cdots+a_\ell)}}(x) \\
&= \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x) + \underbrace{\sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n\neq a_1+a_2+\cdots+a_\ell}} 0\,(x)}_{=0} \\
&= \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x),
\end{aligned}$$

this rewrites as

$$\begin{aligned}
x &= \sum_{\ell=0}^{n} \frac{1}{\ell!} \underbrace{\sum_{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}} p_n\left(\left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x)\right)}_{= \sum\limits_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x)} \\
&= \sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)(x) \\
&= \left(\sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right) \right)(x).
\end{aligned}$$

This proves (177).

f) We are going to use the result (130) once again (but for obvious reasons, we are not going to prove it once again).

g) Now let us finally prove Theorem 20.2:

For every $\ell \in \{1, 2, \ldots, n\}$ and every $(a_1, a_2, \ldots, a_\ell) \in \{1, 2, \ldots, n\}^{\times\ell}$, the map $\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}$ is graded[111]. Hence, the map $\sum\limits_{\ell=0}^{n} \frac{1}{\ell!} \sum\limits_{\substack{(a_1,a_2,\ldots,a_\ell)\in\{1,2,\ldots,n\}^{\times\ell}; \\ n=a_1+a_2+\cdots+a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)$

[111] *Proof.* Let $\ell \in \{1, 2, \ldots, n\}$ and $(a_1, a_2, \ldots, a_\ell) \in \{1, 2, \ldots, n\}^{\times\ell}$. Then, for every $i \in \{1, 2, \ldots, \ell\}$,

is graded (since a k-linear combination of graded maps is always graded). Also, id is graded. The two latter facts, along with the fact that

$$\mathrm{id}\left(x\right) = x = \left(\sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right) \right)(x)$$

for all $x \in H_n$ (by (177)), show that we can apply (130) to $f = \mathrm{id}$ and $g = \sum\limits_{\ell=0}^{n} \frac{1}{\ell!} \sum\limits_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)$. As a result, we conclude that

$$p_n \circ \mathrm{id} = p_n \circ \left(\sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right) \right).$$

Using this identity, we have

$$\begin{aligned}
p_n &= p_n \circ \mathrm{id} \\
&= p_n \circ \left(\sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right) \right) \\
&= \sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} \underbrace{\left(p_n \circ \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right)\right)}_{\substack{= \zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell} \\ \text{(by Corollary 20.5 \textbf{(b)}, since} \\ n = a_1 + a_2 + \cdots + a_\ell)}} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \sum_{\ell=0}^{n} \frac{1}{\ell!} \sum_{\substack{(a_1,a_2,\ldots,a_\ell) \in \{1,2,\ldots,n\}^{\times \ell}; \\ n = a_1 + a_2 + \cdots + a_\ell}} \left(\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}\right).
\end{aligned}$$

This proves Theorem 20.2. □

§21. Logarithms of commutative convolutions

In this section, we are going to study the logarithm (as defined in Definition 3.8) further. We will prove its following property:

Theorem 21.1. Let k be a field of characteristic 0. Let A be a k-algebra, and let C be a connected filtered k-coalgebra. Let $F \in G\left(C, A\right)$ and $H \in G\left(C, A\right)$ be maps satisfying $F * H = H * F$. Then, $F * H \in G\left(C, A\right)$ and $\mathrm{Log}\left(F * H\right) = \mathrm{Log}\, F + \mathrm{Log}\, H$.

the map ζ_{a_i} is graded and concentrated in degree a_i (by Proposition 20.4, applied to a_i instead of n). Hence, by Proposition 16.25 **(c)** (applied to $f_i = \zeta_{a_i}$), the map $\zeta_{a_1} * \zeta_{a_2} * \cdots * \zeta_{a_\ell}$ is graded and concentrated in degree $a_1 + a_2 + \cdots + a_\ell$, qed.

Note that this Theorem 21.1 is a kind of logarithmic "sibling" of Proposition 11.1. It will be harder to prove, though. The proof will require a fact about power series:

Theorem 21.2. Let k be a field of characteristic 0. Consider the ring of formal power series $k[[X,Y]]$ in two (commuting) indeterminates X and Y. For every power series $Q \in k[[X,Y]]$ whose coefficient before X^0Y^0 is 1, let $\log Q$ denote the power series in $k[[X,Y]]$ defined by $\log Q = \sum\limits_{i \geq 1} \dfrac{(-1)^{i-1}}{i} (Q-1)^i$.

Let Q and R be two power series in $k[[X,Y]]$ whose coefficients before X^0Y^0 are both equal to 1. Then, the coefficient of QR before X^0Y^0 is also equal to 1, and we have $\log(QR) = \log Q + \log R$.

We are not going to prove this fact, as it is rather fundamental and well-known. But we derive a "finite version" from it (just as we derived Corollary 5.14 from Theorem 5.2):

Corollary 21.3. Let k be a field of characteristic 0. Let $n \in \mathbb{N}$.

Let $\mathfrak{A}$ be a commutative k-algebra. Let $\mathfrak{I}$ be an ideal of $\mathfrak{A}$ such that $\mathfrak{I}^{n+1} = 0$. Let $a \in \mathfrak{I}$ and $b \in \mathfrak{I}$. Then,

$$\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} a^i + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} b^i = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (a+b+ab)^i .$$

Proof of Corollary 21.3. **a)** First let us notice that

$$\text{every } (\alpha,\beta) \in \mathbb{N}^{\times 2} \text{ such that } \alpha+\beta > n \text{ satisfies } a^\alpha b^\beta = 0. \tag{178}$$

[112] Also, $a^{n+1} = 0$ (since $a \in \mathfrak{I}$, so that $a^{n+1} \in \mathfrak{I}^{n+1} = 0$), and $b^{n+1} = 0$ (for the same reason). Finally, $ab \in \mathfrak{I}$ (since $a \in \mathfrak{I}$ and since $\mathfrak{I}$ is an ideal), so that $\underbrace{a}_{\in \mathfrak{I}} + \underbrace{b}_{\in \mathfrak{I}} + \underbrace{ab}_{\in \mathfrak{I}} \in \mathfrak{I}+\mathfrak{I}+\mathfrak{I} \subseteq \mathfrak{I}$ (since $\mathfrak{I}$ is an ideal), so that $(a+b+ab)^{n+1} = 0$ (since $a+b+ab \in \mathfrak{I}$, so that $(a+b+ab)^{n+1} \in \mathfrak{I}^{n+1} = 0$).

b) Consider the ring of formal power series $k[[X,Y]]$ in two (commuting) indeterminates X and Y. For every power series $P \in k[[X,Y]]$ and every $(\alpha,\beta) \in \mathbb{N}^{\times 2}$, we let $\operatorname{coeff}_{\alpha,\beta}(P)$ denote the coefficient of the power series P before $X^\alpha Y^\beta$. Then, clearly,

$$\text{every power series } P \in k[[X,Y]] \text{ satisfies } P = \sum_{(\alpha,\beta) \in \mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot X^\alpha Y^\beta. \tag{179}$$

By the definition of the sum of two power series, we have

$$\operatorname{coeff}_{\alpha,\beta}(P+Q) = \operatorname{coeff}_{\alpha,\beta}(P) + \operatorname{coeff}_{\alpha,\beta}(Q) \tag{180}$$
$$\text{for any } (\alpha,\beta) \in \mathbb{N}^{\times 2}, \text{ any } P \in k[[X,Y]] \text{ and any } Q \in k[[X,Y]].$$

[112] *Proof of (178).* Let $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfy $\alpha+\beta > n$. Then, $\alpha+\beta \geq n+1$ (since $\alpha+\beta$ and $n+1$ are integers), so that $\mathfrak{I}^{\alpha+\beta} \subseteq \mathfrak{I}^{n+1}$ (since $\mathfrak{I}$ is an ideal of $\mathfrak{A}$).

On the other hand, $a \in \mathfrak{I}$, so that $a^\alpha \in \mathfrak{I}^\alpha$. Also, $b \in \mathfrak{I}$, so that $b^\beta \in \mathfrak{I}^\beta$. Thus, $\underbrace{a^\alpha}_{\in \mathfrak{I}^\alpha} \underbrace{b^\beta}_{\in \mathfrak{I}^\beta} \in \mathfrak{I}^\alpha \mathfrak{I}^\beta = \mathfrak{I}^{\alpha+\beta} \subseteq \mathfrak{I}^{n+1} = 0$. Hence, $a^\alpha b^\beta = 0$. This proves (178).

By the definition of the product of a power series with a scalar, we have

$$\operatorname{coeff}_{\alpha,\beta}(\lambda P) = \lambda \operatorname{coeff}_{\alpha,\beta}(P) \qquad \text{for any } (\alpha,\beta) \in \mathbb{N}^{\times 2}, \text{ any } P \in k[[X,Y]] \text{ and any } \lambda \in k. \tag{181}$$

By the definition of the product of two power series, we have

$$\operatorname{coeff}_{\alpha,\beta}(PQ) = \sum_{\substack{(\gamma,\delta)\in\mathbb{N}^{\times 2};\\ \gamma\leq\alpha;\ \delta\leq\beta}} \operatorname{coeff}_{\gamma,\delta}(P) \cdot \operatorname{coeff}_{\alpha-\gamma,\beta-\delta}(Q) \tag{182}$$
$$\text{for any } (\alpha,\beta) \in \mathbb{N}^{\times 2}, \text{ any } P \in k[[X,Y]] \text{ and any } Q \in k[[X,Y]].$$

c) Let us now define a map $\rho : k[[X,Y]] \to \mathfrak{A}$ by

$$\left(\rho(P) = \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta} \qquad \text{for every } P \in k[[X,Y]] \right). \tag{183}$$

Note that the sum $\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta}$ is a finite sum for every $P \in k[[X,Y]]$ (since there are only finitely many pairs $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfying $\alpha+\beta \leq n$), so this map ρ is well-defined.

d) Let us show that

$$\rho(P) = \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta} \qquad \text{for every } P \in k[[X,Y]]. \tag{184}$$

Here, the infinite sum $\sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta}$ has a well-defined value because all but finitely many addends of this sum are zero.[113]

Proof of (184). We already know that the sum $\sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta}$ is well-defined. Thus, we have

$$\sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta} = \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta}}_{\substack{=\rho(P)\\ \text{(by (183))}}} + \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta>n}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot \underbrace{a^{\alpha} b^{\beta}}_{\substack{=0\\ \text{(by (178),}\\ \text{since } \alpha+\beta>n)}}$$
$$= \rho(P) + \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta>n}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot 0}_{=0} = \rho(P).$$

[113] *Proof.* Only finitely many pairs $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfy $\alpha+\beta \leq n$. Hence, all but finitely many pairs $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ don't satisfy $\alpha+\beta \leq n$. In other words, all but finitely many pairs $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfy $\alpha+\beta > n$. But since every pair $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ which satisfies $\alpha+\beta > n$ must satisfy $\operatorname{coeff}_{\alpha,\beta}(P) \cdot \underbrace{a^{\alpha} b^{\beta}}_{=0 \text{ (by (178))}} = 0$, this yields that all but finitely many pairs $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfy $\operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta} = 0$. In other words, all but finitely many addends of the sum $\sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(P) \cdot a^{\alpha} b^{\beta}$ are zero. Qed.

This proves (184).

e) The map ρ is k-linear.

Proof. Every $P \in k[[X,Y]]$ and $Q \in k[[X,Y]]$ satisfy

$$\rho(P+Q) = \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \underbrace{\operatorname{coeff}_{\alpha,\beta}(P+Q)}_{\substack{=\operatorname{coeff}_{\alpha,\beta}(P)+\operatorname{coeff}_{\alpha,\beta}(Q)\\ \text{(by (180))}}} \cdot a^\alpha b^\beta \qquad \text{(by (183), applied to } P+Q \text{ instead of } P)$$
$$= \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} (\operatorname{coeff}_{\alpha,\beta}(P) + \operatorname{coeff}_{\alpha,\beta}(Q)) \cdot a^\alpha b^\beta$$

and

$$\underbrace{\rho(P)}_{\substack{=\sum\limits_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(P)\cdot a^\alpha b^\beta\\ \text{(by (183))}}} + \underbrace{\rho(Q)}_{\substack{=\sum\limits_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(Q)\cdot a^\alpha b^\beta\\ \text{(by (183), applied to } Q \text{ instead of } P)}}$$
$$= \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(P)\cdot a^\alpha b^\beta + \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(Q)\cdot a^\alpha b^\beta$$
$$= \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} (\operatorname{coeff}_{\alpha,\beta}(P) + \operatorname{coeff}_{\alpha,\beta}(Q)) \cdot a^\alpha b^\beta.$$

Hence, every $P \in k[[X,Y]]$ and $Q \in k[[X,Y]]$ satisfy

$$\rho(P+Q) = \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} (\operatorname{coeff}_{\alpha,\beta}(P) + \operatorname{coeff}_{\alpha,\beta}(Q)) \cdot a^\alpha b^\beta = \rho(P) + \rho(Q). \tag{185}$$

Also, every $P \in k[[X,Y]]$ and $\lambda \in k$ satisfy

$$\rho(\lambda P) = \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \underbrace{\operatorname{coeff}_{\alpha,\beta}(\lambda P)}_{\substack{=\lambda \operatorname{coeff}_{\alpha,\beta}(P)\\ \text{(by (181))}}} \cdot a^\alpha b^\beta \qquad \text{(by (183), applied to } \lambda P \text{ instead of } P)$$
$$= \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \lambda \operatorname{coeff}_{\alpha,\beta}(P)\cdot a^\alpha b^\beta = \lambda \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha+\beta\leq n}} \operatorname{coeff}_{\alpha,\beta}(P)\cdot a^\alpha b^\beta}_{\substack{=\rho(P)\\ \text{(by (183))}}} = \lambda\rho(P).$$

(186)

So we have proven that every $P \in k[[X,Y]]$ and $Q \in k[[X,Y]]$ satisfy (185), and that every $P \in k[[X,Y]]$ and $\lambda \in k$ satisfy (186). In other words, we have proven that ρ is k-linear.

f) The map ρ is a k-algebra homomorphism.

Proof. First of all, it is clear the power series 1 has coefficient 1 before X^0Y^0, while all its other coefficients are zero. In other words, $\operatorname{coeff}_{0,0}(1) = 1$, while $\operatorname{coeff}_{\alpha,\beta}(1) = 0$ for every $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfying $(\alpha,\beta) \neq (0,0)$.

Now, (184) (applied to $P = 1$) yields

$$\rho(1) = \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(1)\cdot a^{\alpha}b^{\beta} = \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)=(0,0)}} \operatorname{coeff}_{\alpha,\beta}(1)\cdot a^{\alpha}b^{\beta}}_{=\operatorname{coeff}_{0,0}(1)\cdot a^0 b^0} + \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)\neq(0,0)}} \underbrace{\operatorname{coeff}_{\alpha,\beta}(1)}_{\substack{=0\\ \text{(since } (\alpha,\beta)\neq(0,0))}} \cdot a^{\alpha}b^{\beta}$$

$$= \underbrace{\operatorname{coeff}_{0,0}(1)}_{=1}\cdot \underbrace{a^0}_{=1}\underbrace{b^0}_{=1} + \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)\neq(0,0)}} 0\cdot a^{\alpha}b^{\beta}}_{=0} = 1.$$

Now let $P \in k[[X,Y]]$ and $Q \in k[[X,Y]]$ be arbitrary. Then, multiplying the equalities

$$\rho(P) = \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(P)\cdot a^{\alpha}b^{\beta} \qquad \text{(by (184))}$$

$$= \sum_{(\gamma,\delta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\gamma,\delta}(P)\cdot a^{\gamma}b^{\delta} \qquad \text{(here, we renamed the index } (\alpha,\beta) \text{ as } (\gamma,\delta) \text{ in the sum)}$$

and

$$\rho(Q) = \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}(Q)\cdot a^{\alpha}b^{\beta} \qquad \text{(by (184), applied to } Q \text{ instead of } P),$$

we obtain

$$\begin{aligned}
\rho\left(P\right)\cdot\rho\left(Q\right) &= \left(\sum_{(\gamma,\delta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot a^{\gamma}b^{\delta}\right)\cdot\left(\sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}\left(Q\right)\cdot a^{\alpha}b^{\beta}\right) \\
&= \sum_{(\gamma,\delta)\in\mathbb{N}^{\times 2}}\ \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \underbrace{\operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot a^{\gamma}b^{\delta}\cdot\operatorname{coeff}_{\alpha,\beta}\left(Q\right)\cdot a^{\alpha}b^{\beta}}_{=\operatorname{coeff}_{\gamma,\delta}(P)\cdot\operatorname{coeff}_{\alpha,\beta}(Q)\cdot a^{\gamma}a^{\alpha}\cdot b^{\delta}b^{\beta}} \\
&= \sum_{(\gamma,\delta)\in\mathbb{N}^{\times 2}}\ \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot\operatorname{coeff}_{\alpha,\beta}\left(Q\right)\cdot\underbrace{a^{\gamma}a^{\alpha}}_{=a^{\gamma+\alpha}}\cdot\underbrace{b^{\delta}b^{\beta}}_{=b^{\delta+\beta}} \\
&= \sum_{(\gamma,\delta)\in\mathbb{N}^{\times 2}}\ \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot\operatorname{coeff}_{\alpha,\beta}\left(Q\right)\cdot a^{\gamma+\alpha}\cdot b^{\delta+\beta} \\
&= \underbrace{\sum_{(\gamma,\delta)\in\mathbb{N}^{\times 2}}\ \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ \alpha\geq\gamma;\ \beta\geq\delta}}}_{=\sum\limits_{(\alpha,\beta)\in\mathbb{N}^{\times 2}}\ \sum\limits_{\substack{(\gamma,\delta)\in\mathbb{N}^{\times 2};\\ \alpha\geq\gamma;\ \beta\geq\delta}}} \operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot\operatorname{coeff}_{\alpha-\gamma,\beta-\delta}\left(Q\right)\cdot\underbrace{a^{\gamma+(\alpha-\gamma)}}_{=a^{\alpha}}\cdot\underbrace{b^{\delta+(\beta-\delta)}}_{=b^{\beta}} \\
&\qquad \text{(here, we substituted } (\alpha,\beta) \text{ for } (\gamma+\alpha,\delta+\beta) \text{ in the second sum)} \\
&= \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}}\ \underbrace{\sum_{\substack{(\gamma,\delta)\in\mathbb{N}^{\times 2};\\ \alpha\geq\gamma;\ \beta\geq\delta}}}_{\substack{=\sum\limits_{\substack{(\gamma,\delta)\in\mathbb{N}^{\times 2};\\ \gamma\leq\alpha;\ \delta\leq\beta}} \\ \text{(since the assertion } (\alpha\geq\gamma \text{ and } \beta\geq\delta) \\ \text{is equivalent to } (\gamma\leq\alpha \text{ and } \delta\leq\beta))}} \operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot\operatorname{coeff}_{\alpha-\gamma,\beta-\delta}\left(Q\right)\cdot a^{\alpha}b^{\beta} \\
&= \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}}\ \sum_{\substack{(\gamma,\delta)\in\mathbb{N}^{\times 2};\\ \gamma\leq\alpha;\ \delta\leq\beta}} \operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot\operatorname{coeff}_{\alpha-\gamma,\beta-\delta}\left(Q\right)\cdot a^{\alpha}b^{\beta}.
\end{aligned}$$

Compared to

$$\begin{aligned}
\rho\left(PQ\right) &= \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \underbrace{\operatorname{coeff}_{\alpha,\beta}\left(PQ\right)}_{\substack{=\sum\limits_{\substack{(\gamma,\delta)\in\mathbb{N}^{\times 2};\\ \gamma\leq\alpha;\ \delta\leq\beta}} \operatorname{coeff}_{\gamma,\delta}(P)\cdot\operatorname{coeff}_{\alpha-\gamma,\beta-\delta}(Q) \\ \text{(by (182))}}} \cdot a^{\alpha}b^{\beta} \qquad \text{(by (184), applied to } PQ \text{ instead of } P) \\
&= \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}}\ \sum_{\substack{(\gamma,\delta)\in\mathbb{N}^{\times 2};\\ \gamma\leq\alpha;\ \delta\leq\beta}} \operatorname{coeff}_{\gamma,\delta}\left(P\right)\cdot\operatorname{coeff}_{\alpha-\gamma,\beta-\delta}\left(Q\right)\cdot a^{\alpha}b^{\beta},
\end{aligned}$$

this yields $\rho\left(P\right)\cdot\rho\left(Q\right)=\rho\left(PQ\right)$.

Now forget that we fixed P and Q. We thus have shown that any $P\in k\left[\left[X,Y\right]\right]$ and $Q\in k\left[\left[X,Y\right]\right]$ satisfy $\rho\left(P\right)\cdot\rho\left(Q\right)=\rho\left(PQ\right)$. Combined with $\rho\left(1\right)=1$, and with the fact that ρ is k-linear, this yields that ρ is a k-algebra homomorphism. This proves part **f)**.

g) Both $1+X$ and $1+Y$ are power series in $k\left[\left[X,Y\right]\right]$ whose coefficients before $X^{0}Y^{0}$ are equal to 1. Hence, we can apply Theorem 21.2 to $Q=1+X$ and $R=1+Y$. As a result, we obtain that the coefficient of $\left(1+X\right)\left(1+Y\right)$ before $X^{0}Y^{0}$ is also equal

to 1 (of course, this is obvious for simpler reasons...) and that

$$\log\left(\left(1+X\right)\left(1+Y\right)\right) = \log\left(1+X\right) + \log\left(1+Y\right). \tag{187}$$

h) The power series X has the coefficient 1 before X^1Y^0, while all its other coefficients are zero. In other words, $\operatorname{coeff}_{1,0}\left(X\right) = 1$, while $\operatorname{coeff}_{\alpha,\beta}\left(X\right) = 0$ for all $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfying $(\alpha,\beta) \neq (1,0)$. Now, (184) (applied to $P = X$) yields

$$\begin{aligned}
\rho\left(X\right) &= \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}\left(X\right) \cdot a^{\alpha} b^{\beta} \\
&= \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)=(1,0)}} \operatorname{coeff}_{\alpha,\beta}\left(X\right) \cdot a^{\alpha} b^{\beta}}_{=\operatorname{coeff}_{1,0}(X)\cdot a^1 b^0} + \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)\neq(1,0)}} \underbrace{\operatorname{coeff}_{\alpha,\beta}\left(X\right)}_{\substack{=0\\ \text{(since } (\alpha,\beta)\neq(1,0))}} \cdot a^{\alpha} b^{\beta} \\
&= \underbrace{\operatorname{coeff}_{1,0}\left(X\right)}_{=1} \cdot \underbrace{a^1}_{=a} \underbrace{b^0}_{=1} + \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)\neq(1,0)}} 0 \cdot a^{\alpha} b^{\beta}}_{=0} = a.
\end{aligned}$$

The power series Y has the coefficient 1 before X^0Y^1, while all its other coefficients are zero. In other words, $\operatorname{coeff}_{0,1}\left(Y\right) = 1$, while $\operatorname{coeff}_{\alpha,\beta}\left(Y\right) = 0$ for all $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfying $(\alpha,\beta) \neq (0,1)$. Now, (184) (applied to $P = Y$) yields

$$\begin{aligned}
\rho\left(Y\right) &= \sum_{(\alpha,\beta)\in\mathbb{N}^{\times 2}} \operatorname{coeff}_{\alpha,\beta}\left(Y\right) \cdot a^{\alpha} b^{\beta} \\
&= \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)=(0,1)}} \operatorname{coeff}_{\alpha,\beta}\left(Y\right) \cdot a^{\alpha} b^{\beta}}_{=\operatorname{coeff}_{0,1}(Y)\cdot a^0 b^1} + \sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)\neq(0,1)}} \underbrace{\operatorname{coeff}_{\alpha,\beta}\left(Y\right)}_{\substack{=0\\ \text{(since } (\alpha,\beta)\neq(0,1))}} \cdot a^{\alpha} b^{\beta} \\
&= \underbrace{\operatorname{coeff}_{0,1}\left(Y\right)}_{=1} \cdot \underbrace{a^0}_{=1} \underbrace{b^1}_{=b} + \underbrace{\sum_{\substack{(\alpha,\beta)\in\mathbb{N}^{\times 2};\\ (\alpha,\beta)\neq(0,1)}} 0 \cdot a^{\alpha} b^{\beta}}_{=0} = b.
\end{aligned}$$

Since ρ is a k-algebra homomorphism, we have $\rho\left(X+Y+XY\right) = \underbrace{\rho\left(X\right)}_{=a} + \underbrace{\rho\left(Y\right)}_{=b} + \underbrace{\rho\left(X\right)}_{=a} \cdot \underbrace{\rho\left(Y\right)}_{=b} = a + b + ab$.

i) By the definition of log, we have

$$\begin{aligned}
\log(1+X) &= \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} \left(\underbrace{(1+X)-1}_{=X} \right)^i = \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} X^i \\
&= \underbrace{\sum_{\substack{i\geq 1; \\ i<n+1}}}_{=\sum_{i=1}^{n}} \frac{(-1)^{i-1}}{i} X^i + \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} \underbrace{X^i}_{\substack{=X^{n+1}\cdot X^{i-(n+1)} \\ \text{(since } i\geq n+1\text{)}}} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} X^i + \underbrace{\sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} X^{n+1}\cdot X^{i-(n+1)}}_{=X^{n+1}\sum\limits_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} X^{i-(n+1)}} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} X^i + X^{n+1} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} X^{i-(n+1)}.
\end{aligned}$$

Hence,

$$\begin{aligned}
\rho(\log(1+X)) &= \rho\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} X^i + X^{n+1} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} X^{i-(n+1)} \right) \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (\rho(X))^i + (\rho(X))^{n+1} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} (\rho(X))^{i-(n+1)} \\
&\qquad \text{(since } \rho \text{ is a } k\text{-algebra homomorphism)} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} a^i + \underbrace{a^{n+1}}_{=0} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} a^{i-(n+1)} \qquad (\text{since } \rho(X) = a) \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} a^i + \underbrace{0 \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} a^{i-(n+1)}}_{=0} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} a^i. \qquad (188)
\end{aligned}$$

The same argument, but with X and a replaced by Y and b, yields

$$\rho(\log(1+Y)) = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} b^i. \qquad (189)$$

On the other hand, the definition of log yields

$$
\begin{aligned}
&\log\left(\left(1+X\right)\left(1+Y\right)\right) \\
&= \sum_{i\geq 1} \frac{\left(-1\right)^{i-1}}{i} \left(\underbrace{\left(1+X\right)\left(1+Y\right)-1}_{=X+Y+XY} \right)^i = \sum_{i\geq 1} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^i \\
&= \underbrace{\sum_{\substack{i\geq 1; \\ i<n+1}}}_{=\sum_{i=1}^{n}} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^i + \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{\left(-1\right)^{i-1}}{i} \underbrace{\left(X+Y+XY\right)^i}_{\substack{=(X+Y+XY)^{n+1}\cdot(X+Y+XY)^{i-(n+1)} \\ (\text{since } i\geq n+1)}} \\
&= \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^i + \underbrace{\sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^{n+1} \cdot \left(X+Y+XY\right)^{i-(n+1)}}_{=(X+Y+XY)^{n+1} \sum\limits_{\substack{i\geq 1; \\ i\geq n+1}} \frac{(-1)^{i-1}}{i} (X+Y+XY)^{i-(n+1)}} \\
&= \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^i + \left(X+Y+XY\right)^{n+1} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^{i-(n+1)}.
\end{aligned}
$$

Hence,

$$
\begin{aligned}
&\rho\left(\log\left(\left(1+X\right)\left(1+Y\right)\right)\right) \\
&= \rho\left(\sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^i + \left(X+Y+XY\right)^{n+1} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{\left(-1\right)^{i-1}}{i} \left(X+Y+XY\right)^{i-(n+1)} \right) \\
&= \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} \left(\rho\left(X+Y+XY\right)\right)^i + \left(\rho\left(X+Y+XY\right)\right)^{n+1} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{\left(-1\right)^{i-1}}{i} \left(\rho\left(X+Y+XY\right)\right)^{i-(n+1)} \\
&\qquad (\text{since } \rho \text{ is a } k\text{-algebra homomorphism}) \\
&= \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} \left(a+b+ab\right)^i + \underbrace{\left(a+b+ab\right)^{n+1}}_{=0} \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{\left(-1\right)^{i-1}}{i} \left(a+b+ab\right)^{i-(n+1)} \\
&\qquad (\text{since } \rho\left(X+Y+XY\right) = a+b+ab) \\
&= \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} \left(a+b+ab\right)^i + \underbrace{0 \sum_{\substack{i\geq 1; \\ i\geq n+1}} \frac{\left(-1\right)^{i-1}}{i} \left(a+b+ab\right)^{i-(n+1)}}_{=0} = \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} \left(a+b+ab\right)^i.
\end{aligned}
$$

Compared with

$$\rho\left(\underbrace{\log\left(\left(1+X\right)\left(1+Y\right)\right)}_{\substack{=\log(1+X)+\log(1+Y)\\ \text{(by (187))}}}\right)$$
$$= \rho\left(\log\left(1+X\right)+\log\left(1+Y\right)\right) = \underbrace{\rho\left(\log\left(1+X\right)\right)}_{\substack{=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}a^i\\ \text{(by (188))}}} + \underbrace{\rho\left(\log\left(1+Y\right)\right)}_{\substack{=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}b^i\\ \text{(by (189))}}} \qquad \text{(since } \rho \text{ is } k\text{-linear)}$$
$$= \sum_{i=1}^{n}\frac{\left(-1\right)^{i-1}}{i}a^i + \sum_{i=1}^{n}\frac{\left(-1\right)^{i-1}}{i}b^i,$$

this yields

$$\sum_{i=1}^{n}\frac{\left(-1\right)^{i-1}}{i}a^i + \sum_{i=1}^{n}\frac{\left(-1\right)^{i-1}}{i}b^i = \sum_{i=1}^{n}\frac{\left(-1\right)^{i-1}}{i}\left(a+b+ab\right)^i.$$

This proves Corollary 21.3. □

We further prepare for proving Theorem 21.1 by showing a useful result that we ought to have proven long ago:

Proposition 21.4. Let k be a field. Let A be a k-algebra, and let C be a filtered k-coalgebra. In this proposition, we shall denote the convolution on $\mathcal{L}\left(C, A\right)$ as ordinary multiplication (i.e., we write fg for the convolution $f * g$ of two maps $f, g \in \mathcal{L}\left(C, A\right)$).

(a) Any $a \in \mathbb{N}$ and $b \in \mathbb{N}$ satisfy $\left(\mathcal{L}^a\left(C, A\right)\right) \cdot \left(\mathcal{L}^b\left(C, A\right)\right) \subseteq \mathcal{L}^{a+b}\left(C, A\right)$.

(b) Any $n \in \mathbb{N}$ satisfies $\left(\mathcal{L}^1\left(C, A\right)\right)^n \subseteq \mathcal{L}^n\left(C, A\right)$.

Proof of Proposition 21.4. **(a)** Let $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

Due to how we defined $\mathcal{L}^n\left(C, A\right)$ (in Definition 3.1 **(b)**), we have

$$\mathcal{L}^n\left(C, A\right) = \left\{f \in \mathcal{L}\left(C, A\right) \mid f\mid_{C_{\leq n-1}} = 0\right\}$$
$$= \left\{h \in \mathcal{L}\left(C, A\right) \mid h\mid_{C_{\leq n-1}} = 0\right\} \qquad \text{(here, we renamed } f \text{ as } h\text{)} \quad (190)$$

for every $n \in \mathbb{N}$.

It is easy to see that every $(f, g) \in \left(\mathcal{L}^a\left(C, A\right)\right) \times \left(\mathcal{L}^b\left(C, A\right)\right)$ satisfies $f * g \in \mathcal{L}^{a+b}\left(C, A\right)$. [114] In other words,

$$\left\{f * g \mid (f, g) \in \left(\mathcal{L}^a\left(C, A\right)\right) \times \left(\mathcal{L}^b\left(C, A\right)\right)\right\} \subseteq \mathcal{L}^{a+b}\left(C, A\right).$$

[114] *Proof.* Let $(f, g) \in \left(\mathcal{L}^a\left(C, A\right)\right) \times \left(\mathcal{L}^b\left(C, A\right)\right)$ be arbitrary. Then, $f \in \mathcal{L}^a\left(C, A\right)$ and $g \in \mathcal{L}^b\left(C, A\right)$. Now, $f \in \mathcal{L}^a\left(C, A\right) = \left\{h \in \mathcal{L}\left(C, A\right) \mid h\mid_{C_{\leq a-1}} = 0\right\}$ (by (190), applied to $n = a$), so that $f\mid_{C_{\leq a-1}} = 0$. Hence, $f\left(C_{\leq a-1}\right) = \underbrace{\left(f\mid_{C_{\leq a-1}}\right)}_{=0}\left(C_{\leq a-1}\right) = 0\left(C_{\leq a-1}\right) = 0$. Similarly, $g\left(C_{\leq b-1}\right) = 0$.

Since C is a filtered k-coalgebra, we have $\Delta_C\left(C_{\leq a+b-1}\right) \subseteq \sum_{u=0}^{a+b-1} C_{\leq u} \otimes C_{\leq a+b-1-u}$.

Thus, (154) (applied to $M = \mathcal{L}(C, A)$, $S = \left\{ f * g \mid (f, g) \in \left(\mathcal{L}^a(C, A)\right) \times \left(\mathcal{L}^b(C, A)\right) \right\}$ and $Q = \mathcal{L}^{a+b}(C, A)$) yields

$$\left\langle \left\{ f * g \mid (f, g) \in \left(\mathcal{L}^a(C, A)\right) \times \left(\mathcal{L}^b(C, A)\right) \right\} \right\rangle \subseteq \mathcal{L}^{a+b}(C, A).$$

Since

$$\begin{aligned}
&\left\langle \left\{ f * g \mid (f, g) \in \left(\mathcal{L}^a(C, A)\right) \times \left(\mathcal{L}^b(C, A)\right) \right\} \right\rangle \\
&= \left\langle \underbrace{f * g}_{=fg} \mid (f, g) \in \left(\mathcal{L}^a(C, A)\right) \times \left(\mathcal{L}^b(C, A)\right) \right\rangle \\
&= \left\langle fg \mid (f, g) \in \left(\mathcal{L}^a(C, A)\right) \times \left(\mathcal{L}^b(C, A)\right) \right\rangle = \left(\mathcal{L}^a(C, A)\right) \cdot \left(\mathcal{L}^b(C, A)\right),
\end{aligned}$$

this becomes $\left(\mathcal{L}^a(C, A)\right) \cdot \left(\mathcal{L}^b(C, A)\right) \subseteq \mathcal{L}^{a+b}(C, A)$. This proves Proposition 21.4 **(a)**.

(b) We are going to prove Proposition 21.4 **(b)** by induction over n:

Induction base: From Definition 3.1 **(b)** (applied to C instead of H), we know that $\mathcal{L}^0(C, A) = \mathcal{L}(C, A)$. Now, clearly, $\left(\mathcal{L}^1(C, A)\right)^0 \subseteq \mathcal{L}(C, A) = \mathcal{L}^0(C, A)$. In other words, Proposition 21.4 **(b)** holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that Proposition 21.4 **(b)** holds for $n = N$. We must now prove that Proposition 21.4 **(b)** also holds for $n = N + 1$.

Since Proposition 21.4 **(b)** holds for $n = N$, we have $\left(\mathcal{L}^1(C, A)\right)^N \subseteq \mathcal{L}^N(C, A)$. Now,

$$\begin{aligned}
\left(\mathcal{L}^1(C, A)\right)^{N+1} &= \underbrace{\left(\mathcal{L}^1(C, A)\right)^N}_{\subseteq \mathcal{L}^N(C,A)} \cdot \left(\mathcal{L}^1(C, A)\right) \subseteq \left(\mathcal{L}^N(C, A)\right) \cdot \left(\mathcal{L}^1(C, A)\right) \\
&\subseteq \mathcal{L}^{N+1}(C, A) \qquad \text{(by Proposition 21.4 \textbf{(a)}, applied to } a = N \text{ and } b = 1).
\end{aligned}$$

In other words, Proposition 21.4 **(b)** holds for $n = N+1$. This completes the induction step. Thus, the induction proof of Proposition 21.4 **(b)** is complete. □

Here is, finally, an equivalent version of Corollary 21.3 for use in our proof of Theorem 21.1:

Corollary 21.5. Let k be a field of characteristic 0. Let $n \in \mathbb{N}$.

Let $\mathfrak{B}$ be a commutative k-algebra. Let $\mathfrak{K}$ be an ideal of $\mathfrak{B}$. Let $a \in \mathfrak{K}$ and $b \in \mathfrak{K}$. Then,

$$\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} a^i + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} b^i - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (a + b + ab)^i \in \mathfrak{K}^{n+1}.$$

Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$. This yields

$$C_{\leq u} \subseteq C_{\leq a-1} \text{ for every } u \in \mathbb{N} \text{ satisfying } u \leq a - 1, \tag{191}$$

and

$$C_{\leq v} \subseteq C_{\leq b-1} \text{ for every } v \in \mathbb{N} \text{ satisfying } v \leq b - 1. \tag{192}$$

Thus,

$$C_{\leq a+b-1-u} \subseteq C_{\leq b-1} \text{ for every } u \in \mathbb{N} \text{ satisfying } u \geq a \text{ and } u \leq a + b - 1 \tag{193}$$

(because for every $u \in \mathbb{N}$ satisfying $u \geq a$ and $u \leq a + b - 1$, we have $a + b - 1 - u \in \mathbb{N}$ (since $\underbrace{a + b - 1}_{\geq u} - u \geq u - u = 0$) and $a + b - 1 - \underbrace{u}_{\geq a} \leq a + b - 1 - a = b - 1$, and thus $C_{\leq a+b-1-u} \subseteq C_{\leq b-1}$ (by (192), applied to $v = a + b - 1 - u$)).

Proof of Corollary 21.5. Since $\mathfrak{K}$ is an ideal of $\mathfrak{B}$, it is clear that $\mathfrak{K}^{n+1}$ is an ideal of $\mathfrak{B}$.

Let π be the canonical projection $\mathfrak{B} \to \mathfrak{B} / \mathfrak{K}^{n+1}$. Then, π is a k-algebra homomorphism (since $\mathfrak{K}^{n+1}$ is an ideal of $\mathfrak{B}$, so that $\mathfrak{B} / \mathfrak{K}^{n+1}$ is a factor algebra), so that

$$(\pi(\mathfrak{K}))^{n+1} = \pi\left(\mathfrak{K}^{n+1}\right) = 0 \qquad \left(\text{since } \pi \text{ is the canonical projection } \mathfrak{B} \to \mathfrak{B} / \mathfrak{K}^{n+1}\right).$$

Let $\mathfrak{A}$ be the k-algebra $\mathfrak{B} / \mathfrak{K}^{n+1}$, and let $\mathfrak{I}$ be the subset $\pi(\mathfrak{K})$ of $\mathfrak{B} / \mathfrak{K}^{n+1} = \mathfrak{A}$. The k-algebra $\mathfrak{A}$ is commutative (because $\mathfrak{A}$ is a quotient of the commutative k-algebra $\mathfrak{B}$).

By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$, so that

$$\begin{aligned}
&(f * g)\left(C_{\leq a+b-1}\right) \\
&= \left(\mu_A \circ (f \otimes g) \circ \Delta_C\right)\left(C_{\leq a+b-1}\right) = \mu_A\left((f \otimes g)\underbrace{\left(\Delta_C\left(C_{\leq a+b-1}\right)\right)}_{\subseteq \sum_{u=0}^{a+b-1} C_{\leq u} \otimes C_{\leq a+b-1-u}}\right) \\
&\subseteq \mu_A\left(\underbrace{(f \otimes g)\left(\sum_{u=0}^{a+b-1} C_{\leq u} \otimes C_{\leq a+b-1-u}\right)}_{\substack{\subseteq \sum_{u=0}^{a+b-1} (f \otimes g)\left(C_{\leq u} \otimes C_{\leq a+b-1-u}\right) \\ \text{(since } f \otimes g \text{ is } k\text{-linear)}}}\right) \subseteq \mu_A\left(\sum_{u=0}^{a+b-1} \underbrace{(f \otimes g)\left(C_{\leq u} \otimes C_{\leq a+b-1-u}\right)}_{\subseteq f\left(C_{\leq u}\right) \otimes g\left(C_{\leq a+b-1-u}\right)}\right) \\
&\subseteq \mu_A\left(\underbrace{\sum_{u=0}^{a+b-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq a+b-1-u}\right)}_{= \sum_{u=0}^{a-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq a+b-1-u}\right) + \sum_{u=a}^{a+b-1} f\left(C_{\leq u}\right) \otimes g\left(C_{\leq a+b-1-u}\right)}\right) \\
&= \mu_A\left(\sum_{u=0}^{a-1} f\left(\underbrace{C_{\leq u}}_{\substack{\subseteq C_{\leq a-1} \\ \text{(by (191), since } u \leq a-1)}}\right) \otimes g\left(C_{\leq a+b-1-u}\right) + \sum_{u=a}^{a+b-1} f\left(C_{\leq u}\right) \otimes g\left(\underbrace{C_{\leq a+b-1-u}}_{\substack{\subseteq C_{\leq b-1} \\ \text{(by (193), since } u \geq a \text{ and } u \leq a+b-1)}}\right)\right) \\
&= \mu_A\left(\sum_{u=0}^{a-1} \underbrace{f\left(C_{\leq a-1}\right)}_{=0} \otimes g\left(C_{\leq a+b-1-u}\right) + \sum_{u=a}^{a+b-1} f\left(C_{\leq u}\right) \otimes \underbrace{g\left(C_{\leq b-1}\right)}_{=0}\right) \\
&= \mu_A\left(\sum_{u=0}^{a-1} \underbrace{0 \otimes g\left(C_{\leq a+b-1-u}\right)}_{=0} + \sum_{u=a}^{a+b-1} \underbrace{f\left(C_{\leq u}\right) \otimes 0}_{=0}\right) = \mu_A\left(\underbrace{\sum_{u=0}^{a-1} 0 + \sum_{u=a}^{a+b-1} 0}_{=0}\right) = \mu_A(0) = 0.
\end{aligned}$$

Hence, $f * g \in \left\{h \in \mathcal{L}(C, A) \mid h|_{C_{\leq a+b-1}} = 0\right\}$. Since $\mathcal{L}^{a+b}(C, A) = \left\{h \in \mathcal{L}(C, A) \mid h|_{C_{\leq a+b-1}} = 0\right\}$ (by (190), applied to $n = a + b$), this becomes

$$f * g \in \left\{h \in \mathcal{L}(C, A) \mid h|_{C_{\leq a+b-1}} = 0\right\} = \mathcal{L}^{a+b}(C, A),$$

qed.

Since π is the canonical projection $\mathfrak{B} \to \mathfrak{B} / \mathfrak{K}^{n+1}$, this map π is surjective. Thus, $\pi(\mathfrak{B}) = \mathfrak{B} / \mathfrak{K}^{n+1} = \mathfrak{A}$.

Since $\mathfrak{K}$ is an ideal of $\mathfrak{B}$, we have $\mathfrak{BK} \subseteq \mathfrak{K}$. Now,

$$\underbrace{\mathfrak{A}}_{=\pi(\mathfrak{B})} \underbrace{\mathfrak{I}}_{=\pi(\mathfrak{K})} = \pi(\mathfrak{B})\,\pi(\mathfrak{K}) = \pi\left(\underbrace{\mathfrak{BK}}_{\subseteq \mathfrak{K}}\right) \qquad \text{(since } \pi \text{ is a } k\text{-algebra homomorphism)}$$
$$\subseteq \pi(\mathfrak{K}) = \mathfrak{I}.$$

In other words, $\mathfrak{I}$ is a right ideal of $\mathfrak{A}$. Since $\mathfrak{A}$ is commutative, this yields that $\mathfrak{I}$ is an ideal of $\mathfrak{A}$. Also, $\mathfrak{I} = \pi(\mathfrak{K})$ leads to $\mathfrak{I}^{n+1} = (\pi(\mathfrak{K}))^{n+1} = 0$.

Since $a \in \mathfrak{K}$, we have $\pi(a) \in \pi(\mathfrak{K}) = \mathfrak{I}$. Similarly, $\pi(b) \in \mathfrak{I}$. Therefore, we can apply Corollary 21.3 to $\pi(a)$ and $\pi(b)$ instead of a and b. We obtain

$$\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (\pi(a))^i + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (\pi(b))^i = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (\pi(a) + \pi(b) + \pi(a)\,\pi(b))^i.$$

Hence,

$$0 = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (\pi(a))^i + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (\pi(b))^i - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (\pi(a) + \pi(b) + \pi(a)\,\pi(b))^i$$
$$= \pi\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} a^i + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} b^i - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (a + b + ab)^i\right)$$

(since π is a k-algebra homomorphism). In other words,

$$\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} a^i + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} b^i - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (a + b + ab)^i \in \operatorname{Ker} \pi = \mathfrak{K}^{n+1}$$

(since π is the canonical projection $\mathfrak{B} \to \mathfrak{B} / \mathfrak{K}^{n+1}$). This proves Corollary 21.5. $\square$

Proof of Theorem 21.1. **a)** First, we notice that $F * H \in G(C, A)$.

Proof. By the definition of $G(C, A)$, we have

$$G(C, A) = \{f \in \mathcal{L}(C, A) \mid f(1_C) = 1_A\}.$$

Now, $F \in G(C, A) = \{f \in \mathcal{L}(C, A) \mid f(1_C) = 1_A\}$, so that $F(1_C) = 1_A$. Similarly, $G(1_C) = 1_A$. But since 1_C is the unity of the unital coalgebra C, we have $\Delta_C(1_C) = 1_C \otimes 1_C$ and $\varepsilon_C(1_C) = 1$ (by the definition of a unital coalgebra).

By the definition of convolution, $F * H = \mu_A \circ (F \otimes H) \circ \Delta_C$. Hence,

$$(F * H)(1_C) = (\mu_A \circ (F \otimes H) \circ \Delta_C)(1_C) = \mu_A\left((F \otimes H)\underbrace{(\Delta_C(1_C))}_{=1_C \otimes 1_C}\right) = \mu_A\left(\underbrace{(F \otimes H)(1_C \otimes 1_C)}_{=F(1_C) \otimes H(1_C)}\right)$$
$$= \mu_A\left(\underbrace{F(1_C)}_{=1_A} \otimes \underbrace{H(1_C)}_{=1_A}\right) = \mu_A(1_A \otimes 1_A)$$
$$= 1_A 1_A \qquad \text{(since } \mu_A \text{ is the multiplication map)}$$
$$= 1_A.$$

In other words,

$$F * H \in \{f \in \mathcal{L}(C, A) \mid f(1_C) = 1_A\} = G(C, A).$$

Thus we have proven that $F * H \in G(C, A)$. This completes the proof of **a)**.

b) Now let us prove that $\operatorname{Log}(F * H) = \operatorname{Log} F + \operatorname{Log} H$.

Proof. Let $x \in C$. We are now going to prove that $(\operatorname{Log} F + \operatorname{Log} H - \operatorname{Log}(F * H))(x) = 0$.

Since C is filtered, there exists some $n \in \mathbb{N}$ such that $x \in C_{\leq n}$. Consider this n.

Due to how we defined $\mathcal{L}^{n+1}(C, A)$ (in Definition 3.1 **(b)**), we have

$$\mathcal{L}^{n+1}(C, A) = \left\{ f \in \mathcal{L}(C, A) \mid \underbrace{f|_{C_{\leq n+1-1}}}_{=f|_{C_{\leq n}}} = 0 \right\} = \left\{ f \in \mathcal{L}(C, A) \mid f|_{C_{\leq n}} = 0 \right\}$$
$$= \left\{ g \in \mathcal{L}(C, A) \mid g|_{C_{\leq n}} = 0 \right\} \qquad \text{(here, we renamed } f \text{ as } g\text{)}. \quad (194)$$

Let $f = F - e_{C,A}$ and $h = H - e_{C,A}$. Then, $\underbrace{f}_{=F-e_{C,A}} + e_{C,A} = F - e_{C,A} + e_{C,A} = F$ and similarly $h + e_{C,A} = H$. Hence,

$$\underbrace{F}_{=f+e_{C,A}} * \underbrace{H}_{=h+e_{C,A}} - e_{C,A} = \underbrace{(f + e_{C,A}) * (h + e_{C,A})}_{=f*h+f*e_{C,A}+e_{C,A}*h+e_{C,A}*e_{C,A}} - e_{C,A}$$
$$= f * h + \underbrace{f * e_{C,A}}_{=f} + \underbrace{e_{C,A} * h}_{=h} + \underbrace{e_{C,A} * e_{C,A}}_{=e_{C,A}} - e_{C,A}$$
$$= f * h + f + h + e_{C,A} - e_{C,A} = f + h + f * h. \quad (195)$$

Note that $f = F - e_{C,A}$ and $h = H - e_{C,A}$ lead to

$$\underbrace{f}_{=F-e_{C,A}} * \underbrace{h}_{=H-e_{C,A}} = (F - e_{C,A}) * (H - e_{C,A}) = \underbrace{F * H}_{=H*F} - \underbrace{F * e_{C,A}}_{=F=e_{C,A}*F} - \underbrace{e_{C,A} * H}_{=H=H*e_{C,A}} + e_{C,A} * e_{C,A}$$
$$= H * F - e_{C,A} * F - H * e_{C,A} + e_{C,A} * e_{C,A}$$
$$= \underbrace{(H - e_{C,A})}_{=h} * \underbrace{(F - e_{C,A})}_{=f} = h * f.$$

Since $F \in G(C, A) = e_{C,A} + \mathfrak{g}(C, A)$, we have $F - e_{C,A} \in \mathfrak{g}(C, A)$. Since $F - e_{C,A} = f$, this rewrites as $f \in \mathfrak{g}(C, A)$. Similarly, $h \in \mathfrak{g}(C, A)$. Moreover, since $F * H \in G(C, A) = e_{C,A} + \mathfrak{g}(C, A)$, we have $F * H - e_{C,A} \in \mathfrak{g}(C, A)$. By (195), this becomes $f + h + f * h \in \mathfrak{g}(C, A)$.

We recall that $\mathcal{L}^1(C, A) = \mathfrak{g}(C, A)$ (by Definition 3.1 **(b)**, applied to C instead of H). Since $\mathcal{L}^1(C, A)$ is an ideal of $\mathcal{L}(C, A)$ (by Proposition 14.2, applied to 1 and C instead of n and H), this yields that $\mathfrak{g}(C, A)$ is an ideal of $\mathcal{L}(C, A)$.

We know that $f * h = h * f$. In other words, f and h commute (as elements of $\mathcal{L}(C, A)$). Let $\mathfrak{B}$ be the k-subalgebra of $\mathcal{L}(C, A)$ generated by f and h. Then, the k-algebra $\mathfrak{B}$ is commutative (by Corollary 11.3, applied to $\mathcal{L}(C, A)$, h and $\mathfrak{B}$ instead of A, g and $\mathfrak{H}$).

Let $\mathfrak{K} = \mathfrak{B} \cap \mathfrak{g}(C, A)$. Then, $\mathfrak{K} = \mathfrak{B} \cap \mathfrak{g}(C, A) \subseteq \mathfrak{B}$ and $\mathfrak{K} = \mathfrak{B} \cap \mathfrak{g}(C, A) \subseteq \mathfrak{g}(C, A)$.

Since $\mathfrak{g}(C,A)$ is an ideal of $\mathcal{L}(C,A)$, we have $(\mathcal{L}(C,A)) \cdot (\mathfrak{g}(C,A)) \subseteq \mathfrak{g}(C,A)$. Now, combining

$$\underbrace{\mathfrak{B}}_{\subseteq \mathcal{L}(C,A)} \cdot \underbrace{\mathfrak{K}}_{\subseteq \mathfrak{g}(C,A)} \subseteq (\mathcal{L}(C,A)) \cdot (\mathfrak{g}(C,A)) \subseteq \mathfrak{g}(C,A)$$

with

$$\mathfrak{B} \cdot \underbrace{\mathfrak{K}}_{\subseteq \mathfrak{B}} \subseteq \mathfrak{B} \cdot \mathfrak{B} \subseteq \mathfrak{B} \qquad \text{(since } \mathfrak{B} \text{ is a } k\text{-algebra)},$$

we get $\mathfrak{B} \cdot \mathfrak{K} \subseteq \mathfrak{B} \cap \mathfrak{g}(C,A) = \mathfrak{K}$. Thus, $\mathfrak{K}$ is a left ideal of $\mathfrak{B}$. Since $\mathfrak{B}$ is commutative, this means that $\mathfrak{K}$ is an ideal of $\mathfrak{B}$.

Since $f \in \mathfrak{B}$ (by the definition of $\mathfrak{B}$) and $f \in \mathfrak{g}(C,A)$, we have $f \in \mathfrak{B} \cap \mathfrak{g}(C,A) = \mathfrak{K}$. Similarly, $h \in \mathfrak{K}$. Hence, Corollary 21.5 (applied to $a = f$ and $b = h$) yields

$$\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i} + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} h^{*i} - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (f + h + f * h)^{*i} \in \mathfrak{K}^{n+1}. \tag{196}$$

Since $\mathfrak{K} \subseteq \mathfrak{g}(C,A) = \mathcal{L}^1(C,A)$, we have $\mathfrak{K}^{n+1} \subseteq (\mathcal{L}^1(C,A))^{n+1} \subseteq \mathcal{L}^{n+1}(C,A)$ (by Proposition 21.4 **(b)**, applied to $n+1$ instead of n). Hence, (196) becomes

$$\begin{aligned}
&\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i} + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} h^{*i} - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (f + h + f * h)^{*i} \\
&\in \mathfrak{K}^{n+1} \subseteq \mathcal{L}^{n+1}(C,A) = \left\{ g \in \mathcal{L}(C,A) \mid g|_{C_{\leq n}} = 0 \right\} \qquad \text{(by (194))}.
\end{aligned}$$

In other words,

$$\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i} + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} h^{*i} - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (f + h + f * h)^{*i} \right) |_{C_{\leq n}} = 0.$$

Hence,

$$\begin{aligned}
&\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i} + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} h^{*i} - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (f + h + f * h)^{*i} \right)(x) \\
&= \underbrace{\left(\left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i} + \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} h^{*i} - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} (f + h + f * h)^{*i} \right) |_{C_{\leq n}} \right)(x)}_{=0} \\
&\qquad \text{(since } x \in C_{\leq n}\text{)} \\
&= 0(x) = 0.
\end{aligned} \tag{197}$$

Now, by the definition of Log, we have $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{C,A})}_{=f} = \operatorname{Log}_1 f$, so that

$$\begin{aligned}
(\operatorname{Log} F)(x) &= (\operatorname{Log}_1 f)(x) \\
&= \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) \qquad \text{(by the definition of } \operatorname{Log}_1\text{)} \\
&= \underbrace{\sum_{\substack{i \geq 1; \\ i \leq n}}}_{=\sum_{i=1}^{n}} \frac{(-1)^{i-1}}{i} f^{*i}(x) + \sum_{\substack{i \geq 1; \\ i > n}} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{\substack{=0 \text{ (since} \\ x \in C_{\leq n} \text{ and thus } f^{*i}(x) \in f^{*i}\left(C_{\leq n}\right) = 0 \\ \text{(by Remark 3.5 (applied to } C \\ \text{instead of } H\text{), since } i > n\text{))}}} \\
&= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i}(x) + \underbrace{\sum_{\substack{i \geq 1; \\ i > n}} \frac{(-1)^{i-1}}{i} 0}_{=0} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i}(x). \qquad (198)
\end{aligned}$$

The same argument, applied to H and h instead of F and f, shows that

$$(\operatorname{Log} H)(x) = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} h^{*i}(x). \qquad (199)$$

But for every $i \in \mathbb{N}$ satisfying $i > n$, we have

$$(f + h + f * h)^{*i}(x) = 0 \qquad (200)$$

[115].

Finally, by the definition of Log, we have $\operatorname{Log}(F * H) = \operatorname{Log}_1 \underbrace{(F * H - e_{C,A})}_{\substack{=f+h+f*h \\ \text{(by (195))}}} =$

[115] *Proof of (200):* Let $i \in \mathbb{N}$ be such that $i > n$. Then, Remark 3.5 (applied to C instead of H) yields $(f + h + f * h)^{*i}(C_{\leq n}) = 0$ (since $f + h + f * h \in \mathfrak{g}(C, A)$ and $i > n$). Now,

$$(f + h + f * h)^{*i} \left(\underbrace{x}_{\in C_{\leq n}} \right) \in (f + h + f * h)^{*i}(C_{\leq n}) = 0,$$

so that $(f + h + f * h)^{*i}(x) = 0$. This proves (200).

$\mathrm{Log}_1(f+h+f*h)$. Thus,

$$\begin{aligned}
&(\mathrm{Log}(F*H))(x)\\
&=(f+h+f*h)(x)\\
&=\sum_{i\geq 1}\frac{(-1)^{i-1}}{i}(f+h+f*h)^{*i}(x) \qquad \text{(by the definition of } \mathrm{Log}_1\text{)}\\
&=\underbrace{\sum_{\substack{i\geq 1;\\ i\leq n}}}_{=\sum_{i=1}^{n}}\frac{(-1)^{i-1}}{i}(f+h+f*h)^{*i}(x)+\sum_{\substack{i\geq 1;\\ i>n}}\frac{(-1)^{i-1}}{i}\underbrace{(f+h+f*h)^{*i}(x)}_{\substack{=0\\ \text{(by (200))}}}\\
&=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}(f+h+f*h)^{*i}(x)+\underbrace{\sum_{\substack{i\geq 1;\\ i>n}}\frac{(-1)^{i-1}}{i}0}_{=0}\\
&=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}(f+h+f*h)^{*i}(x). \qquad (201)
\end{aligned}$$

Now,

$$\begin{aligned}
&(\mathrm{Log}\,F+\mathrm{Log}\,H-\mathrm{Log}(F*H))(x)\\
&=\underbrace{(\mathrm{Log}\,F)(x)}_{\substack{=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}f^{*i}(x)\\ \text{(by (198))}}}+\underbrace{(\mathrm{Log}\,H)(x)}_{\substack{=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}h^{*i}(x)\\ \text{(by (199))}}}-\underbrace{(\mathrm{Log}(F*H))(x)}_{\substack{=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}(f+h+f*h)^{*i}(x)\\ \text{(by (201))}}}\\
&=\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}f^{*i}(x)+\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}h^{*i}(x)-\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}(f+h+f*h)^{*i}(x)\\
&=\left(\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}f^{*i}+\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}h^{*i}-\sum_{i=1}^{n}\frac{(-1)^{i-1}}{i}(f+h+f*h)^{*i}\right)(x)=0
\end{aligned}$$

(by (197)).

Now forget that we fixed x. We thus have shown that every $x\in C$ satisfies $(\mathrm{Log}\,F+\mathrm{Log}\,H-\mathrm{Log}(F*H))(x)=0$. In other words, $\mathrm{Log}\,F+\mathrm{Log}\,H-\mathrm{Log}(F*H)=0$. Thus, $\mathrm{Log}\,F+\mathrm{Log}\,H=\mathrm{Log}(F*H)$. This completes the proof of **b)**.

The proof of Theorem 21.1 is thus complete. □

§22. Logarithms of tensor products

In this Section §22, we will apply Theorem 21.1 to compute the logarithm of the *tensor* product of two maps (using the logarithms of these maps). First, to make sure that we can talk about the logarithm of a tensor product, we need a proposition:

Proposition 22.1. Let k be a field. Let C and D be two filtered k-coalgebras. For every $\ell \in \mathbb{N}$, define a subspace $(C \otimes D)_{\leq \ell}$ of $C \otimes D$ by

$$(C \otimes D)_{\leq \ell} = \sum_{\substack{(a,b) \in \mathbb{N}^{\times 2}; \\ a+b=\ell}} C_{\leq a} \otimes D_{\leq b}.$$

(a) Then, $\left(C \otimes D, \left((C \otimes D)_{\leq \ell}\right)_{\ell \geq 0}\right)$ is a filtered k-coalgebra.

We are going to denote this filtered k-coalgebra $\left(C \otimes D, \left((C \otimes D)_{\leq \ell}\right)_{\ell \geq 0}\right)$ by $C \otimes D$. Thus, when we speak of "the filtered k-coalgebra $C \otimes D$", we actually mean the filtered k-coalgebra $\left(C \otimes D, \left((C \otimes D)_{\leq \ell}\right)_{\ell \geq 0}\right)$.

(b) If the filtered k-coalgebras C and D are connected, then the filtered k-coalgebra $C \otimes D$ is connected, too.

(c) Assume that the filtered k-coalgebras C and D are connected. Then, all three filtered k-coalgebras C, D and $C \otimes D$ are connected[116], and hence induce unital coalgebras C, D and $C \otimes D$ according to Definition 2.7. These unital coalgebras satisfy $1_{C \otimes D} = 1_C \otimes 1_D$.

A boring linear-algebraic lemma ahead:

Lemma 22.2. Let k be a field.

(a) Let U and V be two k-vector spaces. Let a be a nonnegative integer. Let U_c be a subspace of U for every $c \in \{0, 1, \ldots, a\}$. Then,

$$\left(\sum_{c=0}^{a} U_c\right) \otimes V = \sum_{c=0}^{a} U_c \otimes V, \tag{202}$$

where both sides $\left(\sum_{c=0}^{a} U_c\right) \otimes V$ and $\sum_{c=0}^{a} U_c \otimes V$ of this equality are to be understood as subspaces of $U \otimes V$.

(b) Let U and V be two k-vector spaces. Let b be a nonnegative integer. Let V_d be a subspace of V for every $d \in \{0, 1, \ldots, b\}$. Then,

$$U \otimes \left(\sum_{d=0}^{b} V_d\right) = \sum_{d=0}^{b} U \otimes V_d, \tag{203}$$

where both sides $U \otimes \left(\sum_{d=0}^{b} V_d\right)$ and $\sum_{d=0}^{b} U \otimes V_d$ of this equality are to be understood as subspaces of $U \otimes V$.

(c) Let U and V be two k-vector spaces. Let a and b be two nonnegative integers. Let U_c be a subspace of U for every $c \in \{0, 1, \ldots, a\}$. Let V_d be a subspace of V for every $d \in \{0, 1, \ldots, b\}$. Then,

$$\left(\sum_{c=0}^{a} U_c\right) \otimes \left(\sum_{d=0}^{b} V_d\right) = \sum_{c=0}^{a} \sum_{d=0}^{b} U_c \otimes V_d, \tag{204}$$

[116] *Proof.* For C and D, this is clear. For $C \otimes D$, this follows from Proposition 22.1 **(b)**.

where both sides $\left(\sum_{c=0}^{a} U_c\right) \otimes \left(\sum_{d=0}^{b} V_d\right)$ and $\sum_{c=0}^{a} \sum_{d=0}^{b} U_c \otimes V_d$ of this equality are to be understood as subspaces of $U \otimes V$.

Proof of Lemma 22.2. **(a)** First, let us introduce some conventions:

- Whenever T is a k-vector space, W_c is a k-vector space for every $c \in \{0, 1, \ldots, a\}$, and f_c is a k-linear map $W_c \to T$ for every $c \in \{0, 1, \ldots, a\}$, we are going to denote by $\sum_{c=0}^{a} f_c$ the canonical k-linear map $\bigoplus_{c=0}^{a} W_c \to T$ induced by the family $(f_c)_{c \in \{0,1,\ldots,a\}}$ of maps by the universal property of the direct sum. This map $\sum_{c=0}^{a} f_c$ sends every $(w_0, w_1, \ldots, w_a) \in \bigoplus_{c=0}^{a} W_c$ to $f_0(w_0) + f_1(w_1) + \cdots + f_a(w_a) \in T$.
- Whenever T is a k-vector space and U is a subspace of T, we denote by $\mathrm{inc}_{U,T}$ the inclusion map $U \to T$.

It is clear that, whenever T is a k-vector space and T_c is a subspace of T for every $c \in \{0, 1, \ldots, a\}$, then

$$\left(\sum_{c=0}^{a} \mathrm{inc}_{T_c,T}\right)\left(\bigoplus_{c=0}^{a} T_c\right) = \sum_{c=0}^{a} T_c \tag{205}$$

where the $\bigoplus_{c=0}^{a} T_c$ on the left hand side denotes an **external** direct sum.[117]

Now let us actually prove Lemma 22.2 **(a)**. In the following, let id denote the identity map id_V. For every $c \in \{0, 1, \ldots, a\}$, let i_c denote the canonical inclusion map $\mathrm{inc}_{U_c,U} : U_c \to U$.

[117] *Proof of (205):* Let T be a k-vector space. Let T_c be a k-vector subspace of T for every $c \in \{0, 1, \ldots, a\}$. We have

$$\begin{aligned}
&\left(\sum_{c=0}^{a} \mathrm{inc}_{T_c,T}\right)\left(\bigoplus_{c=0}^{a} T_c\right) \\
&= \left\{\left(\sum_{c=0}^{a} \mathrm{inc}_{T_c,T}\right)(w_0, w_1, \ldots, w_a) \;\mid\; (w_0, w_1, \ldots, w_a) \in \bigoplus_{c=0}^{a} T_c\right\}.
\end{aligned} \tag{206}$$

But every $(w_0, w_1, \ldots, w_a) \in \bigoplus_{c=0}^{a} T_c$ satisfies

$$\begin{aligned}
&\left(\sum_{c=0}^{a} \mathrm{inc}_{T_c,T}\right)(w_0, w_1, \ldots, w_a) \\
&= \mathrm{inc}_{T_0,T}(w_0) + \mathrm{inc}_{T_1,T}(w_1) + \cdots + \mathrm{inc}_{T_a,T}(w_a) \qquad \left(\text{by the definition of } \sum_{c=0}^{a} \mathrm{inc}_{T_c,T}\right) \\
&= \sum_{c=0}^{a} \underbrace{\left(\mathrm{inc}_{T_c,T}(w_c)\right)}_{\substack{=w_c \\ (\text{since } \mathrm{inc}_{T_c,T} \text{ is an inclusion map})}} = \sum_{c=0}^{a} w_c.
\end{aligned}$$

For every $c \in \{0, 1, \ldots, a\}$, we are identifying $U_c \otimes V$ with a subspace of $U \otimes V$. We are doing this identification by means of the map $\underbrace{\operatorname{inc}_{U_c,U}}_{=i_c} \otimes \underbrace{\operatorname{inc}_{V,V}}_{=\mathrm{id}} = i_c \otimes \mathrm{id}$. Hence, for every $c \in \{0, 1, \ldots, a\}$, we consider $i_c \otimes \mathrm{id}$ to be the canonical inclusion map $U_c \otimes V \to U \otimes V$. Thus, for every $c \in \{0, 1, \ldots, a\}$, we have

$$i_c \otimes \mathrm{id} = (\text{the canonical inclusion map } U_c \otimes V \to U \otimes V) = \operatorname{inc}_{U_c \otimes V, U \otimes V}.$$

Hence, (206) becomes

$$\begin{aligned}
&\left(\sum_{c=0}^{a} \operatorname{inc}_{T_c,T}\right)\left(\bigoplus_{c=0}^{a} T_c\right) \\
&= \left\{ \underbrace{\left(\sum_{c=0}^{a} \operatorname{inc}_{T_c,T}\right)(w_0, w_1, \ldots, w_a)}_{=\sum_{c=0}^{a} w_c} \;\mid\; (w_0, w_1, \ldots, w_a) \in \bigoplus_{c=0}^{a} T_c \right\} \\
&= \left\{ \sum_{c=0}^{a} w_c \;\mid\; \underbrace{(w_0, w_1, \ldots, w_a) \in \bigoplus_{c=0}^{a} T_c}_{\text{this is equivalent to}} \right. \\
&\qquad \left. \left(\begin{array}{c} (w_0, w_1, \ldots, w_a) \in \prod_{c=0}^{a} T_c, \text{ and} \\ \text{all but finitely many } i \in \{0, 1, \ldots, a\} \text{ satisfy } w_i = 0 \end{array} \right) \right\} \\
&\qquad \begin{array}{c} \left(\text{since } \bigoplus_{c=0}^{a} T_c \text{ is the set of all } (u_0, u_1, \ldots, u_a) \in \prod_{c=0}^{a} T_c \text{ such that} \right. \\ \left. \text{all but finitely many } i \in \{0,1,\ldots,a\} \text{ satisfy } u_i = 0 \right) \end{array} \\
&= \left\{ \sum_{c=0}^{a} w_c \;\mid\; \left(\begin{array}{c} (w_0, w_1, \ldots, w_a) \in \prod_{c=0}^{a} T_c, \text{ and} \\ \text{all but finitely many } i \in \{0, 1, \ldots, a\} \text{ satisfy } w_i = 0 \end{array} \right) \right\}.
\end{aligned}$$

Compared with

$$\sum_{c=0}^{a} T_c = \left\{ \sum_{c=0}^{a} w_c \;\mid\; \left(\begin{array}{c} (w_0, w_1, \ldots, w_a) \in \prod_{c=0}^{a} T_c, \text{ and} \\ \text{all but finitely many } i \in \{0, 1, \ldots, a\} \text{ satisfy } w_i = 0 \end{array} \right) \right\}$$

(by the definition of $\sum_{c=0}^{a} T_c$), this yields $\left(\sum_{c=0}^{a} \operatorname{inc}_{T_c,T}\right)\left(\bigoplus_{c=0}^{a} T_c\right) = \sum_{c=0}^{a} T_c$. This proves (205).

Hence,

$$\left(\sum_{c=0}^{a} \underbrace{(i_c \otimes \mathrm{id})}_{=\mathrm{inc}_{U_c \otimes V, U \otimes V}}\right)\left(\bigoplus_{c=0}^{a}(U_c \otimes V)\right) = \left(\sum_{c=0}^{a} \mathrm{inc}_{U_c \otimes V, U \otimes V}\right)\left(\bigoplus_{c=0}^{a}(U_c \otimes V)\right)$$
$$= \sum_{c=0}^{a} U_c \otimes V$$

(by (205), applied to $T = U \otimes V$ and $T_c = U_c \otimes V$).

On the other hand, the map $\sum_{c=0}^{a} i_c : \bigoplus_{c=0}^{a} U_c \to U$ satisfies

$$\left(\sum_{c=0}^{a} \underbrace{i_c}_{=\mathrm{inc}_{U_c, U}}\right)\left(\bigoplus_{c=0}^{a} U_c\right) = \left(\sum_{c=0}^{a} \mathrm{inc}_{U_c, U}\right)\left(\bigoplus_{c=0}^{a} U_c\right) = \sum_{c=0}^{a} U_c$$

(by (205), applied to $T = U$ and $T_c = U_c$).

Since the tensor product is known to commute with direct sums, there is a canonical k-vector space isomorphism $\left(\bigoplus_{c=0}^{a} U_c\right) \otimes V \to \bigoplus_{c=0}^{a}(U_c \otimes V)$. Denote this isomorphism by I. By the universal property of I, we know that whenever W is a k-vector space, and f_c is a k-vector space homomorphism $U_c \to W$ for every $c \in \{0, 1, \ldots, a\}$, the diagram

$$\begin{array}{ccc} \left(\bigoplus_{c=0}^{a} U_c\right) \otimes V & \xrightarrow{I} & \bigoplus_{c=0}^{a}(U_c \otimes V) \\ & \searrow^{\left(\sum_{c=0}^{a} f_c\right) \otimes \mathrm{id}} & \downarrow{\scriptstyle \sum_{c=0}^{a}(f_c \otimes \mathrm{id})} \\ & & W \otimes V \end{array}$$

commutes (where id denotes the identity map id_V). Applying this to $W = U$ and $f_c = i_c$, we obtain the following result: The diagram

$$\begin{array}{ccc} \left(\bigoplus_{c=0}^{a} U_c\right) \otimes V & \xrightarrow{I} & \bigoplus_{c=0}^{a}(U_c \otimes V) \\ & \searrow^{\left(\sum_{c=0}^{a} i_c\right) \otimes \mathrm{id}} & \downarrow{\scriptstyle \sum_{c=0}^{a}(i_c \otimes \mathrm{id})} \\ & & U \otimes V \end{array}$$

commutes (where id denotes the identity map id_V). In other words,

$$\left(\sum_{c=0}^{a} i_c\right) \otimes \mathrm{id} = \left(\sum_{c=0}^{a}(i_c \otimes \mathrm{id})\right) \circ I.$$

Thus,

$$\begin{aligned}
&\left(\left(\sum_{c=0}^{a} i_c\right) \otimes \mathrm{id}\right)\left(\left(\bigoplus_{c=0}^{a} U_c\right) \otimes V\right) \\
&= \left(\left(\sum_{c=0}^{a} (i_c \otimes \mathrm{id})\right) \circ I\right)\left(\left(\bigoplus_{c=0}^{a} U_c\right) \otimes V\right) \\
&= \left(\sum_{c=0}^{a} (i_c \otimes \mathrm{id})\right) \underbrace{\left(I\left(\left(\bigoplus_{c=0}^{a} U_c\right) \otimes V\right)\right)}_{\substack{=\bigoplus_{c=0}^{a} (U_c \otimes V) \\ \text{(since } I \text{ is an isomorphism)}}} \\
&= \left(\sum_{c=0}^{a} (i_c \otimes \mathrm{id})\right)\left(\bigoplus_{c=0}^{a} (U_c \otimes V)\right) = \sum_{c=0}^{a} U_c \otimes V.
\end{aligned}$$

Compared with

$$\begin{aligned}
\left(\left(\sum_{c=0}^{a} i_c\right) \otimes \mathrm{id}\right)\left(\left(\bigoplus_{c=0}^{a} U_c\right) \otimes V\right) &= \underbrace{\left(\left(\sum_{c=0}^{a} i_c\right)\left(\bigoplus_{c=0}^{a} U_c\right)\right)}_{=\sum_{c=0}^{a} U_c} \otimes \underbrace{\mathrm{id}\,(V)}_{=V} \\
&= \left(\sum_{c=0}^{a} U_c\right) \otimes V,
\end{aligned}$$

this yields $\left(\sum_{c=0}^{a} U_c\right) \otimes V = \sum_{c=0}^{a} U_c \otimes V$. This proves Lemma 22.2 **(a)**.

(b) The proof of Lemma 22.2 **(b)** proceeds by the same arguments as the proof of Lemma 22.2 **(a)** that we gave above (the only real difference is that this time, the sum stands in the second tensorand rather than in the first one).

(c) We have

$$\begin{aligned}
\left(\sum_{c=0}^{a} U_c\right) \otimes \left(\sum_{d=0}^{b} V_d\right) &= \sum_{c=0}^{a} \left(\underbrace{U_c \otimes \left(\sum_{d=0}^{b} V_d\right)}_{\substack{=\sum_{d=0}^{b} U_c \otimes V_d \\ \text{(by Lemma 22.2 (b), applied to } U_c \text{ instead of } U)}} \right) \\
&\qquad \left(\text{by Lemma 22.2 (a), applied to } \sum_{d=0}^{b} V_d \text{ instead of } V\right) \\
&= \sum_{c=0}^{a} \sum_{d=0}^{b} U_c \otimes V_d.
\end{aligned}$$

This proves Lemma 22.2 **(c)**. □

One more linear-algebraic triviality will be useful:

Lemma 22.3. Let k be a field. Let V and W be two k-vector spaces. Let V' be a vector subspace of V. Let W' be a vector subspace of W. Then, $\tau_{V,W}\left(V' \otimes W'\right) = W' \otimes V'$, where $\tau_{V,W}$ is the (V,W)-flip defined in Definition 9.2.

Proof of Lemma 22.3. Since a tensor product of k-vector spaces is always generated by pure tensors, we have

$$V' \otimes W' = \langle v \otimes w \ \mid \ (v,w) \in V' \times W' \rangle = \langle \{ v \otimes w \ \mid \ (v,w) \in V' \times W' \} \rangle .$$

Hence,

$$\begin{aligned}
\tau_{V,W}\left(V' \otimes W'\right) &= \tau_{V,W}\left(\langle \{ v \otimes w \ \mid \ (v,w) \in V' \times W' \} \rangle\right) \\
&= \left\langle \underbrace{\tau_{V,W}\left(\{ v \otimes w \ \mid \ (v,w) \in V' \times W' \}\right)}_{= \left\{ \tau_{V,W}(v \otimes w) \ \mid \ (v,w) \in V' \times W' \right\}} \right\rangle \qquad \text{(by (165))} \\
&= \left\langle \left\{ \underbrace{\tau_{V,W}\left(v \otimes w\right)}_{\substack{= w \otimes v \\ \text{(by the definition of } \tau_{V,W}\text{)}}} \ \mid \ (v,w) \in V' \times W' \right\} \right\rangle \\
&= \langle \{ w \otimes v \ \mid \ (v,w) \in V' \times W' \} \rangle = \langle w \otimes v \ \mid \ (v,w) \in V' \times W' \rangle \\
&= \langle x \otimes y \ \mid \ (x,y) \in W' \times V' \rangle \\
&\qquad \left(\begin{array}{c} \text{here, we substituted } (w,v) \text{ by } (x,y), \\ \text{since the map } V' \times W' \to W' \times V',\ (v,w) \mapsto (w,v) \text{ is a bijection} \end{array} \right).
\end{aligned}$$

Compared with

$$W' \otimes V' = \langle x \otimes y \ \mid \ (x,y) \in W' \times V' \rangle$$
$$\text{(since a tensor product is always generated by pure tensors)},$$

this yields $\tau_{V,W}\left(V' \otimes W'\right) = W' \otimes V'$. This proves Lemma 22.3. □

Proof of Proposition 22.1. **(a)** For every $a \in \mathbb{N}$, we have $\Delta_C\left(C_{\leq a}\right) \subseteq \sum_{c=0}^{a} C_{\leq c} \otimes C_{\leq a-c}$ (since C is a filtered k-coalgebra). For every $b \in \mathbb{N}$, we have $\Delta_D\left(D_{\leq b}\right) \subseteq \sum_{d=0}^{b} D_{\leq d} \otimes D_{\leq b-d}$ (since D is a filtered k-coalgebra).

We notice that

$$C_{\leq \alpha} \otimes D_{\leq \beta} \subseteq (C \otimes D)_{\leq \alpha+\beta} \qquad \text{for any } (\alpha,\beta) \in \mathbb{N}^{\times 2}. \tag{207}$$

118

[118] *Proof of (207).* Let $(\alpha,\beta) \in \mathbb{N}^{\times 2}$. Then, this pair $(\alpha,\beta) \in \mathbb{N}^{\times 2}$ satisfies $\alpha+\beta = \alpha+\beta$. Hence, $C_{\leq \alpha} \otimes D_{\leq \beta}$ is an addend of the sum $\sum_{\substack{(a,b) \in \mathbb{N}^{\times 2}; \\ a+b=\alpha+\beta}} C_{\leq a} \otimes D_{\leq b}$ (namely, the addend for $(a,b) = (\alpha,\beta)$).

Now, let $\ell \in \mathbb{N}$.

Let $\tau_{C,D} : C \otimes D \to D \otimes C$ be the (C, D)-flip, defined as in Definition 9.2. Then, by the definition of the k-coalgebra $C \otimes D$, we have $\Delta_{C\otimes D} = (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D)$. Hence,

$$\begin{aligned}
\Delta_{C\otimes D}\left((C\otimes D)_{\leq \ell}\right) &= \left((\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D) \circ (\Delta_C \otimes \Delta_D)\right)\left((C\otimes D)_{\leq \ell}\right) \\
&= (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D)\left((\Delta_C \otimes \Delta_D)\underbrace{\left((C\otimes D)_{\leq \ell}\right)}_{= \sum\limits_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} C_{\leq a}\otimes D_{\leq b}}\right) \\
&= (\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D)\left((\Delta_C \otimes \Delta_D)\left(\sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} C_{\leq a}\otimes D_{\leq b}\right)\right).
\end{aligned}$$

Thus, $C_{\leq \alpha}\otimes D_{\leq \beta} \subseteq \sum\limits_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\alpha+\beta}} C_{\leq a}\otimes D_{\leq b}$. Since $(C\otimes D)_{\leq \alpha+\beta} = \sum\limits_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\alpha+\beta}} C_{\leq a}\otimes D_{\leq b}$ (by the definition of $(C\otimes D)_{\leq \alpha+\beta}$), we thus have

$$C_{\leq \alpha}\otimes D_{\leq \beta} \subseteq \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\alpha+\beta}} C_{\leq a}\otimes D_{\leq b} = (C\otimes D)_{\leq \alpha+\beta}.$$

This proves (207).

But since

$$
\begin{aligned}
&(\Delta_C \otimes \Delta_D)\left(\sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} C_{\leq a}\otimes D_{\leq b}\right)\\
&= \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} \underbrace{(\Delta_C\otimes\Delta_D)\left(C_{\leq a}\otimes D_{\leq b}\right)}_{\subseteq\left(\Delta_C\left(C_{\leq a}\right)\right)\otimes\left(\Delta_D\left(D_{\leq b}\right)\right)} \qquad \text{(since } \Delta_C\otimes\Delta_D \text{ is } k\text{-linear)}\\
&\subseteq \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} \underbrace{\left(\Delta_C\left(C_{\leq a}\right)\right)}_{\subseteq\sum_{c=0}^{a} C_{\leq c}\otimes C_{\leq a-c}} \otimes \underbrace{\left(\Delta_D\left(D_{\leq b}\right)\right)}_{\subseteq\sum_{d=0}^{b} D_{\leq d}\otimes D_{\leq b-d}}\\
&\subseteq \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} \underbrace{\left(\sum_{c=0}^{a} C_{\leq c}\otimes C_{\leq a-c}\right)\otimes\left(\sum_{d=0}^{b} D_{\leq d}\otimes D_{\leq b-d}\right)}_{=\sum_{c=0}^{a}\sum_{d=0}^{b}\left(C_{\leq c}\otimes C_{\leq a-c}\right)\otimes\left(D_{\leq d}\otimes D_{\leq b-d}\right)}\\
&\qquad \text{(by Lemma 22.2 } \textbf{(c)}\text{, applied to } U=C\otimes C,\ V=D\otimes D,\\
&\qquad U_c=C_{\leq c}\otimes C_{\leq a-c} \text{ and } V_d=D_{\leq d}\otimes D_{\leq b-d})\\
&= \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} \sum_{c=0}^{a}\sum_{d=0}^{b} \underbrace{\left(C_{\leq c}\otimes C_{\leq a-c}\right)\otimes\left(D_{\leq d}\otimes D_{\leq b-d}\right)}_{=C_{\leq c}\otimes C_{\leq a-c}\otimes D_{\leq d}\otimes D_{\leq b-d}}\\
&= \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} \sum_{c=0}^{a}\sum_{d=0}^{b} C_{\leq c}\otimes C_{\leq a-c}\otimes D_{\leq d}\otimes D_{\leq b-d},
\end{aligned}
$$

this becomes

$$
\begin{aligned}
&\Delta_{C\otimes D}\left((C\otimes D)_{\leq \ell}\right) \\
&\subseteq \left(\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D\right) \left(\underbrace{\left(\Delta_C \otimes \Delta_D\right)\left(\sum_{\substack{(a,b)\in\mathbb{N}^{\times 2}; \\ a+b=\ell}} C_{\leq a} \otimes D_{\leq b} \right)}_{\subseteq \sum\limits_{\substack{(a,b)\in\mathbb{N}^{\times 2}; \\ a+b=\ell}} \sum\limits_{c=0}^{a} \sum\limits_{d=0}^{b} C_{\leq c}\otimes C_{\leq a-c}\otimes D_{\leq d}\otimes D_{\leq b-d}} \right) \\
&\subseteq \left(\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D\right) \left(\sum_{\substack{(a,b)\in\mathbb{N}^{\times 2}; \\ a+b=\ell}} \sum_{c=0}^{a} \sum_{d=0}^{b} C_{\leq c} \otimes C_{\leq a-c} \otimes D_{\leq d} \otimes D_{\leq b-d} \right) \\
&= \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2}; \\ a+b=\ell}} \sum_{c=0}^{a} \sum_{d=0}^{b} \underbrace{\left(\mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D\right)\left(C_{\leq c} \otimes C_{\leq a-c} \otimes D_{\leq d} \otimes D_{\leq b-d}\right)}_{=\mathrm{id}_C\left(C_{\leq c}\right)\otimes \tau_{C,D}\left(C_{\leq a-c}\otimes D_{\leq d}\right)\otimes \mathrm{id}_D\left(D_{\leq b-d}\right)} \\
&\qquad \left(\text{since } \mathrm{id}_C \otimes \tau_{C,D} \otimes \mathrm{id}_D \text{ is } k\text{-linear}\right) \\
&= \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2}; \\ a+b=\ell}} \sum_{c=0}^{a} \sum_{d=0}^{b} \underbrace{\mathrm{id}_C\left(C_{\leq c}\right)}_{=C_{\leq c}} \otimes \underbrace{\tau_{C,D}\left(C_{\leq a-c} \otimes D_{\leq d}\right)}_{\substack{=D_{\leq d}\otimes C_{\leq a-c} \\ \text{(by Lemma 22.3, applied to} \\ V=C,\ W=D,\ V'=C_{\leq a-c} \text{ and } W'=D_{\leq d})}} \otimes \underbrace{\mathrm{id}_D\left(D_{\leq b-d}\right)}_{=D_{\leq b-d}} \\
&= \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2}; \\ a+b=\ell}} \sum_{c=0}^{a} \sum_{d=0}^{b} C_{\leq c} \otimes D_{\leq d} \otimes C_{\leq a-c} \otimes D_{\leq b-d}. \qquad (208)
\end{aligned}
$$

But we can easily see that

$$
\left(\begin{array}{c} \text{for every } (a,b) \in \mathbb{N}^{\times 2} \text{ satisfying } a+b=\ell, \text{ for every} \\ c \in \{0,1,\ldots,a\} \text{ and for every } d \in \{0,1,\ldots,b\}, \text{ we have} \\ C_{\leq c} \otimes D_{\leq d} \otimes C_{\leq a-c} \otimes D_{\leq b-d} \subseteq \sum\limits_{m=0}^{\ell} (C\otimes D)_{\leq m} \otimes (C\otimes D)_{\leq \ell-m} \end{array} \right). \qquad (209)
$$

[119] Hence, (208) becomes

$$\Delta_{C\otimes D}\left((C\otimes D)_{\leq \ell}\right) \subseteq \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} \sum_{c=0}^{a}\sum_{d=0}^{b} \underbrace{C_{\leq c}\otimes D_{\leq d}\otimes C_{\leq a-c}\otimes D_{\leq b-d}}_{\substack{\subseteq \sum_{m=0}^{\ell}(C\otimes D)_{\leq m}\otimes(C\otimes D)_{\leq \ell-m} \\ \text{(by (209) (since } (a,b)\in\mathbb{N}^{\times 2},\ a+b=\ell, \\ c\in\{0,1,\ldots,a\} \text{ and } d\in\{0,1,\ldots,b\}))}}$$

$$\subseteq \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=\ell}} \sum_{c=0}^{a}\sum_{d=0}^{b}\sum_{m=0}^{\ell} (C\otimes D)_{\leq m}\otimes (C\otimes D)_{\leq \ell-m}$$

$$\subseteq \sum_{m=0}^{\ell} (C\otimes D)_{\leq m}\otimes (C\otimes D)_{\leq \ell-m}$$

$$\left(\text{since } \sum_{m=0}^{\ell} (C\otimes D)_{\leq m}\otimes (C\otimes D)_{\leq \ell-m} \text{ is a } k\text{-vector space}\right).$$

Now forget that we fixed ℓ. We thus have proved that every $\ell \in \mathbb{N}$ satisfies $\Delta_{C\otimes D}\left((C\otimes D)_{\leq \ell}\right) \subseteq \sum_{m=0}^{\ell} (C\otimes D)_{\leq m}\otimes (C\otimes D)_{\leq \ell-m}$. In other words, $\left(C\otimes D, \left((C\otimes D)_{\leq \ell}\right)_{\ell\geq 0}\right)$ is a filtered k-coalgebra. This proves Proposition 22.1 **(a)**.

(b) Assume that the filtered k-coalgebras C and D are connected.

By the definition of $(C\otimes D)_{\leq 0}$, we have $(C\otimes D)_{\leq 0} = \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=0}} C_{\leq a}\otimes D_{\leq b}$. But the

[119] *Proof of (209).* Let $(a,b)\in\mathbb{N}^{\times 2}$ satisfy $a+b=\ell$. Let $c\in\{0,1,\ldots,a\}$ and $d\in\{0,1,\ldots,b\}$ be arbitrary. Then, $0\leq c\leq a$ (since $c\in\{0,1,\ldots,a\}$) and $0\leq d\leq b$ (since $d\in\{0,1,\ldots,b\}$). Hence, $\underbrace{c}_{\leq a}+\underbrace{d}_{\leq b}\leq a+b=\ell$ and $\underbrace{c}_{\geq 0}+\underbrace{d}_{\geq 0}\geq 0+0=0$. Thus, $c+d\in\{0,1,\ldots,\ell\}$. Hence, $(C\otimes D)_{\leq c+d}\otimes(C\otimes D)_{\leq \ell-(c+d)}$ is an addend of the sum $\sum_{m=0}^{\ell}(C\otimes D)_{\leq m}\otimes(C\otimes D)_{\leq \ell-m}$ (namely, the addend for $m=c+d$). Thus,

$$(C\otimes D)_{\leq c+d}\otimes(C\otimes D)_{\leq \ell-(c+d)} \subseteq \sum_{m=0}^{\ell}(C\otimes D)_{\leq m}\otimes(C\otimes D)_{\leq \ell-m}.$$

But now,

$$\underbrace{C_{\leq c}\otimes D_{\leq d}}_{\substack{\subseteq (C\otimes D)_{\leq c+d} \\ \text{(by (207), applied to } (\alpha,\beta)=(c,d))}} \otimes \underbrace{C_{\leq a-c}\otimes D_{\leq b-d}}_{\substack{\subseteq (C\otimes D)_{\leq (a-c)+(b-d)} \\ \text{(by (207), applied to } (\alpha,\beta)=(a-c,b-d))}}$$

$$\subseteq (C\otimes D)_{\leq c+d}\otimes(C\otimes D)_{\leq (a-c)+(b-d)} = (C\otimes D)_{\leq c+d}\otimes(C\otimes D)_{\leq \ell-(c+d)}$$

$$\left(\text{since } (a-c)+(b-d) = \underbrace{(a+b)}_{=\ell}-(c+d) = \ell-(c+d)\right)$$

$$\subseteq \sum_{m=0}^{\ell}(C\otimes D)_{\leq m}\otimes(C\otimes D)_{\leq \ell-m}.$$

This proves (209).

only pair $(a,b) \in \mathbb{N}^{\times 2}$ satisfying $a+b=0$ is $(0,0)$. Hence, the sum $\sum\limits_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=0}} C_{\leq a} \otimes D_{\leq b}$ has only one addend, namely $C_{\leq 0} \otimes D_{\leq 0}$. Thus, $\sum\limits_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=0}} C_{\leq a} \otimes D_{\leq b} = C_{\leq 0} \otimes D_{\leq 0}$, so we conclude that

$$(C \otimes D)_{\leq 0} = \sum_{\substack{(a,b)\in\mathbb{N}^{\times 2};\\ a+b=0}} C_{\leq a} \otimes D_{\leq b} = C_{\leq 0} \otimes D_{\leq 0}.$$

Since C is connected, the map $\varepsilon_C \mid_{C_{\leq 0}} : C_{\leq 0} \to k$ is a k-vector space isomorphism (by Definition 1.16). Similarly, the map $\varepsilon_D \mid_{D_{\leq 0}} : D_{\leq 0} \to k$ is a k-vector space isomorphism.

Since the maps $\varepsilon_C \mid_{C_{\leq 0}} : C_{\leq 0} \to k$ and $\varepsilon_D \mid_{D_{\leq 0}} : D_{\leq 0} \to k$ are k-vector space isomorphisms, their tensor product $\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)$ must also be a k-vector space isomorphism (since the tensor product of two k-vector space isomorphisms always is a k-vector space isomorphism).

Let μ_k be the canonical k-vector space isomorphism $k \otimes k \to k$. Now, we have $\mu_k \circ \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right) = \varepsilon_{C\otimes D} \mid_{C_{\leq 0}\otimes D_{\leq 0}}$ [120]. Hence,

$$\mu_k \circ \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right) = \varepsilon_{C\otimes D} \mid_{C_{\leq 0}\otimes D_{\leq 0}} = \varepsilon_{C\otimes D} \mid_{(C\otimes D)_{\leq 0}} \qquad \left(\text{since } C_{\leq 0} \otimes D_{\leq 0} = (C \otimes D)_{\leq 0}\right).$$

Since we know that $\mu_k \circ \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right)$ is a k-vector space isomorphism (because μ_k and $\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)$ are k-vector space isomorphisms, and because the composition of two k-vector space isomorphisms is always a k-vector space isomorphism), we can thus conclude that $\varepsilon_{C\otimes D} \mid_{(C\otimes D)_{\leq 0}}$ is a k-vector space isomorphism.

Now, by Definition 1.16 (applied to $C \otimes D$ instead of C), the filtered k-coalgebra $C \otimes D$ is connected if and only if the map $\varepsilon_{C\otimes D} \mid_{(C\otimes D)_{\leq 0}} : (C \otimes D)_{\leq 0} \to k$ is a k-vector space isomorphism. Since we already know that the map $\varepsilon_{C\otimes D} \mid_{(C\otimes D)_{\leq 0}}$ is a

[120] *Proof.* For every $(x,y) \in C_{\leq 0} \times D_{\leq 0}$, we have

$$\begin{aligned}
&\left(\mu_k \circ \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right)\right)(x \otimes y) \\
&= \mu_k \left(\underbrace{\left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right)(x \otimes y)}_{=\left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right)(x)\right) \otimes \left(\left(\varepsilon_D \mid_{D_{\leq 0}}\right)(y)\right)} \right) = \mu_k \left(\underbrace{\left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right)(x)\right)}_{=\varepsilon_C(x)} \otimes \underbrace{\left(\left(\varepsilon_D \mid_{D_{\leq 0}}\right)(y)\right)}_{=\varepsilon_D(y)} \right) \\
&= \mu_k \left(\underbrace{\left(\varepsilon_C(x)\right) \otimes \left(\varepsilon_D(y)\right)}_{=(\varepsilon_C \otimes \varepsilon_D)(x\otimes y)} \right) = \mu_k\left(\left(\varepsilon_C \otimes \varepsilon_D\right)(x \otimes y)\right) = \left(\mu_k \circ \left(\varepsilon_C \otimes \varepsilon_D\right)\right)(x \otimes y)
\end{aligned}$$

and

$$\left(\varepsilon_{C\otimes D} \mid_{C_{\leq 0}\otimes D_{\leq 0}}\right)(x \otimes y) = \varepsilon_{C\otimes D}(x \otimes y) = \left(\mu_k \circ \left(\varepsilon_C \otimes \varepsilon_D\right)\right)(x \otimes y)$$

(since, by the definition of the k-coalgebra $C \otimes D$, we have $\varepsilon_{C\otimes D} = \mu_k \circ (\varepsilon_C \otimes \varepsilon_D)$). Thus, for every $(x,y) \in C_{\leq 0} \times D_{\leq 0}$, we have

$$\left(\mu_k \circ \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right)\right)(x \otimes y) = \left(\mu_k \circ \left(\varepsilon_C \otimes \varepsilon_D\right)\right)(x \otimes y) = \left(\varepsilon_{C\otimes D} \mid_{C_{\leq 0}\otimes D_{\leq 0}}\right)(x \otimes y).$$

In other words, the two maps $\mu_k \circ \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right)$ and $\varepsilon_{C\otimes D} \mid_{C_{\leq 0}\otimes D_{\leq 0}}$ are equal to each other on each pure tensor in $C_{\leq 0} \otimes D_{\leq 0}$. Since these two maps are k-linear, this yields that these two maps must be identic (because any two k-linear maps from a tensor product which are equal to each other on each pure tensor must be identic). In other words, $\mu_k \circ \left(\left(\varepsilon_C \mid_{C_{\leq 0}}\right) \otimes \left(\varepsilon_D \mid_{D_{\leq 0}}\right)\right) = \varepsilon_{C\otimes D} \mid_{C_{\leq 0}\otimes D_{\leq 0}}$, qed.

k-vector space isomorphism, we can thus conclude that the filtered k-coalgebra $C \otimes D$ is connected. This proves Proposition 22.1 **(b)**.

(c) Assume that the filtered k-coalgebras C and D are connected.

Since 1_C is the unity of the unital coalgebra C, we see that $(C, 1_C)$ is a unital coalgebra, so that $\Delta_C(1_C) = 1_C \otimes 1_C$ and $\varepsilon_C(1_C) = 1$ (by the definition of a unital coalgebra). Similarly to $\varepsilon_C(1_C) = 1$, we can prove that $\varepsilon_D(1_D) = 1$.

Let μ_k be the canonical k-vector space isomorphism $k \otimes k \to k$. Now, by the definition of the k-coalgebra $C \otimes D$, we have $\varepsilon_{C \otimes D} = \mu_k \circ (\varepsilon_C \otimes \varepsilon_D)$, so that

$$\begin{aligned}
\varepsilon_{C\otimes D}(1_C \otimes 1_D) &= (\mu_k \circ (\varepsilon_C \otimes \varepsilon_D))(1_C \otimes 1_D) = \mu_k \left(\underbrace{(\varepsilon_C \otimes \varepsilon_D)(1_C \otimes 1_D)}_{=\varepsilon_C(1_C)\otimes\varepsilon_D(1_D)} \right) \\
&= \mu_k \left(\underbrace{\varepsilon_C(1_C)}_{=1} \otimes \underbrace{\varepsilon_D(1_D)}_{=1} \right) = \mu_k(1 \otimes 1) = 1 \cdot 1 \qquad \text{(by the definition of } \mu_k\text{)} \\
&= 1.
\end{aligned}$$

By Remark 2.10, we have $1_C = \left(\varepsilon_C|_{C_{\leq 0}}\right)^{-1}(1) \in C_{\leq 0}$. Similarly, $1_D \in D_{\leq 0}$. Thus, $\underbrace{1_C}_{\in C_{\leq 0}} \otimes \underbrace{1_D}_{\in D_{\leq 0}} \in C_{\leq 0} \otimes D_{\leq 0} = (C \otimes D)_{\leq 0}$ (by the above proof of Proposition 22.1 **(b)**). Hence, $\left(\varepsilon_{C\otimes D}|_{(C\otimes D)_{\leq 0}}\right)(1_C \otimes 1_D)$ is well-defined, and we have

$$\left(\varepsilon_{C\otimes D}|_{(C\otimes D)_{\leq 0}}\right)(1_C \otimes 1_D) = \varepsilon_{C\otimes D}(1_C \otimes 1_D) = 1.$$

Since the filtered k-coalgebra $C \otimes D$ is connected (by Proposition 22.1 **(b)**), the map $\varepsilon_{C\otimes D}|_{(C\otimes D)_{\leq 0}}$ is a k-vector space isomorphism (by the definition of "connected"). Thus, the identity $\left(\varepsilon_{C\otimes D}|_{(C\otimes D)_{\leq 0}}\right)(1_C \otimes 1_D) = 1$ (which was proven above) rewrites as $1_C \otimes 1_D = \left(\varepsilon_{C\otimes D}|_{(C\otimes D)_{\leq 0}}\right)^{-1}(1)$.

Now,

$$\begin{aligned}
1_{C\otimes D} &= \left(\varepsilon_{C\otimes D}|_{(C\otimes D)_{\leq 0}}\right)^{-1}(1) \qquad \text{(by Remark 2.10, applied to } C \otimes D \text{ instead of } C\text{)} \\
&= 1_C \otimes 1_D.
\end{aligned}$$

This proves Proposition 22.1 **(c)**. □

Now to the question of how the logarithm acts on tensor products:

Proposition 22.4. Let k be a field of characteristic 0. Let C and D be two connected filtered k-coalgebras. Let A and B be k-algebras. Let a map $e_{D,B} : D \to B$ be defined as in Definition 1.12. Recall that $C \otimes D$ is a k-coalgebra and $A \otimes B$ is a k-algebra; hence, $\mathcal{L}(C \otimes D, A \otimes B)$ becomes a k-algebra with respect to convolution. We notice that the filtered k-coalgebra $C \otimes D$ is connected (by Proposition 22.1 **(b)**), so that there is a well-defined notion of $\operatorname{Log} T$ for maps $T \in G(C \otimes D, A \otimes B)$.

(a) For any $F \in G(C, A)$, we have $F \otimes e_{D,B} \in G(C \otimes D, A \otimes B)$ and $\operatorname{Log}(F \otimes e_{D,B}) = (\operatorname{Log} F) \otimes e_{D,B}$.

(b) For any $H \in G(D, B)$, we have $e_{C,A} \otimes H \in G(C \otimes D, A \otimes B)$ and $\operatorname{Log}(e_{C,A} \otimes H) = e_{C,A} \otimes (\operatorname{Log} H)$.

(c) For any $F \in G(C, A)$ and $H \in G(D, B)$, we have $F \otimes H \in G(C \otimes D, A \otimes B)$ and $\operatorname{Log}(F \otimes H) = (\operatorname{Log} F) \otimes e_{D,B} + e_{C,A} \otimes (\operatorname{Log} H)$.

First, again, a harmless lemma:

Lemma 22.5. Let k be a field. Let C and D be two connected filtered k-coalgebras. Let A and B be two k-algebras. Let $F \in G(C, A)$ and $H \in G(D, B)$ be arbitrary. Then, $F \otimes H \in G(C \otimes D, A \otimes B)$. (Here, we are using the notation $G(C \otimes D, A \otimes B)$; this notation makes sense since $C \otimes D$ is a connected filtered k-coalgebra (by Proposition 22.1 **(b)**).)

Proof of Lemma 22.5. We have

$$F \in G(C, A) = \{f \in \mathcal{L}(C, A) \mid f(1_C) = 1_A\} \qquad \text{(by the definition of } G(C, A)),$$

so that $F(1_C) = 1_A$. Similarly, $H(1_D) = 1_B$. Now, $1_{C \otimes D} = 1_C \otimes 1_D$, and thus

$$(F \otimes H)(1_{C \otimes D}) = (F \otimes H)(1_C \otimes 1_D) = \underbrace{F(1_C)}_{=1_A} \otimes \underbrace{H(1_D)}_{=1_B} = 1_A \otimes 1_B = 1_{A \otimes B},$$

so that

$$F \otimes H \in \{f \in \mathcal{L}(C \otimes D, A \otimes B) \mid f(1_{C \otimes D}) = 1_{A \otimes B}\} = G(C \otimes D, A \otimes B)$$
$$\left(\begin{array}{c} \text{since } G(C \otimes D, A \otimes B) = \{f \in \mathcal{L}(C \otimes D, A \otimes B) \mid f(1_{C \otimes D}) = 1_{A \otimes B}\} \\ \text{by the definition of } G(C \otimes D, A \otimes B) \end{array} \right).$$

This proves Lemma 22.5. □

Proof of Proposition 22.4. **(a)** Let $F \in G(C, A)$. By Lemma 22.5 (applied to $H = e_{D,B}$), we obtain $F \otimes e_{D,B} \in G(C \otimes D, A \otimes B)$. In order to prove Proposition 22.4 **(a)**, it thus remains to show that $\operatorname{Log}(F \otimes e_{D,B}) = (\operatorname{Log} F) \otimes e_{D,B}$.

Let $f = F - e_{C,A}$. Then,

$$\underbrace{f}_{=F-e_{C,A}} \otimes e_{D,B} = (F - e_{C,A}) \otimes e_{D,B} = F \otimes e_{D,B} - \underbrace{e_{C,A} \otimes e_{D,B}}_{\substack{=e_{C \otimes D, A \otimes B} \\ \text{(by Corollary 9.11 (b))}}}$$
$$= F \otimes e_{D,B} - e_{C \otimes D, A \otimes B}. \tag{210}$$

Now let $(c, d) \in C \times D$. Then, $c \in C$ and $d \in D$.

By the definition of Log, we have $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{C,A})}_{=f} = \operatorname{Log}_1 f$, so that

$$(\operatorname{Log} F)(c) = (\operatorname{Log}_1 f)(c) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(c) \qquad \text{(by (8), applied to } C \text{ and } c \text{ instead of } H \text{ and } x).$$

Now,

$$\begin{aligned}
&((\operatorname{Log} F) \otimes e_{D,B})(c \otimes d) \\
&= \underbrace{(\operatorname{Log} F)(c)}_{=\sum_{i\geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(c)} \otimes e_{D,B}(d) \qquad \text{(by the definition of } (\operatorname{Log} F) \otimes e_{D,B}) \\
&= \left(\sum_{i\geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(c) \right) \otimes e_{D,B}(d) \\
&= \sum_{i\geq 1} \left(\frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(c) \otimes e_{D,B}(d)}_{=\left(f^{*i} \otimes e_{D,B}\right)(c\otimes d)} \right) \qquad \text{(since the tensor product is } k\text{-bilinear)} \\
&= \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} \left(f^{*i} \otimes e_{D,B}\right)(c \otimes d).
\end{aligned}$$

On the other hand, by the definition of Log, we have

$$\operatorname{Log}(F \otimes e_{D,B}) = \operatorname{Log}_1 \underbrace{(F \otimes e_{D,B} - e_{C\otimes D, A\otimes B})}_{\substack{=f\otimes e_{D,B} \\ \text{(by (210))}}} = \operatorname{Log}_1 (f \otimes e_{D,B}),$$

so that

$$\begin{aligned}
(\operatorname{Log}(F \otimes e_{D,B}))(c \otimes d) &= (\operatorname{Log}_1 (f \otimes e_{D,B}))(c \otimes d) = \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} \underbrace{(f \otimes e_{D,B})^{*i}}_{\substack{=f^{*i}\otimes e_{D,B} \\ \text{(by Corollary 9.11 (c))}}} (c \otimes d) \\
&\qquad \left(\begin{array}{c} \text{by (8), applied to } f \otimes e_{D,B},\ C \otimes D,\ A \otimes B \text{ and } c \otimes d \\ \text{instead of } f,\ H,\ A \text{ and } x \end{array} \right) \\
&= \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} \left(f^{*i} \otimes e_{D,B}\right)(c \otimes d).
\end{aligned}$$

Hence,

$$((\operatorname{Log} F) \otimes e_{D,B})(c \otimes d) = \sum_{i\geq 1} \frac{(-1)^{i-1}}{i} \left(f^{*i} \otimes e_{D,B}\right)(c \otimes d) = (\operatorname{Log}(F \otimes e_{D,B}))(c \otimes d).$$

Now forget that we fixed (c, d). We have proven that every $(c, d) \in C \times D$ satisfies $((\operatorname{Log} F) \otimes e_{D,B})(c \otimes d) = (\operatorname{Log}(F \otimes e_{D,B}))(c \otimes d)$. In other words, we have shown that the two maps $(\operatorname{Log} F) \otimes e_{D,B}$ and $\operatorname{Log}(F \otimes e_{D,B})$ are equal to each other on each pure tensor in $C \otimes D$. Since these two maps are k-linear, this yields that these two maps are identic (because if two k-linear maps from a tensor product are equal to each other on each pure tensor, then these two maps must be identic). In other words, $(\operatorname{Log} F) \otimes e_{D,B} = \operatorname{Log}(F \otimes e_{D,B})$. This proves Proposition 22.4 **(a)**.

(b) The proof of Proposition 22.4 **(b)** differs from the proof of Proposition 22.4 **(a)** only in the order of the tensorands, so there is no need to write down this proof here.

(c) Let $F \in G(C, A)$ and $H \in G(D, B)$. Lemma 22.5 yields $F \otimes H \in G(C \otimes D, A \otimes B)$. In order to prove Proposition 22.4 **(c)**, it thus remains only to prove that $\operatorname{Log}(F \otimes H) = (\operatorname{Log} F) \otimes e_{D,B} + e_{C,A} \otimes (\operatorname{Log} H)$.

Applying Corollary 9.10 to $f = F$ and $g = H$, we obtain

$$(F \otimes e_{D,B}) * (e_{C,A} \otimes H) = F \otimes H = (e_{C,A} \otimes H) * (F \otimes e_{D,B}).$$

In particular, this yields $(F \otimes e_{D,B}) * (e_{C,A} \otimes H) = (e_{C,A} \otimes H) * (F \otimes e_{D,B})$. Due to this equality, and also due to the facts that $F \otimes e_{D,B} \in G(C \otimes D, A \otimes B)$ (by Proposition 22.4 **(a)**) and $e_{C,A} \otimes H \in G(C \otimes D, A \otimes B)$ (by Proposition 22.4 **(b)**), we can apply Theorem 21.1 to $C \otimes D$, $A \otimes B$, $F \otimes e_{D,B}$ and $e_{C,A} \otimes H$ instead of C, A, F and H. This gives us $(F \otimes e_{D,B}) * (e_{C,A} \otimes H) \in G(C \otimes D, A \otimes B)$ and

$$\operatorname{Log}((F \otimes e_{D,B}) * (e_{C,A} \otimes H)) = \operatorname{Log}(F \otimes e_{D,B}) + \operatorname{Log}(e_{C,A} \otimes H).$$

Thus,

$$\begin{aligned}
\operatorname{Log}\left(\underbrace{F \otimes H}_{=(F \otimes e_{D,B}) * (e_{C,A} \otimes H)}\right) &= \operatorname{Log}((F \otimes e_{D,B}) * (e_{C,A} \otimes H)) \\
&= \underbrace{\operatorname{Log}(F \otimes e_{D,B})}_{\substack{=(\operatorname{Log} F) \otimes e_{D,B} \\ \text{(by Proposition 22.4 (a))}}} + \underbrace{\operatorname{Log}(e_{C,A} \otimes H)}_{\substack{=e_{C,A} \otimes (\operatorname{Log} H) \\ \text{(by Proposition 22.4 (b))}}} \\
&= (\operatorname{Log} F) \otimes e_{D,B} + e_{C,A} \otimes (\operatorname{Log} H).
\end{aligned}$$

This completes the proof of Proposition 22.4 **(c)**. □

§23. When graded bialgebras are Hopf

The following section (§23) is only tangentially related to the above. The only reason I am putting this section here is that it extends Proposition 16.18 **(c)** to the case of $n \in \mathbb{Z}$ for $*$-invertible f. More precisely, this section will (among other things) prove the following fact:

Proposition 23.1. Let k be a field. Let C be a graded k-coalgebra. Let A be a graded k-algebra. Let $f : C \to A$ be a graded $*$-invertible linear map (i. e., a graded linear map which has an inverse with respect to the operation $*$ in $\mathcal{L}(C, A)$).

(a) The map $f^{*(-1)}$ (that is, the inverse of f with respect to the operation $*$ in $\mathcal{L}(C, A)$) is graded.

(b) For every $n \in \mathbb{Z}$, the map f^{*n} is graded.

A consequence of this proposition is a curious property of graded bialgebras which are Hopf algebras:

Theorem 23.2. Let k be a field. Let H be a graded k-bialgebra. Assume that the k-bialgebra H is a Hopf algebra. Then, the antipode of the Hopf algebra H is a graded map.

Note that there is a notion of a "graded k-Hopf algebra". There are two possible ways to define this notion. One way is to define a graded k-Hopf algebra as a graded k-bialgebra whose underlying k-bialgebra (without grading) is a Hopf algebra. The other way is to define a graded k-Hopf algebra as a graded k-bialgebra whose underlying k-bialgebra (without grading) is a Hopf algebra with its antipode being a graded map. Theorem 23.2 shows that these two ways are equivalent.

Here is how to prove Theorem 23.2 using Proposition 23.1:

Proof of Theorem 23.2. Let S be the antipode of the Hopf algebra H. Then, S is the $*$-inverse of the identity map id_H (because the antipode of a Hopf algebra is defined as the $*$-inverse of its identity map). In other words, $S = \mathrm{id}_H^{*(-1)}$. As a consequence, the map id_H is $*$-invertible. Since the map id_H is also graded, we can thus apply Proposition 23.1 **(a)** to $f = \mathrm{id}_H$, and conclude that the map $\mathrm{id}_H^{*(-1)}$ is graded. Since $\mathrm{id}_H^{*(-1)} = S$ is the antipode of H, this rewrites as follows: The antipode of H is graded. This proves Theorem 23.2. $\square$

What remains to be done now is proving Proposition 23.1. For this, we will construct a way to assign to every map $f \in \mathcal{L}(C, A)$ a map $T_f \in \mathrm{End}(A \otimes C)$ in such a way that the convolution of maps in $\mathcal{L}(C, A)$ corresponds to the composition of maps in $\mathrm{End}(A \otimes C)$ (in reverse order). (In other words, we will make $A \otimes C$ into a representation of the k-algebra $(\mathcal{L}(C, A))^{\mathrm{op}}$.) This construction does not require C or A to be graded; it works in general.

Definition 23.3. Let k be a field. Let C be a k-coalgebra. Let A be a k-algebra. For every k-linear map $f : C \to A$, we define a k-linear map $T_f : A \otimes C \to A \otimes C$ by

$$T_f = (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C).$$

Proposition 23.4. Let k be a field. Let C be a k-coalgebra. Let A be a k-algebra.

(a) For any two k-linear maps $f : C \to A$ and $g : C \to A$, we have $T_{f+g} = T_f + T_g$.

(b) We have $T_0 = 0$.

(c) For any k-linear map $f : C \to A$ and any $\lambda \in k$, we have $T_{\lambda f} = \lambda T_f$.

(d) For any two k-linear maps $f : C \to A$ and $g : C \to A$, we have $T_{g*f} = T_f \circ T_g$.

(e) We have $T_{e_{C,A}} = \mathrm{id}_{A \otimes C}$.

(f) If C is a graded k-coalgebra, A is a graded k-algebra, and f is a graded map, then T_f also is a graded map.

(g) For any $*$-invertible k-linear map $f : C \to A$, the map T_f is invertible and satisfies $T_{f^{*(-1)}} = (T_f)^{-1}$.

(h) Let $\mathrm{kan}_{C,k\otimes C} : C \to k \otimes C$ be the canonical isomorphism which sends c to $1 \otimes c$ for every $c \in C$. Let $\mathrm{kan}_{A\otimes k,A} : A \otimes k \to A$ be the canonical

isomorphism which sends $a \otimes \lambda$ to λa for every $(a, \lambda) \in A \times k$. For any k-linear map $f : C \to A$, we have

$$\operatorname{kan}_{A\otimes k,A} \circ (\operatorname{id}_A \otimes \varepsilon_C) \circ T_f \circ (\eta_A \otimes \operatorname{id}_C) \circ \operatorname{kan}_{C,k\otimes C} = f.$$

(i) If C is a graded k-coalgebra, A is a graded k-algebra, and f is a k-linear map such that T_f is graded, then f is graded.

Proposition 23.4 is again an easy exercise to prove with the use of the Sweedler notation, but we are going to stay pure and prove it by manipulation of maps. First, let us make two general observations about vector spaces and tensor products:

- *Observation 1:*

$$\left(\begin{array}{c} \text{Any five } k\text{-vector spaces } P,\ Q,\ R_1,\ R_2,\ R_3 \text{ and any } k\text{-linear maps} \\ \varphi : R_1 \to R_2 \text{ and } \psi : R_2 \to R_3 \text{ satisfy} \\ (\operatorname{id}_P \otimes \psi \otimes \operatorname{id}_Q) \circ (\operatorname{id}_P \otimes \varphi \otimes \operatorname{id}_Q) = \operatorname{id}_P \otimes (\psi \circ \varphi) \otimes \operatorname{id}_Q \end{array} \right). \tag{211}$$

[121]

- *Observation 2:*

$$\left(\begin{array}{c} \text{Any four } k\text{-vector spaces } P,\ Q,\ R \text{ and } S \text{ and any two} \\ k\text{-linear maps } \gamma : P \to Q \text{ and } \delta : R \to S \text{ satisfy} \\ (\operatorname{id}_Q \otimes \delta) \circ (\gamma \otimes \operatorname{id}_R) = (\gamma \otimes \operatorname{id}_S) \circ (\operatorname{id}_P \otimes \delta) \end{array} \right). \tag{212}$$

[122]

---

[121] *Proof of (211).* Let P, Q, R_1, R_2, R_3 be five k-vector space, and let $\varphi : R_1 \to R_2$ and $\psi : R_2 \to R_3$ be two k-linear maps. By (21) (applied to $U = P$, $V = P$, $W = P$, $U' = R_1$, $V' = R_2$, $W' = R_3$, $\alpha = \operatorname{id}_P$, $\beta = \operatorname{id}_P$, $\alpha' = \varphi$ and $\beta' = \psi$), we have $(\operatorname{id}_P \circ \operatorname{id}_P) \otimes (\psi \circ \varphi) = (\operatorname{id}_P \otimes \psi) \circ (\operatorname{id}_P \otimes \varphi)$. By (21) (applied to $U = P \otimes R_1$, $V = P \otimes R_2$, $W = P \otimes R_3$, $U' = Q$, $V' = Q$, $W' = Q$, $\alpha = \operatorname{id}_P \otimes \varphi$, $\beta = \operatorname{id}_P \otimes \psi$, $\alpha' = \operatorname{id}_Q$ and $\beta' = \operatorname{id}_Q$), we have

$$((\operatorname{id}_P \otimes \psi) \circ (\operatorname{id}_P \otimes \varphi)) \otimes (\operatorname{id}_Q \circ \operatorname{id}_Q) = (\operatorname{id}_P \otimes \psi \otimes \operatorname{id}_Q) \circ (\operatorname{id}_P \otimes \varphi \otimes \operatorname{id}_Q).$$

Thus,

$$\begin{aligned} (\operatorname{id}_P \otimes \psi \otimes \operatorname{id}_Q) \circ (\operatorname{id}_P \otimes \varphi \otimes \operatorname{id}_Q) &= \underbrace{((\operatorname{id}_P \otimes \psi) \circ (\operatorname{id}_P \otimes \varphi))}_{=(\operatorname{id}_P \circ \operatorname{id}_P) \otimes (\psi \circ \varphi)} \otimes \underbrace{(\operatorname{id}_Q \circ \operatorname{id}_Q)}_{=\operatorname{id}_Q} \\ &= \underbrace{(\operatorname{id}_P \circ \operatorname{id}_P)}_{=\operatorname{id}_P} \otimes (\psi \circ \varphi) \otimes \operatorname{id}_Q = \operatorname{id}_P \otimes (\psi \circ \varphi) \otimes \operatorname{id}_Q . \end{aligned}$$

This proves (211).

[122] *Proof of (212).* Let P, Q, R and S be four k-vector spaces. Let $\gamma : P \to Q$ and $\delta : R \to S$ be two k-linear maps.

Applying (21) to $U = P$, $V = Q$, $W = Q$, $U' = R$, $V' = R$, $W' = S$, $\alpha = \gamma$, $\beta = \operatorname{id}_Q$, $\alpha' = \operatorname{id}_R$ and $\beta' = \delta$, we obtain $(\operatorname{id}_Q \circ \gamma) \otimes (\delta \circ \operatorname{id}_R) = (\operatorname{id}_Q \otimes \delta) \circ (\gamma \otimes \operatorname{id}_R)$, so that

$$(\operatorname{id}_Q \otimes \delta) \circ (\gamma \otimes \operatorname{id}_R) = \underbrace{(\operatorname{id}_Q \circ \gamma)}_{=\gamma} \otimes \underbrace{(\delta \circ \operatorname{id}_R)}_{=\delta} = \gamma \otimes \delta.$$

Applying (21) to $U = P$, $V = P$, $W = Q$, $U' = R$, $V' = S$, $W' = S$, $\alpha = \operatorname{id}_P$, $\beta = \gamma$, $\alpha' = \delta$ and

Proof of Proposition 23.4. **(a)** Let $f : C \to A$ and $g : C \to A$ be two k-linear maps. Since tensoring of k-linear maps is distributive, we have $(f+g)\otimes \mathrm{id}_C = f\otimes \mathrm{id}_C + g\otimes \mathrm{id}_C$, so that

$$\mathrm{id}_A \otimes (f+g) \otimes \mathrm{id}_C = \mathrm{id}_A \otimes (f \otimes \mathrm{id}_C + g \otimes \mathrm{id}_C) = \mathrm{id}_A \otimes f \otimes \mathrm{id}_C + \mathrm{id}_A \otimes g \otimes \mathrm{id}_C$$

(since tensoring of k-linear maps is distributive), so that

$$\begin{aligned}(\mathrm{id}_A \otimes (f+g) \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) &= (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C + \mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) + (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)\end{aligned}$$

(since composition of k-linear maps is distributive), so that

$$\begin{aligned}&(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes (f+g) \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= (\mu_A \otimes \mathrm{id}_C) \circ ((\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) + (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)) \\ &= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) + (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)\end{aligned}$$

(since composition of k-linear maps is distributive). Now, by the definition of T_{f+g}, we have

$$\begin{aligned}T_{f+g} &= (\mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes (f+g) \otimes \mathrm{id}_C)}_{\substack{=\mathrm{id}_A \otimes f \otimes \mathrm{id}_C + \mathrm{id}_A \otimes g \otimes \mathrm{id}_C \\ \text{(since the tensor product of } k\text{-linear maps is distributive)}}} \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C + \mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= \underbrace{(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)}_{\substack{=T_f \\ \text{(since } T_f \text{ was defined as } (\mu_A \otimes \mathrm{id}_C)\circ(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C)\circ(\mathrm{id}_A \otimes \Delta_C))}} \\ &\quad + \underbrace{(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)}_{\substack{=T_g \\ \text{(since } T_g \text{ was defined as } (\mu_A \otimes \mathrm{id}_C)\circ(\mathrm{id}_A \otimes g \otimes \mathrm{id}_C)\circ(\mathrm{id}_A \otimes \Delta_C))}} \\ &\qquad \text{(since the composition of } k\text{-linear maps is distributive)} \\ &= T_f + T_g.\end{aligned}$$

This proves Proposition 23.4 **(a)**.

(c) Let $f : C \to A$ be a k-linear map, and let $\lambda \in k$. Since tensoring of k-linear maps is k-bilinear, we have $(\lambda f) \otimes \mathrm{id}_C = \lambda\,(f \otimes \mathrm{id}_C)$ and $\mathrm{id}_A \otimes (\lambda\,(f \otimes \mathrm{id}_C)) = \lambda\,(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C)$. Thus,

$$\mathrm{id}_A \otimes \underbrace{(\lambda f) \otimes \mathrm{id}_C}_{=\lambda(f\otimes \mathrm{id}_C)} = \mathrm{id}_A \otimes (\lambda\,(f \otimes \mathrm{id}_C)) = \lambda\,(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C)\,.$$

Since composition of k-linear maps is k-bilinear, we have

$$(\lambda\,(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C)) \circ (\mathrm{id}_A \otimes \Delta_C) = \lambda\,((\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C))\,.$$

$\beta' = \mathrm{id}_S$, we obtain $(\gamma \circ \mathrm{id}_P) \otimes (\mathrm{id}_S \circ \delta) = (\gamma \otimes \mathrm{id}_S) \circ (\mathrm{id}_P \otimes \delta)$, so that

$$(\gamma \otimes \mathrm{id}_S) \circ (\mathrm{id}_P \otimes \delta) = \underbrace{(\gamma \circ \mathrm{id}_P)}_{=\gamma} \circ \underbrace{(\mathrm{id}_S \circ \delta)}_{=\delta} = \gamma \otimes \delta = (\mathrm{id}_Q \otimes \delta) \circ (\gamma \otimes \mathrm{id}_R)\,.$$

This proves (212).

By the definition of $T_{\lambda f}$, we have

$$\begin{aligned}
T_f &= (\mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes (\lambda f) \otimes \mathrm{id}_C)}_{=\lambda(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C)} \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= (\mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\lambda\,(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C)) \circ (\mathrm{id}_A \otimes \Delta_C)}_{=\lambda((\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C))} \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\lambda\,((\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C))) \\
&= \lambda \cdot \underbrace{(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)}_{=T_f} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \lambda T_f .
\end{aligned}$$

This proves Proposition 23.4 **(c)**.

(b) Applying Proposition 23.4 **(b)** to $\lambda = 0$ and $f = 0$, we obtain $T_{0 \cdot 0} = 0 T_0 = 0$. In other words, $T_0 = 0$. This proves Proposition 23.4 **(c)**.

(d) Let $f : C \to A$ and $g : C \to A$ be two k-linear maps.

Applying (212) to $P = A \otimes A$, $Q = A$, $R = C$, $S = C \otimes C$, $\gamma = \mu_A$ and $\delta = \Delta_C$, we obtain

$$(\mathrm{id}_A \otimes \Delta_C) \circ (\mu_A \otimes \mathrm{id}_C) = (\mu_A \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_{A \otimes A} \otimes \Delta_C) . \tag{213}$$

Next, we notice that

$$(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C}) = ((\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C \tag{214}$$

[123]. Using this equality, we can easily get

$$(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C}) = (\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C \tag{215}$$

[123] *Proof.* Applying (212) to $P = A \otimes A$, $Q = A$, $R = C$, $S = A$, $\gamma = \mu_A$ and $\delta = f$, we obtain

$$(\mathrm{id}_A \otimes f) \circ (\mu_A \otimes \mathrm{id}_C) = (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f) .$$

Applying (21) to $U = A \otimes A \otimes C$, $V = A \otimes C$, $W = A \otimes A$, $U' = C$, $V' = C$, $W' = C$, $\alpha = \mu_A \otimes \mathrm{id}_C$, $\beta = \mathrm{id}_A \otimes f$, $\alpha' = \mathrm{id}_C$ and $\beta' = \mathrm{id}_C$, we obtain

$$\begin{aligned}
((\mathrm{id}_A \otimes f) \circ (\mu_A \otimes \mathrm{id}_C)) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) &= (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ \left(\mu_A \otimes \underbrace{\mathrm{id}_C \otimes \mathrm{id}_C}_{=\mathrm{id}_{C \otimes C}} \right) \\
&= (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C}) ,
\end{aligned}$$

so that

$$\begin{aligned}
(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C}) &= \underbrace{((\mathrm{id}_A \otimes f) \circ (\mu_A \otimes \mathrm{id}_C))}_{=(\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)} \otimes \underbrace{(\mathrm{id}_C \circ \mathrm{id}_C)}_{=\mathrm{id}_C} \\
&= ((\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C .
\end{aligned}$$

This proves (214).

[124]. Since $\mu_A \circ (\mu_A \otimes \mathrm{id}_A) = \mu_A \circ (\mathrm{id}_A \otimes \mu_A)$ (by the axioms of a k-algebra, since A is a k-algebra), this becomes

$$
\begin{aligned}
&(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C}) \\
&= \left(\underbrace{\mu_A \circ (\mu_A \otimes \mathrm{id}_A)}_{= \mu_A \circ (\mathrm{id}_A \otimes \mu_A)} \circ (\mathrm{id}_{A \otimes A} \otimes f) \right) \otimes \underbrace{\mathrm{id}_C}_{= \mathrm{id}_C \circ \mathrm{id}_C} \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) \\
&= \left((\mu_A \circ (\mathrm{id}_A \otimes \mu_A)) \otimes \underbrace{\mathrm{id}_C}_{= \mathrm{id}_C \circ \mathrm{id}_C} \right) \circ \left(\underbrace{\mathrm{id}_{A \otimes A}}_{= \mathrm{id}_A \otimes \mathrm{id}_A} \otimes f \otimes \mathrm{id}_C \right) \\
&\qquad \left(\begin{array}{c} \text{by (21), applied to } U = A \otimes A \otimes C,\ V = A \otimes A \otimes A,\ W = A,\ U' = C,\ V' = C, \\ W' = C,\ \alpha = \mathrm{id}_{A \otimes A} \otimes f,\ \beta = \mu_A \circ (\mathrm{id}_A \otimes \mu_A),\ \alpha' = \mathrm{id}_C \text{ and } \beta' = \mathrm{id}_C \end{array} \right) \\
&= \underbrace{((\mu_A \circ (\mathrm{id}_A \otimes \mu_A)) \otimes (\mathrm{id}_C \circ \mathrm{id}_C))}_{= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_C)} \circ (\mathrm{id}_A \otimes \mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \\
&\qquad \begin{array}{c} \text{(by (21), applied to } U = A \otimes A \otimes A,\ V = A \otimes A,\ W = A, \\ U' = C,\ V' = C,\ W' = C,\ \alpha = \mathrm{id}_A \otimes \mu_A,\ \beta = \mu_A,\ \alpha' = \mathrm{id}_C \text{ and } \beta' = \mathrm{id}_C) \end{array} \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mathrm{id}_A \otimes f \otimes \mathrm{id}_C) . \qquad (216)
\end{aligned}
$$

On the other hand,

$$
(\mathrm{id}_{A \otimes A} \otimes \Delta_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) = \mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C)) \qquad (217)
$$

[125]. Using this equality, we can easily get

$$
(\mathrm{id}_{A \otimes A} \otimes \Delta_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) = \mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C) \qquad (218)
$$

---

[124] *Proof of (215).* Applying (21) to $U = A \otimes A \otimes C$, $V = A \otimes A$, $W = A$, $U' = C$, $V' = C$, $W' = C$, $\alpha = (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)$, $\beta = \mu_A$, $\alpha' = \mathrm{id}_C$ and $\beta' = \mathrm{id}_C$, we obtain

$$
(\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) = (\mu_A \otimes \mathrm{id}_C) \circ (((\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C) ,
$$

so that

$$
\begin{aligned}
&(\mu_A \otimes \mathrm{id}_C) \circ (((\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C) \\
&= (\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \underbrace{(\mathrm{id}_C \circ \mathrm{id}_C)}_{= \mathrm{id}_C} \\
&= (\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C .
\end{aligned}
$$

Now,

$$
\begin{aligned}
(\mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C})}_{\substack{= ((\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C \\ \text{(by (214))}}} &= (\mu_A \otimes \mathrm{id}_C) \circ (((\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C) \\
&= (\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_{A \otimes A} \otimes f)) \otimes \mathrm{id}_C .
\end{aligned}
$$

This proves (215).

[125] *Proof.* Applying (212) to $P = C$, $Q = A$, $R = C$, $S = C \otimes C$, $\gamma = g$ and $\delta = \Delta_C$, we obtain

$$
(\mathrm{id}_A \otimes \Delta_C) \circ (g \otimes \mathrm{id}_C) = (g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) .
$$

Applying (21) to $U = A$, $V = A$, $W = A$, $U' = C \otimes C$, $V' = A \otimes C$, $W' = A \otimes C \otimes C$, $\alpha = \mathrm{id}_A$,

[126]. Since $(\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C = (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C$ (by the axioms of a k-coalgebra, since $\beta = \mathrm{id}_A$, $\alpha' = g \otimes \mathrm{id}_C$ and $\beta' = \mathrm{id}_A \otimes \Delta_C$, we obtain

$$\begin{aligned}(\mathrm{id}_A \circ \mathrm{id}_A) \otimes ((\mathrm{id}_A \otimes \Delta_C) \circ (g \otimes \mathrm{id}_C)) &= \left(\underbrace{\mathrm{id}_A \otimes \mathrm{id}_A}_{=\mathrm{id}_{A \otimes A}} \otimes \Delta_C \right) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \\ &= (\mathrm{id}_{A \otimes A} \otimes \Delta_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C)\,,\end{aligned}$$

so that

$$\begin{aligned}(\mathrm{id}_{A \otimes A} \otimes \Delta_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) &= \underbrace{(\mathrm{id}_A \circ \mathrm{id}_A)}_{=\mathrm{id}_A} \otimes \underbrace{((\mathrm{id}_A \otimes \Delta_C) \circ (g \otimes \mathrm{id}_C))}_{=(g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C)} \\ &= \mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C))\,.\end{aligned}$$

This proves (217).

[126] *Proof of (218).* Applying (21) to $U = A$, $V = A$, $W = A$, $U' = C$, $V' = C \otimes C$, $W' = A \otimes C \otimes C$, $\alpha = \mathrm{id}_A$, $\beta = \mathrm{id}_A$, $\alpha' = \Delta_C$ and $\beta' = (g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C)$, we obtain

$$(\mathrm{id}_A \circ \mathrm{id}_A) \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C) = (\mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C))) \circ (\mathrm{id}_A \otimes \Delta_C)\,,$$

so that

$$\begin{aligned}&(\mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C))) \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= \underbrace{(\mathrm{id}_A \circ \mathrm{id}_A)}_{=\mathrm{id}_A} \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C) \\ &= \mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C)\,.\end{aligned}$$

Now,

$$\begin{aligned}&\underbrace{(\mathrm{id}_{A \otimes A} \otimes \Delta_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C)}_{\substack{=\mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C)) \\ \text{(by (217))}}} \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= (\mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C))) \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= \mathrm{id}_A \otimes ((g \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C)\,.\end{aligned}$$

This proves (218).

C is a k-coalgebra), this becomes

$$
\begin{aligned}
&(\mathrm{id}_{A\otimes A}\otimes\Delta_C)\circ(\mathrm{id}_A\otimes g\otimes\mathrm{id}_C)\circ(\mathrm{id}_A\otimes\Delta_C)\\
&= \underbrace{\mathrm{id}_A}_{=\mathrm{id}_A\circ\mathrm{id}_A}\otimes\left((g\otimes\mathrm{id}_{C\otimes C})\circ\underbrace{(\mathrm{id}_C\otimes\Delta_C)\circ\Delta_C}_{=(\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C}\right)\\
&= (\mathrm{id}_A\circ\mathrm{id}_A)\otimes((g\otimes\mathrm{id}_{C\otimes C})\circ(\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C)\\
&= \left(\mathrm{id}_A\otimes g\otimes\underbrace{\mathrm{id}_{C\otimes C}}_{=\mathrm{id}_C\otimes\mathrm{id}_C}\right)\circ\left(\underbrace{\mathrm{id}_A}_{=\mathrm{id}_A\circ\mathrm{id}_A}\otimes((\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C)\right)\\
&\qquad\left(\begin{array}{c}\text{by (21), applied to } U=A,\ V=A,\ W=A,\ U'=C,\ V'=C\otimes C\otimes C,\\ W'=A\otimes C\otimes C,\ \alpha=\mathrm{id}_A,\ \beta=\mathrm{id}_A,\ \alpha'=(\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C \text{ and } \beta'=g\otimes\mathrm{id}_{C\otimes C}\end{array}\right)\\
&= (\mathrm{id}_A\otimes g\otimes\mathrm{id}_C\otimes\mathrm{id}_C)\circ\underbrace{((\mathrm{id}_A\circ\mathrm{id}_A)\otimes((\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C))}_{\substack{=(\mathrm{id}_A\otimes\Delta_C\otimes\mathrm{id}_C)\circ(\mathrm{id}_A\otimes\Delta_C)\\ \text{(by (21), applied to } U=A,\ V=A,\ W=A,\ U'=C,\ V'=C\otimes C,\ W'=C\otimes C\otimes C,\\ \alpha=\mathrm{id}_A,\ \beta=\mathrm{id}_A,\ \alpha'=\Delta_C \text{ and } \beta'=\Delta_C\otimes\mathrm{id}_C)}}\\
&= (\mathrm{id}_A\otimes g\otimes\mathrm{id}_C\otimes\mathrm{id}_C)\circ(\mathrm{id}_A\otimes\Delta_C\otimes\mathrm{id}_C)\circ(\mathrm{id}_A\otimes\Delta_C). \qquad (219)
\end{aligned}
$$

Applying (21) to $U=C$, $V=A$, $W=A$, $U'=C$, $V'=C$, $W'=A$, $\alpha=g$, $\beta=\mathrm{id}_A$, $\alpha'=\mathrm{id}_C$ and $\beta'=f$, we obtain $(\mathrm{id}_A\circ g)\otimes(f\circ\mathrm{id}_C)=(\mathrm{id}_A\otimes f)\circ(g\otimes\mathrm{id}_C)$, so that

$$(\mathrm{id}_A\otimes f)\circ(g\otimes\mathrm{id}_C)=\underbrace{(\mathrm{id}_A\circ g)}_{=g}\otimes\underbrace{(f\circ\mathrm{id}_C)}_{=f}=g\otimes f. \qquad (220)$$

Now, $T_f=(\mu_A\otimes\mathrm{id}_C)\circ(\mathrm{id}_A\otimes f\otimes\mathrm{id}_C)\circ(\mathrm{id}_A\otimes\Delta_C)$ (by the definition of T_f) and

$T_g = (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)$ (by the definition of T_g), so that

$$
\begin{aligned}
&T_f \circ T_g \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes \Delta_C) \circ (\mu_A \otimes \mathrm{id}_C)}_{\substack{= (\mu_A \otimes \mathrm{id}_{C\otimes C}) \circ (\mathrm{id}_{A\otimes A} \otimes \Delta_C) \\ \text{(by (213))}}} \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= \underbrace{(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mu_A \otimes \mathrm{id}_{C\otimes C})}_{\substack{= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \\ \text{(by (216))}}} \circ \underbrace{(\mathrm{id}_{A\otimes A} \otimes \Delta_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)}_{\substack{= (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\ \text{(by (219))}}} \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes \mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes g \otimes \mathrm{id}_C \otimes \mathrm{id}_C)}_{\substack{= \mathrm{id}_A \otimes ((\mathrm{id}_A \otimes f) \circ (g \otimes \mathrm{id}_C)) \otimes \mathrm{id}_C \\ \text{(by (211), applied to } P=A,\ Q=C,\ R_1=C\otimes C, \\ R_2=A\otimes C,\ R_3=A\otimes A,\ \varphi=g\otimes \mathrm{id}_C \text{ and } \psi=\mathrm{id}_A \otimes f)}} \\
&\qquad \circ (\mathrm{id}_A \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_C) \circ \left(\mathrm{id}_A \otimes \underbrace{((\mathrm{id}_A \otimes f) \circ (g \otimes \mathrm{id}_C))}_{\substack{= g \otimes f \\ \text{(by (220))}}} \otimes \mathrm{id}_C \right) \\
&\qquad \circ (\mathrm{id}_A \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= (\mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes g \otimes f \otimes \mathrm{id}_C)}_{\substack{= \mathrm{id}_A \otimes (\mu_A \circ (g \otimes f)) \otimes \mathrm{id}_C \\ \text{(by (211), applied to } P=A,\ Q=C,\ R_1=C\otimes C, \\ R_2=A\otimes A,\ R_3=A,\ \varphi=g\otimes f \text{ and } \psi=\mu_A)}} \circ (\mathrm{id}_A \otimes \Delta_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= (\mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes (\mu_A \circ (g \otimes f)) \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C \otimes \mathrm{id}_C)}_{\substack{= \mathrm{id}_A \otimes (\mu_A \circ (g \otimes f) \circ \Delta_C) \otimes \mathrm{id}_C \\ \text{(by (211), applied to } P=A,\ Q=C,\ R_1=C, \\ R_2=C\otimes C,\ R_3=A,\ \varphi=\Delta_C \text{ and } \psi=\mu_A \circ (g\otimes f))}} \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes (\mu_A \circ (g \otimes f) \circ \Delta_C) \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)\,. \qquad (221)
\end{aligned}
$$

But by the definition of T_{g*f}, we have

$$
\begin{aligned}
T_{g*f} &= (\mu_A \otimes \mathrm{id}_C) \circ \left(\mathrm{id}_A \otimes \underbrace{(g * f)}_{\substack{= \mu_A \circ (g\otimes f) \circ \Delta_C \\ \text{(by the definition of convolution)}}} \otimes \mathrm{id}_C \right) \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes (\mu_A \circ (g \otimes f) \circ \Delta_C) \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) = T_f \circ T_g
\end{aligned}
$$

(by (221)). This proves Proposition 23.4 **(d)**.

(e) By (211) (applied to $P = A$, $Q = C$, $R_1 = C$, $R_2 = k$, $R_3 = A$, $\varphi = \varepsilon_C$ and $\psi = \eta_A$), we have

$$
(\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_C) = \mathrm{id}_A \otimes \underbrace{(\eta_A \circ \varepsilon_C)}_{= e_{C,A}} \otimes \mathrm{id}_C = \mathrm{id}_A \otimes e_{C,A} \otimes \mathrm{id}_C\,.
$$

Now, by the definition of $T_{e_{C,A}}$, we have

$$
\begin{aligned}
T_{e_{C,A}} &= (\mu_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_A \otimes e_{C,A} \otimes \mathrm{id}_C)}_{= (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_C)} \circ (\mathrm{id}_A \otimes \Delta_C) \\
&= (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)\,. \qquad (222)
\end{aligned}
$$

Now, consider the isomorphisms $\mathrm{kan}_{A\otimes k,A}$ and $\mathrm{kan}_{C,k\otimes C}$ defined in Proposition 23.4 **(h)**. Then, by the axioms of a k-coalgebra, we have $(\varepsilon_C \otimes \mathrm{id}_C)\circ\Delta_C = \mathrm{kan}_{C,k\otimes C}$ (since C is a k-coalgebra). Also, by the axioms of a k-algebra, we have $\mu_A\circ(\mathrm{id}_A \otimes\eta_A) = \mathrm{kan}_{A\otimes k,A}$ (since A is a k-algebra).

By (21) (applied to $U = A\otimes k$, $V = A\otimes A$, $W = A$, $U' = C$, $V' = C$, $W' = C$, $\alpha = \mathrm{id}_A \otimes\eta_A$, $\beta = \mu_A$, $\alpha' = \mathrm{id}_C$ and $\beta' = \mathrm{id}_C$), we have

$$(\mu_A \circ (\mathrm{id}_A \otimes\eta_A)) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) = (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes\eta_A \otimes \mathrm{id}_C)\,,$$

so that

$$(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes\eta_A \otimes \mathrm{id}_C) = \underbrace{(\mu_A \circ (\mathrm{id}_A \otimes\eta_A))}_{=\mathrm{kan}_{A\otimes k,A}} \otimes \underbrace{(\mathrm{id}_C \circ \mathrm{id}_C)}_{=\mathrm{id}_C} = \mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C\,. \tag{223}$$

By (21) (applied to $U = A$, $V = A$, $W = A$, $U' = C$, $V' = C\otimes C$, $W' = k\otimes C$, $\alpha = \mathrm{id}_A$, $\beta = \mathrm{id}_A$, $\alpha' = \Delta_C$ and $\beta' = \varepsilon_C \otimes \mathrm{id}_C$), we have

$$(\mathrm{id}_A \circ \mathrm{id}_A) \otimes ((\varepsilon_C \otimes \mathrm{id}_C) \circ \Delta_C) = (\mathrm{id}_A \otimes\varepsilon_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes\Delta_C)\,,$$

so that

$$(\mathrm{id}_A \otimes\varepsilon_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes\Delta_C) = \underbrace{(\mathrm{id}_A \circ \mathrm{id}_A)}_{=\mathrm{id}_A} \otimes \underbrace{((\varepsilon_C \otimes \mathrm{id}_C) \circ \Delta_C)}_{=\mathrm{kan}_{C,k\otimes C}} = \mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C}\,. \tag{224}$$

Now, (222) becomes

$$\begin{aligned} T_{e_{C,A}} &= \underbrace{(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes\eta_A \otimes \mathrm{id}_C)}_{=\mathrm{kan}_{A\otimes k,A}\otimes \mathrm{id}_C} \circ \underbrace{(\mathrm{id}_A \otimes\varepsilon_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes\Delta_C)}_{=\mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C}} \\ &= (\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C}) = \mathrm{id}_{A\otimes C} \end{aligned}$$

(because a very easy linear-algebraic fact says that $(\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C)\circ(\mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C}) = \mathrm{id}_{A\otimes C}$ [127]). This proves Proposition 23.4 **(e)**.

[127] *Proof.* For any $(a, c) \in A \times C$, we have

$$\begin{aligned} ((\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C}))\,(a \otimes c) &= (\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C)\,\underbrace{((\mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C})\,(a \otimes c))}_{=\mathrm{id}_A(a)\otimes\mathrm{kan}_{C,k\otimes C}(c)} \\ &= (\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C) \left(\underbrace{\mathrm{id}_A\,(a)}_{=a} \otimes \underbrace{\mathrm{kan}_{C,k\otimes C}\,(c)}_{\substack{=1\otimes c \\ \text{(by the definition of } \mathrm{kan}_{C,k\otimes C}\text{)}}} \right) \\ &= (\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C)\,(a \otimes 1 \otimes c) = \underbrace{\mathrm{kan}_{A\otimes k,A}\,(a \otimes 1)}_{\substack{=1a \\ \text{(by the definition of } \mathrm{kan}_{A\otimes k,A}\text{)}}} \otimes \underbrace{\mathrm{id}_C\,(c)}_{=c} \\ &= 1a \otimes c = a \otimes c = \mathrm{id}_{A\otimes C}\,(a \otimes c)\,. \end{aligned}$$

In other words, the two k-linear maps $(\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C})$ and $\mathrm{id}_{A\otimes C}$ are equal to each other on each pure tensor in $A \otimes C$. Thus, these two maps must be identical (since two k-linear maps from a tensor product which are equal to each other on each pure tensor must necessarily be identical). In other words, $(\mathrm{kan}_{A\otimes k,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \mathrm{kan}_{C,k\otimes C}) = \mathrm{id}_{A\otimes C}$, qed.

(f) Assume that C is a graded k-coalgebra, and that A is a graded k-algebra, and that f is a graded map.

The map μ_A is graded (since A is a graded k-algebra), and so is the map Δ_C (since C is a graded k-coalgebra). Thus, the maps μ_A, id_C, id_A, f and Δ_C are all graded. Hence, the maps $\mu_A \otimes \mathrm{id}_C$, $\mathrm{id}_A \otimes f \otimes \mathrm{id}_C$ and $\mathrm{id}_A \otimes \Delta_C$ are graded (since tensor products of graded maps are always graded). Hence, the map $(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)$ is graded (since compositions of graded maps are always graded). Since $(\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) = T_f$, this rewrites as follows: The map T_f is graded. Proposition 23.4 **(f)** is thus proven.

(g) Let $f : C \to A$ be a $*$-invertible k-linear map.

Applying Proposition 23.4 **(d)** to $g = f^{*(-1)}$, we obtain $T_{f^{*(-1)} * f} = T_f \circ T_{f^{*(-1)}}$. Since $f^{*(-1)} * f = e_{C,A}$, this rewrites as $T_{e_{C,A}} = T_f \circ T_{f^{*(-1)}}$. Since $T_{e_{C,A}} = \mathrm{id}_{A \otimes C}$ (by Proposition 23.4 **(e)**), this rewrites as $\mathrm{id}_{A \otimes C} = T_f \circ T_{f^{*(-1)}}$.

Applying Proposition 23.4 **(d)** to $f^{*(-1)}$ and f instead of f and g, we obtain $T_{f * f^{*(-1)}} = T_{f^{*(-1)}} \circ T_f$. Since $f * f^{*(-1)} = e_{C,A}$, this rewrites as $T_{e_{C,A}} = T_{f^{*(-1)}} \circ T_f$. Since $T_{e_{C,A}} = \mathrm{id}_{A \otimes C}$, this rewrites as $\mathrm{id}_{A \otimes C} = T_{f^{*(-1)}} \circ T_f$.

From $T_{f^{*(-1)}} \circ T_f = \mathrm{id}_{A \otimes C}$ and $T_f \circ T_{f^{*(-1)}} = \mathrm{id}_{A \otimes C}$, we conclude that the map T_f is invertible and satisfies $T_{f^{*(-1)}} = (T_f)^{-1}$. Proposition 23.4 **(g)** is thus proven.

(h) Let $f : C \to A$ be a k-linear map.

By the axioms of a k-coalgebra, we have $(\varepsilon_C \otimes \mathrm{id}_C) \circ \Delta_C = \mathrm{kan}_{C, k \otimes C}$ (since C is a k-coalgebra).

By the axioms of a k-algebra, we have $\mu_A \circ (\mathrm{id}_A \otimes \eta_A) = \mathrm{kan}_{A \otimes k, A}$ (since A is a k-algebra).

Let $\mathrm{kan}_{C, C \otimes k} : C \to C \otimes k$ be the canonical isomorphism which sends every $c \in C$ to $c \otimes 1 \in C \otimes k$.

Every $x \in C$ satisfies

$$\mathrm{kan}_{C, k \otimes C}(x) = 1 \otimes x \tag{225}$$

(by the definition of $\mathrm{kan}_{C, k \otimes C}$).

We have $(\mathrm{id}_A \otimes \varepsilon_C) \circ (\mu_A \otimes \mathrm{id}_C) = (\mu_A \otimes \mathrm{id}_k) \circ (\mathrm{id}_{A \otimes A} \otimes \varepsilon_C)$ (by (212), applied to $P = A \otimes A$, $Q = A$, $R = C$, $S = k$, $\gamma = \mu_A$ and $\delta = \varepsilon_C$).

We have $(\mathrm{id}_{A \otimes A} \otimes \varepsilon_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) = (\mathrm{id}_A \otimes f \otimes \mathrm{id}_k) \circ (\mathrm{id}_{A \otimes C} \otimes \varepsilon_C)$ (by (212), applied to $P = A \otimes C$, $Q = A \otimes A$, $R = C$, $S = k$, $\gamma = \mathrm{id}_A \otimes f$ and $\delta = \varepsilon_C$).

By the definition of η_A, we have $\eta_A(1) = 1 \cdot 1_A = 1_A$.

By (21) (applied to $U = A$, $V = A$, $W = A$, $U' = C$, $V' = C \otimes C$, $W' = C \otimes k$, $\alpha = \mathrm{id}_A$, $\beta = \mathrm{id}_A$, $\alpha' = \Delta_C$ and $\beta' = \mathrm{id}_C \otimes \varepsilon_C$), we have

$$\begin{aligned}(\mathrm{id}_A \circ \mathrm{id}_A) \otimes ((\mathrm{id}_C \otimes \varepsilon_C) \circ \Delta_C) &= \left(\underbrace{\mathrm{id}_A \otimes \mathrm{id}_C}_{= \mathrm{id}_{A \otimes C}} \otimes \varepsilon_C \right) \circ (\mathrm{id}_A \otimes \Delta_C) \\ &= (\mathrm{id}_{A \otimes C} \otimes \varepsilon_C) \circ (\mathrm{id}_A \otimes \Delta_C),\end{aligned}$$

so that

$$(\mathrm{id}_{A \otimes C} \otimes \varepsilon_C) \circ (\mathrm{id}_A \otimes \Delta_C) = \underbrace{(\mathrm{id}_A \circ \mathrm{id}_A)}_{= \mathrm{id}_A} \otimes \underbrace{((\mathrm{id}_C \otimes \varepsilon_C) \circ \Delta_C)}_{\substack{= \mathrm{kan}_{C, C \otimes k} \\ \text{(by the axioms of a } k\text{-coalgebra,} \\ \text{since } C \text{ is a } k\text{-coalgebra)}}} = \mathrm{id}_A \otimes \mathrm{kan}_{C, C \otimes k}.$$

Since $T_f = (\mu_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C)$, we have

$$
\begin{aligned}
&\mathrm{kan}_{A\otimes k,A} \circ (\mathrm{id}_A \otimes \varepsilon_C) \circ T_f \circ (\eta_A \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C} \\
&= \mathrm{kan}_{A\otimes k,A} \circ \underbrace{(\mathrm{id}_A \otimes \varepsilon_C) \circ (\mu_A \otimes \mathrm{id}_C)}_{=(\mu_A \otimes \mathrm{id}_k) \circ (\mathrm{id}_{A\otimes A} \otimes \varepsilon_C)} \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_A \otimes \Delta_C) \circ (\eta_A \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C} \\
&= \mathrm{kan}_{A\otimes k,A} \circ (\mu_A \otimes \mathrm{id}_k) \circ \underbrace{(\mathrm{id}_{A\otimes A} \otimes \varepsilon_C) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_C)}_{=(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k) \circ (\mathrm{id}_{A\otimes C} \otimes \varepsilon_C)} \circ (\mathrm{id}_A \otimes \Delta_C) \circ (\eta_A \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C} \\
&= \mathrm{kan}_{A\otimes k,A} \circ (\mu_A \otimes \mathrm{id}_k) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_k) \circ \underbrace{(\mathrm{id}_{A\otimes C} \otimes \varepsilon_C) \circ (\mathrm{id}_A \otimes \Delta_C)}_{=\mathrm{id}_A \otimes \mathrm{kan}_{C,C\otimes k}} \circ (\eta_A \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C} \\
&= \mathrm{kan}_{A\otimes k,A} \circ (\mu_A \otimes \mathrm{id}_k) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_k) \circ (\mathrm{id}_A \otimes \mathrm{kan}_{C,C\otimes k}) \circ (\eta_A \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C} \,.
\end{aligned}
$$

Thus, every $x \in C$ satisfies

$$
\begin{aligned}
&\left(\mathrm{kan}_{A\otimes k,A} \circ \left(\mathrm{id}_A \otimes \varepsilon_C\right) \circ T_f \circ \left(\eta_A \otimes \mathrm{id}_C\right) \circ \mathrm{kan}_{C,k\otimes C}\right)(x) \\
&= \left(\mathrm{kan}_{A\otimes k,A} \circ \left(\mu_A \otimes \mathrm{id}_k\right) \circ \left(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k\right) \circ \left(\mathrm{id}_A \otimes \mathrm{kan}_{C,C\otimes k}\right) \circ \left(\eta_A \otimes \mathrm{id}_C\right) \circ \mathrm{kan}_{C,k\otimes C}\right)(x) \\
&= \mathrm{kan}_{A\otimes k,A}\left(\left(\mu_A \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes \mathrm{kan}_{C,C\otimes k}\right)\left(\left(\eta_A \otimes \mathrm{id}_C\right)\underbrace{\left(\mathrm{kan}_{C,k\otimes C}(x)\right)}_{\substack{=1\otimes x \\ \text{(by (225))}}}\right)\right)\right)\right) \\
&= \mathrm{kan}_{A\otimes k,A}\left(\left(\mu_A \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes \mathrm{kan}_{C,C\otimes k}\right)\underbrace{\left(\left(\eta_A \otimes \mathrm{id}_C\right)(1\otimes x)\right)}_{=\eta_A(1)\otimes \mathrm{id}_C(x)}\right)\right)\right) \\
&= \mathrm{kan}_{A\otimes k,A}\left(\left(\mu_A \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes \mathrm{kan}_{C,C\otimes k}\right)\left(\underbrace{\eta_A(1)}_{=1_A}\otimes \underbrace{\mathrm{id}_C(x)}_{=x}\right)\right)\right)\right) \\
&= \mathrm{kan}_{A\otimes k,A}\left(\left(\mu_A \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k\right)\underbrace{\left(\left(\mathrm{id}_A \otimes \mathrm{kan}_{C,C\otimes k}\right)(1_A\otimes x)\right)}_{=\mathrm{id}_A(1_A)\otimes \mathrm{kan}_{C,C\otimes k}(x)}\right)\right) \\
&= \mathrm{kan}_{A\otimes k,A}\left(\left(\mu_A \otimes \mathrm{id}_k\right)\left(\left(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k\right)\left(\underbrace{\mathrm{id}_A(1_A)}_{=1_A}\otimes \underbrace{\mathrm{kan}_{C,C\otimes k}(x)}_{\substack{=x\otimes 1 \\ \text{(by the definition of } \mathrm{kan}_{C,C\otimes k}\text{)}}}\right)\right)\right) \\
&= \mathrm{kan}_{A\otimes k,A}\left(\left(\mu_A \otimes \mathrm{id}_k\right)\underbrace{\left(\left(\mathrm{id}_A \otimes f \otimes \mathrm{id}_k\right)(1_A\otimes x\otimes 1)\right)}_{=\mathrm{id}_A(1_A)\otimes f(x)\otimes \mathrm{id}_k(1)}\right) \\
&= \mathrm{kan}_{A\otimes k,A}\left(\left(\mu_A \otimes \mathrm{id}_k\right)\left(\underbrace{\mathrm{id}_A(1_A)}_{=1_A}\otimes f(x)\otimes \underbrace{\mathrm{id}_k(1)}_{=1}\right)\right) \\
&= \mathrm{kan}_{A\otimes k,A}\underbrace{\left(\left(\mu_A \otimes \mathrm{id}_k\right)(1_A\otimes f(x)\otimes 1)\right)}_{=\mu_A(1_A\otimes f(x))\otimes \mathrm{id}_k(1)} \\
&= \mathrm{kan}_{A\otimes k,A}\left(\underbrace{\mu_A(1_A\otimes f(x))}_{\substack{=1_A f(x) \\ \text{(since } \mu_A \text{ is the multiplication map of } A\text{)}}}\otimes \underbrace{\mathrm{id}_k(1)}_{=1}\right) \\
&= \mathrm{kan}_{A\otimes k,A}\left(1_A f(x), 1\right) = 1\cdot 1_A f(x) \qquad \left(\text{by the definition of } \mathrm{kan}_{A\otimes k,A}\right) \\
&= f(x).
\end{aligned}
$$

Hence, $\mathrm{kan}_{A\otimes k,A} \circ \left(\mathrm{id}_A \otimes \varepsilon_C\right) \circ T_f \circ \left(\eta_A \otimes \mathrm{id}_C\right) \circ \mathrm{kan}_{C,k\otimes C} = f$. This proves Proposition 23.4 **(h)**.

(i) Assume that C is a graded k-coalgebra, that A is a graded k-algebra, and that f is a k-linear map such that T_f is graded.

Consider the isomorphisms $\mathrm{kan}_{A\otimes k,A}$ and $\mathrm{kan}_{C,k\otimes C}$ defined in Proposition 23.4 **(h)**. These isomorphisms are clearly graded.

Since C is a graded k-coalgebra, the map ε_C is graded. Since A is a graded k-algebra, the map η_A is graded.

Thus, the maps $\operatorname{kan}_{A\otimes k,A}$, id_A, ε_C, T_f, η_A, id_C and $\operatorname{kan}_{C,k\otimes C}$ all are graded. Hence, the maps $\operatorname{kan}_{A\otimes k,A}$, $\operatorname{id}_A \otimes \varepsilon_C$, T_f, $\eta_A \otimes \operatorname{id}_C$, $\operatorname{kan}_{C,k\otimes C}$ all are graded (since tensor products of graded maps are always graded). Hence, the map $\operatorname{kan}_{A\otimes k,A} \circ (\operatorname{id}_A \otimes \varepsilon_C) \circ T_f \circ (\eta_A \otimes \operatorname{id}_C) \circ \operatorname{kan}_{C,k\otimes C}$ is graded (since compositions of graded maps are always graded). Since $\operatorname{kan}_{A\otimes k,A} \circ (\operatorname{id}_A \otimes \varepsilon_C) \circ T_f \circ (\eta_A \otimes \operatorname{id}_C) \circ \operatorname{kan}_{C,k\otimes C} = f$ (by Proposition 23.4 **(h)**), this rewrites as follows: The map f is graded. Thus, we have verified Proposition 23.4 **(i)**. □

Now that Proposition 23.4 is completely proven, we can fulfill our debt of proving Proposition 23.1:

Proof of Proposition 23.1. **(a)** Let us use Definition 23.3. By Proposition 23.4 **(f)**, the map T_f is graded. By Proposition 23.4 **(g)**, this map T_f is invertible. Thus, T_f is a graded invertible k-linear map. Hence, $(T_f)^{-1}$ is also a graded map (because it is well-known that the inverse of a graded invertible k-linear map must always be graded). In other words, $T_{f^{*(-1)}}$ is a graded map (because Proposition 23.4 **(g)** yields $T_{f^{*(-1)}} = (T_f)^{-1}$). Now, Proposition 23.4 **(i)** (applied to $f^{*(-1)}$ instead of f) yields that $f^{*(-1)}$ is graded. This proves Proposition 23.1 **(a)**.

(b) Let $n \in \mathbb{Z}$. If $n \in \mathbb{N}$, then Proposition 23.1 **(b)** immediately follows from Proposition 16.18 **(c)**. Hence, for the rest of the proof of Proposition 23.1 **(b)**, we can WLOG assume that $n \in \mathbb{N}$ does not hold. Assume this. Then, $n \notin \mathbb{N}$, so that n is negative, and thus $-n \in \mathbb{N}$. Hence, Proposition 16.18 **(c)** (applied to $f^{*(-1)}$ and $-n$ instead of f and n) yields that $\left(f^{*(-1)}\right)^{*(-n)}$ is graded (because Proposition 23.1 **(a)** shows that $f^{*(-1)}$ is a graded map). Since $\left(f^{*(-1)}\right)^{*(-n)} = f^{*((-1)\cdot(-n))} = f^{*n}$, this rewrites as follows: The map f^{*n} is graded. This proves Proposition 23.1 **(b)**.

The proof of Proposition 23.1 is thus complete, and with it Theorem 23.2 is proven. □

We have used Proposition 23.4 to prove Proposition 23.1. This, however, is not its only application. For a different application, let us show an alternative proof of Proposition 10.1 with its help. First, a lemma:

Lemma 23.5. Let k be a field. Let C be a cocommutative k-coalgebra. Then, Δ_C is a k-coalgebra homomorphism from C to $C \otimes C$, and ε_C is a k-coalgebra homomorphism from C to k.

Proof of Lemma 23.5. Lemma 9.6 **(b)** shows that ε_C is a k-coalgebra homomorphism from C to k. Hence, the only thing that remains to be done in order to prove Lemma 23.5 is to show that Δ_C is a k-coalgebra homomorphism from C to $C \otimes C$.

By the definition of the k-coalgebra $C \otimes C$, we have $\Delta_{C\otimes C} = (\operatorname{id}_C \otimes \tau_{C,C} \otimes \operatorname{id}_C) \circ (\Delta_C \otimes \Delta_C)$. Thus,

$$\Delta_{C\otimes C} \circ \Delta_C = (\operatorname{id}_C \otimes \tau_{C,C} \otimes \operatorname{id}_C) \circ (\Delta_C \otimes \Delta_C) \circ \Delta_C = (\Delta_C \otimes \Delta_C) \circ \Delta_C$$

(by Lemma 9.5). Also, $\varepsilon_{C\otimes C} \circ \Delta_C = \varepsilon_C$ [128].

[128] *Proof.* Lemma 9.6 **(a)** shows that every $x \in C$ satisfies $((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x) = \varepsilon_C(x)\, 1 \otimes 1$.

We have thus proven that $\Delta_{C\otimes C} \circ \Delta_C = (\Delta_C \otimes \Delta_C) \circ \Delta_C$ and $\varepsilon_{C\otimes C} \circ \Delta_C = \varepsilon_C$. These two equations combined yield that Δ_C is a k-coalgebra homomorphism from C to $C \otimes C$. This completes the proof of Lemma 23.5. $\square$

Alternative proof of Proposition 10.1. Applying Definition 23.3 to $A = H$, we obtain a map $T_f : H \otimes C \to H \otimes C$. Similarly, we obtain maps $T_g : H \otimes C \to H \otimes C$ and $T_{f*g} : H \otimes C \to H \otimes C$. Proposition 23.4 **(d)** (applied to H, g and f instead of A, f and g) yields $T_{f*g} = T_g \circ T_f$.

By Lemma 23.5, we know that Δ_C and ε_C are k-coalgebra homomorphisms.

Also, H is a k-bialgebra, so that μ_H and η_H are k-coalgebra homomorphisms (by the axioms of a bialgebra).

Since μ_H and id_C are k-coalgebra homomorphisms, the map $\mu_H \otimes \mathrm{id}_C$ is also a k-coalgebra homomorphism (because a tensor product of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism).

Since id_H, f and id_C are k-coalgebra homomorphisms, the map $\mathrm{id}_H \otimes f \otimes \mathrm{id}_C$ is also a k-coalgebra homomorphism (because a tensor product of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism).

Since id_H and Δ_C are k-coalgebra homomorphisms, the map $\mathrm{id}_H \otimes \Delta_C$ is also a k-coalgebra homomorphism (because a tensor product of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism).

Since $\mu_H \otimes \mathrm{id}_C$, $\mathrm{id}_H \otimes f \otimes \mathrm{id}_C$ and $\mathrm{id}_H \otimes \Delta_C$ are k-coalgebra homomorphisms, the map $(\mu_H \otimes \mathrm{id}_C) \circ (\mathrm{id}_H \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_H \otimes \Delta_C)$ is also a k-coalgebra homomorphism (because a composition of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism).

By the definition of T_f, we have

$$T_f = (\mu_H \otimes \mathrm{id}_C) \circ (\mathrm{id}_H \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_H \otimes \Delta_C) .$$

Thus, T_f is a k-coalgebra homomorphism (because $(\mu_H \otimes \mathrm{id}_C) \circ (\mathrm{id}_H \otimes f \otimes \mathrm{id}_C) \circ (\mathrm{id}_H \otimes \Delta_C)$ is a k-coalgebra homomorphism). Similarly, T_g is a k-coalgebra homomorphism.

Since T_g and T_f are k-coalgebra homomorphisms, the map $T_g \circ T_f$ is also a k-coalgebra homomorphism (because a composition of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism). Since $T_g \circ T_f = T_{f*g}$, this rewrites as follows: The map T_{f*g} is a k-coalgebra homomorphism.

Let $\mathrm{kan}_{C,k\otimes C} : C \to k \otimes C$ be the canonical isomorphism which sends c to $1 \otimes c$ for every $c \in C$. Let $\mathrm{kan}_{H\otimes k,H} : H \otimes k \to H$ be the canonical isomorphism which sends $a \otimes \lambda$ to λa for every $(a, \lambda) \in H \times k$. Both $\mathrm{kan}_{C,k\otimes C}$ and $\mathrm{kan}_{H\otimes k,H}$ are k-coalgebra homomorphisms.

By the definition of the k-coalgebra $C \otimes C$, we have $\varepsilon_{C\otimes C} = \mathrm{kan}_{k\otimes k,k} \circ (\varepsilon_C \otimes \varepsilon_C)$, where $\mathrm{kan}_{k\otimes k,k} : k \otimes k \to k$ is the canonical isomorphism which sends every $\lambda \otimes \lambda' \in k \otimes k$ to $\lambda\lambda' \in k$. Now, for every $x \in C$, we have

$$\begin{aligned}
\left(\underbrace{\varepsilon_{C\otimes C}}_{=\mathrm{kan}_{k\otimes k,k} \circ (\varepsilon_C \otimes \varepsilon_C)} \circ \Delta_C \right)(x) &= \left(\mathrm{kan}_{k\otimes k,k} \circ (\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C\right)(x)) = \mathrm{kan}_{k\otimes k,k} \underbrace{\left(((\varepsilon_C \otimes \varepsilon_C) \circ \Delta_C)(x)\right)}_{=\varepsilon_C(x) 1 \otimes 1} \\
&= \mathrm{kan}_{k\otimes k,k}(\varepsilon_C(x)\, 1 \otimes 1) = \varepsilon_C(x)\, 1 \cdot 1 \qquad \text{(by the definition of } \mathrm{kan}_{k\otimes k,k}) \\
&= \varepsilon_C(x) .
\end{aligned}$$

In other words, $\varepsilon_{C\otimes C} \circ \Delta_C = \varepsilon_C$, qed.

Since id_H and ε_C are k-coalgebra homomorphisms, the map $\mathrm{id}_H \otimes \varepsilon_C$ is also a k-coalgebra homomorphism (because a tensor product of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism).

Since η_H and id_C are k-coalgebra homomorphisms, the map $\eta_H \otimes \mathrm{id}_C$ is also a k-coalgebra homomorphism (because a tensor product of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism).

Since $\mathrm{kan}_{H\otimes k,H}$, $\mathrm{id}_H \otimes \varepsilon_C$, T_{f*g}, $\eta_H \otimes \mathrm{id}_C$ and $\mathrm{kan}_{C,k\otimes C}$ are k-coalgebra homomorphisms, the map $\mathrm{kan}_{H\otimes k,H} \circ (\mathrm{id}_H \otimes \varepsilon_C) \circ T_{f*g} \circ (\eta_H \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C}$ is also a k-coalgebra homomorphism (because a composition of k-coalgebra homomorphisms must always be a k-coalgebra homomorphism).

Proposition 23.4 **(h)** (applied to H and $f * g$ instead of A and f) yields

$$\mathrm{kan}_{H\otimes k,H} \circ (\mathrm{id}_H \otimes \varepsilon_C) \circ T_{f*g} \circ (\eta_H \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C} = f * g.$$

Thus, $f * g$ is a k-coalgebra homomorphism (since we know that $\mathrm{kan}_{H\otimes k,H} \circ (\mathrm{id}_H \otimes \varepsilon_C) \circ T_{f*g} \circ (\eta_H \otimes \mathrm{id}_C) \circ \mathrm{kan}_{C,k\otimes C}$ is a k-coalgebra homomorphism). Proposition 10.1 is thus proven. □

A similar argument allows us to construct a new proof of Proposition 15.15. The analogue of Lemma 23.5 now takes the following form:

Lemma 23.6. Let k be a field. Let A be a commutative k-algebra. Then, μ_A is a k-algebra homomorphism from $A \otimes A$ to A, and η_A is a k-algebra homomorphism from A to k.

Proof of Lemma 23.6. Every $a \in A$, $b \in A$, $c \in A$ and $d \in A$ satisfy

$$\begin{aligned}
&(\mu_A \circ \mu_{A\otimes A})(a \otimes b \otimes c \otimes d) \\
&= \mu_A \underbrace{(\mu_{A\otimes A}(a \otimes b \otimes c \otimes d))}_{\substack{=(a\otimes b)\cdot(c\otimes d) \\ \text{(by the definition of } \mu_{A\otimes A}\text{)}}} = \mu_A \underbrace{((a \otimes b) \cdot (c \otimes d))}_{\substack{=ac\otimes bd \\ \text{(by the definition of the } k\text{-algebra } A\otimes A\text{)}}} \\
&= \mu_A(ac \otimes bd) = (ac)(bd) \qquad \text{(by the definition of } \mu_A\text{)} \\
&= acbd = abcd \qquad \text{(since } A \text{ is commutative)}
\end{aligned}$$

and

$$\begin{aligned}
&(\mu_A \circ (\mu_A \otimes \mu_A))(a \otimes b \otimes c \otimes d) \\
&= \mu_A \underbrace{((\mu_A \otimes \mu_A)(a \otimes b \otimes c \otimes d))}_{=\mu_A(a\otimes b)\otimes\mu_A(c\otimes d)} = \mu_A \left(\underbrace{\mu_A(a \otimes b)}_{\substack{=ab \\ \text{(by the definition of } \mu_A\text{)}}} \otimes \underbrace{\mu_A(c \otimes d)}_{\substack{=cd \\ \text{(by the definition of } \mu_A\text{)}}} \right) \\
&= \mu_A(ab \otimes cd) = (ab)(cd) \qquad \text{(by the definition of } \mu_A\text{)}.
\end{aligned}$$

Thus, every $a \in A$, $b \in A$, $c \in A$ and $d \in A$ satisfy

$$\begin{aligned}
&(\mu_A \circ \mu_{A\otimes A})(a \otimes b \otimes c \otimes d) \\
&= abcd = (ab)(cd) = (\mu_A \circ (\mu_A \otimes \mu_A))(a \otimes b \otimes c \otimes d).
\end{aligned}$$

In other words, the two maps $\mu_A \circ \mu_{A \otimes A}$ and $\mu_A \circ (\mu_A \otimes \mu_A)$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $\mu_A \circ \mu_{A \otimes A} = \mu_A \circ (\mu_A \otimes \mu_A)$.

Besides, by the definition of the k-algebra $A \otimes A$, we have $1_{A \otimes A} = 1_A \otimes 1_A$, so that

$$\begin{aligned} \mu_A(1_{A \otimes A}) &= \mu_A(1_A \otimes 1_A) = 1_A \cdot 1_A \qquad \text{(by the definition of } \mu_A\text{)} \\ &= 1_A. \end{aligned}$$

Now, every $\lambda \in k$ satisfies

$$\begin{aligned} (\mu_A \circ \eta_{A \otimes A})(\lambda) &= \mu_A \underbrace{(\eta_{A \otimes A}(\lambda))}_{\substack{=\lambda \cdot 1_{A \otimes A} \\ \text{(by the definition of } \eta_{A \otimes A}\text{)}}} = \mu_A(\lambda \cdot 1_{A \otimes A}) \\ &= \lambda \cdot \underbrace{\mu_A(1_{A \otimes A})}_{=1_A} \qquad \text{(since } \mu_A \text{ is } k\text{-linear)} \\ &= \lambda \cdot 1_A = \eta_A(\lambda) \qquad \text{(since } \eta_A(\lambda) = \lambda \cdot 1_A \text{ by the definition of } \eta_A\text{)}. \end{aligned}$$

In other words, $\mu_A \circ \eta_{A \otimes A} = \eta_A$. Combined with $\mu_A \circ \mu_{A \otimes A} = \mu_A \circ (\mu_A \otimes \mu_A)$ (which we proved above), this yields that μ_A is a k-algebra homomorphism (because μ_A is a k-algebra homomorphism if and only if it satisfies $\mu_A \circ \eta_{A \otimes A} = \eta_A$ and $\mu_A \circ \mu_{A \otimes A} = \mu_A \circ (\mu_A \otimes \mu_A)$ (due to the definition of k-algebra homomorphisms using arrows)).

Now, it remains to prove that η_A is a k-algebra homomorphism.

Any $x \in k$ and $y \in k$ satisfy

$$\underbrace{\eta_A(x)}_{\substack{=x \cdot 1_A \\ \text{(by the definition} \\ \text{of } \eta_A\text{)}}} \cdot \underbrace{\eta_A(y)}_{\substack{=y \cdot 1_A \\ \text{(by the definition} \\ \text{of } \eta_A\text{)}}} = (x \cdot 1_A) \cdot (y \cdot 1_A) = xy \cdot 1_A = \eta_A(xy)$$

(since $\eta_A(xy) = xy \cdot 1_A$ (by the definition of η_A)). Combined with the fact that $\eta_A(1) = 1_A$ (because the definition of η_A yields $\eta_A(1) = 1 \cdot 1_A = 1_A$), this yields that η_A is a k-algebra homomorphism. This completes the proof of Lemma 23.6. $\square$

Alternative proof of Proposition 15.15. Applying Definition 23.3 to $C = H$, we obtain a map $T_f : A \otimes H \to A \otimes H$. Similarly, we obtain maps $T_g : A \otimes H \to A \otimes H$ and $T_{f*g} : A \otimes H \to A \otimes H$. Proposition 23.4 **(d)** (applied to H, g and f instead of C, f and g) yields $T_{f*g} = T_g \circ T_f$.

Since H is a k-bialgebra, the maps Δ_H and ε_H are k-algebra homomorphisms (by the axioms of a bialgebra).

By Lemma 23.6, the maps μ_A and η_A are k-algebra homomorphisms.

Since μ_A and id_H are k-algebra homomorphisms, the map $\mu_A \otimes \mathrm{id}_H$ is also a k-algebra homomorphism (because a tensor product of k-algebra homomorphisms must always be a k-algebra homomorphism).

Since id_A, f and id_H are k-algebra homomorphisms, the map $\mathrm{id}_A \otimes f \otimes \mathrm{id}_H$ is also a k-algebra homomorphism (because a tensor product of k-algebra homomorphisms must always be a k-algebra homomorphism).

Since id_A and Δ_H are k-algebra homomorphisms, the map $\mathrm{id}_A \otimes \Delta_H$ is also a k-algebra homomorphism (because a tensor product of k-algebra homomorphisms must always be a k-algebra homomorphism).

Since $\mu_A \otimes \mathrm{id}_H$, $\mathrm{id}_A \otimes f \otimes \mathrm{id}_H$ and $\mathrm{id}_A \otimes \Delta_H$ are k-algebra homomorphisms, the map $(\mu_A \otimes \mathrm{id}_H) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_H) \circ (\mathrm{id}_A \otimes \Delta_H)$ is also a k-algebra homomorphism (because a composition of k-algebra homomorphisms must always be a k-algebra homomorphism).

By the definition of T_f, we have

$$T_f = (\mu_A \otimes \mathrm{id}_H) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_H) \circ (\mathrm{id}_A \otimes \Delta_H).$$

Thus, T_f is a k-algebra homomorphism (because $(\mu_A \otimes \mathrm{id}_H) \circ (\mathrm{id}_A \otimes f \otimes \mathrm{id}_H) \circ (\mathrm{id}_A \otimes \Delta_H)$ is a k-algebra homomorphism). Similarly, T_g is a k-algebra homomorphism.

Since T_g and T_f are k-algebra homomorphisms, the map $T_g \circ T_f$ is also a k-algebra homomorphism (because a composition of k-algebra homomorphisms must always be a k-algebra homomorphism). Since $T_g \circ T_f = T_{f*g}$, this rewrites as follows: The map T_{f*g} is a k-algebra homomorphism.

Let $\mathrm{kan}_{H,k\otimes H} : H \to k \otimes H$ be the canonical isomorphism which sends c to $1 \otimes c$ for every $c \in H$. Let $\mathrm{kan}_{A\otimes k,A} : A \otimes k \to A$ be the canonical isomorphism which sends $a \otimes \lambda$ to λa for every $(a, \lambda) \in A \times k$. Both $\mathrm{kan}_{H,k\otimes H}$ and $\mathrm{kan}_{A\otimes k,A}$ are k-algebra homomorphisms.

Since id_A and ε_H are k-algebra homomorphisms, the map $\mathrm{id}_A \otimes \varepsilon_H$ is also a k-algebra homomorphism (because a tensor product of k-algebra homomorphisms must always be a k-algebra homomorphism).

Since η_A and id_H are k-algebra homomorphisms, the map $\eta_A \otimes \mathrm{id}_H$ is also a k-algebra homomorphism (because a tensor product of k-algebra homomorphisms must always be a k-algebra homomorphism).

Since $\mathrm{kan}_{A\otimes k,A}$, $\mathrm{id}_A \otimes \varepsilon_H$, T_{f*g}, $\eta_A \otimes \mathrm{id}_H$ and $\mathrm{kan}_{H,k\otimes H}$ are k-algebra homomorphisms, the map $\mathrm{kan}_{A\otimes k,A} \circ (\mathrm{id}_A \otimes \varepsilon_H) \circ T_{f*g} \circ (\eta_A \otimes \mathrm{id}_H) \circ \mathrm{kan}_{H,k\otimes H}$ is also a k-algebra homomorphism (because a composition of k-algebra homomorphisms must always be a k-algebra homomorphism).

Proposition 23.4 **(h)** (applied to H and $f * g$ instead of C and f) yields

$$\mathrm{kan}_{A\otimes k,A} \circ (\mathrm{id}_A \otimes \varepsilon_H) \circ T_{f*g} \circ (\eta_A \otimes \mathrm{id}_H) \circ \mathrm{kan}_{H,k\otimes H} = f * g.$$

Thus, $f * g$ is a k-algebra homomorphism (since we know that $\mathrm{kan}_{A\otimes k,A} \circ (\mathrm{id}_A \otimes \varepsilon_H) \circ T_{f*g} \circ (\eta_A \otimes \mathrm{id}_H) \circ \mathrm{kan}_{H,k\otimes H}$ is a k-algebra homomorphism). Proposition 15.15 is thus proven. □

§24. A graded comultiplication makes a coalgebra graded

Next we discuss another elementary property of coalgebras which has not much to do with what we did above. We will prove the following:

Theorem 24.1. Let k be a field. Let C be a k-coalgebra which is, at the same time, a graded k-vector space such that the underlying vector space of the k-coalgebra C is identical with the underlying vector space of the graded k-vector space C. Assume that the map $\Delta_C : C \to C \otimes C$ is graded. Then, C is a graded k-coalgebra (i. e., the map $\varepsilon_C : C \to k$ is also graded).

This is an analogue of the following well-known result about algebras:

Theorem 24.2. Let k be a field. Let A be a k-algebra which is, at the same time, a graded k-vector space such that the underlying vector space of the k-algebra A is identical with the underlying vector space of the graded k-vector space A. Assume that $A_i A_j \subseteq A_{i+j}$ for all $i \in \mathbb{N}$ and $j \in \mathbb{N}$. Then, A is a graded k-algebra (i. e., we have $1_A \in A_0$).

Proof of Theorem 24.1. Consider the k-algebra k. Clearly, $\eta_k = \mathrm{id}_k$, and the map μ_k is the canonical isomorphism $k \otimes k \to k$.

By applying Definition 1.9 to $A = k$, we obtain a convolution algebra $(\mathcal{L}(C, k), *)$. The unity of this k-algebra is $e_{k,C} = \underbrace{\eta_k}_{=\mathrm{id}_k} \circ \varepsilon_C = \varepsilon_C$.

Let us use the notations of Definition 16.16. Clearly, $\varepsilon_C \circ p_{0,C} : C \to k$ is also an element of the convolution algebra $(\mathcal{L}(C, k), *)$. Thus, $\varepsilon_C * (\varepsilon_C \circ p_{0,C}) = \varepsilon_C \circ p_{0,C}$ (since ε_C is the unity of the k-algebra $(\mathcal{L}(C, k), *)$).

We will now prove that $\varepsilon_C \circ p_{0,C} = \varepsilon_C$. This will very easily yield that ε_C is graded.

Let $\ell \in \mathbb{N}$ be arbitrary. Let $x \in C_\ell$. As in the proof of Proposition 16.6, we can show that (107) holds, i. e., that $\Delta_C(C_\ell) \subseteq \sum_{i=0}^{\ell} C_i \otimes C_{\ell-i}$. Since $x \in C_\ell$, we now have $\Delta_C(x) \in \Delta_C(C_\ell) \subseteq \sum_{i=0}^{\ell} C_i \otimes C_{\ell-i}$. Hence, there exists an $(\ell+1)$-tuple of $(t_0, t_1, \ldots, t_\ell)$ of elements of $C \otimes C$ such that $\Delta_C(x) = \sum_{i=0}^{\ell} t_i$ and such that every $i \in \{0, 1, \ldots, \ell\}$ satisfies $t_i \in C_i \otimes C_{\ell-i}$. Consider this $(\ell+1)$-tuple.

For every $i \in \{0, 1, \ldots, \ell-1\}$, we have $p_{0,C}(C_{\ell-i}) = 0$ [129] and thus

$$\begin{aligned}(\mathrm{id}_C \otimes p_{0,C})(t_i) &\in (\mathrm{id}_C \otimes p_{0,C})(C_i \otimes C_{\ell-i}) \qquad (\text{since } t_i \in C_i \otimes C_{\ell-i}) \\ &= \mathrm{id}_C(C_i) \otimes \underbrace{p_{0,C}(C_{\ell-i})}_{=0} = 0,\end{aligned}$$

so that $(\mathrm{id}_C \otimes p_{0,C})(t_i) = 0$.

On the other hand, it is easy to see that $(p_{0,C} - \mathrm{id}_C)(C_0) = 0$ [130], so that

$$\begin{aligned}(\mathrm{id}_C \otimes (p_{0,C} - \mathrm{id}_C))(t_\ell) &\in (\mathrm{id}_C \otimes (p_{0,C} - \mathrm{id}_C)) \left(C_\ell \otimes \underbrace{C_{\ell-\ell}}_{=C_0} \right) \\ &\qquad \left(\begin{array}{c} \text{since } t_\ell \in C_\ell \otimes C_{\ell-\ell} \text{ (because every} \\ i \in \{0, 1, \ldots, \ell-1\} \text{ satisfies } t_i \in C_i \otimes C_{\ell-i}) \end{array} \right) \\ &= (\mathrm{id}_C \otimes (p_{0,C} - \mathrm{id}_C))(C_\ell \otimes C_0) = \mathrm{id}_C(C_\ell) \otimes \underbrace{(p_{0,C} - \mathrm{id}_C)(C_0)}_{=0} = 0,\end{aligned}$$

[129] *Proof.* For every $i \in \{0, 1, \ldots, \ell-1\}$, we have $i \neq \ell$, thus $0 \neq \ell - i$, thus $p_{0,C}(C_{\ell-i}) = \left(p_{0,C} \mid_{C_{\ell-i}}\right)(C_{\ell-i}) = 0$ (since (111) (applied to $V = C$, $n = 0$ and $m = \ell - i$) yields $p_{0,C} \mid_{C_{\ell-i}} = 0$), qed.

[130] *Proof.* Since $p_{0,C} \mid_{C_0} = \mathrm{id}_C \mid_{C_0}$ (by (110), applied to $V = C$ and $n = 0$), we have

$$(p_{0,C} - \mathrm{id}_C) \mid_{C_0} = \underbrace{p_{0,C} \mid_{C_0}}_{=\mathrm{id}_C \mid_{C_0}} - \mathrm{id}_C \mid_{C_0} = \mathrm{id}_C \mid_{C_0} - \mathrm{id}_C \mid_{C_0} = 0,$$

so that $(p_{0,C} - \mathrm{id}_C)(C_0) = \underbrace{\left((p_{0,C} - \mathrm{id}_C) \mid_{C_0}\right)}_{=0}(C_0) = 0$, qed.

so that $\left(\mathrm{id}_C \otimes \left(p_{0,C} - \mathrm{id}_C\right)\right)\left(t_\ell\right) = 0$.

From $\Delta_C\left(x\right) = \sum\limits_{i=0}^{\ell} t_i$, we conclude that

$$\begin{aligned}
\left(\mathrm{id}_C \otimes p_{0,C}\right)\left(\Delta_C\left(x\right)\right) &= \left(\mathrm{id}_C \otimes p_{0,C}\right)\left(\sum_{i=0}^{\ell} t_i\right) = \sum_{i=0}^{\ell}\left(\mathrm{id}_C \otimes p_{0,C}\right)\left(t_i\right) \\
&\qquad \left(\text{since } \mathrm{id}_C \otimes p_{0,C} \text{ is } k\text{-linear}\right) \\
&= \sum_{i=0}^{\ell-1} \underbrace{\left(\mathrm{id}_C \otimes p_{0,C}\right)\left(t_i\right)}_{\substack{=0 \\ \left(\text{since we know that } \left(\mathrm{id}_C \otimes p_{0,C}\right)\left(t_i\right)=0 \right. \\ \left. \text{for every } i \in \{0,1,\ldots,\ell-1\}\right)}} + \left(\mathrm{id}_C \otimes \underbrace{p_{0,C}}_{=\mathrm{id}_C + \left(p_{0,C} - \mathrm{id}_C\right)}\right)\left(t_\ell\right) \\
&= \underbrace{\sum_{i=0}^{\ell-1}}_{=0} 0 + \left(\mathrm{id}_C \otimes \left(\mathrm{id}_C + \left(p_{0,C} - \mathrm{id}_C\right)\right)\right)\left(t_\ell\right) \\
&= \underbrace{\left(\mathrm{id}_C \otimes \left(\mathrm{id}_C + \left(p_{0,C} - \mathrm{id}_C\right)\right)\right)}_{\substack{= \mathrm{id}_C \otimes \mathrm{id}_C + \mathrm{id}_C \otimes \left(p_{0,C} - \mathrm{id}_C\right) \\ \left(\text{since tensoring of } k\text{-linear maps is } k\text{-bilinear}\right)}}\left(t_\ell\right) \\
&= \left(\underbrace{\mathrm{id}_C \otimes \mathrm{id}_C}_{=\mathrm{id}_{C \otimes C}} + \mathrm{id}_C \otimes \left(p_{0,C} - \mathrm{id}_C\right)\right)\left(t_\ell\right) = \left(\mathrm{id}_{C \otimes C} + \mathrm{id}_C \otimes \left(p_{0,C} - \mathrm{id}_C\right)\right)\left(t_\ell\right) \\
&= \underbrace{\mathrm{id}_{C \otimes C}\left(t_\ell\right)}_{=t_\ell} + \underbrace{\left(\mathrm{id}_C \otimes \left(p_{0,C} - \mathrm{id}_C\right)\right)\left(t_\ell\right)}_{=0} = t_\ell + 0 = t_\ell. \qquad (226)
\end{aligned}$$

On the other hand, let kan denote the canonical isomorphism $C \otimes k \to C$ which sends $c \otimes \lambda$ to λc for every $(c, \lambda) \in C \times k$. Then, clearly, kan^{-1} is the isomorphism $C \to C \otimes k$ which sends every $\xi \in C$ to $\xi \otimes 1$.

Every $i \in \{0, 1, \ldots, \ell\}$ satisfies

$$\begin{aligned}
\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right) &\in \left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(C_i \otimes C_{\ell-i}\right) \qquad \left(\text{since } t_i \in C_i \otimes C_{\ell-i}\right) \\
&= \underbrace{\mathrm{id}_C\left(C_i\right)}_{=C_i} \otimes \underbrace{\varepsilon_C\left(C_{\ell-i}\right)}_{\subseteq k} \subseteq C_i \otimes k = \left(C \otimes k\right)_i,
\end{aligned}$$

and thus

$$\mathrm{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right) \in \mathrm{kan}\left(\left(C \otimes k\right)_i\right) \subseteq C_i \qquad \left(\text{since kan is a graded map}\right). \quad (227)$$

But every $i \in \{0, 1, \ldots, \ell - 1\}$ satisfies $p_{\ell,C}\left(C_i\right) = 0$ [131] and thus $p_{\ell,C}\left(\underbrace{\mathrm{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right)}_{\substack{\in C_i \\ \text{(by (227))}}}\right) \in$ $p_{\ell,C}\left(C_i\right) = 0$, so that

$$p_{\ell,C}\left(\mathrm{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right)\right) = 0. \qquad (228)$$

[131] *Proof.* For every $i \in \{0, 1, \ldots, \ell - 1\}$, we have $\ell \neq i$, and thus $p_{\ell,C}\left(C_i\right) = \left(p_{\ell,C} \mid_{C_i}\right)\left(C_i\right) = 0$ (since (111) (applied to $V = C$, $n = \ell$ and $m = i$) yields $p_{\ell,C} \mid_{C_i} = 0$), qed.

On the other hand, (227) (applied to $i = \ell$) yields $\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right) \in C_\ell$, so that

$$\begin{aligned} p_{\ell,C}\left(\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right)\right) &= \underbrace{\left(p_{\ell,C} \mid_{C_\ell}\right)}_{\substack{=\mathrm{id}_C \mid_{C_\ell} \\ \text{(by (110), applied to } V=C \text{ and } n=\ell)}} \left(\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right)\right) \\ &= \left(\mathrm{id}_C \mid_{C_\ell}\right)\left(\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right)\right) \\ &= \operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right). \end{aligned} \tag{229}$$

Now, since C is a k-coalgebra, we have $\operatorname{kan} \circ \left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \Delta_C = \mathrm{id}_C$ (by the axioms of a k-coalgebra), so that $\left(\operatorname{kan} \circ \left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \Delta_C\right)(x) = \mathrm{id}_C(x) = x$. Thus,

$$x = \left(\operatorname{kan} \circ \left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \Delta_C\right)(x) = \left(\operatorname{kan} \circ \left(\mathrm{id}_C \otimes \varepsilon_C\right)\right) \underbrace{\left(\Delta_C(x)\right)}_{=\sum_{i=0}^{\ell} t_i} = \left(\operatorname{kan} \circ \left(\mathrm{id}_C \otimes \varepsilon_C\right)\right)\left(\sum_{i=0}^{\ell} t_i\right)$$

$$= \sum_{i=0}^{\ell} \underbrace{\left(\operatorname{kan} \circ \left(\mathrm{id}_C \otimes \varepsilon_C\right)\right)\left(t_i\right)}_{=\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right)} \qquad \left(\text{since } \operatorname{kan} \circ \left(\mathrm{id}_C \otimes \varepsilon_C\right) \text{ is } k\text{-linear}\right)$$

$$= \sum_{i=0}^{\ell} \operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right).$$

Hence,

$$\begin{aligned} p_{\ell,C}(x) &= p_{\ell,C}\left(\sum_{i=0}^{\ell} \operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right)\right) \\ &= \sum_{i=0}^{\ell} p_{\ell,C}\left(\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right)\right) \qquad \left(\text{since } p_{\ell,C} \text{ is } k\text{-linear}\right) \\ &= \sum_{i=0}^{\ell-1} \underbrace{p_{\ell,C}\left(\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_i\right)\right)\right)}_{\substack{=0 \\ \text{(by (228))}}} + \underbrace{p_{\ell,C}\left(\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right)\right)}_{\substack{=\operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right) \\ \text{(by (229))}}} \\ &= \underbrace{\sum_{i=0}^{\ell-1} 0}_{=0} + \operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right) = \operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right). \end{aligned} \tag{230}$$

Since $p_{\ell,C} \mid_{C_\ell} = \mathrm{id}_C \mid_{C_\ell}$ (by (110), applied to $V = C$ and $n = \ell$), we have $\left(p_{\ell,C} \mid_{C_\ell}\right)(x) = \left(\mathrm{id}_C \mid_{C_\ell}\right)(x) = x$, so that $p_{\ell,C}(x) = \left(p_{\ell,C} \mid_{C_\ell}\right)(x) = x$. Thus, (230) rewrites as

$$\begin{aligned} x = \operatorname{kan}\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(t_\ell\right)\right) &= \operatorname{kan}\left(\underbrace{\left(\mathrm{id}_C \otimes \varepsilon_C\right)\left(\left(\mathrm{id}_C \otimes p_{0,C}\right)\left(\Delta_C(x)\right)\right)}_{=\left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \left(\mathrm{id}_C \otimes p_{0,C}\right) \circ \Delta_C}\right) \\ &\qquad \left(\text{since } t_\ell = \left(\mathrm{id}_C \otimes p_{0,C}\right)\left(\Delta_C(x)\right) \text{ by (226)}\right) \\ &= \operatorname{kan}\left(\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \left(\mathrm{id}_C \otimes p_{0,C}\right) \circ \Delta_C\right)(x)\right). \end{aligned}$$

Since kan is an isomorphism, this rewrites as

$$\left(\left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \left(\mathrm{id}_C \otimes p_{0,C}\right) \circ \Delta_C\right)(x) = \mathrm{kan}^{-1}(x) = x \otimes 1 \tag{231}$$

(because kan^{-1} is the isomorphism $C \to C \otimes k$ which sends every $\xi \in C$ to $\xi \otimes 1$). Now it is easy to see that $\mathrm{id}_C \otimes (\varepsilon_C \circ p_{0,C}) = (\mathrm{id}_C \otimes \varepsilon_C) \circ (\mathrm{id}_C \otimes p_{0,C})$ [132]. Hence,

$$\begin{aligned}\left(\underbrace{\left(\mathrm{id}_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right)}_{=\left(\mathrm{id}_C \otimes \varepsilon_C\right)\circ\left(\mathrm{id}_C \otimes p_{0,C}\right)} \circ \Delta_C\right)(x) &= \left(\left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \left(\mathrm{id}_C \otimes p_{0,C}\right) \circ \Delta_C\right)(x) \\ &= x \otimes 1 \qquad \text{(by (231))},\end{aligned}$$

so that

$$\left(\varepsilon_C \otimes \mathrm{id}_k\right)\left(\left(\left(\mathrm{id}_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right) \circ \Delta_C\right)(x)\right) = \left(\varepsilon_C \otimes \mathrm{id}_k\right)(x \otimes 1) = \varepsilon_C(x) \otimes \underbrace{\mathrm{id}_k(1)}_{=1} = \varepsilon_C(x) \otimes 1.$$

This rewrites as

$$\begin{aligned}\varepsilon_C(x) \otimes 1 &= \left(\varepsilon_C \otimes \mathrm{id}_k\right)\left(\left(\left(\mathrm{id}_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right) \circ \Delta_C\right)(x)\right) \\ &= \left(\begin{array}{c}\underbrace{\left(\varepsilon_C \otimes \mathrm{id}_k\right) \circ \left(\mathrm{id}_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right)}_{=\left(\varepsilon_C \circ \mathrm{id}_C\right)\otimes\left(\mathrm{id}_k \circ \varepsilon_C \circ p_{0,C}\right)} \\ \text{(because (21) (applied to } U=C,\ V=C,\ W=k,\ U'=C,\ V'=k,\ W'=k, \\ \alpha=\mathrm{id}_C,\ \beta=\varepsilon_C,\ \alpha'=\varepsilon_C \circ p_{0,C} \text{ and } \beta'=\mathrm{id}_k\text{) yields} \\ \left(\varepsilon_C \circ \mathrm{id}_C\right)\otimes\left(\mathrm{id}_k \circ \varepsilon_C \circ p_{0,C}\right) = \left(\varepsilon_C \otimes \mathrm{id}_k\right)\circ\left(\mathrm{id}_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right)\end{array} \circ \Delta_C\right)(x) \\ &= \left(\left(\underbrace{\left(\varepsilon_C \circ \mathrm{id}_C\right)}_{=\varepsilon_C} \otimes \underbrace{\left(\mathrm{id}_k \circ \varepsilon_C \circ p_{0,C}\right)}_{=\varepsilon_C \circ p_{0,C}}\right) \circ \Delta_C\right)(x) \\ &= \left(\left(\varepsilon_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right) \circ \Delta_C\right)(x). \end{aligned} \tag{232}$$

But by the definition of convolution, we have $\varepsilon_C * (\varepsilon_C \circ p_{0,C}) = \mu_k \circ (\varepsilon_C \otimes (\varepsilon_C \circ p_{0,C})) \circ \Delta_C$, so that

$$\begin{aligned}\left(\varepsilon_C * \left(\varepsilon_C \circ p_{0,C}\right)\right)(x) &= \left(\mu_k \circ \left(\varepsilon_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right) \circ \Delta_C\right)(x) \\ &= \mu_k \underbrace{\left(\left(\left(\varepsilon_C \otimes \left(\varepsilon_C \circ p_{0,C}\right)\right) \circ \Delta_C\right)(x)\right)}_{\substack{=\varepsilon_C(x)\otimes 1 \\ \text{(by (232))}}} \\ &= \mu_k\left(\varepsilon_C(x) \otimes 1\right) = \varepsilon_C(x) \cdot 1 \qquad \text{(by the definition of } \mu_k\text{)} \\ &= \varepsilon_C(x).\end{aligned}$$

[132] *Proof.* By (21) (applied to $U = C$, $V = C$, $W = C$, $U' = C$, $V' = C$, $W' = k$, $\alpha = \mathrm{id}_C$, $\beta = \mathrm{id}_C$, $\alpha' = p_{0,C}$ and $\beta' = \varepsilon_C$), we have $(\mathrm{id}_C \circ \mathrm{id}_C) \otimes (\varepsilon_C \circ p_{0,C}) = (\mathrm{id}_C \otimes \varepsilon_C) \circ (\mathrm{id}_C \otimes p_{0,C})$, so that

$$\left(\mathrm{id}_C \otimes \varepsilon_C\right) \circ \left(\mathrm{id}_C \otimes p_{0,C}\right) = \underbrace{\left(\mathrm{id}_C \circ \mathrm{id}_C\right)}_{=\mathrm{id}_C} \otimes \left(\varepsilon_C \circ p_{0,C}\right) = \mathrm{id}_C \otimes \left(\varepsilon_C \circ p_{0,C}\right),$$

qed.

Thus,

$$\varepsilon_C(x) = (\varepsilon_C * (\varepsilon_C \circ p_{0,C}))(x) = (\varepsilon_C \circ p_{0,C})(x)$$
$$\left(\begin{array}{c} \text{since } \varepsilon_C \text{ is the unity of the } k\text{-algebra } (\mathcal{L}(C,k), *), \text{ and thus satisfies} \\ \varepsilon_C * (\varepsilon_C \circ p_{0,C}) = \varepsilon_C \circ p_{0,C} \end{array} \right).$$

Now forget that we fixed x. We thus have shown that

$$\varepsilon_C(x) = (\varepsilon_C \circ p_{0,C})(x) \qquad \text{for every } x \in C_\ell. \tag{233}$$

Now, it is very easy to see that $\varepsilon_C(C_\ell) \subseteq k_\ell$ [133].

Now forget that we fixed ℓ. We thus have shown that $\varepsilon_C(C_\ell) \subseteq k_\ell$ for every $\ell \in \mathbb{N}$. In other words, ε_C is a graded map. Combined with the fact that Δ_C is a graded map, this yields that C is a graded k-coalgebra. Theorem 24.1 is thus proven. □

§25. $*$-inverses of coalgebra homomorphisms

In §23, we extended Proposition 16.18 **(c)** to the case of negative n whenever f is $*$-invertible. This extension (which we formulated as Proposition 23.4) was proven using Proposition 23.4 (particularly, parts **(g)** and **(h)**) as the main ingredient. Let us now, in a similar manner, extend Corollary 10.2 to the case of negative n whenever f is $*$-invertible:

Proposition 25.1. Let k be a field. Let C be a cocommutative k-coalgebra. Let H be a k-bialgebra. Let $f : C \to H$ be a $*$-invertible k-coalgebra homomorphism.

(a) Then, $f^{*(-1)} : C \to H$ is also a k-coalgebra homomorphism.

(b) Let $n \in \mathbb{Z}$. Then, $f^{*n} : C \to H$ is also a k-coalgebra homomorphism.

Our goal here is not just to prove Proposition 25.1; in fact, that would be pretty easy: Proposition 25.1 **(a)** can be proven with the help of Proposition 23.4 in the same way as we proved Proposition 10.1 in §24 with the help of Proposition 23.4. And Proposition 25.1 **(b)** is a quick corollary of Proposition 25.1 **(a)**. But instead of doing this proof, we will show something more general than Proposition 25.1:

[133] *Proof.* We distinguish between two cases:

Case 1: We have $\ell = 0$.

Case 2: We have $\ell \neq 0$.

Let us consider Case 1 first. In this case, $\ell = 0$, so that $k_\ell = k_0 = k$ (because this is how the grading on k is defined), so that $\varepsilon_C(C_\ell) \subseteq k = k_\ell$. Thus, $\varepsilon_C(C_\ell) \subseteq k_\ell$ is proven in Case 1.

Next, let us consider Case 2. In this case, $\ell \neq 0$, thus $0 \neq \ell$, so that $p_{0,C}\mid_{C_\ell} = 0$ (by (111) (applied to $V = C$, $n = 0$ and $m = \ell$)), so that every $x \in C_\ell$ satisfies $p_{0,C}(x) = \underbrace{(p_{0,C}\mid_{C_\ell})}_{=0}(x) = 0$. Thus, every $x \in C_\ell$ satisfies

$$\begin{aligned} \varepsilon_C(x) &= (\varepsilon_C \circ p_{0,C})(x) \qquad \text{(by (233))} \\ &= \varepsilon_C\underbrace{(p_{0,C}(x))}_{=0} = \varepsilon_C(0) = 0 \qquad \text{(since } \varepsilon_C \text{ is } k\text{-linear)} \\ &\in k_\ell. \end{aligned}$$

In other words, $\varepsilon_C(C_\ell) \subseteq k_\ell$. We thus have proven $\varepsilon_C(C_\ell) \subseteq k_\ell$ in Case 2.

Hence, $\varepsilon_C(C_\ell) \subseteq k_\ell$ is proven in both possible cases. Thus, $\varepsilon_C(C_\ell) \subseteq k_\ell$ always holds, qed.

Proposition 25.2. Let k be a field. Let C be a k-coalgebra. Let A be a k-bialgebra. Let $f : C \to A$ be a $*$-invertible k-coalgebra homomorphism. Then, $f^{*(-1)}$ is a k-coalgebra homomorphism from C^{cop} to A.

Here, we are using the following definition:

Definition 25.3. Let k be a field. Let C be a k-coalgebra. The *coopposite coalgebra* of C is defined to be the k-coalgebra $(C, \tau_{C,C} \circ \Delta_C, \varepsilon_C)$ (this is easily seen to be a k-coalgebra), and denoted by C^{cop}.

Note that Proposition 25.2 cannot be easily derived from Proposition 23.4 anymore (mainly because there is no generalization of Lemma 23.5 to non-cocommutative coalgebras C).

Before we prove Proposition 25.2, let us show how Proposition 25.1 can be derived from it:

Proof of Proposition 25.1. **(a)** Since C is cocommutative, we have $\tau_{C,C} \circ \Delta_C = \Delta_C$. By the definition of C^{cop}, we have $C^{\mathrm{cop}} = \left(C, \underbrace{\tau_{C,C} \circ \Delta_C}_{=\Delta_C}, \varepsilon_C\right) = (C, \Delta_C, \varepsilon_C) = C$. By Proposition 25.2 (applied to $A = H$), we know that $f^{*(-1)}$ is a k-coalgebra homomorphism from C^{cop} to H. Since $C^{\mathrm{cop}} = C$, this rewrites as follows: $f^{*(-1)}$ is a k-coalgebra homomorphism from C to H. This proves Proposition 25.1 **(a)**.

(b) Let us first check that, for every $m \in \mathbb{N}$,

$$\text{the map } f^{*(-m)} : C \to H \text{ is a } k\text{-coalgebra homomorphism.} \tag{234}$$

Proof of (234): We will prove (234) by induction over m:

Induction base: From the proof of Corollary 10.2, we know that f^{*0} is a k-coalgebra homomorphism. In other words, $f^{*(-0)}$ is a k-coalgebra homomorphism (since $0 = -0$). In other words, (234) holds for $m = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that (234) holds for $m = N$. We must now prove that (234) also holds for $m = N + 1$.

Since (234) holds for $m = N$, we know that $f^{*(-N)}$ is a k-coalgebra homomorphism. Proposition 10.1 (applied to $f^{*(-1)}$ and $f^{*(-N)}$ instead of f and g) now yields that $f^{*(-1)} * f^{*(-N)}$ is a k-coalgebra homomorphism (because we know from Proposition 25.1 **(a)** that $f^{*(-1)}$ is a k-coalgebra homomorphism). Since $f^{*(-1)} * f^{*(-N)} = f^{*(-(N+1))}$, this yields that $f^{*(-(N+1))}$ is a k-coalgebra homomorphism. In other words, (234) holds for $m = N + 1$. This completes the induction step. The induction proof of (234) is thus complete.

Now, let us distinguish between two cases:

Case 1: We have $n \geq 0$.

Case 2: We have $n < 0$.

Let us consider Case 1 first. In this case, $n \geq 0$, so that $n \in \mathbb{N}$, and thus Corollary 10.2 shows that $f^{*n} : C \to H$ is a k-coalgebra homomorphism. Hence, Proposition 25.1 **(b)** is proven in Case 1.

Now, let us consider Case 2. In this case, $n < 0$, so that $-n > 0$ and thus $-n \in \mathbb{N}$. Hence, (234) (applied to $m = -n$) yields that the map $f^{*(-(-n))} : C \to H$ is a k-coalgebra homomorphism. Since $-(-n) = n$, this rewrites as follows: The map

$f^{*n} : C \to H$ is a k-coalgebra homomorphism. Thus, Proposition 25.1 **(b)** is proven in Case 2.

Hence, Proposition 25.1 **(b)** is proven in each of the cases 1 and 2. Since these two cases cover all possibilities, this yields that Proposition 25.1 **(b)** always holds. The proof of Proposition 25.1 **(b)** is thus complete (up to proving Proposition 25.2). $\square$

Let us show another consequence of Proposition 25.2:

Proposition 25.4. Let k be a field. Let H be a k-Hopf algebra. Then, the antipode of H is a k-coalgebra homomorphism from H^{cop} to H.

Proof of Proposition 25.4. The antipode of H is the $*$-inverse of the identity map $\mathrm{id}_H : H \to H$ (by the definition of the antipode of a Hopf algebra). In other words, the antipode of H is the map $\mathrm{id}_H^{*(-1)}$. In particular, this yields that the map id_H is $*$-invertible. Thus, Proposition 25.2 (applied to $C = H$, $A = H$ and $f = \mathrm{id}_H$) yields that $\mathrm{id}_H^{*(-1)}$ is a k-coalgebra homomorphism from H^{cop} to H. Since $\mathrm{id}_H^{*(-1)}$ is the antipode of H, this rewrites as follows: The antipode of H is a k-coalgebra homomorphism from H^{cop} to H. This proves Proposition 25.4. $\square$

Let us now prepare for proving Proposition 25.2. Our proof will involve lengthy computations, but we can simplify them by showing some lemmas first:

Lemma 25.5. Let k be a field. Let U, V and W be three k-vector spaces. Then,

$$(\mathrm{id}_V \otimes \tau_{U,W}) \circ (\tau_{U,V} \otimes \mathrm{id}_W) = \tau_{U,V\otimes W}.$$

Proof of Lemma 25.5. Every $u \in U$, $v \in V$ and $w \in W$ satisfy

$$\begin{aligned}
&((\mathrm{id}_V \otimes \tau_{U,W}) \circ (\tau_{U,V} \otimes \mathrm{id}_W))(u \otimes v \otimes w) \\
&= (\mathrm{id}_V \otimes \tau_{U,W}) \underbrace{((\tau_{U,V} \otimes \mathrm{id}_W)(u \otimes v \otimes w))}_{= \tau_{U,V}(u\otimes v)\otimes \mathrm{id}_W(w)} \\
&= (\mathrm{id}_V \otimes \tau_{U,W}) \left(\underbrace{\tau_{U,V}(u \otimes v)}_{\substack{= v\otimes u \\ (\text{by the definition of } \tau_{U,V})}} \otimes \underbrace{\mathrm{id}_W(w)}_{= w} \right) \\
&= (\mathrm{id}_V \otimes \tau_{U,W})(v \otimes u \otimes w) = \underbrace{\mathrm{id}_V(v)}_{= v} \otimes \underbrace{\tau_{U,W}(u \otimes w)}_{\substack{= w\otimes u \\ (\text{by the definition of } \tau_{U,W})}} \\
&= v \otimes w \otimes u = \tau_{U,V\otimes W}(u \otimes v \otimes w) \\
&\qquad (\text{since } \tau_{U,V\otimes W}(u \otimes v \otimes w) = v \otimes w \otimes u \text{ by the definition of } \tau_{U,V\otimes W}).
\end{aligned}$$

In other words, the two maps $(\mathrm{id}_V \otimes \tau_{U,W}) \circ (\tau_{U,V} \otimes \mathrm{id}_W)$ and $\tau_{U,V\otimes W}$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $(\mathrm{id}_V \otimes \tau_{U,W}) \circ (\tau_{U,V} \otimes \mathrm{id}_W) = \tau_{U,V\otimes W}$. This proves Lemma 25.5. $\square$

Lemma 25.6. Let k be a field. Let U, V, W, T and Q be five k-vector spaces. Let $r : Q \to V \otimes W$ be a k-linear map. Then,

$$\begin{aligned}&(\mathrm{id}_V \otimes \tau_{U,W} \otimes \mathrm{id}_T) \circ (\tau_{U,V} \otimes \mathrm{id}_W \otimes \mathrm{id}_T) \circ (\mathrm{id}_U \otimes r \otimes \mathrm{id}_T)\\ &= (r \otimes \mathrm{id}_U \otimes \mathrm{id}_T) \circ (\tau_{U,Q} \otimes \mathrm{id}_T)\,.\end{aligned}$$

Proof of Lemma 25.6. By (21) (applied to $U \otimes V \otimes W$, $V \otimes U \otimes W$, $V \otimes W \otimes U$, T, T, T, $\tau_{U,V} \otimes \mathrm{id}_W$, $\mathrm{id}_V \otimes \tau_{U,W}$, id_T, id_T instead of U, V, W, U', V', W', α, β, α', β'), we have

$$((\mathrm{id}_V \otimes \tau_{U,W}) \circ (\tau_{U,V} \otimes \mathrm{id}_W)) \otimes (\mathrm{id}_T \circ \mathrm{id}_T) = (\mathrm{id}_V \otimes \tau_{U,W} \otimes \mathrm{id}_T) \circ (\tau_{U,V} \otimes \mathrm{id}_W \otimes \mathrm{id}_T)\,.$$

Thus,

$$\begin{aligned}&(\mathrm{id}_V \otimes \tau_{U,W} \otimes \mathrm{id}_T) \circ (\tau_{U,V} \otimes \mathrm{id}_W \otimes \mathrm{id}_T)\\ &= \underbrace{((\mathrm{id}_V \otimes \tau_{U,W}) \circ (\tau_{U,V} \otimes \mathrm{id}_W))}_{\substack{=\tau_{U,V\otimes W}\\ \text{(by Lemma 25.5)}}} \otimes \underbrace{(\mathrm{id}_T \circ \mathrm{id}_T)}_{=\mathrm{id}_T} = \tau_{U,V\otimes W} \otimes \mathrm{id}_T\,. \qquad (235)\end{aligned}$$

On the other hand, by (21) (applied to $U \otimes Q$, $U \otimes V \otimes W$, $V \otimes W \otimes U$, T, T, T, $\mathrm{id}_U \otimes r$, $\tau_{U,V\otimes W}$, id_T, id_T instead of U, V, W, U', V', W', α, β, α', β'), we have

$$(\tau_{U,V\otimes W} \circ (\mathrm{id}_U \otimes r)) \otimes (\mathrm{id}_T \circ \mathrm{id}_T) = (\tau_{U,V\otimes W} \otimes \mathrm{id}_T) \circ (\mathrm{id}_U \otimes r \otimes \mathrm{id}_T)\,. \qquad (236)$$

By Proposition 9.3 **(a)** (applied to U, Q, U, $V \otimes W$, id_U and r instead of V, W, V', W', f and g), we have

$$(r \otimes \mathrm{id}_U) \circ \tau_{U,Q} = \tau_{U,V\otimes W} \circ (\mathrm{id}_U \otimes r)\,. \qquad (237)$$

Besides, by (21) (applied to $U \otimes Q$, $Q \otimes U$, $V \otimes W \otimes U$, T, T, T, $\tau_{U,Q}$, $r \otimes \mathrm{id}_U$, id_T, id_T instead of U, V, W, U', V', W', α, β, α', β'), we have

$$((r \otimes \mathrm{id}_U) \circ \tau_{U,Q}) \otimes (\mathrm{id}_T \circ \mathrm{id}_T) = (r \otimes \mathrm{id}_U \otimes \mathrm{id}_T) \circ (\tau_{U,Q} \otimes \mathrm{id}_T)\,. \qquad (238)$$

Now,

$$\begin{aligned}&\underbrace{(\mathrm{id}_V \otimes \tau_{U,W} \otimes \mathrm{id}_T) \circ (\tau_{U,V} \otimes \mathrm{id}_W \otimes \mathrm{id}_T)}_{\substack{=\tau_{U,V\otimes W}\otimes \mathrm{id}_T\\ \text{(by (235))}}} \circ (\mathrm{id}_U \otimes r \otimes \mathrm{id}_T)\\ &= (\tau_{U,V\otimes W} \otimes \mathrm{id}_T) \circ (\mathrm{id}_U \otimes r \otimes \mathrm{id}_T)\\ &= \underbrace{(\tau_{U,V\otimes W} \circ (\mathrm{id}_U \otimes r))}_{\substack{=(r\otimes \mathrm{id}_U)\circ\tau_{U,Q}\\ \text{(by (237))}}} \otimes (\mathrm{id}_T \circ \mathrm{id}_T) \qquad \text{(by (236))}\\ &= ((r \otimes \mathrm{id}_U) \circ \tau_{U,Q}) \otimes (\mathrm{id}_T \circ \mathrm{id}_T) = (r \otimes \mathrm{id}_U \otimes \mathrm{id}_T) \circ (\tau_{U,Q} \otimes \mathrm{id}_T) \qquad \text{(by (238))}\,.\end{aligned}$$

This proves Lemma 25.6. □

Proof of Proposition 25.2. Let $g = f^{*(-1)}$. Then, $f * g = f * f^{*(-1)} = e_{C,A}$ and $g * f = f^{*(-1)} * f = e_{C,A}$.

We are now going to show that

$$((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * (\Delta_A \circ f) = e_{C, A \otimes A} \tag{239}$$

and

$$(\Delta_A \circ f) * (\Delta_A \circ g) = e_{C, A \otimes A} \tag{240}$$

(where $*$ stands for convolution of maps from C to $A \otimes A$). Once these formulas are shown, it will be easy to conclude that $(g \otimes g) \circ \Delta_{C^{\mathrm{cop}}} = \Delta_A \circ g$, which will settle the hardest part of Proposition 25.2.

But let us prove (239) and (240) now:

Proof of (239): Since f is a k-coalgebra homomorphism, we have $\Delta_A \circ f = (f \otimes f) \circ$

Δ_C. Thus,

$$\begin{aligned}
&((g\otimes g)\circ\Delta_{C^{\mathrm{cop}}})*\underbrace{(\Delta_A\circ f)}_{=(f\otimes f)\circ\Delta_C}\\
&=((g\otimes g)\circ\Delta_{C^{\mathrm{cop}}})*((f\otimes f)\circ\Delta_C)\\
&=\underbrace{\mu_{A\otimes A}}_{\substack{=(\mu_A\otimes\mu_A)\circ\left(\mathrm{id}_A\otimes\tau_{A,A}\otimes\mathrm{id}_A\right)\\ \text{(by the definition of the } k\text{-algebra } A\otimes A)}}\circ\underbrace{(((g\otimes g)\circ\Delta_{C^{\mathrm{cop}}})\otimes((f\otimes f)\circ\Delta_C))}_{\substack{=(g\otimes g\otimes f\otimes f)\circ(\Delta_{C^{\mathrm{cop}}}\otimes\Delta_C)\\ \text{(by (21), applied to } C,\ C\otimes C,\ A\otimes A,\ C,\ C\otimes C,\ A\otimes A,\\ \Delta_{C^{\mathrm{cop}}},\ g\otimes g,\ \Delta_C,\ f\otimes f \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta')}}\circ\Delta_C\\
&\qquad\text{(by the definition of convolution)}\\
&=(\mu_A\otimes\mu_A)\circ\underbrace{(\mathrm{id}_A\otimes\tau_{A,A}\otimes\mathrm{id}_A)\circ(g\otimes g\otimes f\otimes f)}_{\substack{=(g\otimes f\otimes g\otimes f)\circ\left(\mathrm{id}_C\otimes\tau_{C,C}\otimes\mathrm{id}_C\right)\\ \text{(by Proposition 9.3 \textbf{(b)}, applied to } C,\ C,\ C,\ C,\\ A,\ A,\ A,\ A,\ g,\ g,\ f,\ f \text{ instead of}\\ U,\ V,\ W,\ T,\ U',\ V',\ W',\ T',\ e,\ f,\ g,\ h)}}\circ\left(\underbrace{\Delta_{C^{\mathrm{cop}}}}_{\substack{=\tau_{C,C}\circ\Delta_C\\ \text{(by the definition}\\ \text{of the}\\ k\text{-coalgebra } C^{\mathrm{cop}})}}\otimes\underbrace{\Delta_C}_{=\mathrm{id}_{C\otimes C}\circ\Delta_C}\right)\circ\Delta_C\\
&=(\mu_A\otimes\mu_A)\circ(g\otimes f\otimes g\otimes f)\circ(\mathrm{id}_C\otimes\tau_{C,C}\otimes\mathrm{id}_C)\circ\underbrace{((\tau_{C,C}\circ\Delta_C)\otimes(\mathrm{id}_{C\otimes C}\circ\Delta_C))}_{\substack{=\left(\tau_{C,C}\otimes\mathrm{id}_{C\otimes C}\right)\circ(\Delta_C\otimes\Delta_C)\\ \text{(by (21), applied to } C,\ C\otimes C,\ C\otimes C,\\ C,\ C\otimes C,\ C\otimes C,\ \Delta_C,\ \tau_{C,C},\ \Delta_C,\ \mathrm{id}_{C\otimes C}\\ \text{instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta')}}\circ\Delta_C\\
&=(\mu_A\otimes\mu_A)\circ(g\otimes f\otimes g\otimes f)\\
&\qquad\circ(\mathrm{id}_C\otimes\tau_{C,C}\otimes\mathrm{id}_C)\circ\left(\tau_{C,C}\otimes\underbrace{\mathrm{id}_{C\otimes C}}_{=\mathrm{id}_C\otimes\mathrm{id}_C}\right)\circ\underbrace{(\Delta_C\otimes\Delta_C)\circ\Delta_C}_{\substack{=(\mathrm{id}_C\otimes\Delta_C\otimes\mathrm{id}_C)\circ(\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C\\ \text{(by Lemma 9.4)}}}\\
&=(\mu_A\otimes\mu_A)\circ(g\otimes f\otimes g\otimes f)\\
&\qquad\circ\underbrace{(\mathrm{id}_C\otimes\tau_{C,C}\otimes\mathrm{id}_C)\circ(\tau_{C,C}\otimes\mathrm{id}_C\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\Delta_C\otimes\mathrm{id}_C)}_{\substack{=(\Delta_C\otimes\mathrm{id}_C\otimes\mathrm{id}_C)\circ\left(\tau_{C,C}\otimes\mathrm{id}_C\right)\\ \text{(by Lemma 25.6, applied to } U{=}C,\ V{=}C,\ W{=}C,\ T{=}C,\ Q{=}C \text{ and } r{=}\Delta_C)}}\circ(\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C\\
&=(\mu_A\otimes\mu_A)\circ(g\otimes f\otimes g\otimes f)\circ\left(\Delta_C\otimes\underbrace{\mathrm{id}_C\otimes\mathrm{id}_C}_{=\mathrm{id}_{C\otimes C}}\right)\circ(\tau_{C,C}\otimes\mathrm{id}_C)\circ(\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C\\
&=(\mu_A\otimes\mu_A)\circ(g\otimes f\otimes g\otimes f)\circ(\Delta_C\otimes\mathrm{id}_{C\otimes C})\circ(\tau_{C,C}\otimes\mathrm{id}_C)\circ(\Delta_C\otimes\mathrm{id}_C)\circ\Delta_C.
\end{aligned}\tag{241}$$

Applying (21) to $A\otimes A$, A, A, $A\otimes A$, $A\otimes A$, A, μ_A, id_A, $\mathrm{id}_{A\otimes A}$, μ_A instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mathrm{id}_A\circ\mu_A)\otimes(\mu_A\circ\mathrm{id}_{A\otimes A})=(\mathrm{id}_A\otimes\mu_A)\circ(\mu_A\otimes\mathrm{id}_{A\otimes A}).$$

Since $\mathrm{id}_A\circ\mu_A=\mu_A$ and $\mu_A\circ\mathrm{id}_{A\otimes A}=\mu_A$, this rewrites as

$$\mu_A\otimes\mu_A=(\mathrm{id}_A\otimes\mu_A)\circ(\mu_A\otimes\mathrm{id}_{A\otimes A}).\tag{242}$$

Applying (21) to $C \otimes C$, $A \otimes A$, $A \otimes A$, $C \otimes C$, $C \otimes C$, $A \otimes A$, $g \otimes f$, $\mathrm{id}_{A \otimes A}$, $\mathrm{id}_{C \otimes C}$, $g \otimes f$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mathrm{id}_{A \otimes A} \circ (g \otimes f)) \otimes ((g \otimes f) \circ \mathrm{id}_{C \otimes C}) = (\mathrm{id}_{A \otimes A} \otimes g \otimes f) \circ (g \otimes f \otimes \mathrm{id}_{C \otimes C}) .$$

Since $\mathrm{id}_{A \otimes A} \circ (g \otimes f) = g \otimes f$ and $(g \otimes f) \circ \mathrm{id}_{C \otimes C} = g \otimes f$, this rewrites as

$$g \otimes f \otimes g \otimes f = (\mathrm{id}_{A \otimes A} \otimes g \otimes f) \circ (g \otimes f \otimes \mathrm{id}_{C \otimes C}) . \tag{243}$$

By (212) (applied to $P = A \otimes A$, $Q = A$, $R = C \otimes C$, $S = A \otimes A$, $\gamma = \mu_A$ and $\delta = g \otimes f$), we have

$$(\mathrm{id}_A \otimes g \otimes f) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C}) = (\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (\mathrm{id}_{A \otimes A} \otimes g \otimes f) . \tag{244}$$

By the definition of convolution, $g * f = \mu_A \circ (g \otimes f) \circ \Delta_C$, so that

$$\mu_A \circ (g \otimes f) \circ \Delta_C = g * f = e_{C,A}. \tag{245}$$

Applying (21) to C, $C \otimes C$, $A \otimes A$, $C \otimes C$, $C \otimes C$, $C \otimes C$, Δ_C, $g \otimes f$, $\mathrm{id}_{C \otimes C}$, $\mathrm{id}_{C \otimes C}$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$((g \otimes f) \circ \Delta_C) \otimes (\mathrm{id}_{C \otimes C} \circ \mathrm{id}_{C \otimes C}) = (g \otimes f \otimes \mathrm{id}_{C \otimes C}) \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C}) .$$

Since $\mathrm{id}_{C \otimes C} \circ \mathrm{id}_{C \otimes C} = \mathrm{id}_{C \otimes C}$, this rewrites as

$$((g \otimes f) \circ \Delta_C) \otimes \mathrm{id}_{C \otimes C} = (g \otimes f \otimes \mathrm{id}_{C \otimes C}) \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C}) . \tag{246}$$

Applying (21) to C, $A \otimes A$, A, $C \otimes C$, $C \otimes C$, $C \otimes C$, $(g \otimes f) \circ \Delta_C$, μ_A, $\mathrm{id}_{C \otimes C}$, $\mathrm{id}_{C \otimes C}$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mu_A \circ (g \otimes f) \circ \Delta_C) \otimes (\mathrm{id}_{C \otimes C} \circ \mathrm{id}_{C \otimes C}) = (\mu_A \otimes \mathrm{id}_{C \otimes C}) \circ (((g \otimes f) \circ \Delta_C) \otimes \mathrm{id}_{C \otimes C}) . \tag{247}$$

Thus,

$$\begin{aligned}
&(\mu_A \otimes \mathrm{id}_{C \otimes C}) \circ \underbrace{(g \otimes f \otimes \mathrm{id}_{C \otimes C}) \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C})}_{\substack{= ((g \otimes f) \circ \Delta_C) \otimes \mathrm{id}_{C \otimes C} \\ \text{(by (246))}}} \\
&= (\mu_A \otimes \mathrm{id}_{C \otimes C}) \circ (((g \otimes f) \circ \Delta_C) \otimes \mathrm{id}_{C \otimes C}) \\
&= \underbrace{(\mu_A \circ (g \otimes f) \circ \Delta_C)}_{\substack{= e_{C,A} \\ \text{(by (245))}}} \otimes \underbrace{(\mathrm{id}_{C \otimes C} \circ \mathrm{id}_{C \otimes C})}_{= \mathrm{id}_{C \otimes C}} \qquad \text{(by (247))} \\
&= e_{C,A} \otimes \mathrm{id}_{C \otimes C} .
\end{aligned} \tag{248}$$

Now, (241) becomes

$$
\begin{aligned}
&((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * (\Delta_A \circ f) \\
&= \underbrace{(\mu_A \otimes \mu_A)}_{\substack{=(\mathrm{id}_A \otimes \mu_A) \circ (\mu_A \otimes \mathrm{id}_{A \otimes A}) \\ \text{(by (242))}}} \circ \underbrace{(g \otimes f \otimes g \otimes f)}_{\substack{=(\mathrm{id}_{A \otimes A} \otimes g \otimes f) \circ (g \otimes f \otimes \mathrm{id}_{C \otimes C}) \\ \text{(by (243))}}} \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C}) \circ (\tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C \\
&= (\mathrm{id}_A \otimes \mu_A) \circ \underbrace{(\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (\mathrm{id}_{A \otimes A} \otimes g \otimes f)}_{\substack{=(\mathrm{id}_A \otimes g \otimes f) \circ (\mu_A \otimes \mathrm{id}_{C \otimes C}) \\ \text{(by (244))}}} \circ (g \otimes f \otimes \mathrm{id}_{C \otimes C}) \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C}) \\
&\qquad \circ (\tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C \\
&= (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ \underbrace{(\mu_A \otimes \mathrm{id}_{C \otimes C}) \circ (g \otimes f \otimes \mathrm{id}_{C \otimes C}) \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C})}_{\substack{=e_{C,A} \otimes \mathrm{id}_{C \otimes C} \\ \text{(by (248))}}} \\
&\qquad \circ (\tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C \\
&= (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ \left(e_{C,A} \otimes \underbrace{\mathrm{id}_{C \otimes C}}_{=\mathrm{id}_C \otimes \mathrm{id}_C} \right) \circ (\tau_{C,C} \otimes \mathrm{id}_C) \circ \underbrace{(\Delta_C \otimes \mathrm{id}_C) \circ \Delta_C}_{\substack{=(\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C \\ \text{(by the axioms of a} \\ \text{coalgebra, since } C \text{ is} \\ \text{a coalgebra)}}} \\
&= (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ (e_{C,A} \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\tau_{C,C} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C) \circ \Delta_C .
\end{aligned}
\tag{249}
$$

On the other hand, Proposition 9.3 **(a)** (applied to C, C, C, A, id_C, $e_{C,A}$ instead of V, W, V', W', f, g) yields

$$
(e_{C,A} \otimes \mathrm{id}_C) \circ \tau_{C,C} = \tau_{C,A} \circ (\mathrm{id}_C \otimes e_{C,A}) . \tag{250}
$$

But applying (21) to $C \otimes C$, $C \otimes C$, $A \otimes C$, C, C, C, $\tau_{C,C}$, $e_{C,A} \otimes \mathrm{id}_C$, id_C, id_C instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$
((e_{C,A} \otimes \mathrm{id}_C) \circ \tau_{C,C}) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) = (e_{C,A} \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\tau_{C,C} \otimes \mathrm{id}_C) .
$$

Thus,

$$
\begin{aligned}
&(e_{C,A} \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\tau_{C,C} \otimes \mathrm{id}_C) \\
&= \underbrace{((e_{C,A} \otimes \mathrm{id}_C) \circ \tau_{C,C})}_{\substack{=\tau_{C,A} \circ \left(\mathrm{id}_C \otimes e_{C,A}\right) \\ \text{(by (250))}}} \otimes (\mathrm{id}_C \circ \mathrm{id}_C) = (\tau_{C,A} \circ (\mathrm{id}_C \otimes e_{C,A})) \otimes (\mathrm{id}_C \circ \mathrm{id}_C) \\
&= (\tau_{C,A} \otimes \mathrm{id}_C) \circ \left(\mathrm{id}_C \otimes \underbrace{e_{C,A}}_{\substack{=\eta_A \circ \varepsilon_C \\ \text{(by the definition of } e_{C,A}\text{)}}} \otimes \mathrm{id}_C \right) \\
&\qquad \left(\begin{array}{c} \text{by (21), applied to } C \otimes C,\ C \otimes A,\ A \otimes C,\ C,\ C,\ C,\ \mathrm{id}_C \otimes e_{C,A},\ \tau_{C,A},\ \mathrm{id}_C ,\ \mathrm{id}_C \\ \text{instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta' \end{array} \right) \\
&= (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes (\eta_A \circ \varepsilon_C) \otimes \mathrm{id}_C) .
\end{aligned}
\tag{251}
$$

But (211) (applied to $P = C$, $Q = C$, $R_1 = C$, $R_2 = k$, $R_3 = A$, $\varphi = \varepsilon_C$ and $\psi = \eta_A$) yields

$$(\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \varepsilon_C \otimes \mathrm{id}_C) = \mathrm{id}_C \otimes (\eta_A \circ \varepsilon_C) \otimes \mathrm{id}_C \,. \tag{252}$$

Hence, (251) becomes

$$\begin{aligned}
&(e_{C,A} \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\tau_{C,C} \otimes \mathrm{id}_C) \\
&= (\tau_{C,A} \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_C \otimes (\eta_A \circ \varepsilon_C) \otimes \mathrm{id}_C)}_{\substack{= (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \varepsilon_C \otimes \mathrm{id}_C) \\ \text{(by (252))}}} \\
&= (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \varepsilon_C \otimes \mathrm{id}_C) \,.
\end{aligned} \tag{253}$$

Now, let $\mathrm{kan}_{C,k\otimes C}$ be the canonical isomorphism $C \to k \otimes C$ which sends every $c \in C$ to $1 \otimes c \in k \otimes C$. Then, by the axioms of a coalgebra, we have $(\varepsilon_C \otimes \mathrm{id}_C) \circ \Delta_C = \mathrm{kan}_{C,k\otimes C}$ (since C is a k-coalgebra).

Applying (21) to C, C, C, C, $C \otimes C$, $k \otimes C$, id_C, id_C, Δ_C, $\varepsilon_C \otimes \mathrm{id}_C$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mathrm{id}_C \circ \mathrm{id}_C) \otimes ((\varepsilon_C \otimes \mathrm{id}_C) \circ \Delta_C) = (\mathrm{id}_C \otimes \varepsilon_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C) \,.$$

Thus,

$$\begin{aligned}
(\mathrm{id}_C \otimes \varepsilon_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C) &= \underbrace{(\mathrm{id}_C \circ \mathrm{id}_C)}_{= \mathrm{id}_C} \otimes \underbrace{((\varepsilon_C \otimes \mathrm{id}_C) \circ \Delta_C)}_{= \mathrm{kan}_{C,k\otimes C}} \\
&= \mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C} \,.
\end{aligned} \tag{254}$$

Now,

$$\begin{aligned}
&\underbrace{(e_{C,A} \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\tau_{C,C} \otimes \mathrm{id}_C)}_{\substack{= \left(\tau_{C,A} \otimes \mathrm{id}_C\right) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \varepsilon_C \otimes \mathrm{id}_C) \\ \text{(by (253))}}} \circ (\mathrm{id}_C \otimes \Delta_C) \\
&= (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ \underbrace{(\mathrm{id}_C \otimes \varepsilon_C \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C)}_{\substack{= \mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C} \\ \text{(by (254))}}} \\
&= (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C}) \,.
\end{aligned} \tag{255}$$

Thus, (249) becomes

$$\begin{aligned}
&((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * (\Delta_A \circ f) \\
&= (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ \underbrace{(e_{C,A} \otimes \mathrm{id}_C \otimes \mathrm{id}_C) \circ (\tau_{C,C} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \Delta_C)}_{\substack{= \left(\tau_{C,A} \otimes \mathrm{id}_C\right) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ \left(\mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C}\right) \\ \text{(by (255))}}} \circ \Delta_C \\
&= (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C}) \circ \Delta_C .
\end{aligned} \tag{256}$$

Now, let $\mathrm{kan}_{A,k\otimes A}$ be the canonical isomorphism $A \to k \otimes A$ which sends every $a \in A$ to $1 \otimes a \in k \otimes A$. Then, it is easy to see that

$$\begin{aligned}
&(\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C}) \\
&= (\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \mu_A \circ (g \otimes f) \,.
\end{aligned} \tag{257}$$

[134] Hence, (256) becomes

$$
\begin{aligned}
&((g\otimes g)\circ\Delta_{C^{\mathrm{cop}}})*(\Delta_A\circ f)\\
&=\underbrace{(\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\eta_A\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\mathrm{kan}_{C,k\otimes C})}_{\substack{=(\eta_A\otimes\mathrm{id}_A)\circ\mathrm{kan}_{A,k\otimes A}\circ\mu_A\circ(g\otimes f)\\ \text{(by (257))}}}\circ\Delta_C\\
&=(\eta_A\otimes\mathrm{id}_A)\circ\mathrm{kan}_{A,k\otimes A}\circ\underbrace{\mu_A\circ(g\otimes f)\circ\Delta_C}_{\substack{=e_{C,A}\\ \text{(by (245))}}}=(\eta_A\otimes\mathrm{id}_A)\circ\mathrm{kan}_{A,k\otimes A}\circ\underbrace{e_{C,A}}_{\substack{=\eta_A\circ\varepsilon_C\\ \text{(by the definition of } e_{C,A})}}\\
&=(\eta_A\otimes\mathrm{id}_A)\circ\mathrm{kan}_{A,k\otimes A}\circ\eta_A\circ\varepsilon_C.
\end{aligned}
$$

[134] *Proof of (257):* By the definition of η_A, we have $\eta_A(1)=1\cdot 1_A=1_A$. Every $c\in C$ and $d\in C$ satisfy

$$
\begin{aligned}
&((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\eta_A\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\mathrm{kan}_{C,k\otimes C}))(c\otimes d)\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\eta_A\otimes\mathrm{id}_C))\underbrace{((\mathrm{id}_C\otimes\mathrm{kan}_{C,k\otimes C})(c\otimes d))}_{=\mathrm{id}_C(c)\otimes\mathrm{kan}_{C,k\otimes C}(d)}\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\eta_A\otimes\mathrm{id}_C))\left(\underbrace{\mathrm{id}_C(c)}_{=c}\otimes\underbrace{\mathrm{kan}_{C,k\otimes C}(d)}_{\substack{=1\otimes d\\ \text{(by the definition of } \mathrm{kan}_{C,k\otimes C})}}\right)\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C)\circ(\mathrm{id}_C\otimes\eta_A\otimes\mathrm{id}_C))(c\otimes 1\otimes d)\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C))\underbrace{((\mathrm{id}_C\otimes\eta_A\otimes\mathrm{id}_C)(c\otimes 1\otimes d))}_{=\mathrm{id}_C(c)\otimes\eta_A(1)\otimes\mathrm{id}_C(d)}\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C))\left(\underbrace{\mathrm{id}_C(c)}_{=c}\otimes\underbrace{\eta_A(1)}_{=1_A}\otimes\underbrace{\mathrm{id}_C(d)}_{=d}\right)\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f)\circ(\tau_{C,A}\otimes\mathrm{id}_C))(c\otimes 1_A\otimes d)\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f))\underbrace{((\tau_{C,A}\otimes\mathrm{id}_C)(c\otimes 1_A\otimes d))}_{=\tau_{C,A}(c\otimes 1_A)\otimes\mathrm{id}_C(d)}\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f))\left(\underbrace{\tau_{C,A}(c\otimes 1_A)}_{\substack{=1_A\otimes c\\ \text{(by the definition of } \tau_{C,A})}}\otimes\underbrace{\mathrm{id}_C(d)}_{=d}\right)\\
&=((\mathrm{id}_A\otimes\mu_A)\circ(\mathrm{id}_A\otimes g\otimes f))(1_A\otimes c\otimes d)=(\mathrm{id}_A\otimes\mu_A)\underbrace{((\mathrm{id}_A\otimes g\otimes f)(1_A\otimes c\otimes d))}_{=\mathrm{id}_A(1_A)\otimes g(c)\otimes f(d)}\\
&=(\mathrm{id}_A\otimes\mu_A)\left(\underbrace{\mathrm{id}_A(1_A)}_{=1_A}\otimes g(c)\otimes f(d)\right)=(\mathrm{id}_A\otimes\mu_A)(1_A\otimes g(c)\otimes f(d))\\
&=\underbrace{\mathrm{id}_A(1_A)}_{=1_A}\otimes\underbrace{\mu_A(g(c)\otimes f(d))}_{\substack{=g(c)f(d)\\ \text{(by the definition of } \mu_A)}}=1_A\otimes g(c)f(d)
\end{aligned}
$$

Thus, every $c \in C$ satisfies

$$\begin{aligned}
&(((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * (\Delta_A \circ f))(c) \\
&= ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \eta_A \circ \varepsilon_C)(c) = ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \eta_A)(\varepsilon_C(c)) \\
&= ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A}) \underbrace{(\eta_A(\varepsilon_C(c)))}_{\substack{=\varepsilon_C(c)\cdot 1_A \\ \text{(by the definition} \\ \text{of } \eta_A)}} = ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A})(\varepsilon_C(c) \cdot 1_A) \\
&= (\eta_A \otimes \mathrm{id}_A) \underbrace{(\mathrm{kan}_{A,k\otimes A}(\varepsilon_C(c) \cdot 1_A))}_{\substack{=1\otimes\varepsilon_C(c)\cdot 1_A \\ \text{(by the definition} \\ \text{of } \mathrm{kan}_{A,k\otimes A}\text{)}}} = (\eta_A \otimes \mathrm{id}_A)(1 \otimes \varepsilon_C(c) \cdot 1_A) \\
&= \underbrace{\eta_A(1)}_{\substack{=1\cdot 1_A \\ \text{(by the definition of } \eta_A\text{)}}} \otimes \underbrace{\mathrm{id}_A(\varepsilon_C(c) \cdot 1_A)}_{=\varepsilon_C(c)\cdot 1_A} \\
&= 1 \cdot 1_A \otimes \varepsilon_C(c) \cdot 1_A = \varepsilon_C(c) \cdot \underbrace{1_A \otimes 1_A}_{=1_{A\otimes A}} = \varepsilon_C(c) \cdot 1_{A\otimes A} = \eta_{A\otimes A}(\varepsilon_C(c)) \\
&\qquad \text{(since } \eta_{A\otimes A}(\varepsilon_C(c)) = \varepsilon_C(c) \cdot 1_{A\otimes A} \text{ by the definition of } \eta_{A\otimes A}\text{)} \\
&= (\eta_{A\otimes A} \circ \varepsilon_C)(c) = e_{C,A\otimes A}(c) \\
&\qquad \text{(since } e_{C,A\otimes A} \text{ is defined as } \eta_{A\otimes A} \circ \varepsilon_C\text{, so that } \eta_{A\otimes A} \circ \varepsilon_C = e_{C,A\otimes A}\text{)}.
\end{aligned}$$

In other words, $((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * (\Delta_A \circ f) = e_{C,A\otimes A}$. This proves (239).

---

and

$$\begin{aligned}
&((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \mu_A \circ (g \otimes f))(c \otimes d) \\
&= ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \mu_A) \underbrace{((g \otimes f)(c \otimes d))}_{=g(c)\otimes f(d)} = ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \mu_A)(g(c) \otimes f(d)) \\
&= ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A}) \underbrace{(\mu_A(g(c) \otimes f(d)))}_{\substack{=g(c)f(d) \\ \text{(by the definition of } \mu_A\text{)}}} = ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A})(g(c)\, f(d)) \\
&= (\eta_A \otimes \mathrm{id}_A) \underbrace{(\mathrm{kan}_{A,k\otimes A}(g(c)\, f(d)))}_{\substack{=1\otimes g(c)f(d) \\ \text{(by the definition of } \mathrm{kan}_{A,k\otimes A}\text{)}}} = (\eta_A \otimes \mathrm{id}_A)(1 \otimes g(c)\, f(d)) \\
&= \underbrace{\eta_A(1)}_{=1} \otimes \underbrace{\mathrm{id}_A(g(c)\, f(d))}_{=g(c)f(d)} = 1 \otimes g(c)\, f(d).
\end{aligned}$$

Thus, every $c \in C$ and $d \in C$ satisfy

$$\begin{aligned}
&((\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C}))(c \otimes d) \\
&= 1 \otimes g(c)\, f(d) = ((\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \mu_A \circ (g \otimes f))(c \otimes d).
\end{aligned}$$

In other words, the two maps
$(\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C})$ and
$(\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \mu_A \circ (g \otimes f)$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words,

$$\begin{aligned}
&(\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes g \otimes f) \circ (\tau_{C,A} \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \eta_A \otimes \mathrm{id}_C) \circ (\mathrm{id}_C \otimes \mathrm{kan}_{C,k\otimes C}) \\
&= (\eta_A \otimes \mathrm{id}_A) \circ \mathrm{kan}_{A,k\otimes A} \circ \mu_A \circ (g \otimes f).
\end{aligned}$$

This proves (257).

Proof of (240): Since A is a k-bialgebra, the comultiplication map Δ_A of A is a k-algebra homomorphism (by the axioms of a bialgebra). Thus, $\mu_{A\otimes A} \circ (\Delta_A \otimes \Delta_A) = \Delta_A \circ \mu_A$ and $\eta_{A\otimes A} = \Delta_A \circ \eta_A$.

By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$. Thus,

$$\mu_A \circ (f \otimes g) \circ \Delta_C = f * g = e_{C,A} = \eta_A \circ \varepsilon_C \tag{258}$$

(by the definition of $e_{C,A}$).

By the definition of convolution,

$$\begin{aligned}
(\Delta_A \circ f) * (\Delta_A \circ g) &= \mu_{A\otimes A} \circ \underbrace{((\Delta_A \circ f) \otimes (\Delta_A \circ g))}_{\substack{=(\Delta_A\otimes\Delta_A)\circ(f\otimes g) \\ \text{(by (21), applied to } C,\ A,\ A\otimes A,\ C,\ A,\ A\otimes A, \\ f,\ \Delta_A,\ g,\ \Delta_A \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta')}} \circ \Delta_C \\
&= \underbrace{\mu_{A\otimes A} \circ (\Delta_A \otimes \Delta_A)}_{=\Delta_A\circ\mu_A} \circ (f \otimes g) \circ \Delta_C = \Delta_A \circ \underbrace{\mu_A \circ (f \otimes g) \circ \Delta_C}_{\substack{=\eta_A\circ\varepsilon_C \\ \text{(by (258))}}} \\
&= \underbrace{\Delta_A \circ \eta_A}_{=\eta_{A\otimes A}} \circ \varepsilon_C = \eta_{A\otimes A} \circ \varepsilon_C = e_{C,A\otimes A}
\end{aligned}$$

(since $e_{C,A\otimes A}$ is defined as $\eta_{A\otimes A} \circ \varepsilon_C$). This proves (240).

Now, let us finish the proof of Proposition 25.2: Comparing the equalities

$$\begin{aligned}
&\underbrace{((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * (\Delta_A \circ f)}_{\substack{=e_{C,A\otimes A} \\ \text{(by (239))}}} * (\Delta_A \circ g) \\
&= e_{C,A\otimes A} * (\Delta_A \circ g) = \Delta_A \circ g
\end{aligned}$$

and

$$\begin{aligned}
&((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * \underbrace{(\Delta_A \circ f) * (\Delta_A \circ g)}_{\substack{=e_{C,A\otimes A} \\ \text{(by (240))}}} \\
&= ((g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}) * e_{C,A\otimes A} = (g \otimes g) \circ \Delta_{C^{\mathrm{cop}}},
\end{aligned}$$

we obtain

$$\Delta_A \circ g = (g \otimes g) \circ \Delta_{C^{\mathrm{cop}}}. \tag{259}$$

We will now prove that $\varepsilon_A \circ g = \varepsilon_{C^{\mathrm{cop}}}$.

Since A is a k-bialgebra, the counit map ε_A of A is a k-algebra homomorphism (by the axioms of a bialgebra). Thus, $\varepsilon_A \circ \mu_A = \mu_k \circ (\varepsilon_A \otimes \varepsilon_A)$ and $\varepsilon_A \circ \eta_A = \eta_k$.

Since f is a k-coalgebra homomorphism $C \to A$, we have $\varepsilon_A \circ f = \varepsilon_C$.

Applying (21) to C, A, k, C, A, k, f, ε_A, g, ε_A instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\varepsilon_A \circ f) \otimes (\varepsilon_A \circ g) = (\varepsilon_A \otimes \varepsilon_A) \circ (f \otimes g).$$

Thus,

$$(\varepsilon_A \otimes \varepsilon_A) \circ (f \otimes g) = \underbrace{(\varepsilon_A \circ f)}_{=\varepsilon_C} \otimes (\varepsilon_A \circ g) = \varepsilon_C \otimes (\varepsilon_A \circ g). \tag{260}$$

The unity of the k-algebra $(\mathcal{L}(C,k),*)$ is $\underbrace{\eta_k}_{=\mathrm{id}} \circ \varepsilon_C = \varepsilon_C$.

But now,

$$\varepsilon_A \circ \underbrace{\mu_A \circ (f \otimes g) \circ \Delta_C}_{\substack{=\eta_A \circ \varepsilon_C \\ \text{(by (258))}}} = \underbrace{\varepsilon_A \circ \eta_A}_{=\eta_k = \mathrm{id}_k} \circ \varepsilon_C = \varepsilon_C = \varepsilon_{C^{\mathrm{cop}}}$$

(since $\varepsilon_{C^{\mathrm{cop}}} = \varepsilon_C$ by the definition of C^{cop}). Thus,

$$\begin{aligned}
\varepsilon_{C^{\mathrm{cop}}} &= \underbrace{\varepsilon_A \circ \mu_A}_{=\mu_k \circ (\varepsilon_A \otimes \varepsilon_A)} \circ (f \otimes g) \circ \Delta_C = \mu_k \circ \underbrace{(\varepsilon_A \otimes \varepsilon_A) \circ (f \otimes g)}_{\substack{=\varepsilon_C \otimes (\varepsilon_A \circ g) \\ \text{(by (260))}}} \circ \Delta_C \\
&= \mu_k \circ (\varepsilon_C \otimes (\varepsilon_A \circ g)) \circ \Delta_C = \varepsilon_C * (\varepsilon_A \circ g) \\
&\qquad \left(\begin{array}{c} \text{since } \varepsilon_C * (\varepsilon_A \circ g) = \mu_k \circ (\varepsilon_C \otimes (\varepsilon_A \circ g)) \circ \Delta_C \\ \text{by the definition of convolution} \end{array} \right) \\
&= \varepsilon_A \circ g \qquad (\text{since } \varepsilon_C \text{ is the unity of the } k\text{-algebra } (\mathcal{L}(C,k),*)).
\end{aligned}$$

We thus have proven that $\varepsilon_A \circ g = \varepsilon_{C^{\mathrm{cop}}}$. Combined with (259), this yields that g is a k-coalgebra homomorphism from C^{cop} to A. Since $g = f^{*(-1)}$, this rewrites as follows: $f^{*(-1)}$ is a k-coalgebra homomorphism from C^{cop} to A. This proves Proposition 25.2. □

§26. $*$-inverses of algebra homomorphisms

In this section, we are going to prove the dual versions of the results of §25, dual in the sense that coalgebras become algebras. The proofs are mostly identical to the ones of §25 up to "reversing arrows", except in some of the cases when we worked with elements in §25.

Let us extend Corollary 15.16 to the case of negative n whenever f is $*$-invertible:

Proposition 26.1. Let k be a field. Let H be a k-bialgebra. Let A be a commutative k-algebra. Let $f : H \to A$ be a $*$-invertible k-algebra homomorphism.

(a) Then, $f^{*(-1)} : H \to A$ is also a k-algebra homomorphism.

(b) Let $n \in \mathbb{Z}$. Then, $f^{*n} : H \to A$ is also a k-algebra homomorphism.

Again, this proposition (like Proposition 25.1) can be easily shown using Proposition 23.4 in the same way as we proved Proposition 15.15 in §24 with the help of Proposition 23.4. Again, we are not going to present this proof, but instead we will show something more general than Proposition 26.1:

Proposition 26.2. Let k be a field. Let C be a k-bialgebra. Let A be a k-algebra. Let $f : C \to A$ be a $*$-invertible k-algebra homomorphism. Then, $f^{*(-1)}$ is a k-algebra homomorphism from C to A^{op}.

Here, we are using the following definition:

Definition 26.3. Let k be a field. Let A be a k-algebra. The *opposite algebra* of A is defined to be the k-algebra $(A, \mu_A \circ \tau_{A,A}, \eta_A)$ (this is easily seen to be a k-algebra), and denoted by A^{op}.

Before we prove Proposition 26.2, let us show how Proposition 26.1 can be derived from it:

Proof of Proposition 26.1. **(a)** Since A is commutative, we have $\mu_A \circ \tau_{A,A} = \mu_A$ [135]. By the definition of A^{op}, we have $A^{\mathrm{op}} = \left(A, \underbrace{\mu_A \circ \tau_{A,A}}_{=\mu_A}, \eta_A\right) = (A, \mu_A, \eta_A) = A$. By Proposition 26.2 (applied to $C = H$), we know that $f^{*(-1)}$ is a k-algebra homomorphism from H to A^{op}. Since $A^{\mathrm{op}} = A$, this rewrites as follows: $f^{*(-1)}$ is a k-algebra homomorphism from H to A. This proves Proposition 26.1 **(a)**.

(b) Let us first check that, for every $m \in \mathbb{N}$,

$$\text{the map } f^{*(-m)} : H \to A \text{ is a } k\text{-algebra homomorphism.} \tag{261}$$

Proof of (261): We will prove (261) by induction over m:

Induction base: From the proof of Corollary 15.16, we know that f^{*0} is a k-algebra homomorphism. In other words, $f^{*(-0)}$ is a k-algebra homomorphism (since $0 = -0$). In other words, (261) holds for $m = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that (261) holds for $m = N$. We must now prove that (261) also holds for $m = N + 1$.

Since (261) holds for $m = N$, we know that $f^{*(-N)}$ is a k-algebra homomorphism. Proposition 15.15 (applied to $f^{*(-1)}$ and $f^{*(-N)}$ instead of f and g) now yields that $f^{*(-1)} * f^{*(-N)}$ is a k-algebra homomorphism (because we know from Proposition 26.1 **(a)** that $f^{*(-1)}$ is a k-algebra homomorphism). Since $f^{*(-1)} * f^{*(-N)} = f^{*(-(N+1))}$, this yields that $f^{*(-(N+1))}$ is a k-algebra homomorphism. In other words, (261) holds for $m = N + 1$. This completes the induction step. The induction proof of (261) is thus complete.

Now, let us distinguish between two cases:

Case 1: We have $n \geq 0$.

Case 2: We have $n < 0$.

Let us consider Case 1 first. In this case, $n \geq 0$, so that $n \in \mathbb{N}$, and thus Corollary 15.16 shows that $f^{*n} : H \to A$ is a k-algebra homomorphism. Hence, Proposition 26.1 **(b)** is proven in Case 1.

Now, let us consider Case 2. In this case, $n < 0$, so that $-n > 0$ and thus $-n \in \mathbb{N}$. Hence, (261) (applied to $m = -n$) yields that the map $f^{*(-(-n))} : H \to A$ is a k-algebra homomorphism. Since $-(-n) = n$, this rewrites as follows: The map $f^{*n} : H \to A$ is a k-algebra homomorphism. Thus, Proposition 26.1 **(b)** is proven in Case 2.

[135] *Proof.* Every $a \in A$ and $b \in A$ satisfy

$$\begin{aligned}
(\mu_A \circ \tau_{A,A})(a \otimes b) &= \mu_A \underbrace{(\tau_{A,A}(a \otimes b))}_{\substack{=b \otimes a \\ \text{(by the definition} \\ \text{of } \tau_{A,A})}} = \mu_A(b \otimes a) = ba \qquad \text{(by the definition of } \mu_A) \\
&= ab \qquad \text{(since } A \text{ is commutative)} \\
&= \mu_A(a \otimes b) \qquad \text{(since } \mu_A(a \otimes b) = ab \text{ by the definition of } \mu_A).
\end{aligned}$$

In other words, the two maps $\mu_A \circ \tau_{A,A}$ and μ_A are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $\mu_A \circ \tau_{A,A} = \mu_A$, qed.

Hence, Proposition 26.1 **(b)** is proven in each of the cases 1 and 2. Since these two cases cover all possibilities, this yields that Proposition 26.1 **(b)** always holds. The proof of Proposition 26.1 **(b)** is thus complete (up to proving Proposition 26.2). $\square$

Let us show another consequence of Proposition 26.2:

Proposition 26.4. Let k be a field. Let H be a k-Hopf algebra. Then, the antipode of H is a k-algebra homomorphism from H to H^{op}.

Proof of Proposition 26.4. The antipode of H is the $*$-inverse of the identity map $\mathrm{id}_H : H \to H$ (by the definition of the antipode of a Hopf algebra). In other words, the antipode of H is the map $\mathrm{id}_H^{*(-1)}$. In particular, this yields that the map id_H is $*$-invertible. Thus, Proposition 26.2 (applied to $C = H$, $A = H$ and $f = \mathrm{id}_H$) yields that $\mathrm{id}_H^{*(-1)}$ is a k-algebra homomorphism from H to H^{op}. Since $\mathrm{id}_H^{*(-1)}$ is the antipode of H, this rewrites as follows: The antipode of H is a k-algebra homomorphism from H to H^{op}. This proves Proposition 26.4. $\square$

Let us now prepare for proving Proposition 26.2. Our proof will involve lengthy computations, but we can simplify them by showing some lemmas first:

Lemma 26.5. Let k be a field. Let A be a k-algebra. Then,

$$\mu_A \circ (\mu_A \otimes \mu_A) = \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A) .$$

Proof of Lemma 26.5. Every $a \in A$, $b \in A$, $c \in A$ and $d \in A$ satisfy

$$\begin{aligned}
&(\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A))\,(a \otimes b \otimes c \otimes d) \\
&= (\mu_A \circ (\mu_A \otimes \mathrm{id}_A))\,\underbrace{((\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A)\,(a \otimes b \otimes c \otimes d))}_{=\mathrm{id}_A(a) \otimes \mu_A(b \otimes c) \otimes \mathrm{id}_A(d)} \\
&= (\mu_A \circ (\mu_A \otimes \mathrm{id}_A))\left(\underbrace{\mathrm{id}_A(a)}_{=a} \otimes \underbrace{\mu_A(b \otimes c)}_{\substack{=bc \\ \text{(by the definition of } \mu_A\text{)}}} \otimes \underbrace{\mathrm{id}_A(d)}_{=d}\right) \\
&= (\mu_A \circ (\mu_A \otimes \mathrm{id}_A))\,(a \otimes bc \otimes d) = \mu_A\,\underbrace{((\mu_A \otimes \mathrm{id}_A)\,(a \otimes bc \otimes d))}_{=\mu_A(a \otimes bc) \otimes \mathrm{id}_A(d)} \\
&= \mu_A\left(\underbrace{\mu_A(a \otimes bc)}_{\substack{=a(bc) \\ \text{(by the definition of } \mu_A\text{)}}} \otimes \underbrace{\mathrm{id}_A(d)}_{=d}\right) = \mu_A\,(a\,(bc) \otimes d) = (a\,(bc))\,d \\
&\qquad \text{(by the definition of } \mu_A\text{)}
\end{aligned}$$

and

$$\begin{aligned}
&(\mu_A \circ (\mu_A \otimes \mu_A))\,(a \otimes b \otimes c \otimes d) \\
&= \mu_A\,\underbrace{((\mu_A \otimes \mu_A)\,(a \otimes b \otimes c \otimes d))}_{=\mu_A(a \otimes b) \otimes \mu_A(c \otimes d)} = \mu_A\left(\underbrace{\mu_A(a \otimes b)}_{\substack{=ab \\ \text{(by the definition of } \mu_A\text{)}}} \otimes \underbrace{\mu_A(c \otimes d)}_{\substack{=cd \\ \text{(by the definition of } \mu_A\text{)}}}\right) \\
&= \mu_A(ab \otimes cd) = (ab)\,(cd) \qquad \text{(by the definition of } \mu_A\text{)} .
\end{aligned}$$

Thus, every $a \in A$, $b \in A$, $c \in A$ and $d \in A$ satisfy

$$\begin{aligned}&(\mu_A \circ (\mu_A \otimes \mu_A))(a \otimes b \otimes c \otimes d)\\ &= (ab)(cd) = abcd = (a(bc))\, d = (\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A))(a \otimes b \otimes c \otimes d).\end{aligned}$$

In other words, the two maps $\mu_A \circ (\mu_A \otimes \mu_A)$ and $\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A)$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $\mu_A \circ (\mu_A \otimes \mu_A) = \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A)$, so that Lemma 26.5 is proven. □

Lemma 26.6. Let k be a field. Let U, V and W be three k-vector spaces. Then,

$$(\tau_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes \tau_{V,W}) = \tau_{U \otimes V, W}.$$

Proof of Lemma 26.6. Every $u \in U$, $v \in V$ and $w \in W$ satisfy

$$\begin{aligned}&((\tau_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes \tau_{V,W}))(u \otimes v \otimes w)\\ &= (\tau_{U,W} \otimes \mathrm{id}_V) \underbrace{((\mathrm{id}_U \otimes \tau_{V,W})(u \otimes v \otimes w))}_{= \mathrm{id}_U(u) \otimes \tau_{V,W}(v \otimes w)}\\ &= (\tau_{U,W} \otimes \mathrm{id}_V) \left(\underbrace{\mathrm{id}_U(u)}_{=u} \otimes \underbrace{\tau_{V,W}(v \otimes w)}_{\substack{=w \otimes v \\ (\text{by the definition of } \tau_{V,W})}} \right)\\ &= (\tau_{U,W} \otimes \mathrm{id}_V)(u \otimes w \otimes v) = \underbrace{\tau_{U,W}(u \otimes w)}_{\substack{=w \otimes u \\ (\text{by the definition of } \tau_{U,W})}} \otimes \underbrace{\mathrm{id}_V(v)}_{=v}\\ &= w \otimes u \otimes v = \tau_{U \otimes V, W}(u \otimes v \otimes w)\\ &\qquad (\text{since } \tau_{U \otimes V, W}(u \otimes v \otimes w) = w \otimes u \otimes v \text{ by the definition of } \tau_{U \otimes V, W}).\end{aligned}$$

In other words, the two maps $(\tau_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes \tau_{V,W})$ and $\tau_{U \otimes V, W}$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $(\tau_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes \tau_{V,W}) = \tau_{U \otimes V, W}$. This proves Lemma 26.6. □

Lemma 26.7. Let k be a field. Let U, V, W, T and Q be five k-vector spaces. Let $r : U \otimes V \to Q$ be a k-linear map. Then,

$$\begin{aligned}&(\mathrm{id}_W \otimes r \otimes \mathrm{id}_T) \circ (\tau_{U,W} \otimes \mathrm{id}_V \otimes \mathrm{id}_T) \circ (\mathrm{id}_U \otimes \tau_{V,W} \otimes \mathrm{id}_T)\\ &= (\tau_{Q,W} \otimes \mathrm{id}_T) \circ (r \otimes \mathrm{id}_W \otimes \mathrm{id}_T).\end{aligned}$$

Proof of Lemma 26.7. By (21) (applied to $U \otimes V \otimes W$, $U \otimes W \otimes V$, $W \otimes U \otimes V$, T, T, T, $\mathrm{id}_U \otimes \tau_{V,W}$, $\tau_{U,W} \otimes \mathrm{id}_V$, id_T, id_T instead of U, V, W, U', V', W', α, β, α', β'), we have

$$((\tau_{U,W} \otimes \mathrm{id}_V) \circ (\mathrm{id}_U \otimes \tau_{V,W})) \otimes (\mathrm{id}_T \circ \mathrm{id}_T) = (\tau_{U,W} \otimes \mathrm{id}_V \otimes \mathrm{id}_T) \circ (\mathrm{id}_U \otimes \tau_{V,W} \otimes \mathrm{id}_T).$$

Thus,

$$\begin{aligned}&(\tau_{U,W}\otimes \mathrm{id}_V\otimes \mathrm{id}_T)\circ(\mathrm{id}_U\otimes\tau_{V,W}\otimes \mathrm{id}_T)\\&=\underbrace{((\tau_{U,W}\otimes \mathrm{id}_V)\circ(\mathrm{id}_U\otimes\tau_{V,W}))}_{\substack{=\tau_{U\otimes V,W}\\ \text{(by Lemma 26.6)}}}\otimes\underbrace{(\mathrm{id}_T\circ \mathrm{id}_T)}_{=\mathrm{id}_T}=\tau_{U\otimes V,W}\otimes \mathrm{id}_T\,. \end{aligned}\tag{262}$$

On the other hand, by (21) (applied to $U\otimes V\otimes W$, $W\otimes U\otimes V$, $W\otimes Q$, T, T, T, $\tau_{U\otimes V,W}$, $\mathrm{id}_W\otimes r$, id_T, id_T instead of U, V, W, U', V', W', α, β, α', β'), we have

$$((\mathrm{id}_W\otimes r)\circ\tau_{U\otimes V,W})\otimes(\mathrm{id}_T\circ \mathrm{id}_T)=(\mathrm{id}_W\otimes r\otimes \mathrm{id}_T)\circ(\tau_{U\otimes V,W}\otimes \mathrm{id}_T)\,.\tag{263}$$

By Proposition 9.3 **(a)** (applied to $U\otimes V$, W, Q, W, r and id_W instead of V, W, V', W', f and g), we have

$$(\mathrm{id}_W\otimes r)\circ\tau_{U\otimes V,W}=\tau_{Q,W}\circ(r\otimes \mathrm{id}_W)\,.\tag{264}$$

Besides, by (21) (applied to $U\otimes V\otimes W$, $Q\otimes W$, $W\otimes Q$, T, T, T, $r\otimes \mathrm{id}_W$, $\tau_{Q,W}$, id_T, id_T instead of U, V, W, U', V', W', α, β, α', β'), we have

$$(\tau_{Q,W}\circ(r\otimes \mathrm{id}_W))\otimes(\mathrm{id}_T\circ \mathrm{id}_T)=(\tau_{Q,W}\otimes \mathrm{id}_T)\circ(r\otimes \mathrm{id}_W\otimes \mathrm{id}_T)\,.\tag{265}$$

Now,

$$\begin{aligned}&(\mathrm{id}_W\otimes r\otimes \mathrm{id}_T)\circ\underbrace{(\tau_{U,W}\otimes \mathrm{id}_V\otimes \mathrm{id}_T)\circ(\mathrm{id}_U\otimes\tau_{V,W}\otimes \mathrm{id}_T)}_{\substack{=\tau_{U\otimes V,W}\otimes \mathrm{id}_T\\ \text{(by (262))}}}\\&=(\mathrm{id}_W\otimes r\otimes \mathrm{id}_T)\circ(\tau_{U\otimes V,W}\otimes \mathrm{id}_T)\\&=\underbrace{((\mathrm{id}_W\otimes r)\circ\tau_{U\otimes V,W})}_{\substack{=\tau_{Q,W}\circ(r\otimes \mathrm{id}_W)\\ \text{(by (264))}}}\otimes(\mathrm{id}_T\circ \mathrm{id}_T)\qquad\text{(by (263))}\\&=(\tau_{Q,W}\circ(r\otimes \mathrm{id}_W))\otimes(\mathrm{id}_T\circ \mathrm{id}_T)=(\tau_{Q,W}\otimes \mathrm{id}_T)\circ(r\otimes \mathrm{id}_W\otimes \mathrm{id}_T)\qquad\text{(by (265))}\,.\end{aligned}$$

This proves Lemma 26.7. □

Proof of Proposition 26.2. Let $g=f^{*(-1)}$. Then, $f*g=f*f^{*(-1)}=e_{C,A}$ and $g*f=f^{*(-1)}*f=e_{C,A}$.

We are now going to show that

$$(\mu_{A^{\mathrm{op}}}\circ(g\otimes g))*(f\circ\mu_C)=e_{C\otimes C,A}\tag{266}$$

and

$$(f\circ\mu_C)*(g\circ\mu_C)=e_{C\otimes C,A}\tag{267}$$

(where $*$ stands for convolution of maps from $C\otimes C$ to A). Once these formulas are shown, it will be easy to conclude that $\mu_{A^{\mathrm{op}}}\circ(g\otimes g)=g\circ\mu_C$, which will settle the hardest part of Proposition 26.2.

But let us prove (266) and (267) now:

Proof of (266): Since f is a k-algebra homomorphism, we have $f \circ \mu_C = \mu_A \circ (f \otimes f)$. Thus,

$$
\begin{aligned}
&(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * \underbrace{(f \circ \mu_C)}_{=\mu_A \circ (f \otimes f)} \\
&= (\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (\mu_A \circ (f \otimes f)) \\
&= \mu_A \circ \underbrace{((\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) \otimes (\mu_A \circ (f \otimes f)))}_{\substack{=(\mu_{A^{\mathrm{op}}} \otimes \mu_A) \circ (g \otimes g \otimes f \otimes f) \\ \text{(by (21), applied to } C \otimes C,\ A \otimes A,\ A,\ C \otimes C,\ A \otimes A,\ A, \\ g \otimes g,\ \mu_{A^{\mathrm{op}}},\ f \otimes f,\ \mu_A \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta')}} \circ \underbrace{\Delta_{C \otimes C}}_{\substack{=\left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right) \circ (\Delta_C \otimes \Delta_C) \\ \text{(by the definition of the } k\text{-coalgebra } C \otimes C)}} \\
&\qquad \text{(by the definition of convolution)} \\
&= \mu_A \circ \left(\underbrace{\mu_{A^{\mathrm{op}}}}_{\substack{=\mu_A \circ \tau_{A,A} \\ \text{(by the definition of the} \\ k\text{-algebra } A^{\mathrm{op}})}} \otimes \underbrace{\mu_A}_{=\mu_A \circ \mathrm{id}_{A \otimes A}} \right) \circ \underbrace{(g \otimes g \otimes f \otimes f) \circ (\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C)}_{\substack{=\left(\mathrm{id}_A \otimes \tau_{A,A} \otimes \mathrm{id}_A\right) \circ (g \otimes f \otimes g \otimes f) \\ \text{(since Proposition 9.3 } \mathbf{(b)} \text{ (applied to } C,\ C,\ C,\ C, \\ A,\ A,\ A,\ A,\ g,\ f,\ g,\ f \text{ instead of} \\ U,\ V,\ W,\ T,\ U',\ V',\ W',\ T',\ e,\ f,\ g,\ h) \text{ yields} \\ \left(\mathrm{id}_A \otimes \tau_{A,A} \otimes \mathrm{id}_A\right) \circ (g \otimes f \otimes g \otimes f) \\ = (g \otimes g \otimes f \otimes f) \circ \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right))}} \circ (\Delta_C \otimes \Delta_C) \\
&= \mu_A \circ \underbrace{((\mu_A \circ \tau_{A,A}) \otimes (\mu_A \circ \mathrm{id}_{A \otimes A}))}_{\substack{=(\mu_A \otimes \mu_A) \circ \left(\tau_{A,A} \otimes \mathrm{id}_{A \otimes A}\right) \\ \text{(by (21), applied to } A \otimes A,\ A \otimes A,\ A, \\ A \otimes A,\ A \otimes A,\ A,\ \tau_{A,A},\ \mu_A,\ \mathrm{id}_{A \otimes A},\ \mu_A \\ \text{instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta')}} \circ (\mathrm{id}_A \otimes \tau_{A,A} \otimes \mathrm{id}_A) \circ (g \otimes f \otimes g \otimes f) \circ (\Delta_C \otimes \Delta_C) \\
&= \underbrace{\mu_A \circ (\mu_A \otimes \mu_A)}_{\substack{=\mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A) \\ \text{(by Lemma 26.5)}}} \circ \left(\tau_{A,A} \otimes \underbrace{\mathrm{id}_{A \otimes A}}_{=\mathrm{id}_A \otimes \mathrm{id}_A} \right) \circ (\mathrm{id}_A \otimes \tau_{A,A} \otimes \mathrm{id}_A) \\
&\qquad \circ (g \otimes f \otimes g \otimes f) \circ (\Delta_C \otimes \Delta_C) \\
&= \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ \underbrace{(\mathrm{id}_A \otimes \mu_A \otimes \mathrm{id}_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \tau_{A,A} \otimes \mathrm{id}_A)}_{\substack{=\left(\tau_{A,A} \otimes \mathrm{id}_A\right) \circ (\mu_A \otimes \mathrm{id}_A \otimes \mathrm{id}_A) \\ \text{(by Lemma 26.7, applied to } U{=}A,\ V{=}A,\ W{=}A,\ T{=}A,\ Q{=}A \text{ and } r{=}\mu_A)}} \\
&\qquad \circ (g \otimes f \otimes g \otimes f) \circ (\Delta_C \otimes \Delta_C) \\
&= \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A) \circ \left(\mu_A \otimes \underbrace{\mathrm{id}_A \otimes \mathrm{id}_A}_{=\mathrm{id}_{A \otimes A}} \right) \circ (g \otimes f \otimes g \otimes f) \circ (\Delta_C \otimes \Delta_C) \\
&= \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A) \circ (\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (g \otimes f \otimes g \otimes f) \circ (\Delta_C \otimes \Delta_C) \,.
\end{aligned}
\tag{268}
$$

Applying (21) to C, C, $C \otimes C$, C, $C \otimes C$, $C \otimes C$, id_C, Δ_C, Δ_C, $\mathrm{id}_{C \otimes C}$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\Delta_C \circ \mathrm{id}_C) \otimes (\mathrm{id}_{C \otimes C} \circ \Delta_C) = (\Delta_C \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \,.$$

Since $\Delta_C \circ \mathrm{id}_C = \Delta_C$ and $\mathrm{id}_{C \otimes C} \circ \Delta_C = \Delta_C$, this rewrites as

$$\Delta_C \otimes \Delta_C = (\Delta_C \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \,. \tag{269}$$

Applying (21) to $C \otimes C$, $C \otimes C$, $A \otimes A$, $C \otimes C$, $A \otimes A$, $A \otimes A$, $\mathrm{id}_{C \otimes C}$, $g \otimes f$, $g \otimes f$, $\mathrm{id}_{A \otimes A}$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$((g \otimes f) \circ \mathrm{id}_{C \otimes C}) \otimes (\mathrm{id}_{A \otimes A} \circ (g \otimes f)) = (g \otimes f \otimes \mathrm{id}_{A \otimes A}) \circ (\mathrm{id}_{C \otimes C} \otimes g \otimes f)\,.$$

Since $(g \otimes f) \circ \mathrm{id}_{C \otimes C} = g \otimes f$ and $\mathrm{id}_{A \otimes A} \circ (g \otimes f) = g \otimes f$, this rewrites as

$$g \otimes f \otimes g \otimes f = (g \otimes f \otimes \mathrm{id}_{A \otimes A}) \circ (\mathrm{id}_{C \otimes C} \otimes g \otimes f)\,. \tag{270}$$

By (212) (applied to $P = C$, $Q = C \otimes C$, $R = C \otimes C$, $S = A \otimes A$, $\gamma = \Delta_C$ and $\delta = g \otimes f$), we have

$$(\mathrm{id}_{C \otimes C} \otimes g \otimes f) \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C}) = (\Delta_C \otimes \mathrm{id}_{A \otimes A}) \circ (\mathrm{id}_C \otimes g \otimes f)\,. \tag{271}$$

By the definition of convolution, $g * f = \mu_A \circ (g \otimes f) \circ \Delta_C$, so that

$$\mu_A \circ (g \otimes f) \circ \Delta_C = g * f = e_{C,A}. \tag{272}$$

Applying (21) to $C \otimes C$, $A \otimes A$, A, $A \otimes A$, $A \otimes A$, $A \otimes A$, $g \otimes f$, μ_A, $\mathrm{id}_{A \otimes A}$, $\mathrm{id}_{A \otimes A}$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mu_A \circ (g \otimes f)) \otimes (\mathrm{id}_{A \otimes A} \circ \mathrm{id}_{A \otimes A}) = (\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (g \otimes f \otimes \mathrm{id}_{A \otimes A})\,.$$

Since $\mathrm{id}_{A \otimes A} \circ \mathrm{id}_{A \otimes A} = \mathrm{id}_{A \otimes A}$, this rewrites as

$$(\mu_A \circ (g \otimes f)) \otimes \mathrm{id}_{A \otimes A} = (\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (g \otimes f \otimes \mathrm{id}_{A \otimes A})\,. \tag{273}$$

Applying (21) to C, $C \otimes C$, A, $A \otimes A$, $A \otimes A$, $A \otimes A$, Δ_C, $\mu_A \circ (g \otimes f)$, $\mathrm{id}_{A \otimes A}$, $\mathrm{id}_{A \otimes A}$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mu_A \circ (g \otimes f) \circ \Delta_C) \otimes (\mathrm{id}_{A \otimes A} \circ \mathrm{id}_{A \otimes A}) = ((\mu_A \circ (g \otimes f)) \otimes \mathrm{id}_{A \otimes A}) \circ (\Delta_C \otimes \mathrm{id}_{A \otimes A})\,. \tag{274}$$

Thus,

$$\begin{aligned}
&\underbrace{(\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (g \otimes f \otimes \mathrm{id}_{A \otimes A})}_{\substack{= (\mu_A \circ (g \otimes f)) \otimes \mathrm{id}_{A \otimes A} \\ \text{(by (273))}}} \circ (\Delta_C \otimes \mathrm{id}_{A \otimes A}) \\
&= ((\mu_A \circ (g \otimes f)) \otimes \mathrm{id}_{A \otimes A}) \circ (\Delta_C \otimes \mathrm{id}_{A \otimes A}) \\
&= \underbrace{(\mu_A \circ (g \otimes f) \circ \Delta_C)}_{\substack{= e_{C,A} \\ \text{(by (272))}}} \otimes \underbrace{(\mathrm{id}_{A \otimes A} \circ \mathrm{id}_{A \otimes A})}_{= \mathrm{id}_{C \otimes C}} \qquad \text{(by (274))} \\
&= e_{C,A} \otimes \mathrm{id}_{A \otimes A}\,.
\end{aligned} \tag{275}$$

Now, (268) becomes

$$
\begin{aligned}
&(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C) \\
&= \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A) \circ (\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ \underbrace{(g \otimes f \otimes g \otimes f)}_{\substack{= (g \otimes f \otimes \mathrm{id}_{A \otimes A}) \circ (\mathrm{id}_{C \otimes C} \otimes g \otimes f) \\ \text{(by (270))}}} \circ \underbrace{(\Delta_C \otimes \Delta_C)}_{\substack{= (\Delta_C \otimes \mathrm{id}_{C \otimes C}) \circ (\mathrm{id}_C \otimes \Delta_C) \\ \text{(by (269))}}} \\
&= \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A) \\
&\qquad \circ (\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (g \otimes f \otimes \mathrm{id}_{A \otimes A}) \circ \underbrace{(\mathrm{id}_{C \otimes C} \otimes g \otimes f) \circ (\Delta_C \otimes \mathrm{id}_{C \otimes C})}_{\substack{= (\Delta_C \otimes \mathrm{id}_{A \otimes A}) \circ (\mathrm{id}_C \otimes g \otimes f) \\ \text{(by (271))}}} \circ (\mathrm{id}_C \otimes \Delta_C) \\
&= \mu_A \circ (\mu_A \otimes \mathrm{id}_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A) \\
&\qquad \circ \underbrace{(\mu_A \otimes \mathrm{id}_{A \otimes A}) \circ (g \otimes f \otimes \mathrm{id}_{A \otimes A}) \circ (\Delta_C \otimes \mathrm{id}_{A \otimes A})}_{\substack{= e_{C,A} \otimes \mathrm{id}_{A \otimes A} \\ \text{(by (275))}}} \circ (\mathrm{id}_C \otimes g \otimes f) \circ (\mathrm{id}_C \otimes \Delta_C) \\
&= \underbrace{\mu_A \circ (\mu_A \otimes \mathrm{id}_A)}_{\substack{= \mu_A \circ (\mathrm{id}_A \otimes \mu_A) \\ \text{(by the axioms of an} \\ \text{algebra, since } A \text{ is an} \\ \text{algebra)}}} \circ (\tau_{A,A} \otimes \mathrm{id}_A) \circ \left(e_{C,A} \otimes \underbrace{\mathrm{id}_{A \otimes A}}_{= \mathrm{id}_A \otimes \mathrm{id}_A} \right) \circ (\mathrm{id}_C \otimes g \otimes f) \circ (\mathrm{id}_C \otimes \Delta_C) \\
&= \mu_A \circ (\mathrm{id}_A \otimes \mu_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A) \circ (e_{C,A} \otimes \mathrm{id}_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f) \circ (\mathrm{id}_C \otimes \Delta_C) \,.
\end{aligned}
\tag{276}
$$

On the other hand, Proposition 9.3 **(a)** (applied to C, A, A, A, $e_{C,A}$, id_A instead of V, W, V', W', f, g) yields

$$
(\mathrm{id}_A \otimes e_{C,A}) \circ \tau_{C,A} = \tau_{A,A} \circ (e_{C,A} \otimes \mathrm{id}_A) \,. \tag{277}
$$

But applying (21) to $C \otimes A$, $A \otimes A$, $A \otimes A$, A, A, A, $e_{C,A} \otimes \mathrm{id}_A$, $\tau_{A,A}$, id_A, id_A instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$
(\tau_{A,A} \circ (e_{C,A} \otimes \mathrm{id}_A)) \otimes (\mathrm{id}_A \circ \mathrm{id}_A) = (\tau_{A,A} \otimes \mathrm{id}_A) \circ (e_{C,A} \otimes \mathrm{id}_A \otimes \mathrm{id}_A) \,.
$$

Thus,

$$
\begin{aligned}
&(\tau_{A,A} \otimes \mathrm{id}_A) \circ (e_{C,A} \otimes \mathrm{id}_A \otimes \mathrm{id}_A) \\
&= \underbrace{(\tau_{A,A} \circ (e_{C,A} \otimes \mathrm{id}_A))}_{\substack{= \left(\mathrm{id}_A \otimes e_{C,A}\right) \circ \tau_{C,A} \\ \text{(by (277))}}} \otimes (\mathrm{id}_A \circ \mathrm{id}_A) = ((\mathrm{id}_A \otimes e_{C,A}) \circ \tau_{C,A}) \otimes (\mathrm{id}_A \circ \mathrm{id}_A) \\
&= \left(\mathrm{id}_A \otimes \underbrace{e_{C,A}}_{\substack{= \eta_A \circ \varepsilon_C \\ \text{(by the definition of } e_{C,A}\text{)}}} \otimes \mathrm{id}_A \right) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \\
&\qquad \left(\begin{array}{c} \text{by (21), applied to } C \otimes A,\ A \otimes C,\ A \otimes A,\ A,\ A,\ A,\ \tau_{C,A},\ \mathrm{id}_A \otimes e_{C,A},\ \mathrm{id}_A\,,\ \mathrm{id}_A \\ \text{instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta' \end{array} \right) \\
&= (\mathrm{id}_A \otimes (\eta_A \circ \varepsilon_C) \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \,.
\end{aligned}
\tag{278}
$$

But (211) (applied to $P = A$, $Q = A$, $R_1 = C$, $R_2 = k$, $R_3 = A$, $\varphi = \varepsilon_C$ and $\psi = \eta_A$) yields

$$(\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) = \mathrm{id}_A \otimes (\eta_A \circ \varepsilon_C) \otimes \mathrm{id}_A \,. \tag{279}$$

Hence, (278) becomes

$$\begin{aligned} &(\tau_{A,A} \otimes \mathrm{id}_A) \circ (e_{C,A} \otimes \mathrm{id}_A \otimes \mathrm{id}_A) \\ &= \underbrace{(\mathrm{id}_A \otimes (\eta_A \circ \varepsilon_C) \otimes \mathrm{id}_A)}_{\substack{= (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \\ \text{(by (279))}}} \circ (\tau_{C,A} \otimes \mathrm{id}_A) \\ &= (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \,. \end{aligned} \tag{280}$$

Now, let $\mathrm{kan}_{k \otimes A, A}$ be the canonical isomorphism $k \otimes A \to A$ which sends every $\lambda \otimes a \in k \otimes A$ to $\lambda a \in A$. Then, by the axioms of an algebra, we have $\mu_A \circ (\eta_A \otimes \mathrm{id}_A) = \mathrm{kan}_{k \otimes A, A}$ (since A is a k-algebra).

Applying (21) to A, A, A, $k \otimes A$, $A \otimes A$, A, id_A, id_A, $\eta_A \otimes \mathrm{id}_A$, μ_A instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mathrm{id}_A \circ \mathrm{id}_A) \otimes (\mu_A \circ (\eta_A \otimes \mathrm{id}_A)) = (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_A) \,.$$

Thus,

$$\begin{aligned} (\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_A) &= \underbrace{(\mathrm{id}_A \circ \mathrm{id}_A)}_{= \mathrm{id}_A} \otimes \underbrace{(\mu_A \circ (\eta_A \otimes \mathrm{id}_A))}_{= \mathrm{kan}_{k \otimes A, A}} \\ &= \mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A, A} \,. \end{aligned} \tag{281}$$

Now,

$$\begin{aligned} &(\mathrm{id}_A \otimes \mu_A) \circ \underbrace{(\tau_{A,A} \otimes \mathrm{id}_A) \circ (e_{C,A} \otimes \mathrm{id}_A \otimes \mathrm{id}_A)}_{\substack{= (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_A) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ \left(\tau_{C,A} \otimes \mathrm{id}_A\right) \\ \text{(by (280))}}} \\ &= \underbrace{(\mathrm{id}_A \otimes \mu_A) \circ (\mathrm{id}_A \otimes \eta_A \otimes \mathrm{id}_A)}_{\substack{= \mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A, A} \\ \text{(by (281))}}} \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \\ &= (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A, A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \,. \end{aligned} \tag{282}$$

Thus, (276) becomes

$$\begin{aligned} &(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C) \\ &= \mu_A \circ \underbrace{(\mathrm{id}_A \otimes \mu_A) \circ (\tau_{A,A} \otimes \mathrm{id}_A) \circ (e_{C,A} \otimes \mathrm{id}_A \otimes \mathrm{id}_A)}_{\substack{= \left(\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A, A}\right) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ \left(\tau_{C,A} \otimes \mathrm{id}_A\right) \\ \text{(by (282))}}} \circ (\mathrm{id}_C \otimes g \otimes f) \circ (\mathrm{id}_C \otimes \Delta_C) \\ &= \mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A, A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f) \circ (\mathrm{id}_C \otimes \Delta_C) \,. \end{aligned} \tag{283}$$

From this point on, our proof will not be analogous to the proof of Proposition 25.2 anymore. We can easily show that

$$\begin{aligned} &\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A, A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f) \\ &= \mathrm{kan}_{k \otimes A, A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f))) \,. \end{aligned} \tag{284}$$

[136]

Also, applying (21) to C, C, C, C, $C \otimes C$, A, id_C, id_C, Δ_C, $\mu_A \circ (g \otimes f)$ instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\mathrm{id}_C \circ \mathrm{id}_C) \otimes (\mu_A \circ (g \otimes f) \circ \Delta_C) = (\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f))) \circ (\mathrm{id}_C \otimes \Delta_C),$$

so that

$$\begin{aligned}(\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f))) \circ (\mathrm{id}_C \otimes \Delta_C) &= \underbrace{(\mathrm{id}_C \circ \mathrm{id}_C)}_{=\mathrm{id}_C} \otimes \underbrace{(\mu_A \circ (g \otimes f) \circ \Delta_C)}_{\substack{=e_{C,A} \\ \text{(by (272))}}} \\ &= \mathrm{id}_C \otimes e_{C,A}. \end{aligned} \tag{285}$$

[136] *Proof of (284):* Every $c \in C$, $d \in C$ and $e \in C$ satisfy

$$\begin{aligned}
&(\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f))(c \otimes d \otimes e) \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A)) \underbrace{((\mathrm{id}_C \otimes g \otimes f)(c \otimes d \otimes e))}_{=\mathrm{id}_C(c) \otimes g(d) \otimes f(e)} \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A)) \left(\underbrace{\mathrm{id}_C(c)}_{=c} \otimes g(d) \otimes f(e) \right) \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A))(c \otimes g(d) \otimes f(e)) \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A)) \underbrace{((\tau_{C,A} \otimes \mathrm{id}_A)(c \otimes g(d) \otimes f(e)))}_{=\tau_{C,A}(c \otimes g(d)) \otimes \mathrm{id}_A(f(e))} \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A)) \left(\underbrace{\tau_{C,A}(c \otimes g(d))}_{\substack{=g(d) \otimes c \\ \text{(by the definition of } \tau_{C,A}\text{)}}} \otimes \underbrace{\mathrm{id}_A(f(e))}_{=f(e)} \right) \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A))(g(d) \otimes c \otimes f(e)) \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A})) \underbrace{((\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A)(g(d) \otimes c \otimes f(e)))}_{=\mathrm{id}_A(g(d)) \otimes \varepsilon_C(c) \otimes \mathrm{id}_A(f(e))} \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A})) \left(\underbrace{\mathrm{id}_A(g(d))}_{=g(d)} \otimes \varepsilon_C(c) \otimes \underbrace{\mathrm{id}_A(f(e))}_{=f(e)} \right) \\
&= (\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A}))(g(d) \otimes \varepsilon_C(c) \otimes f(e)) \\
&= \mu_A \underbrace{((\mathrm{id}_A \otimes \mathrm{kan}_{k \otimes A,A})(g(d) \otimes \varepsilon_C(c) \otimes f(e)))}_{=\mathrm{id}_A(g(d)) \otimes \mathrm{kan}_{k \otimes A,A}(\varepsilon_C(c) \otimes f(e))} \\
&= \mu_A(\mathrm{id}_A(g(d)) \otimes \mathrm{kan}_{k \otimes A,A}(\varepsilon_C(c) \otimes f(e))) \\
&= \underbrace{\mathrm{id}_A(g(d))}_{=g(d)} \cdot \underbrace{\mathrm{kan}_{k \otimes A,A}(\varepsilon_C(c) \otimes f(e))}_{\substack{=\varepsilon_C(c) f(e) \\ \text{(by the definition of } \mathrm{kan}_{k \otimes A,A}\text{)}}} \qquad \text{(by the definition of } \mu_A\text{)} \\
&= g(d)\, \varepsilon_C(c)\, f(e) = \varepsilon_C(c)\, g(d)\, f(e)
\end{aligned}$$

Now, (283) becomes

$$
\begin{aligned}
&(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C) \\
&= \underbrace{\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k\otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f)}_{\substack{= \mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f))) \\ \text{(by (284))}}} \circ (\mathrm{id}_C \otimes \Delta_C) \\
&= \mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ \underbrace{(\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f))) \circ (\mathrm{id}_C \otimes \Delta_C)}_{\substack{= \mathrm{id}_C \otimes e_{C,A} \\ \text{(by (285))}}} \\
&= \mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes e_{C,A}) .
\end{aligned}
$$

---

and

$$
\begin{aligned}
&(\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f)))) (c \otimes d \otimes e) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) \underbrace{((\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f))) (c \otimes d \otimes e))}_{= \mathrm{id}_C(c) \otimes (\mu_A \circ (g \otimes f))(d \otimes e)} \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) \left(\underbrace{\mathrm{id}_C (c)}_{=c} \otimes \underbrace{(\mu_A \circ (g \otimes f)) (d \otimes e)}_{= \mu_A((g\otimes f)(d\otimes e))} \right) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) \left(c \otimes \mu_A \underbrace{((g \otimes f) (d \otimes e))}_{= g(d) \otimes f(e)} \right) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) \left(c \otimes \underbrace{\mu_A (g (d) \otimes f (e))}_{\substack{= g(d) f(e) \\ \text{(by the definition of } \mu_A\text{)}}} \right) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) (c \otimes g (d) f (e)) = (\mu_A \circ \mathrm{kan}_{k\otimes A,A}) \underbrace{((\varepsilon_C \otimes \mathrm{id}_A) (c \otimes g (d) f (e)))}_{= \varepsilon_C(c) \otimes \mathrm{id}_A(g(d) f(e))} \\
&= \mathrm{kan}_{k\otimes A,A} \left(\varepsilon_C (c) \otimes \underbrace{\mathrm{id}_A (g (d) f (e))}_{= g(d) f(e)} \right) = \mathrm{kan}_{k\otimes A,A} (\varepsilon_C (c) \otimes g (d) f (e)) \\
&= \varepsilon_C (c) g (d) f (e) \qquad \text{(by the definition of } \mathrm{kan}_{k\otimes A,A}) .
\end{aligned}
$$

Thus, every $c \in C$, $d \in C$ and $e \in C$ satisfy

$$
\begin{aligned}
&(\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k\otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f)) (c \otimes d \otimes e) \\
&= \varepsilon_C (c) g (d) f (e) = (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f)))) (c \otimes d \otimes e) .
\end{aligned}
$$

In other words, the two maps
$\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k\otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f)$ and
$\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f)))$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words,

$$
\begin{aligned}
&\mu_A \circ (\mathrm{id}_A \otimes \mathrm{kan}_{k\otimes A,A}) \circ (\mathrm{id}_A \otimes \varepsilon_C \otimes \mathrm{id}_A) \circ (\tau_{C,A} \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes g \otimes f) \\
&= \mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes (\mu_A \circ (g \otimes f))) .
\end{aligned}
$$

This proves (284).

Thus, any $c \in C$ and $d \in C$ satisfy

$$\begin{aligned}
&((\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C))(c \otimes d) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A) \circ (\mathrm{id}_C \otimes e_{C,A}))(c \otimes d) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) \underbrace{((\mathrm{id}_C \otimes e_{C,A})(c \otimes d))}_{=\mathrm{id}_C(c)\otimes e_{C,A}(d)} \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) \left(\underbrace{\mathrm{id}_C(c)}_{=c} \otimes \underbrace{e_{C,A}}_{\substack{=\eta_A\circ\varepsilon_C \\ \text{(by the definition} \\ \text{of } e_{C,A})}} (d) \right) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A)) \left(c \otimes \underbrace{(\eta_A \circ \varepsilon_C)(d)}_{=\eta_A(\varepsilon_C(d))} \right) \\
&= (\mathrm{kan}_{k\otimes A,A} \circ (\varepsilon_C \otimes \mathrm{id}_A))(c \otimes \eta_A(\varepsilon_C(d))) = \mathrm{kan}_{k\otimes A,A} \underbrace{((\varepsilon_C \otimes \mathrm{id}_A)(c \otimes \eta_A(\varepsilon_C(d))))}_{=\varepsilon_C(c)\otimes \mathrm{id}_A(\eta_A(\varepsilon_C(d)))} \\
&= \mathrm{kan}_{k\otimes A,A} \left(\varepsilon_C(c) \otimes \underbrace{\mathrm{id}_A(\eta_A(\varepsilon_C(d)))}_{=\eta_A(\varepsilon_C(d))} \right) = \mathrm{kan}_{k\otimes A,A}(\varepsilon_C(c) \otimes \eta_A(\varepsilon_C(d))) \\
&= \varepsilon_C(c)\,\eta_A(\varepsilon_C(d)) \qquad \text{(by the definition of } \mathrm{kan}_{k\otimes A,A}) \\
&= \eta_A(\varepsilon_C(c)\,\varepsilon_C(d)) \qquad \text{(since } \eta_A \text{ is } k\text{-linear}). \qquad (286)
\end{aligned}$$

On the other hand, any $c \in C$ and $d \in C$ satisfy $\varepsilon_{C\otimes C}(c \otimes d) = \varepsilon_C(c)\,\varepsilon_C(d)$ [137]. Hence, every $c \in C$ and $d \in C$ satisfy

$$\begin{aligned}
e_{C\otimes C,A}(c \otimes d) &= (\eta_A \circ \varepsilon_{C\otimes C})(c \otimes d) \\
&\qquad \text{(since } e_{C\otimes C,A} = \eta_A \circ \varepsilon_{C\otimes C} \text{ by the definition of } e_{C\otimes C,A}) \\
&= \eta_A \underbrace{(\varepsilon_{C\otimes C}(c \otimes d))}_{=\varepsilon_C(c)\varepsilon_C(d)} = \eta_A(\varepsilon_C(c)\,\varepsilon_C(d)).
\end{aligned}$$

Comparing this with (286), we see that any $c \in C$ and $d \in C$ satisfy

$$((\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C))(c \otimes d) = e_{C\otimes C,A}(c \otimes d).$$

In other words, the two maps $(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C)$ and $e_{C\otimes C,A}$ are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be

[137] *Proof.* Let $c \in C$ and $d \in C$. By the definition of the k-coalgebra $C \otimes C$, we have $\varepsilon_{C\otimes C} = \mathrm{kan}_{k\otimes k,k} \circ (\varepsilon_C \otimes \varepsilon_C)$, where $\mathrm{kan}_{k\otimes k,k} : k \otimes k \to k$ is the canonical isomorphism which sends every $\lambda \otimes \lambda' \in k \otimes k$ to $\lambda\lambda' \in k$. Thus,

$$\begin{aligned}
\varepsilon_{C\otimes C}(c \otimes d) &= (\mathrm{kan}_{k\otimes k,k} \circ (\varepsilon_C \otimes \varepsilon_C))(c \otimes d) = \mathrm{kan}_{k\otimes k,k} \underbrace{((\varepsilon_C \otimes \varepsilon_C)(c \otimes d))}_{=\varepsilon_C(c)\otimes\varepsilon_C(d)} \\
&= \mathrm{kan}_{k\otimes k,k}(\varepsilon_C(c) \otimes \varepsilon_C(d)) = \varepsilon_C(c)\,\varepsilon_C(d)
\end{aligned}$$

(by the definition of $\mathrm{kan}_{k\otimes k,k}$), qed.

identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C) = e_{C \otimes C, A}$, so that (266) is proven.

Proof of (267): Since C is a k-bialgebra, the multiplication map μ_C of C is a k-coalgebra homomorphism (by the axioms of a bialgebra). Thus, $(\mu_C \otimes \mu_C) \circ \Delta_{C \otimes C} = \Delta_C \circ \mu_C$ and $\varepsilon_{C \otimes C} = \varepsilon_C \circ \mu_C$.

By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$. Thus,

$$\mu_A \circ (f \otimes g) \circ \Delta_C = f * g = e_{C,A} = \eta_A \circ \varepsilon_C \tag{287}$$

(by the definition of $e_{C,A}$).

By the definition of convolution,

$$\begin{aligned}
(f \circ \mu_C) * (g \circ \mu_C) &= \mu_A \circ \underbrace{((f \circ \mu_C) \otimes (g \circ \mu_C))}_{\substack{= (f \otimes g) \circ (\mu_C \otimes \mu_C) \\ \text{(by (21), applied to } C \otimes C,\ C,\ A,\ C \otimes C,\ C,\ A, \\ \mu_C,\ f,\ \mu_C,\ g \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta')}} \circ \Delta_{C \otimes C} \\
&= \mu_A \circ (f \otimes g) \circ \underbrace{(\mu_C \otimes \mu_C) \circ \Delta_{C \otimes C}}_{= \Delta_C \circ \mu_C} = \underbrace{\mu_A \circ (f \otimes g) \circ \Delta_C}_{\substack{= \eta_A \circ \varepsilon_C \\ \text{(by (287))}}} \circ \mu_C \\
&= \eta_A \circ \underbrace{\varepsilon_C \circ \mu_C}_{= \varepsilon_{C \otimes C}} = \eta_A \circ \varepsilon_{C \otimes C} = e_{C \otimes C, A}
\end{aligned}$$

(since $e_{C \otimes C, A}$ is defined as $\eta_A \circ \varepsilon_{C \otimes C}$). This proves (267).

Now, let us finish the proof of Proposition 26.2: Comparing the equalities

$$\begin{aligned}
&\underbrace{(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * (f \circ \mu_C)}_{\substack{= e_{C \otimes C, A} \\ \text{(by (266))}}} * (g \circ \mu_C) \\
&= e_{C \otimes C, A} * (g \circ \mu_C) = g \circ \mu_C
\end{aligned}$$

and

$$\begin{aligned}
&(\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * \underbrace{(f \circ \mu_C) * (g \circ \mu_C)}_{\substack{= e_{C \otimes C, A} \\ \text{(by (267))}}} \\
&= (\mu_{A^{\mathrm{op}}} \circ (g \otimes g)) * e_{C \otimes C, A} = \mu_{A^{\mathrm{op}}} \circ (g \otimes g),
\end{aligned}$$

we obtain

$$g \circ \mu_C = \mu_{A^{\mathrm{op}}} \circ (g \otimes g). \tag{288}$$

We will now prove that $g \circ \eta_C = \eta_{A^{\mathrm{op}}}$.

We know that C is a k-bialgebra. By the axioms of a bialgebra, this yields

$\Delta_C(1_C) = 1_C \otimes 1_C$ and $\varepsilon_C(1_C) = 1$. Now,

$$\underbrace{(\eta_A \circ \varepsilon_C)}_{\substack{=\mu_A \circ (f \otimes g) \circ \Delta_C \\ \text{(by (287))}}}(1_C) = (\mu_A \circ (f \otimes g) \circ \Delta_C)(1_C) = (\mu_A \circ (f \otimes g))\underbrace{(\Delta_C(1_C))}_{=1_C \otimes 1_C} = (\mu_A \circ (f \otimes g))(1_C \otimes 1_C)$$

$$= \mu_A \underbrace{((f \otimes g)(1_C \otimes 1_C))}_{=f(1_C) \otimes g(1_C)} = \mu_A(f(1_C) \otimes g(1_C))$$

$$= \underbrace{f(1_C)}_{\substack{=1_A \\ \text{(since } f \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} g(1_C) \qquad \text{(by the definition of } \mu_A)$$

$$= 1_A g(1_C) = g(1_C).$$

Compared to

$$(\eta_A \circ \varepsilon_C)(1_C) = \eta_A \underbrace{(\varepsilon_C(1_C))}_{=1} = \eta_A(1) = 1 \cdot 1_A \qquad \text{(by the definition of } \eta_A)$$

$$= 1_A,$$

this yields $g(1_C) = 1_A$. Thus, every $\lambda \in k$ satisfies

$$(g \circ \eta_C)(\lambda) = g \underbrace{(\eta_C(\lambda))}_{\substack{=\lambda \cdot 1_C \\ \text{(by the definition of } \eta_C)}} = g(\lambda \cdot 1_C) = \lambda \underbrace{g(1_C)}_{=1_A} \qquad \text{(since } g \text{ is } k\text{-linear)}$$

$$= \lambda \cdot 1_A = \eta_A(\lambda) \qquad (\text{since } \eta_A(\lambda) = \lambda \cdot 1_A \text{ by the definition of } \eta_A)$$

$$= \eta_{A^{\mathrm{op}}}(\lambda) \qquad (\text{since } \eta_{A^{\mathrm{op}}} = \eta_A \text{ (by the definition of } A^{\mathrm{op}}), \text{ so that } \eta_{A^{\mathrm{op}}}(\lambda) = \eta_A(\lambda))$$

In other words, $g \circ \eta_C = \eta_{A^{\mathrm{op}}}$. Combined with (288), this yields that g is a k-algebra homomorphism from C to A^{op}. Since $g = f^{*(-1)}$, this rewrites as follows: $f^{*(-1)}$ is a k-algebra homomorphism from C to A^{op}. This proves Proposition 26.2. □

§27. The Euler operator

Recall what we did in Theorems 4.1 and 15.3: We showed that if k is a field of characteristic 0, and H is a connected filtered k-bialgebra, then the map $\operatorname{Log}\mathrm{id} \in \mathcal{L}(H, H)$ is a projection if H is either commutative or cocommutative. (This is not an "if and only if" assertion since $\operatorname{Log}\mathrm{id}$ can also be a projection for some connected filtered k-bialgebras H which are neither commutative nor cocommutative; but in general, $\operatorname{Log}\mathrm{id}$ is not a projection[138].) We will now study two maps that have similar properties to those of $\operatorname{Log}\mathrm{id}$, but are defined for **graded** Hopf algebras only. Whereas $\operatorname{Log}\mathrm{id}$ is often referred to in literature as the *Eulerian idempotent*, these new maps are known as the called *Dynkin idempotents*. But let us first develop some theory of graded vector spaces.

Definition 27.1. Let k be a field. Let V be a graded k-vector space. Then, $V = \bigoplus_{\ell \in \mathbb{N}} V_\ell$. The map $\bigoplus_{\ell \in \mathbb{N}} (\ell \cdot \mathrm{id}_{V_\ell}) : \bigoplus_{\ell \in \mathbb{N}} V_\ell \to \bigoplus_{\ell \in \mathbb{N}} V_\ell$ is a k-linear map from

[138] Not even when H is a connected graded involutive k-Hopf algebra.

V to V (because it is a k-linear map from $\bigoplus_{\ell\in\mathbb{N}} V_\ell$ to $\bigoplus_{\ell\in\mathbb{N}} V_\ell$, but we have $\bigoplus_{\ell\in\mathbb{N}} V_\ell = V$). This map will be denoted by E_V and referred to as the *Euler operator*[139] of the graded k-vector space V.

Here is something pretty obvious:

Proposition 27.2. Let k be a field. Let V be a graded k-vector space.

(a) For any $n \in \mathbb{N}$ and $v \in V_n$, we have $E_V(v) = nv$.

(b) The map E_V is graded.

(c) Let k be a field of characteristic 0. Then, $\operatorname{Ker}(E_V) = V_0$.

We will give a detailed proof of this later.

We next state a fact about Euler operators on tensor products:

Proposition 27.3. Let k be a field. Let V and W be two graded k-vector spaces. Then,

$$E_{V\otimes W} = E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W.$$

Again, this will be shown later. Also:

Proposition 27.4. Let k be a field. Let V and W be graded k-vector spaces. Let $f : V \to W$ be a graded k-linear map. Then, $f \circ E_V = E_W \circ f$.

Before we show these facts, we make a definition that generalizes Definition 27.1:

Definition 27.5. Let k be a field. Let $(a_\ell)_{\ell\in\mathbb{N}}$ be a sequence of elements of k. Let V be a graded k-vector space. Then, $V = \bigoplus_{\ell\in\mathbb{N}} V_\ell$. The map $\bigoplus_{\ell\in\mathbb{N}} (a_\ell \cdot \mathrm{id}_{V_\ell}) : \bigoplus_{\ell\in\mathbb{N}} V_\ell \to \bigoplus_{\ell\in\mathbb{N}} V_\ell$ is a k-linear map from V to V (because it is a k-linear map from $\bigoplus_{\ell\in\mathbb{N}} V_\ell$ to $\bigoplus_{\ell\in\mathbb{N}} V_\ell$, but we have $\bigoplus_{\ell\in\mathbb{N}} V_\ell = V$). This map will be denoted by $E_V^{(a_\ell)_{\ell\in\mathbb{N}}}$ and referred to as the $(a_\ell)_{\ell\in\mathbb{N}}$-*Euler operator*[140] of the graded k-vector space V.

Remark 27.6. Let k be a field. Let V be a graded k-vector space. Then, $E_V = E_V^{(\ell)_{\ell\in\mathbb{N}}}$.

Proof of Remark 27.6. By the definition of E_V, we have $E_V = \bigoplus_{\ell\in\mathbb{N}} (\ell \cdot \mathrm{id}_{V_\ell})$. By the definition of $E_V^{(\ell)_{\ell\in\mathbb{N}}}$, we have $E_V^{(\ell)_{\ell\in\mathbb{N}}} = \bigoplus_{\ell\in\mathbb{N}} (\ell \cdot \mathrm{id}_{V_\ell})$. Thus, $E_V = \bigoplus_{\ell\in\mathbb{N}} (\ell \cdot \mathrm{id}_{V_\ell}) = E_V^{(\ell)_{\ell\in\mathbb{N}}}$. This proves Remark 27.6. □

Proposition 27.7. Let k be a field. Let $(a_\ell)_{\ell\in\mathbb{N}}$ be a sequence of elements of k. Let V be a graded k-vector space.

(a) For any $n \in \mathbb{N}$ and $v \in V_n$, we have $E_V^{(a_\ell)_{\ell\in\mathbb{N}}}(v) = a_n v$.

(b) The map $E_V^{(a_\ell)_{\ell\in\mathbb{N}}}$ is graded.

[139] not to be confused with the Eulerian idempotent

[140] not to be confused with the Eulerian idempotent

Proof of Proposition 27.7. **(a)** Let $n \in \mathbb{N}$. Let $\iota_n : V_n \to \bigoplus_{\ell \in \mathbb{N}} V_\ell$ be the canonical injection of the n-th addend into the direct sum. Then, by the universal property of the direct sum of linear maps, the diagram

$$\begin{array}{ccc} V_n & \xrightarrow{\iota_n} & \bigoplus_{\ell \in \mathbb{N}} V_\ell \\ {\scriptstyle a_n \cdot \mathrm{id}_{V_n}} \downarrow & & \downarrow {\scriptstyle \bigoplus_{\ell \in \mathbb{N}} \left(a_\ell \cdot \mathrm{id}_{V_\ell}\right)} \\ V_n & \xrightarrow[\iota_n]{} & \bigoplus_{\ell \in \mathbb{N}} V_\ell \end{array}$$

is commutative. In other words, $\left(\bigoplus_{\ell \in \mathbb{N}} (a_\ell \cdot \mathrm{id}_{V_\ell}) \right) \circ \iota_n = \iota_n \circ (a_n \cdot \mathrm{id}_{V_n})$. Now, let $v \in V_n$ be arbitrary. Then, $\iota_n(v) = v$ (because we regard the canonical injection ι_n as an inclusion). Also, by the definition of E_V, we have $E_V^{(a_\ell)_{\ell \in \mathbb{N}}} = \bigoplus_{\ell \in \mathbb{N}} (a_\ell \cdot \mathrm{id}_{V_\ell})$ and thus

$$\underbrace{E_V^{(a_\ell)_{\ell \in \mathbb{N}}}}_{= \bigoplus_{\ell \in \mathbb{N}} \left(a_\ell \cdot \mathrm{id}_{V_\ell}\right)} \underbrace{(v)}_{= \iota_n(v)} = \left(\bigoplus_{\ell \in \mathbb{N}} (a_\ell \cdot \mathrm{id}_{V_\ell}) \right) (\iota_n(v)) = \underbrace{\left(\left(\bigoplus_{\ell \in \mathbb{N}} (a_\ell \cdot \mathrm{id}_{V_\ell}) \right) \circ \iota_n \right)}_{= \iota_n \circ (a_n \cdot \mathrm{id}_{V_n})} (v)$$

$$= (\iota_n \circ (a_n \cdot \mathrm{id}_{V_n}))(v) = \iota_n \underbrace{((a_n \cdot \mathrm{id}_{V_n})(v))}_{= a_n v} = \iota_n(a_n v) = a_n v$$

(since we regard the canonical injection ι_n as an inclusion).

This proves Proposition 27.7 **(a)**.

(b) Let $n \in \mathbb{N}$. Then, every $v \in V_n$ satisfies

$$E_V^{(a_\ell)_{\ell \in \mathbb{N}}}(v) = \underbrace{a_n}_{\in k} \underbrace{v}_{\in V_n} \qquad \text{(by Proposition 27.2 (a))}$$

$$\in kV_n \subseteq V_n \qquad \text{(since } V_n \text{ is a } k\text{-vector space)}.$$

In other words, $E_V^{(a_\ell)_{\ell \in \mathbb{N}}}(V_n) \subseteq V_n$.

Now, forget that we fixed v. We have thus shown that $E_V^{(a_\ell)_{\ell \in \mathbb{N}}}(V_n) \subseteq V_n$ for every $n \in \mathbb{N}$. In other words, $E_V^{(a_\ell)_{\ell \in \mathbb{N}}}$ is graded. This proves Proposition 27.7 **(b)**. □

Proposition 27.8. Let k be a field. Let $(a_\ell)_{\ell \in \mathbb{N}}$ be a sequence of elements of k. Let V and W be graded k-vector spaces. Let $f : V \to W$ be a graded k-linear map. Then, $f \circ E_V^{(a_\ell)_{\ell \in \mathbb{N}}} = E_W^{(a_\ell)_{\ell \in \mathbb{N}}} \circ f$.

Proof of Proposition 27.8. Let $n \in \mathbb{N}$ be arbitrary. Let $v \in V_n$. Then, $f(v) \in f(V_n) \subseteq W_n$ (since f is graded), so that $E_W^{(a_\ell)_{\ell \in \mathbb{N}}}(f(v)) = a_n f(v)$ (by Proposition 27.7 **(a)**, applied to $f(v)$ and W instead of v and V). On the other hand, since $v \in V_n$, we have $E_V^{(a_\ell)_{\ell \in \mathbb{N}}}(v) = a_n v$ (by Proposition 27.7 **(a)**). Thus,

$$\left(f \circ E_V^{(a_\ell)_{\ell \in \mathbb{N}}} \right)(v) = f \underbrace{\left(E_V^{(a_\ell)_{\ell \in \mathbb{N}}}(v) \right)}_{= a_n v} = f(a_n v) = a_n f(v) \qquad \text{(since } f \text{ is } k\text{-linear)}$$

$$= E_W^{(a_\ell)_{\ell \in \mathbb{N}}}(f(v)) = \left(E_W^{(a_\ell)_{\ell \in \mathbb{N}}} \circ f \right)(v),$$

so that

$$\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)(v) = \underbrace{\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}}\right)(v)}_{=\left(E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)(v)} - \left(E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)(v)$$
$$= \left(E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)(v) - \left(E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)(v) = 0.$$

Thus, $v \in \operatorname{Ker}\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)$.

Now, forget that we fixed v. We thus have shown that every $v \in V_n$ satisfies $v \in \operatorname{Ker}\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)$. In other words, $V_n \subseteq \operatorname{Ker}\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)$.

Now forget that we fixed n. We thus have shown that every $n \in \mathbb{N}$ satisfies $V_n \subseteq \operatorname{Ker}\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)$. But V is a graded k-vector space, so that $V = \bigoplus_{n\in\mathbb{N}} V_n = \sum_{n\in\mathbb{N}} V_n$ (since direct sums are sums). Thus,

$$V = \sum_{n\in\mathbb{N}} \underbrace{V_n}_{\subseteq \operatorname{Ker}\left(f\circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}}\circ f\right)} \subseteq \sum_{n\in\mathbb{N}} \operatorname{Ker}\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)$$
$$\subseteq \operatorname{Ker}\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)$$

(since $\operatorname{Ker}\left(f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f\right)$ is a k-vector space). In other words, $f\circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} - E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f = 0$, so that $f \circ E_V^{(a_\ell)_{\ell\in\mathbb{N}}} = E_W^{(a_\ell)_{\ell\in\mathbb{N}}} \circ f$. This proves Proposition 27.8. □

Proof of Proposition 27.2. **(a)** Let $n \in \mathbb{N}$ and $v \in V_n$. Applying Proposition 27.7 **(a)** to $(a_\ell)_{\ell\in\mathbb{N}} = (\ell)_{\ell\in\mathbb{N}}$, we see that $E_V^{(\ell)_{\ell\in\mathbb{N}}}(v) = nv$. Since $E_V^{(\ell)_{\ell\in\mathbb{N}}} = E_V$ (by Remark 27.6), this rewrites as $E_V(v) = nv$. This proves Proposition 27.2 **(a)**.

(b) Applying Proposition 27.7 **(b)** to $(a_\ell)_{\ell\in\mathbb{N}} = (\ell)_{\ell\in\mathbb{N}}$, we see that $E_V^{(\ell)_{\ell\in\mathbb{N}}}$ is graded. Since $E_V^{(\ell)_{\ell\in\mathbb{N}}} = E_V$ (by Remark 27.6), this shows that E_V is graded. This proves Proposition 27.2 **(b)**.

(c) Let $v \in \operatorname{Ker}(E_V)$. Then, $v \in V$ and $E_V(v) = 0$. Since $v \in V = \bigoplus_{\ell\in\mathbb{N}} V_\ell$, we can write v in the form $v = \sum_{\ell\in\mathbb{N}} v_\ell$ for some family $(v_\ell)_{\ell\in\mathbb{N}}$ of vectors in V satisfying the following properties:

- All but finitely many $\ell \in \mathbb{N}$ satisfy $v_\ell = 0$.
- We have $v_\ell \in V_\ell$ for every $\ell \in \mathbb{N}$.

Consider this family $(v_\ell)_{\ell\in\mathbb{N}}$. Every $\ell \in \mathbb{N}$ satisfies $v_\ell \in V_\ell$ and thus $E_V(v_\ell) = \ell v_\ell$ (by Proposition 27.2 **(a)**, applied to ℓ and v_ℓ instead of n and v). Since $E_V(v) = 0$,

we have

$$\begin{aligned} 0 = E_V(v) &= E_V\left(\sum_{\ell\in\mathbb{N}} v_\ell\right) \qquad \left(\text{since } v = \sum_{\ell\in\mathbb{N}} v_\ell\right) \\ &= \sum_{\ell\in\mathbb{N}} \underbrace{E_V(v_\ell)}_{=\ell v_\ell} \qquad (\text{since } E_V \text{ is } k\text{-linear}) \\ &= \sum_{\ell\in\mathbb{N}} \ell v_\ell. \end{aligned}$$

In other words, $\sum_{\ell\in\mathbb{N}} \ell v_\ell = 0$.

Note that all but finitely many $\ell \in \mathbb{N}$ satisfy $\ell v_\ell = 0$ (because all but finitely many $\ell \in \mathbb{N}$ satisfy $v_\ell = 0$). Also, $\ell v_\ell \in V_\ell$ for every $\ell \in \mathbb{N}$ (because $v_\ell \in V_\ell$ for every $\ell \in \mathbb{N}$, and therefore $\underbrace{\ell}_{\in k}\underbrace{v_\ell}_{\in V_\ell} \in kV_\ell \subseteq V_\ell$ (since V_ℓ is a k-vector space) for every $\ell \in \mathbb{N}$).

But $\bigoplus_{\ell\in\mathbb{N}} V_\ell$ is a direct sum. Therefore, the vector spaces V_ℓ for $\ell \in \mathbb{N}$ are linearly disjoint. In other words, every family $(a_\ell)_{\ell\in\mathbb{N}}$ satisfying the conditions

$$\begin{aligned} &(\text{all but finitely many } \ell \in \mathbb{N} \text{ satisfy } a_\ell = 0), \\ &(a_\ell \in V_\ell \text{ for every } \ell \in \mathbb{N}), \qquad \text{and} \\ &\sum_{\ell\in\mathbb{N}} a_\ell = 0 \end{aligned}$$

must satisfy $(a_\ell)_{\ell\in\mathbb{N}} = (0)_{\ell\in\mathbb{N}}$. Applied to $(a_\ell)_{\ell\in\mathbb{N}} = (\ell v_\ell)_{\ell\in\mathbb{N}}$, this yields that $(\ell v_\ell)_{\ell\in\mathbb{N}} = 0$ (because we have shown that (all but finitely many $\ell \in \mathbb{N}$ satisfy $\ell v_\ell = 0$), that ($\ell v_\ell \in V_\ell$ for every $\ell \in \mathbb{N}$) and that $\sum_{\ell\in\mathbb{N}} \ell v_\ell = 0$). In other words, every $\ell \in \mathbb{N}$ satisfies $\ell v_\ell = 0$.

Now, for every positive integer ℓ, we have $v_\ell = \dfrac{1}{\ell}\underbrace{\ell v_\ell}_{=0} = \dfrac{1}{\ell}0 = 0$ (here, we used that k is a field of characteristic 0, so that $\dfrac{1}{\ell}$ is well-defined in k). Thus,

$$v = \sum_{\ell\in\mathbb{N}} v_\ell = v_0 + \sum_{\substack{\ell\in\mathbb{N};\\ \ell>0}} \underbrace{v_\ell}_{\substack{=0\\ (\text{since } \ell \text{ is a}\\ \text{positive integer})}} = v_0 + \sum_{\substack{\ell\in\mathbb{N};\\ \ell>0}} \underbrace{0}_{=0} = v_0 \in V_0$$

(since $v_\ell \in V_\ell$ for every $\ell \in \mathbb{N}$).

Now, forget that we fixed v. We have thus shown that every $v \in \operatorname{Ker}(E_V)$ satisfies $v \in V_0$. In other words, $\operatorname{Ker}(E_V) \subseteq V_0$. Combined with the fact that $V_0 \subseteq \operatorname{Ker}(E_V)$ [141], this yields that $\operatorname{Ker}(E_V) = V_0$. This proves Proposition 27.2 **(c)**. □

Proof of Proposition 27.4. By Remark 27.6, we have $E_V = E_V^{(\ell)_{\ell\in\mathbb{N}}}$. By Remark 27.6 (applied to W instead of V), we have $E_W = E_W^{(\ell)_{\ell\in\mathbb{N}}}$. By Proposition 27.8 (applied to

[141] *Proof.* Let $v \in V_0$ be arbitrary. Then, Proposition 27.2 **(a)** (applied to $n = 0$) yields that $E_V(v) = 0v = 0$, so that $v \in \operatorname{Ker}(E_V)$. Now forget that we fixed v. We have thus shown that every $v \in V_0$ satisfies $v \in \operatorname{Ker}(E_V)$. In other words, $V_0 \subseteq \operatorname{Ker}(E_V)$, qed.

$(a_\ell)_{\ell\in\mathbb{N}} = (\ell)_{\ell\in\mathbb{N}}$), we have $f \circ E_V^{(\ell)_{\ell\in\mathbb{N}}} = E_W^{(\ell)_{\ell\in\mathbb{N}}} \circ f$. Since $E_V^{(\ell)_{\ell\in\mathbb{N}}} = E_V$ and $E_W^{(\ell)_{\ell\in\mathbb{N}}} = E_W$, this rewrites as $f \circ E_V = E_W \circ f$. This proves Proposition 27.4. $\square$

Proof of Proposition 27.3. Since V is a graded k-vector space, we have $V = \bigoplus_{\ell\in\mathbb{N}} V_\ell$. Since W is a graded k-vector space, we have $W = \bigoplus_{m\in\mathbb{N}} W_m$. Since $V = \bigoplus_{\ell\in\mathbb{N}} V_\ell$ and $W = \bigoplus_{m\in\mathbb{N}} W_m$, we have

$$V \otimes W = \left(\bigoplus_{\ell\in\mathbb{N}} V_\ell\right) \otimes \left(\bigoplus_{m\in\mathbb{N}} W_m\right) = \bigoplus_{(\ell,m)\in\mathbb{N}^{\times 2}} V_\ell \otimes W_m$$

(by the distributivity of the tensor product).

Now, fix any $(\ell, m) \in \mathbb{N}^{\times 2}$. We are going to prove that $\left(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W}\right)|_{V_\ell \otimes W_m} = 0$.

By the usual definition of the grading on the tensor product $V \otimes W$, we have

$$(V \otimes W)_n = \sum_{i=0}^{n} V_i \otimes W_{n-i} \qquad \text{for every } n \in \mathbb{N}. \tag{289}$$

Now, let $v \in V_\ell$ and $w \in W_m$ be arbitrary. Let $n = \ell + m$. Then, $0 \le \ell \le n$. We have

$$\begin{aligned}
\underbrace{v}_{\in V_\ell} \otimes \underbrace{w}_{\in W_m} &\in V_\ell \otimes W_m = V_\ell \otimes W_{n-\ell} \qquad \left(\text{since } m = \underbrace{\ell + m}_{=n} - \ell = n - \ell\right) \\
&\subseteq \sum_{i=0}^{n} V_i \otimes W_{n-i} \qquad \left(\begin{array}{c}\text{since } V_\ell \otimes W_{n-\ell} \text{ is an addend of the sum } \sum_{i=0}^{n} V_i \otimes W_{n-i} \\ \text{(namely, the addend for } i = \ell)\end{array}\right) \\
&= (V \otimes W)_n \qquad (\text{by (289)}),
\end{aligned}$$

so that $E_{V\otimes W}(v \otimes w) = n(v \otimes w)$ (by Proposition 27.2 **(a)**, applied to $v \otimes w$ and $V \otimes W$ instead of v and V). On the other hand, due to $v \in V_\ell$, we have $E_V(v) = \ell v$ (by Proposition 27.2 **(a)**, applied to ℓ instead of n). Due to $w \in W_m$, we have $E_W(w) = mw$ (by Proposition 27.2 **(a)**, applied to m, w and W instead of n, v and V). Thus,

$$\begin{aligned}
&\left(\left(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W}\right)|_{V_\ell \otimes W_m}\right)(v \otimes w) \\
&= \left(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W}\right)(v \otimes w) \\
&= \underbrace{\left(E_V \otimes \mathrm{id}_W\right)(v \otimes w)}_{=E_V(v)\otimes \mathrm{id}_W(w)} + \underbrace{\left(\mathrm{id}_V \otimes E_W\right)(v \otimes w)}_{=\mathrm{id}_V(v)\otimes E_W(w)} - \underbrace{E_{V\otimes W}(v \otimes w)}_{=n(v\otimes w)} \\
&= \underbrace{E_V(v)}_{=\ell v} \otimes \underbrace{\mathrm{id}_W(w)}_{=w} + \underbrace{\mathrm{id}_V(v)}_{=v} \otimes \underbrace{E_W(w)}_{=mw} - \underbrace{n}_{=\ell+m}(v \otimes w) \\
&= \underbrace{\ell v \otimes w}_{=\ell(v\otimes w)} + \underbrace{v \otimes mw}_{=m(v\otimes w)} - (\ell + m)(v \otimes w) = \ell(v \otimes w) + m(v \otimes w) - (\ell + m)(v \otimes w) \\
&= \underbrace{(\ell + m - (\ell + m))}_{=0}(v \otimes w) = 0 = 0(v \otimes w).
\end{aligned}$$

Now, forget that we fixed v and w. We thus have proven that $((E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W}) \mid_{V_\ell \otimes W_m})(v \otimes w) = 0\,(v \otimes w)$ for any $v \in V_\ell$ and $w \in W_m$. In other words, the two maps $(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W}) \mid_{V_\ell \otimes W_m}$ and 0 are equal on every pure tensor. But since these two maps are k-linear, this yields that these maps must be identic (because whenever two k-linear maps from a tensor product are equal on every pure tensor, they must be identic). In other words, $(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W}) \mid_{V_\ell \otimes W_m} = 0$. Hence,

$$\begin{aligned}(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W})(V_\ell \otimes W_m) &= \underbrace{((E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W}) \mid_{V_\ell \otimes W_m})}_{=0}(V_\ell \otimes W_m) \\ &= 0\,(V_\ell \otimes W_m) = 0.\end{aligned}$$

Now, forget that we fixed ℓ and m. We thus have proven that every $\ell \in \mathbb{N}$ and $m \in \mathbb{N}$ satisfy

$$(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W})(V_\ell \otimes W_m) = 0. \tag{290}$$

But

$$V \otimes W = \bigoplus_{(\ell,m)\in\mathbb{N}^{\times 2}} V_\ell \otimes W_m = \sum_{(\ell,m)\in\mathbb{N}^{\times 2}} V_\ell \otimes W_m \qquad \text{(since direct sums are sums)},$$

so that

$$\begin{aligned}(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W})(V \otimes W) &= (E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W})\left(\sum_{(\ell,m)\in\mathbb{N}^{\times 2}} V_\ell \otimes W_m\right) \\ &= \sum_{(\ell,m)\in\mathbb{N}^{\times 2}} \underbrace{(E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W})(V_\ell \otimes W_m)}_{\substack{=0 \\ \text{(by (290))}}} \\ &\qquad \text{(since } E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W} \text{ is } k\text{-linear)} \\ &= \sum_{(\ell,m)\in\mathbb{N}^{\times 2}} 0 = 0.\end{aligned}$$

Thus, $E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W - E_{V\otimes W} = 0$, so that $E_V \otimes \mathrm{id}_W + \mathrm{id}_V \otimes E_W = E_{V\otimes W}$. This proves Proposition 27.3. □

We will now construct a "partial inverse" to E_V in characteristic 0:

Definition 27.9. Let k be a field of characteristic 0. Let $(b_\ell)_{\ell\in\mathbb{N}}$ be the sequence of elements of k defined by

$$\left(b_\ell = \begin{cases} \dfrac{1}{\ell}, & \text{if } \ell > 0; \\ 0, & \text{if } \ell = 0 \end{cases} \qquad \text{for every } \ell \in \mathbb{N}\right).$$

Let V be a graded k-vector space. Then, $V = \bigoplus_{\ell\in\mathbb{N}} V_\ell$. The map $\bigoplus_{\ell\in\mathbb{N}} (b_\ell \cdot \mathrm{id}_{V_\ell}) : \bigoplus_{\ell\in\mathbb{N}} V_\ell \to \bigoplus_{\ell\in\mathbb{N}} V_\ell$ is a k-linear map from V to V (because it is a k-linear map from $\bigoplus_{\ell\in\mathbb{N}} V_\ell$ to $\bigoplus_{\ell\in\mathbb{N}} V_\ell$, but we have $\bigoplus_{\ell\in\mathbb{N}} V_\ell = V$). This map will be denoted by E_V^{inv}.

Remark 27.10. Let k be a field of characteristic 0. Let $(b_\ell)_{\ell\in\mathbb{N}}$ be as defined in Definition 27.9. Let V be a graded k-vector space. Then, $E_V^{\mathrm{inv}} = E_V^{(b_\ell)_{\ell\in\mathbb{N}}}$.

Proof of Remark 27.10. By the definition of E_V^{inv}, we have $E_V^{\mathrm{inv}} = \bigoplus_{\ell\in\mathbb{N}} (b_\ell \cdot \mathrm{id}_{V_\ell})$. By the definition of $E_V^{(b_\ell)_{\ell\in\mathbb{N}}}$, we have $E_V^{(b_\ell)_{\ell\in\mathbb{N}}} = \bigoplus_{\ell\in\mathbb{N}} (b_\ell \cdot \mathrm{id}_{V_\ell})$. Thus, $E_V^{\mathrm{inv}} = \bigoplus_{\ell\in\mathbb{N}} (b_\ell \cdot \mathrm{id}_{V_\ell}) = E_V^{(b_\ell)_{\ell\in\mathbb{N}}}$. This proves Remark 27.10. □

Proposition 27.11. Let k be a field. Let $(c_\ell)_{\ell\in\mathbb{N}}$ and $(d_\ell)_{\ell\in\mathbb{N}}$ be two sequences of elements of k. Let V be a graded k-vector space. Then,

$$E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} = E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}} = E_V^{(d_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(c_\ell)_{\ell\in\mathbb{N}}}.$$

Proof of Proposition 27.11. Let $n \in \mathbb{N}$. Every $v \in V_n$ satisfies

$$\begin{aligned}
\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}}\right)(v) &= E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \underbrace{\left(E_V^{(d_\ell)_{\ell\in\mathbb{N}}}(v)\right)}_{\substack{=d_n v \\ \text{(by Proposition 27.7 (a),} \\ \text{applied to } (a_\ell)_{\ell\in\mathbb{N}}=(d_\ell)_{\ell\in\mathbb{N}})}} = E_V^{(c_\ell)_{\ell\in\mathbb{N}}}(d_n v) \\
&= d_n \underbrace{E_V^{(c_\ell)_{\ell\in\mathbb{N}}}(v)}_{\substack{=c_n v \\ \text{(by Proposition 27.7 (a),} \\ \text{applied to } (a_\ell)_{\ell\in\mathbb{N}}=(c_\ell)_{\ell\in\mathbb{N}})}} \qquad \left(\text{since } E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \text{ is } k\text{-linear}\right) \\
&= d_n c_n v = c_n d_n v = E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}(v)
\end{aligned}$$

(since $E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}} = c_n d_n v$ by Proposition 27.7 **(a)** (applied to $(a_\ell)_{\ell\in\mathbb{N}} = (c_\ell d_\ell)_{\ell\in\mathbb{N}}$)) and thus

$$\begin{aligned}
\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right)(v) &= \underbrace{\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}}\right)(v)}_{=E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}(v)} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}(v) \\
&= E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}(v) - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}(v) = 0,
\end{aligned}$$

so that $v \in \mathrm{Ker}\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right)$. Thus, $V_n \subseteq \mathrm{Ker}\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right)$.

Now, forget that we fixed n. We have thus shown that every $n \in \mathbb{N}$ satisfies $V_n \subseteq \mathrm{Ker}\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right)$. Since V is a graded k-vector space, we have

$$\begin{aligned}
V = \bigoplus_{n\in\mathbb{N}} V_n &= \sum_{n\in\mathbb{N}} \underbrace{V_n}_{\subseteq \mathrm{Ker}\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right)} \subseteq \sum_{n\in\mathbb{N}} \mathrm{Ker}\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right) \\
&\subseteq \mathrm{Ker}\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right)
\end{aligned}$$

(since $\mathrm{Ker}\left(E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}\right)$ is a k-vector space), so that $E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} - E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}} = 0$, and thus $E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} = E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}}$. The same argument, but with

the roles of $(c_\ell)_{\ell\in\mathbb{N}}$ and $(d_\ell)_{\ell\in\mathbb{N}}$ interchanged, proves that $E_V^{(d_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(c_\ell)_{\ell\in\mathbb{N}}} = E_V^{(d_\ell c_\ell)_{\ell\in\mathbb{N}}}$. Thus,

$$E_V^{(c_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(d_\ell)_{\ell\in\mathbb{N}}} = E_V^{(c_\ell d_\ell)_{\ell\in\mathbb{N}}} = E_V^{(d_\ell c_\ell)_{\ell\in\mathbb{N}}} = E_V^{(d_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(c_\ell)_{\ell\in\mathbb{N}}}.$$

This proves Proposition 27.11. □

Corollary 27.12. Let k be a field of characteristic 0. Let V be a graded k-vector space. Then:

(a) We have $E_V \circ E_V^{\mathrm{inv}} = E_V^{\mathrm{inv}} \circ E_V$.

(b) Every $v \in \bigoplus_{n\geq 1} V_n$ satisfies $\left(E_V^{\mathrm{inv}} \circ E_V\right)(v) = v$.

(c) The map E_V^{inv} is graded.

Proof of Corollary 27.12. Define $(b_\ell)_{\ell\in\mathbb{N}}$ as in Definition 27.9. Proposition 27.11 (applied to $(c_\ell)_{\ell\in\mathbb{N}} = (\ell)_{\ell\in\mathbb{N}}$ and $(d_\ell)_{\ell\in\mathbb{N}} = (b_\ell)_{\ell\in\mathbb{N}}$) yields

$$E_V^{(\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(b_\ell)_{\ell\in\mathbb{N}}} = E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} = E_V^{(b_\ell)_{\ell\in\mathbb{N}}} \circ E_V^{(\ell)_{\ell\in\mathbb{N}}}.$$

Since $E_V^{(\ell)_{\ell\in\mathbb{N}}} = E_V$ (by Remark 27.6) and $E_V^{(b_\ell)_{\ell\in\mathbb{N}}} = E_V^{\mathrm{inv}}$ (by Remark 27.10), this rewrites as

$$E_V \circ E_V^{\mathrm{inv}} = E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} = E_V^{\mathrm{inv}} \circ E_V.$$

This proves Corollary 27.12 **(a)**.

(b) Since V is a graded k-vector space, we have $V = \bigoplus_{n\in\mathbb{N}} V_n$. Thus, the internal direct sum $\bigoplus_{n\geq 1} V_n$ is well-defined (as a subsum of the direct sum $\bigoplus_{n\in\mathbb{N}} V_n$).

Now, let $n \in \mathbb{N}$ be positive. By the definition of b_n, we then have

$$b_n = \begin{cases} \dfrac{1}{n}, & \text{if } n > 0; \\ 0, & \text{if } n = 0 \end{cases} = \frac{1}{n}$$

(since $n > 0$), so that $nb_n = 1$. Every $v \in V_n$ satisfies

$$\begin{aligned} E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}}(v) &= \underbrace{nb_n}_{=1} v \qquad \left(\text{by Proposition 27.7 } \mathbf{(a)}, \text{ applied to } (a_\ell)_{\ell\in\mathbb{N}} = (\ell b_\ell)_{\ell\in\mathbb{N}}\right) \\ &= v, \end{aligned}$$

so that $\left(E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id}\right) v = \underbrace{E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}}(v)}_{=v} - \underbrace{\mathrm{id}(v)}_{=v} = v - v = 0$. Thus, $\left(E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id}\right)(V_n) = 0$.

Now, forget that we fixed n. We thus have showed that every positive $n \in \mathbb{N}$ satisfies $\left(E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id}\right)(V_n) = 0$. Thus, $\sum_{n\geq 1} \underbrace{\left(E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id}\right)(V_n)}_{=0} = \sum_{n\geq 1} 0 = 0$.

Since direct sums are sums, we have $\bigoplus_{n\geq 1} V_n = \sum_{n\geq 1} V_n$ and thus

$$\begin{aligned} \left(E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id}\right)\left(\bigoplus_{n\geq 1} V_n\right) &= \left(E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id}\right)\left(\sum_{n\geq 1} V_n\right) = \sum_{n\geq 1}\left(E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id}\right)(V_n) \\ &\qquad \left(\text{since the map } E_V^{(\ell b_\ell)_{\ell\in\mathbb{N}}} - \mathrm{id} \text{ is } k\text{-linear}\right) \\ &= 0. \end{aligned}$$

Hence, every $v \in \bigoplus_{n \geq 1} V_n$ satisfies $\left(E_V^{(\ell b_\ell)_{\ell \in \mathbb{N}}} - \mathrm{id}\right)(v) = 0$ and thus

$$0 = \left(E_V^{(\ell b_\ell)_{\ell \in \mathbb{N}}} - \mathrm{id}\right)(v) = \underbrace{E_V^{(\ell b_\ell)_{\ell \in \mathbb{N}}}(v)}_{= E_V^{\mathrm{inv}} \circ E_V} - \underbrace{\mathrm{id}(v)}_{= v} = \left(E_V^{\mathrm{inv}} \circ E_V\right)(v) - v,$$

so that $\left(E_V^{\mathrm{inv}} \circ E_V\right)(v) = v$. This proves Corollary 27.12 **(b)**.

(c) Proposition 27.7 **(b)** (applied to $(a_\ell)_{\ell \in \mathbb{N}} = (b_\ell)_{\ell \in \mathbb{N}}$) shows that the map $E_V^{(b_\ell)_{\ell \in \mathbb{N}}}$ is graded. Since $E_V^{(b_\ell)_{\ell \in \mathbb{N}}} = E_V^{\mathrm{inv}}$ (by Remark 27.10), this rewrites as follows: The map E_V^{inv} is graded. This proves Corollary 27.12 **(c)**. □

§28. The Dynkin idempotents in cocommutative Hopf algebras

We are now ready to state the main property of the Dynkin idempotents in cocommutative Hopf algebras:

Theorem 28.1. Let k be a field of characteristic 0. Let H be a cocommutative graded k-Hopf algebra. Let S be the antipode of H. Define a map $E_H : H \to H$ according to Definition 27.1. Define a map $E_H^{\mathrm{inv}} : H \to H$ according to Definition 27.9. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H. Let $(\operatorname{Prim} H)^+$ denote the intersection $(\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n\right)$. Then:

(a) The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$.

(b) The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$.

Note that in the case when H is connected, it is easy to see that $(\operatorname{Prim} H)^+ = \operatorname{Prim} H$, and thus this yields:

Theorem 28.2. Let k be a field of characteristic 0. Let H be a cocommutative connected graded k-Hopf algebra. Let S be the antipode of H. Define a map $E_H : H \to H$ according to Definition 27.1. Define a map $E_H^{\mathrm{inv}} : H \to H$ according to Definition 27.9. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H. Then:

(a) The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection from H to the subspace $\operatorname{Prim} H$.

(b) The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection from H to the subspace $\operatorname{Prim} H$.

The maps $E_H^{\mathrm{inv}} \circ (E_H * S)$ and $E_H^{\mathrm{inv}} \circ (S * E_H)$ are called the *Dynkin idempotents* of H.

We will prove Theorems 28.1 and 28.2, but also more general facts, in the rest of §28. In §29, we will dualize them to commutative Hopf algebras (again obtaining projections, but not necessarily on $(\operatorname{Prim} H)^+$ anymore). In §30, we will "interpolate" between $E_H * S$ and $S * E_H$, obtaining infinitely many "intermediate" Dynkin idempotents.

But let us first define the notion of a *coderivation*:

Definition 28.3. Let k be a field. Let H be a k-coalgebra. Let $f : H \to H$ be a k-linear map. Then, f is said to be a *coderivation* if and only if $\Delta_H \circ f = (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f) \circ \Delta_H$.

Keep in mind that **a coderivation is not the same as an $(\varepsilon, \varepsilon)$-coderivation**. (The latter has been defined in Definition 7.1.) We will, however, connect these two notions in the following results.

Definition 28.3 could be generalized to k-linear maps $f : M \to H$ with M being a (H, H)-bicomodule; but we will not need this generalization and we will not even define the notion of a (H, H)-bicomodule.

Before we prove anything about coderivations, let us show a technical lemma:

Lemma 28.4. Let k be a field. Let C be a cocommutative k-coalgebra. Let A be a k-bialgebra. Let $\alpha : C \to A$ and $\beta : C \to A$ be any k-linear maps. Let $g : C \to A$ be a k-coalgebra homomorphism. Let $f : C \to A$ be a k-linear map satisfying

$$\Delta_A \circ f = (\alpha \otimes f + f \otimes \beta) \circ \Delta_C.$$

Then:

(a) We have

$$\Delta_A \circ (f * g) = ((\alpha * g) \otimes (f * g) + (f * g) \otimes (\beta * g)) \circ \Delta_C.$$

(b) We have

$$\Delta_A \circ (g * f) = ((g * \alpha) \otimes (g * f) + (g * f) \otimes (g * \beta)) \circ \Delta_C.$$

Proof of Lemma 28.4. By the axioms of a bialgebra, $\Delta_A : A \to A \otimes A$ is a k-algebra homomorphism (since A is a k-bialgebra). Thus, $\Delta_A \circ \mu_A = \mu_{A \otimes A} \circ (\Delta_A \otimes \Delta_A)$.

In the following, the sign $*$ will denote the convolution in $\mathcal{L}(C, A)$, but also the convolution in $\mathcal{L}(C \otimes C, A \otimes A)$ (which is well-defined since $C \otimes C$ is a k-coalgebra and $A \otimes A$ is a k-algebra).

(a) By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$, so that

$$\begin{aligned} \Delta_A \circ \underbrace{(f * g)}_{=\mu_A \circ (f \otimes g) \circ \Delta_C} &= \underbrace{\Delta_A \circ \mu_A}_{=\mu_{A \otimes A} \circ (\Delta_A \otimes \Delta_A)} \circ (f \otimes g) \circ \Delta_C \\ &= \mu_{A \otimes A} \circ (\Delta_A \otimes \Delta_A) \circ (f \otimes g) \circ \Delta_C. \end{aligned} \tag{291}$$

But applying (21) to C, A, $A \otimes A$, C, A, $A \otimes A$, f, Δ_A, g, Δ_A instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(\Delta_A \circ f) \otimes (\Delta_A \circ g) = (\Delta_A \otimes \Delta_A) \circ (f \otimes g),$$

so that

$$
\begin{aligned}
&(\Delta_A \otimes \Delta_A) \circ (f \otimes g) \\
&= \underbrace{(\Delta_A \circ f)}_{=(\alpha \otimes f + f \otimes \beta) \circ \Delta_C} \otimes \underbrace{(\Delta_A \circ g)}_{\substack{=(g \otimes g) \circ \Delta_C \\ \text{(since } g \text{ is a } k\text{-coalgebra} \\ \text{homomorphism)}}} \\
&= ((\alpha \otimes f + f \otimes \beta) \circ \Delta_C) \otimes ((g \otimes g) \circ \Delta_C) \\
&= \underbrace{((\alpha \otimes f + f \otimes \beta) \otimes (g \otimes g))}_{\substack{=\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g \\ \text{(since the tensor product of } k\text{-linear maps} \\ \text{is distributive)}}} \circ (\Delta_C \otimes \Delta_C) \\
&\qquad \left(\begin{array}{c} \text{by (21) (applied to } C, C \otimes C, A \otimes A, C, C \otimes C, A \otimes A, \\ \Delta_C, \alpha \otimes f + f \otimes \beta, \Delta_C, g \otimes g \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta') \end{array} \right) \\
&= (\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g) \circ (\Delta_C \otimes \Delta_C) \, . \qquad (292)
\end{aligned}
$$

Now, (291) becomes

$$
\begin{aligned}
&\Delta_A \circ (f * g) \\
&= \mu_{A\otimes A} \circ \underbrace{(\Delta_A \otimes \Delta_A) \circ (f \otimes g)}_{\substack{=(\alpha\otimes f\otimes g\otimes g + f\otimes\beta\otimes g\otimes g)\circ(\Delta_C\otimes\Delta_C) \\ \text{(by (292))}}} \circ \Delta_C \\
&= \mu_{A\otimes A} \circ (\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g) \circ \underbrace{(\Delta_C \otimes \Delta_C) \circ \Delta_C}_{\substack{=\left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)\circ(\Delta_C\otimes\Delta_C)\circ\Delta_C \\ \text{(by (26))}}} \\
&= \mu_{A\otimes A} \circ (\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g) \circ \underbrace{(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C) \circ (\Delta_C \otimes \Delta_C)}_{\substack{=\Delta_{C\otimes C} \\ \text{(since the definition of the } k\text{-coalgebra } C\otimes C \text{ yields} \\ \Delta_{C\otimes C} = \left(\mathrm{id}_C \otimes \tau_{C,C} \otimes \mathrm{id}_C\right)\circ(\Delta_C\otimes\Delta_C))}} \circ \Delta_C \\
&= \mu_{A\otimes A} \circ \underbrace{(\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g) \circ \Delta_{C\otimes C}}_{\substack{=(\alpha\otimes f\otimes g\otimes g)\circ\Delta_{C\otimes C} + (f\otimes\beta\otimes g\otimes g)\circ\Delta_{C\otimes C} \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \circ \Delta_C \\
&= \underbrace{\mu_{A\otimes A} \circ ((\alpha \otimes f \otimes g \otimes g) \circ \Delta_{C\otimes C} + (f \otimes \beta \otimes g \otimes g) \circ \Delta_{C\otimes C})}_{\substack{=\mu_{A\otimes A}\circ(\alpha\otimes f\otimes g\otimes g)\circ\Delta_{C\otimes C} + \mu_{A\otimes A}\circ(f\otimes\beta\otimes g\otimes g)\circ\Delta_{C\otimes C} \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \circ \Delta_C \\
&= \left(\underbrace{\mu_{A\otimes A} \circ (\alpha \otimes f \otimes g \otimes g) \circ \Delta_{C\otimes C}}_{\substack{=(\alpha\otimes f)*(g\otimes g) \\ \text{(because the definition of convolution yields} \\ (\alpha\otimes f)*(g\otimes g) = \mu_{A\otimes A}\circ(\alpha\otimes f\otimes g\otimes g)\circ\Delta_{C\otimes C})}} + \underbrace{\mu_{A\otimes A} \circ (f \otimes \beta \otimes g \otimes g) \circ \Delta_{C\otimes C}}_{\substack{=(f\otimes\beta)*(g\otimes g) \\ \text{(because the definition of convolution yields} \\ (f\otimes\beta)*(g\otimes g) = \mu_{A\otimes A}\circ(f\otimes\beta\otimes g\otimes g)\circ\Delta_{C\otimes C})}} \right) \circ \Delta_C \\
&= \left(\underbrace{(\alpha \otimes f) * (g \otimes g)}_{\substack{=(\alpha * g)\otimes(f * g) \\ \text{(by Corollary 9.9, applied to } D=C,\ B=A, \\ p=\alpha,\ q=g,\ r=f,\ s=g)}} + \underbrace{(f \otimes \beta) * (g \otimes g)}_{\substack{=(f * g)\otimes(\beta * g) \\ \text{(by Corollary 9.9, applied to } D=C,\ B=A, \\ p=f,\ q=g,\ r=\beta,\ s=g)}} \right) \circ \Delta_C \\
&= ((\alpha * g) \otimes (f * g) + (f * g) \otimes (\beta * g)) \circ \Delta_C.
\end{aligned}
$$

This proves Lemma 28.4 **(a)**.

(b) By the definition of convolution, $g * f = \mu_A \circ (g \otimes f) \circ \Delta_C$, so that

$$
\begin{aligned}
\Delta_A \circ \underbrace{(g * f)}_{=\mu_A\circ(g\otimes f)\circ\Delta_C} &= \underbrace{\Delta_A \circ \mu_A}_{=\mu_{A\otimes A}\circ(\Delta_A\otimes\Delta_A)} \circ (g \otimes f) \circ \Delta_C \\
&= \mu_{A\otimes A} \circ (\Delta_A \otimes \Delta_A) \circ (g \otimes f) \circ \Delta_C. \qquad (293)
\end{aligned}
$$

But applying (21) to C, A, $A \otimes A$, C, A, $A \otimes A$, g, Δ_A, f, Δ_A instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$
(\Delta_A \circ g) \otimes (\Delta_A \circ f) = (\Delta_A \otimes \Delta_A) \circ (g \otimes f),
$$

so that

$$
\begin{aligned}
&(\Delta_A \otimes \Delta_A) \circ (g \otimes f) \\
&= \underbrace{(\Delta_A \circ g)}_{\substack{=(g\otimes g)\circ\Delta_C \\ \text{(since } g \text{ is a } k\text{-coalgebra} \\ \text{homomorphism)}}} \otimes \underbrace{(\Delta_A \circ f)}_{=(\alpha\otimes f+f\otimes\beta)\circ\Delta_C} \\
&= ((g \otimes g) \circ \Delta_C) \otimes ((\alpha \otimes f + f \otimes \beta) \circ \Delta_C) \\
&= \underbrace{((g \otimes g) \otimes (\alpha \otimes f + f \otimes \beta))}_{\substack{=g\otimes g\otimes\alpha\otimes f+g\otimes g\otimes f\otimes\beta \\ \text{(since the tensor product of } k\text{-linear maps} \\ \text{is distributive)}}} \circ (\Delta_C \otimes \Delta_C) \\
&\qquad \left(\begin{array}{c} \text{by (21) (applied to } C,\ C \otimes C,\ A \otimes A,\ C,\ C \otimes C,\ A \otimes A, \\ \Delta_C,\ g \otimes g,\ \Delta_C,\ \alpha \otimes f + f \otimes \beta \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta') \end{array} \right) \\
&= (g \otimes g \otimes \alpha \otimes f + g \otimes g \otimes f \otimes \beta) \circ (\Delta_C \otimes \Delta_C)\,. \qquad (294)
\end{aligned}
$$

Now, (293) becomes

$$
\begin{aligned}
&\Delta_A \circ (g * f) \\
&= \mu_{A\otimes A} \circ \underbrace{(\Delta_A \otimes \Delta_A) \circ (g \otimes f)}_{\substack{=(g\otimes g\otimes\alpha\otimes f+g\otimes g\otimes f\otimes\beta)\circ(\Delta_C\otimes\Delta_C) \\ \text{(by (294))}}} \circ\Delta_C \\
&= \mu_{A\otimes A} \circ (g\otimes g\otimes\alpha\otimes f + g\otimes g\otimes f\otimes\beta) \circ \underbrace{(\Delta_C\otimes\Delta_C)\circ\Delta_C}_{\substack{=\left(\mathrm{id}_C\otimes\tau_{C,C}\otimes\mathrm{id}_C\right)\circ(\Delta_C\otimes\Delta_C)\circ\Delta_C \\ \text{(by (26))}}} \\
&= \mu_{A\otimes A} \circ (g\otimes g\otimes\alpha\otimes f + g\otimes g\otimes f\otimes\beta) \circ \underbrace{(\mathrm{id}_C\otimes\tau_{C,C}\otimes\mathrm{id}_C)\circ(\Delta_C\otimes\Delta_C)}_{\substack{=\Delta_{C\otimes C} \\ \text{(since the definition of the } k\text{-coalgebra } C\otimes C \text{ yields} \\ \Delta_{C\otimes C}=\left(\mathrm{id}_C\otimes\tau_{C,C}\otimes\mathrm{id}_C\right)\circ(\Delta_C\otimes\Delta_C))}} \circ\Delta_C \\
&= \mu_{A\otimes A} \circ \underbrace{(g\otimes g\otimes\alpha\otimes f + g\otimes g\otimes f\otimes\beta)\circ\Delta_{C\otimes C}}_{\substack{=(g\otimes g\otimes\alpha\otimes f)\circ\Delta_{C\otimes C}+(g\otimes g\otimes f\otimes\beta)\circ\Delta_{C\otimes C} \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \circ\Delta_C \\
&= \underbrace{\mu_{A\otimes A}\circ((g\otimes g\otimes\alpha\otimes f)\circ\Delta_{C\otimes C} + (g\otimes g\otimes f\otimes\beta)\circ\Delta_{C\otimes C})}_{\substack{=\mu_{A\otimes A}\circ(g\otimes g\otimes\alpha\otimes f)\circ\Delta_{C\otimes C}+\mu_{A\otimes A}\circ(g\otimes g\otimes f\otimes\beta)\circ\Delta_{C\otimes C} \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \circ\Delta_C \\
&= \left(\underbrace{\mu_{A\otimes A}\circ(g\otimes g\otimes\alpha\otimes f)\circ\Delta_{C\otimes C}}_{\substack{=(g\otimes g)*(\alpha\otimes f) \\ \text{(because the definition of convolution yields} \\ (g\otimes g)*(\alpha\otimes f)=\mu_{A\otimes A}\circ(g\otimes g\otimes\alpha\otimes f)\circ\Delta_{C\otimes C})}} + \underbrace{\mu_{A\otimes A}\circ(g\otimes g\otimes f\otimes\beta)\circ\Delta_{C\otimes C}}_{\substack{=(g\otimes g)*(f\otimes\beta) \\ \text{(because the definition of convolution yields} \\ (g\otimes g)*(f\otimes\beta)=\mu_{A\otimes A}\circ(g\otimes g\otimes f\otimes\beta)\circ\Delta_{C\otimes C})}} \right) \circ\Delta_C \\
&= \left(\underbrace{(g\otimes g)*(\alpha\otimes f)}_{\substack{=(g*\alpha)\otimes(g*f) \\ \text{(by Corollary 9.9, applied to } D=C,\ B=A, \\ p=g,\ q=\alpha,\ r=g,\ s=f)}} + \underbrace{(g\otimes g)*(f\otimes\beta)}_{\substack{=(g*f)\otimes(g*\beta) \\ \text{(by Corollary 9.9, applied to } D=C,\ B=A, \\ p=g,\ q=f,\ r=g,\ s=\beta)}} \right) \circ\Delta_C \\
&= ((g*\alpha)\otimes(g*f) + (g*f)\otimes(g*\beta))\circ\Delta_C.
\end{aligned}
$$

This proves Lemma 28.4 **(b)**. □

Now comes the reason why we proved Lemma 28.4:

Theorem 28.5. Let k be a field. Let H be a cocommutative k-bialgebra. Let $P : H \to H$ and $Q : H \to H$ be two k-coalgebra homomorphisms satisfying $P * \mathrm{id}_H * Q = e_{H,H}$. Let $K : H \to H$ be a coderivation. Then, $P * K * Q : H \to H$ is an $(\varepsilon,\varepsilon)$-coderivation. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Proof of Theorem 28.5. Since K is a coderivation, we have $\Delta_H \circ K = (K\otimes\mathrm{id}_H + \mathrm{id}_H\otimes K)\circ\Delta_H$ (because Definition 28.3 yields that K is a coderivation if and only if $\Delta_H \circ K =$

$(K \otimes \mathrm{id}_H + \mathrm{id}_H \otimes K) \circ \Delta_H)$. Thus,

$$\Delta_H \circ K = \underbrace{(K \otimes \mathrm{id}_H + \mathrm{id}_H \otimes K)}_{= \mathrm{id}_H \otimes K + K \otimes \mathrm{id}_H} \circ \Delta_H = (\mathrm{id}_H \otimes K + K \otimes \mathrm{id}_H) \circ \Delta_H.$$

Hence, Lemma 28.4 **(b)** (applied to $C = H$, $A = H$, $\alpha = \mathrm{id}_H$, $\beta = \mathrm{id}_H$, $f = K$ and $g = P$) yields

$$\Delta_H \circ (P * K) = ((P * \mathrm{id}_H) \otimes (P * K) + (P * K) \otimes (P * \mathrm{id}_H)) \circ \Delta_H.$$

Thus, Lemma 28.4 **(a)** (applied to $C = H$, $A = H$, $\alpha = P * \mathrm{id}_H$, $\beta = P * \mathrm{id}_H$, $f = P * K$ and $g = Q$) yields

$$\begin{aligned}
\Delta_H \circ (P * K * Q) &= \left(\underbrace{(P * \mathrm{id}_H * Q)}_{= e_{H,H}} \otimes (P * K * Q) + (P * K * Q) \otimes \underbrace{(P * \mathrm{id}_H * Q)}_{= e_{H,H}} \right) \circ \Delta_H \\
&= \underbrace{(e_{H,H} \otimes (P * K * Q) + (P * K * Q) \otimes e_{H,H})}_{= (P*K*Q) \otimes e_{H,H} + e_{H,H} \otimes (P*K*Q)} \circ \Delta_H \\
&= ((P * K * Q) \otimes e_{H,H} + e_{H,H} \otimes (P * K * Q)) \circ \Delta_H.
\end{aligned}$$

Thus, $P * K * Q$ is an $(\varepsilon, \varepsilon)$-coderivation (because by Definition 7.1, the map $P * K * Q$ is an $(\varepsilon, \varepsilon)$-coderivation if and only if $\Delta_H \circ (P * K * Q) = ((P * K * Q) \otimes e_{H,H} + e_{H,H} \otimes (P * K * Q)) \circ \Delta_H$). This proves Theorem 28.5. □

Corollary 28.6. Let k be a field. Let H be a cocommutative k-Hopf algebra. Let S be the antipode of H. Let $K : H \to H$ be a coderivation.

(a) Then, $S * K$ is an $(\varepsilon, \varepsilon)$-coderivation.

(b) Then, $K * S$ is an $(\varepsilon, \varepsilon)$-coderivation.

Proof of Corollary 28.6. By Definition 25.3, we have $H^{\mathrm{cop}} = (H, \tau_{H,H} \circ \Delta_H, \varepsilon_H)$. Since H is cocommutative, we have $\tau_{H,H} \circ \Delta_H = \Delta_H$. Thus, $H^{\mathrm{cop}} = \left(H, \underbrace{\tau_{H,H} \circ \Delta_H}_{= \Delta_H}, \varepsilon_H \right) = (H, \Delta_H, \varepsilon_H) = H$.

Proposition 25.4 yields that the antipode of H is a k-coalgebra homomorphism from H^{cop} to H. Since the antipode of H is the map S, whereas H^{cop} is H, this rewrites as follows: The map S is a k-coalgebra homomorphism from H to H.

Corollary 10.2 (applied to $n = 0$, $C = H$ and $f = \mathrm{id}_H$) yields that id_H^{*0} is a k-coalgebra homomorphism. Since $\mathrm{id}_H^{*0} = e_{H,H}$, this shows that $e_{H,H}$ is a k-coalgebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).

The antipode of a Hopf algebra is defined as the $*$-inverse of its identity map. Thus, the antipode of H is the map $\mathrm{id}_H^{*(-1)}$. Since the antipode of H is S, this yields that S is the map $\mathrm{id}_H^{*(-1)}$. In other words, $S = \mathrm{id}_H^{*(-1)}$. Hence, $S * \mathrm{id}_H * e_{H,H} = \underbrace{\mathrm{id}_H^{*(-1)} * \mathrm{id}_H}_{= e_{H,H}} * e_{H,H} = e_{H,H}$. Thus, Theorem 28.5 (applied to $P = S$ and $Q = e_{H,H}$) yields that $S * K * e_{H,H}$ is an $(\varepsilon, \varepsilon)$-coderivation. In other words, $S * K$ is an $(\varepsilon, \varepsilon)$-coderivation (since $S * K * e_{H,H} = S * K$). This proves Corollary 28.6 **(a)**.

Since $S = \mathrm{id}_H^{*(-1)}$, we have $e_{H,H} * \mathrm{id}_H * S = e_{H,H} * \underbrace{\mathrm{id}_H * \mathrm{id}_H^{*(-1)}}_{=e_{H,H}} = e_{H,H}$. Thus, Theorem 28.5 (applied to $P = e_{H,H}$ and $Q = S$) yields that $e_{H,H} * K * S$ is an $(\varepsilon, \varepsilon)$-coderivation. In other words, $K * S$ is an $(\varepsilon, \varepsilon)$-coderivation (since $e_{H,H} * K * S = K * S$). This proves Corollary 28.6 **(b)**. $\square$

Next, something easy:

Proposition 28.7. Let k be a field. Let H be a k-bialgebra. Let $P : H \to H$, $Q : H \to H$ and $K : H \to H$ be three k-linear maps such that $P(1_H) = 1_H$, $Q(1_H) = 1_H$ and $K(1_H) = 0$. Then, every $x \in \operatorname{Prim} H$ satisfies $(P * K * Q)(x) = K(x)$.

Proof of Proposition 28.7. Let $x \in \operatorname{Prim} H$.

Since $x \in \operatorname{Prim} H =$ (the set of primitive elements of H), the element x of H is primitive. Thus, $\Delta(x) = x \otimes 1_H + 1_H \otimes x$ (because Definition 6.1 yields that x is primitive if and only if $\Delta(x) = x \otimes 1_H + 1_H \otimes x$). Since $\Delta = \Delta_H$, this rewrites as $\Delta_H(x) = x \otimes 1_H + 1_H \otimes x$.

But $P * K = \mu_H \circ (P \otimes K) \circ \Delta_H$ (by the definition of convolution). Thus,

$$\begin{aligned}
(P * K)(x) &= (\mu_H \circ (P \otimes K) \circ \Delta_H)(x) = (\mu_H \circ (P \otimes K)) \underbrace{(\Delta_H(x))}_{=x\otimes 1_H + 1_H \otimes x} \\
&= (\mu_H \circ (P \otimes K))(x \otimes 1_H + 1_H \otimes x) \\
&= \underbrace{(\mu_H \circ (P \otimes K))(x \otimes 1_H)}_{=\mu_H((P\otimes K)(x\otimes 1_H))} + \underbrace{(\mu_H \circ (P \otimes K))(1_H \otimes x)}_{=\mu_H((P\otimes K)(1_H\otimes x))} \\
&\qquad \text{(since } \mu_H \circ (P \otimes K) \text{ is } k\text{-linear)} \\
&= \mu_H \underbrace{((P \otimes K)(x \otimes 1_H))}_{=P(x)\otimes K(1_H)} + \mu_H \underbrace{((P \otimes K)(1_H \otimes x))}_{=P(1_H)\otimes K(x)} \\
&= \underbrace{\mu_H(P(x) \otimes K(1_H))}_{\substack{=P(x)K(1_H) \\ \text{(since } \mu_H \text{ is the} \\ \text{multiplication map)}}} + \underbrace{\mu_H(P(1_H) \otimes K(x))}_{\substack{=P(1_H)K(x) \\ \text{(since } \mu_H \text{ is the} \\ \text{multiplication map)}}} \\
&= P(x) \underbrace{K(1_H)}_{=0} + \underbrace{P(1_H)}_{=1_H} K(x) = \underbrace{P(x)\,0}_{=0} + \underbrace{1_H K(x)}_{=K(x)} = K(x).
\end{aligned}$$

On the other hand, by the axioms of a bialgebra, we have $\Delta_H(1_H) = 1_H \otimes 1_H$ (since H is a k-bialgebra), so that

$$\begin{aligned}
\underbrace{(P * K)}_{=\mu_H\circ(P\otimes K)\circ\Delta_H}(1_H) &= (\mu_H \circ (P \otimes K) \circ \Delta_H)(1_H) = (\mu_H \circ (P \otimes K))\underbrace{(\Delta_H(1_H))}_{=1_H\otimes 1_H} \\
&= (\mu_H \circ (P \otimes K))(1_H \otimes 1_H) = \mu_H \underbrace{((P \otimes K)(1_H \otimes 1_H))}_{=P(1_H)\otimes K(1_H)} \\
&= \mu_H\left(\underbrace{P(1_H)}_{=1_H} \otimes \underbrace{K(1_H)}_{=0}\right) = \mu_H \underbrace{(1_H \otimes 0)}_{=0} = \mu_H(0) = 0
\end{aligned}$$

(since μ_H is K-linear). Now, by the definition of convolution, $(P * K) * Q = \mu_H \circ ((P * K) \otimes Q) \circ \Delta$, so that

$$\begin{aligned}
&((P * K) * Q)(x) \\
&= (\mu_H \circ ((P * K) \otimes Q) \circ \Delta_H)(x) = (\mu_H \circ ((P * K) \otimes Q)) \underbrace{(\Delta_H(x))}_{=x\otimes 1_H + 1_H \otimes x} \\
&= (\mu_H \circ ((P * K) \otimes Q))(x \otimes 1_H + 1_H \otimes x) \\
&= \underbrace{(\mu_H \circ ((P * K) \otimes Q))(x \otimes 1_H)}_{=\mu_H(((P*K)\otimes Q)(x\otimes 1_H))} + \underbrace{(\mu_H \circ ((P * K) \otimes Q))(1_H \otimes x)}_{=\mu_H(((P*K)\otimes Q)(1_H\otimes x))} \\
&\qquad (\text{since } \mu_H \circ ((P * K) \otimes Q) \text{ is } k\text{-linear}) \\
&= \mu_H \underbrace{(((P * K) \otimes Q)(x \otimes 1_H))}_{=(P*K)(x)\otimes Q(1_H)} + \mu_H \underbrace{(((P * K) \otimes Q)(1_H \otimes x))}_{=(P*K)(1_H)\otimes Q(x)} \\
&= \underbrace{\mu_H((P * K)(x) \otimes Q(1_H))}_{\substack{=(P*K)(x)Q(1_H) \\ (\text{since } \mu_H \text{ is the} \\ \text{multiplication map})}} + \underbrace{\mu_H((P * K)(1_H) \otimes Q(x))}_{\substack{=(P*K)(1_H)Q(x) \\ (\text{since } \mu_H \text{ is the} \\ \text{multiplication map})}} \\
&= \underbrace{(P * K)(x)}_{=K(x)} \underbrace{Q(1_H)}_{=1_H} + \underbrace{(P * K)(1_H)}_{=0} Q(x) = \underbrace{K(x)\,1_H}_{=K(x)} + \underbrace{0Q(x)}_{=0} = K(x).
\end{aligned}$$

Since $(P * K) * Q = P * K * Q$, this rewrites as $(P * K * Q)(x) = K(x)$. This proves Proposition 28.7. □

Now, let us study a particular coderivation that any graded coalgebra has: the Euler operator:

Proposition 28.8. Let k be a field. Let H be a graded k-coalgebra. Let E_H be defined according to Definition 27.1. Then, $E_H : H \to H$ is a coderivation.

Proof of Proposition 28.8. Since H is a graded k-coalgebra, the map $\Delta_H : H \to H \otimes H$ is graded. Thus, Proposition 27.4 (applied to $V = H$, $W = H \otimes H$ and $f = \Delta_H$) yields

$$\Delta_H \circ E_H = \underbrace{E_{H\otimes H}}_{\substack{=E_H\otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H \\ (\text{by Proposition 27.3, applied to } V=H \text{ and } W=H)}} \circ \Delta_H = (E_H \otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H) \circ \Delta_H.$$

Thus, E_H is a coderivation (because Definition 28.3 yields that E_H is a coderivation if and only if $\Delta_H \circ E_H = (E_H \otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H) \circ \Delta_H$). Proposition 28.8 is proven. □

Now, let us come as close as possible to Theorem 28.1 without requiring k to be of characteristic 0:

Theorem 28.9. Let k be a field. Let H be a cocommutative graded k-bialgebra. Let E_H be defined according to Definition 27.1. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H. Let $(\operatorname{Prim} H)^+$ denote the intersection $(\operatorname{Prim} H) \cap \left(\bigoplus_{n\geq 1} H_n \right)$.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-coalgebra homomorphisms satisfying $P(1_H) = 1_H$, $Q(1_H) = 1_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here,

the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

(a) Then, $(P * E_H * Q)(H) \subseteq (\operatorname{Prim} H)^+$.

(b) Besides, $E_H\left((\operatorname{Prim} H)^+\right) \subseteq (P * E_H * Q)(H)$.

(c) We have $(P * E_H * Q) \circ (P * E_H * Q) = E_H \circ (P * E_H * Q) = (P * E_H * Q) \circ E_H$.

Proof of Theorem 28.9. Notice that H is a k-bialgebra, thus a unital coalgebra.

By Proposition 28.8, the map E_H is a coderivation. Thus, Theorem 28.5 (applied to $K = E_H$) yields that $P * E_H * Q : H \to H$ is an $(\varepsilon, \varepsilon)$-coderivation. Thus,

$$(P * E_H * Q)(H) \subseteq \operatorname{Prim} H \tag{295}$$

(because Theorem 7.2 (applied to $C = H$ and $f = P * E_H * Q$) yields that $P * E_H * Q$ is an $(\varepsilon, \varepsilon)$-coderivation if and only if $(P * E_H * Q)(H) \subseteq \operatorname{Prim} H$).

On the other hand, since H is a graded k-coalgebra, we have

$$\Delta_H(H_\ell) \subseteq \bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=\ell}} H_i \otimes H_j \qquad \text{for every } \ell \in \mathbb{N}.$$

Applied to $\ell = 0$, this yields $\Delta_H(H_0) \subseteq \bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=0}} H_i \otimes H_j$.

There exists only one $(i,j) \in \mathbb{N}^{\times 2}$ satisfying $i + j = 0$: namely, $(i,j) = (0,0)$. Thus, the direct sum $\bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=0}} H_i \otimes H_j$ has only one addend, namely the one for $(i,j) = (0,0)$. As a consequence, $\bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=0}} H_i \otimes H_j = H_0 \otimes H_0$. Thus, $\Delta_H(H_0) \subseteq \bigoplus_{\substack{(i,j) \in \mathbb{N}^{\times 2}; \\ i+j=0}} H_i \otimes H_j = H_0 \otimes H_0$.

Notice that $E_H(H_0) = 0$ [142]. By the definition of convolution, $P * E_H = \mu_H \circ (P \otimes E_H) \circ \Delta_H$. Thus,

$$\begin{aligned}
(P * E_H)(H_0) &= (\mu_H \circ (P \otimes E_H) \circ \Delta_H)(H_0) = \mu_H\left((P \otimes E_H)\underbrace{(\Delta_H(H_0))}_{\subseteq H_0 \otimes H_0}\right) \\
&\subseteq \mu_H \underbrace{((P \otimes E_H)(H_0 \otimes H_0))}_{=P(H_0) \otimes E_H(H_0)} = \mu_H\left(P(H_0) \otimes \underbrace{E_H(H_0)}_{=0}\right) \\
&= \mu_H\left(\underbrace{P(H_0) \otimes 0}_{=0}\right) = \mu_H(0) = 0 \qquad \text{(since } \mu_H \text{ is } k\text{-linear)}.
\end{aligned}$$

[142] This is because every $v \in H_0$ satisfies

$$\begin{aligned}
E_H(v) &= 0v \qquad \text{(by Proposition 27.2 \textbf{(a)}, applied to } n = 0) \\
&= 0.
\end{aligned}$$

By the definition of convolution, $(P * E_H) * Q = \mu_H \circ ((P * E_H) \otimes Q) \circ \Delta_H$. Thus,

$$((P * E_H) * Q)(H_0) = (\mu_H \circ ((P * E_H) \otimes Q) \circ \Delta_H)(H_0) = \mu_H\left(((P * E_H) \otimes Q)\underbrace{(\Delta_H(H_0))}_{\subseteq H_0 \otimes H_0}\right)$$

$$\subseteq \mu_H\underbrace{(((P * E_H) \otimes Q)(H_0 \otimes H_0))}_{=(P*E_H)(H_0)\otimes Q(H_0)} = \mu_H\left(\underbrace{(P * E_H)(H_0)}_{\subseteq 0} \otimes Q(H_0)\right)$$

$$\subseteq \mu_H\left(\underbrace{0 \otimes Q(H_0)}_{=0}\right) = \mu_H(0) = 0 \qquad \text{(since } \mu_H \text{ is } k\text{-linear)},$$

so that $((P * E_H) * Q)(H_0) = 0$. Since $(P * E_H) * Q = P * E_H * Q$, this rewrites as

$$(P * E_H * Q)(H_0) = 0. \tag{296}$$

Since E_H is graded (by Proposition 27.2 **(b)**, applied to $V = H$) and Q is graded, we conclude (by Proposition 16.18 **(a)**, applied to $C = H$, $A = H$, $f = E_H$ and $g = Q$) that $E_H * Q$ is graded.

Since P is graded and $E_H * Q$ is graded, we conclude (by Proposition 16.18 **(a)**, applied to $C = H$, $A = H$, $f = P$ and $g = E_H * Q$) that $P * E_H * Q$ is graded. Thus, every $n \in \mathbb{N}$ satisfies $(P * E_H * Q)(H_n) \subseteq H_n$. Now, since H is graded, we have $H = \bigoplus_{n\in\mathbb{N}} H_n = \sum_{n\in\mathbb{N}} H_n$ (since direct sums are sums), so that

$$(P * E_H * Q)(H) = (P * E_H * Q)\left(\sum_{n\in\mathbb{N}} H_n\right) = \sum_{n\in\mathbb{N}} (P * E_H * Q)(H_n)$$

$$\text{(since } P * E_H * Q \text{ is } k\text{-linear)}$$

$$= \underbrace{(P * E_H * Q)(H_0)}_{\substack{=0 \\ \text{(by (296))}}} + \sum_{n\geq 1} \underbrace{(P * E_H * Q)(H_n)}_{\substack{\subseteq H_n \\ \text{(since } P*E_H*Q \text{ is graded)}}}$$

$$\subseteq \sum_{n\geq 1} H_n = \bigoplus_{n\geq 1} H_n$$

(because the sum $\sum_{n\geq 1} H_n$ is a direct sum (since it is a subsum of the direct sum $\bigoplus_{n\in\mathbb{N}} H_n$)). Combining (295) with $(P * E_H * Q)(H) \subseteq \bigoplus_{n\geq 1} H_n$, we obtain

$$(P * E_H * Q)(H) \subseteq (\operatorname{Prim} H) \cap \left(\bigoplus_{n\geq 1} H_n\right) = (\operatorname{Prim} H)^+.$$

This proves Theorem 28.9 **(a)**.

(b) We have $1_H \in H_0$ (since H is a graded k-algebra). Thus, Proposition 27.2 **(a)** (applied to $V = H$, $n = 0$ and $v = 1_H$) yields $E_H(1_H) = 0 \cdot 1_H = 0$. Thus, Proposition 28.7 (applied to $K = E_H$) yields that

$$\text{every } x \in \operatorname{Prim} H \text{ satisfies } (P * E_H * Q)(x) = E_H(x). \tag{297}$$

Thus, every $x \in \operatorname{Prim} H$ satisfies $E_H(x) = (P * E_H * Q)(x) \in (P * E_H * Q)(H)$ (since $x \in H$). In other words, $E_H(\operatorname{Prim} H) \subseteq (P * E_H * Q)(H)$. Since $(\operatorname{Prim} H)^+ = (\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right) \subseteq \operatorname{Prim} H$, we have $E_H\left((\operatorname{Prim} H)^+\right) \subseteq E_H(\operatorname{Prim} H) \subseteq (P * E_H * Q)(H)$. This proves Theorem 28.9 **(b)**.

(c) Let $x \in H$. Then, $(P * E_H * Q)(x) \in (P * E_H * Q)(H) \subseteq \operatorname{Prim} H$ (by (295)). Thus, (297) (applied to $(P * E_H * Q)(x)$ instead of x) yields

$$(P * E_H * Q)((P * E_H * Q)(x)) = E_H((P * E_H * Q)(x)).$$

Thus,

$$\begin{aligned}((P * E_H * Q) \circ (P * E_H * Q))(x) &= (P * E_H * Q)((P * E_H * Q)(x)) \\ &= E_H((P * E_H * Q)(x)) = (E_H \circ (P * E_H * Q))(x).\end{aligned}$$

Now forget that we fixed x. We thus have proven that every $x \in H$ satisfies $((P * E_H * Q) \circ (P * E_H * Q))(x) = (E_H \circ (P * E_H * Q))(x)$. In other words,

$$(P * E_H * Q) \circ (P * E_H * Q) = E_H \circ (P * E_H * Q). \tag{298}$$

Since $P * E_H * Q$ is graded, we have $(P * E_H * Q) \circ E_H = E_H \circ (P * E_H * Q)$ (by Proposition 27.4, applied to $V = H$, $W = H$ and $f = P * E_H * Q$). Combined with (298), this yields

$$(P * E_H * Q) \circ (P * E_H * Q) = E_H \circ (P * E_H * Q) = (P * E_H * Q) \circ E_H.$$

This proves Theorem 28.9 **(c)**. □

Corollary 28.10. Let k be a field. Let H be a cocommutative graded k-Hopf algebra. Let S be the antipode of H. Let E_H be defined according to Definition 27.1. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H. Let $(\operatorname{Prim} H)^+$ denote the intersection $(\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right)$.

(a) Then, $(E_H * S)(H) \subseteq (\operatorname{Prim} H)^+$.

(b) Besides, $E_H\left((\operatorname{Prim} H)^+\right) \subseteq (E_H * S)(H)$.

(c) We have $(E_H * S) \circ (E_H * S) = E_H \circ (E_H * S) = (E_H * S) \circ E_H$.

(d) Also, $(S * E_H)(H) \subseteq (\operatorname{Prim} H)^+$.

(e) Besides, $E_H\left((\operatorname{Prim} H)^+\right) \subseteq (S * E_H)(H)$.

(f) We have $(S * E_H) \circ (S * E_H) = E_H \circ (S * E_H) = (S * E_H) \circ E_H$.

Proof of Corollary 28.10. Just as in the proof of Corollary 28.6, we can prove the following facts:

- The map S is a k-coalgebra homomorphism from H to H.
- The map $e_{H,H}$ is a k-coalgebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).

- We have $S = \mathrm{id}_H^{*(-1)}$.
- We have $S * \mathrm{id}_H * e_{H,H} = e_{H,H}$ and $e_{H,H} * \mathrm{id}_H * S = e_{H,H}$.

Notice that $e_{H,H} = \eta_H \circ \varepsilon_H$ (by the definition of $e_{H,H}$), so that

$$\begin{aligned} e_{H,H}(1_H) &= (\eta_H \circ \varepsilon_H)(1_H) = \eta_H \underbrace{(\varepsilon_H(1_H))}_{\substack{=1 \\ \text{(by the axioms of a bialgebra,} \\ \text{since } H \text{ is a } k\text{-bialgebra)}}} \\ &= \eta_H(1) = 1 \cdot 1_H \qquad \text{(by the definition of } \eta_H) \\ &= 1_H. \end{aligned}$$

Since $S = \mathrm{id}_H^{*(-1)}$, we have $S * \mathrm{id}_H = e_{H,H}$. But the definition of convolution yields $S * \mathrm{id}_H = \mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H$. Since H is a k-bialgebra, we have $\Delta_H(1_H) = 1_H \otimes 1_H$. Thus,

$$\begin{aligned} \underbrace{(S * \mathrm{id}_H)}_{=\mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H}(1_H) &= (\mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H)(1_H) = \mu_H\left((S \otimes \mathrm{id}_H)\underbrace{(\Delta_H(1_H))}_{=1_H \otimes 1_H}\right) \\ &= \mu_H\left(\underbrace{(S \otimes \mathrm{id}_H)(1_H \otimes 1_H)}_{=S(1_H) \otimes \mathrm{id}_H(1_H)}\right) = \mu_H(S(1_H) \otimes \mathrm{id}_H(1_H)) \\ &= S(1_H) \cdot \underbrace{\mathrm{id}_H(1_H)}_{=1_H} \qquad \text{(since } \mu_H \text{ is the multiplication map)} \\ &= S(1_H). \end{aligned}$$

Compared with $\underbrace{(S * \mathrm{id}_H)}_{=e_{H,H}}(1_H) = e_{H,H}(1_H) = 1_H$, this yields $S(1_H) = 1_H$. Also, $e_{H,H}(1_H) = 1_H$.

Also, the map $e_{H,H}$ is graded (by Proposition 16.18 **(b)**, applied to $C = H$ and $A = H$), and the map S is graded (since S is the antipode of H, while H is a graded k-Hopf algebra).

Thus, we can apply Theorem 28.9 to $P = e_{H,H}$ and $Q = S$.

Applying Theorem 28.9 **(a)** to $P = e_{H,H}$ and $Q = S$, we obtain $(e_{H,H} * E_H * S)(H) \subseteq (\mathrm{Prim}\, H)^+$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as $(E_H * S)(H) \subseteq (\mathrm{Prim}\, H)^+$. This proves Corollary 28.10 **(a)**.

Applying Theorem 28.9 **(b)** to $P = e_{H,H}$ and $Q = S$, we obtain $E_H\left((\mathrm{Prim}\, H)^+\right) \subseteq (e_{H,H} * E_H * S)(H)$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as $E_H\left((\mathrm{Prim}\, H)^+\right) \subseteq (E_H * S)(H)$. This proves Corollary 28.10 **(b)**.

Applying Theorem 28.9 **(c)** to $P = e_{H,H}$ and $Q = S$, we obtain $(e_{H,H} * E_H * S) \circ (e_{H,H} * E_H * S) = E_H \circ (e_{H,H} * E_H * S) = (e_{H,H} * E_H * S) \circ E_H$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as $(E_H * S) \circ (E_H * S) = E_H \circ (E_H * S) = (E_H * S) \circ E_H$. This proves Corollary 28.10 **(c)**.

But we can also apply Theorem 28.9 to $P = S$ and $Q = e_{H,H}$.

Applying Theorem 28.9 **(a)** to $P = S$ and $Q = e_{H,H}$, we obtain $(S * E_H * e_{H,H})(H) \subseteq (\mathrm{Prim}\, H)^+$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as $(S * E_H)(H) \subseteq (\mathrm{Prim}\, H)^+$. This proves Corollary 28.10 **(d)**.

Applying Theorem 28.9 **(b)** to $P = S$ and $Q = e_{H,H}$, we obtain $E_H\left(\left(\operatorname{Prim} H\right)^+\right) \subseteq \left(S * E_H * e_{H,H}\right)(H)$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as $E_H\left(\left(\operatorname{Prim} H\right)^+\right) \subseteq \left(S * E_H\right)(H)$. This proves Corollary 28.10 **(e)**.

Applying Theorem 28.9 **(c)** to $P = S$ and $Q = e_{H,H}$, we obtain $\left(S * E_H * e_{H,H}\right) \circ \left(S * E_H * e_{H,H}\right) = E_H \circ \left(S * E_H * e_{H,H}\right) = \left(S * E_H * e_{H,H}\right) \circ E_H$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as $\left(S * E_H\right) \circ \left(S * E_H\right) = E_H \circ \left(S * E_H\right) = \left(S * E_H\right) \circ E_H$. This proves Corollary 28.10 **(f)**. □

In order to specialize the above results to connected graded Hopf algebras, we first observe a simple fact:

Proposition 28.11. Let k be a field. Let H be a connected graded k-bialgebra. Then, $\operatorname{Prim} H \subseteq \bigoplus_{n \geq 1} H_n$.

Proof of Proposition 28.11. Let $x \in \operatorname{Prim} H$. Since H is graded, we have $H = \bigoplus_{n \in \mathbb{N}} H_n$. Now, $x \in \operatorname{Prim} H \subseteq H = \bigoplus_{n \in \mathbb{N}} H_n = H_0 \oplus \left(\bigoplus_{n \geq 1} H_n\right)$. Thus, there exists an $\alpha \in H_0$ and a $\beta \in \bigoplus_{n \geq 1} H_n$ such that $x = \alpha + \beta$. Consider these α and β.

Since H is a graded k-coalgebra, we have $\varepsilon_H\left(H_n\right) = 0$ for every integer $n \geq 1$. Since $\beta \in \bigoplus_{n \geq 1} H_n = \sum_{n \geq 1} H_n$ (since direct sums are sums), we have

$$\begin{aligned} \varepsilon_H(\beta) \in \varepsilon_H\left(\sum_{n \geq 1} H_n\right) &= \sum_{n \geq 1} \underbrace{\varepsilon_H\left(H_n\right)}_{\substack{=0 \\ (\text{since } n \geq 1)}} \qquad (\text{since } \varepsilon_H \text{ is } k\text{-linear}) \\ &= \sum_{n \geq 1} 0 = 0, \end{aligned}$$

so that $\varepsilon_H(\beta) = 0$. But Remark 6.3 shows that $\varepsilon(x) = 0$ (since H is a k-bialgebra, thus a unital coalgebra). Since $x = \alpha + \beta$, we have

$$\varepsilon_H(x) = \varepsilon_H(\alpha + \beta) = \varepsilon_H(\alpha) + \underbrace{\varepsilon_H(\beta)}_{=0} = \varepsilon_H(\alpha).$$

Compared with $\underbrace{\varepsilon_H}_{=\varepsilon}(x) = \varepsilon(x) = 0$, this yields $\varepsilon_H(\alpha) = 0$. Since $\alpha \in H_0$, we have $\varepsilon_H(\alpha) = \left(\varepsilon_H|_{H_0}\right)(\alpha)$. Thus, the equality $\varepsilon_H(\alpha) = 0$ (which we just proved) rewrites as $\left(\varepsilon_H|_{H_0}\right)(\alpha) = 0$.

But since H is connected, the map $\varepsilon_H|_{H_0}\colon H_0 \to k$ is a k-vector space isomorphism (because Definition 16.10 yields that H is connected if and only if the map $\varepsilon_H|_{H_0}\colon H_0 \to k$ is a k-vector space isomorphism). Thus, from the equality $\left(\varepsilon_H|_{H_0}\right)(\alpha) = 0$ (which we proved above), we can conclude that $\alpha = 0$. Now, $x = \underbrace{\alpha}_{=0} + \beta = \beta \in \bigoplus_{n \geq 1} H_n$.

Now, forget that we fixed x. We have thus proven that every $x \in \operatorname{Prim} H$ satisfies $x \in \bigoplus_{n \geq 1} H_n$. In other words, $\operatorname{Prim} H \subseteq \bigoplus_{n \geq 1} H_n$. Proposition 28.11 is proven. □

Here come equivalent versions of parts **(a)** and **(b)** of Theorem 28.9:

Corollary 28.12. Let k be a field. Let H be a cocommutative graded k-bialgebra. Let E_H be defined according to Definition 27.1. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-coalgebra homomorphisms satisfying $P(1_H) = 1_H$, $Q(1_H) = 1_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

(a) Then, $(P * E_H * Q)(H) \subseteq \operatorname{Prim} H$.

(b) Besides, $E_H(\operatorname{Prim} H) \subseteq (P * E_H * Q)(H)$.

Proof of Corollary 28.12. Define $(\operatorname{Prim} H)^+$ as in Theorem 28.9. Then, $(\operatorname{Prim} H)^+ = (\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right) \subseteq \operatorname{Prim} H$.

Theorem 28.9 **(a)** states that $(P * E_H * Q)(H) \subseteq (\operatorname{Prim} H)^+$. Combined with $(\operatorname{Prim} H)^+ \subseteq \operatorname{Prim} H$, this yields $(P * E_H * Q)(H) \subseteq \operatorname{Prim} H$. This proves Corollary 28.12 **(a)**.

In the proof of Theorem 28.9 **(b)**, we showed that $E_H(\operatorname{Prim} H) \subseteq (P * E_H * Q)(H)$. This proves Corollary 28.12 **(b)**.

(Note that we referred to the proof of Theorem 28.9 **(b)** here; but this was not strictly necessary since we could have just as well derived Corollary 28.12 **(b)** from Theorem 28.9 **(b)** without recourse to its proof. This would have taken a bit more work, though.) □

Now, let us do the same to parts **(a)**, **(b)**, **(d)** and **(e)** of Corollary 28.10:

Corollary 28.13. Let k be a field. Let H be a cocommutative graded k-Hopf algebra. Let S be the antipode of H. Let E_H be defined according to Definition 27.1. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H.

(a) Then, $(E_H * S)(H) \subseteq \operatorname{Prim} H$.

(b) Besides, $E_H(\operatorname{Prim} H) \subseteq (E_H * S)(H)$.

(c) Also, $(S * E_H)(H) \subseteq \operatorname{Prim} H$.

(d) Besides, $E_H(\operatorname{Prim} H) \subseteq (S * E_H)(H)$.

Proof of Corollary 28.13. Just as in the proof of Corollary 28.6, we can prove the following facts:

- The map S is a k-coalgebra homomorphism from H to H.
- The map $e_{H,H}$ is a k-coalgebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).
- We have $S * \mathrm{id}_H * e_{H,H} = e_{H,H}$ and $e_{H,H} * \mathrm{id}_H * S = e_{H,H}$.

Just as in the proof of Corollary 28.10, we can prove the following facts:

- We have $e_{H,H}(1_H) = 1_H$ and $S(1_H) = 1_H$.
- The maps $e_{H,H}$ and S are graded.

As a consequence, we can apply Corollary 28.12 to $P = e_{H,H}$ and $Q = S$.

Applying Corollary 28.12 **(a)** to $P = e_{H,H}$ and $Q = S$, we obtain that $(e_{H,H} * E_H * S)(H) \subseteq \operatorname{Prim} H$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as $(E_H * S)(H) \subseteq \operatorname{Prim} H$. This proves Corollary 28.13 **(a)**.

Applying Corollary 28.12 **(b)** to $P = e_{H,H}$ and $Q = S$, we obtain that $E_H(\operatorname{Prim} H) \subseteq (e_{H,H} * E_H * S)(H)$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as $E_H(\operatorname{Prim} H) \subseteq (E_H * S)(H)$. This proves Corollary 28.13 **(b)**.

But we can also apply Corollary 28.12 to $P = S$ and $Q = e_{H,H}$.

Applying Corollary 28.12 **(a)** to $P = S$ and $Q = e_{H,H}$, we obtain that $(S * E_H * e_{H,H})(H) \subseteq \operatorname{Prim} H$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as $(S * E_H)(H) \subseteq \operatorname{Prim} H$. This proves Corollary 28.13 **(c)**.

Applying Corollary 28.12 **(b)** to $P = S$ and $Q = e_{H,H}$, we obtain that $E_H(\operatorname{Prim} H) \subseteq (S * E_H * e_{H,H})(H)$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as $E_H(\operatorname{Prim} H) \subseteq (S * E_H)(H)$. This proves Corollary 28.13 **(d)**. □

We now come to the case of fields of characteristic 0. The following generalizes Theorem 28.1:

Theorem 28.14. Let k be a field of characteristic 0. Let H be a cocommutative graded k-bialgebra. Let E_H be defined according to Definition 27.1. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H. Let $(\operatorname{Prim} H)^+$ denote the intersection $(\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right)$.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-coalgebra homomorphisms satisfying $P(1_H) = 1_H$, $Q(1_H) = 1_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Then, the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$.

Proof of Theorem 28.14. Recall that $(\operatorname{Prim} H)^+ = (\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right) = (\operatorname{Prim} H) \cap \left(\bigoplus_{\ell \geq 1} H_\ell \right)$ (here, we renamed the index n as ℓ in the direct sum). Notice that $(\operatorname{Prim} H)^+ = (\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right) \subseteq \operatorname{Prim} H$.

Proposition 18.3 yields that $\operatorname{Prim} H$ is a homogeneous subspace of H. In other words, $\operatorname{Prim} H = \bigoplus_{n \in \mathbb{N}} ((\operatorname{Prim} H) \cap H_n)$ (because Definition 18.1 yields that $\operatorname{Prim} H$ is a homogeneous subspace of H if and only if $\operatorname{Prim} H = \bigoplus_{n \in \mathbb{N}} ((\operatorname{Prim} H) \cap H_n)$).

Now, it is easy to see that every $n \in \mathbb{N}$ satisfies

$$E_H^{\mathrm{inv}}((\operatorname{Prim} H) \cap H_n) \subseteq (\operatorname{Prim} H)^+. \tag{299}$$

[143] Now, since $\operatorname{Prim} H = \bigoplus_{n\in\mathbb{N}} ((\operatorname{Prim} H) \cap H_n) = \sum_{n\in\mathbb{N}} (\operatorname{Prim} H) \cap H_n$ (since direct sums are sums), we have

$$E_H^{\mathrm{inv}}(\operatorname{Prim} H) = E_H^{\mathrm{inv}}\left(\sum_{n\in\mathbb{N}} (\operatorname{Prim} H)\cap H_n\right) = \sum_{n\in\mathbb{N}} \underbrace{E_H^{\mathrm{inv}}((\operatorname{Prim} H)\cap H_n)}_{\substack{\subseteq (\operatorname{Prim} H)^+ \\ \text{(by (299))}}}$$
$$\subseteq \sum_{n\in\mathbb{N}} (\operatorname{Prim} H)^+ \subseteq (\operatorname{Prim} H)^+ \qquad \left(\text{since } (\operatorname{Prim} H)^+ \text{ is a } k\text{-vector space}\right). \tag{300}$$

Now,

$$\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)(H) = E_H^{\mathrm{inv}} \underbrace{\left((P * E_H * Q)(H)\right)}_{\substack{\subseteq (\operatorname{Prim} H)^+ \\ \text{(by Theorem 28.9 \textbf{(a)})}}} \subseteq E_H^{\mathrm{inv}}\left(\underbrace{(\operatorname{Prim} H)^+}_{\subseteq \operatorname{Prim} H}\right)$$
$$\subseteq E_H^{\mathrm{inv}}(\operatorname{Prim} H) \subseteq (\operatorname{Prim} H)^+ \qquad \text{(by (300))}. \tag{301}$$

On the other hand,

$$\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)|_{(\operatorname{Prim} H)^+} = \mathrm{id}_{(\operatorname{Prim} H)^+}. \tag{302}$$

[144]

---

[143] *Proof of (299).* Let $n \in \mathbb{N}$. Let $v \in (\operatorname{Prim} H) \cap H_n$. We will prove that $E_H^{\mathrm{inv}}(v) \in (\operatorname{Prim} H)^+$ now.

In fact, define $(b_\ell)_{\ell\in\mathbb{N}}$ as in Definition 27.9. Note that this definition yields $b_0 = \begin{cases} \frac{1}{0}, & \text{if } 0 > 0; \\ 0, & \text{if } 0 = 0 \end{cases} = 0$ (since $0 = 0$).

By Remark 27.10 (applied to $V = H$), we have $E_H^{\mathrm{inv}} = E_H^{(b_\ell)_{\ell\in\mathbb{N}}}$.

We have $v \in (\operatorname{Prim} H) \cap H_n \subseteq H_n$ and thus $E_H^{(b_\ell)_{\ell\in\mathbb{N}}}(v) = b_n v$ (by Proposition 27.7 **(a)**, applied to $(a_\ell)_{\ell\in\mathbb{N}} = (b_\ell)_{\ell\in\mathbb{N}}$). Since $E_H^{(b_\ell)_{\ell\in\mathbb{N}}} = E_H^{\mathrm{inv}}$, this rewrites as $E_H^{\mathrm{inv}}(v) = b_n v$.

We must be in one of the following two cases:

Case 1: We have $n = 0$.

Case 2: We have $n > 0$.

Let us consider Case 1 first. In this case, $n = 0$, so that $b_n v = \underbrace{b_0}_{=0} v = 0v = 0$. Thus, $E_H^{\mathrm{inv}}(v) = b_n v = 0 \in (\operatorname{Prim} H)^+$. Thus, $E_H^{\mathrm{inv}}(v) \in (\operatorname{Prim} H)^+$ is proven in Case 1.

Next, let us consider Case 2. In this case, $n > 0$, so that $n \geq 1$ and thus $H_n \subseteq \bigoplus_{\ell\geq 1} H_\ell$. Thus, $v \in H_n \subseteq \bigoplus_{\ell\geq 1} H_\ell$. Combined with $v \in (\operatorname{Prim} H) \cap H_n \subseteq \operatorname{Prim} H$, this yields $v \in (\operatorname{Prim} H) \cap \left(\bigoplus_{\ell\geq 1} H_\ell\right) = (\operatorname{Prim} H)^+$. Now, $E_H^{\mathrm{inv}}(v) = b_n \underbrace{v}_{\in (\operatorname{Prim} H)^+} \in b_n (\operatorname{Prim} H)^+ \subseteq (\operatorname{Prim} H)^+$ (since $(\operatorname{Prim} H)^+$ is a k-vector space). Thus, $E_H^{\mathrm{inv}}(v) \in (\operatorname{Prim} H)^+$ is proven in Case 2.

We have therefore proven $E_H^{\mathrm{inv}}(v) \in (\operatorname{Prim} H)^+$ in both cases 1 and 2. Since these cases cover all possibilities, we conclude that $E_H^{\mathrm{inv}}(v) \in (\operatorname{Prim} H)^+$ always holds.

Now forget that we fixed v. We have thus shown that every $v \in (\operatorname{Prim} H) \cap H_n$ satisfies $E_H^{\mathrm{inv}}(v) \in (\operatorname{Prim} H)^+$. In other words, $E_H^{\mathrm{inv}}((\operatorname{Prim} H) \cap H_n) \subseteq (\operatorname{Prim} H)^+$, thus proving (299).

[144] *Proof of (302).* We have $1_H \in H_0$ (since H is a graded k-algebra). Thus, Proposition 27.2 **(a)**

So we know that $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a k-linear map satisfying $\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)(H) \subseteq (\operatorname{Prim} H)^+$ (by (301)) and $\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)|_{(\operatorname{Prim} H)^+} = \mathrm{id}_{(\operatorname{Prim} H)^+}$ (by (302)). In other words, $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$. This proves Theorem 28.14. $\square$

We can now get Theorem 28.1 as a corollary:

Proof of Theorem 28.1. Just as in the proof of Corollary 28.6, we can prove the following facts:

- The map S is a k-coalgebra homomorphism from H to H.
- The map $e_{H,H}$ is a k-coalgebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).
- We have $S = \mathrm{id}_H^{*(-1)}$.
- We have $S * \mathrm{id}_H * e_{H,H} = e_{H,H}$ and $e_{H,H} * \mathrm{id}_H * S = e_{H,H}$.

Just as in the proof of Corollary 28.10, we can prove the following facts:

- We have $e_{H,H}(1_H) = 1_H$ and $S(1_H) = 1_H$.
- The maps $e_{H,H}$ and S are graded.

As a consequence, we can apply Theorem 28.14 to $P = e_{H,H}$ and $Q = S$. As a result, we obtain that the map $E_H^{\mathrm{inv}} \circ (e_{H,H} * E_H * S)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$. This proves Theorem 28.1 **(a)**.

But we can also apply Theorem 28.14 to $P = S$ and $Q = e_{H,H}$. As a result, we obtain that the map $E_H^{\mathrm{inv}} \circ (S * E_H * e_{H,H})$ is a projection from H to the subspace

---

(applied to $n = 0$ and $v = 1_H$) yields $E_H(1_H) = 0 \cdot 1_H = 0$. Thus, Proposition 28.7 (applied to $K = E_H$) yields that

$$\text{every } x \in \operatorname{Prim} H \text{ satisfies } (P * E_H * Q)(x) = E_H(x). \tag{303}$$

Now, let $x \in (\operatorname{Prim} H)^+$. Then, $x \in (\operatorname{Prim} H)^+ = (\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n\right) \subseteq \bigoplus_{n \geq 1} H_n$. Hence, Corollary 27.12 **(b)** (applied to $V = H$ and $v = x$) yields $\left(E_H^{\mathrm{inv}} \circ E_H\right)(x) = x$.

On the other hand, $x \in (\operatorname{Prim} H)^+ \subseteq \operatorname{Prim} H$, so that $(P * E_H * Q)(x) = E_H(x)$ (by (303)). Now,

$$\begin{aligned}
&\left(\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)|_{(\operatorname{Prim} H)^+}\right)(x) \\
&= \left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)(x) = E_H^{\mathrm{inv}}\underbrace{\left((P * E_H * Q)(x)\right)}_{=E_H(x)} = E_H^{\mathrm{inv}}\left(E_H(x)\right) \\
&= \left(E_H^{\mathrm{inv}} \circ E_H\right)(x) = x = \mathrm{id}_{(\operatorname{Prim} H)^+}(x).
\end{aligned}$$

Now forget that we fixed x. We have thus proven that every $x \in (\operatorname{Prim} H)^+$ satisfies $\left(\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)|_{(\operatorname{Prim} H)^+}\right)(x) = \mathrm{id}_{(\operatorname{Prim} H)^+}(x)$. In other words, $\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)|_{(\operatorname{Prim} H)^+} = \mathrm{id}_{(\operatorname{Prim} H)^+}$. This proves (302).

$(\operatorname{Prim} H)^+$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$. This proves Theorem 28.1 **(b)**. $\square$

Next, we specialize our results to connected graded bialgebras. First, the specialization of Theorem 28.14:

Corollary 28.15. Let k be a field of characteristic 0. Let H be a cocommutative connected graded k-bialgebra. Let E_H be defined according to Definition 27.1. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-coalgebra homomorphisms satisfying $P(1_H) = 1_H$, $Q(1_H) = 1_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Then, the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection from H to the subspace $\operatorname{Prim} H$.

Proof of Corollary 28.15. Define $(\operatorname{Prim} H)^+$ as in Theorem 28.9. Then, $(\operatorname{Prim} H)^+ = (\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right) = \operatorname{Prim} H$ (since Proposition 28.11 yields $\operatorname{Prim} H \subseteq \bigoplus_{n \geq 1} H_n$).

Theorem 28.14 says that the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$. Since $(\operatorname{Prim} H)^+ = \operatorname{Prim} H$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection from H to the subspace $\operatorname{Prim} H$. This proves Corollary 28.15. $\square$

The specialization of Theorem 28.1 is Theorem 28.2, and here is its (obvious) proof:

Proof of Theorem 28.2. Define $(\operatorname{Prim} H)^+$ as in Theorem 28.1. Then, $(\operatorname{Prim} H)^+ = (\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right) = \operatorname{Prim} H$ (since Proposition 28.11 yields $\operatorname{Prim} H \subseteq \bigoplus_{n \geq 1} H_n$).

Theorem 28.1 **(a)** says that the map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$. Since $(\operatorname{Prim} H)^+ = \operatorname{Prim} H$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection from H to the subspace $\operatorname{Prim} H$. This proves Theorem 28.2 **(a)**.

Theorem 28.1 **(b)** says that the map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection from H to the subspace $(\operatorname{Prim} H)^+$. Since $(\operatorname{Prim} H)^+ = \operatorname{Prim} H$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection from H to the subspace $\operatorname{Prim} H$. This proves Theorem 28.2 **(b)**. $\square$

Finally, let us prove a relation between the maps $S * E_H$ and $E_H * S$:

Theorem 28.16. Let k be a field. Let H be a cocommutative graded k-Hopf algebra. Let S be the antipode of H. Let E_H be defined according to Definition 27.1.

(a) We have

$$(E_H * S) \circ S = S \circ (S * E_H) = -S * E_H.$$

(b) We have

$$(S * E_H) \circ S = S \circ (E_H * S) = -E_H * S.$$

To prove Theorem 28.16, we need a (famous) fact:

Theorem 28.17. Let k be a field. Let H be a k-Hopf algebra. Let S be the antipode of H.

(a) We have $\varepsilon_H \circ S = \varepsilon_H$.

(b) If H is cocommutative, we have $\Delta_H \circ S = (S \otimes S) \circ \Delta_H$.

(c) If H is cocommutative, we have $S \circ S = \mathrm{id}_H$.

Proof of Theorem 28.17. Let us define H^{cop} as according to Definition 25.3. Then, $H^{\mathrm{cop}} = (H, \tau_{H,H} \circ \Delta_H, \varepsilon_H)$, so that $\varepsilon_{H^{\mathrm{cop}}} = \varepsilon_H$.

But Proposition 25.4 yields that the antipode of H is a k-coalgebra homomorphism from H^{cop} to H. Since the antipode of H is the map S, this rewrites as follows: The map S is a k-coalgebra homomorphism from H^{cop} to H. Thus, $\varepsilon_{H^{\mathrm{cop}}} \circ S = \varepsilon_H$. Since $\varepsilon_{H^{\mathrm{cop}}} = \varepsilon_H$, this rewrites as $\varepsilon_H \circ S = \varepsilon_H$. This proves Theorem 28.17 **(a)**.

(b) Assume that H is cocommutative. Then, $\tau_{H,H} \circ \Delta_H = \Delta_H$, so that $H^{\mathrm{cop}} = \left(H, \underbrace{\tau_{H,H} \circ \Delta_H}_{=\Delta_H}, \varepsilon_H\right) = (H, \Delta_H, \varepsilon_H) = H$.

We have showed above that the map S is a k-coalgebra homomorphism from H^{cop} to H. Since $H^{\mathrm{cop}} = H$, this rewrites as follows: The map S is a k-coalgebra homomorphism from H to H. Thus, $\Delta_H \circ S = (S \otimes S) \circ \Delta_H$. This proves Theorem 28.17 **(b)**.

(c) The antipode of H is the $*$-inverse of the map id_H (because the antipode of a Hopf algebra is defined as the $*$-inverse of its identity map). Since the antipode of H is S, we thus have shown that S is the $*$-inverse of the map id_H. Thus, $S * \mathrm{id}_H = \mathrm{id}_H * S = e_{H,H}$ (where $e_{H,H}$ is defined as according to Definition 1.12).

Applying (21) to H, H, H, H, H, H, S, S, S, id_H instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(S \circ S) \otimes (\mathrm{id}_H \circ S) = (S \otimes \mathrm{id}_H) \circ (S \otimes S). \tag{304}$$

Now, by the definition of convolution,

$$\begin{aligned}
(S \circ S) * S &= \mu_H \circ \left((S \circ S) \otimes \underbrace{S}_{=\mathrm{id}_H \circ S}\right) \circ \Delta_H = \mu_H \circ \underbrace{((S \circ S) \otimes (\mathrm{id}_H \circ S))}_{\substack{=(S \otimes \mathrm{id}_H) \circ (S \otimes S) \\ \text{(by (304))}}} \circ \Delta_H \\
&= \mu_H \circ (S \otimes \mathrm{id}_H) \circ \underbrace{(S \otimes S) \circ \Delta_H}_{\substack{=\Delta_H \circ S \\ \text{(by Theorem 28.17 (b))}}} = \underbrace{\mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H}_{\substack{=S * \mathrm{id}_H \\ \text{(because } S*\mathrm{id}_H = \mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H \\ \text{by the definition of convolution)}}} \circ S \\
&= \underbrace{(S * \mathrm{id}_H)}_{\substack{=e_{H,H} = \eta_H \circ \varepsilon_H \\ \text{(by the definition of } e_{H,H})}} \circ S = \eta_H \circ \underbrace{\varepsilon_H \circ S}_{\substack{=\varepsilon_H \\ \text{(by Theorem 28.17 (a))}}} = \eta_H \circ \varepsilon_H = e_{H,H}
\end{aligned}$$

(since $e_{H,H} = \eta_H \circ \varepsilon_H$ by the definition of $e_{H,H}$). Thus,

$$\underbrace{(S \circ S) * S}_{=e_{H,H}} * \mathrm{id}_H = e_{H,H} * \mathrm{id}_H = \mathrm{id}_H .$$

Comparing this with

$$(S \circ S) * \underbrace{S * \mathrm{id}_H}_{=e_{H,H}} = (S \circ S) * e_{H,H} = S \circ S,$$

we obtain $S \circ S = \mathrm{id}_H$. This proves Theorem 28.17 **(c)**. □

Furthermore, we need something very easy and well-known:

Proposition 28.18. Let k be a field. Let H be a k-Hopf algebra. Let S be the antipode of H. Let $x \in \operatorname{Prim} H$. Then, $S(x) = -x$.

Proof of Proposition 28.18. Since $x \in \operatorname{Prim} H =$ (the set of all primitive elements of H), the element x of H is primitive. Thus, $\Delta(x) = x \otimes 1_H + 1_H \otimes x$ (since Definition 6.1 yields that x is primitive if and only if $\Delta(x) = x \otimes 1_H + 1_H \otimes x$).

The antipode of H is the $*$-inverse of the map id_H (because the antipode of a Hopf algebra is defined as the $*$-inverse of its identity map). Since the antipode of H is S, we thus have shown that S is the $*$-inverse of the map id_H. Thus, $S * \mathrm{id}_H = \mathrm{id}_H * S = e_{H,H}$ (where $e_{H,H}$ is defined as according to Definition 1.12) and $S = \mathrm{id}_H^{*(-1)}$.

Since $e_{H,H} = \eta_H \circ \varepsilon_H$ (by the definition of $e_{H,H}$), we have

$$e_{H,H}(x) = (\eta_H \circ \varepsilon_H)(x) = \eta_H \left(\underbrace{\varepsilon_H}_{=\varepsilon}(x) \right) = \eta_H \underbrace{(\varepsilon(x))}_{\substack{=0 \\ \text{(by Remark 6.3)}}} = \eta_H(0) = 0$$

(since η_H is k-linear).

Just as in the proof of Corollary 28.10, we can now show that $S(1_H) = 1_H$. Now,

since $e_{H,H} = S * \mathrm{id}_H = \mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H$ (by the definition of convolution), we have

$$\begin{aligned}
e_{H,H}(x) &= (\mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H)(x) = \mu_H\left((S \otimes \mathrm{id}_H)\left(\underbrace{\Delta_H}_{=\Delta}(x)\right)\right) \\
&= \mu_H\left((S \otimes \mathrm{id}_H)\underbrace{(\Delta(x))}_{=x\otimes 1_H + 1_H \otimes x}\right) = \mu_H\left(\underbrace{(S \otimes \mathrm{id}_H)(x \otimes 1_H + 1_H \otimes x)}_{\substack{=(S\otimes \mathrm{id}_H)(x\otimes 1_H)+(S\otimes \mathrm{id}_H)(1_H\otimes x) \\ (\text{since } S\otimes \mathrm{id}_H \text{ is } k\text{-linear})}}\right) \\
&= \mu_H\left(\underbrace{(S \otimes \mathrm{id}_H)(x \otimes 1_H)}_{=S(x)\otimes \mathrm{id}_H(1_H)} + \underbrace{(S \otimes \mathrm{id}_H)(1_H \otimes x)}_{=S(1_H)\otimes \mathrm{id}_H(x)}\right) \\
&= \mu_H\left(S(x) \otimes \underbrace{\mathrm{id}_H(1_H)}_{=1_H} + \underbrace{S(1_H)}_{=1_H} \otimes \underbrace{\mathrm{id}_H(x)}_{=x}\right) = \mu_H(S(x) \otimes 1_H + 1_H \otimes x) \\
&= \underbrace{\mu_H(S(x) \otimes 1_H)}_{\substack{=S(x)1_H \\ (\text{since } \mu_H \text{ is the} \\ \text{multiplication map})}} + \underbrace{\mu_H(1_H \otimes x)}_{\substack{=1_H x \\ (\text{since } \mu_H \text{ is the} \\ \text{multiplication map})}} \qquad (\text{since } \mu_H \text{ is } k\text{-linear}) \\
&= S(x)\,1_H + 1_H x = S(x) + x.
\end{aligned}$$

Compared with $e_{H,H}(x) = 0$, this yields $S(x) + x = 0$, and thus $S(x) = -x$. This proves Proposition 28.18. □

Proof of Theorem 28.16. Let us first notice that

$$E_H \circ e_{H,H} = 0. \tag{305}$$

145

Since H is a graded k-algebra, the multiplication map $\mu_H : H \otimes H \to H$ of H is graded. Thus, Proposition 27.4 (applied to $V = H \otimes H$ and $W = H$) yields $\mu_H \circ E_{H\otimes H} =$

[145] *Proof of (305):* Let $x \in H$. Then, $e_{H,H} = \eta_H \circ \varepsilon_H$ (by the definition of $e_{H,H}$), so that

$$\begin{aligned}
e_{H,H}(x) &= (\eta_H \circ \varepsilon_H)(x) = \eta_H(\varepsilon_H(x)) = \underbrace{\varepsilon_H(x)}_{\in k} \cdot \underbrace{1_H}_{\substack{\in H_0 \\ (\text{since } H \text{ is a graded} \\ k\text{-algebra})}} \qquad (\text{by the definition of } \eta_H) \\
&\in kH_0 \subseteq H_0 \qquad (\text{since } H_0 \text{ is a } k\text{-vector space}),
\end{aligned}$$

and thus $E_H(e_{H,H}(x)) = 0 e_{H,H}(x)$ (by Proposition 27.2 **(a)**, applied to $V = H$, $n = 0$ and $v = e_{H,H}(x)$). Thus, $(E_H \circ e_{H,H})(x) = E_H(e_{H,H}(x)) = 0 e_{H,H}(x) = 0$.

Now, forget that we fixed x. We thus have proven that every $x \in H$ satisfies $(E_H \circ e_{H,H})(x) = 0$. Thus, $E_H \circ e_{H,H} = 0$, so that (305) is proven.

$E_H \circ \mu_H$. Thus,

$$\begin{aligned} E_H \circ \mu_H &= \mu_H \circ \underbrace{E_{H \otimes H}}_{\substack{= E_H \otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H \\ \text{(by Proposition 27.3,} \\ \text{applied to } V=H \text{ and } W=H)}} = \mu_H \circ (E_H \otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H) \\ &= \mu_H \circ (E_H \otimes \mathrm{id}_H) + \mu_H \circ (\mathrm{id}_H \otimes E_H) \\ &\qquad \text{(since composition of } k\text{-linear maps is distributive)}. \end{aligned}$$

This equality can be rewritten in two ways: first,

$$\mu_H \circ (E_H \otimes \mathrm{id}_H) = E_H \circ \mu_H - \mu_H \circ (\mathrm{id}_H \otimes E_H); \tag{306}$$

second,

$$\mu_H \circ (\mathrm{id}_H \otimes E_H) = E_H \circ \mu_H - \mu_H \circ (E_H \otimes \mathrm{id}_H). \tag{307}$$

The antipode of H is the $*$-inverse of the map id_H (because the antipode of a Hopf algebra is defined as the $*$-inverse of its identity map). Since the antipode of H is S, we thus have shown that S is the $*$-inverse of the map id_H. Thus, $S * \mathrm{id}_H = \mathrm{id}_H * S = e_{H,H}$ (where $e_{H,H}$ is defined as according to Definition 1.12).

(a) By the definition of convolution, $E_H * S = \mu_H \circ (E_H \otimes S) \circ \Delta_H$, so that

$$
\begin{aligned}
&(E_H * S) \circ S \\
&= \mu_H \circ (E_H \otimes S) \circ \underbrace{\Delta_H \circ S}_{\substack{=(S\otimes S)\circ\Delta_H \\ \text{(by Theorem 28.17 (b))}}} = \mu_H \circ \underbrace{(E_H \otimes S) \circ (S \otimes S)}_{\substack{=(E_H\circ S)\otimes(S\circ S) \\ \text{(because (21) (applied to } H, H, H, H, H, H, \\ S, E_H, S, S \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta') \\ \text{yields } (E_H\circ S)\otimes(S\circ S)=(E_H\otimes S)\circ(S\otimes S))}} \circ \Delta_H \\
&= \mu_H \circ \left((E_H \circ S) \otimes \underbrace{(S \circ S)}_{\substack{=\mathrm{id}_H \\ \text{(by Theorem 28.17 (c))}}} \right) \circ \Delta_H = \mu_H \circ \left((E_H \circ S) \otimes \underbrace{\mathrm{id}_H}_{=\mathrm{id}_H \circ \mathrm{id}_H} \right) \circ \Delta_H \\
&= \mu_H \circ \underbrace{((E_H \circ S) \otimes (\mathrm{id}_H \circ \mathrm{id}_H))}_{\substack{=(E_H\otimes \mathrm{id}_H)\circ(S\otimes \mathrm{id}_H) \\ \text{(by (21) (applied to } H, H, H, H, H, H, \\ S, E_H, \mathrm{id}_H, \mathrm{id}_H \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta'))}} \circ \Delta_H \\
&= \underbrace{\mu_H \circ (E_H \otimes \mathrm{id}_H)}_{\substack{=E_H\circ\mu_H-\mu_H\circ(\mathrm{id}_H\otimes E_H) \\ \text{(by (306))}}} \circ (S \otimes \mathrm{id}_H) \circ \Delta_H = (E_H \circ \mu_H - \mu_H \circ (\mathrm{id}_H \otimes E_H)) \circ (S \otimes \mathrm{id}_H) \circ \Delta_H \\
&= E_H \circ \underbrace{\mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H}_{\substack{=S*\mathrm{id}_H \\ \text{(since } S*\mathrm{id}_H=\mu_H\circ(S\otimes\mathrm{id}_H)\circ\Delta_H \\ \text{by the definition of convolution)}}} - \mu_H \circ \underbrace{(\mathrm{id}_H \otimes E_H) \circ (S \otimes \mathrm{id}_H)}_{\substack{=(\mathrm{id}_H\circ S)\otimes(E_H\circ\mathrm{id}_H) \\ \text{(because (21) (applied to } H, H, H, H, H, H, \\ S, \mathrm{id}_H, \mathrm{id}_H, E_H \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta') \\ \text{yields } (\mathrm{id}_H\circ S)\otimes(E_H\circ\mathrm{id}_H)=(\mathrm{id}_H\otimes E_H)\circ(S\otimes\mathrm{id}_H))}} \circ \Delta_H \\
&\qquad \text{(since composition of } k\text{-linear maps is distributive)} \\
&= E_H \circ \underbrace{(S * \mathrm{id}_H)}_{=e_{H,H}} - \mu_H \circ \left(\underbrace{(\mathrm{id}_H \circ S)}_{=S} \otimes \underbrace{(E_H \circ \mathrm{id}_H)}_{=E_H} \right) \circ \Delta_H \\
&= \underbrace{E_H \circ e_{H,H}}_{\substack{=0 \\ \text{(by (305))}}} - \underbrace{\mu_H \circ (S \otimes E_H) \circ \Delta_H}_{\substack{=S*E_H \\ \text{(since } S*E_H=\mu_H\circ(S\otimes E_H)\circ\Delta_H \\ \text{by the definition of convolution)}}} = -S * E_H. \qquad (308)
\end{aligned}
$$

Let $(\operatorname{Prim} H)^+$ denote the intersection $(\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right)$. Then, $(\operatorname{Prim} H)^+ \subseteq \operatorname{Prim} H$.

Now, let $y \in H$. Then,

$$
\begin{aligned}
(S * E_H)(y) &\in (S * E_H)(H) \subseteq (\operatorname{Prim} H)^+ \qquad \text{(by Corollary 28.10 (d))} \\
&\subseteq \operatorname{Prim} H,
\end{aligned}
$$

so that Proposition 28.18 (applied to $x = (S * E_H)(y)$) yields $S((S * E_H)(y)) = -(S * E_H)(y)$. Thus,

$$
(S \circ (S * E_H))(y) = S((S * E_H)(y)) = -(S * E_H)(y) = (-S * E_H)(y).
$$

Now, forget that we fixed y. We have thus proven that every $y \in H$ satisfies $(S \circ (S * E_H))(y) = (-S * E_H)(y)$. In other words, $S \circ (S * E_H) = -S * E_H$. Combined with (308), this yields $(E_H * S) \circ S = S \circ (S * E_H) = -S * E_H$. This proves Theorem 28.16 **(a)**.

(b) By the definition of convolution, $S * E_H = \mu_H \circ (S \otimes E_H) \circ \Delta_H$, so that

$$
\begin{aligned}
&(S * E_H) \circ S \\
&= \mu_H \circ (S \otimes E_H) \circ \underbrace{\Delta_H \circ S}_{\substack{=(S \otimes S) \circ \Delta_H \\ \text{(by Theorem 28.17 (b))}}} = \mu_H \circ \underbrace{(S \otimes E_H) \circ (S \otimes S)}_{\substack{=(S \circ S) \otimes (E_H \circ S) \\ \text{(because (21) (applied to } H, H, H, H, H, H, \\ S, S, S, E_H \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta') \\ \text{yields } (S \circ S) \otimes (E_H \circ S) = (S \otimes E_H) \circ (S \otimes S))}} \circ \Delta_H \\
&= \mu_H \circ \left(\underbrace{(S \circ S)}_{\substack{=\mathrm{id}_H \\ \text{(by Theorem 28.17 (c))}}} \otimes (E_H \circ S) \right) \circ \Delta_H = \mu_H \circ \left(\underbrace{\mathrm{id}_H}_{=\mathrm{id}_H \circ \mathrm{id}_H} \otimes (E_H \circ S) \right) \circ \Delta_H \\
&= \mu_H \circ \underbrace{((\mathrm{id}_H \circ \mathrm{id}_H) \otimes (E_H \circ S))}_{\substack{=(\mathrm{id}_H \otimes E_H) \circ (\mathrm{id}_H \otimes S) \\ \text{(by (21) (applied to } H, H, H, H, H, H, \\ \mathrm{id}_H, \mathrm{id}_H, S, E_H \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta'))}} \circ \Delta_H \\
&= \underbrace{\mu_H \circ (\mathrm{id}_H \otimes E_H)}_{\substack{=E_H \circ \mu_H - \mu_H \circ (E_H \otimes \mathrm{id}_H) \\ \text{(by (307))}}} \circ (\mathrm{id}_H \otimes S) \circ \Delta_H = (E_H \circ \mu_H - \mu_H \circ (E_H \otimes \mathrm{id}_H)) \circ (\mathrm{id}_H \otimes S) \circ \Delta_H \\
&= E_H \circ \underbrace{\mu_H \circ (\mathrm{id}_H \otimes S) \circ \Delta_H}_{\substack{=\mathrm{id}_H * S \\ \text{(since } \mathrm{id}_H * S = \mu_H \circ (\mathrm{id}_H \otimes S) \circ \Delta_H \\ \text{by the definition of convolution)}}} - \mu_H \circ \underbrace{(E_H \otimes \mathrm{id}_H) \circ (\mathrm{id}_H \otimes S)}_{\substack{=(E_H \circ \mathrm{id}_H) \otimes (\mathrm{id}_H \circ S) \\ \text{(because (21) (applied to } H, H, H, H, H, H, \\ \mathrm{id}_H, E_H, S, \mathrm{id}_H \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta') \\ \text{yields } (E_H \circ \mathrm{id}_H) \otimes (\mathrm{id}_H \circ S) = (E_H \otimes \mathrm{id}_H) \circ (\mathrm{id}_H \otimes S))}} \circ \Delta_H \\
&\qquad \text{(since composition of } k\text{-linear maps is distributive)} \\
&= E_H \circ \underbrace{(\mathrm{id}_H * S)}_{=e_{H,H}} - \mu_H \circ \left(\underbrace{(E_H \circ \mathrm{id}_H)}_{=E_H} \otimes \underbrace{(\mathrm{id}_H \circ S)}_{=S} \right) \circ \Delta_H \\
&= \underbrace{E_H \circ e_{H,H}}_{\substack{=0 \\ \text{(by (305))}}} - \underbrace{\mu_H \circ (E_H \otimes S) \circ \Delta_H}_{\substack{=E_H * S \\ \text{(since } E_H * S = \mu_H \circ (E_H \otimes S) \circ \Delta_H \\ \text{by the definition of convolution)}}} = -E_H * S. \qquad (309)
\end{aligned}
$$

Let $(\operatorname{Prim} H)^+$ denote the intersection $(\operatorname{Prim} H) \cap \left(\bigoplus_{n \geq 1} H_n \right)$. Then, $(\operatorname{Prim} H)^+ \subseteq \operatorname{Prim} H$.

Now, let $y \in H$. Then,

$$
\begin{aligned}
(E_H * S)(y) &\in (E_H * S)(H) \subseteq (\operatorname{Prim} H)^+ \qquad \text{(by Corollary 28.10 (a))} \\
&\subseteq \operatorname{Prim} H,
\end{aligned}
$$

so that Proposition 28.18 (applied to $x = (E_H * S)(y)$) yields $S((E_H * S)(y)) = -(E_H * S)(y)$. Thus,

$$
(S \circ (E_H * S))(y) = S((E_H * S)(y)) = -(E_H * S)(y) = (-E_H * S)(y).
$$

Now, forget that we fixed y. We have thus proven that every $y \in H$ satisfies $(S \circ (E_H * S))(y) = (-E_H * S)(y)$. In other words, $S \circ (E_H * S) = -E_H * S$. Combined with (309), this yields $(S * E_H) \circ S = S \circ (E_H * S) = -E_H * S$. This proves Theorem 28.16 **(b)**. $\square$

§29. The Dynkin idempotents in commutative Hopf algebras

This section, §29, is devoted to the dual statements of the ones from §28. Here comes the dual of Theorem 28.1:

Theorem 29.1. Let k be a field of characteristic 0. Let H be a commutative graded k-Hopf algebra. Let S be the antipode of H. Define a map $E_H : H \to H$ according to Definition 27.1. Define a map $E_H^{\mathrm{inv}} : H \to H$ according to Definition 27.9. Then:

(a) The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (E_H * S)\right) = H_0 + \left(\operatorname{Ker}(\varepsilon_H)\right)^2$. [146]

(b) The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (S * E_H)\right) = H_0 + \left(\operatorname{Ker}(\varepsilon_H)\right)^2$.

Note that in the case when H is connected, it is easy to see that $H_0 = k \cdot 1_H$, and thus this yields:

Theorem 29.2. Let k be a field of characteristic 0. Let H be a commutative connected graded k-Hopf algebra. Let S be the antipode of H. Define a map $E_H : H \to H$ according to Definition 27.1. Define a map $E_H^{\mathrm{inv}} : H \to H$ according to Definition 27.9. Then:

(a) The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (E_H * S)\right) = k \cdot 1_H + \left(\operatorname{Ker}(\varepsilon_H)\right)^2$. [147]

(b) The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (S * E_H)\right) = k \cdot 1_H + \left(\operatorname{Ker}(\varepsilon_H)\right)^2$.

The maps $E_H^{\mathrm{inv}} \circ (E_H * S)$ and $E_H^{\mathrm{inv}} \circ (S * E_H)$ are called the *Dynkin idempotents* of H.

We will prove these theorems through a generalization, which requires us to define the notion of a *derivation*:

Definition 29.3. Let k be a field. Let H be a k-algebra. Let $f : H \to H$ be a k-linear map. Then, f is said to be a *derivation* if and only if $f \circ \mu_H = \mu_H \circ (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f)$.

Keep in mind that **a derivation is not the same as an $(\varepsilon_H, \varepsilon_H)$-derivation**. (The latter has been defined in Definitions 15.6 and 15.7.) We will, however, connect these two notions in the following results.

Definition 29.3 could be generalized to k-linear maps $f : H \to M$ with M being a (H, H)-bimodule; but we will not need this generalization and we will not even define the notion of a (H, H)-bimodule. Let us, however, give an equivalent rewriting of Definition 29.3:

[146] Recall that the notation $\left(\operatorname{Ker}(\varepsilon_H)\right)^2$ is to be understood according to Convention 15.2. Hence, $\left(\operatorname{Ker}(\varepsilon_H)\right)^2$ means the subspace $\left(\operatorname{Ker}(\varepsilon_H)\right) \cdot \left(\operatorname{Ker}(\varepsilon_H)\right)$ of H.

[147] Recall that the notation $\left(\operatorname{Ker}(\varepsilon_H)\right)^2$ is to be understood according to Convention 15.2. Hence, $\left(\operatorname{Ker}(\varepsilon_H)\right)^2$ means the subspace $\left(\operatorname{Ker}(\varepsilon_H)\right) \cdot \left(\operatorname{Ker}(\varepsilon_H)\right)$ of H.

Definition 29.4. Let k be a field. Let H be a k-algebra. Let $f : H \to H$ be a k-linear map. Then, f is said to be a *derivation* if and only if every $(a, b) \in H \times H$ satisfies $f(ab) = f(a)\, b + af(b)$.

We will be able to use both Definitions 29.3 and 29.4 in parallel as soon as we have shown the following proposition:

Proposition 29.5. Definition 29.3 and Definition 29.4 are equivalent.

Proof of Proposition 29.5. Let k be a field. Let H be a k-algebra. Let $f : H \to H$ be a k-linear map.

It is well-known that two k-linear maps from a tensor product are equal if and only if they are equal on each pure tensor. Applying this fact to the two k-linear maps $f \circ \mu_H : H \otimes H \to H$ and $\mu_H \circ (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f) : H \otimes H \to H$, we conclude that we have the following equivalence:

$$\begin{aligned} &(\text{the two maps } f \circ \mu_H \text{ and } \mu_H \circ (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f) \text{ are equal}) \\ \iff\ &(\text{the two maps } f \circ \mu_H \text{ and } \mu_H \circ (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f) \text{ are equal on each pure tensor}). \end{aligned} \tag{310}$$

Since pure tensors in $H \otimes H$ are tensors of the form $a \otimes b$ with $(a, b) \in H \times H$, we have the equivalence

$$\begin{aligned} &(\text{the two maps } f \circ \mu_H \text{ and } \mu_H \circ (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f) \text{ are equal on each pure tensor}) \\ \iff\ &(\text{the two maps } f \circ \mu_H \text{ and } \mu_H \circ (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f) \text{ are} \\ &\qquad \text{equal on } a \otimes b \text{ for each } (a, b) \in H \times H) \\ \iff\ &((f \circ \mu_H)(a \otimes b) = (\mu_H \circ (f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f))(a \otimes b) \text{ for each } (a, b) \in H \times H). \end{aligned} \tag{311}$$

But every $(a, b) \in H \times H$ satisfies

$$(f \circ \mu_H)(a \otimes b) = f\left(\underbrace{\mu_H(a \otimes b)}_{\substack{=ab \\ (\text{since } \mu_H \text{ is the multiplication map})}} \right) = f(ab)$$

and

$$
\begin{aligned}
&\left(\mu_H \circ \left(f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f\right)\right)(a \otimes b) \\
&= \mu_H\left(\underbrace{\left(f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f\right)(a \otimes b)}_{=(f \otimes \mathrm{id}_H)(a \otimes b) + (\mathrm{id}_H \otimes f)(a \otimes b)}\right) \\
&= \mu_H\left(\underbrace{\left(f \otimes \mathrm{id}_H\right)(a \otimes b)}_{=f(a) \otimes \mathrm{id}_H(b)} + \underbrace{\left(\mathrm{id}_H \otimes f\right)(a \otimes b)}_{=\mathrm{id}_H(a) \otimes f(b)}\right) \\
&= \mu_H\left(f(a) \otimes \underbrace{\mathrm{id}_H(b)}_{=b} + \underbrace{\mathrm{id}_H(a)}_{=a} \otimes f(b)\right) = \mu_H\left(f(a) \otimes b + a \otimes f(b)\right) \\
&= \underbrace{\mu_H\left(f(a) \otimes b\right)}_{\substack{=f(a)b \\ \text{(since } \mu_H \text{ is the} \\ \text{multiplication map)}}} + \underbrace{\mu_H\left(a \otimes f(b)\right)}_{\substack{=af(b) \\ \text{(since } \mu_H \text{ is the} \\ \text{multiplication map)}}} \qquad \text{(since } \mu_H \text{ is } k\text{-linear)} \\
&= f(a)\, b + a f(b)\,.
\end{aligned}
$$

Now, we have the following chain of equivalences:

$$
\begin{aligned}
&\text{(the map } f \text{ is a derivation in the sense of Definition 29.3)} \\
&\iff \left(f \circ \mu_H = \mu_H \circ \left(f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f\right)\right) \qquad \text{(by Definition 29.3)} \\
&\iff \text{(the two maps } f \circ \mu_H \text{ and } \mu_H \circ \left(f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f\right) \text{ are equal)} \\
&\iff \text{(the two maps } f \circ \mu_H \text{ and } \mu_H \circ \left(f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f\right) \text{ are equal on each pure tensor)} \\
&\qquad \text{(by (310))} \\
&\iff \left(\underbrace{\left(f \circ \mu_H\right)(a \otimes b)}_{=f(ab)} = \underbrace{\left(\mu_H \circ \left(f \otimes \mathrm{id}_H + \mathrm{id}_H \otimes f\right)\right)(a \otimes b)}_{=f(a)b + af(b)} \text{ for each } (a,b) \in H \times H\right) \\
&\qquad \text{(by (311))} \\
&\iff \left(f(ab) = f(a)\, b + a f(b) \text{ for each } (a,b) \in H \times H\right) \\
&\iff \text{(the map } f \text{ is a derivation in the sense of Definition 29.4)} \\
&\qquad \text{(by Definition 29.4)}\,.
\end{aligned}
$$

Now, forget that we fixed f. We have thus proven that, for every k-linear map $f : H \to H$, we have the equivalence

$$
\begin{aligned}
&\text{(the map } f \text{ is a derivation in the sense of Definition 29.3)} \\
&\iff \text{(the map } f \text{ is a derivation in the sense of Definition 29.4)}\,.
\end{aligned}
$$

In other words, Definition 29.3 and Definition 29.4 are equivalent. This proves Proposition 29.5. □

Before we prove anything more serious about derivations, let us show a technical lemma:

Lemma 29.6. Let k be a field. Let C be a k-bialgebra. Let A be a commutative k-algebra. Let $\alpha : C \to A$ and $\beta : C \to A$ be any k-linear maps. Let $g : C \to A$ be a k-algebra homomorphism. Let $f : C \to A$ be a k-linear map satisfying

$$f \circ \mu_C = \mu_A \circ (\alpha \otimes f + f \otimes \beta) .$$

Then:

(a) We have

$$(f * g) \circ \mu_C = \mu_A \circ ((\alpha * g) \otimes (f * g) + (f * g) \otimes (\beta * g)) .$$

(b) We have

$$(g * f) \circ \mu_C = \mu_A \circ ((g * \alpha) \otimes (g * f) + (g * f) \otimes (g * \beta)) .$$

This is a dual of Lemma 28.4, and unsurprisingly the proof will be analogous.

Proof of Lemma 29.6. By the axioms of a bialgebra, $\mu_C : C \otimes C \to C$ is a k-coalgebra homomorphism (since C is a k-bialgebra). Thus, $\Delta_C \circ \mu_C = (\mu_C \otimes \mu_C) \circ \Delta_{C \otimes C}$.

In the following, the sign $*$ will denote the convolution in $\mathcal{L}(C, A)$, but also the convolution in $\mathcal{L}(C \otimes C, A \otimes A)$ (which is well-defined since $C \otimes C$ is a k-coalgebra and $A \otimes A$ is a k-algebra).

(a) By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$, so that

$$\underbrace{(f * g)}_{= \mu_A \circ (f \otimes g) \circ \Delta_C} \circ \mu_C = \mu_A \circ (f \otimes g) \circ \underbrace{\Delta_C \circ \mu_C}_{= (\mu_C \otimes \mu_C) \circ \Delta_{C \otimes C}}$$
$$= \mu_A \circ (f \otimes g) \circ (\mu_C \otimes \mu_C) \circ \Delta_{C \otimes C} . \tag{312}$$

But applying (21) to $C \otimes C$, C, A, $C \otimes C$, C, A, μ_C, f, μ_C, g instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(f \circ \mu_C) \otimes (g \circ \mu_C) = (f \otimes g) \circ (\mu_C \otimes \mu_C) ,$$

so that

$$\begin{aligned}
&(f \otimes g) \circ (\mu_C \otimes \mu_C) \\
&= \underbrace{(f \circ \mu_C)}_{= \mu_A \circ (\alpha \otimes f + f \otimes \beta)} \otimes \underbrace{(g \circ \mu_C)}_{\substack{= \mu_A \circ (g \otimes g) \\ \text{(since } g \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} \\
&= (\mu_A \circ (\alpha \otimes f + f \otimes \beta)) \otimes (\mu_A \circ (g \otimes g)) \\
&= (\mu_A \otimes \mu_A) \circ \underbrace{((\alpha \otimes f + f \otimes \beta) \otimes (g \otimes g))}_{\substack{= \alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g \\ \text{(since the tensor product of } k\text{-linear maps} \\ \text{is distributive)}}} \\
&\quad \left(\begin{array}{c} \text{by (21) (applied to } C \otimes C, A \otimes A, A, C \otimes C, A \otimes A, A, \\ \alpha \otimes f + f \otimes \beta, \mu_A, g \otimes g, \mu_A \text{ instead of } U, V, W, U', V', W', \alpha, \beta, \alpha', \beta') \end{array} \right) \\
&= (\mu_A \otimes \mu_A) \circ (\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g) .
\end{aligned} \tag{313}$$

Now, (312) becomes

$$
\begin{aligned}
&(f * g) \circ \mu_C \\
&= \mu_A \circ \underbrace{(f \otimes g) \circ (\mu_C \otimes \mu_C)}_{\substack{=(\mu_A \otimes \mu_A) \circ (\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g) \\ \text{(by (313))}}} \circ \Delta_{C \otimes C} \\
&= \underbrace{\mu_A \circ (\mu_A \otimes \mu_A)}_{\substack{=\mu_A \circ \mu_{A \otimes A} \\ \text{(since } \mu_A : A \otimes A \to A \text{ is a } k\text{-algebra} \\ \text{homomorphism (by Lemma 23.6))}}} \circ (\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g) \circ \Delta_{C \otimes C} \\
&= \mu_A \circ \underbrace{\mu_{A \otimes A} \circ (\alpha \otimes f \otimes g \otimes g + f \otimes \beta \otimes g \otimes g)}_{\substack{=\mu_{A \otimes A} \circ (\alpha \otimes f \otimes g \otimes g) + \mu_{A \otimes A} \circ (f \otimes \beta \otimes g \otimes g) \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \circ \Delta_{C \otimes C} \\
&= \mu_A \circ \underbrace{(\mu_{A \otimes A} \circ (\alpha \otimes f \otimes g \otimes g) + \mu_{A \otimes A} \circ (f \otimes \beta \otimes g \otimes g)) \circ \Delta_{C \otimes C}}_{\substack{=\mu_{A \otimes A} \circ (\alpha \otimes f \otimes g \otimes g) \circ \Delta_{C \otimes C} + \mu_{A \otimes A} \circ (f \otimes \beta \otimes g \otimes g) \circ \Delta_{C \otimes C} \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \\
&= \mu_A \circ \left(\underbrace{\mu_{A \otimes A} \circ (\alpha \otimes f \otimes g \otimes g) \circ \Delta_{C \otimes C}}_{\substack{=(\alpha \otimes f) * (g \otimes g) \\ \text{(because the definition of convolution yields} \\ (\alpha \otimes f) * (g \otimes g) = \mu_{A \otimes A} \circ (\alpha \otimes f \otimes g \otimes g) \circ \Delta_{C \otimes C})}} + \underbrace{\mu_{A \otimes A} \circ (f \otimes \beta \otimes g \otimes g) \circ \Delta_{C \otimes C}}_{\substack{=(f \otimes \beta) * (g \otimes g) \\ \text{(because the definition of convolution yields} \\ (f \otimes \beta) * (g \otimes g) = \mu_{A \otimes A} \circ (f \otimes \beta \otimes g \otimes g) \circ \Delta_{C \otimes C})}} \right) \\
&= \mu_A \circ \left(\underbrace{(\alpha \otimes f) * (g \otimes g)}_{\substack{=(\alpha * g) \otimes (f * g) \\ \text{(by Corollary 9.9, applied to } D=C,\ B=A, \\ p=\alpha,\ q=g,\ r=f,\ s=g)}} + \underbrace{(f \otimes \beta) * (g \otimes g)}_{\substack{=(f * g) \otimes (\beta * g) \\ \text{(by Corollary 9.9, applied to } D=C,\ B=A, \\ p=f,\ q=g,\ r=\beta,\ s=g)}} \right) \\
&= \mu_A \circ ((\alpha * g) \otimes (f * g) + (f * g) \otimes (\beta * g)) .
\end{aligned}
$$

This proves Lemma 29.6 **(a)**.

(b) By the definition of convolution, $g * f = \mu_A \circ (g \otimes f) \circ \Delta_C$, so that

$$
\begin{aligned}
\underbrace{(g * f)}_{=\mu_A \circ (g \otimes f) \circ \Delta_C} \circ \mu_C &= \mu_A \circ (g \otimes f) \circ \underbrace{\Delta_C \circ \mu_C}_{=(\mu_C \otimes \mu_C) \circ \Delta_{C \otimes C}} \\
&= \mu_A \circ (g \otimes f) \circ (\mu_C \otimes \mu_C) \circ \Delta_{C \otimes C}. \qquad (314)
\end{aligned}
$$

But applying (21) to $C \otimes C$, C, A, $C \otimes C$, C, A, μ_C, g, μ_C, f instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$
(g \circ \mu_C) \otimes (f \circ \mu_C) = (g \otimes f) \circ (\mu_C \otimes \mu_C) ,
$$

so that

$$
\begin{aligned}
&(g \otimes f) \circ (\mu_C \otimes \mu_C) \\
&= \underbrace{(g \circ \mu_C)}_{\substack{= \mu_A \circ (g \otimes g) \\ \text{(since } g \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} \otimes \underbrace{(f \circ \mu_C)}_{= \mu_A \circ (\alpha \otimes f + f \otimes \beta)} \\
&= (\mu_A \circ (g \otimes g)) \otimes (\mu_A \circ (\alpha \otimes f + f \otimes \beta)) \\
&= (\mu_A \otimes \mu_A) \circ \underbrace{((g \otimes g) \otimes (\alpha \otimes f + f \otimes \beta))}_{\substack{= g \otimes g \otimes \alpha \otimes f + g \otimes g \otimes f \otimes \beta \\ \text{(since the tensor product of } k\text{-linear maps} \\ \text{is distributive)}}} \\
&\qquad \left(\begin{array}{c} \text{by (21) (applied to } C \otimes C,\ A \otimes A,\ A,\ C \otimes C,\ A \otimes A,\ A, \\ g \otimes g,\ \mu_A,\ \alpha \otimes f + f \otimes \beta,\ \mu_A \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta') \end{array} \right) \\
&= (\mu_A \otimes \mu_A) \circ (g \otimes g \otimes \alpha \otimes f + g \otimes g \otimes f \otimes \beta)\,. \qquad (315)
\end{aligned}
$$

Now, (314) becomes

$$
\begin{aligned}
&(g * f) \circ \mu_C \\
&= \mu_A \circ \underbrace{(g \otimes f) \circ (\mu_C \otimes \mu_C)}_{\substack{= (\mu_A \otimes \mu_A) \circ (g \otimes g \otimes \alpha \otimes f + g \otimes g \otimes f \otimes \beta) \\ \text{(by (315))}}} \circ \Delta_{C \otimes C} \\
&= \underbrace{\mu_A \circ (\mu_A \otimes \mu_A)}_{\substack{= \mu_A \circ \mu_{A \otimes A} \\ \text{(since } \mu_A : A \otimes A \to A \text{ is a } k\text{-algebra} \\ \text{homomorphism (by Lemma 23.6))}}} \circ (g \otimes g \otimes \alpha \otimes f + g \otimes g \otimes f \otimes \beta) \circ \Delta_{C \otimes C} \\
&= \mu_A \circ \underbrace{\mu_{A \otimes A} \circ (g \otimes g \otimes \alpha \otimes f + g \otimes g \otimes f \otimes \beta)}_{\substack{= \mu_{A \otimes A} \circ (g \otimes g \otimes \alpha \otimes f) + \mu_{A \otimes A} \circ (g \otimes g \otimes f \otimes \beta) \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \circ \Delta_{C \otimes C} \\
&= \mu_A \circ \underbrace{(\mu_{A \otimes A} \circ (g \otimes g \otimes \alpha \otimes f) + \mu_{A \otimes A} \circ (g \otimes g \otimes f \otimes \beta)) \circ \Delta_{C \otimes C}}_{\substack{= \mu_{A \otimes A} \circ (g \otimes g \otimes \alpha \otimes f) \circ \Delta_{C \otimes C} + \mu_{A \otimes A} \circ (g \otimes g \otimes f \otimes \beta) \circ \Delta_{C \otimes C} \\ \text{(since composition of } k\text{-linear maps is distributive)}}} \\
&= \mu_A \circ \left(\underbrace{\mu_{A \otimes A} \circ (g \otimes g \otimes \alpha \otimes f) \circ \Delta_{C \otimes C}}_{\substack{= (g \otimes g) * (\alpha \otimes f) \\ \text{(because the definition of convolution yields} \\ (g \otimes g) * (\alpha \otimes f) = \mu_{A \otimes A} \circ (g \otimes g \otimes \alpha \otimes f) \circ \Delta_{C \otimes C})}} + \underbrace{\mu_{A \otimes A} \circ (g \otimes g \otimes f \otimes \beta) \circ \Delta_{C \otimes C}}_{\substack{= (g \otimes g) * (f \otimes \beta) \\ \text{(because the definition of convolution yields} \\ (g \otimes g) * (f \otimes \beta) = \mu_{A \otimes A} \circ (g \otimes g \otimes f \otimes \beta) \circ \Delta_{C \otimes C})}} \right) \\
&= \mu_A \circ \left(\underbrace{(g \otimes g) * (\alpha \otimes f)}_{\substack{= (g * \alpha) \otimes (g * f) \\ \text{(by Corollary 9.9, applied to } D = C,\ B = A, \\ p = g,\ q = \alpha,\ r = g,\ s = f)}} + \underbrace{(g \otimes g) * (f \otimes \beta)}_{\substack{= (g * f) \otimes (g * \beta) \\ \text{(by Corollary 9.9, applied to } D = C,\ B = A, \\ p = g,\ q = f,\ r = g,\ s = \beta)}} \right) \\
&= \mu_A \circ ((g * \alpha) \otimes (g * f) + (g * f) \otimes (g * \beta))\,.
\end{aligned}
$$

This proves Lemma 29.6 **(b)**. □

Now, let us show the reason why we proved Lemma 29.6:

Theorem 29.7. Let k be a field. Let H be a commutative k-bialgebra. Let $P : H \to H$ and $Q : H \to H$ be two k-algebra homomorphisms satisfying $P * \mathrm{id}_H * Q = e_{H,H}$. Let $K : H \to H$ be a derivation. Then, $P * K * Q : H \to H$ is an $(\varepsilon_H, \varepsilon_H)$-derivation. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Theorem 29.7 is the dual of Theorem 28.5.

Proof of Theorem 29.7. Since K is a derivation, we have $K \circ \mu_H = \mu_H \circ (K \otimes \mathrm{id}_H + \mathrm{id}_H \otimes K)$ (because Definition 29.3 yields that K is a derivation if and only if $K \circ \mu_H = \mu_H \circ (K \otimes \mathrm{id}_H + \mathrm{id}_H \otimes K)$). Thus,

$$K \circ \mu_H = \mu_H \circ \underbrace{(K \otimes \mathrm{id}_H + \mathrm{id}_H \otimes K)}_{= \mathrm{id}_H \otimes K + K \otimes \mathrm{id}_H} = \mu_H \circ (\mathrm{id}_H \otimes K + K \otimes \mathrm{id}_H) .$$

Hence, Lemma 29.6 **(b)** (applied to $C = H$, $A = H$, $\alpha = \mathrm{id}_H$, $\beta = \mathrm{id}_H$, $f = K$ and $g = P$) yields

$$(P * K) \circ \mu_H = \mu_H \circ ((P * \mathrm{id}_H) \otimes (P * K) + (P * K) \otimes (P * \mathrm{id}_H)) .$$

Thus, Lemma 29.6 **(a)** (applied to $C = H$, $A = H$, $\alpha = P * \mathrm{id}_H$, $\beta = P * \mathrm{id}_H$, $f = P * K$ and $g = Q$) yields

$$\begin{aligned}
(P * K * Q) \circ \mu_H &= \mu_H \circ \left(\underbrace{(P * \mathrm{id}_H * Q)}_{= e_{H,H}} \otimes (P * K * Q) + (P * K * Q) \otimes \underbrace{(P * \mathrm{id}_H * Q)}_{= e_{H,H}} \right) \\
&= \mu_H \circ \underbrace{(e_{H,H} \otimes (P * K * Q) + (P * K * Q) \otimes e_{H,H})}_{= (P*K*Q) \otimes e_{H,H} + e_{H,H} \otimes (P*K*Q)} \\
&= \mu_H \circ ((P * K * Q) \otimes e_{H,H} + e_{H,H} \otimes (P * K * Q)) .
\end{aligned}$$

Thus, $P * K * Q$ is an $(\varepsilon_H, \varepsilon_H)$-derivation (because by Definition 15.6, the map $P * K * Q$ is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $(P * K * Q) \circ \mu_H = \mu_H \circ ((P * K * Q) \otimes e_{H,H} + e_{H,H} \otimes (P * K * Q))$). This proves Theorem 29.7. ☐

The analogue of Corollary 28.6 is the following fact:

Corollary 29.8. Let k be a field. Let H be a commutative k-Hopf algebra. Let S be the antipode of H. Let $K : H \to H$ be a derivation.

(a) Then, $S * K$ is an $(\varepsilon_H, \varepsilon_H)$-derivation.

(b) Then, $K * S$ is an $(\varepsilon_H, \varepsilon_H)$-derivation.

Proof of Corollary 29.8. By Definition 26.3, we have $H^{\mathrm{op}} = (H, \mu_H \circ \tau_{H,H}, \eta_H)$. Since H is commutative, we have $\mu_H \circ \tau_{H,H} = \mu_H$. Thus, $H^{\mathrm{op}} = \left(H, \underbrace{\mu_H \circ \tau_{H,H}}_{= \mu_H}, \eta_H \right) = (H, \mu_H, \eta_H) = H$.

Proposition 26.4 yields that the antipode of H is a k-algebra homomorphism from H to H^{op}. Since the antipode of H is the map S, whereas H^{op} is H, this rewrites as follows: The map S is a k-algebra homomorphism from H to H.

Corollary 15.16 (applied to $n = 0$, $A = H$ and $f = \mathrm{id}_H$) yields that id_H^{*0} is a k-algebra homomorphism. Since $\mathrm{id}_H^{*0} = e_{H,H}$, this shows that $e_{H,H}$ is a k-algebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).

The antipode of a Hopf algebra is defined as the $*$-inverse of its identity map. Thus, the antipode of H is the map $\mathrm{id}_H^{*(-1)}$. Since the antipode of H is S, this yields that S is the map $\mathrm{id}_H^{*(-1)}$. In other words, $S = \mathrm{id}_H^{*(-1)}$. Hence, $S * \mathrm{id}_H * e_{H,H} = \underbrace{\mathrm{id}_H^{*(-1)} * \mathrm{id}_H}_{=e_{H,H}} * e_{H,H} = e_{H,H}$. Thus, Theorem 29.7 (applied to $P = S$ and $Q = e_{H,H}$) yields that $S * K * e_{H,H}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation. In other words, $S * K$ is an $(\varepsilon_H, \varepsilon_H)$-derivation (since $S * K * e_{H,H} = S * K$). This proves Corollary 29.8 **(a)**.

Since $S = \mathrm{id}_H^{*(-1)}$, we have $e_{H,H} * \mathrm{id}_H * S = e_{H,H} * \underbrace{\mathrm{id}_H * \mathrm{id}_H^{*(-1)}}_{=e_{H,H}} = e_{H,H}$. Thus, Theorem 29.7 (applied to $P = e_{H,H}$ and $Q = S$) yields that $e_{H,H} * K * S$ is an $(\varepsilon_H, \varepsilon_H)$-derivation. In other words, $K * S$ is an $(\varepsilon_H, \varepsilon_H)$-derivation (since $e_{H,H} * K * S = K * S$). This proves Corollary 29.8 **(b)**. □

Next, the dual of Proposition 28.7:

Proposition 29.9. Let k be a field. Let H be a k-bialgebra. Let $P : H \to H$, $Q : H \to H$ and $K : H \to H$ be three k-linear maps such that $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$ and $\varepsilon_H \circ K = 0$. Then, every $x \in H$ satisfies $(P * K * Q)(x) - K(x) \in (\mathrm{Ker}(\varepsilon_H))^2$. [148]

In order to prove this, we invoke a simple fact:

Lemma 29.10. Let k be a field. Let C be a k-coalgebra. Let A be a k-algebra. Let $f : C \to A$ and $g : C \to A$ be two k-linear maps. Then, $(f * g)(C) \subseteq f(C) \cdot g(C)$.

Proof of Lemma 29.10. By the definition of convolution, $f * g = \mu_A \circ (f \otimes g) \circ \Delta_C$. Thus,

$$(f * g)(C) = (\mu_A \circ (f \otimes g) \circ \Delta_C)(C) = (\mu_A \circ (f \otimes g)) \underbrace{(\Delta_C(C))}_{\subseteq C \otimes C} \subseteq (\mu_A \circ (f \otimes g))(C \otimes C)$$

$$= \mu_A \underbrace{((f \otimes g)(C \otimes C))}_{\substack{=f(C)\otimes g(C) \\ \text{(where we consider } f(C)\otimes g(C) \text{ as a} \\ \text{vector subspace of } A\otimes A \text{ by tensoring the} \\ \text{inclusion maps } f(C)\to A \text{ and } g(C)\to A)}} = \mu_A(f(C) \otimes g(C)) = f(C) \cdot g(C)$$

(by (74), applied to $U = f(C)$ and $V = g(C)$). This proves Lemma 29.10. □

Proof of Proposition 29.9. Let $x \in H$. Define $e_{H,H}$ according to Definition 1.12.

[148] Recall that the notation $(\mathrm{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\mathrm{Ker}(\varepsilon_H))^2$ means the subspace $(\mathrm{Ker}(\varepsilon_H)) \cdot (\mathrm{Ker}(\varepsilon_H))$ of H.

Notice that

$$(P - e_{H,H})(H) \subseteq \operatorname{Ker}(\varepsilon_H) \tag{316}$$

[149] and similarly

$$(Q - e_{H,H})(H) \subseteq \operatorname{Ker}(\varepsilon_H) \tag{317}$$

Also,

$$K(H) \subseteq \operatorname{Ker}(\varepsilon_H) \tag{318}$$

(because every $x \in H$ satisfies $K(x) \in \operatorname{Ker}(\varepsilon_H)$ (since $\varepsilon_H(K(x)) = \underbrace{(\varepsilon_H \circ K)}_{=0}(x) = 0(x) = 0$)).

Since H is a k-bialgebra, the map ε_H is a k-algebra homomorphism (by the axioms of a bialgebra), so that $\operatorname{Ker}(\varepsilon_H)$ is an ideal of H. Thus, $\operatorname{Ker}(\varepsilon_H) \cdot H \subseteq \operatorname{Ker}(\varepsilon_H)$ and $H \cdot \operatorname{Ker}(\varepsilon_H) \subseteq \operatorname{Ker}(\varepsilon_H)$.

Applying Lemma 29.10 to $C = H$, $A = H$, $f = P - e_{H,H}$ and $g = K * Q$, we obtain

$$\begin{aligned}
((P - e_{H,H}) * K * Q)(H) &\subseteq \underbrace{(P - e_{H,H})(H)}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_H) \\ \text{(by (316))}}} \cdot \underbrace{(K * Q)(H)}_{\substack{\subseteq K(H) \cdot Q(H) \\ \text{(by Lemma 29.10, applied to} \\ C=H,\ A=H,\ f=K \text{ and } g=Q)}} \\
&\subseteq \operatorname{Ker}(\varepsilon_H) \cdot \underbrace{K(H)}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_H) \\ \text{(by (318))}}} \cdot \underbrace{Q(H)}_{\subseteq H} \\
&\subseteq \operatorname{Ker}(\varepsilon_H) \cdot \underbrace{\operatorname{Ker}(\varepsilon_H) \cdot H}_{\subseteq \operatorname{Ker}(\varepsilon_H)} \subseteq \operatorname{Ker}(\varepsilon_H) \cdot \operatorname{Ker}(\varepsilon_H) \\
&= (\operatorname{Ker}(\varepsilon_H))^2 .
\end{aligned} \tag{319}$$

Applying Lemma 29.10 to $C = H$, $A = H$, $f = K$ and $g = Q - e_{H,H}$, we obtain

$$\begin{aligned}
(K * (Q - e_{H,H}))(H) &\subseteq \underbrace{K(H)}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_H) \\ \text{(by (318))}}} \cdot \underbrace{(Q - e_{H,H})(H)}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_H) \\ \text{(by (317))}}} \\
&\subseteq \operatorname{Ker}(\varepsilon_H) \cdot \operatorname{Ker}(\varepsilon_H) = (\operatorname{Ker}(\varepsilon_H))^2 .
\end{aligned} \tag{320}$$

[149] *Proof of (316):* Let $x \in H$. Then, $e_{H,H} = \eta_H \circ \varepsilon_H$ (by the definition of $e_{H,H}$), so that $e_{H,H}(x) = (\eta_H \circ \varepsilon_H)(x) = \eta_H(\varepsilon_H(x)) = \varepsilon_H(x) \cdot 1_H$ (by the definition of η_H). Thus,

$$\varepsilon_H(e_{H,H}(x)) = \varepsilon_H(\varepsilon_H(x) \cdot 1_H) = \varepsilon_H(x) \cdot \underbrace{\varepsilon_H(1_H)}_{\substack{=1 \\ \text{(by the axioms of} \\ \text{a bialgebra, since } H \\ \text{is a } k\text{-bialgebra)}}} \qquad \text{(since } \varepsilon_H \text{ is } k\text{-linear)}$$

$$= \varepsilon_H(x).$$

On the other hand, $\varepsilon_H(P(x)) = \underbrace{(\varepsilon_H \circ P)}_{=\varepsilon_H}(x) = \varepsilon_H(x)$. Now,

$$\varepsilon_H(\underbrace{(P - e_{H,H})(x)}_{=P(x)-e_{H,H}(x)}) = \varepsilon_H(P(x) - e_{H,H}(x)) = \underbrace{\varepsilon_H(P(x))}_{=\varepsilon_H(x)} - \underbrace{\varepsilon_H(e_{H,H}(x))}_{=\varepsilon_H(x)} = \varepsilon_H(x) - \varepsilon_H(x) = 0,$$

so that $(P - e_{H,H})(x) \in \operatorname{Ker}(\varepsilon_H)$.

Now, forget that we fixed x. We thus have proven that every $x \in H$ satisfies $(P - e_{H,H})(x) \in \operatorname{Ker}(\varepsilon_H)$. In other words, $(P - e_{H,H})(H) \subseteq \operatorname{Ker}(\varepsilon_H)$. This proves (316).

Since

$$\begin{aligned}
&\underbrace{(P - e_{H,H}) * K * Q}_{=P*K*Q-e_{H,H}*K*Q} + \underbrace{K * (Q - e_{H,H})}_{=K*Q-K*e_{H,H}} \\
&= P * K * Q - \underbrace{e_{H,H} * K * Q}_{=K*Q} + K * Q - \underbrace{K * e_{H,H}}_{=K} \\
&= P * K * Q - K * Q + K * Q - K = P * K * Q - K, \qquad (321)
\end{aligned}$$

we have

$$\begin{aligned}
&(P * K * Q)(x) - K(x) \\
&= \underbrace{(P * K * Q - K)}_{=\left(P-e_{H,H}\right)*K*Q+K*\left(Q-e_{H,H}\right)}(x) = ((P - e_{H,H}) * K * Q + K * (Q - e_{H,H}))(x) \\
&= ((P - e_{H,H}) * K * Q)\left(\underbrace{x}_{\in H}\right) + (K * (Q - e_{H,H}))\left(\underbrace{x}_{\in H}\right) \\
&\in \underbrace{((P - e_{H,H}) * K * Q)(H)}_{\substack{\subseteq (\operatorname{Ker}(\varepsilon_H))^2 \\ \text{(by (319))}}} + \underbrace{(K * (Q - e_{H,H}))(H)}_{\substack{\subseteq (\operatorname{Ker}(\varepsilon_H))^2 \\ \text{(by (320))}}} \\
&\subseteq (\operatorname{Ker}(\varepsilon_H))^2 + (\operatorname{Ker}(\varepsilon_H))^2 \subseteq (\operatorname{Ker}(\varepsilon_H))^2 \qquad \left(\text{since } (\operatorname{Ker}(\varepsilon_H))^2 \text{ is a } k\text{-vector space}\right).
\end{aligned}$$

This proves Proposition 29.9. □

Now, let us study a particular derivation that any graded algebra has: the Euler operator. We state the dual of Proposition 28.8:

Proposition 29.11. Let k be a field. Let H be a graded k-algebra. Let E_H be defined according to Definition 27.1. Then, $E_H : H \to H$ is a derivation.

Proof of Proposition 29.11. Since H is a graded k-algebra, the map $\mu_H : H \otimes H \to H$ is graded. Thus, Proposition 27.4 (applied to $V = H \otimes H$, $W = H$ and $f = \mu_H$) yields $\mu_H \circ E_{H\otimes H} = E_H \circ \mu_H$, so that

$$E_H \circ \mu_H = \mu_H \circ \underbrace{E_{H\otimes H}}_{\substack{=E_H\otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H \\ \text{(by Proposition 27.3, applied to } V=H \text{ and } W=H)}} = \mu_H \circ (E_H \otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H).$$

Thus, E_H is a derivation (because Definition 29.3 yields that E_H is a derivation if and only if $E_H \circ \mu_H = \mu_H \circ (E_H \otimes \mathrm{id}_H + \mathrm{id}_H \otimes E_H)$). Proposition 29.11 is proven. □

Now, let us come as close as possible to Theorem 29.1 without requiring k to be of characteristic 0:

Theorem 29.12. Let k be a field. Let H be a commutative graded k-bialgebra. Let E_H be defined according to Definition 27.1.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-algebra homomorphisms satisfying $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

(a) Then, $(P * E_H * Q)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) = 0$. [150]

(b) Besides, every $x \in H$ satisfies $(P * E_H * Q)(x) - E_H(x) \in (\operatorname{Ker}(\varepsilon_H))^2$.

(c) We have $(P * E_H * Q) \circ (P * E_H * Q) = E_H \circ (P * E_H * Q) = (P * E_H * Q) \circ E_H$.

This Theorem 29.12, of course, is the dual of Theorem 28.9, although not precisely (part **(b)** of Theorem 29.12 is slightly stronger than the dual of part **(b)** of Theorem 28.9, but the difference is negligible).

Proof of Theorem 29.12. Since H is a k-bialgebra, the map $\varepsilon_H : H \to k$ is a k-algebra homomorphism (by the axioms of a bialgebra).

By Proposition 29.11, the map E_H is a derivation. Thus, Theorem 29.7 (applied to $K = E_H$) yields that $P * E_H * Q : H \to H$ is an $(\varepsilon_H, \varepsilon_H)$-derivation. Thus,

$$(P * E_H * Q)\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0 \tag{322}$$

(because Theorem 15.9 (applied to $A = H$ and $f = P * E_H * Q$) yields that $P * E_H * Q$ is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $(P * E_H * Q)\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$). Thus,

$$(P * E_H * Q) \underbrace{\left((\operatorname{Ker}(\varepsilon_H))^2\right)}_{\subseteq (\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H} \subseteq (P * E_H * Q)\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$$

(by (322)), so that

$$(P * E_H * Q)\left((\operatorname{Ker}(\varepsilon_H))^2\right) = 0. \tag{323}$$

On the other hand, just as in the proof of Theorem 28.9, we can prove that (296) holds. In other words,

$$(P * E_H * Q)(H_0) = 0. \tag{324}$$

Now, since $P * E_H * Q$ is k-linear, we have

$$\begin{aligned}(P * E_H * Q)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) &= \underbrace{(P * E_H * Q)(H_0)}_{\substack{=0 \\ \text{(by (324))}}} + \underbrace{(P * E_H * Q)\left((\operatorname{Ker}(\varepsilon_H))^2\right)}_{\substack{=0 \\ \text{(by (323))}}} \\ &= 0 + 0 = 0.\end{aligned}$$

This proves Theorem 29.12 **(a)**.

Recall that the grading on the k-vector space k satisfies $k_0 = k$. Thus, $E_k = 0$ [151]. Since ε_H is a graded map (because H is a graded k-coalgebra), we have $\varepsilon_H \circ E_H = E_k \circ \varepsilon_H$ (by Proposition 27.4, applied to $V = H$, $W = k$ and $f = \varepsilon_H$). Thus, $\varepsilon_H \circ E_H = \underbrace{E_k}_{=0} \circ \varepsilon_H = 0 \circ \varepsilon_H = 0$. Combined with the fact that the map E_H is graded (by Proposition 27.2 **(b)**, applied to $V = H$), this shows that we can apply

[150] Recall that the notation $(\operatorname{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

[151] *Proof.* Every $v \in k$ satisfies $E_k(v) = 0$ (since $v \in k = k_0$, and thus Proposition 27.2 **(a)** (applied to $V = k$ and $n = 0$) yields $E_k(v) = 0v = 0$). Thus, $E_k = 0$, qed.

Proposition 29.9 to $K = E_H$. As a result, we conclude that every $x \in H$ satisfies $(P * E_H * Q)(x) - E_H(x) \in (\operatorname{Ker}(\varepsilon_H))^2$. This proves Theorem 29.12 **(b)**.

(c) Let $x \in H$. Then, Theorem 29.12 **(b)** yields

$$(P * E_H * Q)(x) - E_H(x) \in (\operatorname{Ker}(\varepsilon_H))^2 \subseteq H_0 + (\operatorname{Ker}(\varepsilon_H))^2,$$

so that

$$(P * E_H * Q)((P * E_H * Q)(x) - E_H(x)) \in (P * E_H * Q)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) = 0$$

(by Theorem 29.12 **(a)**), thus $(P * E_H * Q)((P * E_H * Q)(x) - E_H(x)) = 0$. Thus,

$$\begin{aligned}
0 &= (P * E_H * Q)((P * E_H * Q)(x) - E_H(x)) \\
&= \underbrace{(P * E_H * Q)((P * E_H * Q)(x))}_{=((P*E_H*Q)\circ(P*E_H*Q))(x)} - \underbrace{(P * E_H * Q)(E_H(x))}_{=((P*E_H*Q)\circ E_H)(x)} \qquad \text{(since } P * E_H * Q \text{ is } k\text{-linear)} \\
&= ((P * E_H * Q) \circ (P * E_H * Q))(x) - ((P * E_H * Q) \circ E_H)(x),
\end{aligned}$$

so that $((P * E_H * Q) \circ (P * E_H * Q))(x) = ((P * E_H * Q) \circ E_H)(x)$.

Now forget that we fixed x. We thus have proven that every $x \in H$ satisfies $((P * E_H * Q) \circ (P * E_H * Q))(x) = ((P * E_H * Q) \circ E_H)(x)$. In other words,

$$(P * E_H * Q) \circ (P * E_H * Q) = (P * E_H * Q) \circ E_H. \tag{325}$$

Since E_H is graded (by Proposition 27.2 **(b)**, applied to $V = H$) and Q is graded, we conclude (by Proposition 16.18 **(a)**, applied to $C = H$, $A = H$, $f = E_H$ and $g = Q$) that $E_H * Q$ is graded.

Since P is graded and $E_H * Q$ is graded, we conclude (by Proposition 16.18 **(a)**, applied to $C = H$, $A = H$, $f = P$ and $g = E_H * Q$) that $P * E_H * Q$ is graded. Thus, $(P * E_H * Q) \circ E_H = E_H \circ (P * E_H * Q)$ (by Proposition 27.4, applied to $V = H$, $W = H$ and $f = P * E_H * Q$). Combined with (325), this yields

$$(P * E_H * Q) \circ (P * E_H * Q) = E_H \circ (P * E_H * Q) = (P * E_H * Q) \circ E_H.$$

This proves Theorem 29.12 **(c)**. □

The dual of Corollary 28.10 (not the exact dual, though, but an almost equivalent statement) takes the following form:

Corollary 29.13. Let k be a field. Let H be a commutative graded k-Hopf algebra. Let S be the antipode of H. Let E_H be defined according to Definition 27.1.

(a) Then, $(E_H * S)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) = 0$. [152]

(b) Every $x \in H$ satisfies $(E_H * S)(x) - E_H(x) \in (\operatorname{Ker}(\varepsilon_H))^2$.

(c) We have $(E_H * S) \circ (E_H * S) = E_H \circ (E_H * S) = (E_H * S) \circ E_H$.

(d) Also, $(S * E_H)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) = 0$.

(e) Every $x \in H$ satisfies $(S * E_H)(x) - E_H(x) \in (\operatorname{Ker}(\varepsilon_H))^2$.

(f) We have $(S * E_H) \circ (S * E_H) = E_H \circ (S * E_H) = (S * E_H) \circ E_H$.

[152] Recall that the notation $(\operatorname{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

Proof of Corollary 29.13. Just as in the proof of Corollary 29.8, we can prove the following facts:

- The map S is a k-algebra homomorphism from H to H.
- The map $e_{H,H}$ is a k-algebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).
- We have $S = \mathrm{id}_H^{*(-1)}$.
- We have $S * \mathrm{id}_H * e_{H,H} = e_{H,H}$ and $e_{H,H} * \mathrm{id}_H * S = e_{H,H}$.

Notice that $e_{H,H} = \eta_H \circ \varepsilon_H$ (by the definition of $e_{H,H}$) and $\varepsilon_H \circ \eta_H = \mathrm{id}_k$ (by the axioms of a bialgebra, since H is a k-bialgebra), so that $\varepsilon_H \circ \underbrace{e_{H,H}}_{=\varepsilon_H \circ \eta_H} = \underbrace{\varepsilon_H \circ \eta_H}_{=\mathrm{id}_k} \circ \varepsilon_H = \varepsilon_H$. Also, Theorem 28.17 **(a)** yields $\varepsilon_H \circ S = \varepsilon_H$.

Also, the map $e_{H,H}$ is graded (by Proposition 16.18 **(b)**, applied to $C = H$ and $A = H$), and the map S is graded (since S is the antipode of H, while H is a graded k-Hopf algebra).

Thus, we can apply Theorem 29.12 to $P = e_{H,H}$ and $Q = S$.

Applying Theorem 29.12 **(a)** to $P = e_{H,H}$ and $Q = S$, we obtain $(e_{H,H} * E_H * S)\left(H_0 + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as $(E_H * S)\left(H_0 + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. This proves Corollary 29.13 **(a)**.

Applying Theorem 29.12 **(b)** to $P = e_{H,H}$ and $Q = S$, we conclude that every $x \in H$ satisfies $(e_{H,H} * E_H * S)(x) - E_H(x) \in (\mathrm{Ker}\,(\varepsilon_H))^2$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as follows: Every $x \in H$ satisfies $(E_H * S)(x) - E_H(x) \in (\mathrm{Ker}\,(\varepsilon_H))^2$. This proves Corollary 29.13 **(b)**.

Applying Theorem 29.12 **(c)** to $P = e_{H,H}$ and $Q = S$, we obtain $(e_{H,H} * E_H * S) \circ (e_{H,H} * E_H * S) = E_H \circ (e_{H,H} * E_H * S) = (e_{H,H} * E_H * S) \circ E_H$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as $(E_H * S) \circ (E_H * S) = E_H \circ (E_H * S) = (E_H * S) \circ E_H$. This proves Corollary 29.13 **(c)**.

But we can also apply Theorem 29.12 to $P = S$ and $Q = e_{H,H}$.

Applying Theorem 29.12 **(a)** to $P = S$ and $Q = e_{H,H}$, we obtain $(S * E_H * e_{H,H})\left(H_0 + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as $(S * E_H)\left(H_0 + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. This proves Corollary 29.13 **(d)**.

Applying Theorem 29.12 **(b)** to $P = S$ and $Q = e_{H,H}$, we conclude that every $x \in H$ satisfies $(S * E_H * e_{H,H})(x) - E_H(x) \in (\mathrm{Ker}\,(\varepsilon_H))^2$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as follows: Every $x \in H$ satisfies $(S * E_H)(x) - E_H(x) \in (\mathrm{Ker}\,(\varepsilon_H))^2$. This proves Corollary 29.13 **(e)**.

Applying Theorem 29.12 **(c)** to $P = S$ and $Q = e_{H,H}$, we obtain $(S * E_H * e_{H,H}) \circ (S * E_H * e_{H,H}) = E_H \circ (S * E_H * e_{H,H}) = (S * E_H * e_{H,H}) \circ E_H$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as $(S * E_H) \circ (S * E_H) = E_H \circ (S * E_H) = (S * E_H) \circ E_H$. This proves Corollary 29.13 **(f)**. □

In order to specialize the above results to connected graded Hopf algebras, we first observe a simple fact:

Proposition 29.14. Let k be a field. Let H be a connected graded k-bialgebra. Then, $H_0 = k \cdot 1_H$.

Proof of Proposition 29.14. By the definition of $H_{\leq 0}$, we have $H_{\leq 0} = \bigoplus_{\ell=0}^{0} H_\ell = H_0$. But since H is connected, we have $H_{\leq 0} = k \cdot 1_H$ (because Remark 2.12 yields that H is connected if and only if $H_{\leq 0} = k \cdot 1_H$), so that $H_0 = H_{\leq 0} = k \cdot 1_H$. This proves Proposition 29.14. $\square$

Here comes an equivalent version of part **(a)** of Theorem 29.12:

Corollary 29.15. Let k be a field. Let H be a commutative graded k-bialgebra. Let E_H be defined according to Definition 27.1.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-algebra homomorphisms satisfying $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Then, $(P * E_H * Q)\left(k \cdot 1_H + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. [153]

Proof of Corollary 29.15. Since $1_H \in H_0$ (because H is a graded k-algebra), we have $k \cdot 1_H \subseteq kH_0 \subseteq H_0$ (since H_0 is a k-vector space). Thus,

$$(P * E_H * Q)\left(\underbrace{k \cdot 1_H}_{\subseteq H_0} + (\mathrm{Ker}\,(\varepsilon_H))^2\right) \subseteq (P * E_H * Q)\left(H_0 + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$$

(by Theorem 29.12 **(a)**). Thus, $(P * E_H * Q)\left(k \cdot 1_H + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. This proves Corollary 29.15. $\square$

Now, let us do the same to parts **(a)** and **(d)** of Corollary 29.13:

Corollary 29.16. Let k be a field. Let H be a commutative graded k-Hopf algebra. Let S be the antipode of H. Let E_H be defined according to Definition 27.1.

(a) Then, $(E_H * S)\left(k \cdot 1_H + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. [154]

(b) Also, $(S * E_H)\left(k \cdot 1_H + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$.

Proof of Corollary 29.16. Since $1_H \in H_0$ (because H is a graded k-algebra), we have $k \cdot 1_H \subseteq kH_0 \subseteq H_0$ (since H_0 is a k-vector space).

(a) We have

$$(E_H * S)\left(\underbrace{k \cdot 1_H}_{\subseteq H_0} + (\mathrm{Ker}\,(\varepsilon_H))^2\right) \subseteq (E_H * S)\left(H_0 + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$$

(by Corollary 29.13 **(a)**), so that $(E_H * S)\left(k \cdot 1_H + (\mathrm{Ker}\,(\varepsilon_H))^2\right) = 0$. Corollary 29.16 **(a)** is proven.

[153] Recall that the notation $(\mathrm{Ker}\,(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\mathrm{Ker}\,(\varepsilon_H))^2$ means the subspace $(\mathrm{Ker}\,(\varepsilon_H)) \cdot (\mathrm{Ker}\,(\varepsilon_H))$ of H.

[154] Recall that the notation $(\mathrm{Ker}\,(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\mathrm{Ker}\,(\varepsilon_H))^2$ means the subspace $(\mathrm{Ker}\,(\varepsilon_H)) \cdot (\mathrm{Ker}\,(\varepsilon_H))$ of H.

(b) We have

$$(S * E_H)\left(\underbrace{k \cdot 1_H}_{\subseteq H_0} + (\operatorname{Ker}(\varepsilon_H))^2\right) \subseteq (S * E_H)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) = 0$$

(by Corollary 29.13 **(d)**), so that $(S * E_H)\left(k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2\right) = 0$. Corollary 29.16 **(b)** is proven. □

We now come to the case of fields of characteristic 0. The following generalizes Theorem 29.1 and is a dual of Theorem 28.14:

Theorem 29.17. Let k be a field of characteristic 0. Let H be a commutative graded k-bialgebra. Let E_H be defined according to Definition 27.1.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-algebra homomorphisms satisfying $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Then, the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right) = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$. [155]

Proof of Theorem 29.17. Let M denote the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$. Then,

$$\underbrace{M}_{=E_H^{\mathrm{inv}} \circ (P * E_H * Q)}\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) = \left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right)$$

$$= E_H^{\mathrm{inv}}\left(\underbrace{(P * E_H * Q)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right)}_{\substack{=0 \\ \text{(by Theorem 29.12 (a))}}}\right)$$

$$= E_H^{\mathrm{inv}}(0) = 0 \tag{326}$$

(since the map E_H^{inv} is k-linear), so that

$$H_0 + (\operatorname{Ker}(\varepsilon_H))^2 \subseteq \operatorname{Ker} M. \tag{327}$$

Since E_H is graded (by Proposition 27.2 **(b)**, applied to $V = H$) and Q is graded, we conclude (by Proposition 16.18 **(a)**, applied to $C = H$, $A = H$, $f = E_H$ and $g = Q$) that $E_H * Q$ is graded.

Since P is graded and $E_H * Q$ is graded, we conclude (by Proposition 16.18 **(a)**, applied to $C = H$, $A = H$, $f = P$ and $g = E_H * Q$) that $P * E_H * Q$ is graded. Thus,

$$(P * E_H * Q) \circ E_H = E_H \circ (P * E_H * Q) \tag{328}$$

(by Proposition 27.4, applied to $V = H$, $W = H$ and $f = P * E_H * Q$).

[155] Recall that the notation $(\operatorname{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

Since the map E_H^{inv} is graded[156] and the map $P * E_H * Q$ is graded, the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is graded as well (because the composition of two graded maps must always be graded). Since $E_H^{\mathrm{inv}} \circ (P * E_H * Q) = M$, we have thus shown that the map M is graded. Since the maps M and id_H are graded, the map $M - \mathrm{id}_H$ must also be graded (because the difference of two graded maps must always be graded).

We are now going to prove that

$$(M - \mathrm{id}_H)(H_m) \subseteq H_0 + (\mathrm{Ker}(\varepsilon_H))^2 \qquad \text{for every } m \in \mathbb{N}. \tag{329}$$

Proof of (329): Let $m \in \mathbb{N}$. Then, we must be in one of the following cases:
Case 1: We have $m = 0$.
Case 2: We have $m > 0$.
First, let us consider Case 1. In this case, $m = 0$. Thus,

$$\begin{aligned}(M - \mathrm{id}_H)(H_m) &= (M - \mathrm{id}_H)(H_0) \subseteq H_0 \qquad (\text{since } M - \mathrm{id}_H \text{ is graded}) \\ &\subseteq H_0 + (\mathrm{Ker}(\varepsilon_H))^2.\end{aligned}$$

Hence, (329) is proven in Case 1.

Now, let us consider Case 2. In this case, $m > 0$, so that $\dfrac{1}{m}$ is well-defined in k (since k has characteristic 0). Also, since $m > 0$, we have $m \geq 1$, and thus H_m is an addend in the direct sum $\bigoplus_{n \geq 1} H_n$. Thus, $H_m \subseteq \bigoplus_{n \geq 1} H_n$.

Let $x \in H_m$. Then, $E_H(x) = mx$ (by Proposition 27.2 **(a)**, applied to $V = H$, $n = m$ and $v = x$). On the other hand, $(P * E_H * Q)(H_m) \subseteq H_m$ (since $P * E_H * Q$ is graded). Since $x \in H_m$, we have

$$(P * E_H * Q)(x) \in (P * E_H * Q)(H_m) \subseteq H_m \subseteq \bigoplus_{n \geq 1} H_n.$$

Thus, Corollary 27.12 **(b)** (applied to $V = H$ and $v = (P * E_H * Q)(x)$) yields

$$\left(E_H^{\mathrm{inv}} \circ E_H\right)((P * E_H * Q)(x)) = (P * E_H * Q)(x). \tag{330}$$

But since

$$\begin{aligned}(M - \mathrm{id}_H) \circ E_H &= \underbrace{M}_{= E_H^{\mathrm{inv}} \circ (P * E_H * Q)} \circ E_H - \underbrace{\mathrm{id}_H \circ E_H}_{= E_H} = E_H^{\mathrm{inv}} \circ \underbrace{(P * E_H * Q) \circ E_H}_{\substack{= E_H \circ (P * E_H * Q) \\ (\text{by (328)})}} - E_H \\ &= E_H^{\mathrm{inv}} \circ E_H \circ (P * E_H * Q) - E_H,\end{aligned}$$

we have

$$\begin{aligned}((M - \mathrm{id}_H) \circ E_H)(x) &= \left(E_H^{\mathrm{inv}} \circ E_H \circ (P * E_H * Q) - E_H\right)(x) \\ &= \underbrace{\left(E_H^{\mathrm{inv}} \circ E_H \circ (P * E_H * Q)\right)(x)}_{\substack{= \left(E_H^{\mathrm{inv}} \circ E_H\right)((P * E_H * Q)(x)) = (P * E_H * Q)(x) \\ (\text{by (330)})}} - E_H(x) \\ &= (P * E_H * Q)(x) - E_H(x) \in (\mathrm{Ker}(\varepsilon_H))^2\end{aligned}$$

[156] *Proof.* Define $(b_\ell)_{\ell \in \mathbb{N}}$ as in Definition 27.9. By Remark 27.10 (applied to $V = H$), we have $E_H^{\mathrm{inv}} = E_H^{(b_\ell)_{\ell \in \mathbb{N}}}$. Since the map $E_H^{(b_\ell)_{\ell \in \mathbb{N}}}$ is graded (by Proposition 27.7 **(b)**, applied to $(a_\ell)_{\ell \in \mathbb{N}} = (b_\ell)_{\ell \in \mathbb{N}}$), this yields that the map E_H^{inv} is graded, qed.

(by Theorem 29.12 **(b)**). Since

$$((M-\mathrm{id}_H)\circ E_H)(x) = (M-\mathrm{id}_H)\underbrace{(E_H(x))}_{=mx} = (M-\mathrm{id}_H)(mx) = m(M-\mathrm{id}_H)(x)$$

(since $M-\mathrm{id}_H$ is k-linear), this rewrites as $m(M-\mathrm{id}_H)(x) \in (\mathrm{Ker}(\varepsilon_H))^2$. Hence, $(M-\mathrm{id}_H)(x) \in \frac{1}{m}(\mathrm{Ker}(\varepsilon_H))^2 \subseteq (\mathrm{Ker}(\varepsilon_H))^2$ (since $(\mathrm{Ker}(\varepsilon_H))^2$ is a k-vector space).

Now, forget that we fixed x. We thus have proven that every $x \in H_m$ satisfies $(M-\mathrm{id}_H)(x) \in (\mathrm{Ker}(\varepsilon_H))^2$. In other words, $(M-\mathrm{id}_H)(H_m) \subseteq (\mathrm{Ker}(\varepsilon_H))^2$. Thus,

$$(M-\mathrm{id}_H)(H_m) \subseteq (\mathrm{Ker}(\varepsilon_H))^2 \subseteq H_0 + (\mathrm{Ker}(\varepsilon_H))^2.$$

Hence, (329) is proven in Case 2.

We have thus proven (329) in each of the two cases 1 and 2. Since these two cases cover all possibilities, this yields that (329) always holds.

Now, since H is graded, we have $H = \bigoplus_{m\in\mathbb{N}} H_m = \sum_{m\in\mathbb{N}} H_m$ (since direct sums are sums). Thus,

$$\begin{aligned}(M-\mathrm{id}_H)(H) &= (M-\mathrm{id}_H)\left(\sum_{m\in\mathbb{N}} H_m\right) = \sum_{m\in\mathbb{N}} \underbrace{(M-\mathrm{id}_H)(H_m)}_{\substack{\subseteq H_0+(\mathrm{Ker}(\varepsilon_H))^2 \\ \text{(by (329))}}} \\ &\qquad \text{(since } M-\mathrm{id}_H \text{ is } k\text{-linear)} \\ &\subseteq \sum_{m\in\mathbb{N}} \left(H_0 + (\mathrm{Ker}(\varepsilon_H))^2\right) \subseteq H_0 + (\mathrm{Ker}(\varepsilon_H))^2 \qquad (331)\end{aligned}$$

(since $H_0 + (\mathrm{Ker}(\varepsilon_H))^2$ is a k-vector space). Thus,

$$\begin{aligned}\left(M\circ M - \underbrace{M}_{=M\circ\mathrm{id}_H}\right)(H) &= \underbrace{(M\circ M - M\circ\mathrm{id}_H)}_{\substack{=M\circ(M-\mathrm{id}_H) \\ \text{(since composition of } k\text{-linear maps} \\ \text{is distributive)}}}(H) \\ &= (M\circ(M-\mathrm{id}_H))(H) = M\left(\underbrace{(M-\mathrm{id}_H)(H)}_{\substack{\subseteq H_0+(\mathrm{Ker}(\varepsilon_H))^2 \\ \text{(by (331))}}}\right) \\ &\subseteq M\left(H_0 + (\mathrm{Ker}(\varepsilon_H))^2\right) = 0 \qquad \text{(by (326))},\end{aligned}$$

so that $(M\circ M - M)(H) = 0$. Thus, $M\circ M - M = 0$, so that $M\circ M = M$. In other words, M is a projection.

We will now prove that $\mathrm{Ker}\, M = H_0 + (\mathrm{Ker}(\varepsilon_H))^2$.

In fact, let $x \in \mathrm{Ker}\, M$ be arbitrary. Then, $M(x) = 0$, so that $(M-\mathrm{id}_H)(x) = \underbrace{M(x)}_{=0} - \underbrace{\mathrm{id}_H(x)}_{=x} = -x$. Thus,

$$-x = (M-\mathrm{id}_H)\left(\underbrace{x}_{\in H}\right) \in (M-\mathrm{id}_H)(H) \subseteq H_0 + (\mathrm{Ker}(\varepsilon_H))^2$$

(by (331)). Consequently, $x \in -\left(H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2\right) \subseteq H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$ (since $H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$ is a k-vector space).

Now forget that we fixed x. We have thus proven that every $x \in \operatorname{Ker} M$ satisfies $x \in H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. In other words, $\operatorname{Ker} M \subseteq H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. Combined with (327), this yields $\operatorname{Ker} M = H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$.

So we know that the map M is a projection such that $\operatorname{Ker} M = H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. Since $M = E_H^{\mathrm{inv}} \circ (P * E_H * Q)$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right) = H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. This proves Theorem 29.17. $\square$

We can now get Theorem 29.1 as a corollary:

Proof of Theorem 29.1. Just as in the proof of Corollary 29.8, we can prove the following facts:

- The map S is a k-algebra homomorphism from H to H.
- The map $e_{H,H}$ is a k-algebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).
- We have $S = \mathrm{id}_H^{*(-1)}$.
- We have $S * \mathrm{id}_H * e_{H,H} = e_{H,H}$ and $e_{H,H} * \mathrm{id}_H * S = e_{H,H}$.

Just as in the proof of Corollary 29.13, we can prove the following facts:

- We have $\varepsilon_H \circ e_{H,H} = \varepsilon_H$ and $\varepsilon_H \circ S = \varepsilon_H$.
- The maps $e_{H,H}$ and S are graded.

As a consequence, we can apply Theorem 29.17 to $P = e_{H,H}$ and $Q = S$. As a result, we obtain that the map $E_H^{\mathrm{inv}} \circ (e_{H,H} * E_H * S)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (e_{H,H} * E_H * S)\right) = H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. Since $e_{H,H} * E_H * S = E_H * S$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (E_H * S)\right) = H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. This proves Theorem 29.1 **(a)**.

But we can also apply Theorem 29.17 to $P = S$ and $Q = e_{H,H}$. As a result, we obtain that the map $E_H^{\mathrm{inv}} \circ (S * E_H * e_{H,H})$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (S * E_H * e_{H,H})\right) = H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. Since $S * E_H * e_{H,H} = S * E_H$, this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (S * E_H)\right) = H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2$. This proves Theorem 29.1 **(b)**. $\square$

Next, we specialize our results to connected graded bialgebras. The following fact is the specialization of Theorem 29.17 and the dual of Corollary 28.15:

Corollary 29.18. Let k be a field of characteristic 0. Let H be a commutative connected graded k-bialgebra. Let E_H be defined according to Definition 27.1.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-algebra homomorphisms satisfying $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map

$e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Then, the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right) = k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2$. [157]

Proof of Corollary 29.18. According to Theorem 29.17, the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right) = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$. Since $H_0 = k \cdot 1_H$ (by Proposition 29.14), this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right) = k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2$. This proves Corollary 29.18. □

The specialization of Theorem 29.1 is Theorem 29.2, and here is its (obvious) proof:

Proof of Theorem 29.2. Theorem 29.1 **(a)** says that the map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (E_H * S)\right) = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$. Since $H_0 = k \cdot 1_H$ (by Proposition 29.14), this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (E_H * S)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (E_H * S)\right) = k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2$. This proves Theorem 29.2 **(a)**.

Theorem 29.1 **(b)** says that the map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (S * E_H)\right) = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$. Since $H_0 = k \cdot 1_H$ (by Proposition 29.14), this rewrites as follows: The map $E_H^{\mathrm{inv}} \circ (S * E_H)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (S * E_H)\right) = k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2$. This proves Theorem 29.2 **(b)**. □

Finally, let us prove a relation between the maps $S * E_H$ and $E_H * S$ which is dual to Theorem 28.16:

Theorem 29.19. Let k be a field. Let H be a commutative graded k-Hopf algebra. Let S be the antipode of H. Let E_H be defined according to Definition 27.1.

(a) We have

$$S \circ (E_H * S) = (S * E_H) \circ S = -S * E_H.$$

(b) We have

$$S \circ (S * E_H) = (E_H * S) \circ S = -E_H * S.$$

We choose to prove this not in the same way as we proved Theorem 28.16, but differently. But still, let us formulate and verify the dual of Theorem 28.17:

Theorem 29.20. Let k be a field. Let H be a k-Hopf algebra. Let S be the antipode of H.

(a) We have $S \circ \eta_H = \eta_H$.

(b) If H is commutative, we have $S \circ \mu_H = \mu_H \circ (S \otimes S)$.

(c) If H is commutative, we have $S \circ S = \mathrm{id}_H$.

[157] Recall that the notation $(\operatorname{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

Proof of Theorem 29.20. Let us define H^{op} as according to Definition 26.3. Then, $H^{\mathrm{op}} = (H, \mu_H \circ \tau_{H,H}, \eta_H)$, so that $\eta_{H^{\mathrm{op}}} = \eta_H$.

But Proposition 26.4 yields that the antipode of H is a k-algebra homomorphism from H to H^{op}. Since the antipode of H is the map S, this rewrites as follows: The map S is a k-algebra homomorphism from H to H^{op}. Thus, $S \circ \eta_H = \eta_{H^{\mathrm{op}}}$. Since $\eta_{H^{\mathrm{op}}} = \eta_H$, this rewrites as $S \circ \eta_H = \eta_H$. This proves Theorem 29.20 **(a)**.

(b) Assume that H is commutative. Then, $\mu_H \circ \tau_{H,H} = \mu_H$, so that $H^{\mathrm{op}} = \left(H, \underbrace{\mu_H \circ \tau_{H,H}}_{=\mu_H}, \eta_H\right) = (H, \mu_H, \eta_H) = H$.

We have showed above that the map S is a k-algebra homomorphism from H to H^{op}. Since $H^{\mathrm{op}} = H$, this rewrites as follows: The map S is a k-algebra homomorphism from H to H. Thus, $S \circ \mu_H = \mu_H \circ (S \otimes S)$. This proves Theorem 29.20 **(b)**.

(c) The antipode of H is the $*$-inverse of the map id_H (because the antipode of a Hopf algebra is defined as the $*$-inverse of its identity map). Since the antipode of H is S, we thus have shown that S is the $*$-inverse of the map id_H. Thus, $S * \mathrm{id}_H = \mathrm{id}_H * S = e_{H,H}$ (where $e_{H,H}$ is defined as according to Definition 1.12).

Applying (21) to H, H, H, H, H, H, S, S, id_H, S instead of U, V, W, U', V', W', α, β, α', β', we obtain

$$(S \circ S) \otimes (S \circ \mathrm{id}_H) = (S \otimes S) \circ (S \otimes \mathrm{id}_H). \tag{332}$$

Now, by the definition of convolution,

$$\begin{aligned}
(S \circ S) * S &= \mu_H \circ \left((S \circ S) \otimes \underbrace{S}_{=S \circ \mathrm{id}_H} \right) \circ \Delta_H = \mu_H \circ \underbrace{\left((S \circ S) \otimes (S \circ \mathrm{id}_H)\right)}_{\substack{=(S \otimes S) \circ (S \otimes \mathrm{id}_H) \\ \text{(by (332))}}} \circ \Delta_H \\
&= \underbrace{\mu_H \circ (S \otimes S)}_{\substack{=S \circ \mu_H \\ \text{(by Theorem 29.20 (b))}}} \circ (S \otimes \mathrm{id}_H) \circ \Delta_H = s \circ \underbrace{\mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H}_{\substack{=S * \mathrm{id}_H \\ \text{(because } S * \mathrm{id}_H = \mu_H \circ (S \otimes \mathrm{id}_H) \circ \Delta_H \\ \text{by the definition of convolution)}}} \\
&= S \circ \underbrace{(S * \mathrm{id}_H)}_{\substack{=e_{H,H} = \eta_H \circ \varepsilon_H \\ \text{(by the definition of } e_{H,H}\text{)}}} = \underbrace{S \circ \eta_H}_{\substack{=\eta_H \\ \text{(by Theorem 29.20 (a))}}} \circ \varepsilon_H = \eta_H \circ \varepsilon_H = e_{H,H}
\end{aligned}$$

(since $e_{H,H} = \eta_H \circ \varepsilon_H$ by the definition of $e_{H,H}$). Thus,

$$\underbrace{(S \circ S) * S}_{=e_{H,H}} * \mathrm{id}_H = e_{H,H} * \mathrm{id}_H = \mathrm{id}_H.$$

Comparing this with

$$(S \circ S) * \underbrace{S * \mathrm{id}_H}_{=e_{H,H}} = (S \circ S) * e_{H,H} = S \circ S,$$

we obtain $S \circ S = \mathrm{id}_H$. This proves Theorem 29.20 **(c)**. □

The following fact is (more or less) a dual of Proposition 28.18 and will be used in our proof of Theorem 29.19:

Proposition 29.21. Let k be a field. Let H be a k-Hopf algebra. Let S be the antipode of H. Let $x \in H$.

(a) Then, $S(x) + x \in k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2$.

(b) Assume that H is a graded k-algebra. Then, $S(x) + x \in H_0 + (\operatorname{Ker}(\varepsilon_H))^2$.

Proof of Proposition 29.21. The antipode of H is the $*$-inverse of the map id_H (because the antipode of a Hopf algebra is defined as the $*$-inverse of its identity map). Since the antipode of H is S, we thus have shown that S is the $*$-inverse of the map id_H. Thus, $S * \mathrm{id}_H = \mathrm{id}_H * S = e_{H,H}$ (where $e_{H,H}$ is defined as according to Definition 1.12) and $S = \mathrm{id}_H^{*(-1)}$.

Since H is a bialgebra, we have $\varepsilon_H \circ \eta_H = \mathrm{id}_k$ (by the axioms of a bialgebra). But $e_{H,H} = \eta_H \circ \varepsilon_H$ (by the definition of $e_{H,H}$). Thus, $\varepsilon_H \circ e_{H,H} = \underbrace{\varepsilon_H \circ \eta_H}_{=\mathrm{id}_k} \circ \varepsilon_H = \varepsilon_H$.

Theorem 28.17 **(a)** yields $\varepsilon_H \circ S = \varepsilon_H$. Now,

$$\varepsilon_H \circ (S - e_{H,H}) = \underbrace{\varepsilon_H \circ S}_{=\varepsilon_H} - \underbrace{\varepsilon_H \circ e_{H,H}}_{=\varepsilon_H} \qquad \text{(since composition of } k\text{-linear maps is distributive)}$$
$$= \varepsilon_H - \varepsilon_H = 0.$$

Thus,

$$\varepsilon_H((S - e_{H,H})(H)) = \underbrace{(\varepsilon_H \circ (S - e_{H,H}))}_{=0}(H) = 0(H) = 0,$$

so that

$$(S - e_{H,H})(H) \subseteq \operatorname{Ker}(\varepsilon_H). \tag{333}$$

Also,

$$\varepsilon_H \circ (\mathrm{id}_H - e_{H,H}) = \underbrace{\varepsilon_H \circ \mathrm{id}_H}_{=\varepsilon_H} - \underbrace{\varepsilon_H \circ e_{H,H}}_{=\varepsilon_H}$$
$$\text{(since composition of } k\text{-linear maps is distributive)}$$
$$= \varepsilon_H - \varepsilon_H = 0.$$

Thus,

$$\varepsilon_H((\mathrm{id}_H - e_{H,H})(H)) = \underbrace{(\varepsilon_H \circ (\mathrm{id}_H - e_{H,H}))}_{=0}(H) = 0(H) = 0,$$

so that

$$(\mathrm{id}_H - e_{H,H})(H) \subseteq \operatorname{Ker}(\varepsilon_H). \tag{334}$$

On the other hand,

$$\underbrace{e_{H,H}}_{=\eta_H \circ \varepsilon_H}(H) = (\eta_H \circ \varepsilon_H)(H) = \eta_H \underbrace{(\varepsilon_H(H))}_{\subseteq k}$$
$$\subseteq \eta_H(k) = \left\{ \underbrace{\eta_H(\lambda)}_{\substack{=\lambda \cdot 1_H \\ \text{(by the definition of } \eta_H\text{)}}} \;\middle|\; \lambda \in k \right\} = \{\lambda \cdot 1_H \mid \lambda \in k\}$$
$$= k \cdot 1_H. \tag{335}$$

Now, Lemma 29.10 (applied to $C = H$, $A = H$, $f = S - e_{H,H}$ and $g = \mathrm{id}_H - e_{H,H}$) yields

$$\begin{aligned}\left((S - e_{H,H}) * (\mathrm{id}_H - e_{H,H})\right)(H) &\subseteq \underbrace{(S - e_{H,H})(H)}_{\substack{\subseteq \mathrm{Ker}(\varepsilon_H) \\ \text{(by (333))}}} \cdot \underbrace{(\mathrm{id}_H - e_{H,H})(H)}_{\substack{\subseteq \mathrm{Ker}(\varepsilon_H) \\ \text{(by (334))}}} \\ &\subseteq \mathrm{Ker}(\varepsilon_H) \cdot \mathrm{Ker}(\varepsilon_H) = (\mathrm{Ker}(\varepsilon_H))^2. \end{aligned} \tag{336}$$

But

$$\begin{aligned}(S - e_{H,H}) * (\mathrm{id}_H - e_{H,H}) &= \underbrace{S * \mathrm{id}_H}_{=e_{H,H}} - \underbrace{S * e_{H,H}}_{=S} - \underbrace{e_{H,H} * \mathrm{id}_H}_{=\mathrm{id}_H} + \underbrace{e_{H,H} * e_{H,H}}_{=e_{H,H}} \\ &= e_{H,H} - S - \mathrm{id}_H + e_{H,H} = 2e_{H,H} - (S + \mathrm{id}_H),\end{aligned}$$

so that

$$S + \mathrm{id}_H = 2e_{H,H} - (S - e_{H,H}) * (\mathrm{id}_H - e_{H,H}).$$

Thus,

$$\begin{aligned}(S + \mathrm{id}_H)(x) &= \left(2e_{H,H} - (S - e_{H,H}) * (\mathrm{id}_H - e_{H,H})\right)(x) \\ &= 2e_{H,H}\left(\underbrace{x}_{\in H}\right) - \left((S - e_{H,H}) * (\mathrm{id}_H - e_{H,H})\right)\left(\underbrace{x}_{\in H}\right) \\ &\in 2\underbrace{e_{H,H}(H)}_{\substack{\subseteq k \cdot 1_H \\ \text{(by (335))}}} - \underbrace{\left((S - e_{H,H}) * (\mathrm{id}_H - e_{H,H})\right)(H)}_{\substack{\subseteq (\mathrm{Ker}(\varepsilon_H))^2 \\ \text{(by (336))}}} \\ &\subseteq 2k \cdot 1_H - (\mathrm{Ker}(\varepsilon_H))^2 = \underbrace{2k \cdot 1_H}_{\substack{\subseteq k \cdot 1_H \\ \text{(since } k \cdot 1_H \text{ is a} \\ k\text{-vector space)}}} + \underbrace{\left(-(\mathrm{Ker}(\varepsilon_H))^2\right)}_{\substack{\subseteq (\mathrm{Ker}(\varepsilon_H))^2 \\ \text{(since } (\mathrm{Ker}(\varepsilon_H))^2 \text{ is a} \\ k\text{-vector space)}}} \\ &\subseteq k \cdot 1_H + (\mathrm{Ker}(\varepsilon_H))^2.\end{aligned}$$

Since $(S + \mathrm{id}_H)(x) = S(x) + \underbrace{\mathrm{id}_H(x)}_{=x} = S(x) + x$, this rewrites as $S(x) + x \in k \cdot 1_H + (\mathrm{Ker}(\varepsilon_H))^2$. This proves Proposition 29.21 **(a)**.

(b) The grading on k is such that $k_0 = k$. Thus, $\eta_H\left(\underbrace{k}_{=k_0}\right) = \eta_H(k_0) \subseteq H_0$ (since η_H is a graded map (because H is a graded k-algebra)). But we have shown above that $\eta_H(k) = k \cdot 1_H$. Hence, $k \cdot 1_H = \eta_H(k) \subseteq H_0$.

Proposition 29.21 **(a)** yields

$$S(x) + x \in \underbrace{k \cdot 1_H}_{\subseteq H_0} + (\mathrm{Ker}(\varepsilon_H))^2 \subseteq H_0 + (\mathrm{Ker}(\varepsilon_H))^2.$$

This proves Proposition 29.21 **(b)**. □

We will now generalize part of Theorem 29.19 to graded Hopf algebras which are not necessarily commutative or cocommutative:

Theorem 29.22. Let k be a field. Let H be a graded k-Hopf algebra. Let S be the antipode of H. Let E_H be defined according to Definition 27.1.

(a) We have

$$S \circ (E_H * S) = (S * E_H) \circ S.$$

(b) We have

$$S \circ (S * E_H) = (E_H * S) \circ S.$$

Something even stronger holds:

Theorem 29.23. Let k be a field. Let H be a k-Hopf algebra. Let S be the antipode of H. Let $f : H \to H$ and $g : H \to H$ be two k-linear maps such that $f \circ S = S \circ f$ and $g \circ S = S \circ g$. Then,

$$S \circ (f * g) = (g * f) \circ S.$$

Proof of Theorem 29.23. Proposition 9.3 **(a)** (applied to H, H, H, H, S and S instead of V, W, V', W', f and g) yields

$$(S \otimes S) \circ \tau_{H,H} = \tau_{H,H} \circ (S \otimes S). \tag{337}$$

Proposition 9.3 **(a)** (applied to H, H, H and H instead of V, W, V' and W') yields

$$(g \otimes f) \circ \tau_{H,H} = \tau_{H,H} \circ (f \otimes g). \tag{338}$$

Let us define H^{op} as according to Definition 26.3. Then, $H^{\mathrm{op}} = (H, \mu_H \circ \tau_{H,H}, \eta_H)$, so that $\mu_{H^{\mathrm{op}}} = \mu_H \circ \tau_{H,H}$.

But Proposition 26.4 yields that the antipode of H is a k-algebra homomorphism from H to H^{op}. In other words, S is a k-algebra homomorphism from H to H^{op} (since S is the antipode of H). Thus,

$$\begin{aligned} S \circ \mu_H &= \underbrace{\mu_{H^{\mathrm{op}}}}_{=\mu_H \circ \tau_{H,H}} \circ (S \otimes S) = \mu_H \circ \underbrace{\tau_{H,H} \circ (S \otimes S)}_{\substack{=(S \otimes S) \circ \tau_{H,H} \\ \text{(by (337))}}} \\ &= \mu_H \circ (S \otimes S) \circ \tau_{H,H}. \end{aligned} \tag{339}$$

Let us define H^{cop} as according to Definition 25.3. Then, $H^{\mathrm{cop}} = (H, \tau_{H,H} \circ \Delta_H, \varepsilon_H)$, so that $\Delta_{H^{\mathrm{cop}}} = \tau_{H,H} \circ \Delta_H$.

But Proposition 25.4 yields that the antipode of H is a k-coalgebra homomorphism from H^{cop} to H. In other words, S is a k-coalgebra homomorphism from H^{cop} to H (since S is the antipode of H). Thus,

$$\begin{aligned} \Delta_H \circ S &= (S \otimes S) \circ \underbrace{\Delta_{H^{\mathrm{cop}}}}_{=\tau_{H,H} \circ \Delta_H} = \underbrace{(S \otimes S) \circ \tau_{H,H}}_{\substack{=\tau_{H,H} \circ (S \otimes S) \\ \text{(by (337))}}} \circ \Delta_H \\ &= \tau_{H,H} \circ (S \otimes S) \circ \Delta_H. \end{aligned} \tag{340}$$

By the definition of convolution, we have $f * g = \mu_H \circ (f \otimes g) \circ \Delta_H$ and $g * f = \mu_H \circ (g \otimes f) \circ \Delta_H$.

Now,

$$\underbrace{(g*f)}_{=\mu_H\circ(g\otimes f)\circ\Delta_H}\circ S = \mu_H\circ(g\otimes f)\circ \underbrace{\Delta_H\circ S}_{\substack{=\tau_{H,H}\circ(S\otimes S)\circ\Delta_H \\ \text{(by (340))}}} = \mu_H\circ\underbrace{(g\otimes f)\circ\tau_{H,H}}_{\substack{=\tau_{H,H}\circ(f\otimes g) \\ \text{(by (338))}}}\circ(S\otimes S)\circ\Delta_H$$

$$= \mu_H\circ\tau_{H,H}\circ \underbrace{(f\otimes g)\circ(S\otimes S)}_{\substack{=(f\circ S)\otimes(g\circ S) \\ \text{(since (21) (applied to } H,\ H,\ H,\ H,\ H,\ H, \\ S,\ f,\ S,\ g \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta') \\ \text{yields } (f\circ S)\otimes(g\circ S)=(f\otimes g)\circ(S\otimes S))}}\circ\Delta_H$$

$$= \mu_H\circ\tau_{H,H}\circ\left(\underbrace{(f\circ S)}_{=S\circ f}\otimes\underbrace{(g\circ S)}_{=S\circ g}\right)\circ\Delta_H$$

$$= \mu_H\circ\tau_{H,H}\circ \underbrace{((S\circ f)\otimes(S\circ g))}_{\substack{=(S\otimes S)\circ(f\otimes g) \\ \text{(by (21), applied to } H,\ H,\ H,\ H,\ H,\ H, \\ f,\ S,\ g,\ S \text{ instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha',\ \beta')}}\circ\Delta_H$$

$$= \mu_H\circ\underbrace{\tau_{H,H}\circ(S\otimes S)}_{\substack{=(S\otimes S)\circ\tau_{H,H} \\ \text{(by (337))}}}\circ(f\otimes g)\circ\Delta_H$$

$$= \underbrace{\mu_H\circ(S\otimes S)\circ\tau_{H,H}}_{\substack{=S\circ\mu_H \\ \text{(by (339))}}}\circ(f\otimes g)\circ\Delta_H = S\circ\mu_H\circ(f\otimes g)\circ\Delta_H.$$

Compared with

$$S\circ\underbrace{(f*g)}_{=\mu_H\circ(f\otimes g)\circ\Delta_H} = S\circ\mu_H\circ(f\otimes g)\circ\Delta_H,$$

this yields $(g*f)\circ S = S\circ(f*g)$. This proves Theorem 29.23. □

Proof of Theorem 29.22. Since H is a graded k-Hopf algebra, the antipode of H is graded. Since the antipode of H is S, this shows that S is graded. Thus, $S\circ E_H = E_H\circ S$ (by Proposition 27.4, applied to $V=H$, $W=H$ and $f=S$). In other words, $E_H\circ S = S\circ E_H$. Also, clearly, $S\circ S = S\circ S$. Thus, we can apply Theorem 29.23 to $f=E_H$ and $g=S$. As a consequence, we obtain $S\circ(E_H*S) = (S*E_H)\circ S$. This proves Theorem 29.22 **(a)**.

But we can also apply Theorem 29.23 to $f=S$ and $g=E_H$. As a consequence, we obtain $S\circ(S*E_H) = (E_H*S)\circ S$. This proves Theorem 29.22 **(b)**. □

Proof of Theorem 29.19. **(a)** Let $x\in H$. Then,

$$(S*E_H)\underbrace{(S(x)+x)}_{\substack{\in H_0+(\operatorname{Ker}(\varepsilon_H))^2 \\ \text{(by Proposition 29.21 (b))}}} \in (S*E_H)\left(H_0+(\operatorname{Ker}(\varepsilon_H))^2\right) = 0$$

(by Corollary 29.13 **(d)**). Thus, $(S*E_H)(S(x)+x)=0$. In other words,

$$0 = (S*E_H)(S(x)+x) = \underbrace{(S*E_H)(S(x))}_{=((S*E_H)\circ S)(x)} + (S*E_H)(x) \qquad \text{(since } S*E_H \text{ is } k\text{-linear)}$$

$$= ((S*E_H)\circ S)(x) + (S*E_H)(x).$$

Hence, $((S * E_H) \circ S)(x) = -(S * E_H)(x) = (-S * E_H)(x)$.

Now, forget that we fixed x. We thus have proven that every $x \in H$ satisfies $((S * E_H) \circ S)(x) = (-S * E_H)(x)$. In other words, $(S * E_H) \circ S = -S * E_H$. Combined with $S \circ (E_H * S) = (S * E_H) \circ S$ (which follows from Theorem 29.22 **(a)**), this yields

$$S \circ (E_H * S) = (S * E_H) \circ S = -S * E_H.$$

This proves Theorem 29.19 **(a)**.

(b) Let $x \in H$. Then,

$$(E_H * S) \underbrace{(S(x) + x)}_{\substack{\in H_0 + (\operatorname{Ker}(\varepsilon_H))^2 \\ \text{(by Proposition 29.21 (b))}}} \in (E_H * S)\left(H_0 + (\operatorname{Ker}(\varepsilon_H))^2\right) = 0$$

(by Corollary 29.13 **(a)**). Thus, $(E_H * S)(S(x) + x) = 0$. In other words,

$$0 = (E_H * S)(S(x) + x) = \underbrace{(E_H * S)(S(x))}_{=((E_H * S) \circ S)(x)} + (E_H * S)(x) \qquad \text{(since } E_H * S \text{ is } k\text{-linear)}$$
$$= ((E_H * S) \circ S)(x) + (E_H * S)(x).$$

Hence, $((E_H * S) \circ S)(x) = -(E_H * S)(x) = (-E_H * S)(x)$.

Now, forget that we fixed x. We thus have proven that every $x \in H$ satisfies $((E_H * S) \circ S)(x) = (-E_H * S)(x)$. In other words, $(E_H * S) \circ S = -E_H * S$. Combined with $S \circ (S * E_H) = (E_H * S) \circ S$ (which follows from Theorem 29.22 **(b)**), this yields

$$S \circ (S * E_H) = (E_H * S) \circ S = -E_H * S.$$

This proves Theorem 29.19 **(b)**. □

Note that we could have used this method (along with Proposition 28.18) to give an alternative proof of Theorem 28.16 as well.

§30. Non-integer convolution powers and Dynkin idempotents

In the following, we will introduce and study non-integer powers of linear maps with respect to convolution. These powers are defined for any k-linear map $f \in G(C, A)$, where k is a field of characteristic 0 (the condition that the characteristic of k be 0 cannot be dispensed with!), C is a connected filtered k-coalgebra and A is a k-algebra. The goal will be to obtain "interpolations" between the Dynkin idempotents $E_H * S$ and $S * E_H$ found by Reutenauer and Procesi and mentioned in the Remark in §3 of [PatReu00].

First of all, we define a generalization of the familiar notion of binomial coefficients.

Definition 30.1. Let k be a field of characteristic 0. Let $\gamma \in k$. Let $i \in \mathbb{N}$. Then, we define $\dbinom{\gamma}{i}$ to denote the element $\dfrac{\gamma(\gamma-1)\cdots(\gamma-i+1)}{i!}$ of k.

Of course, when $k = \mathbb{Q}$ and $\gamma \in \mathbb{Z}$, this definition agrees with the standard definition of binomial coefficients.

Next, we define fractional powers of linear maps with respect to convolution:

Definition 30.2. Let k be a field of characteristic 0. Let $\gamma \in k$. Let A be a k-algebra, and let H be a connected filtered k-coalgebra. For every $f \in \mathfrak{g}(H, A)$, let us define a map $\operatorname{Pow}_\gamma f : H \to A$ by the formula

$$\left(\left(\operatorname{Pow}_\gamma f\right)(x) = \sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(x) \qquad \text{for every } x \in H \right) \tag{341}$$

(where $\binom{\gamma}{i}$ is defined as in Definition 30.1). This map $\operatorname{Pow}_\gamma f$ is well-defined, because for every $x \in H$ the infinite sum $\sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(x)$ converges with respect to the discrete topology[158]. Besides, $\operatorname{Pow}_\gamma f$ is a k-linear map[159], so that $\operatorname{Pow}_\gamma f \in \mathcal{L}(H, A)$. More precisely, $\operatorname{Pow}_\gamma f \in G(H, A)$. [160]

Definition 30.3. Let k be a field of characteristic 0. Let $\gamma \in k$. Let A be a k-algebra, and let H be a connected filtered k-coalgebra. For every $F \in G(H, A)$, let us define an element $\operatorname{pow}_\gamma F \in G(H, A)$ by $\operatorname{pow}_\gamma F =$

[158] *Proof.* Let $x \in H$. Then, there exists some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$ (since H is filtered). Consider this n. Then, every integer $i > n$ satisfies $f^{*i}(x) = 0$ (this is proven just as in Definition 3.6). Therefore, every integer $i > n$ satisfies $\binom{\gamma}{i} \underbrace{f^{*i}(x)}_{=0} = 0$. In other words, for every integer $i > n$, the i-th addend of the infinite sum $\sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(x)$ is zero. Hence, this infinite sum $\sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(x)$ has only finitely many nonzero addends. Thus, this sum converges with respect to the discrete topology, qed.

[159] *Proof.* Let $\alpha \in k$, $\beta \in k$, $x \in H$ and $y \in H$ be arbitrary. Then, (341) (applied to y instead of x) yields $\left(\operatorname{Pow}_\gamma f\right)(y) = \sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(y)$. But (341) (applied to $\alpha x + \beta y$ instead of x) yields

$$\begin{aligned}
\left(\operatorname{Pow}_\gamma f\right)(\alpha x + \beta y) &= \sum_{i \in \mathbb{N}} \binom{\gamma}{i} \underbrace{f^{*i}(\alpha x + \beta y)}_{\substack{= \alpha f^{*i}(x) + \beta f^{*i}(y) \\ \text{(since } f^{*i} \text{ is a } k\text{-linear map)}}} = \sum_{i \in \mathbb{N}} \underbrace{\binom{\gamma}{i} \left(\alpha f^{*i}(x) + \beta f^{*i}(y)\right)}_{= \alpha \binom{\gamma}{i} f^{*i}(x) + \beta \binom{\gamma}{i} f^{*i}(y)} \\
&= \alpha \underbrace{\sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(x)}_{= \left(\operatorname{Pow}_\gamma f\right)(x)} + \beta \underbrace{\sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(y)}_{= \left(\operatorname{Pow}_\gamma f\right)(y)} = \alpha \left(\operatorname{Pow}_\gamma f\right)(x) + \beta \left(\operatorname{Pow}_\gamma f\right)(y).
\end{aligned}$$

Since this holds for all $\alpha \in k$, $\beta \in k$, $x \in H$ and $y \in H$, we thus see that $\operatorname{Pow}_\gamma f$ is k-linear, qed.

[160] *Proof.* Every integer $i > 0$ satisfies $f^{*i}(H_{\leq 0}) = 0$ (by Remark 3.5, applied to $n = 0$) and thus $f^{*i}\left(\underbrace{1_H}_{\in H_{\leq 0}}\right) \in f^{*i}(H_{\leq 0}) = 0$, so that $f^{*i}(1_H) = 0$. Also, $f^{*0} = e_{H,A}$ (where $e_{H,A}$ is defined according

$\operatorname{Pow}_\gamma(F - e_{H,A})$. [161]

The notation $\operatorname{pow}_\gamma F$ is suggestive: it generalizes the powers of F with respect to convolution. In fact, we have:

Theorem 30.4. Let k be a field of characteristic 0. Let A be a k-algebra, and let H be a connected filtered k-coalgebra. Let $F \in G(H, A)$.

(a) The map F is $*$-invertible.

(b) Every $n \in \mathbb{Z}$ satisfies $\operatorname{pow}_n F = F^{*n}$ (where the n in $\operatorname{pow}_n F$ means the element $n \cdot 1$ of k).

We will not prove Theorem 30.4 directly, but obtain this as a consequence of a stronger result:

Theorem 30.5. Let k be a field of characteristic 0. Let $\gamma \in k$. Let A be a k-algebra, and let H be a connected filtered k-coalgebra. For every $F \in G(H, A)$, we have $\operatorname{pow}_\gamma F = e^{*(\gamma \operatorname{Log} F)}$.

The proof of this theorem will (like that of Proposition 5.13) proceed by applying identities for formal power series. Just as we used Theorem 5.2 to prove Proposition 5.13, here we need the following fact:

---

to Definition 1.12), so that

$$\begin{aligned} f^{*0}(1_H) &= \underbrace{e_{H,A}}_{\substack{=\eta_A \circ \varepsilon_H \\ \text{(by the definition of } e_{H,A}\text{)}}} (1_H) = (\eta_A \circ \varepsilon_H)(1_H) = \eta_A(\varepsilon_H(1_H)) \\ &= \underbrace{\varepsilon_H(1_H)}_{\substack{=1 \\ \text{(by the axioms of a bialgebra,} \\ \text{since } H \text{ is a } k\text{-bialgebra)}}} \cdot 1_A \qquad \text{(by the definition of } \eta_A\text{)} \\ &= 1_A. \end{aligned}$$

But applying (341) to $x = 1_H$, we get

$$\begin{aligned} (\operatorname{Pow}_\gamma f)(1_H) &= \sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(1_H) = \underbrace{\binom{\gamma}{0}}_{=1} \underbrace{f^{*0}(1_H)}_{=1_A} + \sum_{i>0} \binom{\gamma}{i} \underbrace{f^{*i}(1_H)}_{\substack{=0 \\ \text{(since } i>0\text{)}}} \\ &= 1_A + \underbrace{\sum_{i>0} \binom{\gamma}{i} 0}_{=0} = 1_A. \end{aligned}$$

Thus, $\operatorname{Pow}_\gamma f \in G(H, A)$ (by the definition of $G(H, A)$).

[161] This is well-defined for the following reason:

From Definition 30.2, we know that $\operatorname{Pow}_\gamma f \in G(H, A)$ for every $f \in \mathfrak{g}(H, A)$. Since

$$\underbrace{F}_{\in G(H,A) = e_{H,A} + \mathfrak{g}(H,A)} - e_{H,A} \in e_{H,A} + \mathfrak{g}(H, A) - e_{H,A} = \mathfrak{g}(H, A),$$

we can apply this to $f = F - e_{H,A}$, and conclude that $\operatorname{Pow}_\gamma(F - e_{H,A}) \in G(H, A)$. Hence, $\operatorname{pow}_\gamma F$ is well-defined, qed.

Theorem 30.6. Let k be a field of characteristic 0. Let $\gamma \in k$.

Then, every power series $P \in k\left[\left[X\right]\right]$ whose coefficient before X^0 is 0 satisfies $\sum\limits_{i \in \mathbb{N}} \dbinom{\gamma}{i} P^i = \exp\left(\gamma \log\left(1+P\right)\right)$. (Here, $\dbinom{\gamma}{i}$ is defined as in Definition 30.1, whereas $\log\left(1+P\right)$ and $\exp\left(\gamma\left(\log\left(1+P\right)\right)\right)$ are defined as in Definition 5.1.)

Proof of Theorem 30.6. Here is something very easy to prove: Every $i \in \mathbb{N}$ satisfies

$$\binom{\gamma}{i+1} \cdot (i+1) = \binom{\gamma}{i} \cdot (\gamma - i)\,. \tag{342}$$

[162]

Let $P \in k\left[\left[X\right]\right]$ be a power series whose coefficient before X^0 is 0. Write P in the form $P = \sum\limits_{i \in \mathbb{N}} p_i X^i$, where p_0, p_1, p_2, ... are elements of k. Then, p_0 is the coefficient of P before X^0, and thus equals 0 (since the coefficient of P before X^0 is 0). We have

[162] *Proof of (342):* Every $i \in \mathbb{N}$ satisfies

$$\begin{aligned}
&\underbrace{\binom{\gamma}{i+1}}_{=\frac{\gamma(\gamma-1)\cdots(\gamma-(i+1)+1)}{(i+1)!} \atop \text{(by the definition of } \binom{\gamma}{i}\text{)}} \cdot (i+1) \\
&= \frac{\gamma(\gamma-1)\cdots(\gamma-(i+1)+1)}{(i+1)!} \cdot (i+1) = \left(\gamma(\gamma-1)\cdots\underbrace{(\gamma-(i+1)+1)}_{=\gamma-i}\right) \cdot \underbrace{\frac{i+1}{(i+1)!}}_{=\frac{i+1}{(i+1)\,i!} \atop \text{(since } (i+1)!=(i+1)i!\text{)}} \\
&= \underbrace{(\gamma(\gamma-1)\cdots(\gamma-i))}_{=(\gamma(\gamma-1)\cdots(\gamma-i+1))\cdot(\gamma-i)} \cdot \underbrace{\frac{i+1}{(i+1)\,i!}}_{=\frac{1}{i!}} = (\gamma(\gamma-1)\cdots(\gamma-i+1)) \cdot (\gamma-i) \cdot \frac{1}{i!} \\
&= \underbrace{\frac{\gamma(\gamma-1)\cdots(\gamma-i+1)}{i!}}_{=\binom{\gamma}{i} \atop \text{(since } \binom{\gamma}{i}=\frac{\gamma(\gamma-1)\cdots(\gamma-i+1)}{i!} \text{ by the definition of } \binom{\gamma}{i}\text{)}} \cdot (\gamma-i) = \binom{\gamma}{i} \cdot (\gamma-i)\,.
\end{aligned}$$

This proves (342).

thus shown that $p_0 = 0$. Now,

$$P = \sum_{i \in \mathbb{N}} p_i X^i = \underbrace{p_0}_{=0} X^0 + \sum_{\substack{i \in \mathbb{N}; \\ i \geq 1}} p_i \underbrace{X^i}_{= X^{i-1} X} = \underbrace{0 X^0}_{=0} + \sum_{\substack{i \in \mathbb{N}; \\ i \geq 1}} p_i X^{i-1} X$$

$$= \sum_{\substack{i \in \mathbb{N}; \\ i \geq 1}} p_i X^{i-1} X = \left(\sum_{\substack{i \in \mathbb{N}; \\ i \geq 1}} p_i X^{i-1} \right) X.$$

Hence, $X \mid P$ in $k[[X]]$. Thus, every $i \in \mathbb{N}$ satisfies $X^i \mid P^i$. Hence, every positive $i \in \mathbb{N}$ satisfies $X \mid P^i$ (since $X \mid X^i$ (because i is positive) and $X^i \mid P^i$). In other words,

$$\text{every positive } i \in \mathbb{N} \text{ satisfies } P^i \equiv 0 \bmod Xk[[X]]. \tag{343}$$

Now,

$$\sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i = \underbrace{\binom{\gamma}{0}}_{=1} \underbrace{P^0}_{=1} + \sum_{i > 0} \binom{\gamma}{i} \underbrace{P^i}_{\substack{\equiv 0 \bmod Xk[[X]] \\ \text{(by (343), since} \\ i \text{ is positive)}}}$$

$$\equiv 1 + \underbrace{\sum_{i > 0} \binom{\gamma}{i} 0}_{=0} = 1 \bmod Xk[[X]].$$

In other words, $X \mid \sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i - 1$ in $k[[X]]$. This means that the coefficient of the power series $\sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i - 1$ before X^0 is 0. In other words,

$$0 = \left(\text{the coefficient of the power series } \sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i - 1 \text{ before } X^0 \right)$$

$$= \left(\text{the coefficient of the power series } \sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i \text{ before } X^0 \right)$$

$$- \underbrace{\left(\text{the coefficient of the power series } 1 \text{ before } X^0 \right)}_{=1}$$

$$= \left(\text{the coefficient of the power series } \sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i \text{ before } X^0 \right) - 1.$$

In other words, the coefficient of the power series $\sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i$ before X^0 equals 1. Hence, $\sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i$ is a power series whose coefficient before X^0 is 1. This yields that the power series $\log\left(\sum_{i \in \mathbb{N}} \binom{\gamma}{i} P^i \right) \in k[[X]]$ is well-defined.

Since $\sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i$ is a power series whose coefficient before X^0 is 1, we can apply Proposition 5.10 to $Q = \sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i$. Thus, Proposition 5.10 **(a)** (applied to $Q = \sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i$) shows that the power series $\sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i$ has a multiplicative inverse $\left(\sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i\right)^{-1}$. Furthermore, Proposition 5.10 **(a)** (applied to $Q = \sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i$) shows that it satisfies

$$\frac{d}{dX} \log\left(\sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i\right) = \left(\sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i\right)^{-1} \cdot \frac{d}{dX}\left(\sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i\right). \tag{344}$$

But

$$\frac{d}{dX}\left(\sum_{i\in\mathbb{N}} \binom{\gamma}{i} P^i\right) = \sum_{i\in\mathbb{N}} \binom{\gamma}{i} \frac{d}{dX}\left(P^i\right) = \underbrace{\binom{\gamma}{0}}_{=0} \underbrace{\frac{d}{dX}\left(P^0\right)}_{\substack{=0 \\ (\text{since } P^0=1)}} + \sum_{i>0} \binom{\gamma}{i} \underbrace{\frac{d}{dX}\left(P^i\right)}_{\substack{=iP^{i-1}\cdot\frac{d}{dX}P \\ (\text{by Proposition 5.8} \\ (\text{applied to } i \text{ instead of } n))}}$$

$$= \sum_{i>0} \binom{\gamma}{i} \cdot iP^{i-1} \cdot \left(\frac{d}{dX}P\right) \tag{345}$$

$$= \sum_{i\in\mathbb{N}} \underbrace{\binom{\gamma}{i+1} \cdot (i+1)}_{\substack{=\binom{\gamma}{i}\cdot(\gamma-i) \\ (\text{by (342)})}} \underbrace{P^{(i+1)-1}}_{=P^i} \cdot \left(\frac{d}{dX}P\right)$$

(here, we substituted $i+1$ for i in the sum)

$$= \sum_{i\in\mathbb{N}} \binom{\gamma}{i} \cdot (\gamma - i)\, P^i \cdot \left(\frac{d}{dX}P\right), \tag{346}$$

and

$$\begin{aligned}
&\left(\frac{d}{dX}\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\right)\cdot(1+P)\\
&= \underbrace{\frac{d}{dX}\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)}_{=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot(\gamma-i)P^i\cdot\left(\frac{d}{dX}P\right)\text{ (by (346))}} + \underbrace{\left(\frac{d}{dX}\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\right)}_{=\sum_{i>0}\binom{\gamma}{i}\cdot iP^{i-1}\cdot\left(\frac{d}{dX}P\right)\text{ (by (345))}}\cdot P\\
&= \sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot(\gamma-i)\,P^i\cdot\left(\frac{d}{dX}P\right) + \underbrace{\left(\sum_{i>0}\binom{\gamma}{i}\cdot iP^{i-1}\cdot\left(\frac{d}{dX}P\right)\right)\cdot P}_{=\sum_{i>0}\binom{\gamma}{i}\cdot iP^{i-1}P\cdot\left(\frac{d}{dX}P\right)}\\
&= \sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot(\gamma-i)\,P^i\cdot\left(\frac{d}{dX}P\right) + \sum_{i>0}\binom{\gamma}{i}\cdot i\underbrace{P^{i-1}P}_{=P^i}\cdot\left(\frac{d}{dX}P\right)\\
&= \sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot(\gamma-i)\,P^i\cdot\left(\frac{d}{dX}P\right) + \sum_{i>0}\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right). \qquad (347)
\end{aligned}$$

Since

$$\begin{aligned}
\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right) &= \underbrace{\binom{\gamma}{0}\cdot 0P^0\cdot\left(\frac{d}{dX}P\right)}_{=0} + \sum_{i>0}\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right)\\
&= \sum_{i>0}\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right), \qquad (348)
\end{aligned}$$

the equality (347) becomes

$$\begin{aligned}
&\left(\frac{d}{dX}\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\right)\cdot(1+P)\\
&=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot(\gamma-i)\,P^i\cdot\left(\frac{d}{dX}P\right)+\underbrace{\sum_{i>0}\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right)}_{\substack{=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right)\\ \text{(by (348))}}}\\
&=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot(\gamma-i)\,P^i\cdot\left(\frac{d}{dX}P\right)+\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right)\\
&=\sum_{i\in\mathbb{N}}\underbrace{\left(\binom{\gamma}{i}\cdot(\gamma-i)\,P^i\cdot\left(\frac{d}{dX}P\right)+\binom{\gamma}{i}\cdot iP^i\cdot\left(\frac{d}{dX}P\right)\right)}_{=\binom{\gamma}{i}\cdot((\gamma-i)+i)P^i\cdot\left(\frac{d}{dX}P\right)}\\
&=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot\underbrace{((\gamma-i)+i)}_{=\gamma}P^i\cdot\left(\frac{d}{dX}P\right)=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}\cdot\gamma P^i\cdot\left(\frac{d}{dX}P\right)\\
&=\gamma\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\cdot\left(\frac{d}{dX}P\right). \qquad (349)
\end{aligned}$$

On the other hand,

$$\begin{aligned}
&\left(\text{the coefficient of the power series } 1+P \text{ before } X^0\right)\\
&=\underbrace{\left(\text{the coefficient of the power series } 1 \text{ before } X^0\right)}_{=1}\\
&\qquad+\underbrace{\left(\text{the coefficient of the power series } P \text{ before } X^0\right)}_{=0}\\
&=1.
\end{aligned}$$

In other words, the coefficient of the power series $1+P$ before X^0 equals 1. Hence, $1+P$ is a power series whose coefficient before X^0 is 1. This yields that the power series $\log(1+P)\in k[[X]]$ is well-defined.

Since $1+P$ is a power series whose coefficient before X^0 is 1, we can apply by Proposition 5.10 to $Q=1+P$. Thus, Proposition 5.10 **(a)** (applied to $Q=1+P$) shows that the power series $1+P$ has a multiplicative inverse $(1+P)^{-1}$. Furthermore, Proposition 5.10 **(b)** (applied to $Q=1+P$) shows that it satisfies

$$\begin{aligned}
\frac{d}{dX}\left(\log(1+P)\right)&=(1+P)^{-1}\cdot\underbrace{\frac{d}{dX}(1+P)}_{=\frac{d}{dX}1+\frac{d}{dX}P}=(1+P)^{-1}\cdot\left(\underbrace{\frac{d}{dX}1}_{=0}+\frac{d}{dX}P\right)\\
&=(1+P)^{-1}\cdot\frac{d}{dX}P. \qquad (350)
\end{aligned}$$

Since $1+P$ has a multiplicative inverse, we can divide the equality (349) by $1+P$, and obtain

$$\frac{d}{dX}\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right) = (1+P)^{-1}\cdot\gamma\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\cdot\left(\frac{d}{dX}P\right). \tag{351}$$

Now, (344) becomes

$$\begin{aligned}
\frac{d}{dX}\log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right) &= \left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)^{-1}\cdot \underbrace{\frac{d}{dX}\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)}_{\substack{=(1+P)^{-1}\cdot\gamma\left(\sum\limits_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\cdot\left(\frac{d}{dX}P\right)\\ \text{(by (351))}}} \\
&= \left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)^{-1}\cdot(1+P)^{-1}\cdot\gamma\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\cdot\left(\frac{d}{dX}P\right) \\
&= \gamma\cdot\underbrace{(1+P)^{-1}\cdot\frac{d}{dX}P}_{\substack{=\frac{d}{dX}(\log(1+P))\\ \text{(by (350))}}} = \gamma\cdot\frac{d}{dX}\left(\log(1+P)\right) \\
&= \frac{d}{dX}\left(\gamma\log(1+P)\right). \qquad (352)
\end{aligned}$$

Since $1+P$ is a power series whose coefficient before X^0 is 1, we can apply Proposition 5.12 **(b)** to $Q = 1+P$, and conclude that $\log(1+P)$ is a power series whose coefficient before X^0 is 0. In other words,

$$\left(\text{the coefficient of } \log(1+P) \text{ before } X^0\right) = 0.$$

Thus,

$$\begin{aligned}
&\left(\text{the coefficient of } \gamma\log(1+P) \text{ before } X^0\right) \\
&= \gamma\cdot\underbrace{\left(\text{the coefficient of } \log(1+P) \text{ before } X^0\right)}_{=0} = 0.
\end{aligned}$$

Since $\sum\limits_{i\in\mathbb{N}}\binom{\gamma}{i}P^i$ is a power series whose coefficient before X^0 is 1, we can apply Proposition 5.12 **(b)** to $Q = \sum\limits_{i\in\mathbb{N}}\binom{\gamma}{i}P^i$, and conclude that $\log\left(\sum\limits_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)$ is a power series whose coefficient before X^0 is 0. In other words,

$$\left(\text{the coefficient of } \log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right) \text{ before } X^0\right) = 0.$$

Thus,

$$\begin{aligned}
&\left(\text{the coefficient of } \log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right) \text{ before } X^0\right) \\
&= 0 = \left(\text{the coefficient of } \gamma\log(1+P) \text{ before } X^0\right).
\end{aligned}$$

In other words, the coefficient of $\log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)$ before X^0 equals the coefficient of $\gamma\log(1+P)$ before X^0. Combined with (352), this yields that we can apply Proposition 5.4 to $U=\log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)$ and $V=\gamma\log(1+P)$. As a result, we obtain

$$\log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)=\gamma\log(1+P). \tag{353}$$

But since $\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i$ is a power series whose coefficient before X^0 is 1, we can apply Theorem 5.2 **(b)** to $Q=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i$. As a result, we obtain

$$\exp\left(\log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)\right)=\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i.$$

Thus,

$$\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i=\exp\left(\underbrace{\log\left(\sum_{i\in\mathbb{N}}\binom{\gamma}{i}P^i\right)}_{\substack{=\gamma\log(1+P)\\ \text{(by (353))}}}\right)=\exp\left(\gamma\log(1+P)\right).$$

This proves Theorem 30.6. □

Just as Corollary 5.14 was derived from Theorem 5.2, we can derive from Theorem 30.6 the following corollary:

Corollary 30.7. Let k be a field of characteristic 0. Let $n\in\mathbb{N}$. Let $\gamma\in k$.

Let b be an element of a k-algebra such that $b^{n+1}=0$. Then,

$$\sum_{j=0}^{n}\frac{\left(\gamma\sum\limits_{i=1}^{n}\dfrac{(-1)^{i-1}}{i}b^i\right)^j}{j!}=\sum_{i=0}^{n}\binom{\gamma}{i}b^i$$

(where $\binom{\gamma}{i}$ is defined as in Definition 30.1).

Proof of Corollary 30.7. Consider the ring of power series $k[[X]]$. Clearly, X is a power series whose coefficient before X^0 is 0. Thus, applying Theorem 30.6 to $P=X$, we

obtain $\sum\limits_{i\in\mathbb{N}} \dbinom{\gamma}{i} X^i = \exp\left(\gamma \log\left(1+X\right)\right)$. Now, in the ring $k\left[\left[X\right]\right]$, we have

$$\begin{aligned}
\log\left(1+X\right) &= \sum_{i\geq 1} \frac{\left(-1\right)^{i-1}}{i} \left(\underbrace{\left(1+X\right)-1}_{=X}\right)^i \qquad \text{(by the definition of log)} \\
&= \sum_{i\geq 1} \frac{\left(-1\right)^{i-1}}{i} X^i = \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i + \sum_{i=n+1}^{\infty} \underbrace{\frac{\left(-1\right)^{i-1}}{i} X^i}_{\substack{\equiv 0 \bmod X^{n+1}k\left[\left[X\right]\right] \\ \text{(since } i \geq n+1 \text{ leads to} \\ X^i \equiv 0 \bmod X^{n+1}k\left[\left[X\right]\right)}} \\
&\equiv \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i + \underbrace{\sum_{i=n+1}^{\infty} 0}_{=0} = \sum_{i=1}^{n} \frac{\left(-1\right)^{i-1}}{i} X^i \bmod X^{n+1}k\left[\left[X\right]\right].
\end{aligned}$$

On the other hand, since $X \mid \log\left(1+X\right)$ in $k\left[\left[X\right]\right]$ (because $\log\left(1+X\right) = \sum\limits_{i\geq 1} \dfrac{\left(-1\right)^{i-1}}{i} \underbrace{X^i}_{=XX^{i-1}} = X \sum\limits_{i\geq 1} \dfrac{\left(-1\right)^{i-1}}{i} X^{i-1}$ is divisible by X), we have $X \mid \gamma \log\left(1+X\right)$ in $k\left[\left[X\right]\right]$. Thus, $X^j \mid \left(\gamma \log\left(1+X\right)\right)^j$ for every $j \in \mathbb{N}$. Thus every $j \in \mathbb{N}$ such that $j \geq n+1$ satisfies

$$\left(\gamma \log\left(1+X\right)\right)^j \equiv 0 \bmod X^{n+1}k\left[\left[X\right]\right] \tag{354}$$

(since $j \geq n+1$ leads to $X^{n+1} \mid X^j \mid \left(\gamma \log\left(1+X\right)\right)^j$). Now,

$$\begin{aligned}
\sum_{i\in\mathbb{N}} \binom{\gamma}{i} X^i &= \exp\left(\gamma \log\left(1+X\right)\right) = \sum_{j=0}^{\infty} \frac{\left(\gamma \log\left(1+X\right)\right)^j}{j!} \qquad \text{(by the definition of exp)} \\
&= \sum_{j=0}^{n} \frac{\left(\gamma \log\left(1+X\right)\right)^j}{j!} + \sum_{j=n+1}^{\infty} \underbrace{\frac{\left(\gamma \log\left(1+X\right)\right)^j}{j!}}_{\substack{\equiv 0 \bmod X^{n+1}k\left[\left[X\right]\right] \\ \text{(since } j \geq n+1 \text{ and thus} \\ \left(\gamma \log(1+X)\right)^j \equiv 0 \bmod X^{n+1}k\left[\left[X\right]\right] \\ \text{(by (354)))}}} \\
&\equiv \sum_{j=0}^{n} \frac{\left(\gamma \log\left(1+X\right)\right)^j}{j!} + \underbrace{\sum_{j=n+1}^{\infty} 0}_{=0} = \sum_{j=0}^{n} \frac{\left(\gamma \log\left(1+X\right)\right)^j}{j!} \\
&\equiv \sum_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{\left(-1\right)^{i-1}}{i} X^i\right)^j}{j!} \bmod X^{n+1}k\left[\left[X\right]\right]
\end{aligned} \tag{355}$$

(since $\log(1+X) \equiv \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i \bmod X^{n+1} k[[X]]$). On the other hand,

$$\sum_{i\in\mathbb{N}} \binom{\gamma}{i} X^i = \sum_{i=0}^{n} \binom{\gamma}{i} X^i + \sum_{i=n+1}^{\infty} \binom{\gamma}{i} \underbrace{X^i}_{\substack{\equiv 0 \bmod X^{n+1}k[[X]] \\ \text{(since } i \geq n+1\text{, and thus } X^{n+1} \mid X^i\text{)}}}$$
$$\equiv \sum_{i=0}^{n} \binom{\gamma}{i} X^i + \underbrace{\sum_{i=n+1}^{\infty} \binom{\gamma}{i} 0}_{=0} = \sum_{i=0}^{n} \binom{\gamma}{i} X^i \bmod X^{n+1} k[[X]],$$

so that

$$\sum_{i=0}^{n} \binom{\gamma}{i} X^i \equiv \sum_{i\in\mathbb{N}} \binom{\gamma}{i} X^i \equiv \sum_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!} \bmod X^{n+1} k[[X]]$$

(by (355)). Thus, $X^{n+1} \mid \sum\limits_{i=0}^{n} \binom{\gamma}{i} X^i - \sum\limits_{j=0}^{n} \dfrac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!}$ in $k[[X]]$. This means that the coefficient of the power series $\sum\limits_{i=0}^{n} \binom{\gamma}{i} X^i - \sum\limits_{j=0}^{n} \dfrac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!}$ before X^λ is 0 for every $\lambda \in \{0, 1, \ldots, n\}$. But the power series $\sum\limits_{i=0}^{n} \binom{\gamma}{i} X^i - \sum\limits_{j=0}^{n} \dfrac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!}$ is actually a polynomial, so this rewrites as follows: The coefficient of the polynomial $\sum\limits_{i=0}^{n} \binom{\gamma}{i} X^i - \sum\limits_{j=0}^{n} \dfrac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!}$ before X^λ is 0 for every $\lambda \in \{0, 1, \ldots, n\}$. In other words, $X^{n+1} \mid \sum\limits_{i=0}^{n} \binom{\gamma}{i} X^i - \sum\limits_{j=0}^{n} \dfrac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!}$ in $k[X]$. Hence, there exists a polynomial $\mathbf{Q} \in k[X]$ such that $\sum\limits_{i=0}^{n} \binom{\gamma}{i} X^i - \sum\limits_{j=0}^{n} \dfrac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!} = X^{n+1}\mathbf{Q}$. Consider this polynomial $\mathbf{Q}$.

Applying the polynomial identity $\sum\limits_{i=0}^{n} \binom{\gamma}{i} X^i - \sum\limits_{j=0}^{n} \dfrac{\left(\gamma \sum\limits_{i=1}^{n} \dfrac{(-1)^{i-1}}{i} X^i\right)^j}{j!} = X^{n+1}\mathbf{Q}$

to b instead of X, we get

$$\sum_{i=0}^{n}\binom{\gamma}{i}b^i-\sum_{j=0}^{n}\frac{\left(\gamma\sum\limits_{i=1}^{n}\dfrac{(-1)^{i-1}}{i}b^i\right)^j}{j!}=\underbrace{b^{n+1}}_{=0}\mathbf{Q}\left(b\right)=0,$$

so that $\sum\limits_{j=0}^{n}\dfrac{\left(\gamma\sum\limits_{i=1}^{n}\dfrac{(-1)^{i-1}}{i}b^i\right)^j}{j!}=\sum\limits_{i=0}^{n}\binom{\gamma}{i}b^i$. This proves Corollary 30.7. □

Proof of Theorem 30.5. Due to how we defined $\mathcal{L}^{n+1}\left(H,A\right)$ (in Definition 3.1 **(b)**), we have

$$\mathcal{L}^{n+1}\left(H,A\right)=\left\{f\in\mathcal{L}\left(H,A\right)\ \mid\ \underbrace{f\mid_{H_{\leq n+1-1}}}_{=f\mid_{H_{\leq n}}}=0\right\}=\left\{f\in\mathcal{L}\left(H,A\right)\ \mid\ f\mid_{H_{\leq n}}=0\right\}$$
$$=\left\{h\in\mathcal{L}\left(H,A\right)\ \mid\ h\mid_{H_{\leq n}}=0\right\}\qquad\text{(here, we renamed } f \text{ as } h\text{)}\quad(356)$$

for every $n\in\mathbb{N}$.

Let $F\in G\left(H,A\right)$. Let $n\in\mathbb{N}$.

According to Proposition 14.2 (applied to $n+1$ instead of n), the subset $\mathcal{L}^{n+1}\left(H,A\right)$ of $\mathcal{L}\left(H,A\right)$ is an ideal of $\mathcal{L}\left(H,A\right)$. Thus, there is a factor algebra $\mathcal{L}\left(H,A\right)/\mathcal{L}^{n+1}\left(H,A\right)$. For every $p\in\mathcal{L}\left(H,A\right)$, we are going to denote by $\overline{p}$ the projection of p to this factor algebra (i. e., the residue class of p modulo the ideal $\mathcal{L}^{n+1}\left(H,A\right)$). We are going to denote the multiplication in the factor algebra $\mathcal{L}\left(H,A\right)/\mathcal{L}^{n+1}\left(H,A\right)$ by the $*$ sign, and we are going to write q^{*i} for the i-th power of q (in the factor algebra $\mathcal{L}\left(H,A\right)/\mathcal{L}^{n+1}\left(H,A\right)$) whenever $q\in\mathcal{L}\left(H,A\right)/\mathcal{L}^{n+1}\left(H,A\right)$ and $i\in\mathbb{N}$.

Let $g=F-e_{H,A}$. Then, $g\in\mathfrak{g}\left(H,A\right)$ (since $F\in G\left(H,A\right)=e_{H,A}+\mathfrak{g}\left(H,A\right)$, so that $F-e_{H,A}\in\mathfrak{g}\left(H,A\right)$). Hence, Remark 3.5 (applied to g instead of f) yields $g^{*i}\left(H_{\leq n}\right)=0$ for every $i>n$.

Let $\varphi=\operatorname{Log}F$. Then, $\varphi=\operatorname{Log}F\in\mathfrak{g}\left(H,A\right)$, so that $\gamma\varphi\in\gamma\mathfrak{g}\left(H,A\right)\subseteq\mathfrak{g}\left(H,A\right)$ (because $\mathfrak{g}\left(H,A\right)$ is a k-vector space). Thus, Remark 3.5 (applied to $\gamma\varphi$ instead of f) yields $\left(\gamma\varphi\right)^{*i}\left(H_{\leq n}\right)=0$ for every $i>n$.

By the definition of Log, we have $\operatorname{Log}F=\operatorname{Log}_1\underbrace{\left(F-e_{H,A}\right)}_{=g}=\operatorname{Log}_1 g$. Hence, $\varphi=\operatorname{Log}f=\operatorname{Log}_1 g$.

Thus, every $x \in H_{\leq n}$ satisfies

$$\varphi(x) = (\operatorname{Log}_1 g)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} g^{*i}(x) \qquad \text{(by the definition of } \operatorname{Log}_1\text{)}$$

$$= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} \underbrace{g^{*i}(x)}_{\substack{=0 \text{ (since} \\ x \in H_{\leq n} \text{ and thus} \\ g^{*i}(x) \in g^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{))}}} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x) + \underbrace{\sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} 0}_{=0}$$

$$= \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}(x).$$

In other words,

$$\varphi\,|_{H_{\leq n}} = \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}}.$$

Now,

$$\left(\varphi - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} = \underbrace{\varphi\,|_{H_{\leq n}}}_{= \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}}} - \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}}$$

$$= \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} - \left(\sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right) |_{H_{\leq n}} = 0.$$

In other words,

$$\varphi - \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \in \left\{ h \in \mathcal{L}(H, A) \mid h\,|_{H_{\leq n}} = 0 \right\} = \mathcal{L}^{n+1}(H, A)$$

(by (356)). This rewrites as

$$\varphi \equiv \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \bmod \mathcal{L}^{n+1}(H, A). \tag{357}$$

But every $x \in H_{\leq n}$ satisfies

$$e^{*(\gamma\varphi)}(x) = \sum_{i \geq 0} \frac{(\gamma\varphi)^{*i}(x)}{i!} \qquad \left(\text{by the definition of } e^{*(\gamma\varphi)}\right)$$

$$= \sum_{i=0}^{n} \frac{(\gamma\varphi)^{*i}(x)}{i!} + \sum_{i=n+1}^{\infty} \underbrace{\frac{(\gamma\varphi)^{*i}(x)}{i!}}_{\substack{=0 \text{ (since} \\ x \in H_{\leq n} \text{ and thus} \\ (\gamma\varphi)^{*i}(x) \in (\gamma\varphi)^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{), so that} \\ (\gamma\varphi)^{*i}(x) = 0\text{)}}} = \sum_{i=0}^{n} \frac{(\gamma\varphi)^{*i}(x)}{i!} + \underbrace{\sum_{i=n+1}^{\infty} 0}_{=0} = \sum_{i=0}^{n} \frac{(\gamma\varphi)^{*i}(x)}{i!}$$

$$= \sum_{i=0}^{n} \frac{(\gamma\varphi)^{*i}}{i!}(x) = \sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!}(x) \qquad \text{(here, we substituted } j \text{ for } i \text{ in the sum)}.$$

In other words,

$$e^{*(\gamma\varphi)} \mid_{H_{\leq n}} = \left(\sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \right) \mid_{H_{\leq n}} .$$

But now,

$$\begin{aligned}
&\left(e^{*(\gamma\varphi)} - \sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \right) \mid_{H_{\leq n}} \\
&= \underbrace{e^{*(\gamma\varphi)} \mid_{H_{\leq n}}}_{= \left(\sum\limits_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \right) \mid_{H_{\leq n}}} - \left(\sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \right) \mid_{H_{\leq n}} \\
&= \left(\sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \right) \mid_{H_{\leq n}} - \left(\sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \right) \mid_{H_{\leq n}} = 0.
\end{aligned}$$

In other words,

$$e^{*(\gamma\varphi)} - \sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \in \left\{ h \in \mathcal{L}(H, A) \mid h \mid_{H_{\leq n}} = 0 \right\} = \mathcal{L}^{n+1}(H, A)$$

(by (356)). This rewrites as

$$e^{*(\gamma\varphi)} \equiv \sum_{j=0}^{n} \frac{(\gamma\varphi)^{*j}}{j!} \bmod \mathcal{L}^{n+1}(H, A) .$$

Substituting (357) into the right hand side of this congruence, we get

$$e^{*(\gamma\varphi)} \equiv \sum_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right)^{*j}}{j!} \bmod \mathcal{L}^{n+1}(H, A) . \tag{358}$$

But since $g^{*(n+1)} \mid_{H_{\leq n}} = 0$ (since Remark 3.5 (applied to $n+1$ and g instead of i and f) yields $g^{*(n+1)}(H_{\leq n}) = 0$), we have $g^{*(n+1)} \in \left\{ h \in \mathcal{L}(H, A) \mid h \mid_{H_{\leq n}} = 0 \right\} = \mathcal{L}^{n+1}(H, A)$ (by (356)). In other words, $g^{*(n+1)} \equiv 0 \bmod \mathcal{L}^{n+1}(H, A)$, so that $\overline{g^{*(n+1)}} = 0$. Thus, $\overline{g}^{*(n+1)} = \overline{g^{*(n+1)}} = 0$. Hence, we can apply Corollary 30.7 to $b = \overline{g}$ and obtain $\sum\limits_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} \overline{g}^{*i} \right)^{*j}}{j!} = \sum\limits_{i=0}^{n} \binom{\gamma}{i} \overline{g}^{*i}$ (where $\binom{\gamma}{i}$ is defined as in Definition 30.1). Thus,

$$\overline{\sum_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i} \right)^{*j}}{j!}} = \sum_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} \overline{g}^{*i} \right)^{*j}}{j!} = \sum_{i=0}^{n} \binom{\gamma}{i} \overline{g}^{*i} = \overline{\sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}}.$$

In other words,

$$\sum_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)^{*j}}{j!} \equiv \sum_{i=0}^{n} \binom{\gamma}{i} g^{*i} \bmod \mathcal{L}^{n+1}(H, A). \tag{359}$$

Next, we notice that Definition 30.3 yields

$$\operatorname{pow}_\gamma F = \operatorname{Pow}_\gamma \underbrace{(F - e_{H,A})}_{=g} = \operatorname{Pow}_\gamma g.$$

Thus, every $x \in H_{\leq n}$ satisfies

$$\begin{aligned}
\left(\operatorname{pow}_\gamma F\right)(x) &= \left(\operatorname{Pow}_\gamma g\right)(x) = \sum_{i \in \mathbb{N}} \binom{\gamma}{i} g^{*i}(x) && \text{(by (341), applied to } g \text{ instead of } f\text{)} \\
&= \sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}(x) + \sum_{i=n+1}^{\infty} \binom{\gamma}{i} \underbrace{g^{*i}(x)}_{\substack{=0 \text{ (since} \\ x \in H_{\leq n} \text{ and thus} \\ g^{*i}(x) \in g^{*i}\left(H_{\leq n}\right) = 0 \\ \text{(since } i > n\text{))}}} \\
&= \underbrace{\sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}(x)}_{= \left(\sum\limits_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)(x)} + \underbrace{\sum_{i=n+1}^{\infty} \binom{\gamma}{i} 0}_{=0} = \left(\sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)(x).
\end{aligned}$$

Thus,

$$\left(\operatorname{pow}_\gamma F\right)|_{H_{\leq n}} = \left(\sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)|_{H_{\leq n}}.$$

Now,

$$\begin{aligned}
\left(\operatorname{pow}_\gamma F - \sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)|_{H_{\leq n}} &= \underbrace{\left(\operatorname{pow}_\gamma F\right)|_{H_{\leq n}}}_{= \left(\sum\limits_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)|_{H_{\leq n}}} - \left(\sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)|_{H_{\leq n}} \\
&= \left(\sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)|_{H_{\leq n}} - \left(\sum_{i=0}^{n} \binom{\gamma}{i} g^{*i}\right)|_{H_{\leq n}} = 0.
\end{aligned}$$

In other words,

$$\operatorname{pow}_\gamma F - \sum_{i=0}^{n} \binom{\gamma}{i} g^{*i} \in \left\{h \in \mathcal{L}(H, A) \mid h|_{H_{\leq n}} = 0\right\} = \mathcal{L}^{n+1}(H, A)$$

(by (356)). This rewrites as

$$\operatorname{pow}_\gamma F \equiv \sum_{i=0}^{n} \binom{\gamma}{i} g^{*i} \bmod \mathcal{L}^{n+1}(H, A). \tag{360}$$

Hence,

$$\begin{aligned}\operatorname{pow}_\gamma F &\equiv \sum_{i=0}^{n} \binom{\gamma}{i} g^{*i} \equiv \sum_{j=0}^{n} \frac{\left(\gamma \sum\limits_{i=1}^{n} \frac{(-1)^{i-1}}{i} g^{*i}\right)^{*j}}{j!} && \text{(by (359))} \\ &\equiv e^{*(\gamma\varphi)} \bmod \mathcal{L}^{n+1}(H, A) && \text{(by (358))}.\end{aligned}$$

In other words,

$$\operatorname{pow}_\gamma F - e^{*(\gamma\varphi)} \in \mathcal{L}^{n+1}(H, A) = \left\{h \in \mathcal{L}(H, A) \mid h|_{H_{\leq n}} = 0\right\}$$

(by (356)). In other words, $\left(\operatorname{pow}_\gamma F - e^{*(\gamma\varphi)}\right)|_{H_{\leq n}} = 0$. Thus,

$$0 = \left(\operatorname{pow}_\gamma F - e^{*(\gamma\varphi)}\right)|_{H_{\leq n}} = \left(\operatorname{pow}_\gamma F\right)|_{H_{\leq n}} - e^{*(\gamma\varphi)}|_{H_{\leq n}},$$

so that $\left(\operatorname{pow}_\gamma F\right)|_{H_{\leq n}} = e^{*(\gamma\varphi)}|_{H_{\leq n}}$. Since $\varphi = \operatorname{Log} F$, this becomes $\left(\operatorname{pow}_\gamma F\right)|_{H_{\leq n}} = e^{*(\gamma \operatorname{Log} F)}|_{H_{\leq n}}$.

Now, forget that we fixed n. We have thus proven that

$$\left(\operatorname{pow}_\gamma F\right)|_{H_{\leq n}} = e^{*(\gamma \operatorname{Log} F)}|_{H_{\leq n}} \qquad \text{for every } n \in \mathbb{N}. \tag{361}$$

Now, let $x \in H$ be arbitrary. Since H is filtered, there must exist some $n \in \mathbb{N}$ such that $x \in H_{\leq n}$. Then,

$$\left(\operatorname{pow}_\gamma F\right)(x) = \underbrace{\left(\left(\operatorname{pow}_\gamma F\right)|_{H_{\leq n}}\right)}_{\substack{= e^{*(\gamma \operatorname{Log} F)}|_{H_{\leq n}} \\ \text{(by (361))}}}(x) = \left(e^{*(\gamma \operatorname{Log} F)}|_{H_{\leq n}}\right)(x) = e^{*(\gamma \operatorname{Log} F)}(x).$$

Now, forget that we fixed x. We have thus proven that every $x \in H$ satisfies $\left(\operatorname{pow}_\gamma F\right)(x) = e^{*(\gamma \operatorname{Log} F)}(x)$. In other words, $\operatorname{pow}_\gamma F = e^{*(\gamma \operatorname{Log} F)}$. We are thus done proving Theorem 30.5. □

Proof of Theorem 30.4. Let $f = \operatorname{Log} F$. Let $g = -f$. Then, $f + g = f + (-f) = 0$. Besides, from $f = \operatorname{Log} F$, we obtain $e^{*f} = e^{*(\operatorname{Log} F)} = F$ (by Proposition 5.13 **(b)**).

On the other hand, $f = \operatorname{Log} F \in \mathfrak{g}(H, A)$ and thus $g = -\underbrace{f}_{\in \mathfrak{g}(H,A)} \in -\mathfrak{g}(H, A) \subseteq \mathfrak{g}(H, A)$ (since $\mathfrak{g}(H, A)$ is a k-vector space). Also, $f * \underbrace{g}_{=-f} = f * (-f) = -f * f$ and $\underbrace{g}_{=-f} * f = (-f) * f = -f * f$, so that $f * g = -f * f = g * f$. Hence, Proposition 11.1 (applied to H and A instead of C and H) yields $e^{*(f+g)} = e^{*f} * e^{*g}$. Since $f + g = 0$ and $e^{*f} = F$, this rewrites as $e^{*0} = F * e^{*g}$.

Corollary 11.4 (applied to H, A and 0 instead of C, H and n) yields $e^{*(0f)} = \left(e^{*f}\right)^{*0}$. Since $0f = 0$ and $\left(e^{*f}\right)^{*0} = e_{H,A}$ (where $e_{H,A}$ is defined as in Definition 1.12), this rewrites as $e^{*0} = e_{H,A}$. Compared with $e^{*0} = F * e^{*g}$, this yields $F * e^{*g} = e_{H,A}$.

On the other hand, Proposition 11.1 (applied to g, f, H and A instead of f, g, C and H) yields $e^{*(g+f)} = e^{*g} * e^{*f}$. Since $g + f = f + g = 0$ and $e^{*f} = F$, this rewrites as $e^{*0} = e^{*g} * F$. Compared with $e^{*0} = e_{H,A}$, this yields $e^{*g} * F = e_{H,A}$.

Now, the map F has the $*$-inverse e^{*g} (since $F * e^{*g} = e_{H,A}$ and $e^{*g} * F = e_{H,A}$). Thus, F is $*$-invertible. This proves Theorem 30.4 **(a)**.

(b) Let $n \in \mathbb{Z}$. Since $f = \operatorname{Log} F$, we have

$$e^{*(nf)} = e^{*(n \operatorname{Log} F)} = \operatorname{pow}_n F \tag{362}$$

(because Theorem 30.5 (applied to $\gamma = n$) yields $\operatorname{pow}_n F = e^{*(n \operatorname{Log} F)}$).

We must be in one of the following two cases:

Case 1: We have $n \geq 0$.

Case 2: We have $n < 0$.

First, let us consider Case 1. In this case, $n \geq 0$, so that $n \in \mathbb{N}$, and thus Corollary 11.4 (applied to H and A instead of C and H) yields $e^{*(nf)} = \left(e^{*f}\right)^{*n}$. Since $e^{*(nf)} = \operatorname{pow}_n F$ (by (362)) and $e^{*f} = F$, this rewrites as $\operatorname{pow}_n F = F^{*n}$. Thus, Theorem 30.4 **(b)** is proven in Case 1.

Next, let us consider Case 2. In this case, $n < 0$, so that $-n > 0$ and thus $-n \in \mathbb{N}$. Hence, Corollary 11.4 (applied to $-n$, H and A instead of n, C and H) yields $e^{*((-n)f)} = \left(e^{*f}\right)^{*(-n)}$. Since $e^{*f} = F$, this rewrites as $e^{*((-n)f)} = F^{*(-n)}$. Thus, $\underbrace{e^{*((-n)f)}}_{=F^{*(-n)}} * e^{*(nf)} = F^{*(-n)} * e^{*(nf)}$.

Clearly, $(-n) \underbrace{f}_{\in \mathfrak{g}(H,A)} \in (-n)\,\mathfrak{g}(H,A) \subseteq \mathfrak{g}(H,A)$ (since $\mathfrak{g}(H,A)$ is a k-vector space) and $n \underbrace{f}_{\in \mathfrak{g}(H,A)} \in n\mathfrak{g}(H,A) \subseteq \mathfrak{g}(H,A)$ (since $\mathfrak{g}(H,A)$ is a k-vector space). Also, $((-n)\,f) * (nf) = -n^2\,(f * f) = (nf) * ((-n)\,f)$. Thus, Proposition 11.1 (applied to $(-n)\,f$, nf, H and A instead of f, g, C and H) yields $e^{*((-n)f+nf)} = e^{*(-nf)} * e^{*(nf)}$. Since $(-n)\,f + nf = 0$, this rewrites as $e^{*0} = e^{*(-nf)} * e^{*(nf)}$. Since $e^{*0} = e_{H,A}$, this rewrites as $e_{H,A} = e^{*(-nf)} * e^{*(nf)}$. Thus,

$$e_{H,A} = e^{*(-nf)} * e^{*(nf)} = F^{*(-n)} * e^{*(nf)},$$

so that

$$F^{*n} * \underbrace{e_{H,A}}_{=F^{*(-n)} * e^{*(nf)}} = \underbrace{F^{*n} * F^{*(-n)}}_{=e_{H,A}} * e^{*(nf)} = e_{H,A} * e^{*(nf)} = e^{*(nf)} = \operatorname{pow}_n F$$

(by (362)). Since $F^{*n} * e_{H,A} = F^{*n}$, this rewrites as $F^{*n} = \operatorname{pow}_n F$. In other words, $\operatorname{pow}_n F = F^{*n}$. Thus, Theorem 30.4 **(b)** is proven in Case 2.

We have thus proven Theorem 30.4 **(b)** in each of the cases 1 and 2. Since these two cases cover all possibilities, this yields that Theorem 30.4 **(b)** always holds. This completes the proof of Theorem 30.4. □

Another consequence of Theorem 30.5 is the following:

Theorem 30.8. Let k be a field of characteristic 0. Let $\gamma \in k$. Let A be a k-bialgebra, and let H be a connected filtered cocommutative k-coalgebra. Let $F \in G(H,A)$ be a k-coalgebra homomorphism. Then, $\operatorname{pow}_\gamma F$ is a k-coalgebra homomorphism.

Proof of Theorem 30.8. Let $f = \operatorname{Log} F$. Then, $f = \operatorname{Log} F \in \mathfrak{g}(H, A)$ and $e^{*f} = e^{*(\operatorname{Log} F)} = F$ (by Proposition 5.13 **(b)**). Since F is a k-coalgebra homomorphism, we know that e^{*f} is a k-coalgebra homomorphism (because $e^{*f} = F$). Thus, f is an $(\varepsilon, \varepsilon)$-coderivation (since Theorem 8.1 (applied to H and A instead of C and H) shows that f is an $(\varepsilon, \varepsilon)$-coderivation if and only if e^{*f} is a k-coalgebra homomorphism). Thus,

$$\Delta_A \circ f = (f \otimes e_{H,A} + e_{H,A} \otimes f) \circ \Delta_H$$

(because Definition 7.1 (applied to H and A instead of C and H) shows that f is an $(\varepsilon, \varepsilon)$-coderivation if and only if $\Delta_A \circ f = (f \otimes e_{H,A} + e_{H,A} \otimes f) \circ \Delta_H$). Hence,

$$\begin{aligned}
\Delta_A \circ (\gamma f) &= \gamma \cdot \underbrace{(\Delta_A \circ f)}_{=(f \otimes e_{H,A} + e_{H,A} \otimes f) \circ \Delta_H} && \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \gamma \cdot ((f \otimes e_{H,A} + e_{H,A} \otimes f) \circ \Delta_H) \\
&= \underbrace{(\gamma \cdot (f \otimes e_{H,A} + e_{H,A} \otimes f))}_{= \gamma \cdot (f \otimes e_{H,A}) + \gamma \cdot (e_{H,A} \otimes f)} \circ \Delta_H && \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \left(\underbrace{\gamma \cdot (f \otimes e_{H,A})}_{\substack{= (\gamma f) \otimes e_{H,A} \\ \text{(since tensoring of } k\text{-linear} \\ \text{maps is } k\text{-bilinear)}}} + \underbrace{\gamma \cdot (e_{H,A} \otimes f)}_{\substack{= e_{H,A} \otimes (\gamma f) \\ \text{(since tensoring of } k\text{-linear} \\ \text{maps is } k\text{-bilinear)}}} \right) \circ \Delta_H \\
&= ((\gamma f) \otimes e_{H,A} + e_{H,A} \otimes (\gamma f)) \circ \Delta_H.
\end{aligned}$$

Hence, γf is an $(\varepsilon, \varepsilon)$-coderivation (because Definition 7.1 (applied to γf, H and A instead of f, C and H) shows that γf is an $(\varepsilon, \varepsilon)$-coderivation if and only if $\Delta_A \circ (\gamma f) = ((\gamma f) \otimes e_{H,A} + e_{H,A} \otimes (\gamma f)) \circ \Delta_H)$. Since $\gamma \underbrace{f}_{\in \mathfrak{g}(H,A)} \in \gamma \mathfrak{g}(H, A) \subseteq \mathfrak{g}(H, A)$ (since $\mathfrak{g}(H, A)$ is a k-vector space), this yields that we can apply Theorem 8.1 to γf, H and A instead of f, C and H. As a result, we obtain that γf is an $(\varepsilon, \varepsilon)$-coderivation if and only if $e^{*(\gamma f)}$ is a k-coalgebra homomorphism. Since we know that γf is an $(\varepsilon, \varepsilon)$-coderivation, we thus conclude that $e^{*(\gamma f)}$ is a k-coalgebra homomorphism. Since

$$\begin{aligned}
e^{*(\gamma f)} &= e^{*(\gamma \operatorname{Log} F)} && \text{(because } f = \operatorname{Log} F\text{)} \\
&= \operatorname{pow}_\gamma F && \text{(by Theorem 30.5)},
\end{aligned}$$

this rewrites as follows: The map $\operatorname{pow}_\gamma F$ is a k-coalgebra homomorphism. This proves Theorem 30.8. $\square$

Here is the dual statement to Theorem 30.8 (although not precisely dual due to the presence of filtrations):

Theorem 30.9. Let k be a field of characteristic 0. Let $\gamma \in k$. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a commutative k-algebra. Let $F \in G(H, A)$ be a k-algebra homomorphism. Then, $\operatorname{pow}_\gamma F$ is a k-algebra homomorphism.

Proof of Theorem 30.9. Let $f = \operatorname{Log} F$. Then, $f = \operatorname{Log} F \in \mathfrak{g}(H, A)$ and $e^{*f} = e^{*(\operatorname{Log} F)} = F$ (by Proposition 5.13 **(b)**). Since F is a k-algebra homomorphism, we know that e^{*f} is a k-algebra homomorphism (because $e^{*f} = F$). Thus, f is an $(\varepsilon_H, \varepsilon_H)$-derivation (since Theorem 8.1 shows that f is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if e^{*f} is a k-algebra homomorphism). Thus,

$$f \circ \mu_H = \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f)$$

(because Definition 15.6 shows that f is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $f \circ \mu_H = \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f)$). Hence,

$$\begin{aligned}
(\gamma f) \circ \mu_H &= \gamma \cdot \underbrace{(f \circ \mu_H)}_{= \mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f)} && \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \gamma \cdot (\mu_A \circ (f \otimes e_{H,A} + e_{H,A} \otimes f)) \\
&= \mu_A \circ \underbrace{(\gamma \cdot (f \otimes e_{H,A} + e_{H,A} \otimes f))}_{= \gamma \cdot (f \otimes e_{H,A}) + \gamma \cdot (e_{H,A} \otimes f)} && \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \mu_A \circ \left(\underbrace{\gamma \cdot (f \otimes e_{H,A})}_{\substack{= (\gamma f) \otimes e_{H,A} \\ \text{(since tensoring of } k\text{-linear} \\ \text{maps is } k\text{-bilinear)}}} + \underbrace{\gamma \cdot (e_{H,A} \otimes f)}_{\substack{= e_{H,A} \otimes (\gamma f) \\ \text{(since tensoring of } k\text{-linear} \\ \text{maps is } k\text{-bilinear)}}} \right) \\
&= \mu_A \circ ((\gamma f) \otimes e_{H,A} + e_{H,A} \otimes (\gamma f)) .
\end{aligned}$$

Hence, γf is an $(\varepsilon_H, \varepsilon_H)$-derivation (because Definition 15.6 (applied to γf instead of f) shows that γf is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $(\gamma f) \circ \mu_H = \mu_A \circ ((\gamma f) \otimes e_{H,A} + e_{H,A} \otimes (\gamma f))$). Since $\gamma \underbrace{f}_{\in \mathfrak{g}(H,A)} \in \gamma \mathfrak{g}(H, A) \subseteq \mathfrak{g}(H, A)$ (since $\mathfrak{g}(H, A)$ is a k-vector space), this yields that we can apply Theorem 15.10 to γf instead of f. As a result, we obtain that γf is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $e^{*(\gamma f)}$ is a k-algebra homomorphism. Since we know that γf is an $(\varepsilon_H, \varepsilon_H)$-derivation, we thus conclude that $e^{*(\gamma f)}$ is a k-algebra homomorphism. Since

$$\begin{aligned}
e^{*(\gamma f)} &= e^{*(\gamma \operatorname{Log} F)} && \text{(because } f = \operatorname{Log} F) \\
&= \operatorname{pow}_\gamma F && \text{(by Theorem 30.5)} ,
\end{aligned}$$

this rewrites as follows: The map $\operatorname{pow}_\gamma F$ is a k-algebra homomorphism. This proves Theorem 30.9. $\square$

Next, we prove something fundamental:

Theorem 30.10. Let k be a field of characteristic 0. Let A be a graded k-algebra, and let H be a connected graded k-coalgebra.

(a) For every graded map $f \in \mathfrak{g}(H, A)$, the map e^{*f} is also graded.

(b) For every graded map $F \in G(H, A)$, the map $\operatorname{Log} F$ is also graded.

(c) For every $\gamma \in k$ and every graded map $F \in G(H, A)$, the map $\operatorname{pow}_\gamma F$ is also graded.

Proof of Theorem 30.10. First, we notice that the graded k-coalgebra H is connected. Thus, the filtered k-coalgebra H (defined as according to Convention 16.7) is connected (because Remark 16.11 (applied to $C = H$) yields that the graded k-coalgebra H is connected if and only if the filtered k-coalgebra H is connected).

Define $e_{H,A}$ as according to Definition 1.12.

(a) Let $f \in \mathfrak{g}(H, A)$ be a graded map. For every $i \in \mathbb{N}$, the map f^{*i} is graded (by Proposition 16.18 **(c)**, applied to $n = i$), and thus satisfies

$$f^{*i}(H_n) \subseteq A_n \qquad \text{for every } n \in \mathbb{N}. \tag{363}$$

Let $n \in \mathbb{N}$. Let $x \in H_n$.

By the definition of $H_{\leq n}$, we have $H_{\leq n} = \bigoplus_{\ell=0}^{n} H_\ell$. But since H_n is an addend of the direct sum $\bigoplus_{\ell=0}^{n} H_\ell$, we have $H_n \subseteq \bigoplus_{\ell=0}^{n} H_\ell = H_{\leq n}$. Thus, $x \in H_n \subseteq H_{\leq n}$.

Notice that

$$\text{every } i \in \mathbb{N} \text{ such that } i > n \text{ satisfies } f^{*i}(x) = 0 \tag{364}$$

(because every $i \in \mathbb{N}$ such that $i > n$ satisfies $x \in H_{\leq n}$ and thus $f^{*i}(x) \in f^{*i}(H_{\leq n}) = 0$ (by Remark 3.5), so that $f^{*i}(x) = 0$).

From (6), we have

$$e^{*f}(x) = \sum_{i \geq 0} \underbrace{\frac{f^{*i}(x)}{i!}}_{= \frac{1}{i!} f^{*i}(x)} = \sum_{i \geq 0} \frac{1}{i!} f^{*i}(x) = \sum_{i=0}^{n} \frac{1}{i!} f^{*i}\left(\underbrace{x}_{\in H_n}\right) + \sum_{i=n+1}^{\infty} \frac{1}{i!} \underbrace{f^{*i}(x)}_{\substack{=0 \text{ (because } i>n, \text{ and thus} \\ (364) \text{ yields } f^{*i}(x)=0)}}$$

$$\in \sum_{i=0}^{n} \frac{1}{i!} \underbrace{f^{*i}(H_n)}_{\substack{\subseteq A_n \\ \text{(by (363))}}} + \underbrace{\sum_{i=n+1}^{\infty} \frac{1}{i!} 0}_{=0} \subseteq \sum_{i=0}^{n} \frac{1}{i!} A_n \subseteq A_n$$

(since A_n is a k-vector space).

Now forget that we fixed x. We have thus proven that every $x \in H_n$ satisfies $e^{*f}(x) \in A_n$. In other words, $e^{*f}(H_n) \subseteq A_n$.

Now forget that we fixed n. We thus have proven that every $n \in \mathbb{N}$ satisfies $e^{*f}(H_n) \subseteq A_n$. In other words, e^{*f} is graded. This proves Theorem 30.10 **(a)**.

(b) Let $F \in G(H, A)$ be a graded map. Let $f = F - e_{H,A}$. Since $F \in G(H, A) = e_{H,A} + \mathfrak{g}(H, A)$, we have $F - e_{H,A} \in \mathfrak{g}(H, A)$, so that $f = F - e_{H,A} \in \mathfrak{g}(H, A)$.

For every $i \in \mathbb{N}$, the map f^{*i} is graded (by Proposition 16.18 **(c)**, applied to $n = i$), and thus satisfies

$$f^{*i}(H_n) \subseteq A_n \qquad \text{for every } n \in \mathbb{N}. \tag{365}$$

Let $n \in \mathbb{N}$. Let $x \in H_n$.

By the definition of $H_{\leq n}$, we have $H_{\leq n} = \bigoplus_{\ell=0}^{n} H_\ell$. But since H_n is an addend of the direct sum $\bigoplus_{\ell=0}^{n} H_\ell$, we have $H_n \subseteq \bigoplus_{\ell=0}^{n} H_\ell = H_{\leq n}$. Thus, $x \in H_n \subseteq H_{\leq n}$.

Notice that

$$\text{every } i \in \mathbb{N} \text{ such that } i > n \text{ satisfies } f^{*i}(x) = 0 \tag{366}$$

(because every $i \in \mathbb{N}$ such that $i > n$ satisfies $x \in H_{\leq n}$ and thus $f^{*i}(x) \in f^{*i}(H_{\leq n}) = 0$ (by Remark 3.5), so that $f^{*i}(x) = 0$).

From (8), we have

$$(\operatorname{Log}_1 f)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i}\left(\underbrace{x}_{\in H_n}\right) + \sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{\substack{=0 \text{ (because } i>n, \text{ and thus} \\ (366) \text{ yields } f^{*i}(x)=0)}}$$

$$\in \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(H_n)}_{\substack{\subseteq A_n \\ (\text{by (365)})}} + \underbrace{\sum_{i=n+1}^{\infty} \frac{(-1)^{i-1}}{i} 0}_{=0} \subseteq \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} A_n \subseteq A_n$$

(since A_n is a k-vector space).

Now forget that we fixed x. We have thus proven that every $x \in H_n$ satisfies $(\operatorname{Log}_1 f)(x) \in A_n$. In other words, $(\operatorname{Log}_1 f)(H_n) \subseteq A_n$.

Definition 3.8 yields $\operatorname{Log} F = \operatorname{Log}_1 \underbrace{(F - e_{H,A})}_{=f} = \operatorname{Log}_1 f$. Thus, $(\operatorname{Log} F)(H_n) = (\operatorname{Log}_1 f)(H_n) \subseteq A_n$.

Now forget that we fixed n. We thus have proven that every $n \in \mathbb{N}$ satisfies $(\operatorname{Log} F)(H_n) \subseteq A_n$. In other words, $\operatorname{Log} F$ is graded. This proves Theorem 30.10 **(b)**.

(c) Let $F \in G(H, A)$ be a graded map. Let $f = F - e_{H,A}$. Since $F \in G(H, A) = e_{H,A} + \mathfrak{g}(H, A)$, we have $F - e_{H,A} \in \mathfrak{g}(H, A)$, so that $f = F - e_{H,A} \in \mathfrak{g}(H, A)$.

For every $i \in \mathbb{N}$, the map f^{*i} is graded (by Proposition 16.18 **(c)**, applied to $n = i$), and thus satisfies

$$f^{*i}(H_n) \subseteq A_n \qquad \text{for every } n \in \mathbb{N}. \tag{367}$$

Let $n \in \mathbb{N}$. Let $x \in H_n$.

By the definition of $H_{\leq n}$, we have $H_{\leq n} = \bigoplus_{\ell=0}^{n} H_\ell$. But since H_n is an addend of the direct sum $\bigoplus_{\ell=0}^{n} H_\ell$, we have $H_n \subseteq \bigoplus_{\ell=0}^{n} H_\ell = H_{\leq n}$. Thus, $x \in H_n \subseteq H_{\leq n}$.

Notice that

$$\text{every } i \in \mathbb{N} \text{ such that } i > n \text{ satisfies } f^{*i}(x) = 0 \tag{368}$$

(because every $i \in \mathbb{N}$ such that $i > n$ satisfies $x \in H_{\leq n}$ and thus $f^{*i}(x) \in f^{*i}(H_{\leq n}) = 0$ (by Remark 3.5), so that $f^{*i}(x) = 0$).

From (341), we have

$$(\operatorname{Pow}_\gamma f)(x) = \sum_{i \in \mathbb{N}} \binom{\gamma}{i} f^{*i}(x) = \sum_{i=0}^{\infty} \binom{\gamma}{i} f^{*i}\left(\underbrace{x}_{\in H_n}\right) + \sum_{i=n+1}^{\infty} \binom{\gamma}{i} \underbrace{f^{*i}(x)}_{\substack{=0 \text{ (because } i>n, \text{ and thus} \\ (368) \text{ yields } f^{*i}(x)=0)}}$$

$$\in \sum_{i=0}^{n} \binom{\gamma}{i} \underbrace{f^{*i}(H_n)}_{\substack{\subseteq A_n \\ (\text{by (367)})}} + \underbrace{\sum_{i=n+1}^{\infty} \binom{\gamma}{i} 0}_{=0} \subseteq \sum_{i=0}^{n} \binom{\gamma}{i} A_n \subseteq A_n$$

(since A_n is a k-vector space).

Now forget that we fixed x. We have thus proven that every $x \in H_n$ satisfies $(\operatorname{Pow}_\gamma f)(x) \in A_n$. In other words, $(\operatorname{Pow}_\gamma f)(H_n) \subseteq A_n$.

Definition 30.3 yields $\operatorname{pow}_\gamma F = \operatorname{Pow}_\gamma \underbrace{(F - e_{H,A})}_{=f} = \operatorname{Pow}_\gamma f$. Thus, $\left(\operatorname{pow}_\gamma F\right)(H_n) = (\operatorname{Pow}_\gamma f)(H_n) \subseteq A_n$.

Now forget that we fixed n. We thus have proven that every $n \in \mathbb{N}$ satisfies $\left(\operatorname{pow}_\gamma F\right)(H_n) \subseteq A_n$. In other words, $\operatorname{pow}_\gamma F$ is graded. This proves Theorem 30.10 **(c)**. □

Definition 30.11. Let k be a field of characteristic 0. Let A be a k-algebra, and let H be a connected filtered k-algebra. Let $F \in G(H, A)$.

Whenever γ is an element of k, we will write $F^{*\gamma}$ for $\operatorname{pow}_\gamma F$. This notation does not conflict with the notation $F^{*\gamma}$ for the γ-th power of F with respect to convolution when γ is an integer. (In fact, the only case in which the former notation could conflict with the latter is when γ is an integer, but in this case Theorem 30.4 **(b)** shows that the two notations are equivalent.)

We can now generalize Theorem 28.2:

Theorem 30.12. Let k be a field of characteristic 0. Let H be a cocommutative connected graded k-Hopf algebra. Let S be the antipode of H. Define a map $E_H : H \to H$ according to Definition 27.1. Define a map $E_H^{\mathrm{inv}} : H \to H$ according to Definition 27.9. Let $\operatorname{Prim} H$ denote the subspace of H consisting of all primitive elements of H. Let $\alpha \in k$ and $\beta \in k$ satisfy $\alpha + \beta = 1$. Then, the map $E_H^{\mathrm{inv}} \circ \left(S^{*\alpha} * E_H * S^{*\beta}\right)$ is a projection from H to the subspace $\operatorname{Prim} H$.

Theorem 28.2 **(a)** easily follows from Theorem 30.12 when $\alpha = 0$ and $\beta = 1$. Theorem 28.1 **(b)** easily follows from Theorem 30.12 when $\alpha = 1$ and $\beta = 0$.

Proof of Theorem 30.12. Define the map $e_{H,H}$ as according to Definition 1.12.

It is easy to see that $S \in G(H, H)$ [163].

By the definition of $S^{*\alpha}$, we have $S^{*\alpha} = \operatorname{pow}_\alpha S$.

Since H is a graded k-Hopf algebra, the antipode of H is graded. Since the antipode of H is S, this yields that S is graded. Combined with $S \in G(H, H)$, this yields that we can apply Theorem 30.10 **(c)** to $A = H$, $\gamma = \alpha$ and $F = S$. As a result, we obtain that the map $\operatorname{pow}_\alpha S$ is graded.

By Definition 25.3, we have $H^{\mathrm{cop}} = (H, \tau_{H,H} \circ \Delta_H, \varepsilon_H)$. Since H is cocommutative, we have $\tau_{H,H} \circ \Delta_H = \Delta_H$. Thus, $H^{\mathrm{cop}} = \left(H, \underbrace{\tau_{H,H} \circ \Delta_H}_{=\Delta_H}, \varepsilon_H\right) = (H, \Delta_H, \varepsilon_H) = H$.

Proposition 25.4 yields that the antipode of H is a k-coalgebra homomorphism from H^{cop} to H. Since the antipode of H is the map S, whereas H^{cop} is H, this

[163] *Proof.* As in the proof of Corollary 28.10, we can show that $S(1_H) = 1_H$. Thus,

$$S \in \{f \in \mathcal{L}(H, H) \mid f(1_H) = 1_H\} = G(H, H)$$

(since $G(H, H) = \{f \in \mathcal{L}(H, H) \mid f(1_H) = 1_H\}$ by the definition of $G(H, H)$), qed.

rewrites as follows: The map S is a k-coalgebra homomorphism from H to H. Thus, Theorem 30.8 (applied to $A = H$, $\gamma = \alpha$ and $F = S$) yields that $\operatorname{pow}_\alpha S$ is a k-coalgebra homomorphism.

Altogether, we have now shown that the map $\operatorname{pow}_\alpha S$ is a graded k-coalgebra homomorphism. Since $\operatorname{pow}_\alpha S = S^{*\alpha}$, this rewrites as follows: The map $S^{*\alpha}$ is a graded k-coalgebra homomorphism. The same argument, but with α replaced by β, shows that the map $S^{*\beta}$ is a graded k-coalgebra homomorphism.

We have $S^{*\alpha} = \operatorname{pow}_\alpha S \in G(H,H)$ (because $\operatorname{pow}_\alpha F \in G(H,H)$ for every $F \in G(H,H)$ (due to the definition of $\operatorname{pow}_\alpha F$)). Thus,

$$S^{*\alpha} \in G(H,H) = \{f \in \mathcal{L}(H,H) \mid f(1_H) = 1_H\}$$

(by the definition of $G(H,H)$), so that $S^{*\alpha}(1_H) = 1_H$. The same argument, but with α replaced by β, shows that $S^{*\beta}(1_H) = 1_H$.

Recall that S is the antipode of H. Thus, S is the $*$-inverse of id_H (because the antipode of H is defined as the $*$-inverse of id_H). In other words, $S = \mathrm{id}_H^{*(-1)}$. Hence, S itself is $*$-invertible and satisfies $S^{*(-1)} = \mathrm{id}_H$. But Theorem 30.4 **(b)** (applied to $A = H$, $n = -1$ and $F = S$) yields $\operatorname{pow}_{-1} S = S^{*(-1)}$.

Now, Theorem 30.5 (applied to $A = H$, $\gamma = \alpha$ and $F = S$) yields $\operatorname{pow}_\alpha S = e^{*(\alpha \operatorname{Log} S)}$. By the definition of $S^{*\alpha}$, we have $S^{*\alpha} = \operatorname{pow}_\alpha S = e^{*(\alpha \operatorname{Log} S)}$.

Also, Theorem 30.5 (applied to $A = H$, $\gamma = -1$ and $F = S$) yields $\operatorname{pow}_{-1} S = e^{*((-1)\operatorname{Log} S)}$. Since $\operatorname{pow}_{-1} S = S^{*(-1)} = \mathrm{id}_H$ and $(-1)\operatorname{Log} S = -\operatorname{Log} S$, this rewrites as follows: $\mathrm{id}_H = e^{*(-\operatorname{Log} S)}$.

Also, Theorem 30.5 (applied to $A = H$, $\gamma = \beta$ and $F = S$) yields $\operatorname{pow}_\beta S = e^{*(\beta \operatorname{Log} S)}$. By the definition of $S^{*\beta}$, we have $S^{*\beta} = \operatorname{pow}_\beta S = e^{*(\beta \operatorname{Log} S)}$.

Since $\operatorname{Log} S \in \mathfrak{g}(H,H)$ (because $\operatorname{Log} F \in \mathfrak{g}(H,H)$ for every $F \in G(H,H)$ (due to the definition of $\operatorname{Log} F$)), the elements $\alpha \operatorname{Log} S$, $-\operatorname{Log} S$, $-\beta \operatorname{Log} S$ and $\beta \operatorname{Log} S$ must also lie in $\mathfrak{g}(H,H)$ (since $\mathfrak{g}(H,H)$ is a k-vector space).

Since $(\alpha \operatorname{Log} S) * (-\operatorname{Log} S) = -\alpha((\operatorname{Log} S) * (\operatorname{Log} S)) = (-\operatorname{Log} S) * (\alpha \operatorname{Log} S)$, we can apply Proposition 11.1 to $C = H$, $f = \alpha \operatorname{Log} S$ and $g = -\operatorname{Log} S$. As a result, we obtain

$$e^{*(\alpha \operatorname{Log} S + (-\operatorname{Log} S))} = \underbrace{e^{*(\alpha \operatorname{Log} S)}}_{=S^{*\alpha}} * \underbrace{e^{*(-\operatorname{Log} S)}}_{=\mathrm{id}_H} = S^{*\alpha} * \mathrm{id}_H .$$

Since $\alpha \operatorname{Log} S + (-\operatorname{Log} S) = \underbrace{(\alpha - 1)}_{\substack{=-\beta \\ (\text{since } \alpha+\beta=1)}} \operatorname{Log} S = -\beta \operatorname{Log} S$, this rewrites as follows:

$$e^{*(-\beta \operatorname{Log} S)} = S^{*\alpha} * \mathrm{id}_H . \tag{369}$$

On the other hand, since $(-\beta \operatorname{Log} S) * (\beta \operatorname{Log} S) = -\beta^2((\operatorname{Log} S) * (\operatorname{Log} S)) = (\beta \operatorname{Log} S) * (-\beta \operatorname{Log} S)$, we can apply Proposition 11.1 to $C = H$, $f = -\beta \operatorname{Log} S$ and $g = \beta \operatorname{Log} S$. As a result, we obtain

$$e^{*(-\beta \operatorname{Log} S + \beta \operatorname{Log} S)} = \underbrace{e^{*(-\beta \operatorname{Log} S)}}_{\substack{=S^{*\alpha} * \mathrm{id}_H \\ (\text{by (369)})}} * \underbrace{e^{*(\beta \operatorname{Log} S)}}_{=S^{*\beta}} = S^{*\alpha} * \mathrm{id}_H * S^{*\beta}.$$

Since $-\beta \operatorname{Log} S + \beta \operatorname{Log} S = 0$, this rewrites as

$$e^{*0} = S^{*\alpha} * \mathrm{id}_H * S^{*\beta}. \tag{370}$$

Corollary 11.4 (applied to H, A, 0 and 0 instead of C, H, f and n) yields $e^{*(0\cdot 0)} = (e^{*0})^{*0}$. Since $0 \cdot 0 = 0$ and $(e^{*0})^{*0} = e_{H,H}$, this rewrites as $e^{*0} = e_{H,H}$. Compared with (370), this yields

$$S^{*\alpha} * \mathrm{id}_H * S^{*\beta} = e_{H,H}.$$

Thus, we can apply Corollary 28.15 to $P = S^{*\alpha}$ and $Q = S^{*\beta}$. As a result, we can conclude that the map $E_H^{\mathrm{inv}} \circ \left(S^{*\alpha} * E_H * S^{*\beta}\right)$ is a projection from H to the subspace $\operatorname{Prim} H$. This proves Theorem 30.12. □

Here is the expectable dual of Theorem 30.12:

Theorem 30.13. Let k be a field of characteristic 0. Let H be a commutative connected graded k-Hopf algebra. Let S be the antipode of H. Define a map $E_H : H \to H$ according to Definition 27.1. Define a map $E_H^{\mathrm{inv}} : H \to H$ according to Definition 27.9. Let $\alpha \in k$ and $\beta \in k$ satisfy $\alpha + \beta = 1$. Then, the map $E_H^{\mathrm{inv}} \circ \left(S^{*\alpha} * E_H * S^{*\beta}\right)$ is a projection from H such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ \left(S^{*\alpha} * E_H * S^{*\beta}\right)\right) = k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2$. [164]

Theorem 29.2 **(a)** easily follows from Theorem 30.12 when $\alpha = 0$ and $\beta = 1$. Theorem 29.1 **(b)** easily follows from Theorem 30.12 when $\alpha = 1$ and $\beta = 0$.

Proof of Theorem 30.13. Define the map $e_{H,H}$ as according to Definition 1.12.

Just as in the proof of Theorem 30.12, we can see that $S \in G(H, H)$.

By the definition of $S^{*\alpha}$, we have $S^{*\alpha} = \operatorname{pow}_\alpha S$.

By Definition 26.3, we have $H^{\mathrm{op}} = (H, \mu_H \circ \tau_{H,H}, \eta_H)$. Since H is commutative, we have $\mu_H \circ \tau_{H,H} = \mu_H$. Thus, $H^{\mathrm{op}} = \left(H, \underbrace{\mu_H \circ \tau_{H,H}}_{=\mu_H}, \eta_H\right) = (H, \mu_H, \eta_H) = H$.

Proposition 26.4 yields that the antipode of H is a k-algebra homomorphism from H to H^{op}. Since the antipode of H is the map S, whereas H^{op} is H, this rewrites as follows: The map S is a k-algebra homomorphism from H to H.

Just as in the proof of Theorem 30.12, we can see that $\operatorname{pow}_\alpha S$ is graded.

Altogether, we have now shown that the map $\operatorname{pow}_\alpha S$ is a graded k-algebra homomorphism. Since $\operatorname{pow}_\alpha S = S^{*\alpha}$, this rewrites as follows: The map $S^{*\alpha}$ is a graded k-algebra homomorphism. The same argument, but with α replaced by β, shows that the map $S^{*\beta}$ is a graded k-algebra homomorphism.

Just as in the proof of Theorem 30.12, we can see that $S^{*\alpha} \in G(H, H)$ and $S^{*\alpha}(1_H) = 1_H$. The same argument, but with α replaced by β, shows that $S^{*\beta} \in G(H, H)$ and $S^{*\beta}(1_H) = 1_H$.

It is now easy to see that

$$\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(H_n) = 0 \qquad \text{for every } n \in \mathbb{N}. \tag{371}$$

[164] Recall that the notation $(\operatorname{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Hence, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

[165] Now, it is easy to conclude that $\varepsilon_H \circ S^{*\alpha} = \varepsilon_H$. [166] The same argument, but with α replaced by β, shows that $\varepsilon_H \circ S^{*\beta} = \varepsilon_H$.

Finally, just as in the proof of Theorem 30.12, we can prove that $S^{*\alpha} * \mathrm{id}_H * S^{*\beta} = e_{H,H}$.

Thus, we can apply Corollary 29.18 to $P = S^{*\alpha}$ and $Q = S^{*\beta}$. As a result, we can conclude that the map $E_H^{\mathrm{inv}} \circ \left(S^{*\alpha} * E_H * S^{*\beta}\right)$ is a projection such that $\mathrm{Ker}\left(E_H^{\mathrm{inv}} \circ \left(S^{*\alpha} * E_H * S^{*\beta}\right)\right) =$

---

[165] *Proof of (371):* Let $n \in \mathbb{N}$. Let $x \in H_n$. We are going to show that $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = 0$.

We must be in one of the following two cases:

Case 1: We have $n = 0$.

Case 2: We have $n > 0$.

Let us first consider Case 1. In this case, $n = 0$, so that $H_n = H_0 = k \cdot 1_H$ (by Proposition 29.14). Thus, $x \in H_n = k \cdot 1_H$. In other words, there exists some $\lambda \in k$ such that $x = \lambda \cdot 1_H$. Consider this λ. Then,

$$\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right) \underbrace{(x)}_{=\lambda \cdot 1_H} = \left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(\lambda \cdot 1_H) = \lambda \cdot \underbrace{\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(1_H)}_{=(\varepsilon_H \circ S^{*\alpha})(1_H) - \varepsilon_H(1_H)}$$

(since $\varepsilon_H \circ S^{*\alpha} - \varepsilon_H$ is k-linear)

$$= \lambda \cdot \left(\underbrace{\left(\varepsilon_H \circ S^{*\alpha}\right)(1_H)}_{=\varepsilon_H(S^{*\alpha}(1_H))} - \varepsilon_H(1_H) \right)$$

$$= \lambda \cdot \left(\varepsilon_H \left(\underbrace{S^{*\alpha}(1_H)}_{=1_H} \right) - \varepsilon_H(1_H) \right) = \lambda \cdot \underbrace{\left(\varepsilon_H(1_H) - \varepsilon_H(1_H)\right)}_{=0} = 0.$$

We have thus proven that $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = 0$ in Case 1.

Next, let us consider Case 2. In this case, $n > 0$, so that $\varepsilon_H(H_n) = 0$ (because H is a graded k-coalgebra). On the other hand, $S^{*\alpha}(H_n) \subseteq H_n$ (since $S^{*\alpha}$ is graded). Thus,

$$\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = \left(\varepsilon_H \circ S^{*\alpha}\right)(x) - \varepsilon_H(x) = \varepsilon_H\left(S^{*\alpha}\left(\underbrace{x}_{\in H_n}\right)\right) - \varepsilon_H\left(\underbrace{x}_{\in H_n}\right)$$

$$\in \varepsilon_H\left(\underbrace{S^{*\alpha}(H_n)}_{\subseteq H_n}\right) - \underbrace{\varepsilon_H(H_n)}_{=0} \subseteq \varepsilon_H(H_n) = 0,$$

so that $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = 0$. We have thus proven that $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = 0$ in Case 2.

Hence, $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = 0$ is proven in both cases 1 and 2. Since these two cases cover all possibilities, this yields that $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = 0$ always holds.

Now forget that we fixed x. We thus have shown that every $x \in H_n$ satisfies $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(x) = 0$. In other words, $\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(H_n) = 0$. This proves (371).

[166] *Proof.* Since H is graded, we have $H = \bigoplus_{n \in \mathbb{N}} H_n = \sum_{n \in \mathbb{N}} H_n$ (since direct sums are sums). Thus,

$$\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(H) = \left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)\left(\sum_{n \in \mathbb{N}} H_n\right)$$

$$= \sum_{n \in \mathbb{N}} \underbrace{\left(\varepsilon_H \circ S^{*\alpha} - \varepsilon_H\right)(H_n)}_{\substack{=0 \\ \text{(by (371))}}} \qquad \text{(since } \varepsilon_H \circ S^{*\alpha} - \varepsilon_H \text{ is } k\text{-linear)}$$

$$= \sum_{n \in \mathbb{N}} 0 = 0,$$

so that $\varepsilon_H \circ S^{*\alpha} - \varepsilon_H = 0$, and thus $\varepsilon_H \circ S^{*\alpha} = \varepsilon_H$, qed.

$k \cdot 1_H + (\operatorname{Ker}(\varepsilon_H))^2$. This proves Theorem 30.13. $\square$

§31. On convolution and composition

The following innocuous fact about convolution and composition will help us later in proving the Cartier-Milnor-Moore theorem:

Proposition 31.1. Let k be a field. Let C and D be k-coalgebras. Let A be a k-algebra. Let $\varphi : D \to C$ be a k-coalgebra homomorphism.

(a) Every $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$ satisfy $(f \circ \varphi) * (g \circ \varphi) = (f * g) \circ \varphi$.

(b) We have $e_{C,A} \circ \varphi = e_{D,A}$.

(c) Every $f \in \mathcal{L}(C, A)$ and $i \in \mathbb{N}$ satisfy $(f \circ \varphi)^{*i} = f^{*i} \circ \varphi$.

(d) Assume that the k-coalgebras C and D are connected filtered k-coalgebras. Assume further that the map $\varphi : D \to C$ satisfies $\varphi(1_D) = 1_C$. Assume finally that k is a field of characteristic 0. Then, every $f \in \mathfrak{g}(C, A)$ satisfies $f \circ \varphi \in \mathfrak{g}(D, A)$ and $e^{*(f \circ \varphi)} = e^{*f} \circ \varphi$.

(e) Assume that the k-coalgebras C and D are connected filtered k-coalgebras. Assume further that the map $\varphi : D \to C$ satisfies $\varphi(1_D) = 1_C$. Assume finally that k is a field of characteristic 0. Then, every $F \in G(C, A)$ satisfies $F \circ \varphi \in G(D, A)$ and $\operatorname{Log}(F \circ \varphi) = (\operatorname{Log} F) \circ \varphi$.

Proof of Proposition 31.1. **(a)** Let $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$. By the definition of the convolution $f * g$, we have

$$f * g = \mu_A \circ (f \otimes g) \circ \Delta_C.$$

By the definition of the convolution $(f \circ \varphi) * (g \circ \varphi)$, we have

$$\begin{aligned}
(f \circ \varphi) * (g \circ \varphi) &= \mu_A \circ \underbrace{((f \circ \varphi) \otimes (g \circ \varphi))}_{\substack{= (f \otimes g) \circ (\varphi \otimes \varphi) \\ \text{(by (21), applied to } U=D,\ V=C,\ W=A, \\ U'=D,\ V'=C,\ W'=A,\ \alpha=\varphi,\ \beta=f,\ \alpha'=\varphi \text{ and } \beta'=g)}} \circ \Delta_D \\
&= \mu_A \circ (f \otimes g) \circ \underbrace{(\varphi \otimes \varphi) \circ \Delta_D}_{\substack{= \Delta_C \circ \varphi \\ \text{(since } \varphi \text{ is a } k\text{-coalgebra} \\ \text{homomorphism)}}} = \underbrace{\mu_A \circ (f \otimes g) \circ \Delta_C}_{= f * g} \circ \varphi \\
&= (f * g) \circ \varphi.
\end{aligned}$$

This proves Proposition 31.1 **(a)**.

(b) By the definition of $e_{C,A}$, we have $e_{C,A} = \eta_A \circ \varepsilon_C$. By the definition of $e_{D,A}$, we have $e_{D,A} = \eta_A \circ \varepsilon_D$. Thus,

$$\underbrace{e_{C,A}}_{= \eta_A \circ \varepsilon_C} \circ \varphi = \eta_A \circ \underbrace{\varepsilon_C \circ \varphi}_{\substack{= \varepsilon_D \\ \text{(since } \varphi \text{ is a } k\text{-coalgebra} \\ \text{homomorphism)}}} = \eta_A \circ \varepsilon_D = e_{D,A}.$$

This proves Proposition 31.1 **(b)**.

(c) We are going to prove Proposition 31.1 **(c)** by induction over i:

Induction base: Every $f \in \mathcal{L}(C, A)$ satisfies

$$(f \circ \varphi)^{*0} = e_{D,A} = \underbrace{e_{C,A}}_{=f^{*0}} \circ \varphi \qquad \text{(by Proposition 31.1 (b))}$$
$$= f^{*0} \circ \varphi.$$

In other words, Proposition 31.1 **(c)** holds for $i = 0$. This completes the induction base.

Induction step: Let $I \in \mathbb{N}$. Assume that Proposition 31.1 **(c)** holds for $i = I$. We now must prove that Proposition 31.1 **(c)** holds for $i = I + 1$.

Every $f \in \mathcal{L}(C, A)$ satisfies $(f \circ \varphi)^{*I} = f^{*I} \circ \varphi$ (since Proposition 31.1 **(c)** holds for $i = I$). Now, every $f \in \mathcal{L}(C, A)$ satisfies

$$(f \circ \varphi)^{*(I+1)} = (f \circ \varphi)^{*(1+I)} = (f \circ \varphi) * \underbrace{(f \circ \varphi)^{*I}}_{=f^{*I} \circ \varphi} = (f \circ \varphi) * \left(f^{*I} \circ \varphi\right)$$
$$= \underbrace{\left(f * f^{*I}\right)}_{=f^{*(1+I)} = f^{*(I+1)}} \circ \varphi \qquad \left(\text{by Proposition 31.1 (a), applied to } g = f^{*I}\right)$$
$$= f^{*(I+1)} \circ \varphi.$$

In other words, Proposition 31.1 **(c)** holds for $i = I + 1$. This completes the induction step. The induction proof of Proposition 31.1 **(c)** is thus finished.

(d) For every connected filtered k-coalgebra H, we have

$$\mathfrak{g}(H, A) = \{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\} \qquad \text{(by the definition of } \mathfrak{g}(H, A))$$
$$= \{h \in \mathcal{L}(H, A) \mid h(1_H) = 0\} \tag{372}$$

(here, we renamed the index f as h).

Now, let $f \in \mathfrak{g}(C, A)$. Then,

$$f \in \mathfrak{g}(C, A) = \{h \in \mathcal{L}(C, A) \mid h(1_C) = 0\} \qquad \text{(by (372), applied to } H = C).$$

Hence, $f \in \mathcal{L}(C, A)$ and $f(1_C) = 0$. We have $f \circ \varphi \in \mathcal{L}(D, A)$ and

$$(f \circ \varphi)(1_D) = f\left(\underbrace{\varphi(1_D)}_{=1_C}\right) = f(1_C) = 0.$$

Hence, $f \circ \varphi \in \{h \in \mathcal{L}(D, A) \mid h(1_D) = 0\}$. Applying (372) to $H = D$, we obtain $\mathfrak{g}(D, A) = \{h \in \mathcal{L}(D, A) \mid h(1_D) = 0\}$. Thus, $f \circ \varphi \in \{h \in \mathcal{L}(D, A) \mid h(1_D) = 0\} = \mathfrak{g}(D, A)$. Hence, $e^{*(f \circ \varphi)}$ is well-defined.

Let $x \in D$. By the definition of $e^{*(f \circ \varphi)}$, we have $e^{*(f \circ \varphi)}(x) = \sum_{i \geq 0} \dfrac{(f \circ \varphi)^{*i}(x)}{i!}$.

By the definition of e^{*f}, we have $e^{*f}(y) = \sum_{i \geq 0} \dfrac{f^{*i}(y)}{i!}$ for every $y \in C$. Applying

this to $y = \varphi(x)$, we obtain

$$e^{*f}(\varphi(x))$$
$$= \sum_{i \geq 0} \frac{f^{*i}(\varphi(x))}{i!} = \sum_{i \geq 0} \frac{(f \circ \varphi)^{*i}(x)}{i!}$$
$$\left(\text{since every } i \in \mathbb{N} \text{ satisfies } f^{*i}(\varphi(x)) = \underbrace{\left(f^{*i} \circ \varphi\right)}_{\substack{=(f\circ\varphi)^{*i} \\ \text{(by Proposition 31.1 (c))}}}(x) = (f \circ \varphi)^{*i}(x) \right)$$
$$= e^{*(f\circ\varphi)}(x).$$

Thus, $e^{*(f\circ\varphi)}(x) = e^{*f}(\varphi(x)) = \left(e^{*f} \circ \varphi\right)(x)$.

Now, forget that we fixed x. We thus have proven that $e^{*(f\circ\varphi)}(x) = \left(e^{*f} \circ \varphi\right)(x)$ for every $x \in D$. In other words, $e^{*(f\circ\varphi)} = e^{*f} \circ \varphi$. This proves Proposition 31.1 **(d)**.

(e) For every connected filtered k-coalgebra H, we have

$$G(H,A) = \{f \in \mathcal{L}(H,A) \mid f(1_H) = 1_A\} \qquad \text{(by the definition of } G(H,A)\text{)}$$
$$= \{h \in \mathcal{L}(H,A) \mid h(1_H) = 1_A\} \tag{373}$$

(here, we renamed the index f as h).

Now, let $F \in G(C,A)$. Then,

$$F \in G(C,A) = \{h \in \mathcal{L}(C,A) \mid h(1_C) = 1_A\} \qquad \text{(by (373), applied to } H = C\text{)}.$$

Hence, $F \in \mathcal{L}(C,A)$ and $F(1_C) = 1_A$. We have $F \circ \varphi \in \mathcal{L}(D,A)$ and

$$(F \circ \varphi)(1_D) = F\left(\underbrace{\varphi(1_D)}_{=1_C}\right) = F(1_C) = 1_A.$$

Hence, $F \circ \varphi \in \{h \in \mathcal{L}(D,A) \mid h(1_D) = 1_A\}$. Applying (373) to $H = D$, we obtain $G(D,A) = \{h \in \mathcal{L}(D,A) \mid h(1_D) = 1_A\}$. Thus, $F\circ\varphi \in \{h \in \mathcal{L}(D,A) \mid h(1_D) = 1_A\} = G(D,A)$. Hence, $\operatorname{Log}(F \circ \varphi)$ is well-defined.

Let $f = F - e_{C,A}$. Since $f = F - e_{C,A}$, we have

$$f \circ \varphi = (F - e_{C,A}) \circ \varphi = F \circ \varphi - \underbrace{e_{C,A}}_{\substack{=\eta_A\circ\varepsilon_C \\ \text{(by the definition of } e_{C,A}\text{)}}} \circ\varphi$$
$$= F \circ \varphi - \eta_A \circ \underbrace{\varepsilon_C \circ \varphi}_{\substack{=\varepsilon_D \\ \text{(since } \varphi \text{ is a } k\text{-coalgebra homomorphism)}}} = F \circ \varphi - \underbrace{\eta_A \circ \varepsilon_D}_{\substack{=e_{D,A} \\ \text{(since } e_{D,A}=\eta_A\circ\varepsilon_D \\ \text{(by the definition of } e_{D,A}\text{))}}}$$
$$= F \circ \varphi - e_{D,A}.$$

Let $x \in D$. By the definition of $\operatorname{Log}(F \circ \varphi)$, we have $\operatorname{Log}(F \circ \varphi) = \operatorname{Log}_1\left(\underbrace{F \circ \varphi - e_{D,A}}_{=f\circ\varphi}\right) =$ $\operatorname{Log}_1(f \circ \varphi)$. Thus,

$$(\operatorname{Log}(F \circ \varphi))(x) = (\operatorname{Log}_1(f \circ \varphi))(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} (f \circ \varphi)^{*i}(x)$$

(by the definition of $\operatorname{Log}_1(f \circ \varphi)$).

By the definition of $\operatorname{Log} F$, we have $\operatorname{Log} F = \operatorname{Log}_1 \left(\underbrace{F - e_{C,A}}_{=f} \right) = \operatorname{Log}_1 f$. Hence, for every $y \in C$, we have

$$(\operatorname{Log} F)(y) = (\operatorname{Log}_1 f)(y) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(y)$$

(by the definition of $\operatorname{Log}_1 f$). Applying this to $y = \varphi(x)$, we obtain

$$\begin{aligned}
&(\operatorname{Log} F)(\varphi(x)) \\
&= \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(\varphi(x)) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} (f \circ \varphi)^{*i}(x) \\
&\qquad \left(\text{since every } i \in \mathbb{N} \text{ satisfies } f^{*i}(\varphi(x)) = \underbrace{\left(f^{*i} \circ \varphi\right)}_{\substack{=(f \circ \varphi)^{*i} \\ \text{(by Proposition 31.1 (c))}}}(x) = (f \circ \varphi)^{*i}(x) \right) \\
&= (\operatorname{Log}(F \circ \varphi))(x).
\end{aligned}$$

Thus, $(\operatorname{Log}(F \circ \varphi))(x) = (\operatorname{Log} F)(\varphi(x)) = ((\operatorname{Log} F) \circ \varphi)(x)$.

Now, forget that we fixed x. We thus have proven that $(\operatorname{Log}(F \circ \varphi))(x) = ((\operatorname{Log} F) \circ \varphi)(x)$ for every $x \in D$. In other words, $\operatorname{Log}(F \circ \varphi) = (\operatorname{Log} F) \circ \varphi$. This proves Proposition 31.1 **(e)**. □

The following proposition is "more or less" a dual of Proposition 31.1:

Proposition 31.2. Let k be a field. Let A and B be k-algebras. Let C be a k-coalgebra. Let $\psi : A \to B$ be a k-algebra homomorphism.

(a) Every $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$ satisfy $(\psi \circ f) * (\psi \circ g) = \psi \circ (f * g)$.

(b) We have $\psi \circ e_{C,A} = e_{C,B}$.

(c) Every $f \in \mathcal{L}(C, A)$ and $i \in \mathbb{N}$ satisfy $(\psi \circ f)^{*i} = \psi \circ f^{*i}$.

(d) Assume that the k-coalgebra C is a connected filtered k-coalgebra. Assume finally that k is a field of characteristic 0. Then, every $f \in \mathfrak{g}(C, A)$ satisfies $\psi \circ f \in \mathfrak{g}(C, B)$ and $e^{*(\psi \circ f)} = \psi \circ e^{*f}$.

(e) Assume that the k-coalgebra C is a connected filtered k-coalgebra. Assume finally that k is a field of characteristic 0. Then, every $F \in G(C, A)$ satisfies $\psi \circ F \in G(C, B)$ and $\operatorname{Log}(\psi \circ F) = \psi \circ (\operatorname{Log} F)$.

Notice that the conditions in Proposition 31.2 **(d)** and **(e)** are a bit more liberal than those in Proposition 31.1 **(d)** and **(e)**, whence it would not be proper to call Proposition 31.2 a precise dual of Proposition 31.1; but these conditions were technical in the first place, allowing one to define $e^{*(f \circ \varphi)}$ respectively $\operatorname{Log}(F \circ \varphi)$.

Proof of Proposition 31.2. **(a)** Let $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$. By the definition of the convolution $f * g$, we have

$$f * g = \mu_A \circ (f \otimes g) \circ \Delta_C.$$

By the definition of the convolution $(\psi \circ f) * (\psi \circ g)$, we have

$$\begin{aligned}(\psi \circ f) * (\psi \circ g) &= \mu_B \circ \underbrace{((\psi \circ f) \otimes (\psi \circ g))}_{\substack{=(\psi \otimes \psi) \circ (f \otimes g) \\ \text{(by (21), applied to } U=C,\ V=A,\ W=B, \\ U'=C,\ V'=A,\ W'=B,\ \alpha=f,\ \beta=\psi,\ \alpha'=g \text{ and } \beta'=\psi)}} \circ \Delta_C \\ &= \underbrace{\mu_B \circ (\psi \otimes \psi)}_{\substack{=\psi \circ \mu_A \\ \text{(since } \psi \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} \circ (f \otimes g) \circ \Delta_C = \psi \circ \underbrace{\mu_A \circ (f \otimes g) \circ \Delta_C}_{=f*g} = \psi \circ (f * g).\end{aligned}$$

This proves Proposition 31.2 **(a)**.

(b) By the definition of $e_{C,A}$, we have $e_{C,A} = \eta_A \circ \varepsilon_C$. By the definition of $e_{C,B}$, we have $e_{C,B} = \eta_B \circ \varepsilon_C$. Thus,

$$\psi \circ \underbrace{e_{C,A}}_{=\eta_A \circ \varepsilon_C} = \underbrace{\psi \circ \eta_A}_{\substack{=\eta_B \\ \text{(since } \psi \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} \circ \varepsilon_C = \eta_B \circ \varepsilon_C = e_{C,B}.$$

This proves Proposition 31.2 **(b)**.

(c) We are going to prove Proposition 31.2 **(c)** by induction over i:

Induction base: Every $f \in \mathcal{L}(C, A)$ satisfies

$$\begin{aligned}(f \circ \psi)^{*0} &= e_{C,B} = \psi \circ \underbrace{e_{C,A}}_{=f^{*0}} \qquad \text{(by Proposition 31.2 } \mathbf{(b)}\text{)} \\ &= \psi \circ f^{*0}.\end{aligned}$$

In other words, Proposition 31.2 **(c)** holds for $i = 0$. This completes the induction base.

Induction step: Let $I \in \mathbb{N}$. Assume that Proposition 31.2 **(c)** holds for $i = I$. We now must prove that Proposition 31.2 **(c)** holds for $i = I + 1$.

Every $f \in \mathcal{L}(C, A)$ satisfies $(\psi \circ f)^{*I} = \psi \circ f^{*I}$ (since Proposition 31.2 **(c)** holds for $i = I$). Now, every $f \in \mathcal{L}(C, A)$ satisfies

$$\begin{aligned}(\psi \circ f)^{*(I+1)} &= (\psi \circ f)^{*(1+I)} = (\psi \circ f) * \underbrace{(\psi \circ f)^{*I}}_{=\psi \circ f^{*I}} = (\psi \circ f) * \left(\psi \circ f^{*I}\right) \\ &= \psi \circ \underbrace{\left(f * f^{*I}\right)}_{=f^{*(1+I)}=f^{*(I+1)}} \qquad \left(\text{by Proposition 31.2 } \mathbf{(a)}\text{, applied to } g = f^{*I}\right) \\ &= \psi \circ f^{*(I+1)}.\end{aligned}$$

In other words, Proposition 31.2 **(c)** holds for $i = I + 1$. This completes the induction step. The induction proof of Proposition 31.2 **(c)** is thus finished.

(d) For every connected filtered k-coalgebra H and any k-algebra $\mathfrak{A}$, we have

$$\begin{aligned}\mathfrak{g}(H,\mathfrak{A}) &= \{f \in \mathcal{L}(H,\mathfrak{A}) \mid f(1_H) = 0\} && \text{(by the definition of } \mathfrak{g}(H,\mathfrak{A})) \\ &= \{h \in \mathcal{L}(H,\mathfrak{A}) \mid h(1_H) = 0\} && (374)\end{aligned}$$

(here, we renamed the index f as h).

Now, let $f \in \mathfrak{g}(C,A)$. Then,

$$f \in \mathfrak{g}(C,A) = \{h \in \mathcal{L}(C,A) \mid h(1_C) = 0\} \qquad \text{(by (374), applied to } H = C \text{ and } \mathfrak{A} = A).$$

Hence, $f \in \mathcal{L}(C,A)$ and $f(1_C) = 0$. We have $\psi \circ f \in \mathcal{L}(C,B)$ and

$$(\psi \circ f)(1_C) = \psi\left(\underbrace{f(1_C)}_{=0}\right) = \psi(0) = 0$$

(since ψ is k-linear). Hence, $\psi \circ f \in \{h \in \mathcal{L}(C,B) \mid h(1_C) = 0\}$. Applying (374) to $H = C$ and $\mathfrak{A} = B$, we obtain $\mathfrak{g}(C,B) = \{h \in \mathcal{L}(C,B) \mid h(1_C) = 0\}$. Thus, $\psi \circ f \in \{h \in \mathcal{L}(C,B) \mid h(1_C) = 0\} = \mathfrak{g}(C,B)$. Hence, $e^{*(\psi \circ f)}$ is well-defined.

Let $x \in C$. By the definition of $e^{*(\psi \circ f)}$, we have $e^{*(\psi \circ f)}(x) = \sum\limits_{i \geq 0} \dfrac{(\psi \circ f)^{*i}(x)}{i!}$.

By the definition of e^{*f}, we have $e^{*f}(x) = \sum\limits_{i \geq 0} \dfrac{f^{*i}(x)}{i!}$. Notice that the sum $\sum\limits_{i \geq 0} \dfrac{f^{*i}(x)}{i!}$ converges with respect to the discrete topology. Now,

$$\begin{aligned}\psi\left(e^{*f}(x)\right) &= \psi\left(\sum_{i \geq 0} \frac{f^{*i}(x)}{i!}\right) && \left(\text{since } e^{*f}(x) = \sum_{i \geq 0} \frac{f^{*i}(x)}{i!}\right) \\ &= \sum_{i \geq 0} \frac{\psi\left(f^{*i}(x)\right)}{i!} && \left(\begin{array}{c}\text{since } \psi \text{ is } k\text{-linear, and since the sum } \sum\limits_{i \geq 0} \dfrac{f^{*i}(x)}{i!} \\ \text{converges with respect to the discrete topology}\end{array}\right) \\ &= \sum_{i \geq 0} \frac{(\psi \circ f)^{*i}(x)}{i!} \\ &\qquad \left(\text{since every } i \in \mathbb{N} \text{ satisfies } \psi\left(f^{*i}(x)\right) = \underbrace{\left(\psi \circ f^{*i}\right)}_{\substack{=(\psi \circ f)^{*i} \\ \text{(by Proposition 31.2 (c))}}}(x) = (\psi \circ f)^{*i}(x)\right) \\ &= e^{*(\psi \circ f)}(x).\end{aligned}$$

Thus, $e^{*(\psi \circ f)}(x) = \psi\left(e^{*f}(x)\right) = \left(\psi \circ e^{*f}\right)(x)$.

Now, forget that we fixed x. We thus have proven that $e^{*(\psi \circ f)}(x) = \left(\psi \circ e^{*f}\right)(x)$ for every $x \in C$. In other words, $e^{*(\psi \circ f)} = \psi \circ e^{*f}$. This proves Proposition 31.2 **(d)**.

(e) For every connected filtered k-coalgebra H and any k-algebra $\mathfrak{A}$, we have

$$\begin{aligned}G(H,\mathfrak{A}) &= \{f \in \mathcal{L}(H,\mathfrak{A}) \mid f(1_H) = 1_{\mathfrak{A}}\} && \text{(by the definition of } G(H,\mathfrak{A})) \\ &= \{h \in \mathcal{L}(H,\mathfrak{A}) \mid h(1_H) = 1_{\mathfrak{A}}\} && (375)\end{aligned}$$

(here, we renamed the index f as h).

Now, let $F \in G(C, A)$. Then,

$$F \in G(C,A) = \{h \in \mathcal{L}(C,A) \mid h(1_C) = 1_A\} \qquad \text{(by (375), applied to } H = C \text{ and } \mathfrak{A} = A\text{)}.$$

Hence, $F \in \mathcal{L}(C, A)$ and $F(1_C) = 1_A$. We have $\psi \circ F \in \mathcal{L}(C, B)$ and

$$(\psi \circ F)(1_C) = \psi\left(\underbrace{F(1_C)}_{=1_A}\right) = \psi(1_A) = 1_B$$

(since ψ is a k-algebra homomorphism). Hence, $\psi \circ F \in \{h \in \mathcal{L}(C, B) \mid h(1_C) = 1_B\}$. Applying (375) to $H = C$ and $\mathfrak{A} = B$, we obtain $G(C, B) = \{h \in \mathcal{L}(C, B) \mid h(1_C) = 1_B\}$. Thus, $\psi \circ F \in \{h \in \mathcal{L}(C, B) \mid h(1_C) = 1_B\} = G(C, B)$. Hence, $\operatorname{Log}(\psi \circ F)$ is well-defined.

Let $f = F - e_{C,A}$. Since $f = F - e_{C,A}$, we have

$$\begin{aligned}
\psi \circ f &= \psi \circ (F - e_{C,A}) = \psi \circ F - \psi \circ \underbrace{e_{C,A}}_{\substack{=\eta_A \circ \varepsilon_C \\ \text{(by the definition of } e_{C,A}\text{)}}} \\
&\qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\
&= \psi \circ F - \underbrace{\psi \circ \eta_A}_{\substack{=\eta_B \\ \text{(since } \psi \text{ is a } k\text{-algebra homomorphism)}}} \circ \varepsilon_C = \psi \circ F - \underbrace{\eta_B \circ \varepsilon_C}_{\substack{=e_{C,B} \\ \text{(since } e_{C,B} = \eta_B \circ \varepsilon_C \\ \text{(by the definition of } e_{C,B}\text{))}}} \\
&= \psi \circ F - e_{C,B}.
\end{aligned}$$

Let $x \in C$. By the definition of $\operatorname{Log}(\psi \circ F)$, we have $\operatorname{Log}(\psi \circ F) = \operatorname{Log}_1\left(\underbrace{\psi \circ F - e_{C,B}}_{=\psi \circ f}\right) = \operatorname{Log}_1(\psi \circ f)$. Thus,

$$(\operatorname{Log}(\psi \circ F))(x) = (\operatorname{Log}_1(\psi \circ f))(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} (\psi \circ f)^{*i}(x)$$

(by the definition of $\operatorname{Log}_1(\psi \circ f)$).

By the definition of $\operatorname{Log} F$, we have $\operatorname{Log} F = \operatorname{Log}_1\left(\underbrace{F - e_{C,A}}_{=f}\right) = \operatorname{Log}_1 f$. Hence,

$$(\operatorname{Log} F)(x) = (\operatorname{Log}_1 f)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$$

(by the definition of $\operatorname{Log}_1 f$). Notice that the sum $\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ converges with

respect to the discrete topology. Now,

$$\begin{aligned}
&\psi\left(\left(\operatorname{Log} F\right)(x)\right) \\
&= \psi\left(\sum_{i\geq 1}\frac{(-1)^{i-1}}{i} f^{*i}(x)\right) \qquad \left(\text{since } \left(\operatorname{Log} F\right)(x) = \sum_{i\geq 1}\frac{(-1)^{i-1}}{i} f^{*i}(x)\right) \\
&= \sum_{i\geq 1}\frac{(-1)^{i-1}}{i}\psi\left(f^{*i}(x)\right) \qquad \left(\begin{array}{c}\text{since } \psi \text{ is } k\text{-linear, and since the sum } \sum\limits_{i\geq 1}\dfrac{(-1)^{i-1}}{i} f^{*i}(x) \\ \text{converges with respect to the discrete topology}\end{array}\right) \\
&= \sum_{i\geq 1}\frac{(-1)^{i-1}}{i}\left(\psi\circ f\right)^{*i}(x) \\
&\qquad \left(\text{since every } i\in\mathbb{N} \text{ satisfies } \psi\left(f^{*i}(x)\right) = \underbrace{\left(\psi\circ f^{*i}\right)}_{\substack{=(\psi\circ f)^{*i} \\ \text{(by Proposition 31.2 (c))}}}(x) = \left(\psi\circ f\right)^{*i}(x)\right) \\
&= \left(\operatorname{Log}\left(\psi\circ F\right)\right)(x).
\end{aligned}$$

Thus, $\left(\operatorname{Log}\left(\psi\circ F\right)\right)(x) = \psi\left(\left(\operatorname{Log} F\right)(x)\right) = \left(\psi\circ\left(\operatorname{Log} F\right)\right)(x)$.

Now, forget that we fixed x. We thus have proven that $\left(\operatorname{Log}\left(\psi\circ F\right)\right)(x) = \left(\psi\circ\left(\operatorname{Log} F\right)\right)(x)$ for every $x\in C$. In other words, $\operatorname{Log}\left(\psi\circ F\right) = \psi\circ\left(\operatorname{Log} F\right)$. This proves Proposition 31.2 **(e)**. □

We record, for future use, a consequence of Lemma 15.12:

Corollary 31.3. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a commutative k-algebra. Let $F: H\to A$ be a k-algebra homomorphism. Let $x\in H$ and $y\in H$ satisfy $\varepsilon_H(x) = 0$ and $\varepsilon_H(y) = 0$. Then, $\operatorname{Log} F$ is a well-defined element of $\mathfrak{g}(H, A)$ and satisfies $\left(\operatorname{Log} F\right)(xy) = 0$.

Proof of Corollary 31.3. Recall that $G(H,A) = \{f\in\mathcal{L}(H,A) \mid f(1_H) = 1_A\}$ (by the definition of $G(H,A)$). But F is a k-algebra homomorphism, and thus satisfies $F(1_H) = 1_A$. Now,

$$\begin{aligned}
F &\in \{f\in\mathcal{L}(H,A) \mid f(1_H) = 1_A\} \qquad (\text{since } F\in\mathcal{L}(H,A) \text{ and } F(1_H) = 1_A) \\
&= G(H,A).
\end{aligned}$$

Hence, $\operatorname{Log} F$ is a well-defined element of $\mathfrak{g}(H,A)$.

It remains to prove that $\left(\operatorname{Log} F\right)(xy) = 0$.

Let $f = \operatorname{Log} F$. Thus, $e^{*f} = e^{*(\operatorname{Log} F)} = F$ (by Proposition 5.13 **(b)**). Hence, e^{*f} is a k-algebra homomorphism (since we know that F is a k-algebra homomorphism).

We have $f = \operatorname{Log} F\in\mathfrak{g}(H,A)$. Hence, Lemma 15.12 yields that e^{*f} is a k-algebra homomorphism if and only if f is an $(\varepsilon_H,\varepsilon_H)$-derivation. Thus, f is an $(\varepsilon_H,\varepsilon_H)$-derivation (since we know that e^{*f} is a k-algebra homomorphism).

From Definition 15.7, we know that f is an $(\varepsilon_H,\varepsilon_H)$-derivation if and only if every $(a,b)\in H\times H$ satisfies $f(ab) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\,f(b)$. Hence, every $(a,b)\in$

$H \times H$ satisfies $f(ab) = f(a)\,\varepsilon_H(b) + \varepsilon_H(a)\,f(b)$ (because f is an $(\varepsilon_H, \varepsilon_H)$-derivation). Applying this to $(a,b) = (x,y)$, we obtain

$$f(xy) = f(x)\underbrace{\varepsilon_H(y)}_{=0} + \underbrace{\varepsilon_H(x)}_{=0} f(y) = 0 + 0 = 0.$$

Since $f = \operatorname{Log} F$, this rewrites as $(\operatorname{Log} F)(xy) = 0$. This completes the proof of Corollary 31.3. $\square$

As the following proposition shows, the commutativity requirement on A in Corollary 31.3 can be replaced by a commutativity requirement on H:

Corollary 31.4. Let k be a field of characteristic 0. Let H be a commutative connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a k-algebra. Let $F : H \to A$ be a k-algebra homomorphism. Let $x \in H$ and $y \in H$ satisfy $\varepsilon_H(x) = 0$ and $\varepsilon_H(y) = 0$. Then, $\operatorname{Log} F$ is a well-defined element of $\mathfrak{g}(H, A)$ and satisfies $(\operatorname{Log} F)(xy) = 0$.

Proof of Corollary 31.4. First of all, $F \in G(H, A)$ (this can be proven just as in the proof of Corollary 31.3). Thus, $\operatorname{Log} F$ is a well-defined element of $\mathfrak{g}(H, A)$.

We now need to prove that $(\operatorname{Log} F)(xy) = 0$.

Since $F : H \to A$ is a k-algebra homomorphism, its image $F(H)$ is a k-subalgebra of A. This k-subalgebra $F(H)$ is commutative[167].

Every $x \in H$ satisfies $F\left(\underbrace{x}_{\in H}\right) \in F(H)$. Thus, we can define a map $\widetilde{F} : H \to F(H)$ by

$$\left(\widetilde{F}(x) = F(x) \qquad \text{for every } x \in H\right).$$

This map $\widetilde{F}$ is a k-algebra homomorphism[168]. Hence, $\widetilde{F}(1_H) = 1_{F(H)}$. As a conse-

[167] *Proof.* Let $\alpha \in F(H)$ and $\beta \in F(H)$.

Since $\alpha \in F(H)$, there exists an $\widetilde{\alpha} \in H$ such that $\alpha = F(\widetilde{\alpha})$. Consider this $\widetilde{\alpha}$.

Since $\beta \in F(H)$, there exists a $\widetilde{\beta} \in H$ such that $\beta = F\left(\widetilde{\beta}\right)$. Consider this $\widetilde{\beta}$.

Since H is commutative, we have $\widetilde{\alpha}\widetilde{\beta} = \widetilde{\beta}\widetilde{\alpha}$. Now, multiplying the equalities $\alpha = F(\widetilde{\alpha})$ and $\beta = F\left(\widetilde{\beta}\right)$, we obtain $\alpha\beta = F(\widetilde{\alpha})\,F\left(\widetilde{\beta}\right) = F\left(\widetilde{\alpha}\widetilde{\beta}\right)$ (since F is a k-algebra homomorphism). Multiplying the equalities $\beta = F\left(\widetilde{\beta}\right)$ and $\alpha = F(\widetilde{\alpha})$, we obtain $\beta\alpha = F\left(\widetilde{\beta}\right)F(\widetilde{\alpha}) = F\left(\widetilde{\beta}\widetilde{\alpha}\right)$ (since F is a k-algebra homomorphism). Thus, $\alpha\beta = F\left(\underbrace{\widetilde{\alpha}\widetilde{\beta}}_{=\widetilde{\beta}\widetilde{\alpha}}\right) = F\left(\widetilde{\beta}\widetilde{\alpha}\right) = \beta\alpha$.

Now, forget that we fixed α and β. We thus have shown that every $\alpha \in F(H)$ and $\beta \in F(H)$ satisfy $\alpha\beta = \beta\alpha$. In other words, the k-algebra $F(H)$ is commutative, qed.

[168] *Proof.* Let $\lambda \in k$, $\mu \in k$, $a \in H$ and $b \in H$. By the definition of $\widetilde{F}$, we have the equalities $\widetilde{F}(\lambda a + \mu b) = F(\lambda a + \mu b)$, $\widetilde{F}(a) = F(a)$ and $\widetilde{F}(b) = F(b)$. Now,

$$\begin{aligned}\widetilde{F}(\lambda a + \mu b) &= F(\lambda a + \mu b) = \lambda \underbrace{F(a)}_{=\widetilde{F}(a)} + \mu \underbrace{F(b)}_{=\widetilde{F}(b)} \qquad \text{(since } F \text{ is a } k\text{-algebra homomorphism)} \\ &= \lambda \widetilde{F}(a) + \mu \widetilde{F}(b).\end{aligned}$$

quence, $\widetilde{F} \in G(H, F(H))$ [169].

Let ι be the canonical inclusion $F(H) \to A$. Clearly, ι is a k-algebra homomorphism. Moreover, $\iota \circ \widetilde{F} = F$ [170].

Proposition 31.2 **(e)** (applied to H, $F(H)$, A, $\widetilde{F}$ and ι instead of C, A, B, F and ψ) yields that $\iota \circ \widetilde{F} \in G(H, A)$ and $\operatorname{Log}\left(\iota \circ \widetilde{F}\right) = \iota \circ \left(\operatorname{Log} \widetilde{F}\right)$.

Now, Corollary 31.3 (applied to $F(H)$ and $\widetilde{F}$ instead of A and F) yields that $\operatorname{Log} \widetilde{F}$ is a well-defined element of $\mathfrak{g}(H, F(H))$ and satisfies $\left(\operatorname{Log} \widetilde{F}\right)(xy) = 0$.

Since $F = \iota \circ \widetilde{F}$, we have $\operatorname{Log} F = \operatorname{Log}\left(\iota \circ \widetilde{F}\right) = \iota \circ \left(\operatorname{Log} \widetilde{F}\right)$, so that

$$(\operatorname{Log} F)(xy) = \left(\iota \circ \left(\operatorname{Log} \widetilde{F}\right)\right)(xy) = \iota\left(\underbrace{\left(\operatorname{Log} \widetilde{F}\right)(xy)}_{=0}\right) = \iota(0) = 0$$

(since ι is just an inclusion map). This completes the proof of Corollary 31.4. $\square$

Now, forget that we fixed λ, μ, a and b. We thus have shown that $\widetilde{F}(\lambda a + \mu b) = \lambda \widetilde{F}(a) + \mu \widetilde{F}(b)$ for all $\lambda \in k$, $\mu \in k$, $a \in H$ and $b \in H$. In other words, the map $\widetilde{F}$ is k-linear.

Since $F(H)$ is a k-subalgebra of A, we have $1_{F(H)} = 1_A$. Now, by the definition of $\widetilde{F}$, we have

$$\begin{aligned} \widetilde{F}(1_H) &= F(1_H) = 1_A \qquad \text{(since } F \text{ is a } k\text{-algebra homomorphism)} \\ &= 1_{F(H)}. \end{aligned}$$

Moreover, any $a \in H$ and $b \in H$ satisfy

$$\begin{aligned} \widetilde{F}(ab) &= F(ab) \qquad \left(\text{by the definition of } \widetilde{F}\right) \\ &= \underbrace{F(a)}_{\substack{=\widetilde{F}(a) \\ (\text{since } \widetilde{F}(a)=F(a) \\ (\text{by the definition of } \widetilde{F}))}} \underbrace{F(b)}_{\substack{=\widetilde{F}(b) \\ (\text{since } \widetilde{F}(b)=F(b) \\ (\text{by the definition of } \widetilde{F}))}} \qquad \text{(since } F \text{ is a } k\text{-algebra homomorphism)} \\ &= \widetilde{F}(a)\, \widetilde{F}(b). \end{aligned}$$

Combining this with the fact that $\widetilde{F}(1_H) = 1_{F(H)}$, we conclude that $\widetilde{F}$ is a k-algebra homomorphism (since $\widetilde{F}$ is k-linear), qed.

[169] *Proof.* Recall that $G(H, F(H)) = \left\{f \in \mathcal{L}(H, F(H)) \mid f(1_H) = 1_{F(H)}\right\}$ (by the definition of $G(H, F(H))$). Now,

$$\begin{aligned} \widetilde{F} &\in \left\{f \in \mathcal{L}(H, F(H)) \mid f(1_H) = 1_{F(H)}\right\} \qquad \left(\text{since } F \in \mathcal{L}(H, F(H)) \text{ and } F(1_H) = 1_{F(H)}\right) \\ &= G(H, F(H)), \end{aligned}$$

qed.

[170] *Proof.* Every $x \in H$ satisfies

$$\begin{aligned} \left(\iota \circ \widetilde{F}\right)(x) &= \iota\left(\widetilde{F}(x)\right) = \widetilde{F}(x) \qquad \text{(since } \iota \text{ is just an inclusion map)} \\ &= F(x) \qquad \left(\text{by the definition of } \widetilde{F}\right). \end{aligned}$$

In other words, $\iota \circ \widetilde{F} = F$, qed.

§32. The spaces $\operatorname{symp}_n V$ are spanned by n-th powers

We are now going to take a closer look at the vector spaces $\operatorname{symp}_n V$ defined in Definition 17.11 **(c)**. The backbone of this will be the following algebraic identity:

Theorem 32.1. Let A be a ring. Let $n \in \mathbb{N}$. Let v_1, v_2, ..., v_n be n elements of A. For every set X, let $\mathcal{P}(X)$ denote the power set of X. Then,

$$\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} = \sum_{S \in \mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left(\sum_{s \in S} v_s \right)^n .$$

It is possible to derive Theorem 32.1 from known facts (such as Lemma 1 in [Grinbe08]), but it is more in the spirit of this note to give a self-contained proof.[171] This is what we are going to do now, after we have shown the following simple lemma:

Lemma 32.2. Let A be a finite set. Let B be a subset of A. Let $n \in \mathbb{Z}$.

(a) If $B \neq A$, then

$$\sum_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S}} (-1)^{n-|S|} = 0.$$

(b) If $B = A$ and $n = |A|$, then

$$\sum_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S}} (-1)^{n-|S|} = 1.$$

Proof of Lemma 32.2. **(a)** Assume that $B \neq A$. If we had $A \subseteq B$, then we would have $B = A$ (because $A \subseteq B$ and $B \subseteq A$), contradicting $B \neq A$. Hence, we cannot have $A \subseteq B$. Thus, $A \not\subseteq B$. Hence, there exists an $x \in A$ such that $x \notin B$. Consider such an x.

Let $\mathbf{P}_1 = \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \notin W\}$ and $\mathbf{P}_2 = \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \in W\}$.

For every $S \in \mathbf{P}_1$, we have $S \cup \{x\} \in \mathbf{P}_2$ [172]. Hence, we can define a map $\rho_1 : \mathbf{P}_1 \to \mathbf{P}_2$ by

$$(\rho_1(S) = S \cup \{x\} \qquad \text{for all } S \in \mathbf{P}_1).$$

Consider this map ρ_1.

[171] Notice that Theorem 32.1 also appears as Exercise 6.50 **(c)** in [Grinbe17].

[172] *Proof.* Let $S \in \mathbf{P}_1$.

Since $S \in \mathbf{P}_1 = \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \notin W\}$, we have $S \in \mathcal{P}(A)$ and $B \subseteq S$ and $x \notin S$. Since $S \in \mathcal{P}(A)$, we have $S \subseteq A$. Combining $S \subseteq A$ with $\{x\} \subseteq A$ (because $x \in A$), we obtain $S \cup \{x\} \subseteq A$. In other words, $S \cup \{x\} \in \mathcal{P}(A)$. Also, $B \subseteq S \subseteq S \cup \{x\}$ and $x \in \{x\} \subseteq S \cup \{x\}$.

Altogether, we have thus shown that $S \cup \{x\} \in \mathcal{P}(A)$, that $B \subseteq S \cup \{x\}$ and $x \in S \cup \{x\}$. In other words, $S \cup \{x\} \in \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \in W\} = \mathbf{P}_2$, qed.

For every $S \in \mathbf{P}_2$, we have $S \setminus \{x\} \in \mathbf{P}_1$ [173]. Hence, we can define a map $\rho_2 : \mathbf{P}_2 \to \mathbf{P}_1$ by

$$(\rho_2(S) = S \setminus \{x\} \qquad \text{for all } S \in \mathbf{P}_2).$$

Consider this map ρ_2.

We have $\rho_1 \circ \rho_2 = \mathrm{id}$ [174] and $\rho_2 \circ \rho_1 = \mathrm{id}$ [175]. Hence, the maps ρ_1 and ρ_2 are mutually inverse. Thus, ρ_1 is a bijection from $\mathbf{P}_1$ to $\mathbf{P}_2$.

Notice that

$$(-1)^{n-|\rho_1(S)|} = -(-1)^{n-|S|} \qquad \text{for every } S \in \mathbf{P}_1 \tag{376}$$

[176].

---

[173] *Proof.* Let $S \in \mathbf{P}_2$.

Since $S \in \mathbf{P}_2 = \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \in W\}$, we have $S \in \mathcal{P}(A)$ and $B \subseteq S$ and $x \in S$. Since $S \in \mathcal{P}(A)$, we have $S \subseteq A$. Now, $S \setminus \{x\} \subseteq S \subseteq A$. In other words, $S \setminus \{x\} \in \mathcal{P}(A)$. Also, $B \setminus \{x\} = B$ (since $x \notin B$), so that $B = \underbrace{B}_{\subseteq S} \setminus \{x\} \subseteq S \setminus \{x\}$. Finally, $x \notin S \setminus \{x\}$.

Altogether, we have thus shown that $S \setminus \{x\} \in \mathcal{P}(A)$, that $B \subseteq S \setminus \{x\}$ and $x \notin S \setminus \{x\}$. In other words, $S \setminus \{x\} \in \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \notin W\} = \mathbf{P}_1$, qed.

[174] *Proof.* Let $S \in \mathbf{P}_2$ be arbitrary. Then, $S \in \mathbf{P}_2 = \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \in W\}$. In other words, $S \in \mathcal{P}(A)$ and $B \subseteq S$ and $x \in S$. Since $x \in S$, we have $\{x\} \subseteq S$.

Any two sets X and Y with $Y \subseteq X$ satisfy $(X \setminus Y) \cup Y = X$. Applying this to $X = S$ and $Y = \{x\}$, we obtain $(S \setminus \{x\}) \cup \{x\} = S$ (since $\{x\} \subseteq S$).

By the definition of ρ_1, we have $\rho_1(\rho_2(S)) = \underbrace{\rho_2(S)}_{=S\setminus\{x\}} \cup \{x\} = (S \setminus \{x\}) \cup \{x\} = S$. Thus, $(\rho_1 \circ \rho_2)(S) = \rho_1(\rho_2(S)) = S = \mathrm{id}(S)$.

Now, forget that we fixed S. We thus have shown that $(\rho_1 \circ \rho_2)(S) = \mathrm{id}(S)$ for every $S \in \mathbf{P}_2$. In other words, $\rho_1 \circ \rho_2 = \mathrm{id}$, qed.

[175] *Proof.* Let $S \in \mathbf{P}_1$ be arbitrary. Then, $S \in \mathbf{P}_1 = \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \notin W\}$. In other words, $S \in \mathcal{P}(A)$ and $B \subseteq S$ and $x \notin S$. Since $x \notin S$, we have $S \setminus \{x\} = S$.

By the definition of ρ_2, we have $\rho_2(\rho_1(S)) = \underbrace{\rho_1(S)}_{=S\cup\{x\}} \setminus \{x\} = (S \cup \{x\}) \setminus \{x\} = (S \setminus \{x\}) \cup \underbrace{(\{x\} \setminus \{x\})}_{=\varnothing} = S \setminus \{x\} = S$. Thus, $(\rho_2 \circ \rho_1)(S) = \rho_2(\rho_1(S)) = S = \mathrm{id}(S)$.

Now, forget that we fixed S. We thus have shown that $(\rho_2 \circ \rho_1)(S) = \mathrm{id}(S)$ for every $S \in \mathbf{P}_1$. In other words, $\rho_2 \circ \rho_1 = \mathrm{id}$, qed.

[176] *Proof of (376):* Let $S \in \mathbf{P}_1$. Then, $S \in \mathbf{P}_1 = \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \notin W\}$. In other words, $S \in \mathcal{P}(A)$ and $B \subseteq S$ and $x \notin S$. The set S is disjoint from $\{x\}$ (since $x \notin S$).

Any two disjoint finite sets X and Y satisfy $|X \cup Y| = |X| + |Y|$. Applying this to $X = S$ and $Y = \{x\}$, we obtain $|S \cup \{x\}| = |S| + |\{x\}|$ (since S is disjoint from $\{x\}$).

Now, $\rho_1(S) = S \cup \{x\}$, so that $|\rho_1(S)| = |S \cup \{x\}| = |S| + \underbrace{|\{x\}|}_{=1} = |S| + 1$, hence

$$(-1)^{n-|\rho_1(S)|} = (-1)^{n-(|S|+1)} = (-1)^{n-|S|-1} = \frac{(-1)^{n-|S|}}{-1} = -(-1)^{n-|S|}.$$

This proves (376).

Now, every $S \in \mathcal{P}(A)$ satisfies either $x \in S$ or $x \notin S$. Hence,

$$\sum_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S}} (-1)^{n-|S|} = \underbrace{\sum_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S; \\ x \in S}} (-1)^{n-|S|}}_{\substack{= \sum\limits_{S \in \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \in W\}} \\ = \sum\limits_{S \in \mathbf{P}_2} \\ \text{(since } \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \in W\} = \mathbf{P}_2\text{)}}} + \underbrace{\sum_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S; \\ x \notin S}} (-1)^{n-|S|}}_{\substack{= \sum\limits_{S \in \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \notin W\}} \\ = \sum\limits_{S \in \mathbf{P}_1} \\ \text{(since } \{W \in \mathcal{P}(A) \mid B \subseteq W;\ x \notin W\} = \mathbf{P}_1\text{)}}}$$

$$= \sum_{S \in \mathbf{P}_2} (-1)^{n-|S|} + \sum_{S \in \mathbf{P}_1} (-1)^{n-|S|}$$

$$= \sum_{S \in \mathbf{P}_1} \underbrace{(-1)^{n-|\rho_1(S)|}}_{\substack{= -(-1)^{n-|S|} \\ \text{(by (376))}}} + \sum_{S \in \mathbf{P}_1} (-1)^{n-|S|}$$

$$\left(\begin{array}{c} \text{here, we substituted } \rho_1(S) \text{ for } S \text{ in the first sum, since } \rho_1 \\ \text{is a bijection from } \mathbf{P}_1 \text{ to } \mathbf{P}_2 \end{array} \right)$$

$$= \sum_{S \in \mathbf{P}_1} \left(-(-1)^{n-|S|} \right) + \sum_{S \in \mathbf{P}_1} (-1)^{n-|S|}$$

$$= \sum_{S \in \mathbf{P}_1} \underbrace{\left(-(-1)^{n-|S|} + (-1)^{n-|S|} \right)}_{=0} = \sum_{S \in \mathbf{P}_1} 0 = 0.$$

This proves Lemma 32.2 **(a)**.

(b) Assume that $B = A$ and $n = |A|$. For every $S \in \mathcal{P}(A)$, the assertions $B \subseteq S$ and $S = A$ are equivalent[177]. Hence, we can replace the sign $\sum\limits_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S}}$ by $\sum\limits_{\substack{S \in \mathcal{P}(A); \\ S = A}}$ in $\sum\limits_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S}} (-1)^{n-|S|}$. Consequently,

$$\sum_{\substack{S \in \mathcal{P}(A); \\ B \subseteq S}} (-1)^{n-|S|} = \sum_{\substack{S \in \mathcal{P}(A); \\ S = A}} (-1)^{n-|S|} = (-1)^{n-|A|} \qquad (\text{since } A \in \mathcal{P}(A))$$

$$= (-1)^0 \qquad \left(\text{since } \underbrace{n}_{=|A|} - |A| = |A| - |A| = 0 \right)$$

$$= 1.$$

This proves Lemma 32.2 **(b)**. □

[177] *Proof.* Let $S \in \mathcal{P}(A)$. We need to prove that the assertions $B \subseteq S$ and $S = A$ are equivalent.

First, assume that $B \subseteq S$ holds. Combining $S \subseteq A$ (since $S \in \mathcal{P}(A)$) with $A = B \subseteq S$, we obtain $S = A$. Now, forget that we assumed that $B \subseteq S$ holds. We thus have shown that if $B \subseteq S$, then $S = A$.

On the other hand, if $S = A$, then $B \subseteq S$ (because if $S = A$, then $B = A = S$).

Altogether, we know that if $S = A$, then $B \subseteq S$, and we know that if $B \subseteq S$, then $S = A$. In other words, each of the two assertions $B \subseteq S$ and $S = A$ implies the other. In other words, the assertions $B \subseteq S$ and $S = A$ are equivalent, qed.

Proof of Theorem 32.1. Let us first introduce some notations and make some preliminary observations.

For any sets X and Y, let $\operatorname{Map}(X, Y)$ denote the set of all maps from X to Y.

It is known that for any nonnegative integer m and any set T, the m-tuples of elements of T are in bijection with the maps from $\{1, 2, \ldots, m\}$ to T. More precisely: If m is a nonnegative integer and T is a set, then there is a bijection

$$\operatorname{Map}(\{1, 2, \ldots, m\}, T) \to T^{\times m}$$

which sends every map $f \in \operatorname{Map}(\{1, 2, \ldots, m\}, T)$ to the m-tuple $(f(1), f(2), \ldots, f(m)) \in T^{\times m}$. This bijection will be denoted by $\operatorname{tuple}_{T,m}$. [178] Thus,

$$\operatorname{tuple}_{T,m}(f) = (f(1), f(2), \ldots, f(m)) \qquad \text{for every } f \in \operatorname{Map}(\{1, 2, \ldots, m\}, T). \tag{377}$$

For any nonnegative integer m and any two sets X and Y satisfying $Y \subseteq X$, we regard $Y^{\times m}$ as a subset of $X^{\times m}$ in the obvious way.

For any nonnegative integer m and any m-tuple $\mathbf{t}$ and any $i \in \{1, 2, \ldots, m\}$, we denote by $\mathbf{t}[i]$ the i-th entry of the m-tuple $\mathbf{t}$. Hence, any nonnegative integer m and any m-tuple $\mathbf{t}$ satisfy

$$\mathbf{t} = (\mathbf{t}[1], \mathbf{t}[2], \ldots, \mathbf{t}[m]).$$

Every set T, every nonnegative integer m, every $i \in \{1, 2, \ldots, m\}$ and every $f \in \operatorname{Map}(\{1, 2, \ldots, m\}, T)$ satisfy

$$\left(\operatorname{tuple}_{T,m}(f)\right)[i] = f(i) \tag{378}$$

[179]. Every set T, every nonnegative integer m, every $i \in \{1, 2, \ldots, m\}$ and any m elements t_1, t_2, ..., t_m of T satisfy

$$(t_1, t_2, \ldots, t_m)[i] = t_i. \tag{379}$$

[180]

Here is one last piece of notation I want to introduce: If x and y are two integers such that $y \geq x - 1$, and if B is a ring, and if b_x, b_{x+1}, ..., b_y are elements of B,

[178] Some authors actually **define** m-tuples of elements of T as maps from $\{1, 2, \ldots, m\}$ to T. In that case, this bijection $\operatorname{tuple}_{T,m}$ is simply $\operatorname{id}_{T^{\times m}}$.

[179] *Proof of (378):* Let T be a set. Let m be a nonnegative integer. Let $i \in \{1, 2, \ldots, m\}$. Let $f \in \operatorname{Map}(\{1, 2, \ldots, m\}, T)$. Then, (377) shows that $\operatorname{tuple}_{T,m}(f) = (f(1), f(2), \ldots, f(m))$. Hence,

$$\begin{aligned}\left(\operatorname{tuple}_{T,m}(f)\right)[i] &= (f(1), f(2), \ldots, f(m))[i] \\ &= (\text{the } i\text{-th entry of the } m\text{-tuple } (f(1), f(2), \ldots, f(m))) \\ &\qquad (\text{by the definition of } (f(1), f(2), \ldots, f(m))[i]) \\ &= f(i),\end{aligned}$$

qed.

[180] *Proof of (379):* Let T be a set. Let m be a nonnegative integer. Let t_1, t_2, ..., t_m be m elements of T. Let $i \in \{1, 2, \ldots, m\}$. Then, by the definition of $(t_1, t_2, \ldots, t_m)[i]$, we have

$$(t_1, t_2, \ldots, t_m)[i] = (\text{the } i\text{-th entry of the } m\text{-tuple } (t_1, t_2, \ldots, t_m)) = t_i,$$

qed.

then $\overrightarrow{\prod_{i=x}^{y}} b_i$ will mean the product $b_x b_{x+1} \cdots b_y \in B$. When the ring B is commutative, this product $\overrightarrow{\prod_{i=x}^{y}} b_i$ is identical with the standard product $\prod_{i=x}^{y} b_i$, but when B is not supposed to be commutative, the notation $\prod_{i=x}^{y} b_i$ makes no sense (unless b_x, b_{x+1}, ..., b_y commute).

For every $S \in \mathcal{P}(\{1,2,\ldots,n\})$, we have

$$\left(\sum_{s\in S} v_s\right)^n$$

$$= \sum_{(s_1,s_2,\ldots,s_n)\in S^{\times n}} \underbrace{v_{s_1} v_{s_2} \cdots v_{s_n}}_{=\overrightarrow{\prod_{i=1}^{n}} v_{s_i}} \qquad \text{(by the product rule)}$$

$$= \sum_{(s_1,s_2,\ldots,s_n)\in S^{\times n}} \overrightarrow{\prod_{i=1}^{n}} \underbrace{v_{s_i}}_{\substack{=v_{(s_1,s_2,\ldots,s_n)[i]} \\ \text{(because (379) (applied to } m=n,\ T=S \text{ and } t_i=s_i) \\ \text{yields } (s_1,s_2,\ldots,s_n)[i]=s_i, \text{ so that } v_{(s_1,s_2,\ldots,s_n)[i]}=v_{s_i})}}$$

$$= \sum_{(s_1,s_2,\ldots,s_n)\in S^{\times n}} \overrightarrow{\prod_{i=1}^{n}} v_{(s_1,s_2,\ldots,s_n)[i]} = \underbrace{\sum_{\mathbf{s}\in S^{\times n}}}_{\substack{= \sum\limits_{\mathbf{s}\in\{1,2,\ldots,n\}^{\times n};\ \mathbf{s}\in S^{\times n}} \\ \text{(since } S^{\times n}\subseteq\{1,2,\ldots,n\}^{\times n})}} \overrightarrow{\prod_{i=1}^{n}} v_{\mathbf{s}[i]}$$

(here, we renamed the summation index $(s_1, s_2, \ldots, s_n)$ as $\mathbf{s}$)

$$= \sum_{\substack{\mathbf{s}\in\{1,2,\ldots,n\}^{\times n};\\ \mathbf{s}\in S^{\times n}}} \overrightarrow{\prod_{i=1}^{n}} v_{\mathbf{s}[i]} = \sum_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}} \overrightarrow{\prod_{i=1}^{n}} \underbrace{v_{\left(\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\right)[i]}}_{\substack{=v_{f(i)} \\ \text{(since (378) (applied to } T=\{1,2,\ldots,n\} \\ \text{and } m=n) \text{ yields } \left(\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\right)[i]=f(i))}}$$

$$\left(\begin{array}{c} \text{here, we substituted } \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f) \text{ for } \mathbf{s} \text{ in the sum,} \\ \text{since } \mathrm{tuple}_{\{1,2,\ldots,n\},n} \text{ is a bijection} \\ \text{from } \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\}) \text{ to } \{1,2,\ldots,n\}^{\times n} \end{array}\right)$$

$$= \sum_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}} \underbrace{\overrightarrow{\prod_{i=1}^{n}} v_{f(i)}}_{=v_{f(1)}v_{f(2)}\cdots v_{f(n)}} = \sum_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}} v_{f(1)} v_{f(2)} \cdots v_{f(n)}.$$

Hence,

$$\begin{aligned}
&\sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \underbrace{\left(\sum_{s\in S} v_s\right)^n}_{= \sum\limits_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}} v_{f(1)}v_{f(2)}\cdots v_{f(n)}} \\
&= \sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \sum_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}} v_{f(1)}v_{f(2)}\cdots v_{f(n)} \\
&= \underbrace{\sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} \sum_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}}}_{= \sum\limits_{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})} \sum\limits_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}}} (-1)^{n-|S|} v_{f(1)}v_{f(2)}\cdots v_{f(n)} \\
&= \sum_{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})} \sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}} (-1)^{n-|S|} v_{f(1)}v_{f(2)}\cdots v_{f(n)}. \qquad (380)
\end{aligned}$$

Now, for every $f \in \mathrm{Map}\left(\{1,2,\ldots,n\},\{1,2,\ldots,n\}\right)$ and every $S \in \mathcal{P}\left(\{1,2,\ldots,n\}\right)$, we have the following equivalence of assertions:

$$\left(\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f) \in S^{\times n}\right) \iff \left(f\left(\{1,2,\ldots,n\}\right) \subseteq S\right). \qquad (381)$$

[181] Thus, we can replace the $\sum\limits_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\});\\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}}$ sign by a $\sum\limits_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\});\\ f(\{1,2,\ldots,n\})\subseteq S}}$ sign in (380).

[181] *Proof of (381):* Let $f \in \mathrm{Map}\left(\{1,2,\ldots,n\},\{1,2,\ldots,n\}\right)$ and $S \in \mathcal{P}\left(\{1,2,\ldots,n\}\right)$. Since $\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)$ is an n-tuple, we have $\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f) \in S^{\times n}$ if and only if every of the n entries of $\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)$ belongs to S. In other words, we have $\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f) \in S^{\times n}$ if and only if every $i \in \{1,2,\ldots,n\}$ satisfies $\left(\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\right)[i] \in S$. Thus, we have the following equivalence of assertions:

$$\begin{aligned}
&\left(\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f) \in S^{\times n}\right) \\
&\iff \left(\text{every } i \in \{1,2,\ldots,n\} \text{ satisfies } \underbrace{\left(\mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\right)[i]}_{\substack{=f(i)\\ \text{(by (378) (applied to } T=\{1,2,\ldots,n\} \text{ and } m=n))}} \in S\right) \\
&\iff \left(\text{every } i \in \{1,2,\ldots,n\} \text{ satisfies } f(i) \in S\right) \\
&\iff \left(\underbrace{\{f(i) \mid i \in \{1,2,\ldots,n\}\}}_{=f(\{1,2,\ldots,n\})} \subseteq S\right) \iff \left(f\left(\{1,2,\ldots,n\}\right) \subseteq S\right).
\end{aligned}$$

This proves (381).

Hence, (380) becomes

$$\begin{aligned}
&\sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left(\sum_{s\in S} v_s\right)^n \\
&= \sum_{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})} \underbrace{\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ \mathrm{tuple}_{\{1,2,\ldots,n\},n}(f)\in S^{\times n}}}}_{=\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ f(\{1,2,\ldots,n\})\subseteq S}} \text{ (due to the equivalence (381))}} (-1)^{n-|S|} v_{f(1)} v_{f(2)} \cdots v_{f(n)} \\
&= \sum_{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})} \sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|} v_{f(1)} v_{f(2)} \cdots v_{f(n)} \\
&= \sum_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\}); \\ f \text{ is bijective}}} \sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|} v_{f(1)} v_{f(2)} \cdots v_{f(n)} \\
&\quad + \sum_{\substack{f\in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\}); \\ f \text{ is not bijective}}} \sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|} v_{f(1)} v_{f(2)} \cdots v_{f(n)}. \qquad (382)
\end{aligned}$$

Now, every element f of $\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})$ which is not bijective satisfies

$$\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|} = 0 \qquad (383)$$

[182]. Furthermore, every element f of $\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})$ which is bijective satisfies

$$\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|} = 1 \qquad (384)$$

[183].

[182] *Proof of (383):* Let f be an element of $\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})$ such that f is not bijective.

We know that f is a map from $\{1,2,\ldots,n\}$ to $\{1,2,\ldots,n\}$ (since $f \in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})$). Thus, f is a map from a finite set to itself (since $\{1,2,\ldots,n\}$ is a finite set).

But it is known that every surjective map from a finite set to itself must be bijective. Hence, if f was surjective, then f would be bijective (because f is a map from a finite set to itself), which would contradict the fact that f is not bijective. Hence, f cannot be surjective.

We have $f(\{1,2,\ldots,n\}) \subseteq \{1,2,\ldots,n\}$ (since $f \in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})$). Furthermore, $f(\{1,2,\ldots,n\}) \neq \{1,2,\ldots,n\}$ (because otherwise, we would have $f(\{1,2,\ldots,n\}) = \{1,2,\ldots,n\}$, so that f would be surjective, which contradicts the fact that f is not surjective). Hence, Lemma 32.2 **(a)** (applied to $A = \{1,2,\ldots,n\}$ and $B = f(\{1,2,\ldots,n\})$) yields $\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\}); \\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|} = 0$. This proves (383).

[183] *Proof of (384):* Let f be an element of $\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})$ such that f is bijective.

We know that f is a map from $\{1,2,\ldots,n\}$ to $\{1,2,\ldots,n\}$ (since $f \in \mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\})$). Since f is surjective (because f is bijective), we have $f(\{1,2,\ldots,n\}) = \{1,2,\ldots,n\}$. Moreover, $n = |\{1,2,\ldots,n\}|$. Thus, we can apply Lemma 32.2 **(b)** to

Now, (382) becomes

$$\sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left(\sum_{s\in S} v_s\right)^n$$

$$= \sum_{\substack{f\in\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ f \text{ is bijective}}} \underbrace{\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\});\\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|}}_{\substack{=1\\ \text{(by (384))}}} v_{f(1)}v_{f(2)}\cdots v_{f(n)}$$

$$+ \sum_{\substack{f\in\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ f \text{ is not bijective}}} \underbrace{\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\});\\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|}}_{\substack{=0\\ \text{(by (383))}}} v_{f(1)}v_{f(2)}\cdots v_{f(n)}$$

$$= \sum_{\substack{f\in\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ f \text{ is bijective}}} \underbrace{1v_{f(1)}v_{f(2)}\cdots v_{f(n)}}_{=v_{f(1)}v_{f(2)}\cdots v_{f(n)}} + \underbrace{\sum_{\substack{f\in\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ f \text{ is not bijective}}} 0v_{f(1)}v_{f(2)}\cdots v_{f(n)}}_{=0}$$

$$= \underbrace{\sum_{\substack{f\in\mathrm{Map}(\{1,2,\ldots,n\},\{1,2,\ldots,n\});\\ f \text{ is bijective}}}}_{= \sum_{\substack{f \text{ is a map from } \{1,2,\ldots,n\} \text{ to } \{1,2,\ldots,n\};\\ f \text{ is bijective}}} = \sum_{f \text{ is a bijective map from } \{1,2,\ldots,n\} \text{ to } \{1,2,\ldots,n\}} v_{f(1)}v_{f(2)}\cdots v_{f(n)}$$

$$= \sum_{f \text{ is a permutation of } \{1,2,\ldots,n\}}$$

(since the bijective maps from $\{1,2,\ldots,n\}$ to $\{1,2,\ldots,n\}$ are precisely the permutations of $\{1,2,\ldots,n\}$)

$$= \underbrace{\sum_{f \text{ is a permutation of } \{1,2,\ldots,n\}}}_{= \sum_{f\in(\text{the set of permutations of } \{1,2,\ldots,n\})} = \sum_{f\in S_n}} v_{f(1)}v_{f(2)}\cdots v_{f(n)}$$

(since the set of permutations of $\{1,2,\ldots,n\}$ is S_n)

$$= \sum_{f\in S_n} v_{f(1)}v_{f(2)}\cdots v_{f(n)} = \sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)}$$

(here, we renamed the summation index f as σ). This proves Theorem 32.1. □

Theorem 32.1 has various useful corollaries; here is probably the simplest one:[184]

Corollary 32.3. Let A be a commutative ring. Let $n \in \mathbb{N}$. Let v_1, v_2, …, v_n be n elements of A. For every set X, let $\mathcal{P}(X)$ denote the power set of X. Then,

$$n! \cdot v_1v_2\cdots v_n = \sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left(\sum_{s\in S} v_s\right)^n.$$

$A = \{1,2,\ldots,n\}$ and $B = f(\{1,2,\ldots,n\})$. As a consequence, we obtain $\sum_{\substack{S\in\mathcal{P}(\{1,2,\ldots,n\});\\ f(\{1,2,\ldots,n\})\subseteq S}} (-1)^{n-|S|} = 1$. This proves (384).

[184] Notice that Corollary 32.3 also appears as Exercise 6.50 **(d)** in [Grinbe17].

Proof of Corollary 32.3. Let $\sigma \in S_n$. Then, σ is a permutation of $\{1,2,\ldots,n\}$. In other words, σ is a bijection from $\{1,2,\ldots,n\}$ to $\{1,2,\ldots,n\}$.

Since the ring A is commutative, terms like $\prod_{i\in\{1,2,\ldots,n\}} v_i$ and $\prod_{i\in\{1,2,\ldots,n\}} v_{\sigma(i)}$ make sense. We have

$$\begin{aligned} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} &= \prod_{i\in\{1,2,\ldots,n\}} v_{\sigma(i)} = \prod_{i\in\{1,2,\ldots,n\}} v_i \\ &\qquad \left(\begin{array}{c} \text{here, we have substituted } i \text{ for } \sigma(i) \text{ in the product,} \\ \text{since } \sigma \text{ is a bijection from } \{1,2,\ldots,n\} \text{ to } \{1,2,\ldots,n\} \end{array} \right) \\ &= v_1 v_2 \cdots v_n. \end{aligned}$$

Now, forget that we fixed σ. We thus have proven that $v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} = v_1v_2\cdots v_n$ for every $\sigma \in S_n$. Thus,

$$\sum_{\sigma\in S_n} \underbrace{v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)}}_{=v_1v_2\cdots v_n} = \sum_{\sigma\in S_n} v_1v_2\cdots v_n = \underbrace{|S_n|}_{=n!}\cdot v_1v_2\cdots v_n = n!\cdot v_1v_2\cdots v_n.$$

Comparing this with

$$\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} = \sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|}\left(\sum_{s\in S} v_s\right)^n \qquad \text{(by Theorem 32.1)},$$

we obtain

$$n!\cdot v_1v_2\cdots v_n = \sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|}\left(\sum_{s\in S} v_s\right)^n.$$

This proves Corollary 32.3. □

A more interesting application of Theorem 32.1 concerns the vector spaces $\operatorname{symp}_n V$ defined in Definition 17.11 **(c)**:

Theorem 32.4. Let k be a field of characteristic 0. Let A be a k-algebra. Let V be a k-vector subspace of A. Let $n \in \mathbb{N}$. Consider the k-vector subspace $\operatorname{symp}_n V$ of A defined in Definition 17.11 **(c)**.

We have

$$\operatorname{symp}_n V = \langle v^n \mid v \in V\rangle.$$

Proof of Theorem 32.4. Recall that $\operatorname{symp}_n V$ was defined by

$$\operatorname{symp}_n V = \left\langle \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \mid (v_1,v_2,\ldots,v_n)\in V^{\times n}\right\rangle.$$

a) We have $\operatorname{symp}_n V \subseteq \langle v^n \mid v \in V\rangle$.

Proof. Let $(v_1,v_2,\ldots,v_n) \in V^{\times n}$. Then, $v_s \in V$ for every $s \in \{1,2,\ldots,n\}$. For every $S \in \mathcal{P}(\{1,2,\ldots,n\})$, we have

$$\sum_{s\in S} \underbrace{v_s}_{\in V} \in \sum_{s\in S} V \subseteq V$$

(since V is a k-vector space). Hence, for every $S \in \mathcal{P}\left(\{1,2,\ldots,n\}\right)$, we have

$$\left(\sum_{s\in S} v_s\right)^n \in \left\{v^n \mid v \in V\right\}$$

(because $\left(\sum_{s\in S} v_s\right)^n = v^n$ for $v = \sum_{s\in S} v_s$, and because $\sum_{s\in S} v_s \in V$). Thus, for every $S \in \mathcal{P}\left(\{1,2,\ldots,n\}\right)$, we have

$$\begin{aligned}\left(\sum_{s\in S} v_s\right)^n &\in \left\{v^n \mid v \in V\right\} \subseteq \left\langle \left\{v^n \mid v \in V\right\}\right\rangle \\ &= \left\langle v^n \mid v \in V\right\rangle. \end{aligned} \tag{385}$$

Now,

$$\begin{aligned}&\frac{1}{n!} \underbrace{\sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}}_{= \sum\limits_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left(\sum\limits_{s\in S} v_s\right)^n \text{ (by Theorem 32.1)}} \\ &= \frac{1}{n!} \sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \underbrace{\left(\sum_{s\in S} v_s\right)^n}_{\in \langle v^n \mid v\in V\rangle \text{ (by (385))}} \\ &\in \frac{1}{n!} \sum_{S\in\mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left\langle v^n \mid v \in V\right\rangle \subseteq \left\langle v^n \mid v \in V\right\rangle\end{aligned}$$

(since $\left\langle v^n \mid v \in V\right\rangle$ is a k-vector space).

Now, forget that we fixed $(v_1, v_2, \ldots, v_n)$. We thus have shown that $\frac{1}{n!} \sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \in \left\langle v^n \mid v \in V\right\rangle$ for every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$. In other words,

$$\left\{\frac{1}{n!} \sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n}\right\} \subseteq \left\langle v^n \mid v \in V\right\rangle.$$

Thus, (154) (applied to $M = A$, $S = \left\{\frac{1}{n!} \sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n}\right\}$ and $Q = \left\langle v^n \mid v \in V\right\rangle$) yields that

$$\begin{aligned}&\left\langle \left\{\frac{1}{n!} \sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n}\right\}\right\rangle \\ &\subseteq \left\langle v^n \mid v \in V\right\rangle.\end{aligned}$$

Now,

$$\begin{aligned}\operatorname{symp}_n V &= \left\langle \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \;\mid\; (v_1,v_2,\ldots,v_n)\in V^{\times n}\right\rangle \\ &= \left\langle \left\{ \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \;\mid\; (v_1,v_2,\ldots,v_n)\in V^{\times n}\right\}\right\rangle \\ &\subseteq \left\langle v^n \;\mid\; v\in V\right\rangle.\end{aligned}$$

We have thus proven that $\operatorname{symp}_n V \subseteq \langle v^n \mid v\in V\rangle$.

b) We have $\langle v^n \mid v\in V\rangle \subseteq \operatorname{symp}_n V$.

Proof. Let $v\in V$. Then, $\left(\underbrace{v,v,\ldots,v}_{n \text{ times } v}\right)\in V^{\times n}$ and $\frac{1}{n!}\sum_{\sigma\in S_n}\underbrace{vv\cdots v}_{n \text{ times } v} = \frac{1}{n!}\underbrace{|S_n|}_{=n!}\underbrace{vv\cdots v}_{n \text{ times } v} = \underbrace{v^n}$ $\frac{1}{n!}n!v^n = v^n$. Thus, $v^n = \frac{1}{n!}\sum_{\sigma\in S_n}\underbrace{vv\cdots v}_{n \text{ times } v}$. Hence, the element v^n has the form $\frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)}$ for some $(v_1,v_2,\ldots,v_n)\in V^{\times n}$ (namely, for $(v_1,v_2,\ldots,v_n) = \left(\underbrace{v,v,\ldots,v}_{n \text{ times } v}\right)$). In other words,

$$\begin{aligned}v^n &\in \left\{ \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \;\mid\; (v_1,v_2,\ldots,v_n)\in V^{\times n}\right\} \\ &\subseteq \left\langle \left\{ \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \;\mid\; (v_1,v_2,\ldots,v_n)\in V^{\times n}\right\}\right\rangle \\ &= \left\langle \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \;\mid\; (v_1,v_2,\ldots,v_n)\in V^{\times n}\right\rangle \\ &= \operatorname{symp}_n V.\end{aligned}$$

Now, forget that we fixed v. We thus have shown that $v^n \in \operatorname{symp}_n V$ for every $v\in V$. In other words, $\{v^n \mid v\in V\}\subseteq \operatorname{symp}_n V$. Thus, (154) (applied to $M=A$, $S=\{v^n \mid v\in V\}$ and $Q=\operatorname{symp}_n V$) yields that $\langle\{v^n \mid v\in V\}\rangle \subseteq \operatorname{symp}_n V$. Thus, $\langle v^n \mid v\in V\rangle = \langle\{v^n \mid v\in V\}\rangle \subseteq \operatorname{symp}_n V$. We have thus proven that $\langle v^n \mid v\in V\rangle \subseteq \operatorname{symp}_n V$.

c) We now know that $\operatorname{symp}_n V \subseteq \langle v^n \mid v\in V\rangle$ and $\langle v^n \mid v\in V\rangle \subseteq \operatorname{symp}_n V$. Combining these two inclusions, we obtain $\operatorname{symp}_n V = \langle v^n \mid v\in V\rangle$. Theorem 32.4 is thus proven. □

Theorem 32.4 takes a simpler form in the particular case when the algebra is commutative:

Corollary 32.5. Let k be a field of characteristic 0. Let A be a commutative k-algebra. Let V be a k-vector subspace of A. Let $n\in\mathbb{N}$. Then,

$$V^n = \left\langle v^n \;\mid\; v\in V\right\rangle.$$

Note that this corollary is (generally) wrong when k doesn't have characteristic 0.

Proof of Corollary 32.5. Consider the k-vector subspace $\operatorname{symp}_n V$ of A defined in Definition 17.11 **(c)**. Recall that $\operatorname{symp}_n V$ was defined by

$$\operatorname{symp}_n V = \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle.$$

Every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies $\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} = n! \cdot v_1 v_2 \cdots v_n$ [185]. Hence,

$$\begin{aligned}
&\left\langle \frac{1}{n!} \underbrace{\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}}_{= n! \cdot v_1 v_2 \cdots v_n} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\
&= \left\langle \underbrace{\frac{1}{n!} n! \cdot v_1 v_2 \cdots v_n}_{= v_1 v_2 \cdots v_n} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\
&= \left\langle v_1 v_2 \cdots v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle = V^n \qquad \text{(by (73))}
\end{aligned}$$

But Theorem 32.4 yields $\operatorname{symp}_n V = \langle v^n \mid v \in V \rangle$, so that

$$\begin{aligned}
\langle v^n \mid v \in V \rangle &= \operatorname{symp}_n V \\
&= \left\langle \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle = V^n.
\end{aligned}$$

This proves Corollary 32.5. □

A corollary of this corollary is the following property of symmetric powers:

Corollary 32.6. Let k be a field of characteristic 0. Let V be a k-vector space. Let $n \in \mathbb{N}$. Consider the n-th symmetric power $\operatorname{Sym}^n(V)$ of the vector space V. Then,

$$\operatorname{Sym}^n(V) = \langle v^n \mid v \in V \rangle,$$

where v^n denotes the projection of $\underbrace{v \otimes v \otimes \cdots \otimes v}_{n \text{ times } v} \in V^{\otimes n}$ onto the n-th symmetric power $\operatorname{Sym}^n(V)$.

Corollary 32.6 appears as Lemma 4.56 (i) in [EGHLSVY] (where it is proven using representation theory).

Proof of Corollary 32.6. Let $\operatorname{Sym}(V)$ be the symmetric algebra of the k-vector space V. It is known that both V and $\operatorname{Sym}^n(V)$ canonically inject into $\operatorname{Sym}(V)$. We shall identify V and $\operatorname{Sym}^n(V)$ with k-vector subspaces of $\operatorname{Sym}(V)$ using these injections.

[185] This can be proven in the same way as we did in the proof of Corollary 32.3.

For every $v \in V$, the element v^n of $\operatorname{Sym}^n(V)$ is the actual n-th power of the element $v \in V \subseteq \operatorname{Sym}(V)$ taken in $\operatorname{Sym}(V)$. [186] Hence, the notation v^n in Corollary 32.6 does not conflict with the notation v^n in Corollary 32.5 (applied to $A = \operatorname{Sym}(V)$). Since the symmetric algebra $\operatorname{Sym}(V)$ is commutative, we can apply Corollary 32.5 to $A = \operatorname{Sym}(V)$. We obtain $V^n = \langle v^n \mid v \in V \rangle$. But it is easy to see that $V^n = \operatorname{Sym}^n(V)$ as subspaces of $\operatorname{Sym}(V)$ [187]. Hence, $\operatorname{Sym}^n(V) = V^n = \langle v^n \mid v \in V \rangle$. This proves Corollary 32.6. $\square$

The following consequence of Theorem 32.4 will be of most importance to us:

---

[186] *Proof.* Let $v \in V$. Consider the tensor algebra $\otimes V$ of the k-vector space V. Let π be the canonical projection from $\otimes V$ to $\operatorname{Sym}(V)$. Then, π is a k-algebra homomorphism. Moreover, $\pi(w) = w$ for every $w \in V$. Applied to $w = v$, this yields $\pi(v) = v$.

We have

$$
\begin{aligned}
&(\text{the element } v^n \text{ of } \operatorname{Sym}^n(V)) \\
&= \left(\text{the projection of } \underbrace{v \otimes v \otimes \cdots \otimes v}_{n \text{ times } v} \in V^{\otimes n} \text{ onto the } n\text{-th symmetric power } \operatorname{Sym}^n(V) \right) \\
&\qquad (\text{by the definition of the element } v^n \text{ of } \operatorname{Sym}^n(V)) \\
&= \left(\text{the projection of } \underbrace{v \otimes v \otimes \cdots \otimes v}_{n \text{ times } v} \in \otimes V \text{ onto the symmetric algebra } \operatorname{Sym}(V) \right) \\
&\qquad \left(\begin{array}{c} \text{since the canonical projection from } V^{\otimes n} \text{ onto the } n\text{-th symmetric power } \operatorname{Sym}^n(V) \\ \text{is a restriction of the canonical projection from } \otimes V \text{ onto the symmetric algebra } \operatorname{Sym}(V) \end{array} \right) \\
&= \pi \left(\underbrace{\underbrace{v \otimes v \otimes \cdots \otimes v}_{n \text{ times } v}}_{= (\text{the } n\text{-th power of } v \text{ in the algebra } \otimes V)} \right) \\
&\qquad (\text{since the canonical projection from } \otimes V \text{ onto the symmetric algebra } \operatorname{Sym}(V) \text{ is } \pi) \\
&= \pi (\text{the } n\text{-th power of } v \text{ in the algebra } \otimes V) \\
&= \left(\text{the } n\text{-th power of } \underbrace{\pi(v)}_{=v} \text{ in the algebra } \operatorname{Sym}(V) \right) \qquad (\text{since } \pi \text{ is a } k\text{-algebra homomorphism}) \\
&= (\text{the } n\text{-th power of } v \text{ in the algebra } \operatorname{Sym}(V)).
\end{aligned}
$$

In other words, the element v^n of $\operatorname{Sym}^n(V)$ is the n-th power of v in the algebra $\operatorname{Sym}(V)$, qed.

[187] *Proof.* Consider the tensor algebra $\otimes V$ of the k-vector space V. Let π be the canonical projection from $\otimes V$ to $\operatorname{Sym}(V)$. Then, π is a k-algebra homomorphism. Moreover,

$$\pi(w) = w \qquad \text{for every } w \in V. \tag{386}$$

We know that $\operatorname{Sym}^n(V)$ is the image of $V^{\otimes n}$ under the canonical projection π. In other words, $\operatorname{Sym}^n(V) = \pi(V^{\otimes n})$.

Let $(v_1, v_2, \ldots, v_n) \in V^{\times n}$. Then, in the k-algebra $\otimes V$, we have

$$v_1 v_2 \cdots v_n = v_1 \otimes v_2 \otimes \cdots \otimes v_n \tag{387}$$

(since the multiplication on the k-algebra $\otimes V$ is the tensor product). But we have $v_i \in V$ for every $i \in \{1, 2, \ldots, n\}$. Thus, $\pi(v_i) = v_i$ for every $i \in \{1, 2, \ldots, n\}$ (by (386), applied to $w = v_i$). In other words, $(\pi(v_1), \pi(v_2), \ldots, \pi(v_n)) = (v_1, v_2, \ldots, v_n)$. Hence, $\pi(v_1)\pi(v_2)\cdots\pi(v_n) = v_1 v_2 \cdots v_n$, where

Corollary 32.7. Let k be a field of characteristic 0. Let A be a k-algebra. Let V be a k-vector subspace of A. Assume that

$$xy - yx \in V \qquad \text{for any } x \in V \text{ and } y \in V.$$

Assume further that $A = \sum_{n \in \mathbb{N}} V^n$ [188].

Let W be a k-vector space. Let $f : A \to W$ and $g : A \to W$ be two k-linear maps. Assume that $f(v^n) = g(v^n)$ for every $v \in V$ and $n \in \mathbb{N}$. Then, $f = g$.

Proof of Corollary 32.7. Since f and g are k-linear maps, their difference $f - g$ is also a k-linear map. Hence, $\operatorname{Ker}(f-g)$ is a k-vector subspace of A.

---

both products in this equality are taken in the k-algebra $\operatorname{Sym}(V)$. Now,

$$\begin{aligned}
&\pi\left(\underbrace{v_1 \otimes v_2 \otimes \cdots \otimes v_n}_{\substack{=v_1 v_2 \cdots v_n \\ \text{(by (387))}}}\right) \\
&= \pi(v_1 v_2 \cdots v_n) \\
&= \pi(v_1)\,\pi(v_2) \cdots \pi(v_n) \qquad \text{(since } \pi \text{ is a } k\text{-algebra homomorphism)} \\
&= v_1 v_2 \cdots v_n, \qquad (388)
\end{aligned}$$

where the product $v_1 v_2 \ldots v_n$ is taken in the k-algebra $\operatorname{Sym}(V)$.

Now, forget that we fixed $(v_1, v_2, \ldots, v_n)$. We thus have proven the equality (388) for each $(v_1, v_2, \ldots, v_n) \in V^{\times n}$.

But the n-th tensor power $V^{\otimes n}$ is spanned by all pure tensors. In other words,

$$V^{\otimes n} = \left\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle.$$

Hence,

$$\begin{aligned}
V^{\otimes n} &= \left\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\
&= \left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle.
\end{aligned}$$

Applying the map π to both sides of this equality, we obtain

$$\begin{aligned}
\pi\left(V^{\otimes n}\right) &= \pi\left(\left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle\right) \\
&= \left\langle \underbrace{\pi\left(\left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}\right)}_{= \left\{ \pi(v_1 \otimes v_2 \otimes \cdots \otimes v_n) \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}} \right\rangle \\
&\qquad \left(\begin{array}{c} \text{by (165), applied to } M = \otimes V,\ R = \operatorname{Sym}(V),\ \phi = \pi \\ \text{and } S = \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \end{array} \right) \\
&= \left\langle \left\{ \pi(v_1 \otimes v_2 \otimes \cdots \otimes v_n) \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle \\
&= \left\langle \underbrace{\pi(v_1 \otimes v_2 \otimes \cdots \otimes v_n)}_{\substack{=v_1 v_2 \cdots v_n \\ \text{(by (388))}}} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\
&= \left\langle v_1 v_2 \cdots v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle = V^n.
\end{aligned}$$

Thus, $V^n = \pi\left(V^{\otimes n}\right) = \operatorname{Sym}^n(V)$.

[188] This is an equivalent way to say that the k-algebra A is generated by the subset V. But it is easier for us to word it as $\sum_{n \in \mathbb{N}} V^n$.

Now, let $n \in \mathbb{N}$. We know that every $v \in V$ satisfies

$$(f-g)(v^n) = \underbrace{f(v^n)}_{=g(v^n)} - g(v^n) = g(v^n) - g(v^n) = 0.$$

In other words, every $v \in V$ satisfies $v^n \in \operatorname{Ker}(f-g)$. In other words, $\{v^n \mid v \in V\} \subseteq \operatorname{Ker}(f-g)$. Hence, (154) (applied to $M = A$, $S = \{v^n \mid v \in V\}$ and $Q = \operatorname{Ker}(f-g)$) yields that $\langle \{v^n \mid v \in V\} \rangle \subseteq \operatorname{Ker}(f-g)$. Now, consider the k-vector subspace $\operatorname{symp}_n V$ of A defined in Definition 17.11 **(c)**. Theorem 32.4 yields $\operatorname{symp}_n V = \langle v^n \mid v \in V \rangle \subseteq \operatorname{Ker}(f-g)$.

Now, forget that we have fixed n. We thus have proven that

$$\operatorname{symp}_n V \subseteq \operatorname{Ker}(f-g) \qquad \text{for every } n \in \mathbb{N}. \tag{389}$$

Now, every $\ell \in \mathbb{N}$ satisfies

$$\begin{aligned} V^\ell &\subseteq \sum_{i=0}^{\ell} V^i \qquad \left(\text{since } V^\ell \text{ is an addend in the sum } \sum_{i=0}^{\ell} V^i \right) \\ &= \sum_{i=0}^{\ell} \underbrace{\operatorname{symp}_i V}_{\substack{\subseteq \operatorname{Ker}(f-g) \\ \text{(by (389), applied to } n=i\text{)}}} \qquad \text{(by Proposition 17.16 \textbf{(b)})} \\ &\subseteq \sum_{i=0}^{\ell} \operatorname{Ker}(f-g) \subseteq \operatorname{Ker}(f-g) \end{aligned} \tag{390}$$

(since $\operatorname{Ker}(f-g)$ is a k-vector space). Now,

$$A = \sum_{n \in \mathbb{N}} \underbrace{V^n}_{\substack{\subseteq \operatorname{Ker}(f-g) \\ \text{(by (389), applied to } \ell=n\text{)}}} \subseteq \sum_{n \in \mathbb{N}} \operatorname{Ker}(f-g) \subseteq \operatorname{Ker}(f-g)$$

(since $\operatorname{Ker}(f-g)$ is a k-vector space). In other words, $f - g = 0$. In other words, $f = g$. This proves Corollary 32.7. □

§33. $\operatorname{Log}\operatorname{id}$ on powers of primitives

Our next goal is to prove the following fact:

Theorem 33.1. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let $v \in \operatorname{Prim} H$ and $n \in \mathbb{N}$ be such that $n > 1$. Then,

$$(\operatorname{Log}\operatorname{id})(v^n) = 0.$$

This is a rather light variation on Lemma 2 ii) in [DMTCN13], and our proof is an adaptation of the proof given in [DMTCN13]. Actually we will show a slightly more general fact:

Theorem 33.2. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a k-algebra. Let $F : H \to A$ be a k-algebra homomorphism. Let $v \in \operatorname{Prim} H$ and $n \in \mathbb{N}$ be such that $n > 1$. Then, $F \in G(H, A)$ and

$$(\operatorname{Log} F)(v^n) = 0.$$

In order to prove these theorems, we will use the universal property of the polynomial ring $k[X]$ (a trick I learnt from [DMTCN13]). Here is this universal property:

Theorem 33.3. Let k be a field. Let X be a new symbol. Consider the polynomial ring $k[X]$ over k in one indeterminate X.

For every commutative k-algebra A and every $a \in A$, there exists a unique k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$.

This Theorem 33.3 is just the universal property of the polynomial ring $k[X]$. This theorem also holds if A is not required to be commutative:

Theorem 33.4. Let k be a field. Let X be a new symbol. Consider the polynomial ring $k[X]$ over k in one indeterminate X.

For every k-algebra A and every $a \in A$, there exists a unique k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$.

Proof of Theorem 33.4. Let A be a k-algebra. Let $a \in A$. Let B be the k-subalgebra of A generated by the element a. Hence, the k-algebra B is generated by the element a. Consequently, the k-algebra B is generated by pairwise commuting elements (because the element a is clearly pairwise commuting (since it is only one element)). Thus, the k-algebra B is commutative (since any k-algebra generated by pairwise commuting elements must be commutative). Moreover, we have $a \in B$ (since B is the k-subalgebra of A generated by the element a). Hence, we can apply Theorem 33.3 to B instead of A. As a consequence, we conclude that there exists a unique k-algebra homomorphism $\varphi : k[X] \to B$ satisfying $\varphi(X) = a$. Denote this homomorphism φ by Φ. Thus, Φ is a k-algebra homomorphism $\varphi : k[X] \to B$ satisfying $\varphi(X) = a$. In other words, Φ is a k-algebra homomorphism $k[X] \to B$ and satisfies $\Phi(X) = a$.

Let ι be the canonical inclusion $B \to A$. Clearly, ι is a k-algebra homomorphism. Since Φ and ι are k-algebra homomorphisms, their composition $\iota \circ \Phi$ is a k-algebra homomorphism (because the composition of two k-algebra homomorphisms must always be a k-algebra homomorphism). Also, $(\iota \circ \Phi)(X) = \iota\left(\underbrace{\Phi(X)}_{=a}\right) = \iota(a) = a$ (since ι is an inclusion map). Thus, there exists a k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$ (namely, $\varphi = \iota \circ \Phi$).

Now, let ψ_1 and ψ_2 be any two k-algebra homomorphisms $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$. We are going to show that $\psi_1 = \psi_2$.

Let $p \in k[X]$. Then, p is a polynomial in the indeterminate X over k. Hence, there exists some family $(\lambda_i)_{i \in \mathbb{N}} \in k^{\mathbb{N}}$ such that (all but finitely many $i \in \mathbb{N}$ satisfy $\lambda_i = 0$) and $p = \sum_{i \in \mathbb{N}} \lambda_i X^i$. Consider this family $(\lambda_i)_{i \in \mathbb{N}}$.

We know that ψ_1 is a k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$. In other words, ψ_1 is a k-algebra homomorphism $k[X] \to A$ and satisfies $\psi_1(X) = a$. Since $p = \sum_{i \in \mathbb{N}} \lambda_i X^i$, we have

$$\begin{aligned}\psi_1(p) &= \psi_1\left(\sum_{i \in \mathbb{N}} \lambda_i X^i\right) = \sum_{i \in \mathbb{N}} \lambda_i \left(\underbrace{\psi_1(X)}_{=a}\right)^i \\ &\qquad \text{(since } \psi_1 \text{ is a } k\text{-algebra homomorphism)} \\ &= \sum_{i \in \mathbb{N}} \lambda_i a^i.\end{aligned}$$

The same argument, with ψ_1 replaced by ψ_2, yields that $\psi_2(p) = \sum_{i \in \mathbb{N}} \lambda_i a^i$. Hence, $\psi_1(p) = \sum_{i \in \mathbb{N}} \lambda_i a^i = \psi_2(p)$.

Now, forget that we fixed p. We thus have proven that every $p \in k[X]$ satisfies $\psi_1(p) = \psi_2(p)$. In other words, $\psi_1 = \psi_2$.

Now, forget that we fixed ψ_1 and ψ_2. We thus have shown that if ψ_1 and ψ_2 are any two k-algebra homomorphisms $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$, then $\psi_1 = \psi_2$. In other words, there exists at most one k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$. Combining this with the fact that there exists a k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$, we conclude the following: There exists a unique k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$. This proves Theorem 33.4. □

Definition 33.5. Let k be a field. Let X be a new symbol. Consider the polynomial ring $k[X]$ over k in one indeterminate X.

For every k-algebra A and every $a \in A$, there exists a unique k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$ (according to Theorem 33.4). This homomorphism φ will be denoted by $\mathrm{ev}_{A,\,a}$ or by ev_a (when A is clear from the context). Thus, $\mathrm{ev}_{A,\,a}$ is the unique k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$. Hence, $\mathrm{ev}_{A,\,a}$ is a k-algebra homomorphism $k[X] \to A$ and satisfies

$$\mathrm{ev}_{A,\,a}(X) = a. \tag{391}$$

Corollary 33.6. Let X be a new symbol. Consider the polynomial ring $k[X]$ over k in one indeterminate X.

Let A be a k-algebra. Let $f : k[X] \to A$ and $g : k[X] \to A$ be two k-algebra homomorphisms such that $f(X) = g(X)$. Then, $f = g$.

Proof of Corollary 33.6. Let $a = f(X)$. Then, $a = f(X) = g(X)$.

We know that $\mathrm{ev}_{A,\,a}$ is the unique k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$ (by the definition of $\mathrm{ev}_{A,\,a}$). Hence, every k-algebra homomorphism $\varphi : k[X] \to A$ satisfying $\varphi(X) = a$ must be equal to $\mathrm{ev}_{A,\,a}$. In other words, if $\varphi : k[X] \to A$ is a k-algebra homomorphism satisfying $\varphi(X) = a$, then $\varphi = \mathrm{ev}_{A,\,a}$. Applying this to $\varphi = f$, we obtain $f = \mathrm{ev}_{A,\,a}$ (since $f(X) = a$).

On the other hand, if $\varphi : k[X] \to A$ is a k-algebra homomorphism satisfying $\varphi(X) = a$, then $\varphi = \mathrm{ev}_{A,\, a}$. Applying this to $\varphi = g$, we obtain $g = \mathrm{ev}_{A,\, a}$ (since $g(X) = a$). Hence, $f = \mathrm{ev}_{A,\, a} = g$. This proves Corollary 33.6. $\square$

Here are a number of properties of the k-bialgebra $k[X]$ that we are going to need:

Theorem 33.7. Let k be a field. Let X be a new symbol. Consider the polynomial ring $k[X]$ over k in one indeterminate X. Equip $k[X]$ with the usual grading (by degree).

Let Δ_X be the k-algebra homomorphism $\mathrm{ev}_{k[X]\otimes k[X],\, X\otimes 1+1\otimes X} : k[X] \to k[X] \otimes k[X]$ (where 1 means $1_{k[X]}$).

Let ε_X be the k-algebra homomorphism $\mathrm{ev}_{k,\, 0} : k[X] \to k$.

Then, $(k[X], \Delta_X, \varepsilon_X)$ is a commutative connected graded k-bialgebra.

Remark 33.8. The k-bialgebra $(k[X], \Delta_X, \varepsilon_X)$ of Theorem 33.7 is also cocommutative, but we won't need this in the following.

Proof of Theorem 33.7. Recall that $k[X]$ is the free k-module with basis $(X^n)_{n\in\mathbb{N}}$. Recall also that the grading on $k[X]$ is such that $(k[X])_n$ is a free k-module with basis (X^n) for every $n \in \mathbb{N}$. (Note the difference between $(X^n)_{n\in\mathbb{N}}$ and (X^n): The former is a family indexed by nonnegative integer, while the latter is a one-element family.)

It is known that $k[X]$ is a commutative graded algebra.

For every k-vector space V, let kanl_V be the canonical isomorphism $V \to V \otimes k$ which sends every $v \in V$ to $v \otimes 1 \in V \otimes k$.

For every k-vector space V, let kanr_V be the canonical isomorphism $V \to k \otimes V$ which sends every $v \in V$ to $1 \otimes v \in k \otimes V$.

Notice that if A is a k-algebra, then kanl_A and kanr_A are k-algebra homomorphisms. Applying this to $A = k[X]$, we conclude that $\mathrm{kanl}_{k[X]}$ and $\mathrm{kanr}_{k[X]}$ are k-algebra homomorphisms.

Since $\Delta_X = \mathrm{ev}_{k[X]\otimes k[X],\, X\otimes 1+1\otimes X}$, we have

$$\Delta_X(X) = \mathrm{ev}_{k[X]\otimes k[X],\, X\otimes 1+1\otimes X}(X) = X \otimes 1 + 1 \otimes X$$

(by (391), applied to $A = k[X] \otimes k[X]$ and $a = X \otimes 1 + 1 \otimes X$). Since $\varepsilon_X = \mathrm{ev}_{k,\, 0}$, we have

$$\varepsilon_X(X) = \mathrm{ev}_{k,\, 0}(X) = 0$$

(by (391), applied to $A = k$ and $a = 0$).

We know that $\mathrm{id}_{k[X]}$ and Δ_X are k-algebra homomorphisms. Thus, their tensor product $\mathrm{id}_{k[X]} \otimes \Delta_X$ is a k-algebra homomorphism (since the tensor product of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that Δ_X and $\mathrm{id}_{k[X]}$ are k-algebra homomorphisms. Thus, their tensor product $\Delta_X \otimes \mathrm{id}_{k[X]}$ is a k-algebra homomorphism (since the tensor product of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that $\mathrm{id}_{k[X]}$ and ε_X are k-algebra homomorphisms. Thus, their tensor product $\mathrm{id}_{k[X]} \otimes \varepsilon_X$ is a k-algebra homomorphism (since the tensor product of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that ε_X and $\mathrm{id}_{k[X]}$ are k-algebra homomorphisms. Thus, their tensor product $\varepsilon_X \otimes \mathrm{id}_{k[X]}$ is a k-algebra homomorphism (since the tensor product of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that $\mathrm{id}_{k[X]} \otimes \Delta_X$ and Δ_X are k-algebra homomorphisms. Thus, their composition $\left(\mathrm{id}_{k[X]} \otimes \Delta_X\right) \circ \Delta_X$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that $\Delta_X \otimes \mathrm{id}_{k[X]}$ and Δ_X are k-algebra homomorphisms. Thus, their composition $\left(\Delta_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that $\mathrm{id}_{k[X]} \otimes \varepsilon_X$ and Δ_X are k-algebra homomorphisms. Thus, their composition $\left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \circ \Delta_X$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that $\varepsilon_X \otimes \mathrm{id}_{k[X]}$ and Δ_X are k-algebra homomorphisms. Thus, their composition $\left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism).

Comparing

$$
\begin{aligned}
&\left(\left(\mathrm{id}_{k[X]} \otimes \Delta_X\right) \circ \Delta_X\right)(X) \\
&= \left(\mathrm{id}_{k[X]} \otimes \Delta_X\right)\left(\underbrace{\Delta_X(X)}_{=X\otimes 1+1\otimes X}\right) = \left(\mathrm{id}_{k[X]} \otimes \Delta_X\right)(X \otimes 1 + 1 \otimes X) \\
&= \underbrace{\mathrm{id}_{k[X]}(X)}_{=X} \otimes \underbrace{\Delta_X(1)}_{\substack{=1_{k[X]\otimes k[X]} \\ \text{(since } \Delta_X \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} + \underbrace{\mathrm{id}_{k[X]}(1)}_{=1} \otimes \underbrace{\Delta_X(X)}_{=X\otimes 1+1\otimes X} \\
&\qquad \left(\text{by the definition of } \mathrm{id}_{k[X]} \otimes \Delta_X\right) \\
&= X \otimes \underbrace{1_{k[X]\otimes k[X]}}_{=1\otimes 1} + \underbrace{1 \otimes (X \otimes 1 + 1 \otimes X)}_{\substack{=1\otimes X\otimes 1+1\otimes 1\otimes X \\ \text{(since the tensor product is distributive)}}} \\
&= X \otimes 1 \otimes 1 + 1 \otimes X \otimes 1 + 1 \otimes 1 \otimes X
\end{aligned}
$$

with

$$
\begin{aligned}
&\left(\left(\Delta_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X\right)(X) \\
&= \left(\Delta_X \otimes \mathrm{id}_{k[X]}\right)\left(\underbrace{\Delta_X(X)}_{=X\otimes 1+1\otimes X}\right) = \left(\Delta_X \otimes \mathrm{id}_{k[X]}\right)(X \otimes 1 + 1 \otimes X) \\
&= \underbrace{\Delta_X(X)}_{=X\otimes 1+1\otimes X} \otimes \underbrace{\mathrm{id}_{k[X]}(1)}_{=1} + \underbrace{\Delta_X(1)}_{\substack{=1_{k[X]\otimes k[X]} \\ \text{(since } \Delta_X \text{ is a } k\text{-algebra} \\ \text{homomorphism)}}} \otimes \underbrace{\mathrm{id}_{k[X]}(X)}_{=X} \\
&\qquad \left(\text{by the definition of } \Delta_X \otimes \mathrm{id}_{k[X]}\right) \\
&= \underbrace{(X \otimes 1 + 1 \otimes X) \otimes 1}_{\substack{=X\otimes 1\otimes 1+1\otimes X\otimes 1 \\ \text{(since the tensor product is distributive)}}} + \underbrace{1_{k[X]\otimes k[X]}}_{=1\otimes 1} \otimes X \\
&= X \otimes 1 \otimes 1 + 1 \otimes X \otimes 1 + 1 \otimes 1 \otimes X,
\end{aligned}
$$

we obtain

$$\left(\left(\mathrm{id}_{k[X]} \otimes \Delta_X\right) \circ \Delta_X\right)(X) = \left(\left(\Delta_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X\right)(X).$$

Thus, Corollary 33.6 (applied to $A = k[X] \otimes k[X] \otimes k[X]$, $f = \left(\mathrm{id}_{k[X]} \otimes \Delta_X\right) \circ \Delta_X$ and $g = \left(\Delta_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X$) yields

$$\left(\mathrm{id}_{k[X]} \otimes \Delta_X\right) \circ \Delta_X = \left(\Delta_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X$$

(since $\left(\mathrm{id}_{k[X]} \otimes \Delta_X\right) \circ \Delta_X$ and $\left(\Delta_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X$ are k-algebra homomorphisms).

Comparing

$$\begin{aligned}
&\left(\left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \circ \Delta_X\right)(X) \\
&= \left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right)\left(\underbrace{\Delta_X(X)}_{=X\otimes 1+1\otimes X}\right) = \left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right)(X \otimes 1 + 1 \otimes X) \\
&= \underbrace{\mathrm{id}_{k[X]}(X)}_{=X} \otimes \underbrace{\varepsilon_X(1)}_{\substack{=1 \\ (\text{since } \varepsilon_X \text{ is a } k\text{-algebra} \\ \text{homomorphism})}} + \mathrm{id}_{k[X]}(1) \otimes \underbrace{\varepsilon_X(X)}_{=0} \\
&\qquad \left(\text{by the definition of } \mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \\
&= X \otimes 1 + \underbrace{\mathrm{id}_{k[X]}(1) \otimes 0}_{=0} = X \otimes 1
\end{aligned}$$

with

$$\mathrm{kanl}_{k[X]}(X) = X \otimes 1 \qquad \left(\text{by the definition of } \mathrm{kanl}_{k[X]}\right),$$

we obtain

$$\left(\left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \circ \Delta_X\right)(X) = \mathrm{kanl}_{k[X]}(X).$$

Thus, Corollary 33.6 (applied to $A = k[X] \otimes k$, $f = \left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \circ \Delta_X$ and $g = \mathrm{kanl}_{k[X]}$) yields

$$\left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \circ \Delta_X = \mathrm{kanl}_{k[X]}$$

(since $\left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \circ \Delta_X$ and $\mathrm{kanl}_{k[X]}$ are k-algebra homomorphisms).

Comparing

$$\begin{aligned}
&\left(\left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X\right)(X) \\
&= \left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right)\left(\underbrace{\Delta_X(X)}_{=X\otimes 1+1\otimes X}\right) = \left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right)(X \otimes 1 + 1 \otimes X) \\
&= \underbrace{\varepsilon_X(X)}_{=0} \otimes \mathrm{id}_{k[X]}(1) + \underbrace{\varepsilon_X(1)}_{\substack{=1 \\ (\text{since } \varepsilon_X \text{ is a } k\text{-algebra} \\ \text{homomorphism})}} \otimes \underbrace{\mathrm{id}_{k[X]}(X)}_{=X} \\
&\qquad \left(\text{by the definition of } \varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \\
&= \underbrace{0 \otimes \mathrm{id}_{k[X]}(1)}_{=0} + 1 \otimes X = 1 \otimes X
\end{aligned}$$

with

$$\mathrm{kanr}_{k[X]}(X) = 1 \otimes X \qquad \left(\text{by the definition of } \mathrm{kanr}_{k[X]}\right),$$

we obtain

$$\left(\left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X\right)(X) = \mathrm{kanr}_{k[X]}(X).$$

Thus, Corollary 33.6 (applied to $A = k \otimes k[X]$, $f = \left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X$ and $g = \mathrm{kanr}_{k[X]}$) yields

$$\left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X = \mathrm{kanr}_{k[X]}$$

(since $\left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X$ and $\mathrm{kanr}_{k[X]}$ are k-algebra homomorphisms).

Recall the definition of a k-coalgebra: If C is a k-vector space, and $\Delta : C \to C \otimes C$ and $\varepsilon : C \to k$ are two k-linear maps, then (C, Δ, ε) is a k-coalgebra if and only if the equalities

$$\begin{aligned}
(\mathrm{id}_C \otimes \Delta) \circ \Delta &= (\Delta \otimes \mathrm{id}_C) \circ \Delta, \\
(\mathrm{id}_C \otimes \varepsilon) \circ \Delta &= \mathrm{kanl}_C, \\
(\varepsilon \otimes \mathrm{id}_C) \circ \Delta &= \mathrm{kanr}_C
\end{aligned}$$

hold. Applying this to $(C, \Delta, \varepsilon) = (k[X], \Delta_X, \varepsilon_X)$, we conclude that $(k[X], \Delta_X, \varepsilon_X)$ is a k-coalgebra if and only if the equalities

$$\left(\mathrm{id}_{k[X]} \otimes \Delta_X\right) \circ \Delta_X = \left(\Delta_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X, \tag{392}$$

$$\left(\mathrm{id}_{k[X]} \otimes \varepsilon_X\right) \circ \Delta_X = \mathrm{kanl}_{k[X]}, \tag{393}$$

$$\left(\varepsilon_X \otimes \mathrm{id}_{k[X]}\right) \circ \Delta_X = \mathrm{kanr}_{k[X]} \tag{394}$$

hold. Since we know that these equalities (392), (393) and (394) hold, this yields that $(k[X], \Delta_X, \varepsilon_X)$ is a k-coalgebra.

Now, let us recall the definition of a k-bialgebra, or at least one possible definition of it: If C is a k-algebra, and $\Delta : C \to C \otimes C$ and $\varepsilon : C \to k$ are two k-linear maps such that (C, Δ, ε) is a k-coalgebra, then (C, Δ, ε) (endowed with the given k-algebra structure on C) is a k-bialgebra if and only if the maps Δ and ε are k-algebra homomorphisms. Applying this to $(C, \Delta, \varepsilon) = (k[X], \Delta_X, \varepsilon_X)$, we conclude that $(k[X], \Delta_X, \varepsilon_X)$ is a k-bialgebra if and only if the maps Δ_X and ε_X are k-algebra homomorphisms (because we already know that $(k[X], \Delta_X, \varepsilon_X)$ is a k-coalgebra). Thus, $(k[X], \Delta_X, \varepsilon_X)$ is a k-bialgebra (since we know that the maps Δ_X and ε_X are k-algebra homomorphisms).

The map Δ_X is graded[189]. The map ε_X is graded[190].

[189] *Proof.* Recall that $k[X]$ is a graded k-algebra. Hence, $k[X] \otimes k[X]$ is a graded k-algebra as well (since the tensor product of two graded k-algebras always is a graded k-algebra). Denote this graded k-algebra $k[X] \otimes k[X]$ by A.

We know that the map Δ_X is a k-algebra homomorphism $k[X] \to k[X] \otimes k[X]$. Since $k[X] \otimes k[X] = A$, this rewrites as follows: The map Δ_X is a k-algebra homomorphism $k[X] \to A$.

By the definition of the grading on $k[X] \otimes k[X]$, we have $(k[X] \otimes k[X])_\ell = \sum_{i=0}^{\ell} (k[X])_i \otimes (k[X])_{\ell-i}$ for every $\ell \in \mathbb{N}$. Applying this to $\ell = 1$, we obtain

$$\begin{aligned}(k[X] \otimes k[X])_1 &= \sum_{i=0}^{1} (k[X])_i \otimes (k[X])_{1-i} = (k[X])_0 \otimes \underbrace{(k[X])_{1-0}}_{=(k[X])_1} + (k[X])_1 \otimes \underbrace{(k[X])_{1-1}}_{=(k[X])_0} \\ &= (k[X])_0 \otimes (k[X])_1 + (k[X])_1 \otimes (k[X])_0 .\end{aligned}$$

Now,

$$\begin{aligned}\Delta_X(X) = X \otimes 1 + 1 \otimes X &= \underbrace{1}_{\in (k[X])_0} \otimes \underbrace{X}_{\in (k[X])_1} + \underbrace{X}_{\in (k[X])_1} \otimes \underbrace{1}_{\in (k[X])_0} \\ &\in (k[X])_0 \otimes (k[X])_1 + (k[X])_1 \otimes (k[X])_0 = \left(\underbrace{k[X] \otimes k[X]}_{=A} \right)_1 = A_1.\end{aligned}$$

Now, let us show that

$$\Delta_X(X^n) \in A_n \qquad \text{for every } n \in \mathbb{N}. \tag{395}$$

Proof of (395): We will prove (395) by induction over n:
Induction base: Since $X^0 = 1$, we have

$$\begin{aligned}\Delta_X\left(X^0\right) = \Delta_X(1) &= 1_A \qquad \text{(since } \Delta_X \text{ is a } k\text{-algebra homomorphism)} \\ &\in A_0 \qquad \left(\begin{array}{c} \text{since } A \text{ is a graded } k\text{-algebra, and since any} \\ \text{graded } k\text{-algebra } B \text{ satisfies } 1_B \in B_0 \end{array} \right).\end{aligned}$$

In other words, (395) is proven for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that (395) holds for $n = N$. We need to show that (395) holds for $n = N + 1$.

We have $\Delta_X\left(X^N\right) \in A_N$ (since (395) holds for $n = N$). But every graded k-algebra B and any two nonnegative integers u and v satisfy $B_u B_v \subseteq B_{u+v}$. Applying this to $B = A$, $u = N$ and $v = 1$, we obtain $A_N A_1 \subseteq A_{N+1}$. Now, $X^{N+1} = X^N X$, so that

$$\begin{aligned}\Delta_X\left(X^{N+1}\right) = \Delta_X\left(X^N X\right) &= \underbrace{\Delta_X\left(X^N\right)}_{\in A_N} \cdot \underbrace{\Delta_X(X)}_{\in A_1} \qquad \text{(since } \Delta_X \text{ is a } k\text{-algebra homomorphism)} \\ &\in A_N A_1 \subseteq A_{N+1}.\end{aligned}$$

In other words, (395) holds for $n = N + 1$. This completes the induction step. The induction proof of (395) is thus complete.

Now, let $n \in \mathbb{N}$. We know that $(k[X])_n$ is a free k-module with basis (X^n). Thus, the k-module

Let us now recall one possible definition of a graded k-coalgebra: If C is a graded k-vector space, and $\Delta : C \to C \otimes C$ and $\varepsilon : C \to k$ are two k-linear maps such that (C, Δ, ε) is a k-coalgebra, then the k-coalgebra (C, Δ, ε) is graded if and only if the maps Δ and ε are graded. Applying this to $(C, \Delta, \varepsilon) = (k[X], \Delta_X, \varepsilon_X)$, we conclude that the k-coalgebra $(k[X], \Delta_X, \varepsilon_X)$ is graded if and only if the maps Δ_X and ε_X are graded (because we already know that $(k[X], \Delta_X, \varepsilon_X)$ is a k-coalgebra). Thus, the k-coalgebra $(k[X], \Delta_X, \varepsilon_X)$ is graded (since we know that the maps Δ_X and ε_X are graded). Combining this with the fact that the k-algebra $k[X]$ is graded, we conclude that the k-bialgebra $(k[X], \Delta_X, \varepsilon_X)$ is graded.

Denote the k-coalgebra $(k[X], \Delta_X, \varepsilon_X)$ by $k[X]$. Then, $\Delta_{k[X]} = \Delta_X$ and $\varepsilon_{k[X]} = \varepsilon_X$.

The graded k-coalgebra $k[X]$ is connected[191]. Since the graded k-coalgebra $k[X]$

$(k[X])_n$ is spanned by (X^n). In other words, $(k[X])_n = k \cdot X^n$. Thus,

$$\begin{aligned}\Delta_X\left((k[X])_n\right) &= \Delta_X\left(k \cdot X^n\right) = k \cdot \underbrace{\Delta_X\left(X^n\right)}_{\substack{\in A_n \\ \text{(by (395))}}} && \text{(since } \Delta_X \text{ is } k\text{-linear)} \\ &\subseteq k \cdot A_n \subseteq A_n && \text{(since } A_n \text{ is a } k\text{-vector space)}.\end{aligned}$$

Now, forget that we fixed n. We thus have proven that $\Delta_X\left((k[X])_n\right) \subseteq A_n$ for every $n \in \mathbb{N}$. In other words, the map Δ_X is graded, qed.

[190] *Proof.* Let us show that

$$\varepsilon_X\left(X^n\right) \in k_n \qquad \text{for every } n \in \mathbb{N}. \tag{396}$$

Proof of (396): Let $n \in \mathbb{N}$. If $n > 0$, then

$$\begin{aligned}\varepsilon_X\left(X^n\right) &= \left(\underbrace{\varepsilon_X(X)}_{=0}\right)^n && \text{(since } \varepsilon_X \text{ is a } k\text{-algebra homomorphism)} \\ &= 0^n = 0 && \text{(since } n > 0) \\ &\in k_n && \text{(since } k_n \text{ is a } k\text{-vector space)}.\end{aligned}$$

Hence, if $n > 0$, then (396) holds. Thus, for the rest of the proof of (396), we can WLOG assume that we don't have $n > 0$. Assume this.

We have $n \in \mathbb{N}$, but we don't have $n > 0$. Hence, $n = 0$. Thus, $k_n = k_0 = k$, so that $\varepsilon_X\left(X^n\right) \in k = k_n$. Hence, (396) is proven.

Now, let $n \in \mathbb{N}$. We know that $(k[X])_n$ is a free k-module with basis (X^n). Thus, the k-module $(k[X])_n$ is spanned by (X^n). In other words, $(k[X])_n = k \cdot X^n$. Thus,

$$\begin{aligned}\varepsilon_X\left((k[X])_n\right) &= \varepsilon_X\left(k \cdot X^n\right) = k \cdot \underbrace{\varepsilon_X\left(X^n\right)}_{\substack{\in k_n \\ \text{(by (396))}}} && \text{(since } \varepsilon_X \text{ is } k\text{-linear)} \\ &\subseteq k \cdot k_n \subseteq k_n && \text{(since } k_n \text{ is a } k\text{-vector space)}.\end{aligned}$$

Now, forget that we fixed n. We thus have proven that $\varepsilon_X\left((k[X])_n\right) \subseteq k_n$ for every $n \in \mathbb{N}$. In other words, the map ε_X is graded, qed.

[191] *Proof.* Recall that $(k[X])_n$ is a free k-module with basis (X^n) for every $n \in \mathbb{N}$. Applied to $n = 0$, this yields that $(k[X])_0$ is a free k-module with basis $\left(X^0\right)$. Hence, the k-module $(k[X])_0$ is spanned by $\left(X^0\right)$. In other words, $(k[X])_0 = k \cdot X^0$. Thus, $(k[X])_0 = k \cdot \underbrace{X^0}_{=1} = k \cdot 1$. Moreover, $\underbrace{\varepsilon_{k[X]}}_{=\varepsilon_X}(1) = \varepsilon_X(1) = 1$. Hence, Remark 16.12 (applied to $C = k[X]$ and $\lambda = 1$) yields that the graded k-coalgebra $k[X]$ is connected, qed.

is the graded k-coalgebra $(k[X], \Delta_X, \varepsilon_X)$, this rewrites as follows: The graded k-coalgebra $(k[X], \Delta_X, \varepsilon_X)$ is connected. Combining this with the fact that $(k[X], \Delta_X, \varepsilon_X)$ is a graded k-bialgebra, we conclude that $(k[X], \Delta_X, \varepsilon_X)$ is a connected graded k-bialgebra. Combining this with the fact that $k[X]$ is a commutative k-algebra, we obtain that $(k[X], \Delta_X, \varepsilon_X)$ is a commutative connected graded k-bialgebra. This proves Theorem 33.7. $\square$

Proposition 33.9. Let k be a field. Let X be a new symbol. Denote the commutative connected graded k-bialgebra $(k[X], \Delta_X, \varepsilon_X)$ defined in Theorem 33.7 simply by $k[X]$.

Let A be a k-bialgebra. Let $a \in A$ be a primitive element of A. Then, $\mathrm{ev}_{A,\, a} : k[X] \to A$ is a k-bialgebra homomorphism.

Proof of Proposition 33.9. By the definition of $\mathrm{ev}_{A,\, a}$, we know that $\mathrm{ev}_{A,\, a}$ is a k-algebra homomorphism. Thus, $\mathrm{ev}_{A,\, a}(1) = 1_A$.

We will use the notations defined in Theorem 33.7. The k-bialgebra $k[X]$ is defined as $(k[X], \Delta_X, \varepsilon_X)$. Thus, $\Delta_{k[X]} = \Delta_X$ and $\varepsilon_{k[X]} = \varepsilon_X$.

As in the proof of Theorem 33.7, we can show that

$$\Delta_X(X) = X \otimes 1 + 1 \otimes X \qquad \text{and} \qquad \varepsilon_X(X) = 0.$$

Since A is a k-bialgebra, we know that Δ_A and ε_A are k-algebra homomorphisms (due to the axioms of a k-bialgebra).

We know that $\mathrm{ev}_{A,\, a}$ and $\mathrm{ev}_{A,\, a}$ are k-algebra homomorphisms. Thus, their tensor product $\mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a}$ is a k-algebra homomorphism (since the tensor product of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that $\mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a}$ and $\Delta_{k[X]}$ are k-algebra homomorphisms. Thus, their composition $(\mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a}) \circ \Delta_{k[X]}$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that Δ_A and $\mathrm{ev}_{A,\, a}$ are k-algebra homomorphisms. Thus, their composition $\Delta_A \circ \mathrm{ev}_{A,\, a}$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism).

We know that ε_A and $\mathrm{ev}_{A,\, a}$ are k-algebra homomorphisms. Thus, their composition $\varepsilon_A \circ \mathrm{ev}_{A,\, a}$ is a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism).

Comparing

$$\begin{aligned}
&\left((\mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a}) \circ \Delta_{k[X]}\right)(X) \\
&= (\mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a}) \left(\underbrace{\Delta_{k[X]}}_{=\Delta_X}(X) \right) = (\mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a}) \left(\underbrace{\Delta_X(X)}_{=X\otimes 1 + 1 \otimes X} \right) \\
&= (\mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a})(X \otimes 1 + 1 \otimes X) = \underbrace{\mathrm{ev}_{A,\, a}(X)}_{\substack{=a \\ \text{(by (391))}}} \otimes \underbrace{\mathrm{ev}_{A,\, a}(1)}_{=1_A} + \underbrace{\mathrm{ev}_{A,\, a}(1)}_{=1_A} \otimes \underbrace{\mathrm{ev}_{A,\, a}(X)}_{\substack{=a \\ \text{(by (391))}}} \\
&\qquad \text{(by the definition of } \mathrm{ev}_{A,\, a} \otimes \mathrm{ev}_{A,\, a}) \\
&= a \otimes 1_A + 1_A \otimes a
\end{aligned}$$

with

$$(\Delta_A \circ \mathrm{ev}_{A,\ a})(X) = \Delta_A\left(\underbrace{\mathrm{ev}_{A,\ a}(X)}_{\substack{=a \\ (\text{by (391)})}}\right) = \Delta_A(a)$$
$$= a \otimes 1_A + 1_A \otimes a \qquad (\text{since } a \text{ is primitive}),$$

we obtain

$$\left((\mathrm{ev}_{A,\ a} \otimes \mathrm{ev}_{A,\ a}) \circ \Delta_{k[X]}\right)(X) = (\Delta_A \circ \mathrm{ev}_{A,\ a})(X).$$

Thus, Corollary 33.6 (applied to $A \otimes A$, $(\mathrm{ev}_{A,\ a} \otimes \mathrm{ev}_{A,\ a}) \circ \Delta_{k[X]}$ and $\Delta_A \circ \mathrm{ev}_{A,\ a}$ instead of A, f and g) yields

$$(\mathrm{ev}_{A,\ a} \otimes \mathrm{ev}_{A,\ a}) \circ \Delta_{k[X]} = \Delta_A \circ \mathrm{ev}_{A,\ a}$$

(since $(\mathrm{ev}_{A,\ a} \otimes \mathrm{ev}_{A,\ a}) \circ \Delta_{k[X]}$ and $\Delta_A \circ \mathrm{ev}_{A,\ a}$ are k-algebra homomorphisms).

But A is a k-bialgebra. Hence, Proposition 2.2 (applied to $C = A$) yields that $(A, 1_A)$ is a unital coalgebra. Since a is a primitive element of A, we have $a \in \operatorname{Prim} A$ (since $\operatorname{Prim} A$ is the set of all primitive elements of A). Thus, Remark 6.3 (applied to $H = A$ and $x = a$) yields that $\varepsilon(a) = 0$.

Comparing

$$\underbrace{\varepsilon_{k[X]}}_{=\varepsilon_X}(X) = \varepsilon_X(X) = 0$$

with

$$(\varepsilon_A \circ \mathrm{ev}_{A,\ a})(X) = \varepsilon_A\left(\underbrace{\mathrm{ev}_{A,\ a}(X)}_{\substack{=a \\ (\text{by (391)})}}\right) = \varepsilon_A(a) = \varepsilon(a) = 0,$$

we obtain

$$\varepsilon_{k[X]}(X) = (\varepsilon_A \circ \mathrm{ev}_{A,\ a})(X).$$

Thus, Corollary 33.6 (applied to k, $\varepsilon_{k[X]}$ and $\varepsilon_A \circ \mathrm{ev}_{A,\ a}$ instead of A, f and g) yields

$$\varepsilon_{k[X]} = \varepsilon_A \circ \mathrm{ev}_{A,\ a}$$

(since $\varepsilon_{k[X]}$ and $\varepsilon_A \circ \mathrm{ev}_{A,\ a}$ are k-algebra homomorphisms).

Now, recall the definition of a k-coalgebra homomorphism: If C and D are two k-coalgebras and $f : C \to D$ is a k-linear map, then the map f is a k-coalgebra homomorphism if and only if it satisfies the equalities $(f \otimes f) \circ \Delta_C = \Delta_D \circ f$ and $\varepsilon_C = \varepsilon_D \circ f$. Applying this to $C = k[X]$, $D = A$ and $f = \mathrm{ev}_{A,\ a}$, we obtain the following: The map $\mathrm{ev}_{A,\ a}$ is a k-coalgebra homomorphism if and only if it satisfies the equalities $(\mathrm{ev}_{A,\ a} \otimes \mathrm{ev}_{A,\ a}) \circ \Delta_{k[X]} = \Delta_A \circ \mathrm{ev}_{A,\ a}$ and $\varepsilon_{k[X]} = \varepsilon_A \circ \mathrm{ev}_{A,\ a}$. Thus, the map $\mathrm{ev}_{A,\ a}$ is a k-coalgebra homomorphism (because it satisfies the equalities $(\mathrm{ev}_{A,\ a} \otimes \mathrm{ev}_{A,\ a}) \circ \Delta_{k[X]} = \Delta_A \circ \mathrm{ev}_{A,\ a}$ and $\varepsilon_{k[X]} = \varepsilon_A \circ \mathrm{ev}_{A,\ a}$). Combining this with the fact that $\mathrm{ev}_{A,\ a}$ is a k-algebra homomorphism, we obtain that $\mathrm{ev}_{A,\ a}$ is a k-bialgebra homomorphism. This proves Proposition 33.9. $\square$

Proof of Theorem 33.2. Since F is a k-algebra homomorphism, we have $F(1_H) = 1_A$. Thus, $F \in G(H, A)$ [192]. Hence, $\operatorname{Log} F$ is a well-defined element of $\mathfrak{g}(H, A)$.

We have $v \in \operatorname{Prim} H$. This shows that v is a primitive element of H (since $\operatorname{Prim} H$ is the set of all primitive elements of H).

Let X be a new symbol. Denote the commutative connected graded k-bialgebra $(k[X], \Delta_X, \varepsilon_X)$ defined in Theorem 33.7 simply by $k[X]$. Then, $\Delta_{k[X]} = \Delta_X$ and $\varepsilon_{k[X]} = \varepsilon_X$.

As in the proof of Theorem 33.7, we can show that ε_X is a k-algebra homomorphism, and that $\varepsilon_X(X) = 0$.

Recall that $k[X]$ is a connected graded k-bialgebra, thus a connected graded k-coalgebra. Hence, $k[X]$ canonically becomes a filtered k-coalgebra (according to Convention 16.7, applied to $C = k[X]$). Remark 16.11 (applied to $C = k[X]$) shows that the graded k-coalgebra $k[X]$ is connected if and only if the filtered k-coalgebra $k[X]$ is connected. Thus, the filtered k-coalgebra $k[X]$ is connected (since we know that the graded k-coalgebra $k[X]$ is connected).

Proposition 33.9 (applied to H and v instead of A and a) yields that $\operatorname{ev}_{H,\, v} : k[X] \to H$ is a k-bialgebra homomorphism. In particular, this shows that $\operatorname{ev}_{H,\, v} : k[X] \to H$ is a k-coalgebra homomorphism.

Since $n > 1$, we have $n - 1 > 0$. Thus,

$$\begin{aligned}
\underbrace{\varepsilon_{k[X]}}_{=\varepsilon_X}\left(X^{n-1}\right) &= \varepsilon_X\left(X^{n-1}\right) \\
&= \left(\underbrace{\varepsilon_X(X)}_{=0}\right)^{n-1} && \text{(since } \varepsilon_X \text{ is a } k\text{-algebra homomorphism)} \\
&= 0^{n-1} = 0 && \text{(since } n-1 > 0\text{)}.
\end{aligned}$$

Also, $\underbrace{\varepsilon_{k[X]}}_{=\varepsilon_X}(X) = \varepsilon_X(X) = 0$.

We know that $\operatorname{ev}_{H,\, v}$ and F are k-algebra homomorphisms. Hence, their composition $F \circ \operatorname{ev}_{H,\, v}$ also is a k-algebra homomorphism (since the composition of any two k-algebra homomorphisms must be a k-algebra homomorphism). Thus, we can apply Corollary 31.4 to $k[X]$, $F \circ \operatorname{ev}_{H,\, v}$, X^{n-1} and X instead of H, F, x and y (because $\varepsilon_{k[X]}(X^{n-1}) = 0$ and $\varepsilon_{k[X]}(X) = 0$). As a consequence, we obtain that $\operatorname{Log}(F \circ \operatorname{ev}_{H,\, v})$ is a well-defined element of $\mathfrak{g}(k[X], A)$ and satisfies

$$\left(\operatorname{Log}(F \circ \operatorname{ev}_{H,\, v})\right)\left(X^{n-1} \cdot X\right) = 0. \tag{397}$$

Recall that $\operatorname{ev}_{H,\, v} : k[X] \to H$ is a k-algebra homomorphism, so that $\operatorname{ev}_{H,\, v}\left(1_{k[X]}\right) = 1_H$. Hence, Proposition 31.1 **(e)** (applied to $k[X]$, H and $\operatorname{ev}_{H,\, v}$ instead of D, C and φ) yields that $F \circ \operatorname{ev}_{H,\, v} \in G(k[X], A)$ and that $\operatorname{Log}(F \circ \operatorname{ev}_{H,\, v}) = (\operatorname{Log} F) \circ \operatorname{ev}_{H,\, v}$.

[192] *Proof.* By the definition of $G(H, A)$, we have $G(H, A) = \{f \in \mathcal{L}(H, A) \mid f(1_H) = 1_A\}$.

Now, since $F \in \mathcal{L}(H, A)$ and $F(1_H) = 1_A$, we have $F \in \{f \in \mathcal{L}(H, A) \mid f(1_H) = 1_A\} = G(H, A)$, qed.

Thus,

$$\begin{aligned}
&\left(\underbrace{\operatorname{Log}\left(F \circ \operatorname{ev}_{H,\ v}\right)}_{=(\operatorname{Log} F)\circ \operatorname{ev}_{H,\ v}}\right)\left(\underbrace{X^{n-1}\cdot X}_{=X^{(n-1)+1}=X^n}\right) \\
&= \left((\operatorname{Log} F)\circ \operatorname{ev}_{H,\ v}\right)\left(X^n\right) \\
&= (\operatorname{Log} F)\left(\begin{array}{c}\underbrace{\operatorname{ev}_{H,\ v}\left(X^n\right)}_{=\left(\operatorname{ev}_{H,\ v}(X)\right)^n} \\ \left(\text{since } \operatorname{ev}_{H,\ v} \text{ is a } k\text{-algebra homomorphism}\right)\end{array}\right) \\
&= (\operatorname{Log} F)\left(\left(\begin{array}{c}\underbrace{\operatorname{ev}_{H,\ v}(X)}_{=v} \\ \left(\text{by (391), applied to } H \text{ and } v \text{ instead of } A \text{ and } a\right)\end{array}\right)^n\right) = (\operatorname{Log} F)\left(v^n\right).
\end{aligned}$$

Comparing this with (397), we obtain $(\operatorname{Log} F)\left(v^n\right) = 0$. This completes the proof of Theorem 33.2. □

Proof of Theorem 33.1. We know that $\operatorname{id} : H \to H$ is a k-algebra homomorphism. Hence, we can apply Theorem 33.2 to $A = H$ and $F = \operatorname{id}$. Thus, we conclude that $\operatorname{id} \in G(H, H)$ and that $(\operatorname{Log} \operatorname{id})\left(v^n\right) = 0$. This proves Theorem 33.1. □

Using Theorem 33.2 and Theorem 32.1, we can prove a "symmetrized-product" version of Theorem 33.2:

Theorem 33.10. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a k-algebra. Let $F : H \to A$ be a k-algebra homomorphism. Let $n \in \mathbb{N}$ be such that $n > 1$. Let v_1, v_2, …, v_n be n elements of $\operatorname{Prim} H$. Then, $F \in G(H, A)$ and

$$(\operatorname{Log} F)\left(\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}\right) = 0.$$

Proof of Theorem 33.10. We have $F \in G(H, A)$ (this can be proven just as in the proof of Theorem 33.2).

We have $v_s \in \operatorname{Prim} H$ for every $s \in \{1, 2, \ldots, n\}$. For every $S \in \mathcal{P}(\{1, 2, \ldots, n\})$, we have

$$\sum_{s \in S} \underbrace{v_s}_{\in \operatorname{Prim} H} \in \sum_{s \in S} \operatorname{Prim} H \subseteq \operatorname{Prim} H$$

(since $\operatorname{Prim} H$ is a k-vector space). Hence, for every $S \in \mathcal{P}(\{1, 2, \ldots, n\})$, we have

$$(\operatorname{Log} F)\left(\left(\sum_{s \in S} v_s\right)^n\right) = 0 \tag{398}$$

(by Theorem 33.2, applied to $v = \sum_{s \in S} v_s$). Now, Theorem 32.1 (applied to H instead of A) yields

$$\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} = \sum_{S \in \mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left(\sum_{s \in S} v_s \right)^n .$$

Applying $\operatorname{Log} F$ to this equality, we obtain

$$\begin{aligned}
&(\operatorname{Log} F) \left(\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \right) \\
&= (\operatorname{Log} F) \left(\sum_{S \in \mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \left(\sum_{s \in S} v_s \right)^n \right) \\
&= \sum_{S \in \mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} \underbrace{(\operatorname{Log} F) \left(\left(\sum_{s \in S} v_s \right)^n \right)}_{\substack{=0 \\ \text{(by (398))}}} \qquad \text{(since } \operatorname{Log} F \text{ is } k\text{-linear)} \\
&= \sum_{S \in \mathcal{P}(\{1,2,\ldots,n\})} (-1)^{n-|S|} 0 = 0.
\end{aligned}$$

This proves Theorem 33.10. □

Of course, we can specialize Theorem 33.10 to a "symmetrized-product" version of Theorem 33.1:

Theorem 33.11. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let $n \in \mathbb{N}$ be such that $n > 1$. Let v_1, v_2, …, v_n be n elements of $\operatorname{Prim} H$. Then,

$$(\operatorname{Log} \mathrm{id}) \left(\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \right) = 0.$$

Proof of Theorem 33.11. We know that $\mathrm{id} : H \to H$ is a k-algebra homomorphism. Hence, we can apply Theorem 33.10 to $A = H$ and $F = \mathrm{id}$. Thus, we conclude that $\mathrm{id} \in G(H, H)$ and that $(\operatorname{Log} \mathrm{id}) \left(\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \right) = 0$. This proves Theorem 33.11. □

§34. Finishing the proof of Cartier-Milnor-Moore

We are now going to prepare for finishing the proof of Theorem 17.2. The final result we need is the following universal property of the universal enveloping algebra as a Hopf algebra. Before we state it, let us recall the universal property of the universal enveloping algebra as an algebra:

Proposition 34.1. Let k be a field. Let $\mathfrak{g}$ be a Lie algebra. Consider the universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$.

Let A be any k-algebra. Consider A as a Lie algebra under the commutator of the multiplication.

Let $\iota_{\mathfrak{g}} : \mathfrak{g} \to U(\mathfrak{g})$ be the canonical map from the Lie algebra $\mathfrak{g}$ into its universal enveloping algebra $U(\mathfrak{g})$.

Let $f : \mathfrak{g} \to A$ be a homomorphism of Lie algebras. Then, there exists a unique k-algebra homomorphism $F : U(\mathfrak{g}) \to A$ satisfying $F \circ \iota_{\mathfrak{g}} = f$.

Definition 34.2. In the situation of Proposition 34.1, the unique k-algebra homomorphism $F : U(\mathfrak{g}) \to A$ satisfying $F \circ \iota_{\mathfrak{g}} = f$ will be denoted by $\operatorname{Ulift} f$.

Proposition 34.3. Let k be a field. Let $\mathfrak{g}$ be a Lie algebra. Consider the universal enveloping algebra $U(\mathfrak{g})$ of $\mathfrak{g}$ equipped with its canonical Hopf algebra structure.

Let H be any k-bialgebra. Consider H as a Lie algebra under the commutator of the multiplication.

Let $f : \mathfrak{g} \to H$ be a homomorphism of Lie algebras such that $f(\mathfrak{g}) \subseteq \operatorname{Prim} H$. Then, $\operatorname{Ulift} f : U(\mathfrak{g}) \to H$ is a k-bialgebra homomorphism.

Proof of Proposition 34.3. Let $\iota_{\mathfrak{g}} : \mathfrak{g} \to U(\mathfrak{g})$ be the canonical map from the Lie algebra $\mathfrak{g}$ into its universal enveloping algebra $U(\mathfrak{g})$.

By the definition of $\operatorname{Ulift} f$, we know that $\operatorname{Ulift} f$ is the unique k-algebra homomorphism $F : U(\mathfrak{g}) \to H$ satisfying $F \circ \iota_{\mathfrak{g}} = f$. Hence, $\operatorname{Ulift} f$ is a k-algebra homomorphism $U(\mathfrak{g}) \to H$ and satisfies $(\operatorname{Ulift} f) \circ \iota_{\mathfrak{g}} = f$. Since $\operatorname{Ulift} f$ is a k-algebra homomorphism, it satisfies $(\operatorname{Ulift} f)\left(1_{U(\mathfrak{g})}\right) = 1_H$.

Clearly, $(\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)$ is a k-algebra homomorphism (since $\operatorname{Ulift} f$ is a k-algebra homomorphism, and since the tensor product of two k-algebra homomorphisms is a k-algebra homomorphism).

By the axioms of a k-bialgebra, we know that Δ_B and ε_B are k-algebra homomorphisms for every k-bialgebra B. Applying this to $B = U(\mathfrak{g})$, we see that $\Delta_{U(\mathfrak{g})}$ and $\varepsilon_{U(\mathfrak{g})}$ are k-algebra homomorphisms.

Since $\Delta_{U(\mathfrak{g})}$ and $(\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)$ are k-algebra homomorphisms, we conclude that $((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})}$ is a k-algebra homomorphism (because the composition of two k-algebra homomorphisms is a k-algebra homomorphism).

On the other hand, by the axioms of a k-bialgebra, we know that Δ_B and ε_B are k-algebra homomorphisms for every k-bialgebra B. Applying this to $B = H$, we see that Δ_H and ε_H are k-algebra homomorphisms.

Since $\operatorname{Ulift} f$ and Δ_H are k-algebra homomorphisms, we conclude that $\Delta_H \circ (\operatorname{Ulift} f)$ is a k-algebra homomorphism (because the composition of two k-algebra homomorphisms is a k-algebra homomorphism).

Consider $H \otimes H$ as a Lie algebra under the commutator of the multiplication. Then, Δ_H is a Lie algebra homomorphism (since Δ_H is a k-algebra homomorphism). Since Δ_H and f are Lie algebra homomorphisms, the composition $\Delta_H \circ f$ is a Lie algebra homomorphism (since the composition of two Lie algebra homomorphisms

is a Lie algebra homomorphism). Hence, Proposition 34.1 (applied to $H \otimes H$ and $\Delta_H \circ f$ instead of A and f) yields that there exists a unique k-algebra homomorphism $F : U(\mathfrak{g}) \to H \otimes H$ satisfying $F \circ \iota_{\mathfrak{g}} = \Delta_H \circ f$. In particular, there exists **at most one** such homomorphism. In other words,

$$\left(\begin{array}{c} \text{any two } k\text{-algebra homomorphisms } F : U(\mathfrak{g}) \to H \otimes H \\ \text{satisfying } F \circ \iota_{\mathfrak{g}} = \Delta_H \circ f \text{ must be equal} \end{array} \right). \tag{399}$$

Let $x \in \mathfrak{g}$. Then, $\Delta_{U(\mathfrak{g})}(\iota_{\mathfrak{g}}(x)) = \iota_{\mathfrak{g}}(x) \otimes 1_{U(\mathfrak{g})} + 1_{U(\mathfrak{g})} \otimes \iota_{\mathfrak{g}}(x)$ due to the definition of the comultiplication on the universal enveloping algebra $U(\mathfrak{g})$. Now,

$$\begin{aligned}
&\left(((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})} \circ \iota_{\mathfrak{g}}\right)(x) \\
&= ((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \underbrace{\left(\Delta_{U(\mathfrak{g})}(\iota_{\mathfrak{g}}(x))\right)}_{=\iota_{\mathfrak{g}}(x) \otimes 1_{U(\mathfrak{g})} + 1_{U(\mathfrak{g})} \otimes \iota_{\mathfrak{g}}(x)} \\
&= ((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \left(\iota_{\mathfrak{g}}(x) \otimes 1_{U(\mathfrak{g})} + 1_{U(\mathfrak{g})} \otimes \iota_{\mathfrak{g}}(x)\right) \\
&= \underbrace{(\operatorname{Ulift} f)(\iota_{\mathfrak{g}}(x))}_{\substack{=((\operatorname{Ulift} f) \circ \iota_g)(x) = f(x) \\ (\text{since } (\operatorname{Ulift} f) \circ \iota_g = f)}} \otimes \underbrace{(\operatorname{Ulift} f)\left(1_{U(\mathfrak{g})}\right)}_{=1_H} + \underbrace{(\operatorname{Ulift} f)\left(1_{U(\mathfrak{g})}\right)}_{=1_H} \otimes \underbrace{(\operatorname{Ulift} f)(\iota_{\mathfrak{g}}(x))}_{\substack{=((\operatorname{Ulift} f) \circ \iota_g)(x) = f(x) \\ (\text{since } (\operatorname{Ulift} f) \circ \iota_g = f)}} \\
&\qquad (\text{by the definition of } (\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \\
&= f(x) \otimes 1_H + 1_H \otimes f(x) = \Delta_H(f(x)) \\
&\qquad \left(\begin{array}{c} \text{since } f\left(\underbrace{x}_{\in \mathfrak{g}}\right) \in f(\mathfrak{g}) \subseteq \operatorname{Prim} H, \text{ so that } f(x) \text{ is primitive, and thus} \\ \Delta_H(f(x)) = f(x) \otimes 1_H + 1_H \otimes f(x) \end{array} \right) \\
&= (\Delta_H \circ f)(x).
\end{aligned}$$

Now, forget that we fixed x. We thus have shown that

$$\left(((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})} \circ \iota_{\mathfrak{g}}\right)(x) = (\Delta_H \circ f)(x)$$

for every $x \in \mathfrak{g}$. In other words, $((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})} \circ \iota_{\mathfrak{g}} = \Delta_H \circ f$. Hence, $((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})}$ is a k-algebra homomorphism $F : U(\mathfrak{g}) \to H \otimes H$ satisfying $F \circ \iota_{\mathfrak{g}} = \Delta_H \circ f$ (since we know that $((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})}$ is a k-algebra homomorphism).

On the other hand, $\Delta_H \circ (\operatorname{Ulift} f)$ is a k-algebra homomorphism and satisfies $\Delta_H \circ \underbrace{(\operatorname{Ulift} f) \circ \iota_{\mathfrak{g}}}_{=f} = \Delta_H \circ f$. Hence, $\Delta_H \circ (\operatorname{Ulift} f)$ is a k-algebra homomorphism $F : U(\mathfrak{g}) \to H \otimes H$ satisfying $F \circ \iota_{\mathfrak{g}} = \Delta_H \circ f$.

Now, we know that $((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})}$ and $\Delta_H \circ (\operatorname{Ulift} f)$ are two k-algebra homomorphisms $F : U(\mathfrak{g}) \to H \otimes H$ satisfying $F \circ \iota_{\mathfrak{g}} = \Delta_H \circ f$. Hence, $((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})}$ and $\Delta_H \circ (\operatorname{Ulift} f)$ must be equal (because (399) says that any two k-algebra homomorphisms $F : U(\mathfrak{g}) \to H \otimes H$ satisfying $F \circ \iota_{\mathfrak{g}} = \Delta_H \circ f$ must be equal). In other words,

$$((\operatorname{Ulift} f) \otimes (\operatorname{Ulift} f)) \circ \Delta_{U(\mathfrak{g})} = \Delta_H \circ (\operatorname{Ulift} f). \tag{400}$$

On the other hand, consider k endowed with the trivial Lie algebra structure (which is also given by the commutator of the multiplication on k). Then, $0 : U(\mathfrak{g}) \to k$ is

a Lie algebra homomorphism (since the zero map between two Lie algebras always is a Lie algebra homomorphism). Hence, Proposition 34.1 (applied to k and 0 instead of A and f) yields that there exists a unique k-algebra homomorphism $F : U(\mathfrak{g}) \to k$ satisfying $F \circ \iota_{\mathfrak{g}} = 0$. In particular, there exists **at most one** such homomorphism. In other words,

$$\left(\begin{array}{c} \text{any two } k\text{-algebra homomorphisms } F : U(\mathfrak{g}) \to k \\ \text{satisfying } F \circ \iota_{\mathfrak{g}} = 0 \text{ must be equal} \end{array} \right). \tag{401}$$

Now, every $x \in \mathfrak{g}$ satisfies $\left(\varepsilon_{U(\mathfrak{g})} \circ \iota_{\mathfrak{g}}\right)(x) = \varepsilon_{U(\mathfrak{g})}(\iota_{\mathfrak{g}}(x)) = 0$ (by the definition of the counit on the universal enveloping algebra $U(\mathfrak{g})$). Thus, every $x \in \mathfrak{g}$ satisfies $\left(\varepsilon_{U(\mathfrak{g})} \circ \iota_{\mathfrak{g}}\right)(x) = 0 = 0(x)$. In other words, $\varepsilon_{U(\mathfrak{g})} \circ \iota_{\mathfrak{g}} = 0$. Since $\varepsilon_{U(\mathfrak{g})}$ is a k-algebra homomorphism, this yields that $\varepsilon_{U(\mathfrak{g})}$ is a k-algebra homomorphism $F : U(\mathfrak{g}) \to k$ satisfying $F \circ \iota_{\mathfrak{g}} = 0$.

On the other hand, let $x \in \mathfrak{g}$. Then, $f\left(\underbrace{x}_{\in \mathfrak{g}}\right) \in f(\mathfrak{g}) \subseteq \operatorname{Prim} H$, so that $f(x)$ is a primitive element of H. Since H is a unital coalgebra (by Proposition 2.2), we can apply Remark 6.3 to $f(x)$ instead of x. As a result, we obtain $\varepsilon(f(x)) = 0$. In other words, $\varepsilon_H(f(x)) = 0$. Now,

$$\left(\varepsilon_H \circ \underbrace{(\operatorname{Ulift} f) \circ \iota_{\mathfrak{g}}}_{=f}\right)(x) = (\varepsilon_H \circ f)(x) = \varepsilon_H(f(x)) = 0 = 0(x).$$

Now, forget that we fixed x. We thus have proven that $(\varepsilon_H \circ (\operatorname{Ulift} f) \circ \iota_{\mathfrak{g}})(x) = 0(x)$ for every $x \in \mathfrak{g}$. In other words, $\varepsilon_H \circ (\operatorname{Ulift} f) \circ \iota_{\mathfrak{g}} = 0$. Since ε_H and $\operatorname{Ulift} f$ are k-algebra homomorphisms, their composition $\varepsilon_H \circ (\operatorname{Ulift} f)$ is a k-algebra homomorphism (since the composition of any two k-algebra homomorphisms is a k-algebra homomorphism). Since $\varepsilon_H \circ (\operatorname{Ulift} f) \circ \iota_{\mathfrak{g}} = 0$, this yields that $\varepsilon_H \circ (\operatorname{Ulift} f)$ is a k-algebra homomorphism $F : U(\mathfrak{g}) \to k$ satisfying $F \circ \iota_{\mathfrak{g}} = 0$.

Now, we know that $\varepsilon_{U(\mathfrak{g})}$ and $\varepsilon_H \circ (\operatorname{Ulift} f)$ are two k-algebra homomorphisms $F : U(\mathfrak{g}) \to k$ satisfying $F \circ \iota_{\mathfrak{g}} = 0$. Hence, $\varepsilon_{U(\mathfrak{g})}$ and $\varepsilon_H \circ (\operatorname{Ulift} f)$ must be equal (since (401) says that any two k-algebra homomorphisms $F : U(\mathfrak{g}) \to k$ satisfying $F \circ \iota_{\mathfrak{g}} = 0$ must be equal). In other words,

$$\varepsilon_{U(\mathfrak{g})} = \varepsilon_H \circ (\operatorname{Ulift} f).$$

Combined with (400), this yields that $\operatorname{Ulift} f$ is a k-coalgebra homomorphism. Combining this with the fact that $\operatorname{Ulift} f$ is a k-algebra homomorphism, we conclude that $\operatorname{Ulift} f$ is a k-bialgebra homomorphism. This proves Proposition 34.3. □

We are getting closer to the proof of the Cartier-Milnor-Moore theorem. Let us recall the definition of the tensor Hopf algebra:

Theorem 34.4. Let k be a field. Let V be a k-vector space. Then, there exists a unique k-bialgebra structure on the tensor algebra $\otimes V$ whose comultiplication $\Delta_{\otimes V}$ and counity $\varepsilon_{\otimes V}$ satisfy

$$\left(\begin{array}{ccc} \Delta_{\otimes V}(v) = v \otimes 1_{\otimes V} + 1_{\otimes V} \otimes v & \text{and} & \varepsilon_{\otimes V}(v) = 0 \\ & & \text{for every } v \in V \end{array} \right)$$

(where we consider V as a subspace of $\otimes V$).

Definition 34.5. Let k be a field. Let V be a k-vector space. Then, when we speak of the "k-bialgebra $\otimes V$", we mean the tensor algebra $\otimes V$ endowed with the unique k-bialgebra structure whose comultiplication $\Delta_{\otimes V}$ and counity $\varepsilon_{\otimes V}$ satisfy

$$\left(\begin{array}{ll} \Delta_{\otimes V}(v) = v \otimes 1_{\otimes V} + 1_{\otimes V} \otimes v & \text{and} \quad \varepsilon_{\otimes V}(v) = 0 \\ & \qquad \text{for every } v \in V \end{array} \right)$$

(where we consider V as a subspace of $\otimes V$). (This is well-defined due to Theorem 34.4.)

Theorem 34.6. Let k be a field. Let V be a k-vector space. Consider V as a subspace of $\otimes V$.

(a) The k-bialgebra $\otimes V$ is a Hopf algebra, whose antipode $S_{\otimes V}$ satisfies $S_{\otimes V}(v) = -v$ for every $v \in V$.

(b) The k-bialgebra $\otimes V$ is cocommutative.

(c) The standard grading on the k-vector space $\otimes V$ (the one where $(\otimes V)_n = V^{\otimes n}$ for every $n \in \mathbb{N}$) makes the k-bialgebra $\otimes V$ into a graded k-bialgebra.

(d) This graded k-bialgebra $\otimes V$ is connected.

We are now going to state similar properties of the universal enveloping Hopf algebra:

Theorem 34.7. Let k be a field. Let $\mathfrak{g}$ be a Lie algebra. Let $U(\mathfrak{g})$ denote the universal enveloping algebra of $\mathfrak{g}$.

Let $\iota_{\mathfrak{g}} : \mathfrak{g} \to U(\mathfrak{g})$ be the canonical map from the Lie algebra $\mathfrak{g}$ into its universal enveloping algebra $U(\mathfrak{g})$.

Then, there exists a unique k-bialgebra structure on the k-algebra $U(\mathfrak{g})$ whose comultiplication $\Delta_{U(\mathfrak{g})}$ and counity $\varepsilon_{U(\mathfrak{g})}$ satisfy

$$\left(\begin{array}{ll} \Delta_{U(\mathfrak{g})}(v) = v \otimes 1_{U(\mathfrak{g})} + 1_{U(\mathfrak{g})} \otimes v & \text{and} \quad \varepsilon_{U(\mathfrak{g})}(v) = 0 \\ & \qquad \text{for every } v \in \iota_{\mathfrak{g}}(\mathfrak{g}) \end{array} \right).$$

Definition 34.8. Let k be a field. Let $\mathfrak{g}$ be a Lie algebra. Let $U(\mathfrak{g})$ denote the universal enveloping algebra of $\mathfrak{g}$.

Let $\iota_{\mathfrak{g}} : \mathfrak{g} \to U(\mathfrak{g})$ be the canonical map from the Lie algebra $\mathfrak{g}$ into its universal enveloping algebra $U(\mathfrak{g})$.

Then, when we speak of the "k-bialgebra $U(\mathfrak{g})$", we mean the universal enveloping algebra $U(\mathfrak{g})$ endowed with the unique k-bialgebra structure whose comultiplication $\Delta_{U(\mathfrak{g})}$ and counity $\varepsilon_{U(\mathfrak{g})}$ satisfy

$$\left(\begin{array}{ll} \Delta_{U(\mathfrak{g})}(v) = v \otimes 1_{U(\mathfrak{g})} + 1_{U(\mathfrak{g})} \otimes v & \text{and} \quad \varepsilon_{U(\mathfrak{g})}(v) = 0 \\ & \qquad \text{for every } v \in \iota_{\mathfrak{g}}(\mathfrak{g}) \end{array} \right). \tag{402}$$

(This is well-defined due to Theorem 34.7.)

Theorem 34.9. Let k be a field. Let $\mathfrak{g}$ be a Lie algebra. Let $U(\mathfrak{g})$ denote the universal enveloping algebra of $\mathfrak{g}$.

Let $\iota_{\mathfrak{g}} : \mathfrak{g} \to U(\mathfrak{g})$ be the canonical map from the Lie algebra $\mathfrak{g}$ into its universal enveloping algebra $U(\mathfrak{g})$.

(a) We have $U(\mathfrak{g}) = \sum_{n \in \mathbb{N}} (\iota_{\mathfrak{g}}(\mathfrak{g}))^n$.

(b) The family $\left(\sum_{n=0}^{i} (\iota_{\mathfrak{g}}(\mathfrak{g}))^n \right)_{i \in \mathbb{N}}$ is a filtration of the k-vector space $U(\mathfrak{g})$.

(c) The k-bialgebra $U(\mathfrak{g})$ endowed with the filtration $\left(\sum_{n=0}^{i} (\iota_{\mathfrak{g}}(\mathfrak{g}))^n \right)_{i \in \mathbb{N}}$ is a connected filtered k-bialgebra.

(d) We have $\iota_{\mathfrak{g}}(\mathfrak{g}) \subseteq \operatorname{Prim}(U(\mathfrak{g}))$.

(e) The k-bialgebra $U(\mathfrak{g})$ is cocommutative.

(f) The k-bialgebra $U(\mathfrak{g})$ is a Hopf algebra.

A simple way to prove Theorem 34.9 is to deduce it from analogous properties of the tensor algebra $\otimes\mathfrak{g}$ (which are either part of Theorem 34.6 or trivial), because the k-bialgebra $U(\mathfrak{g})$ is a quotient of $\otimes\mathfrak{g}$ (as a k-bialgebra, not just as a k-algebra). We will use a different strategy. We will only prove the parts of Theorem 34.9 that we need, though.

Before we prove Theorem 34.9 proper, here is an auxiliary result:

Proposition 34.10. Let k be a field. Let H be a k-bialgebra. Let V be a k-vector subspace of H such that $H = \sum_{n \in \mathbb{N}} V^n$ and $\Delta_H(V) \subseteq V \otimes (k \cdot 1_H) + (k \cdot 1_H) \otimes V$. Then:

(a) The family $\left(\sum_{n=0}^{i} V^n \right)_{i \in \mathbb{N}}$ is a filtration of the k-vector space H.

(b) The k-bialgebra H endowed with the filtration $\left(\sum_{n=0}^{i} V^n \right)_{i \in \mathbb{N}}$ is a connected filtered k-bialgebra.

(c) If $V \subseteq \operatorname{Prim} H$, then the k-bialgebra H is cocommutative.

Before we prove this, let us collect some auxiliary facts. The following lemma is a basic fact about algebras:

Lemma 34.11. Let k be a field. Let U and V be two k-algebras. Let A and C be two k-vector subspaces of U. Let B and D be two k-vector subspaces of V. Then,

$$(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$$

(as k-vector subspaces of the k-algebra $U \otimes V$).

Proof of Lemma 34.11. **a)** We have

$$\alpha\gamma \in (AC) \otimes (BD) \qquad \text{for every } \alpha \in A \otimes B \text{ and } \gamma \in C \otimes D. \tag{403}$$

Proof of (403): Let $\alpha \in A \otimes B$ and $\gamma \in C \otimes D$.

We know that every tensor in a tensor product is a k-linear combination of pure tensors. Applying this to the tensor α in the tensor product $A \otimes B$, we conclude that the tensor α is a k-linear combination of pure tensors. In other words, there exists a $p \in \mathbb{N}$ and elements μ_1, μ_2, ..., μ_p of k and elements a_1, a_2, ..., a_p of A and elements b_1, b_2, ..., b_p of B such that $\alpha = \sum_{i=1}^{p} \mu_i a_i \otimes b_i$. Consider this p, these μ_1, μ_2, ..., μ_p, these a_1, a_2, ..., a_p and these b_1, b_2, ..., b_p.

We know that every tensor in a tensor product is a k-linear combination of pure tensors. Applying this to the tensor β in the tensor product $C \otimes D$, we conclude that the tensor γ is a k-linear combination of pure tensors. In other words, there exists a $q \in \mathbb{N}$ and elements ν_1, ν_2, ..., ν_q of k and elements c_1, c_2, ..., c_q of C and elements d_1, d_2, ..., d_q of D such that $\gamma = \sum_{j=1}^{q} \nu_j c_j \otimes d_j$. Consider this q, these ν_1, ν_2, ..., ν_q, these c_1, c_2, ..., c_q and these d_1, d_2, ..., d_q.

Multiplying the equality $\alpha = \sum_{i=1}^{p} \mu_i a_i \otimes b_i$ with the equality $\gamma = \sum_{j=1}^{q} \nu_j c_j \otimes d_j$, we obtain

$$\begin{aligned}
\alpha\gamma &= \left(\sum_{i=1}^{p} \mu_i a_i \otimes b_i \right) \left(\sum_{j=1}^{q} \nu_j c_j \otimes d_j \right) \\
&= \sum_{i=1}^{p} \mu_i \sum_{j=1}^{q} \nu_j \underbrace{\left(a_i \otimes b_i\right)\left(c_j \otimes d_j\right)}_{= a_i c_j \otimes b_i d_j} \\
&= \sum_{i=1}^{p} \mu_i \sum_{j=1}^{q} \nu_j \underbrace{a_i}_{\in A} \underbrace{c_j}_{\in C} \otimes \underbrace{b_i}_{\in B} \underbrace{d_j}_{\in D} \\
&\in \sum_{i=1}^{p} \mu_i \sum_{j=1}^{q} \nu_j \left(AC\right) \otimes \left(BD\right) \subseteq \left(AC\right) \otimes \left(BD\right)
\end{aligned}$$

(since $(AC) \otimes (BD)$ is a k-vector space). This proves (403).

b) We have

$$\left(A \otimes B\right) \cdot \left(C \otimes D\right) \subseteq \left(AC\right) \otimes \left(BD\right). \tag{404}$$

Proof of (404): Let $\xi \in (A \otimes B) \cdot (C \otimes D)$. We know that $(A \otimes B) \cdot (C \otimes D)$ is the k-linear span of the set of all products of the form $\alpha\gamma$ with $\alpha \in A \otimes B$ and $\gamma \in C \otimes D$ (by the definition of $(A \otimes B) \cdot (C \otimes D)$). In other words,

$$\begin{aligned}
&\left(A \otimes B\right) \cdot \left(C \otimes D\right) \\
&= (\text{the } k\text{-linear span of the set of all products of} \\
&\qquad \text{the form } \alpha\gamma \text{ with } \alpha \in A \otimes B \text{ and } \gamma \in C \otimes D) \\
&= (\text{the set of all } k\text{-linear combinations of products of} \\
&\qquad \text{the form } \alpha\gamma \text{ with } \alpha \in A \otimes B \text{ and } \gamma \in C \otimes D).
\end{aligned}$$

Hence,

$$\begin{aligned}&\xi \in (A \otimes B) \cdot (C \otimes D)\\ &= (\text{the set of all } k\text{-linear combinations of products of}\\ &\qquad\qquad \text{the form } \alpha\gamma \text{ with } \alpha \in A \otimes B \text{ and } \gamma \in C \otimes D)\,.\end{aligned}$$

Thus, ξ is a k-linear combination of products of the form $\alpha\gamma$ with $\alpha \in A \otimes B$ and $\gamma \in C \otimes D$. In other words, there exists an $n \in \mathbb{N}$ and elements λ_1, λ_2, ..., λ_n of k and elements α_1, α_2, ..., α_n of $A \otimes B$ and elements γ_1, γ_2, ..., γ_n of $C \otimes D$ such that $\xi = \sum_{\ell=1}^{n} \lambda_\ell \alpha_\ell \gamma_\ell$. Consider this n, these λ_1, λ_2, ..., λ_n, these α_1, α_2, ..., α_n and these γ_1, γ_2, ..., γ_n. Then,

$$\xi = \sum_{\ell=1}^{n} \lambda_\ell \underbrace{\alpha_\ell \gamma_\ell}_{\substack{\in (AC)\otimes(BD)\\ \text{(by (403), applied to } \alpha=\alpha_\ell \text{ and } \gamma=\gamma_\ell\text{)}}} \in \sum_{\ell=1}^{n} \lambda_\ell (AC) \otimes (BD) \subseteq (AC) \otimes (BD)$$

(since $(AC) \otimes (BD)$ is a k-vector space).

Now, forget that we fixed ξ. We thus have proven that every $\xi \in (A \otimes B) \cdot (C \otimes D)$ satisfies $\xi \in (AC) \otimes (BD)$. In other words, $(A \otimes B) \cdot (C \otimes D) \subseteq (AC) \otimes (BD)$. This proves (404).

c) We have

$$x \otimes y \in (A \otimes B) \cdot (C \otimes D) \qquad \text{for every } x \in AC \text{ and } y \in BD. \tag{405}$$

Proof of (405): Let $x \in AB$ and $y \in CD$.

We know that AC is the k-linear span of the set of all products of the form ac with $a \in A$ and $c \in C$ (by the definition of AC). In other words,

$$\begin{aligned}&AC\\ &= (\text{the } k\text{-linear span of the set of all products of the form } ac \text{ with } a \in A \text{ and } c \in C)\\ &= (\text{the set of all } k\text{-linear combinations of products of the form } ac \text{ with } a \in A \text{ and } c \in C)\,.\end{aligned}$$

Hence,

$$\begin{aligned}&x \in AC\\ &\quad = (\text{the set of all } k\text{-linear combinations of products of the form } ac \text{ with } a \in A \text{ and } c \in C)\,.\end{aligned}$$

Thus, x is a k-linear combination of products of the form ac with $a \in A$ and $c \in C$. In other words, there exists an $n \in \mathbb{N}$ and elements μ_1, μ_2, ..., μ_n of k and elements a_1, a_2, ..., a_n of A and elements c_1, c_2, ..., c_n of C such that $x = \sum_{i=1}^{n} \mu_i a_i c_i$. Consider this n, these μ_1, μ_2, ..., μ_n, these a_1, a_2, ..., a_n and these c_1, c_2, ..., c_n.

We know that BD is the k-linear span of the set of all products of the form bd with $b \in B$ and $d \in D$ (by the definition of BD). In other words,

$$\begin{aligned}&BD\\ &= (\text{the } k\text{-linear span of the set of all products of the form } bd \text{ with } b \in B \text{ and } d \in D)\\ &= (\text{the set of all } k\text{-linear combinations of products of the form } bd \text{ with } b \in B \text{ and } d \in D)\,.\end{aligned}$$

Hence,

$y \in BD$

$= (\text{the set of all } k\text{-linear combinations of products of the form } bd \text{ with } b \in B \text{ and } d \in D)$.

Thus, y is a k-linear combination of products of the form bd with $b \in B$ and $d \in D$. In other words, there exists an $m \in \mathbb{N}$ and elements ν_1, ν_2, ..., ν_m of k and elements b_1, b_2, ..., b_m of B and elements d_1, d_2, ..., d_m of D such that $y = \sum_{j=1}^{m} \nu_j b_j d_j$. Consider this m, these ν_1, ν_2, ..., ν_m, these b_1, b_2, ..., b_m and these d_1, d_2, ..., d_m.

Taking the tensor product of the equalities $x = \sum_{i=1}^{n} \mu_i a_i c_i$ and $y = \sum_{j=1}^{m} \nu_j b_j d_j$, we obtain

$$\begin{aligned}
x \otimes y &= \left(\sum_{i=1}^{n} \mu_i a_i c_i \right) \otimes \left(\sum_{j=1}^{m} \nu_j b_j d_j \right) \\
&= \sum_{i=1}^{n} \mu_i \sum_{j=1}^{m} \nu_j \underbrace{(a_i c_i) \otimes (b_j d_j)}_{=(a_i \otimes b_j) \cdot (c_i \otimes d_j)} \qquad \text{(since the tensor product is } k\text{-bilinear)} \\
&= \sum_{i=1}^{n} \mu_i \sum_{j=1}^{m} \nu_j \left(\underbrace{a_i}_{\in A} \otimes \underbrace{b_j}_{\in B} \right) \cdot \left(\underbrace{c_i}_{\in C} \otimes \underbrace{d_j}_{\in D} \right) \\
&\in \sum_{i=1}^{n} \mu_i \sum_{j=1}^{m} \nu_j \, (A \otimes B) \cdot (C \otimes D) \subseteq (A \otimes B) \cdot (C \otimes D)
\end{aligned}$$

(since $(A \otimes B) \cdot (C \otimes D)$ is a k-vector space). This proves (405).

d) We have

$$(AC) \otimes (BD) \subseteq (A \otimes B) \cdot (C \otimes D). \tag{406}$$

Proof. Let $\xi \in (AC) \otimes (BD)$.

We know that every tensor in a tensor product is a k-linear combination of pure tensors. Applying this to the tensor ξ in the tensor product $(AC) \otimes (BD)$, we conclude that the tensor ξ is a k-linear combination of pure tensors. In other words, there exists a $p \in \mathbb{N}$ and elements λ_1, λ_2, ..., λ_p of k and elements x_1, x_2, ..., x_p of AC and elements y_1, y_2, ..., y_p of BD such that $\xi = \sum_{i=1}^{p} \lambda_i x_i \otimes y_i$. Consider this p, these λ_1, λ_2, ..., λ_p, these x_1, x_2, ..., x_p and these y_1, y_2, ..., y_p. Now,

$$\xi = \sum_{i=1}^{p} \lambda_i \underbrace{x_i \otimes y_i}_{\substack{\in (A \otimes B) \cdot (C \otimes D) \\ \text{(by (405), applied to } x = x_i \text{ and } y = y_i)}} \in \sum_{i=1}^{p} \lambda_i \, (A \otimes B) \cdot (C \otimes D) \subseteq (A \otimes B) \cdot (C \otimes D)$$

(since $(A \otimes B) \cdot (C \otimes D)$ is a k-vector space).

Now, forget that we fixed ξ. We thus have shown that every $\xi \in (AC) \otimes (BD)$ satisfies $\xi \in (A \otimes B) \cdot (C \otimes D)$. In other words, $(AC) \otimes (BD) \subseteq (A \otimes B) \cdot (C \otimes D)$. This proves (406).

e) Combining (404) with (406), we obtain $(A \otimes B) \cdot (C \otimes D) = (AC) \otimes (BD)$. This proves Lemma 34.11. $\square$

Here is another very simple property of algebras:

Lemma 34.12. Let k be a field. Let A and B be two k-algebras. Let $f : A \to B$ and $g : A \to B$ be two k-algebra homomorphisms. Then, $\operatorname{Ker}(f-g)$ is a k-subalgebra of A.

Proof of Lemma 34.12. The maps f and g are k-algebra homomorphisms, therefore k-linear. Hence, their difference $f-g$ is also k-linear. Thus, $\operatorname{Ker}(f-g)$ is a k-vector subspace of A.

Since f is a k-algebra homomorphism, we have $f(1_A) = 1_B$. Since g is a k-algebra homomorphism, we have $g(1_A) = 1_B$. Thus, $(f-g)(1_A) = \underbrace{f(1_A)}_{=1_B} - \underbrace{g(1_A)}_{=1_B} = 1_B - 1_B = 0$. Hence, $1_A \in \operatorname{Ker}(f-g)$.

Now, let $a \in \operatorname{Ker}(f-g)$ and $b \in \operatorname{Ker}(f-g)$. Then, $(f-g)(a) = 0$ (since $a \in \operatorname{Ker}(f-g)$) and $(f-g)(b) = 0$ (since $b \in \operatorname{Ker}(f-g)$).

Since f is a k-algebra homomorphism, we have $f(ab) = f(a) f(b)$. Since g is a k-algebra homomorphism, we have $g(ab) = g(a) g(b)$. Since $0 = (f-g)(a) = f(a) - g(a)$, we have $g(a) = f(a)$. Since $0 = (f-g)(b) = f(b) - g(b)$, we have $g(b) = f(b)$. Now, $g(ab) = \underbrace{g(a)}_{=f(a)} \underbrace{g(b)}_{=f(b)} = f(a) f(b) = f(ab)$, so that $0 = f(ab) - g(ab) = (f-g)(ab)$. In other words, $(f-g)(ab) = 0$, so that $ab \in \operatorname{Ker}(f-g)$.

Now, forget that we fixed a and b. We thus have proven that $ab \in \operatorname{Ker}(f-g)$ for any $a \in \operatorname{Ker}(f-g)$ and $b \in \operatorname{Ker}(f-g)$. Combined with the fact that $1_A \in \operatorname{Ker}(f-g)$, this yields that $\operatorname{Ker}(f-g)$ is a k-subalgebra of A (since $\operatorname{Ker}(f-g)$ is a k-vector subspace of A). This proves Lemma 34.12. □

The next two propositions we state are completely elementary:

Proposition 34.13. Let k be a field. Let C and D be two k-coalgebras. Let $f : C \to D$ be an invertible k-coalgebra homomorphism. Then, f is a k-coalgebra isomorphism.

Proposition 34.14. Let k be a field. Let C and D be two k-bialgebras. Let $f : C \to D$ be an invertible k-bialgebra homomorphism. Then, f is a k-bialgebra isomorphism.

Propositions 34.13 and 34.14 are obvious "from the right viewpoint", but let us give down-to-earth proofs for them.

Proof of Proposition 34.13. The map f is an invertible k-coalgebra homomorphism, therefore an invertible k-linear map. Thus, its inverse f^{-1} is also a k-linear map.

Since f is a k-coalgebra homomorphism, we have $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$ and $\varepsilon_D \circ f = \varepsilon_C$. The second of these two equalities yields $\varepsilon_C = \varepsilon_D \circ f$. Now, (21) (applied to $U = C$, $V = D$, $W = C$, $U' = C$, $V' = D$, $W' = C$, $\alpha = f$, $\beta = f^{-1}$, $\gamma = f$ and $\delta = f^{-1}$) yields $(f^{-1} \circ f) \otimes (f^{-1} \circ f) = (f^{-1} \otimes f^{-1}) \circ (f \otimes f)$. Thus,

$$\left(f^{-1} \otimes f^{-1}\right) \circ (f \otimes f) = \underbrace{\left(f^{-1} \circ f\right)}_{=\mathrm{id}_C} \otimes \underbrace{\left(f^{-1} \circ f\right)}_{=\mathrm{id}_C} = \mathrm{id}_C \otimes \mathrm{id}_C = \mathrm{id}_{C \otimes C}.$$

Now,

$$\left(f^{-1} \otimes f^{-1}\right) \circ \underbrace{\Delta_D \circ f}_{=(f \otimes f) \circ \Delta_C} = \underbrace{\left(f^{-1} \otimes f^{-1}\right) \circ (f \otimes f)}_{=\mathrm{id}_{C \otimes C}} \circ \Delta_C = \Delta_C.$$

Hence, $\underbrace{\left(f^{-1} \otimes f^{-1}\right) \circ \Delta_D \circ f}_{=\Delta_C} \circ f^{-1} = \Delta_C \circ f^{-1}$, so that

$$\Delta_C \circ f^{-1} = \left(f^{-1} \otimes f^{-1}\right) \circ \Delta_D \circ \underbrace{f \circ f^{-1}}_{=\mathrm{id}_D} = \left(f^{-1} \otimes f^{-1}\right) \circ \Delta_D.$$

Combined with $\varepsilon_C \circ f^{-1} = \varepsilon_D$ (this follows from $\underbrace{\varepsilon_C}_{=\varepsilon_D \circ f} \circ f^{-1} = \varepsilon_D \circ \underbrace{f \circ f^{-1}}_{=\mathrm{id}_D} = \varepsilon_D$), this shows that f^{-1} is a k-coalgebra homomorphism.

Now, we know that f is a k-coalgebra homomorphism which has an inverse, and this inverse f^{-1} is also a k-coalgebra homomorphism. Hence, the homomorphism f is invertible in the category of k-coalgebras. In other words, f is a k-coalgebra isomorphism. Proposition 34.13 is thus proven. □

Proof of Proposition 34.14. The map f is a k-bialgebra homomorphism, thus a k-coalgebra homomorphism. Hence, f is an invertible k-coalgebra homomorphism. Therefore, Proposition 34.13 shows that f is a k-coalgebra isomorphism. Thus, the inverse f^{-1} of f is also a k-coalgebra homomorphism.

Also, f is a k-algebra homomorphism (since f is a k-bialgebra homomorphism). Thus, f is an invertible k-algebra homomorphism. It is well-known that this yields that f is a k-algebra isomorphism. Thus, we know that f is a k-algebra isomorphism. Hence, the inverse f^{-1} of f is also a k-algebra homomorphism.

Now, f^{-1} is both a k-algebra homomorphism and a k-coalgebra homomorphism. In other words, f^{-1} is a k-bialgebra homomorphism. So we know that f is a k-bialgebra homomorphism which has an inverse, and this inverse f^{-1} is also a k-bialgebra homomorphism. Hence, the homomorphism f is invertible in the category of k-bialgebras. In other words, f is a k-bialgebra isomorphism. Proposition 34.14 is thus proven. □

Proof of Proposition 34.10. **(a)** Clearly, every $i \in \mathbb{N}$ satisfies $\sum_{n=0}^{i} V^n \subseteq \sum_{n=0}^{i+1} V^n$ (since $\sum_{n=0}^{i+1} V^n = \sum_{n=0}^{i} V^n + V^{i+1} \supseteq \sum_{n=0}^{i} V^n$). In other words,

$$\sum_{n=0}^{0} V^n \subseteq \sum_{n=0}^{1} V^n \subseteq \sum_{n=0}^{2} V^n \subseteq \cdots. \tag{407}$$

Now, let $x \in H$. Then, $x \in H = \sum_{n \in \mathbb{N}} V^n$. Hence, there exists a family $(x_n)_{n \in \mathbb{N}} \in \prod_{n \in \mathbb{N}} V^n$ such that (all but finitely many $n \in \mathbb{N}$ satisfy $x_n = 0$) and $x = \sum_{n \in \mathbb{N}} x_n$. Consider this family $(x_n)_{n \in \mathbb{N}}$. We know that all but finitely many $n \in \mathbb{N}$ satisfy $x_n = 0$. Hence, there exists an $N \in \mathbb{N}$ such that every nonnegative integer $n > N$ satisfies $x_n = 0$.

Consider this N. We have

$$x = \sum_{n \in \mathbb{N}} x_n = \underbrace{\sum_{\substack{n \in \mathbb{N}; \\ n \leq N}} x_n}_{= \sum_{n=0}^{N}} + \sum_{\substack{n \in \mathbb{N}; \\ n > N}} \underbrace{x_n}_{\substack{=0 \\ (\text{since } n \geq N)}} = \sum_{n=0}^{N} x_n + \underbrace{\sum_{\substack{n \in \mathbb{N}; \\ n > N}} 0}_{=0}$$

$$= \sum_{n=0}^{N} \underbrace{x_n}_{\in V^n} \in \sum_{n=0}^{N} V^n \subseteq \bigcup_{i \in \mathbb{N}} \left(\sum_{n=0}^{i} V^n \right)$$

(since $N \in \mathbb{N}$, and since $\sum_{n=0}^{N} V^n = \sum_{n=0}^{i} V^n$ for $i = N$).

Now, forget that we fixed x. We thus have shown that every $x \in H$ satisfies $x \in \bigcup_{i \in \mathbb{N}} \left(\sum_{n=0}^{i} V^n \right)$. In other words, $H \subseteq \bigcup_{i \in \mathbb{N}} \left(\sum_{n=0}^{i} V^n \right)$. Combining this with $\bigcup_{i \in \mathbb{N}} \left(\sum_{n=0}^{i} V^n \right) \subseteq H$ (which is obvious), we obtain $H = \bigcup_{i \in \mathbb{N}} \left(\sum_{n=0}^{i} V^n \right)$. Combined with (407), this shows that $\left(\sum_{n=0}^{i} V^n \right)_{i \in \mathbb{N}}$ is a filtration of the k-vector space H. This proves Proposition 34.10 **(a)**.

(b) Let us denote the k-bialgebra H endowed with the filtration $\left(\sum_{n=0}^{i} V^n \right)_{i \in \mathbb{N}}$ simply by H. Then,

$$H_{\leq i} = \sum_{n=0}^{i} V^n \qquad \text{for every } i \in \mathbb{N}. \tag{408}$$

for every $i \in \mathbb{N}$.

We have

$$H_{\leq 0} = \sum_{n=0}^{0} V^n \qquad \text{(by (408), applied to } i = 0\text{)}$$
$$= V^0 = k \cdot 1_H,$$

and $1_H \in k \cdot 1_H = V^0 = H_{\leq 0}$.

Moreover, every $j \in \mathbb{N}$ satisfies

$$H_{\leq j} = \sum_{n=0}^{j} V^n \qquad \text{(by (408), applied to } j \text{ instead of } i\text{)}$$
$$= \sum_{m=0}^{j} V^m \qquad \text{(here, we renamed the summation index } n \text{ as } m\text{)}. \tag{409}$$

Now, every $i \in \mathbb{N}$ and $j \in \mathbb{N}$ satisfy $H_{\leq i} H_{\leq j} \subseteq H_{\leq i+j}$ [193]. Combining this observation with the fact that $1_H \in H_{\leq 0}$, we conclude that H is a filtered k-algebra.

[193] *Proof.* Let $i \in \mathbb{N}$ and $j \in \mathbb{N}$. Let $n \in \{0, 1, \ldots, i\}$ and $m \in \{0, 1, \ldots, j\}$. Then, $0 \leq n$ and

On the other hand, every $m \in \mathbb{N}$ satisfies

$$\Delta_H\left(V^m\right) \subseteq \sum_{u=0}^{m} V^u \otimes V^{m-u}. \tag{411}$$

$0 \leq m$, so that $0 = \underbrace{0}_{\leq n} + \underbrace{0}_{\leq m} \leq n+m$. Also, $n \leq i$ and $m \leq j$, so that $\underbrace{n}_{\leq i} + \underbrace{m}_{\leq j} \leq i+j$. Hence, $0 \leq n+m \leq i+j$, so that $n+m \in \{0,1,\ldots,i+j\}$. Hence, V^{n+m} is an addend in the sum $\sum\limits_{N=0}^{i+j} V^N$. Thus,

$$V^{n+m} \subseteq \sum_{N=0}^{i+j} V^N. \tag{410}$$

Now, forget that we fixed n and m. We thus have shown that (410) holds for all $n \in \{0,1,\ldots,i\}$ and $m \in \{0,1,\ldots,j\}$. Now,

$$\begin{aligned}
&\underbrace{H_{\leq i}}_{\substack{=\sum\limits_{n=0}^{i} V^n \\ \text{(by (408))}}} \cdot \underbrace{H_{\leq j}}_{\substack{=\sum\limits_{m=0}^{j} V^m \\ \text{(by (409))}}} \\
&= \left(\sum_{n=0}^{i} V^n\right) \cdot \left(\sum_{m=0}^{j} V^m\right) = \sum_{n=0}^{i}\sum_{m=0}^{j} \underbrace{V^n \cdot V^m}_{\substack{=V^{n+m} \subseteq \sum\limits_{N=0}^{i+j} V^N \\ \text{(by (410))}}} \subseteq \sum_{n=0}^{i}\sum_{m=0}^{j}\sum_{N=0}^{i+j} V^N \\
&\subseteq \sum_{N=0}^{i+j} V^N \qquad \left(\text{since } \sum_{N=0}^{i+j} V^N \text{ is a } k\text{-vector space}\right) \\
&= \sum_{n=0}^{i+j} V^n \qquad \text{(here, we renamed the summation index } N \text{ as } n) \\
&= H_{\leq i+j} \qquad \left(\text{since } H_{\leq i+j} = \sum_{n=0}^{i+j} V^n \text{ (by (408), applied to } i+j \text{ instead of } i)\right).
\end{aligned}$$

This proves $H_{\leq i} H_{\leq j} \subseteq H_{\leq i+j}$.

[194] Furthermore, every $m \in \mathbb{N}$ satisfies

$$V^i \subseteq H_{\leq m} \qquad \text{for every } i \in \{0, 1, \ldots, m\}. \tag{412}$$

[194] *Proof of (411):* We will prove (411) by induction over m:

Induction base: By the axioms of a k-bialgebra, the map Δ_H is a k-algebra homomorphism (since H is a k-bialgebra). Hence, $\Delta_H(1_H) = 1_{H \otimes H} = 1_H \otimes 1_H$.

We have $V^0 = k \cdot 1_H$, so that

$$\begin{aligned}\Delta_H\left(V^0\right) &= \Delta_H\left(k \cdot 1_H\right) = k \cdot \underbrace{\Delta_H\left(1_H\right)}_{=1_H \otimes 1_H} \qquad \text{(since } \Delta_H \text{ is } k\text{-linear)} \\ &= k \cdot \underbrace{1_H}_{\in V^0} \otimes \underbrace{1_H}_{\in V^0} \subseteq k \cdot V^0 \otimes V^0 \subseteq V^0 \otimes V^0\end{aligned}$$

(since $V^0 \otimes V^0$ is a k-vector space). On the other hand,

$$\sum_{u=0}^{0} V^u \otimes V^{0-u} = V^0 \otimes V^{0-0} = V^0 \otimes V^0.$$

Thus, $\Delta_H\left(V^0\right) \subseteq V^0 \otimes V^0 = \sum_{u=0}^{0} V^u \otimes V^{0-u}$. In other words, (411) holds for $m = 0$. This completes the induction base.

Induction step: Let $M \in \mathbb{N}$. Assume that (411) holds for $m = M$. We must now show that (411) also holds for $m = M + 1$.

We have

$$\Delta_H\left(V^M\right) \subseteq \sum_{u=0}^{M} V^u \otimes V^{M-u}$$

(since (411) holds for $m = M$). Now, $V^{M+1} = V^M \cdot V$, so that

$$\Delta_H\left(V^{M+1}\right) = \Delta_H\left(V^M \cdot V\right) = \underbrace{\Delta_H\left(V^M\right)}_{\subseteq \sum\limits_{u=0}^{M} V^u \otimes V^{M-u}} \cdot \underbrace{\Delta_H\left(V\right)}_{\subseteq V \otimes (k \cdot 1_H) + (k \cdot 1_H) \otimes V}$$

(since Δ_H is a k-algebra homomorphism)

$$\subseteq \left(\sum_{u=0}^{M} V^u \otimes V^{M-u}\right) \cdot \left(V \otimes (k \cdot 1_H) + (k \cdot 1_H) \otimes V\right)$$

$$= \left(\sum_{u=0}^{M} V^u \otimes V^{M-u}\right) \cdot \left(V \otimes (k \cdot 1_H)\right) + \left(\sum_{u=0}^{M} V^u \otimes V^{M-u}\right) \cdot \left((k \cdot 1_H) \otimes V\right)$$

$$= \sum_{u=0}^{M} \underbrace{\left(V^u \otimes V^{M-u}\right) \cdot \left(V \otimes (k \cdot 1_H)\right)}_{= (V^u \cdot V) \otimes \left(V^{M-u} \cdot (k \cdot 1_H)\right)}$$

(by Lemma 34.11, applied to H, H, V^u, V^{M-u}, V and $k \cdot 1_H$ instead of U, V, A, B, C and D)

$$+ \sum_{u=0}^{M} \underbrace{\left(V^u \otimes V^{M-u}\right) \cdot \left((k \cdot 1_H) \otimes V\right)}_{= (V^u \cdot (k \cdot 1_H)) \otimes \left(V^{M-u} \cdot V\right)}$$

(by Lemma 34.11, applied to H, H, V^u, V^{M-u}, $k \cdot 1_H$ and V instead of U, V, A, B, C and D)

$$= \sum_{u=0}^{M} \underbrace{\left(V^u \cdot V\right)}_{= V^{u+1}} \otimes \underbrace{\left(V^{M-u} \cdot (k \cdot 1_H)\right)}_{= V^{M-u} \cdot k \cdot 1_H = V^{M-u} \cdot k \subseteq V^{M-u}}$$

(since V^{M-u} is a k-vector space)

$$+ \sum_{u=0}^{M} \underbrace{\left(V^u \cdot (k \cdot 1_H)\right)}_{= V^u \cdot k \cdot 1_H = V^u \cdot k \subseteq V^u} \otimes \underbrace{\left(V^{M-u} \cdot V\right)}_{= V^{M-u+1} = V^{M+1-u}}$$

(since V^u is a k-vector space)

$$\subseteq \sum_{u=0}^{M} V^{u+1} \otimes V^{M-u} + \sum_{u=0}^{M} V^u \otimes V^{M+1-u}$$

[195] Finally, every $m \in \mathbb{N}$ satisfies

$$\Delta_H\left(H_{\leq m}\right) \subseteq \sum_{u=0}^{m} H_{\leq u} \otimes H_{\leq m-u}. \tag{413}$$

[196] Hence, H is a filtered k-coalgebra.

By the axioms of a k-bialgebra, we have $\varepsilon_H\left(1_H\right) = 1$ (since H is a k-bialgebra).

We have now shown that H is a filtered k-algebra, and that H is a filtered k-coalgebra. Combining these two observations, we conclude that H is a filtered k-bialgebra (since we know that H is a k-bialgebra). Thus, we can apply Remark 16.13

$$= \sum_{u=1}^{M+1} \underbrace{V^{(u-1)+1}}_{=V^u} \otimes \underbrace{V^{M-(u-1)}}_{=V^{M-u+1}=V^{M+1-u}} + \sum_{u=0}^{M} V^u \otimes V^{M+1-u}$$

(here, we substituted $u-1$ for u in the first sum)

$$\subseteq \underbrace{\sum_{u=1}^{M+1} V^u \otimes V^{M+1-u}}_{\substack{\subseteq \sum_{u=0}^{M+1} V^u \otimes V^{M+1-u} \\ \text{(since } 1 \geq 0\text{)}}} + \underbrace{\sum_{u=0}^{M} V^u \otimes V^{M+1-u}}_{\substack{\subseteq \sum_{u=0}^{M+1} V^u \otimes V^{M+1-u} \\ \text{(since } M \leq M+1\text{)}}}$$

$$\subseteq \sum_{u=0}^{M+1} V^u \otimes V^{M+1-u} + \sum_{u=0}^{M+1} V^u \otimes V^{M+1-u} \subseteq \sum_{u=0}^{M+1} V^u \otimes V^{M+1-u}$$

(since $\sum_{u=0}^{M+1} V^u \otimes V^{M+1-u}$ is a k-vector space). In other words, (411) also holds for $m = M+1$. This completes the induction step. The induction proof of (411) is thus finished.

[195] *Proof of (412):* Let $m \in \mathbb{N}$ and $i \in \{0, 1, \ldots, m\}$. We have $H_{\leq m} = \sum_{n=0}^{m} V^n$ (by (408), applied to $i = m$). But V^i is an addend in the sum $\sum_{n=0}^{m} V^n$ (since $i \in \{0, 1, \ldots, m\}$). Hence, $V^i \subseteq \sum_{n=0}^{m} V^n = H_{\leq m}$. This proves (412).

[196] *Proof of (413):* Let $m \in \mathbb{N}$. Applying (408) to $i = m$, we obtain $H_{\leq m} = \sum_{n=0}^{m} V^n$. Thus,

$$\Delta_H\left(H_{\leq m}\right) = \Delta_H\left(\sum_{n=0}^{m} V^n\right) = \sum_{n=0}^{m} \underbrace{\Delta_H\left(V^n\right)}_{\substack{\subseteq \sum_{u=0}^{n} V^u \otimes V^{n-u} \\ \text{(by (411),} \\ \text{applied to } n \text{ instead of } m\text{)}}} \qquad \text{(since } \Delta_H \text{ is } k\text{-linear)}$$

$$\subseteq \sum_{n=0}^{m} \sum_{u=0}^{n} \underbrace{V^u}_{\substack{\subseteq H_{\leq u} \\ \text{(by (412), applied to} \\ u \text{ and } u \text{ instead of } m \text{ and } i \\ \text{(since } u \in \{0,1,\ldots,u\}\text{))}}} \otimes \underbrace{V^{n-u}}_{\substack{\subseteq H_{\leq m-u} \\ \text{(by (412), applied to} \\ m-u \text{ and } n-u \text{ instead of } m \text{ and } i \\ \text{(since } n-u \in \{0,1,\ldots,m-u\} \\ \text{(because } n-u \geq 0 \text{ (since } u \leq n\text{) and} \\ n-u \leq m-u \text{ (since } n \leq m\text{))))}}$$

$$\subseteq \sum_{n=0}^{m} \underbrace{\sum_{u=0}^{n} H_{\leq u} \otimes H_{\leq m-u}}_{\substack{\subseteq \sum_{u=0}^{m} H_{\leq u} \otimes H_{\leq m-u} \\ \text{(since } n \leq m\text{)}}} \subseteq \sum_{n=0}^{m} \sum_{u=0}^{m} H_{\leq u} \otimes H_{\leq m-u} \subseteq \sum_{u=0}^{m} H_{\leq u} \otimes H_{\leq m-u}$$

(since $\sum_{u=0}^{m} H_{\leq u} \otimes H_{\leq m-u}$ is a k-vector space). This proves (413).

to $C = H$ and $\lambda = 1_H$ (since $H_{\leq 0} = k \cdot 1_H$ and $\varepsilon_H(1_H) = 1$). As a result, we conclude that the filtered k-coalgebra H is connected. Thus, the filtered k-bialgebra H is connected.

We thus have shown that H is a connected filtered k-bialgebra. Since the filtration on H is $\left(\sum_{n=0}^{i} V^n\right)_{i \in \mathbb{N}}$, this rewrites as follows: The k-bialgebra H endowed with the filtration $\left(\sum_{n=0}^{i} V^n\right)_{i \in \mathbb{N}}$ is a connected filtered k-bialgebra. Thus, Proposition 34.10 **(b)** is proven.

(c) Assume that $V \subseteq \operatorname{Prim} H$.

Consider the (H,H)-flip $\tau_{H,H} : H \otimes H \to H \otimes H$ (defined according to Definition 9.2).

It is known that for any two k-algebras A and B, the (A,B)-flip $\tau_{A,B} : A \otimes B \to B \otimes A$ is a k-algebra homomorphism. Applying this to $A = H$ and $B = H$, we conclude that the (H,H)-flip $\tau_{H,H} : H \otimes H \to H \otimes H$ is a k-algebra homomorphism.

Also, H is a k-bialgebra. Thus, Δ_H is a k-algebra homomorphism (by the axioms of a k-bialgebra).

We know that $\tau_{H,H}$ and Δ_H are k-algebra homomorphisms. Hence, their composition $\tau_{H,H} \circ \Delta_H$ is a k-algebra homomorphism (because the composition of two k-algebra homomorphisms must always be a k-algebra homomorphism).

Since Δ_H and $\tau_{H,H} \circ \Delta_H$ are k-algebra homomorphisms, we know that $\operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$ is a k-subalgebra of H (by Lemma 34.12, applied to H, $H \otimes H$, Δ_H and $\tau_{H,H} \circ \Delta_H$ instead of A, B, f and g).

Clearly, every k-subalgebra $\mathfrak{A}$ of H satisfies $\mathfrak{A}^n \subseteq \mathfrak{A}$ for every $n \in \mathbb{N}$. Applying this to $\mathfrak{A} = \operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$, we conclude that $(\operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H))^n \subseteq \operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$ for every $n \in \mathbb{N}$ (because $\operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$ is a k-subalgebra of H).

Now, it is easy to see that $V \subseteq \operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$ [197]. Thus, every $n \in \mathbb{N}$ satisfies

$$V^n \subseteq (\operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H))^n \subseteq \operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H).$$

[197] *Proof.* Let $v \in V$. Then, $v \in V \subseteq \operatorname{Prim} H$. In other words, v is a primitive element of H (since $\operatorname{Prim} H$ is the set of all primitive elements of H). In other words, $\Delta_H(x) = x \otimes 1_H + 1_H \otimes x$. Now,

$$\begin{aligned}
(\tau_{H,H} \circ \Delta_H)(x) &= \tau_{H,H}\left(\underbrace{\Delta_H(x)}_{= x \otimes 1_H + 1_H \otimes x}\right) = \tau_{H,H}(x \otimes 1_H + 1_H \otimes x) \\
&= \underbrace{\tau_{H,H}(x \otimes 1_H)}_{\substack{= 1_H \otimes x \\ \text{(by the definition of } \tau_{H,H}\text{)}}} + \underbrace{\tau_{H,H}(1_H \otimes x)}_{\substack{= x \otimes 1_H \\ \text{(by the definition of } \tau_{H,H}\text{)}}} \qquad \text{(since } \tau_{H,H} \text{ is } k\text{-linear)} \\
&= 1_H \otimes x + x \otimes 1_H = x \otimes 1_H + 1_H \otimes x = \Delta_H(x).
\end{aligned}$$

Thus,

$$(\Delta_H - \tau_{H,H} \circ \Delta_H)(x) = \Delta_H(x) - \underbrace{(\tau_{H,H} \circ \Delta_H)(x)}_{= \Delta_H(x)} = \Delta_H(x) - \Delta_H(x) = 0.$$

In other words, $x \in \operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$.

Now, forget that we fixed x. We thus have shown that every $x \in V$ satisfies $x \in \operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$. In other words, $V \subseteq \operatorname{Ker}(\Delta_H - \tau_{H,H} \circ \Delta_H)$, qed.

Now,

$$H = \sum_{n \in \mathbb{N}} \underbrace{V^n}_{\subseteq \operatorname{Ker}\left(\Delta_H - \tau_{H,H} \circ \Delta_H\right)} \subseteq \sum_{n \in \mathbb{N}} \operatorname{Ker}\left(\Delta_H - \tau_{H,H} \circ \Delta_H\right) \subseteq \operatorname{Ker}\left(\Delta_H - \tau_{H,H} \circ \Delta_H\right)$$

(since $\operatorname{Ker}\left(\Delta_H - \tau_{H,H} \circ \Delta_H\right)$ is a k-vector space). In other words, every $x \in H$ satisfies $x \in \operatorname{Ker}\left(\Delta_H - \tau_{H,H} \circ \Delta_H\right)$. In other words, every $x \in H$ satisfies $\left(\Delta_H - \tau_{H,H} \circ \Delta_H\right)(x) = 0$. In other words, $\Delta_H - \tau_{H,H} \circ \Delta_H = 0$. Thus, $\Delta_H = \tau_{H,H} \circ \Delta_H$. In other words, $\tau_{H,H} \circ \Delta_H = \Delta_H$.

Now, let us recall the definition of a cocommutative k-coalgebra: A k-coalgebra C is cocommutative if and only if $\tau_{C,C} \circ \Delta_C = \Delta_C$. Applying this to $C = H$, we conclude that the k-coalgebra H is cocommutative if and only if $\tau_{H,H} \circ \Delta_H = \Delta_H$. Thus, the k-coalgebra H is cocommutative (since $\tau_{H,H} \circ \Delta_H = \Delta_H$). In other words, the k-bialgebra H is cocommutative. This proves Proposition 34.10 **(c)**. □

Partial proof of Theorem 34.9. First of all, we have $\iota_{\mathfrak{g}}(\mathfrak{g}) \subseteq \operatorname{Prim}(U(\mathfrak{g}))$ [198]. This proves Theorem 34.9 **(d)**.

Let π be the canonical projection $\otimes\mathfrak{g} \to U(\mathfrak{g})$. Then, π is a surjective k-algebra homomorphism. [Actually, π is a k-bialgebra homomorphism, but we don't need to know this.]

The canonical map $\iota_{\mathfrak{g}}$ from $\mathfrak{g}$ to $U(\mathfrak{g})$ factors through the projection $\pi : \otimes\mathfrak{g} \to U(\mathfrak{g})$. More precisely, $\iota_{\mathfrak{g}}(x) = \pi(x)$ for every $x \in \mathfrak{g}$ (this follows from the definition of $\iota_{\mathfrak{g}}$). Thus,

$$\iota_{\mathfrak{g}}(\mathfrak{g}) = \left\{ \underbrace{\iota_{\mathfrak{g}}(x)}_{=\pi(x)} \mid x \in \mathfrak{g} \right\} = \{\pi(x) \mid x \in \mathfrak{g}\} = \pi(\mathfrak{g}). \tag{414}$$

By the definition of the tensor algebra, we have $\otimes\mathfrak{g} = \bigoplus_{n \in \mathbb{N}} \mathfrak{g}^{\otimes n}$. Thus, $\otimes\mathfrak{g} = \bigoplus_{n \in \mathbb{N}} \mathfrak{g}^{\otimes n} = \sum_{n \in \mathbb{N}} \mathfrak{g}^{\otimes n}$ (since direct sums are sums).

For every $n \in \mathbb{N}$, we have $\mathfrak{g}^{\otimes n} = \mathfrak{g}^n$ as k-vector subspaces of $\otimes\mathfrak{g}$ (where $\mathfrak{g}^n$ means $\underbrace{\mathfrak{g} \cdot \mathfrak{g} \cdot \cdots \cdot \mathfrak{g}}_{n \text{ times}}$, as usual) [199]. Hence, $\sum_{n \in \mathbb{N}} \mathfrak{g}^{\otimes n} = \sum_{n \in \mathbb{N}} \mathfrak{g}^n$.

---

[198] *Proof.* Let $v \in \iota_{\mathfrak{g}}(\mathfrak{g})$. Then, $\Delta_{U(\mathfrak{g})}(v) = v \otimes 1_{U(\mathfrak{g})} + 1_{U(\mathfrak{g})} \otimes v$ (according to (402)). In other words, the element v of $U(\mathfrak{g})$ is primitive. In other words, $v \in \operatorname{Prim}(U(\mathfrak{g}))$ (since $\operatorname{Prim}(U(\mathfrak{g}))$ is the set of all primitive elements of $U(\mathfrak{g})$).

Now, forget that we fixed v. We thus have shown that every $v \in \iota_{\mathfrak{g}}(\mathfrak{g})$ satisfies $v \in \operatorname{Prim}(U(\mathfrak{g}))$. In other words, $\iota_{\mathfrak{g}}(\mathfrak{g}) \subseteq \operatorname{Prim}(U(\mathfrak{g}))$, qed.

[199] *Proof.* Let $n \in \mathbb{N}$. The n-th tensor power $\mathfrak{g}^{\otimes n}$ is spanned by all pure tensors. In other words,

$$\mathfrak{g}^{\otimes n} = \left\langle \underbrace{v_1 \otimes v_2 \otimes \cdots \otimes v_n}_{\substack{=v_1 v_2 \cdots v_n \\ \text{(because the multiplication on } \otimes\mathfrak{g} \text{ is the} \\ \text{tensor product, so we have} \\ v_1 v_2 \cdots v_n = v_1 \otimes v_2 \otimes \cdots \otimes v_n)}} \mid (v_1, v_2, \ldots, v_n) \in \mathfrak{g}^{\times n} \right\rangle$$
$$= \left\langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in \mathfrak{g}^{\times n} \right\rangle.$$

Compared with

$$\mathfrak{g}^n = \left\langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in \mathfrak{g}^{\times n} \right\rangle,$$

this yields $\mathfrak{g}^{\otimes n} = \mathfrak{g}^n$, qed.

Now, $\otimes\mathfrak{g} = \sum\limits_{n\in\mathbb{N}} \mathfrak{g}^{\otimes n} = \sum\limits_{n\in\mathbb{N}} \mathfrak{g}^n$. Applying the map π to this equality, we obtain

$$\pi\left(\otimes\mathfrak{g}\right) = \pi\left(\sum_{n\in\mathbb{N}} \mathfrak{g}^n\right) = \sum_{n\in\mathbb{N}} \left(\underbrace{\pi\left(\mathfrak{g}\right)}_{\substack{=\iota_{\mathfrak{g}}(\mathfrak{g}) \\ \text{(by (414))}}}\right)^n \qquad \text{(since } \pi \text{ is a } k\text{-algebra homomorphism)}$$
$$= \sum_{n\in\mathbb{N}} \left(\iota_{\mathfrak{g}}\left(\mathfrak{g}\right)\right)^n.$$

Since $\pi\left(\otimes\mathfrak{g}\right) = U\left(\mathfrak{g}\right)$ (because π is surjective), this rewrites as $U\left(\mathfrak{g}\right) = \sum\limits_{n\in\mathbb{N}} \left(\iota_{\mathfrak{g}}\left(\mathfrak{g}\right)\right)^n$. Thus, Theorem 34.9 **(a)** is proven.

We have

$$\Delta_{U(\mathfrak{g})}\left(\iota_{\mathfrak{g}}\left(\mathfrak{g}\right)\right) \subseteq \iota_{\mathfrak{g}}\left(\mathfrak{g}\right) \otimes \left(k\cdot 1_{U(\mathfrak{g})}\right) + \left(k\cdot 1_{U(\mathfrak{g})}\right) \otimes \iota_{\mathfrak{g}}\left(\mathfrak{g}\right).$$

[200] Combining this with the equality $U\left(\mathfrak{g}\right) = \sum\limits_{n\in\mathbb{N}} \left(\iota_{\mathfrak{g}}\left(\mathfrak{g}\right)\right)^n$, we see that we can apply Proposition 34.10 to $H = U\left(\mathfrak{g}\right)$ and $V = \iota_{\mathfrak{g}}\left(\mathfrak{g}\right)$.

Proposition 34.10 **(a)** (applied to $H = U\left(\mathfrak{g}\right)$ and $V = \iota_{\mathfrak{g}}\left(\mathfrak{g}\right)$) yields that the family $\left(\sum\limits_{n=0}^{i} \left(\iota_{\mathfrak{g}}\left(\mathfrak{g}\right)\right)^n\right)_{i\in\mathbb{N}}$ is a filtration of the k-vector space $U\left(\mathfrak{g}\right)$. This proves Theorem 34.9 **(b)**.

Proposition 34.10 **(b)** (applied to $H = U\left(\mathfrak{g}\right)$ and $V = \iota_{\mathfrak{g}}\left(\mathfrak{g}\right)$) yields that the k-bialgebra $U\left(\mathfrak{g}\right)$ endowed with the filtration $\left(\sum\limits_{n=0}^{i} \left(\iota_{\mathfrak{g}}\left(\mathfrak{g}\right)\right)^n\right)_{i\in\mathbb{N}}$ is a connected filtered k-bialgebra. This proves Theorem 34.9 **(c)**.

Finally, Proposition 34.10 **(c)** (applied to $H = U\left(\mathfrak{g}\right)$ and $V = \iota_{\mathfrak{g}}\left(\mathfrak{g}\right)$) yields that the k-bialgebra $U\left(\mathfrak{g}\right)$ is cocommutative (since $\iota_{\mathfrak{g}}\left(\mathfrak{g}\right) \subseteq \operatorname{Prim}\left(U\left(\mathfrak{g}\right)\right)$). This proves Theorem 34.9 **(e)**.

We are not going to prove Theorem 34.9 **(f)** (as we are not going to need it). □

Now, we can finally prove the Cartier-Milnor-Moore theorem:

Proof of Theorem 17.2. Consider H as a Lie algebra under the commutator of the multiplication of H. Then, $\operatorname{Prim} H$ is a Lie subalgebra of H [201].

In the following, the symbol "id" without a subscript will always mean id_H.

Let $\mathfrak{i}$ be the inclusion map $\operatorname{Prim} H \to H$. Clearly, $\mathfrak{i}$ is a Lie algebra homomorphism. Hence, a k-algebra homomorphism $\operatorname{Ulift}\mathfrak{i} : U\left(\operatorname{Prim} H\right) \to H$ is well-defined (according to Definition 34.2).

---

[200] *Proof.* Every $v \in \iota_{\mathfrak{g}}\left(\mathfrak{g}\right)$ satisfies

$$\Delta_{U(\mathfrak{g})}\left(v\right) = \underbrace{v}_{\in\iota_{\mathfrak{g}}(\mathfrak{g})} \otimes \underbrace{1_{U(\mathfrak{g})}}_{\in k\cdot 1_{U(\mathfrak{g})}} + \underbrace{1_{U(\mathfrak{g})}}_{\in k\cdot 1_{U(\mathfrak{g})}} \otimes \underbrace{v}_{\in\iota_{\mathfrak{g}}(\mathfrak{g})} \qquad \text{(according to (402))}$$
$$\in \iota_{\mathfrak{g}}\left(\mathfrak{g}\right) \otimes \left(k\cdot 1_{U(\mathfrak{g})}\right) + \left(k\cdot 1_{U(\mathfrak{g})}\right) \otimes \iota_{\mathfrak{g}}\left(\mathfrak{g}\right).$$

In other words, $\Delta_{U(\mathfrak{g})}\left(\iota_{\mathfrak{g}}\left(\mathfrak{g}\right)\right) \subseteq \iota_{\mathfrak{g}}\left(\mathfrak{g}\right) \otimes \left(k\cdot 1_{U(\mathfrak{g})}\right) + \left(k\cdot 1_{U(\mathfrak{g})}\right) \otimes \iota_{\mathfrak{g}}\left(\mathfrak{g}\right)$, qed.

[201] since every $x \in \operatorname{Prim} H$ and $y \in \operatorname{Prim} H$ satisfy $xy - yx \in \operatorname{Prim} H$ (according to Proposition 17.14)

Since $\mathfrak{i}$ is the inclusion map $\operatorname{Prim} H \to H$, we have $\mathfrak{i}(\operatorname{Prim} H) = \operatorname{Prim} H$. Thus, Proposition 34.3 (applied to $\mathfrak{g} = \operatorname{Prim} H$ and $f = \mathfrak{i}$) yields that $\operatorname{Ulift} \mathfrak{i} : U(\operatorname{Prim} H) \to H$ is a k-bialgebra homomorphism.

Let $\iota_{\operatorname{Prim} H} : \operatorname{Prim} H \to U(\operatorname{Prim} H)$ be the canonical map from the Lie algebra $\operatorname{Prim} H$ into its universal enveloping algebra $U(\operatorname{Prim} H)$. By the definition of $\operatorname{Ulift} \mathfrak{i}$, we know that $\operatorname{Ulift} \mathfrak{i}$ is the unique k-algebra homomorphism $F : U(\operatorname{Prim} H) \to H$ satisfying $F \circ \iota_{\operatorname{Prim} H} = \mathfrak{i}$. Hence, $\operatorname{Ulift} \mathfrak{i}$ is a k-algebra homomorphism $U(\operatorname{Prim} H) \to H$ and satisfies $(\operatorname{Ulift} \mathfrak{i}) \circ \iota_{\operatorname{Prim} H} = \mathfrak{i}$.

a) The map $\operatorname{Ulift} \mathfrak{i}$ is surjective.

Proof. Since $\operatorname{Ulift} \mathfrak{i}$ is a k-algebra homomorphism, its image $(\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H))$ is a k-subalgebra of H. We have

$$(\operatorname{Ulift} \mathfrak{i})(\iota_{\operatorname{Prim} H}(\operatorname{Prim} H)) = \underbrace{((\operatorname{Ulift} \mathfrak{i}) \circ \iota_{\operatorname{Prim} H})}_{=\mathfrak{i}}(\operatorname{Prim} H) = \mathfrak{i}(\operatorname{Prim} H) = \operatorname{Prim} H.$$

Hence,

$$\operatorname{Prim} H = (\operatorname{Ulift} \mathfrak{i}) \left(\underbrace{\iota_{\operatorname{Prim} H}(\operatorname{Prim} H)}_{\subseteq U(\operatorname{Prim} H)} \right) \subseteq (\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H)).$$

Hence, $(\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H))$ contains $\operatorname{Prim} H$ as a subset. Thus, $(\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H))$ is a k-subalgebra of H containing $\operatorname{Prim} H$ as a subset (since $(\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H))$ is a k-subalgebra of H).

Now, Theorem 17.1 yields

$$H = \operatorname{AlgGen}_k(\operatorname{Prim} H) = (\text{the } k\text{-subalgebra of } H \text{ generated by } \operatorname{Prim} H)$$

(by the definition of $\operatorname{AlgGen}_k(\operatorname{Prim} H)$). In other words, the k-subalgebra of H generated by $\operatorname{Prim} H$ is the algebra H.

But the k-subalgebra of H generated by $\operatorname{Prim} H$ is the smallest k-subalgebra of H containing $\operatorname{Prim} H$ as a subset (by the definition of the k-subalgebra of H generated by $\operatorname{Prim} H$). Since the k-subalgebra of H generated by $\operatorname{Prim} H$ is the algebra H, this rewrites as follows: The algebra H is the smallest k-subalgebra of H containing $\operatorname{Prim} H$ as a subset. This means that whenever V is a k-subalgebra of H containing $\operatorname{Prim} H$ as a subset, we must necessarily have $H \subseteq V$. Applying this to $V = (\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H))$, we obtain $H \subseteq (\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H))$ (since $(\operatorname{Ulift} \mathfrak{i})(U(\operatorname{Prim} H))$ is a k-subalgebra of H containing $\operatorname{Prim} H$ as a subset). In other words, the map $\operatorname{Ulift} \mathfrak{i}$ is surjective.

b) Theorem 4.1 yields that the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$ is a projection from H to the subspace $\operatorname{Prim} H$ of all primitive elements of H. Thus, $(\operatorname{Log} \operatorname{id})(H) \subseteq \operatorname{Prim} H$. Hence, every $x \in H$ satisfies $(\operatorname{Log} \operatorname{id}) \left(\underbrace{x}_{\in H} \right) \in (\operatorname{Log} \operatorname{id})(H) \subseteq \operatorname{Prim} H$. Thus, we can define a map $\operatorname{eul} : H \to \operatorname{Prim} H$ by

$$(\operatorname{eul} x = (\operatorname{Log} \operatorname{id})(x) \qquad \text{for every } x \in H).$$

This map eul is k-linear[202]. Moreover, $\operatorname{eul}(1_H) = 0$ [203].

Now, let $\widetilde{\iota}$ be the map $\iota_{\operatorname{Prim} H} \circ \operatorname{eul} : H \to U(\operatorname{Prim} H)$. This map $\widetilde{\iota}$ is k-linear (since it is the composition of the k-linear maps $\iota_{\operatorname{Prim} H}$ and eul). Moreover, $\widetilde{\iota}(1_H) = 0$ [204]. Thus, $\widetilde{\iota} \in \mathfrak{g}(H, U(\operatorname{Prim} H))$ [205].

c) Applying Theorem 34.9 **(b)** to $\mathfrak{g} = \operatorname{Prim} H$, we see that the family $\left(\sum_{n=0}^{i} \left(\iota_{\operatorname{Prim} H}(\operatorname{Prim} H)\right)^n\right)_{i \in \mathbb{N}}$ is a filtration of the k-vector space $U(\operatorname{Prim} H)$. Applying Theorem 34.9 **(c)** to $\mathfrak{g} = \operatorname{Prim} H$, we see that the k-bialgebra $U(\operatorname{Prim} H)$ endowed with the filtration $\left(\sum_{n=0}^{i} \left(\iota_{\operatorname{Prim} H}(\operatorname{Prim} H)\right)^n\right)_{i \in \mathbb{N}}$ is a connected filtered k-bialgebra. This connected filtered k-bialgebra will be simply denoted by $U(\operatorname{Prim} H)$ in the following. Thus, $(U(\operatorname{Prim} H))_{\leq i} = \sum_{n=0}^{i} \left(\iota_{\operatorname{Prim} H}(\operatorname{Prim} H)\right)^n$ for every $i \in \mathbb{N}$.

We know that $U(\operatorname{Prim} H)$ is a connected filtered k-bialgebra. Hence, $U(\operatorname{Prim} H)$ is a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure.

Every k-bialgebra A satisfies $\operatorname{id}_A \in G(A, A)$ [206]. Applying this to $A = U(\operatorname{Prim} H)$, we obtain $\operatorname{id}_{U(\operatorname{Prim} H)} \in G(U(\operatorname{Prim} H), U(\operatorname{Prim} H))$. Hence, $\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)$ is a well-defined element of $\mathfrak{g}(U(\operatorname{Prim} H), U(\operatorname{Prim} H))$. Therefore,

$$\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(1_{U(\operatorname{Prim} H)}\right) = 0 \tag{415}$$

---

[202] *Proof.* Let $\lambda \in k$, $\mu \in k$, $a \in H$ and $b \in H$. By the definition of eul, we have the equalities $\operatorname{eul}(\lambda a + \mu b) = (\operatorname{Log} \operatorname{id})(\lambda a + \mu b)$, $\operatorname{eul} a = (\operatorname{Log} \operatorname{id})(a)$ and $\operatorname{eul} b = (\operatorname{Log} \operatorname{id})(b)$. Now,

$$\begin{aligned}\operatorname{eul}(\lambda a + \mu b) &= (\operatorname{Log} \operatorname{id})(\lambda a + \mu b) = \lambda \underbrace{(\operatorname{Log} \operatorname{id})(a)}_{=\operatorname{eul} a} + \mu \underbrace{(\operatorname{Log} \operatorname{id})(b)}_{=\operatorname{eul} b} \qquad \text{(since } \operatorname{Log} \operatorname{id} \text{ is } k\text{-linear)} \\ &= \lambda \operatorname{eul}(a) + \mu \operatorname{eul}(b).\end{aligned}$$

Now, forget that we fixed λ, μ, a and b. We thus have shown that $\operatorname{eul}(\lambda a + \mu b) = \lambda \operatorname{eul}(a) + \mu \operatorname{eul}(b)$ for all $\lambda \in k$, $\mu \in k$, $a \in H$ and $b \in H$. In other words, the map eul is k-linear, qed.

[203] *Proof.* We have $\operatorname{Log} F \in \mathfrak{g}(H, H)$ for every $F \in G(H, H)$. Applying this to $F = \operatorname{id}$, we obtain

$$\operatorname{Log} \operatorname{id} \in \mathfrak{g}(H, H) = \{f \in \mathcal{L}(H, H) \mid f(1_H) = 0\}$$

(by the definition of $\mathfrak{g}(H, H)$). In other words, $\operatorname{Log} \operatorname{id}$ is an element of $\mathcal{L}(H, H)$ and satisfies $(\operatorname{Log} \operatorname{id})(1_H) = 0$.

Now, by the definition of eul, we have $\operatorname{eul}(1_H) = (\operatorname{Log} \operatorname{id})(1_H) = 0$, qed.

[204] *Proof.* Since $\widetilde{\iota} = \iota_{\operatorname{Prim} H} \circ \operatorname{eul}$, we have $\widetilde{\iota}(1_H) = (\iota_{\operatorname{Prim} H} \circ \operatorname{eul})(1_H) = \iota_{\operatorname{Prim} H}\left(\underbrace{\operatorname{eul}(1_H)}_{=0}\right) = \iota_{\operatorname{Prim} H}(0) = 0$ (since $\iota_{\operatorname{Prim} H}$ is k-linear), qed.

[205] *Proof.* By the definition of $\mathfrak{g}(H, U(\operatorname{Prim} H))$, we have $\mathfrak{g}(H, U(\operatorname{Prim} H)) = \{f \in \mathcal{L}(H, U(\operatorname{Prim} H)) \mid f(1_H) = 0\}$.

But $\widetilde{\iota}$ satisfies $\widetilde{\iota} \in \mathcal{L}(H, U(\operatorname{Prim} H))$ and $\widetilde{\iota}(1_H) = 0$. In other words, $\widetilde{\iota} \in \{f \in \mathcal{L}(H, U(\operatorname{Prim} H)) \mid f(1_H) = 0\} = \mathfrak{g}(H, U(\operatorname{Prim} H))$, qed.

[206] *Proof.* Let A be a k-bialgebra. By the definition of $G(A, A)$, we have $G(A, A) = \{f \in \mathcal{L}(A, A) \mid f(1_A) = 1_A\}$. Now, id_A satisfies $\operatorname{id}_A \in \mathcal{L}(A, A)$ and $\operatorname{id}_A(1_A) = 1_A$. In other words, $\operatorname{id}_A \in \{f \in \mathcal{L}(A, A) \mid f(1_A) = 1_A\} = G(A, A)$, qed.

[207].

d) We have

$$\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(v^n\right) = \left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right) \qquad \text{for every } v \in \iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right) \text{ and } n \in \mathbb{N}. \tag{416}$$

Proof of (416): Let $v \in \iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right)$ and $n \in \mathbb{N}$. Since $v \in \iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right)$, there exists a $w \in \operatorname{Prim} H$ such that $v = \iota_{\operatorname{Prim} H}\left(w\right)$. Consider this w.

Theorem 34.9 **(d)** (applied to $\mathfrak{g} = \operatorname{Prim} H$) yields $\iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right) \subseteq \operatorname{Prim}\left(U\left(\operatorname{Prim} H\right)\right)$. Thus, $v \in \iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right) \subseteq \operatorname{Prim}\left(U\left(\operatorname{Prim} H\right)\right)$.

Recall that $\left(\operatorname{Ulift} \mathfrak{i}\right) \circ \iota_{\operatorname{Prim} H} = \mathfrak{i}$. Thus, $\left(\left(\operatorname{Ulift} \mathfrak{i}\right) \circ \iota_{\operatorname{Prim} H}\right)\left(w\right) = \mathfrak{i}\left(w\right) = w$ (since $\mathfrak{i}$ is just an inclusion map). Thus,

$$w = \left(\left(\operatorname{Ulift} \mathfrak{i}\right) \circ \iota_{\operatorname{Prim} H}\right)\left(w\right) = \left(\operatorname{Ulift} \mathfrak{i}\right)\left(\underbrace{\iota_{\operatorname{Prim} H}\left(w\right)}_{=v}\right) = \left(\operatorname{Ulift} \mathfrak{i}\right)\left(v\right).$$

Now, since $\operatorname{Ulift} \mathfrak{i}$ is a k-algebra homomorphism, we have

$$\left(\operatorname{Ulift} \mathfrak{i}\right)\left(v^n\right) = \left(\underbrace{\left(\operatorname{Ulift} \mathfrak{i}\right)\left(v\right)}_{=w}\right)^n = w^n,$$

so that

$$\left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right) = \widetilde{\iota}\left(\underbrace{\left(\operatorname{Ulift} \mathfrak{i}\right)\left(v^n\right)}_{=w^n}\right) = \widetilde{\iota}\left(w^n\right). \tag{417}$$

Now, we distinguish between three cases:

Case 1: We have $n = 0$.

Case 2: We have $n = 1$.

Case 3: We have neither $n = 0$ nor $n = 1$.

Let us first consider Case 1. In this case, we have $n = 0$. Thus, $v^n = v^0 = 1_{U(\operatorname{Prim} H)}$, so that

$$\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(v^n\right) = \left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(1_{U(\operatorname{Prim} H)}\right) = 0$$

(by (415)). Comparing this with

$$\begin{aligned}\left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right) &= \widetilde{\iota}\left(w^n\right) && \text{(by (417))} \\ &= \widetilde{\iota}\left(1_H\right) && \left(\text{since } n = 0, \text{ so that } w^n = w^0 = 1_H\right) \\ &= 0,\end{aligned}$$

we obtain $\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(v^n\right) = \left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right)$. Hence, (416) is proven in Case 1.

[207] *Proof of (415):* We have

$$\begin{aligned}\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right) &\in \mathfrak{g}\left(U\left(\operatorname{Prim} H\right), U\left(\operatorname{Prim} H\right)\right) \\ &= \left\{f \in \mathcal{L}\left(U\left(\operatorname{Prim} H\right), U\left(\operatorname{Prim} H\right)\right) \mid f\left(1_{U(\operatorname{Prim} H)}\right) = 0\right\}\end{aligned}$$

(by the definition of $\mathfrak{g}\left(U\left(\operatorname{Prim} H\right), U\left(\operatorname{Prim} H\right)\right)$). In other words, $\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right) \in \mathcal{L}\left(U\left(\operatorname{Prim} H\right), U\left(\operatorname{Prim} H\right)\right)$ and $\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(1_{U(\operatorname{Prim} H)}\right) = 0$. This proves (415).

Let us now consider Case 2. In this case, we have $n = 1$. Thus, $v^n = v^1 = v$.

Now, recall that $\mathrm{id}_{U(\operatorname{Prim} H)} \in G\left(U\left(\operatorname{Prim} H\right), U\left(\operatorname{Prim} H\right)\right)$. Hence, Proposition 6.2 **(c)** (applied to $U\left(\operatorname{Prim} H\right)$, $U\left(\operatorname{Prim} H\right)$ and $\mathrm{id}_{U(\operatorname{Prim} H)}$ instead of H, A and F) yields that

$$\left(\operatorname{Log}\left(\mathrm{id}_{U(\operatorname{Prim} H)}\right)\right)|_{\operatorname{Prim}(U(\operatorname{Prim} H))} = \mathrm{id}_{U(\operatorname{Prim} H)}|_{\operatorname{Prim}(U(\operatorname{Prim} H))}. \tag{418}$$

On the other hand, recall that every k-bialgebra A satisfies $\mathrm{id}_A \in G(A, A)$. Applying this to $A = H$, we obtain $\mathrm{id}_H \in G(H, H)$. In other words, $\mathrm{id} \in G(H, H)$. Thus, Proposition 6.2 **(c)** (applied to H and id instead of A and F) yields that $(\operatorname{Log} \mathrm{id})|_{\operatorname{Prim} H} = \mathrm{id}|_{\operatorname{Prim} H}$.

Now, we have

$$\begin{aligned}
\left(\operatorname{Log}\left(\mathrm{id}_{U(\operatorname{Prim} H)}\right)\right)\left(\underbrace{v^n}_{=v}\right) &= \left(\operatorname{Log}\left(\mathrm{id}_{U(\operatorname{Prim} H)}\right)\right)(v) \\
&= \left(\underbrace{\left(\operatorname{Log}\left(\mathrm{id}_{U(\operatorname{Prim} H)}\right)\right)|_{\operatorname{Prim}(U(\operatorname{Prim} H))}}_{\substack{=\mathrm{id}_{U(\operatorname{Prim} H)}|_{\operatorname{Prim}(U(\operatorname{Prim} H))} \\ \text{(by (418))}}}\right)(v) \\
&\qquad \left(\text{since } v \in \operatorname{Prim}\left(U\left(\operatorname{Prim} H\right)\right)\right) \\
&= \left(\mathrm{id}_{U(\operatorname{Prim} H)}|_{\operatorname{Prim}(U(\operatorname{Prim} H))}\right)(v) = \mathrm{id}_{U(\operatorname{Prim} H)}(v) = v.
\end{aligned}$$

Comparing this with

$$\begin{aligned}
\left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)(v^n) &= \widetilde{\iota}(w^n) \qquad \text{(by (417))} \\
&= \widetilde{\iota}(w) \qquad \left(\text{since } n = 1, \text{ so that } w^n = w^1 = w\right) \\
&= \left(\iota_{\operatorname{Prim} H} \circ \operatorname{eul}\right)(w) \qquad \left(\text{since } \widetilde{\iota} = \iota_{\operatorname{Prim} H} \circ \operatorname{eul}\right) \\
&= \iota_{\operatorname{Prim} H}\left(\underbrace{\operatorname{eul} w}_{\substack{=(\operatorname{Log}\mathrm{id})(w) \\ \text{(by the definition of eul)}}}\right) = \iota_{\operatorname{Prim} H}\left(\underbrace{(\operatorname{Log}\mathrm{id})(w)}_{\substack{=((\operatorname{Log}\mathrm{id})|_{\operatorname{Prim} H})(w) \\ \text{(since } w \in \operatorname{Prim} H\text{)}}}\right) \\
&= \iota_{\operatorname{Prim} H}\left(\underbrace{\left((\operatorname{Log}\mathrm{id})|_{\operatorname{Prim} H}\right)(w)}_{=\mathrm{id}|_{\operatorname{Prim} H}}\right) = \iota_{\operatorname{Prim} H}\left(\underbrace{(\mathrm{id}|_{\operatorname{Prim} H})(w)}_{=\mathrm{id}(w)=w}\right) \\
&= \iota_{\operatorname{Prim} H}(w) = v,
\end{aligned}$$

we obtain $\left(\operatorname{Log}\left(\mathrm{id}_{U(\operatorname{Prim} H)}\right)\right)(v^n) = \left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)(v^n)$. Hence, (416) is proven in Case 2.

Let us finally consider Case 3. In this case, we have neither $n = 0$ nor $n = 1$. Since $n \in \mathbb{N}$, we must thus have $n > 1$. We have $v \in \operatorname{Prim}\left(U\left(\operatorname{Prim} H\right)\right)$. Thus, Theorem 33.1 (applied to $U\left(\operatorname{Prim} H\right)$ instead of H) yields

$$\left(\operatorname{Log}\left(\mathrm{id}_{U(\operatorname{Prim} H)}\right)\right)(v^n) = 0.$$

On the other hand, $w \in \operatorname{Prim} H$. Hence, Theorem 33.1 (applied to w instead of v) yields $(\operatorname{Log}\mathrm{id})(w^n) = 0$. Now, comparing

$$\left(\operatorname{Log}\left(\mathrm{id}_{U(\operatorname{Prim} H)}\right)\right)(v^n) = 0$$

with

$$\begin{aligned}
\left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right) &= \widetilde{\iota}\left(w^n\right) && \text{(by (417))} \\
&= \left(\iota_{\operatorname{Prim} H} \circ \operatorname{eul}\right)\left(w^n\right) && \left(\text{since } \widetilde{\iota} = \iota_{\operatorname{Prim} H} \circ \operatorname{eul}\right) \\
&= \iota_{\operatorname{Prim} H}\left(\underbrace{\operatorname{eul}\left(w^n\right)}_{\substack{=(\operatorname{Log} \operatorname{id})\left(w^n\right) \\ \text{(by the definition of eul)}}}\right) = \iota_{\operatorname{Prim} H}\left(\underbrace{\left(\operatorname{Log} \operatorname{id}\right)\left(w^n\right)}_{=0}\right) \\
&= \iota_{\operatorname{Prim} H}\left(0\right) = 0 && \left(\text{since } \iota_{\operatorname{Prim} H} \text{ is } k\text{-linear}\right),
\end{aligned}$$

we obtain $\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(v^n\right) = \left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right)$. Hence, (416) is proven in Case 3.

We have thus proven (416) in each of the three cases 1, 2 and 3. Since these three cases cover all possibilities, this yields that (416) always holds. The proof of (416) is thus complete.

e) We have

$$\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right) = \widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right). \tag{419}$$

Proof of (419): Let V be the k-vector subspace $\iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right)$ of $U\left(\operatorname{Prim} H\right)$. Then, $xy - yx \in V$ for any $x \in V$ and $y \in V$ [208]. Moreover,

$$\begin{aligned}
U\left(\operatorname{Prim} H\right) &= \sum_{n \in \mathbb{N}} \left(\underbrace{\iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right)}_{=V}\right)^n && \text{(by Theorem 34.9 \textbf{(a)}, applied to } \mathfrak{g} = \operatorname{Prim} H) \\
&= \sum_{n \in \mathbb{N}} V^n.
\end{aligned}$$

Finally, we have $\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(v^n\right) = \left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right)$ for every $v \in V$ and $n \in \mathbb{N}$ [209]. Consequently, we can apply Corollary 32.7 to $U\left(\operatorname{Prim} H\right)$, $U\left(\operatorname{Prim} H\right)$, $\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)$ and $\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)$ instead of A, W, f and g. As a result, we obtain $\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right) = \widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)$. This proves (419).

f) We have

$$\operatorname{id}_{U(\operatorname{Prim} H)} = e^{*\widetilde{\iota}} \circ \left(\operatorname{Ulift} \mathfrak{i}\right). \tag{420}$$

Proof of (420): We know that $\operatorname{id}_{U(\operatorname{Prim} H)} \in G\left(U\left(\operatorname{Prim} H\right), U\left(\operatorname{Prim} H\right)\right)$. Hence, Proposition 5.13 **(b)** (applied to $U\left(\operatorname{Prim} H\right)$, $U\left(\operatorname{Prim} H\right)$ and $\operatorname{id}_{U(\operatorname{Prim} H)}$ instead of H, A and F) yields $e^{*\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)} = \operatorname{id}_{U(\operatorname{Prim} H)}$. Thus,

$$\operatorname{id}_{U(\operatorname{Prim} H)} = e^{*\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)} = e^{*\left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)} \qquad \text{(by (419))}.$$

[208] *Proof.* We know that $\iota_{\operatorname{Prim} H}$ is the canonical map from the Lie algebra $\operatorname{Prim} H$ to the universal enveloping algebra $U\left(\operatorname{Prim} H\right)$. Hence, $\iota_{\operatorname{Prim} H}$ is a Lie algebra homomorphism (where the Lie algebra structure on $U\left(\operatorname{Prim} H\right)$ is given by the commutator of the multiplication). Thus, its image $\iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right)$ is a Lie subalgebra of $U\left(\operatorname{Prim} H\right)$. Since $\iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right) = V$, this rewrites as follows: The set V is a Lie subalgebra of $U\left(\operatorname{Prim} H\right)$. In other words, we have $[x, y] \in V$ for any $x \in V$ and $y \in V$. Since $[x, y] = xy - yx$ for any $x \in V$ and $y \in V$, this rewrites as follows: We have $xy - yx \in V$ for any $x \in V$ and $y \in V$, qed.

[209] *Proof.* Let $v \in V$ and $n \in \mathbb{N}$. Then, $v \in V = \iota_{\operatorname{Prim} H}\left(\operatorname{Prim} H\right)$. Hence, (416) yields $\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)\left(v^n\right) = \left(\widetilde{\iota} \circ \left(\operatorname{Ulift} \mathfrak{i}\right)\right)\left(v^n\right)$, qed.

But recall that $\operatorname{Ulift}\mathfrak{i}$ is a k-bialgebra homomorphism. Hence, $\operatorname{Ulift}\mathfrak{i}$ is a k-coalgebra homomorphism. Also, $(\operatorname{Ulift}\mathfrak{i})\left(1_{U(\operatorname{Prim}H)}\right) = 1_H$ (since $\operatorname{Ulift}\mathfrak{i}$ is a k-algebra homomorphism). Moreover, $\widetilde{\iota} \in \mathfrak{g}\left(H, U\left(\operatorname{Prim}H\right)\right)$. Hence, Proposition 31.1 **(d)** (applied to $U\left(\operatorname{Prim}H\right)$, H, $U\left(\operatorname{Prim}H\right)$, $\operatorname{Ulift}\mathfrak{i}$ and $\widetilde{\iota}$ instead of D, C, A, φ and f) yields $e^{*(\widetilde{\iota}\circ(\operatorname{Ulift}\mathfrak{i}))} = e^{*\widetilde{\iota}} \circ (\operatorname{Ulift}\mathfrak{i})$.

Thus, $\operatorname{id}_{U(\operatorname{Prim}H)} = e^{*(\widetilde{\iota}\circ(\operatorname{Ulift}\mathfrak{i}))} = e^{*\widetilde{\iota}} \circ (\operatorname{Ulift}\mathfrak{i})$. This proves (420).

g) Due to (420), we have $e^{*\widetilde{\iota}} \circ (\operatorname{Ulift}\mathfrak{i}) = \operatorname{id}_{U(\operatorname{Prim}H)}$. Hence, the map $\operatorname{Ulift}\mathfrak{i}$ has a left inverse. Thus, $\operatorname{Ulift}\mathfrak{i}$ is injective. Combining this with the (already proven) fact that $\operatorname{Ulift}\mathfrak{i}$ is surjective, we conclude that $\operatorname{Ulift}\mathfrak{i}$ is bijective. Since $\operatorname{Ulift}\mathfrak{i}$ is a k-linear map, this yields that $\operatorname{Ulift}\mathfrak{i}$ is a k-vector space isomorphism (because every bijective k-linear map is a k-vector space isomorphism). Thus, the map $\operatorname{Ulift}\mathfrak{i}$ is invertible. Since $\operatorname{Ulift}\mathfrak{i}$ is a k-bialgebra homomorphism, this yields that

$$\operatorname{Ulift}\mathfrak{i} \text{ is a } k\text{-bialgebra isomorphism} \tag{421}$$

(because every invertible k-bialgebra homomorphism must be a k-bialgebra isomorphism (by Proposition 34.14)).

Now, recall that the map $\operatorname{Ulift}\mathfrak{i}$ is the canonical k-algebra homomorphism $U\left(\operatorname{Prim}H\right) \to H$ obtained from the Lie algebra homomorphism $\mathfrak{i}$ via the universal property of the universal enveloping algebra. Since the Lie algebra homomorphism $\mathfrak{i}$ is the inclusion map $\operatorname{Prim}H \to H$, this rewrites as follows: The map $\operatorname{Ulift}\mathfrak{i}$ is the canonical k-algebra homomorphism $U\left(\operatorname{Prim}H\right) \to H$ obtained from the inclusion map $\operatorname{Prim}H \to H$ via the universal property of the universal enveloping algebra. Hence, (421) rewrites as follows: The canonical k-algebra homomorphism $U\left(\operatorname{Prim}H\right) \to H$ obtained from the inclusion map $\operatorname{Prim}H \to H$ via the universal property of the universal enveloping algebra is a k-bialgebra isomorphism. Theorem 17.2 is thus proven. □

Our above proof of Theorem 17.2 allows for a corollary:

Corollary 34.15. Let k be a field of characteristic 0, and let H be a connected filtered cocommutative bialgebra over k. Let $\operatorname{Prim}H$ denote the set of all primitive elements of H. For every Lie algebra $\mathfrak{g}$, let $U\left(\mathfrak{g}\right)$ denote the universal enveloping algebra of $\mathfrak{g}$. Consider $U\left(\operatorname{Prim}H\right)$ as a k-bialgebra. Let $\iota_{\operatorname{Prim}H} : \operatorname{Prim}H \to U\left(\operatorname{Prim}H\right)$ be the canonical map from the Lie algebra $\operatorname{Prim}H$ into its universal enveloping algebra $U\left(\operatorname{Prim}H\right)$. Then, $\operatorname{Prim}\left(U\left(\operatorname{Prim}H\right)\right) = \iota_{\operatorname{Prim}H}\left(\operatorname{Prim}H\right)$.

Proof of Corollary 34.15. Let us work with the notations introduced in the proof of Theorem 17.2. The connected filtered k-bialgebra $U\left(\operatorname{Prim}H\right)$ is cocommutative (by Theorem 34.9 **(e)**, applied to $\mathfrak{g} = \operatorname{Prim}H$). Thus, Theorem 4.1 (applied to $U\left(\operatorname{Prim}H\right)$ instead of H) yields that the map $\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim}H)}\right) \in \mathcal{L}\left(U\left(\operatorname{Prim}H\right), U\left(\operatorname{Prim}H\right)\right)$ is a projection from $U\left(\operatorname{Prim}H\right)$ to the subspace $\operatorname{Prim}\left(U\left(\operatorname{Prim}H\right)\right)$ of all primitive elements

of $U(\operatorname{Prim} H)$. Hence, $\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)(U(\operatorname{Prim} H)) = \operatorname{Prim}(U(\operatorname{Prim} H))$. Thus,

$$\begin{aligned}\operatorname{Prim}(U(\operatorname{Prim} H)) &= \underbrace{\left(\operatorname{Log}\left(\operatorname{id}_{U(\operatorname{Prim} H)}\right)\right)}_{\substack{=\widetilde{\iota}\circ(\operatorname{Ulift}\mathfrak{i}) \\ \text{(by (419))}}}(U(\operatorname{Prim} H)) = (\widetilde{\iota}\circ(\operatorname{Ulift}\mathfrak{i}))(U(\operatorname{Prim} H)) \\ &= \widetilde{\iota}\left(\underbrace{(\operatorname{Ulift}\mathfrak{i})(U(\operatorname{Prim} H))}_{\subseteq H}\right) \subseteq \underbrace{\widetilde{\iota}}_{=\iota_{\operatorname{Prim} H}\circ\operatorname{eul}}(H) = (\iota_{\operatorname{Prim} H}\circ\operatorname{eul})(H) \\ &= \iota_{\operatorname{Prim} H}\left(\underbrace{\operatorname{eul}(H)}_{\subseteq\operatorname{Prim} H}\right) \subseteq \iota_{\operatorname{Prim} H}(\operatorname{Prim} H). \end{aligned} \tag{422}$$

But Theorem 34.9 **(d)** (applied to $\mathfrak{g} = \operatorname{Prim} H$) yields $\iota_{\operatorname{Prim} H}(\operatorname{Prim} H) \subseteq \operatorname{Prim}(U(\operatorname{Prim} H))$. Combining this with (422), we obtain $\operatorname{Prim}(U(\operatorname{Prim} H)) = \iota_{\operatorname{Prim} H}(\operatorname{Prim} H)$. This proves Corollary 34.15. □

Notice that Corollary 34.15 is merely a particular case of the following fact:

Corollary 34.16. Let k be a field of characteristic 0, and let $\mathfrak{g}$ be a k-Lie algebra. Consider the universal enveloping algebra $U(\mathfrak{g})$ as a k-bialgebra. Let $\iota_{\mathfrak{g}} : \mathfrak{g} \to U(\mathfrak{g})$ be the canonical map from the Lie algebra $\mathfrak{g}$ into its universal enveloping algebra $U(\mathfrak{g})$. Then, $\operatorname{Prim}(U(\mathfrak{g})) = \iota_{\mathfrak{g}}(\mathfrak{g})$.

However, Corollary 34.16 is not susceptible to the attack we have led on Corollary 34.15; it is commonly proven using the Poincaré-Birkhoff-Witt theorem instead.

Corollary 34.15 and Corollary 34.16 become false if the hypothesis that k have characteristic 0 is lifted. (If k is a field of characteristic p, then the k-vector subspace $\operatorname{Prim}(k[X])$ of $k[X]$ is spanned by $X, X^p, X^{p^2}, X^{p^3}, \ldots$.)

§35. Maps in $\mathfrak{g}(H, A)$ and products of primitives

We next show some properties of products of primitives with respect to maps in $\mathfrak{g}(H, A)$ (that is, linear maps from a k-bialgebra H to a k-algebra A that annihilate 1_H).

Theorem 35.1. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let f_1, f_2, …, f_r be r maps in $\mathfrak{g}(H, A)$.

(a) Every $s \in \{0, 1, \ldots, r-1\}$ and every s elements a_1, a_2, …, a_s of $\operatorname{Prim} H$ satisfy

$$(f_1 * f_2 * \cdots * f_r)(a_1 a_2 \cdots a_s) = 0.$$

(b) Every r elements a_1, a_2, …, a_r of $\operatorname{Prim} H$ satisfy

$$(f_1 * f_2 * \cdots * f_r)(a_1 a_2 \cdots a_r) = \sum_{\sigma \in S_r} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_r\left(a_{\sigma(r)}\right)$$

(where S_r denotes the r-th symmetric group).

Before we prove this theorem, let us show some simple facts:

Lemma 35.2. Let k be a field. Let H be a k-bialgebra. Let V be a k-vector subspace of $\operatorname{Prim} H$. Let $s \in \mathbb{N}$. Let a_1, a_2, ..., a_s be s elements of V. Then,

$$\Delta(a_1 a_2 \cdots a_s) \in \sum_{m=1}^{s} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_s)) + 1_H \otimes (a_1 a_2 \cdots a_s) + \sum_{\ell=0}^{s-2} H \otimes V^{\ell}.$$

210

Proof of Lemma 35.2. We will prove that every $r \in \{0, 1, \ldots, s\}$ satisfies

$$\Delta(a_1 a_2 \cdots a_r) \in \sum_{m=1}^{r} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_r)) + 1_H \otimes (a_1 a_2 \cdots a_r) + \sum_{\ell=0}^{r-2} H \otimes V^{\ell}. \tag{423}$$

Proof of (423): We will prove (423) by induction over r:

Induction base: Let $r = 0$. Then, $a_1 a_2 \cdots a_r = a_1 a_2 \cdots a_0 = (\text{empty product}) = 1_H$. Applying the map Δ to this equality, we obtain

$$\begin{aligned}
\Delta(a_1 a_2 \cdots a_r) &= \Delta(1_H) = 1_H \otimes \underbrace{1_H}_{=a_1 a_2 \cdots a_r} \qquad \text{(by the axioms of a bialgebra)} \\
&\in 1_H \otimes (a_1 a_2 \cdots a_r) \\
&\subseteq \sum_{m=1}^{r} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_r)) \\
&\qquad + 1_H \otimes (a_1 a_2 \cdots a_r) + \sum_{\ell=0}^{r-2} H \otimes V^{\ell}.
\end{aligned}$$

Thus, (423) is proven in the case when $r = 0$. The induction base is hence complete.

Induction step: Let $R \in \{0, 1, \ldots, s-1\}$. Assume that (423) has been proven for $r = R$. We need to prove (423) for $r = R + 1$.

We know that (423) has been proven for $r = R$. In other words,

$$\Delta(a_1 a_2 \cdots a_R) \in \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_R)) + 1_H \otimes (a_1 a_2 \cdots a_R) + \sum_{\ell=0}^{R-2} H \otimes V^{\ell}. \tag{424}$$

We know that $a_{R+1} \in V \subseteq \operatorname{Prim} H = (\text{the set of all primitive elements of } H)$. In other words, a_{R+1} is a primitive element of H. Hence, $\Delta(a_{R+1}) = a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}$ (by the definition of "primitive").

[210] Recall that V^{ℓ} is defined according to Convention 15.2. Hence, V^{ℓ} means the ℓ-th power of the subspace V of the k-algebra H.

It is easy to see that

$$\left(\sum_{\ell=0}^{R-2} H \otimes V^{\ell}\right) \cdot \left(a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}\right) \subseteq \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \tag{425}$$

[211].

It is also easy to find that

$$\begin{aligned}
&\sum_{m=1}^{R+1} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&= \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) + a_{R+1} \otimes \left(a_1 a_2 \cdots a_R\right).
\end{aligned} \tag{427}$$

[211] *Proof of (425):* Let $\ell \in \{0, 1, \ldots, R-2\}$. Then, $\ell \leq R-2$. Adding 1 to this inequality, we obtain $\ell + 1 \leq (R-2) + 1 = R - 1$.

Since $\ell \leq R-2 < R-1$, we know that $H \otimes V^{\ell}$ is an addend in the sum $\sum\limits_{h=0}^{R-1} H \otimes V^{h}$. Hence, $H \otimes V^{\ell} \subseteq \sum\limits_{h=0}^{R-1} H \otimes V^{h}$.

Since $\ell + 1 \leq R - 1$, we know that $H \otimes V^{\ell+1}$ is an addend in the sum $\sum\limits_{h=0}^{R-1} H \otimes V^{h}$. Hence, $H \otimes V^{\ell+1} \subseteq \sum\limits_{h=0}^{R-1} H \otimes V^{h}$.

We are now going to prove that

$$\left(H \otimes V^{\ell}\right) \cdot \left(a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}\right) \subseteq \sum_{h=0}^{R-1} H \otimes V^{h}. \tag{426}$$

Indeed, let $w \in \left(H \otimes V^{\ell}\right) \cdot \left(a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}\right)$. Thus, there exists an $x \in H \otimes V^{\ell}$ such that

$$w = x \cdot \left(a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}\right).$$

Consider this x. Since x is a tensor in $H \otimes V^{\ell}$, we can write x as $x = \sum\limits_{j=1}^{J} \lambda_j h_j \otimes y_j$ for some $J \in \mathbb{N}$, some elements λ_1, λ_2, ..., λ_J of k, some elements h_1, h_2, ..., h_J of H, and some elements y_1, y_2, ..., y_J of V^{ℓ}. Consider this J, these λ_1, λ_2, ..., λ_J, these h_1, h_2, ..., h_J, and these y_1, y_2, ..., y_J. We

have

$$
\begin{aligned}
w = & \underbrace{x}_{=\sum_{j=1}^{J} \lambda_j h_j \otimes y_j} \cdot (a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}) \\
&= \left(\sum_{j=1}^{J} \lambda_j h_j \otimes y_j \right) \cdot (a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}) \\
&= \sum_{j=1}^{J} \lambda_j \underbrace{(h_j \otimes y_j) \cdot (a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1})}_{= (h_j \otimes y_j) \cdot (a_{R+1} \otimes 1_H) + (h_j \otimes y_j) \cdot (1_H \otimes a_{R+1})} \\
&= \sum_{j=1}^{J} \lambda_j \left(\underbrace{(h_j \otimes y_j) \cdot (a_{R+1} \otimes 1_H)}_{= (h_j a_{R+1}) \otimes (y_j 1_H)} + \underbrace{(h_j \otimes y_j) \cdot (1_H \otimes a_{R+1})}_{= (h_j 1_H) \otimes (y_j a_{R+1})} \right) \\
&= \sum_{j=1}^{J} \lambda_j \left(\underbrace{(h_j a_{R+1})}_{\in H} \otimes \underbrace{(y_j 1_H)}_{= y_j \in V^\ell} + \underbrace{(h_j 1_H)}_{\in H} \otimes \left(\underbrace{y_j}_{\in V^\ell} \underbrace{a_{R+1}}_{\in V} \right) \right) \\
&\in \sum_{j=1}^{J} \lambda_j \left(H \otimes V^\ell + H \otimes \underbrace{\left(V^\ell V\right)}_{= V^{\ell+1}} \right) = \sum_{j=1}^{J} \lambda_j \left(H \otimes V^\ell + H \otimes V^{\ell+1} \right) \\
&\subseteq \underbrace{H \otimes V^\ell}_{\subseteq \sum_{h=0}^{R-1} H \otimes V^h} + \underbrace{H \otimes V^{\ell+1}}_{\subseteq \sum_{h=0}^{R-1} H \otimes V^h} \qquad \left(\text{since } H \otimes V^\ell + H \otimes V^{\ell+1} \text{ is a } k\text{-vector space} \right) \\
&\subseteq \sum_{h=0}^{R-1} H \otimes V^h + \sum_{h=0}^{R-1} H \otimes V^h \subseteq \sum_{h=0}^{R-1} H \otimes V^h
\end{aligned}
$$

(since $\sum_{h=0}^{R-1} H \otimes V^h$ is a k-vector space).

Now, forget that we fixed w. We thus have proven that every $w \in \left(H \otimes V^\ell\right) \cdot (a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1})$ satisfies $w \in \sum_{h=0}^{R-1} H \otimes V^h$. In other words,

$$\left(H \otimes V^\ell\right) \cdot (a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}) \subseteq \sum_{h=0}^{R-1} H \otimes V^h.$$

In other words, (426) is proven.

Now, forget that we fixed ℓ. We thus have shown that (426) holds for every $\ell \in \{0, 1, \ldots, R-2\}$.

[212]

Also, notice that

$$\sum_{m=1}^{R} H \otimes V^{R-1} + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \subseteq \sum_{\ell=0}^{(R+1)-2} H \otimes V^{\ell} \tag{428}$$

[213].

Since H is a bialgebra, the comultiplication Δ is a k-algebra homomorphism (by

---

Now,

$$\begin{aligned}
&\left(\sum_{\ell=0}^{R-2} H \otimes V^{\ell}\right) \cdot (a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1}) \\
&= \sum_{\ell=0}^{R-2} \underbrace{\left(H \otimes V^{\ell}\right) \cdot (a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1})}_{\substack{\subseteq \sum_{h=0}^{R-1} H \otimes V^h \\ \text{(by (426))}}} \\
&\subseteq \sum_{\ell=0}^{R-2} \sum_{h=0}^{R-1} H \otimes V^h \subseteq \sum_{h=0}^{R-1} H \otimes V^h \qquad \left(\text{since } \sum_{h=0}^{R-1} H \otimes V^h \text{ is a } k\text{-vector space}\right) \\
&= \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \qquad \text{(here, we renamed the summation index } h \text{ as } \ell\text{)}.
\end{aligned}$$

Thus, (425) is proven.

[212] *Proof of (427):* We have

$$\begin{aligned}
&\sum_{m=1}^{R+1} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_{R+1})) \\
&= \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_{R+1})) \\
&\qquad + a_{R+1} \otimes \left(\underbrace{(a_1 a_2 \cdots a_{(R+1)-1})}_{=a_1 a_2 \cdots a_R} \underbrace{(a_{(R+1)+1} a_{(R+1)+2} \cdots a_{R+1})}_{=(\text{empty product})=1_H} \right) \\
&= \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_{R+1})) + a_{R+1} \otimes \underbrace{((a_1 a_2 \cdots a_R) 1_H)}_{=a_1 a_2 \cdots a_R} \\
&= \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_{R+1})) + a_{R+1} \otimes (a_1 a_2 \cdots a_R).
\end{aligned}$$

This proves (427).

[213] *Proof of (428):* If $R = 0$, then $\sum_{m=1}^{R} H \otimes V^{R-1} = (\text{empty sum}) = 0$. Hence, if $R = 0$, then $\underbrace{\sum_{m=1}^{R} H \otimes V^{R-1}}_{=0} + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} = \sum_{\ell=0}^{R-1} H \otimes V^{\ell} = \sum_{\ell=0}^{(R+1)-2} H \otimes V^{\ell}$ (since $R - 1 = (R+1) - 2$). Thus, if $R = 0$, then (428) holds. Therefore, for the rest of this proof of (428), we can WLOG assume that we don't have $R = 0$. Assume this.

We don't have $R = 0$. Thus, we have $R \geq 1$, so that $R - 1 \geq 0$. Hence, $R - 1 \in \{0, 1, \ldots, R-1\}$.

Hence, $H \otimes V^{R-1}$ is an addend in the sum $\sum\limits_{\ell=0}^{R-1} H \otimes V^{\ell}$. Hence, $H \otimes V^{R-1} \subseteq \sum\limits_{\ell=0}^{R-1} H \otimes V^{\ell}$. Now,

$$\begin{aligned}\sum_{m=1}^{R} H \otimes V^{R-1} &\subseteq H \otimes V^{R-1} \qquad \left(\text{since } H \otimes V^{R-1} \text{ is a } k\text{-vector space}\right) \\ &\subseteq \sum_{\ell=0}^{R-1} H \otimes V^{\ell},\end{aligned}$$

so that

$$\begin{aligned}\underbrace{\sum_{m=1}^{R} H \otimes V^{R-1}}_{\subseteq \sum_{\ell=0}^{R-1} H \otimes V^{\ell}} + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} &\subseteq \sum_{\ell=0}^{R-1} H \otimes V^{\ell} + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \\ &\subseteq \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \qquad \left(\text{since } \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \text{ is a } k\text{-vector space}\right) \\ &= \sum_{\ell=0}^{(R+1)-2} H \otimes V^{\ell} \qquad \left(\text{since } R-1 = (R+1)-2\right).\end{aligned}$$

This proves (428).

the axioms of a bialgebra). We have

$$
\begin{aligned}
&\Delta\left(\underbrace{a_1a_2\cdots a_{R+1}}_{=(a_1a_2\cdots a_R)a_{R+1}}\right) \\
&= \Delta\left(\left(a_1a_2\cdots a_R\right)a_{R+1}\right) \\
&= \underbrace{\Delta\left(a_1a_2\cdots a_R\right)}_{\in \sum_{m=1}^{R} a_m\otimes((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_R))+1_H\otimes(a_1a_2\cdots a_R)+\sum_{\ell=0}^{R-2} H\otimes V^\ell \text{ (by (424))}} \cdot \underbrace{\Delta\left(a_{R+1}\right)}_{=a_{R+1}\otimes 1_H+1_H\otimes a_{R+1}} \\
&\qquad \text{(since } \Delta \text{ is a } k\text{-algebra homomorphism)} \\
&\in \left(\sum_{m=1}^{R} a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_R\right)\right)+1_H\otimes\left(a_1a_2\cdots a_R\right)+\sum_{\ell=0}^{R-2} H\otimes V^\ell\right) \\
&\qquad \cdot\left(a_{R+1}\otimes 1_H+1_H\otimes a_{R+1}\right) \\
&\subseteq \underbrace{\left(\sum_{m=1}^{R} a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_R\right)\right)\right)\cdot\left(a_{R+1}\otimes 1_H+1_H\otimes a_{R+1}\right)}_{\substack{=\left(\sum_{m=1}^{R} a_m\otimes((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_R))\right)\cdot(a_{R+1}\otimes 1_H) \\ +\left(\sum_{m=1}^{R} a_m\otimes((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_R))\right)\cdot(1_H\otimes a_{R+1})}} \\
&\qquad + \underbrace{\left(1_H\otimes\left(a_1a_2\cdots a_R\right)\right)\cdot\left(a_{R+1}\otimes 1_H+1_H\otimes a_{R+1}\right)}_{=(1_H\otimes(a_1a_2\cdots a_R))\cdot(a_{R+1}\otimes 1_H)+(1_H\otimes(a_1a_2\cdots a_R))\cdot(1_H\otimes a_{R+1})} \\
&\qquad + \underbrace{\left(\sum_{\ell=0}^{R-2} H\otimes V^\ell\right)\cdot\left(a_{R+1}\otimes 1_H+1_H\otimes a_{R+1}\right)}_{\subseteq\sum_{\ell=0}^{R-1} H\otimes V^\ell}
\end{aligned}
$$

$$
\begin{aligned}
&\subseteq \underbrace{\left(\sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(a_{R+1} \otimes 1_H\right)}_{=\sum\limits_{m=1}^{R} \left(a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(a_{R+1} \otimes 1_H\right)} \\
&\qquad + \underbrace{\left(\sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)}_{=\sum\limits_{m=1}^{R} \left(a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)} \\
&\qquad + \underbrace{\left(1_H \otimes \left(a_1 a_2 \cdots a_R\right)\right) \cdot \left(a_{R+1} \otimes 1_H\right)}_{=\left(1_H a_{R+1}\right) \otimes \left(\left(a_1 a_2 \cdots a_R\right) 1_H\right)} + \underbrace{\left(1_H \otimes \left(a_1 a_2 \cdots a_R\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)}_{=\left(1_H 1_H\right) \otimes \left(\left(a_1 a_2 \cdots a_R\right) a_{R+1}\right)} \\
&\qquad + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \\
&\subseteq \sum_{m=1}^{R} \underbrace{\left(a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(a_{R+1} \otimes 1_H\right)}_{=\left(a_m a_{R+1}\right) \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right) 1_H\right)} \\
&\qquad + \sum_{m=1}^{R} \underbrace{\left(a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)}_{=\left(a_m 1_H\right) \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right) a_{R+1}\right)} \\
&\qquad + \underbrace{\left(1_H a_{R+1}\right)}_{=a_{R+1}} \otimes \underbrace{\left(\left(a_1 a_2 \cdots a_R\right) 1_H\right)}_{=a_1 a_2 \cdots a_R} + \underbrace{\left(1_H 1_H\right)}_{=1_H} \otimes \underbrace{\left(\left(a_1 a_2 \cdots a_R\right) a_{R+1}\right)}_{=a_1 a_2 \cdots a_R a_{R+1}} \\
&\qquad + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \\
&= \sum_{m=1}^{R} \left(a_m a_{R+1}\right) \otimes \underbrace{\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right) 1_H\right)}_{=\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)} \\
&\qquad + \sum_{m=1}^{R} \underbrace{\left(a_m 1_H\right)}_{=a_m} \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right) \quad \underbrace{\left(a_{m+1} a_{m+2} \cdots a_R\right) a_{R+1}}_{=a_{m+1} a_{m+2} \cdots a_R a_{R+1} = a_{m+1} a_{m+2} \cdots a_{R+1}}\right) \\
&\qquad + a_{R+1} \otimes \left(a_1 a_2 \cdots a_R\right) + 1_H \otimes \underbrace{\left(a_1 a_2 \cdots a_R a_{R+1}\right)}_{=a_1 a_2 \cdots a_{R+1}} \\
&\qquad + \sum_{\ell=0}^{R-1} H \otimes V^{\ell}
\end{aligned}
$$

$$
\begin{aligned}
&= \sum_{m=1}^{R} \underbrace{\left(a_m a_{R+1}\right)}_{\in H} \otimes \left(\underbrace{\left(a_1 a_2 \cdots a_{m-1}\right)}_{\in V^{m-1}} \qquad \underbrace{\left(a_{m+1} a_{m+2} \cdots a_R\right)}_{\in V^{R-m}} \right) \\
&\qquad \begin{array}{l} \text{(since } a_i \in V \text{ for every } i \in \{1,2,\ldots,m-1\}\text{)} \\ \text{(since } a_i \in V \text{ for every } i \in \{m+1,m+2,\ldots,R\}\text{)} \end{array} \\
&\qquad + \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&\qquad + a_{R+1} \otimes \left(a_1 a_2 \cdots a_R\right) + 1_H \otimes \left(a_1 a_2 \cdots a_{R+1}\right) \\
&\qquad + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \\
&\subseteq \sum_{m=1}^{R} H \otimes \left(V^{m-1} V^{R-m}\right) \\
&\qquad + \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&\qquad + a_{R+1} \otimes \left(a_1 a_2 \cdots a_R\right) + 1_H \otimes \left(a_1 a_2 \cdots a_{R+1}\right) \\
&\qquad + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \\
&= \underbrace{\sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) + a_{R+1} \otimes \left(a_1 a_2 \cdots a_R\right)}_{= \sum_{m=1}^{R+1} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \text{ (by (427))}} \\
&\qquad + 1_H \otimes \left(a_1 a_2 \cdots a_{R+1}\right) + \sum_{m=1}^{R} H \otimes \underbrace{\left(V^{m-1} V^{R-m}\right)}_{= V^{(m-1)+(R-m)} = V^{R-1}} + \sum_{\ell=0}^{R-1} H \otimes V^{\ell} \\
&= \sum_{m=1}^{R+1} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&\qquad + 1_H \otimes \left(a_1 a_2 \cdots a_{R+1}\right) + \underbrace{\sum_{m=1}^{R} H \otimes V^{R-1} + \sum_{\ell=0}^{R-1} H \otimes V^{\ell}}_{\subseteq \sum_{\ell=0}^{(R+1)-2} H \otimes V^{\ell} \text{ (by (428))}} \\
&\subseteq \sum_{m=1}^{R+1} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&\qquad + 1_H \otimes \left(a_1 a_2 \cdots a_{R+1}\right) + \sum_{\ell=0}^{(R+1)-2} H \otimes V^{\ell}.
\end{aligned}
$$

In other words, (423) holds for $r = R+1$. We have thus proven (423) for $r = R+1$. The induction step is thus complete.

Hence, (423) is proven by induction. Now, applying (423) to $r = s$, we obtain

$$\Delta\left(a_1 a_2 \cdots a_s\right) \in \sum_{m=1}^{s} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right) + 1_H \otimes \left(a_1 a_2 \cdots a_s\right) + \sum_{\ell=0}^{s-2} H \otimes V^{\ell}.$$

This proves Lemma 35.2. □

From Lemma 35.2, we easily conclude the following weaker statement:

Lemma 35.3. Let k be a field. Let H be a k-bialgebra. Let V be a k-vector subspace of $\operatorname{Prim} H$. Let $s \in \mathbb{N}$. Let a_1, a_2, …, a_s be s elements of V. Then,

$$\Delta\left(a_1 a_2 \cdots a_s\right) \in 1_H \otimes \left(a_1 a_2 \cdots a_s\right) + \sum_{\ell=0}^{s-1} H \otimes V^{\ell}.$$

Proof of Lemma 35.3. Every $m \in \{1, 2, \ldots, s\}$ satisfies

$$a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right) \in \sum_{\ell=0}^{s-1} H \otimes V^{\ell} \tag{429}$$

[215]. Hence,

$$\sum_{m=1}^{s} \underbrace{a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right)}_{\in \sum_{\ell=0}^{s-1} H \otimes V^{\ell} \text{ (by (429))}} \in \sum_{m=1}^{s} \sum_{\ell=0}^{s-1} H \otimes V^{\ell} \subseteq \sum_{\ell=0}^{s-1} H \otimes V^{\ell}$$

[214] Recall that V^{ℓ} is defined according to Convention 15.2. Hence, V^{ℓ} means the ℓ-th power of the subspace V of the k-algebra H.

[215] *Proof of (429):* Let $m \in \{1, 2, \ldots, s\}$. Then, $1 \leq m \leq s$, so that $s \geq 1$ and thus $s - 1 \geq 0$. Hence, $s - 1 \in \{0, 1, \ldots, s-1\}$. Thus, $H \otimes V^{s-1}$ is an addend in the sum $\sum_{\ell=0}^{s-1} H \otimes V^{\ell}$. Consequently, $H \otimes V^{s-1} \subseteq \sum_{\ell=0}^{s-1} H \otimes V^{\ell}$.

Now, $\underbrace{\left(a_1 a_2 \cdots a_{m-1}\right)}_{\in V^{m-1} \text{ (since } a_i \in V \text{ for every } i \in \{1,2,\ldots,m-1\})} \underbrace{\left(a_{m+1} a_{m+2} \cdots a_s\right)}_{\in V^{s-m} \text{ (since } a_i \in V \text{ for every } i \in \{m+1,m+2,\ldots,s\})} \in V^{m-1} V^{s-m} = V^{(m-1)+(s-m)} = V^{s-1}$. Now,

$$\underbrace{a_m}_{\in H} \otimes \left(\underbrace{\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)}_{\in V^{s-1}}\right) \in H \otimes V^{s-1} \subseteq \sum_{\ell=0}^{s-1} H \otimes V^{\ell}.$$

This proves (429).

(since $\sum_{\ell=0}^{s-1} H \otimes V^\ell$ is a k-vector space). Now, Lemma 35.2 yields

$$\begin{aligned}
\Delta(a_1 a_2 \cdots a_s) &\in \underbrace{\sum_{m=1}^{s} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_s))}_{\in \sum_{\ell=0}^{s-1} H \otimes V^\ell} \\
&\quad + 1_H \otimes (a_1 a_2 \cdots a_s) + \underbrace{\sum_{\ell=0}^{s-2} H \otimes V^\ell}_{\substack{\subseteq \sum_{\ell=0}^{s-1} H \otimes V^\ell \\ \text{(since } s-2 \leq s-1\text{)}}} \\
&\subseteq \sum_{\ell=0}^{s-1} H \otimes V^\ell + 1_H \otimes (a_1 a_2 \cdots a_s) + \sum_{\ell=0}^{s-1} H \otimes V^\ell \\
&= 1_H \otimes (a_1 a_2 \cdots a_s) + \underbrace{\sum_{\ell=0}^{s-1} H \otimes V^\ell + \sum_{\ell=0}^{s-1} H \otimes V^\ell}_{\substack{\subseteq \sum_{\ell=0}^{s-1} H \otimes V^\ell \\ \text{(since } \sum_{\ell=0}^{s-1} H \otimes V^\ell \text{ is a } k\text{-vector space)}}} \\
&\subseteq 1_H \otimes (a_1 a_2 \cdots a_s) + \sum_{\ell=0}^{s-1} H \otimes V^\ell.
\end{aligned}$$

This proves Lemma 35.3. □

We are now ready to prove the following result (more or less equivalent to Theorem 35.1 **(a)**):

Lemma 35.4. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let f_1, f_2, …, f_r be r maps in $\mathfrak{g}(H, A)$.

Every $s \in \{0, 1, \ldots, r-1\}$ satisfies

$$(f_1 * f_2 * \cdots * f_r)((\operatorname{Prim} H)^s) = 0.$$

216

Proof of Lemma 35.4. We are going to prove Lemma 35.4 by induction over r:

Induction base: If $r = 0$, then Lemma 35.4 is vacuously true (because if $r = 0$, then there exists no $s \in \{0, 1, \ldots, r-1\}$). Hence, the induction base is complete.

Induction step: Let $R \in \mathbb{N}$ be positive. Assume that Lemma 35.4 is proven for $r = R - 1$. We now are going to prove that Lemma 35.4 holds for $r = R$.

Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let f_1, f_2, …, f_R be R maps in $\mathfrak{g}(H, A)$. Let $s \in \{0, 1, \ldots, R-1\}$. We are going to show that

$$(f_1 * f_2 * \cdots * f_R)((\operatorname{Prim} H)^s) = 0.$$

[216] Recall that $(\operatorname{Prim} H)^s$ is defined according to Convention 15.2. Hence, $(\operatorname{Prim} H)^s$ means the s-th power of the subspace $\operatorname{Prim} H$ of the k-algebra H.

Let $g = f_2 * f_3 * \cdots * f_R$. Then, g is a k-linear map $H \to A$. Let $\ell \in \{0, 1, \ldots, s-1\}$. Hence, $0 \leq \ell \leq s-1$. But $s \leq R-1$ (since $s \in \{0, 1, \ldots, R-1\}$), so that $\ell \leq \underbrace{s}_{\leq R-1} - 1 \leq (R-1) - 1$. Thus, $0 \leq \ell \leq (R-1) - 1$. Hence, $\ell \in \{0, 1, \ldots, (R-1)-1\}$. Thus, we can apply Lemma 35.4 to $R-1$, $(f_2, f_3, \ldots, f_R)$ and ℓ instead of r, $(f_1, f_2, \ldots, f_r)$ and s (since we assumed that Lemma 35.4 is proven for $r = R-1$). As a result, we obtain $(f_2 * f_3 * \cdots * f_R)\left((\operatorname{Prim} H)^\ell\right) = 0$. Thus,

$$\underbrace{g}_{=f_2 * f_3 * \cdots * f_R}\left((\operatorname{Prim} H)^\ell\right) = (f_2 * f_3 * \cdots * f_R)\left((\operatorname{Prim} H)^\ell\right) = 0.$$

Now, forget that we fixed ℓ. We thus have proven that

$$g\left((\operatorname{Prim} H)^\ell\right) = 0 \qquad \text{for every } \ell \in \{0, 1, \ldots, s-1\}. \tag{430}$$

We have $f_1 \in \mathfrak{g}(H, A) = \{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\}$. In other words, f_1 is an element of $\mathcal{L}(H, A)$ and satisfies $f_1(1_H) = 0$.

Now, let a_1, a_2, ..., a_s be s elements of $\operatorname{Prim} H$. We have $f_1 * f_2 * \cdots * f_R = f_1 * \underbrace{(f_2 * f_3 * \cdots * f_R)}_{=g} = f_1 * g = \mu \circ (f_1 \otimes g) \circ \Delta$ (by the definition of convolution), so

that

$$\underbrace{\left(f_1 * f_2 * \cdots * f_R\right)}_{=\mu\circ(f_1\otimes g)\circ\Delta}\left(a_1 a_2 \cdots a_s\right)$$

$$= \left(\mu \circ (f_1 \otimes g) \circ \Delta\right)\left(a_1 a_2 \cdots a_s\right) = \mu\left((f_1 \otimes g)\left(\underbrace{\Delta\left(a_1 a_2 \cdots a_s\right)}_{\in 1_H \otimes (a_1 a_2 \cdots a_s) + \sum_{\ell=0}^{s-1} H \otimes (\operatorname{Prim} H)^{\ell} \text{ (by Lemma 35.3, applied to } V = \operatorname{Prim} H)}\right)\right)$$

$$\in \mu\left(\underbrace{(f_1 \otimes g)\left(1_H \otimes (a_1 a_2 \cdots a_s) + \sum_{\ell=0}^{s-1} H \otimes (\operatorname{Prim} H)^{\ell}\right)}_{= (f_1\otimes g)(1_H \otimes (a_1 a_2 \cdots a_s)) + \sum_{\ell=0}^{s-1} (f_1\otimes g)\left(H \otimes (\operatorname{Prim} H)^{\ell}\right) \text{ (since the map } f_1 \otimes g \text{ is } k\text{-linear)}}\right)$$

$$= \mu\left(\underbrace{(f_1 \otimes g)\left(1_H \otimes (a_1 a_2 \cdots a_s)\right)}_{= f_1(1_H) \otimes g(a_1 a_2 \cdots a_s)} + \sum_{\ell=0}^{s-1} \underbrace{(f_1 \otimes g)\left(H \otimes (\operatorname{Prim} H)^{\ell}\right)}_{\subseteq f_1(H) \otimes g\left((\operatorname{Prim} H)^{\ell}\right)}\right)$$

$$\subseteq \mu\left(\underbrace{f_1\left(1_H\right)}_{=0} \otimes g\left(a_1 a_2 \cdots a_s\right) + \sum_{\ell=0}^{s-1} f_1\left(H\right) \otimes \underbrace{g\left(\left(\operatorname{Prim} H\right)^{\ell}\right)}_{=0 \text{ (by (430) (since } \ell \in \{0,1,\ldots,s-1\}))}\right)$$

$$= \mu\left(\underbrace{0 \otimes g\left(a_1 a_2 \cdots a_s\right)}_{=0} + \underbrace{\sum_{\ell=0}^{s-1} f_1\left(H\right) \otimes 0}_{=0}\right) = \mu\left(0\right) = 0.$$

Hence, $\left(f_1 * f_2 * \cdots * f_R\right)\left(a_1 a_2 \cdots a_s\right) = 0$.

Now, forget that we fixed a_1, a_2, …, a_s. We thus have shown that whenever a_1, a_2, …, a_s are s elements of $\operatorname{Prim} H$, we have

$$\left(f_1 * f_2 * \cdots * f_R\right)\left(a_1 a_2 \cdots a_s\right) = 0. \tag{431}$$

Now, (73) yields

$$\begin{aligned}\left(\operatorname{Prim} H\right)^s &= \left\langle a_1 a_2 \cdots a_s \;\mid\; \left(a_1, a_2, \ldots, a_s\right) \in \left(\operatorname{Prim} H\right)^{\times s}\right\rangle \\ &= \left\langle \left\{ a_1 a_2 \cdots a_s \;\mid\; \left(a_1, a_2, \ldots, a_s\right) \in \left(\operatorname{Prim} H\right)^{\times s}\right\}\right\rangle.\end{aligned}$$

Applying the map $f_1 * f_2 * \cdots * f_R$ to both sides of this equality, we obtain

$$\begin{aligned}
&(f_1 * f_2 * \cdots * f_R)\left((\operatorname{Prim} H)^s\right) \\
&= (f_1 * f_2 * \cdots * f_R)\left(\left\langle \left\{ a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Prim} H)^{\times s} \right\} \right\rangle\right) \\
&= \left\langle \underbrace{(f_1 * f_2 * \cdots * f_R)\left(\left\{ a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Prim} H)^{\times s} \right\}\right)}_{= \left\{ (f_1 * f_2 * \cdots * f_R)(a_1 a_2 \cdots a_s) \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Prim} H)^{\times s} \right\}} \right\rangle \\
&\qquad \left(\begin{array}{c} \text{by (165), applied to } H, A, f_1 * f_2 * \cdots * f_R \text{ and} \\ \left\{ a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Prim} H)^{\times s} \right\} \text{ instead of } M, R, \phi \text{ and } S \end{array} \right) \\
&= \left\langle \left\{ \underbrace{(f_1 * f_2 * \cdots * f_R)(a_1 a_2 \cdots a_s)}_{\substack{=0 \\ \text{(by (431))}}} \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Prim} H)^{\times s} \right\} \right\rangle \\
&= \left\langle \underbrace{\left\{ 0 \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Prim} H)^{\times s} \right\}}_{\subseteq 0} \right\rangle \subseteq \langle 0 \rangle = 0.
\end{aligned}$$

In other words, $(f_1 * f_2 * \cdots * f_R)\left((\operatorname{Prim} H)^s\right) = 0$.

Now, forget that we fixed k, H, A, $(f_1, f_2, \ldots, f_R)$ and s. We thus have shown that if k is a field, if H is a k-bialgebra, if A is a k-algebra, if f_1, f_2, ..., f_R are R maps in $\mathfrak{g}(H, A)$, then every $s \in \{0, 1, \ldots, R-1\}$ satisfies $(f_1 * f_2 * \cdots * f_R)\left((\operatorname{Prim} H)^s\right) = 0$. In other words, we have shown that Lemma 35.4 holds for $r = R$. This completes the induction step. The induction proof of Lemma 35.4 is thus complete. □

To proceed, we introduce a basic operation on permutations:

Lemma 35.5. As usual, let S_n denote the n-th symmetric group for every $n \in \mathbb{N}$.

Let n be a positive integer.

Fix $m \in \{1, 2, \ldots, n\}$. Let $S_{n,m}$ denote the subset $\{\sigma \in S_n \ \mid \ \sigma(1) = m\}$ of S_n.

(a) Define a map $\eta : \{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n\} \setminus \{m\}$ by

$$\left(\eta(i) = \begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} \qquad \text{for every } i \in \{1, 2, \ldots, n-1\} \right). \tag{432}$$

This map η is well-defined.

(b) Define a map $\omega : \{1, 2, \ldots, n\} \setminus \{m\} \to \{1, 2, \ldots, n-1\}$ by

$$\left(\omega(j) = \begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} \qquad \text{for every } j \in \{1, 2, \ldots, n\} \setminus \{m\} \right). \tag{433}$$

This map ω is well-defined.

(c) The maps η and ω are mutually inverse (where η is defined as in Lemma 35.5 **(a)**, and where ω is defined as in Lemma 35.5 **(b)**).

(d) For every $\sigma \in S_{n-1}$, define a map $\operatorname{ins}_m \sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ by

$$\left(\left(\operatorname{ins}_m \sigma\right)(i) = \begin{cases} \eta\left(\sigma\left(i-1\right)\right), & \text{if } i \neq 1; \\ m, & \text{if } i = 1 \end{cases} \qquad \text{for every } i \in \{1,2,\ldots,n\} \right) \tag{434}$$

(where η is defined as in Lemma 35.5 **(a)**). This map $\operatorname{ins}_m \sigma$ is well-defined.

(e) Define a map $\iota_m : S_{n-1} \to S_{n,m}$ by

$$\left(\iota_m\left(\sigma\right) = \operatorname{ins}_m \sigma \qquad \text{for every } \sigma \in S_{n-1}\right) \tag{435}$$

(where $\operatorname{ins}_m \sigma$ is defined as in Lemma 35.5 **(d)**). This map ι_m is well-defined.

(f) For every $\tau \in S_{n,m}$, define a map $\operatorname{del}_m \tau : \{1,2,\ldots,n-1\} \to \{1,2,\ldots,n-1\}$ by

$$\left(\left(\operatorname{del}_m \tau\right)(i) = \omega\left(\tau\left(i+1\right)\right) \qquad \text{for every } i \in \{1,2,\ldots,n-1\}\right) \tag{436}$$

(where ω is defined as in Lemma 35.5 **(b)**). This map $\operatorname{del}_m \tau$ is well-defined.

(g) Define a map $\pi_m : S_{n,m} \to S_{n-1}$ by

$$\left(\pi_m\left(\tau\right) = \operatorname{del}_m \tau \qquad \text{for every } \tau \in S_{n,m}\right) \tag{437}$$

(where $\operatorname{del}_m \tau$ is defined as in Lemma 35.5 **(f)**). This map π_m is well-defined.

(h) The maps ι_m and π_m are mutually inverse (where ι_m is defined as in Lemma 35.5 **(e)**, and where π_m is defined as in Lemma 35.5 **(g)**).

Proof of Lemma 35.5. We have $1 \in \{1,2,\ldots,n\}$ (since n is positive).

(a) For every $i \in \{1,2,\ldots,n-1\}$, we have $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} \in \{1,2,\ldots,n\} \setminus \{m\}$ [217]. Thus, for every $i \in \{1,2,\ldots,n-1\}$, the element $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases}$ is a well-defined element of $\{1,2,\ldots,n\} \setminus \{m\}$. In other words, for every $i \in \{1,2,\ldots,n-1\}$,

[217] *Proof.* Let $i \in \{1,2,\ldots,n-1\}$. We want to prove that $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} \in \{1,2,\ldots,n\} \setminus \{m\}$.

We must be in one of the following two cases:

Case 1: We have $i < m$.

Case 2: We have $i \geq m$.

Let us first consider Case 1. In this case, we have $i < m$. Hence, $i \neq m$. Since $i \in \{1,2,\ldots,n-1\} \subseteq \{1,2,\ldots,n\}$ and $i \neq m$, we have $i \in \{1,2,\ldots,n\} \setminus \{m\}$. Now, $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} = i$ (since $i < m$), so that $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} = i \in \{1,2,\ldots,n\} \setminus \{m\}$. Thus, $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} \in \{1,2,\ldots,n\} \setminus \{m\}$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $i \geq m$. Hence, $i+1 \geq m+1 > m$, so that $i+1 \neq m$. Also, $i \in \{1,2,\ldots,n-1\}$, so that $i+1 \in \{2,3,\ldots,n\} \subseteq \{1,2,\ldots,n\}$. Combining this with $i+1 \neq m$, we obtain $i+1 \in \{1,2,\ldots,n\} \setminus \{m\}$. Now, $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} = i+1$ (since $i \geq m$), so that $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} = i+1 \in \{1,2,\ldots,n\} \setminus \{m\}$. Thus, $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} \in$

the right hand side of (432) is a well-defined element of $\{1,2,\ldots,n\} \setminus \{m\}$. Hence, the map $\eta : \{1,2,\ldots,n-1\} \to \{1,2,\ldots,n\} \setminus \{m\}$ is well-defined (because the map $\eta : \{1,2,\ldots,n-1\} \to \{1,2,\ldots,n\} \setminus \{m\}$ was defined by (432)). Lemma 35.5 **(a)** is thus proven.

(b) For every $j \in \{1,2,\ldots,n\}\setminus\{m\}$, we have $\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} \in \{1,2,\ldots,n-1\}$ [218]. In other words, for every $j \in \{1,2,\ldots,n\}\setminus\{m\}$, the element $\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases}$ is a well-defined element of $\{1,2,\ldots,n-1\}$. In other words, for every $j \in \{1,2,\ldots,n\}\setminus\{m\}$, the right hand side of (433) is a well-defined element of $\{1,2,\ldots,n-1\}$. In other words, Hence, the map $\omega : \{1,2,\ldots,n\} \setminus \{m\} \to \{1,2,\ldots,n-1\}$ is well-defined (because the map $\omega : \{1,2,\ldots,n\} \setminus \{m\} \to \{1,2,\ldots,n-1\}$ was defined by (433)). Lemma 35.5 **(b)** is thus proven.

(c) Clearly, the maps $\eta \circ \omega$ and $\omega \circ \eta$ are well-defined.

$\{1,2,\ldots,n\} \setminus \{m\}$ is proven in Case 2.

We have thus proven $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} \in \{1,2,\ldots,n\} \setminus \{m\}$ in each of the two Cases 1 and 2. Since these two Cases cover all possibilities, this yields that $\begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} \in \{1,2,\ldots,n\} \setminus \{m\}$ always holds, qed.

[218] *Proof.* Let $j \in \{1,2,\ldots,n\} \setminus \{m\}$. We want to prove that $\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} \in \{1,2,\ldots,n-1\}$.

We must be in one of the following two cases:

Case 1: We have $j < m$.

Case 2: We have $j \geq m$.

Let us first consider Case 1. In this case, we have $j < m$. Hence, $j < m \leq n$, so that $j \leq n-1$ (since j and n are integers). But $j \in \{1,2,\ldots,n\} \setminus \{m\} \subseteq \{1,2,\ldots,n\}$, so that $1 \leq j$. Combining $1 \leq j$ and $j \leq n-1$, we obtain $j \in \{1,2,\ldots,n-1\}$, so that

$$\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} = j \qquad (\text{since } j < m)$$
$$\in \{1,2,\ldots,n-1\}.$$

Thus, $\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} \in \{1,2,\ldots,n-1\}$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $j \geq m$. Combined with $j \neq m$ (since $j \in \{1,2,\ldots,n\} \setminus \{m\}$), this yields $j > m$. Thus, $j \geq m+1$ (since j and m are integers), so that $j-1 \geq m \geq 1$. Also, $j \leq n$ (since $j \in \{1,2,\ldots,n\}$), so that $j-1 \leq n-1$. Combining $j-1 \geq 1$ and $j-1 \leq n-1$, we obtain $j-1 \in \{1,2,\ldots,n-1\}$. Now,

$$\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} = j-1 \qquad (\text{since } j \geq m)$$
$$\in \{1,2,\ldots,n-1\}.$$

Thus, $\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} \in \{1,2,\ldots,n-1\}$ is proven in Case 2.

We now have proven $\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} \in \{1,2,\ldots,n-1\}$ in each of the two Cases 1 and 2. Hence, $\begin{cases} j, & \text{if } j < m; \\ j-1, & \text{if } j \geq m \end{cases} \in \{1,2,\ldots,n-1\}$ holds in every situation (because the Cases 1 and 2 cover all possibilities), qed.

First, let $i \in \{1,2,\ldots,n-1\}$ be arbitrary. Then, we are going to show that $(\omega \circ \eta)(i) = i$.

Clearly, $i \in \{1,2,\ldots,n-1\} \subseteq \{1,2,\ldots,n\}$. Also, from $i \in \{1,2,\ldots,n-1\}$, we obtain $i+1 \in \{2,3,\ldots,n\} \subseteq \{1,2,\ldots,n\}$. We must be in one of the following two cases:

Case 1: We have $i < m$.

Case 2: We have $i \geq m$.

Let us first consider Case 1. In this case, we have $i < m$. The definition of η yields $\eta(i) = \begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} = i$ (since $i < m$). But

$$(\omega \circ \eta)(i) = \omega\left(\underbrace{\eta(i)}_{=i}\right) = \omega(i) = \begin{cases} i, & \text{if } i < m; \\ i-1, & \text{if } i \geq m \end{cases} \qquad \text{(by the definition of } \omega\text{)}$$
$$= i \qquad (\text{since } i < m).$$

Thus, $(\omega \circ \eta)(i) = i$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $i \geq m$. Hence, $i+1 \geq m+1 > m$. But the definition of η yields $\eta(i) = \begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} = i+1$ (since $i \geq m$). Now,

$$(\omega \circ \eta)(i) = \omega\left(\underbrace{\eta(i)}_{=i+1}\right) = \omega(i+1) = \begin{cases} i+1, & \text{if } i+1 < m; \\ (i+1)-1, & \text{if } i+1 \geq m \end{cases}$$
$$\text{(by the definition of } \omega(i+1))$$
$$= (i+1) - 1 \qquad (\text{since } i+1 \geq m)$$
$$= i.$$

Hence, $(\omega \circ \eta)(i) = i$ is proven in Case 2.

Now, we have proven that $(\omega \circ \eta)(i) = i$ in each of the two Cases 1 and 2. Thus, $(\omega \circ \eta)(i) = i$ holds in every situation (because these two Cases 1 and 2 cover all situations). Hence, $(\omega \circ \eta)(i) = i = \mathrm{id}(i)$.

Now, forget that we fixed i. We thus have proven that for every $i \in \{1,2,\ldots,n-1\}$, we have $(\omega \circ \eta)(i) = \mathrm{id}(i)$. In other words,

$$\omega \circ \eta = \mathrm{id}. \tag{438}$$

On the other hand, let $p \in \{1,2,\ldots,n\} \setminus \{m\}$ be arbitrary. We will show that $(\eta \circ \omega)(p) = p$.

Indeed, we have $p \in \{1,2,\ldots,n\}$ and $p \neq m$ (since $p \in \{1,2,\ldots,n\} \setminus \{m\}$). From $p \in \{1,2,\ldots,n\}$, we obtain $1 \leq p \leq n$. We must be in one of the following two cases:

Case 1: We have $p < m$.

Case 2: We have $p \geq m$.

Let us first consider Case 1. In this case, we have $p < m$. The definition of $\omega(p)$

yields $\omega(p) = \begin{cases} p, & \text{if } p < m; \\ p-1, & \text{if } p \geq m \end{cases} = p$ (since $p < m$). Now,

$$(\eta \circ \omega)(p) = \eta\left(\underbrace{\omega(p)}_{=p}\right) = \eta(p) = \begin{cases} p, & \text{if } p < m; \\ p+1, & \text{if } p \geq m \end{cases}$$
$$\text{(by the definition of } \eta(p))$$
$$= p \qquad (\text{since } p < m).$$

Hence, $(\eta \circ \omega)(p) = p$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $p \geq m$. Combined with $p \neq m$, this yields $p > m$, and therefore $p \geq m+1$ (since p and m are integers). Hence, $p - 1 \geq m$. The definition of $\omega(p)$ yields $\omega(p) = \begin{cases} p, & \text{if } p < m; \\ p-1, & \text{if } p \geq m \end{cases} = p-1$ (since $p \geq m$). Now,

$$(\eta \circ \omega)(p) = \eta\left(\underbrace{\omega(p)}_{=p-1}\right) = \eta(p-1) = \begin{cases} p-1, & \text{if } p-1 < m; \\ (p-1)+1, & \text{if } p-1 \geq m \end{cases}$$
$$\text{(by the definition of } \eta(p-1))$$
$$= (p-1)+1 \qquad (\text{since } p-1 \geq m)$$
$$= p.$$

Hence, $(\eta \circ \omega)(p) = p$ is proven in Case 2.

Now, we have proven that $(\eta \circ \omega)(p) = p$ in each of the two Cases 1 and 2. Thus, $(\eta \circ \omega)(p) = p$ holds in every situation (because these two Cases 1 and 2 cover all situations). Hence, $(\eta \circ \omega)(p) = p = \mathrm{id}(p)$.

Now, forget that we fixed p. We thus have proven that for every $p \in \{1, 2, \ldots, n\} \setminus \{m\}$, we have $(\eta \circ \omega)(p) = \mathrm{id}(p)$. In other words,

$$\eta \circ \omega = \mathrm{id}.$$

Combined with (438), this yields that the maps η and ω are mutually inverse. This yields that η and ω are bijective. This proves Lemma 35.5 **(c)**.

(d) Let $\sigma \in S_{n-1}$. For every $i \in \{1, 2, \ldots, n\}$, the element $\begin{cases} \eta(\sigma(i-1)), & \text{if } i \neq 1; \\ m, & \text{if } i = 1 \end{cases}$ is a well-defined element of $\{1, 2, \ldots, n\}$ [219]. In other words, for every $i \in \{1, 2, \ldots, n\}$,

---

[219] *Proof.* Let $i \in \{1, 2, \ldots, n\}$. We need to prove that $\begin{cases} \eta(\sigma(i-1)), & \text{if } i \neq 1; \\ m, & \text{if } i = 1 \end{cases}$ is a well-defined element of $\{1, 2, \ldots, n\}$.

If $i = 1$, then

$$\begin{cases} \eta(\sigma(i-1)), & \text{if } i \neq 1; \\ m, & \text{if } i = 1 \end{cases} = m \qquad (\text{since } i = 1)$$

is a well-defined element of $\{1, 2, \ldots, n\}$. Hence, for the rest of our proof (of the fact that $\begin{cases} \eta(\sigma(i-1)), & \text{if } i \neq 1; \\ m, & \text{if } i = 1 \end{cases}$ is a well-defined element of $\{1, 2, \ldots, n\}$), we can WLOG assume that we don't have $i = 1$. Assume this.

We don't have $i = 1$. Thus, $i \neq 1$. Since $i \in \{1, 2, \ldots, n\}$ and $i \neq 1$, we have $i \in$

the right hand side of (434) is a well-defined element of $\{1,2,\ldots,n\}$. Hence, the map $\operatorname{ins}_m \sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ is well-defined (because the map $\operatorname{ins}_m \sigma : \{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$ was defined by (434)). Lemma 35.5 **(d)** is thus proven.

(e) By the definition of $S_{n,m}$, we have

$$S_{n,m} = \{\sigma \in S_n \mid \sigma(1) = m\} = \{\tau \in S_n \mid \tau(1) = m\} \tag{439}$$

(here, we renamed the index σ as τ).

Let $\sigma \in S_{n-1}$. We are going to show that $\operatorname{ins}_m \sigma \in S_{n,m}$.

Consider the map η defined in Lemma 35.5 **(a)** and the map ω defined in Lemma 35.5 **(b)**. The maps η and ω are mutually inverse (by Lemma 35.5 **(c)**). Thus, η is bijective. Hence, η is injective and surjective. On the other hand, σ is an element of S_{n-1}, thus a permutation of $\{1,2,\ldots,n-1\}$. Hence, σ is bijective, and thus injective.

We know that $\operatorname{ins}_m \sigma$ is a map $\{1,2,\ldots,n\} \to \{1,2,\ldots,n\}$. We now will prove that this map $\operatorname{ins}_m \sigma$ is injective.

In fact, let a and b be two elements of $\{1,2,\ldots,n\}$ such that $(\operatorname{ins}_m \sigma)(a) = (\operatorname{ins}_m \sigma)(b)$.

We assume (for the sake of contradiction) that $a \neq b$.

We have $a \neq 1$. [220] Similarly, $b \neq 1$. Now, the definition of $(\operatorname{ins}_m \sigma)(a)$ yields

$$(\operatorname{ins}_m \sigma)(a) = \begin{cases} \eta(\sigma(a-1)), & \text{if } a \neq 1; \\ m, & \text{if } a = 1 \end{cases} = \eta(\sigma(a-1)) \qquad (\text{since } a \neq 1).$$

Similarly, $(\operatorname{ins}_m \sigma)(b) = \eta(\sigma(b-1))$.

We have $(\operatorname{ins}_m \sigma)(a) = (\operatorname{ins}_m \sigma)(b) = \eta(\sigma(b-1))$. Compared with $(\operatorname{ins}_m \sigma)(a) = \eta(\sigma(a-1))$, this yields $\eta(\sigma(a-1)) = \eta(\sigma(b-1))$. Since η is injective, this yields $\sigma(a-1) = \sigma(b-1)$. Hence, $a-1 = b-1$ (since the map σ is also bijective). Thus, $a = b$, which contradicts $a \neq b$. This contradiction shows that our assumption (that $a \neq b$) was wrong. Thus, we cannot have $a \neq b$. We therefore have $a = b$.

$\{1,2,\ldots,n\} \setminus \{1\} = \{2,3,\ldots,n\}$. Hence, $i \in \{1,2,\ldots,n-1\}$. Thus, $\sigma(i-1)$ is a well-defined element of $\{1,2,\ldots,n-1\}$ (since $\sigma \in S_{n-1}$), and therefore $\eta(\sigma(i-1))$ is a well-defined element of $\{1,2,\ldots,n\} \setminus \{m\} \subseteq \{1,2,\ldots,n\}$.

Now,

$$\begin{cases} \eta(\sigma(i-1)), & \text{if } i \neq 1; \\ m, & \text{if } i = 1 \end{cases} = \eta(\sigma(i-1)) \qquad (\text{since } i \neq 1)$$

is a well-defined element of $\{1,2,\ldots,n\}$, qed.

[220] *Proof.* Assume the contrary. Then, we don't have $a \neq 1$. Hence, we have $a = 1$. Now, the definition of $\operatorname{ins}_m \sigma$ yields

$$(\operatorname{ins}_m \sigma)(a) = \begin{cases} \eta(\sigma(a-1)), & \text{if } a \neq 1; \\ m, & \text{if } a = 1 \end{cases} = m \qquad (\text{since } a = 1),$$

so that $m = (\operatorname{ins}_m \sigma)(a)$. But we have $a \neq b$, so that $b \neq a = 1$. The definition of $\operatorname{ins}_m \sigma$ yields

$$\begin{aligned}(\operatorname{ins}_m \sigma)(b) &= \begin{cases} \eta(\sigma(b-1)), & \text{if } b \neq 1; \\ m, & \text{if } b = 1 \end{cases} = \eta(\sigma(b-1)) \qquad (\text{since } b \neq 1) \\ &\in \{1,2,\ldots,n\} \setminus \{m\} \qquad (\text{since the target of } \eta \text{ is } \{1,2,\ldots,n\} \setminus \{m\}),\end{aligned}$$

so that $(\operatorname{ins}_m \sigma)(b) \neq m$. Now, we have $m = (\operatorname{ins}_m \sigma)(a) = (\operatorname{ins}_m \sigma)(b) \neq m$. This is a contradiction. This contradiction proves that our assumption was wrong, qed.

Now, forget that we fixed a and b. We thus have proven that if a and b are two elements of $\{1,2,\ldots,n\}$ such that $(\mathrm{ins}_m\,\sigma)(a) = (\mathrm{ins}_m\,\sigma)(b)$, then $a = b$. In other words, the map $\mathrm{ins}_m\,\sigma$ is injective.

Next, let us notice that $(\mathrm{ins}_m\,\sigma)(1)$ is well-defined (since $1 \in \{1,2,\ldots,n\}$), and the definition of $\mathrm{ins}_m\,\sigma$ yields

$$(\mathrm{ins}_m\,\sigma)(1) = \begin{cases} \eta(\sigma(1-1)), & \text{if } 1 \neq 1; \\ m, & \text{if } 1 = 1 \end{cases} = m \qquad (\text{since } 1 = 1).$$

Next, let us show that the map $\mathrm{ins}_m\,\sigma$ is surjective. In order to do so, we will show that every $j \in \{1,2,\ldots,n\}$ satisfies $j \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$.

Let $j \in \{1,2,\ldots,n\}$. We are going to show that $j \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$.

We must be in one of the following two cases:

Case 1: We have $j = m$.

Case 2: We have $j \neq m$.

Let us first consider Case 1. In this case, we have $j = m$. Recall that $(\mathrm{ins}_m\,\sigma)(1) = m$. Hence, $m = (\mathrm{ins}_m\,\sigma)\left(\underbrace{1}_{\in\{1,2,\ldots,n\}}\right) \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$. Now, $j = m \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$. Hence, $j \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $j \neq m$. Combining $j \in \{1,2,\ldots,n\}$ and $j \neq m$, we obtain $j \in \{1,2,\ldots,n\} \setminus \{m\} = \eta(\{1,2,\ldots,n-1\})$ (because η is surjective). Hence, there exists some $i \in \{1,2,\ldots,n-1\}$ such that $\eta(i) = j$. Consider this i. We have $i \in \{1,2,\ldots,n-1\}$, and thus the element $\sigma^{-1}(i)$ of $\{1,2,\ldots,n-1\}$ is well-defined (because σ is a permutation of $\{1,2,\ldots,n-1\}$). We have $\sigma^{-1}(i) \in \{1,2,\ldots,n-1\}$, thus $\sigma^{-1}(i)+1 \in \{2,3,\ldots,n\} \subseteq \{1,2,\ldots,n\}$. Thus, $(\mathrm{ins}_m\,\sigma)(\sigma^{-1}(i)+1)$ is well-defined. Also, $\sigma^{-1}(i)+1 \neq 1$ (since $\sigma^{-1}(i)+1 \in \{2,3,\ldots,n\}$). The definition of $(\mathrm{ins}_m\,\sigma)(\sigma^{-1}(i)+1)$ yields

$$\begin{aligned}(\mathrm{ins}_m\,\sigma)\left(\sigma^{-1}(i)+1\right) &= \begin{cases} \eta(\sigma((\sigma^{-1}(i)+1)-1)), & \text{if } \sigma^{-1}(i)+1 \neq 1; \\ m, & \text{if } \sigma^{-1}(i)+1 = 1 \end{cases} \\ &= \eta\left(\sigma\left(\underbrace{\left(\sigma^{-1}(i)+1-1\right)}_{=\sigma^{-1}(i)}\right)\right) \qquad \left(\text{since } \sigma^{-1}(i)+1 \neq 1\right) \\ &= \eta\left(\underbrace{\sigma\left(\sigma^{-1}(i)\right)}_{=i}\right) = \eta(i) = j.\end{aligned}$$

Hence,

$$j = (\mathrm{ins}_m\,\sigma)\left(\underbrace{\sigma^{-1}(i)+1}_{\in\{1,2,\ldots,n\}}\right) \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\}).$$

Thus, $j \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$ is proven in Case 2.

We now have proven $j \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$ in each of the two Cases 1 and 2. Since these two Cases cover all possibilities, this yields that $j \in (\mathrm{ins}_m\,\sigma)(\{1,2,\ldots,n\})$ always holds.

Now, forget that we fixed j. We thus have shown that every $j \in \{1, 2, \ldots, n\}$ satisfies $j \in (\mathrm{ins}_m \sigma)(\{1, 2, \ldots, n\})$. In other words, $\{1, 2, \ldots, n\} \subseteq (\mathrm{ins}_m \sigma)(\{1, 2, \ldots, n\})$. In other words, the map $\mathrm{ins}_m \sigma$ is surjective. Combining this with the fact that $\mathrm{ins}_m \sigma$ is injective, we conclude that $\mathrm{ins}_m \sigma$ is bijective. Thus, $\mathrm{ins}_m \sigma$ is a bijective map $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. In other words, $\mathrm{ins}_m \sigma$ is a permutation of $\{1, 2, \ldots, n\}$. In other words, $\mathrm{ins}_m \sigma$ is an element of S_n. We thus have shown that $\mathrm{ins}_m \sigma \in S_n$.

We now know that $\mathrm{ins}_m \sigma$ is an element of S_n and satisfies $(\mathrm{ins}_m \sigma)(1) = m$. In other words,

$$\mathrm{ins}_m \sigma \in \{\tau \in S_n \mid \tau(1) = m\} = S_{n,m} \qquad \text{(by (439))}.$$

Thus, $\mathrm{ins}_m \sigma$ is a well-defined element of $S_{n,m}$.

Now, forget that we fixed σ. We thus have proven that for every $\sigma \in S_{n-1}$, the map $\mathrm{ins}_m \sigma$ is a well-defined element of $S_{n,m}$. In other words, for every $\sigma \in S_{n-1}$, the right hand side of (435) is a well-defined element of $S_{n,m}$. Hence, the map $\iota_m : S_{n-1} \to S_{n,m}$ is well-defined (because the map $\iota_m : S_{n-1} \to S_{n,m}$ was defined by (435)). Lemma 35.5 **(e)** is thus proven.

(f) Let $\tau \in S_{n,m}$. Then, $\tau \in S_{n,m} = \{\sigma \in S_n \mid \sigma(1) = m\}$. In other words, τ is an element of S_n and satisfies $\tau(1) = m$.

We have $\tau \in S_n$. Thus, τ is a permutation of $\{1, 2, \ldots, n\}$, hence a bijection. In particular, this yields that τ is injective.

For every $i \in \{1, 2, \ldots, n-1\}$, the element $\omega(\tau(i+1))$ is a well-defined element of $\{1, 2, \ldots, n-1\}$ [221]. In other words, for every $i \in \{1, 2, \ldots, n-1\}$, the right hand side of (436) is a well-defined element of $\{1, 2, \ldots, n-1\}$. Hence, the map $\mathrm{del}_m \sigma : \{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}$ is well-defined (because the map $\mathrm{del}_m \sigma : \{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}$ was defined by (436)). Lemma 35.5 **(f)** is thus proven.

(g) Let $\tau \in S_{n,m}$. We are going to show that $\mathrm{del}_m \tau \in S_{n-1}$.

We have $\tau \in S_{n,m} = \{\sigma \in S_n \mid \sigma(1) = m\}$ (by the definition of $S_{n,m}$). In other words, τ is an element of S_n and satisfies $\tau(1) = m$.

Consider the map η defined in Lemma 35.5 **(a)** and the map ω defined in Lemma 35.5 **(b)**. The maps η and ω are mutually inverse (by Lemma 35.5 **(c)**). Thus, ω is bijective. Hence, ω is injective and surjective. On the other hand, τ is an element of S_n, thus a permutation of $\{1, 2, \ldots, n\}$. Hence, τ is bijective. Thus, the inverse τ^{-1} of τ is also bijective, and therefore injective. The target of τ^{-1} is $\{1, 2, \ldots, n\}$ (since $\tau^{-1} \in S_n$).

We know that $\mathrm{del}_m \tau$ is a map $\{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}$. We now will prove that this map $\mathrm{del}_m \tau$ is injective.

In fact, let a and b be two elements of $\{1, 2, \ldots, n-1\}$ such that $(\mathrm{del}_m \tau)(a) = (\mathrm{del}_m \tau)(b)$.

The definition of $\mathrm{del}_m \sigma$ yields $(\mathrm{del}_m \sigma)(a) = \omega(\tau(a+1))$. Hence, $\omega(\tau(a+1)) = (\mathrm{del}_m \sigma)(a)$.

[221] *Proof.* Let $i \in \{1, 2, \ldots, n-1\}$. We need to prove that $\omega(\tau(i+1))$ is a well-defined element of $\{1, 2, \ldots, n-1\}$.

We have $i \in \{1, 2, \ldots, n-1\}$, so that $i+1 \in \{2, 3, \ldots, n\}$ and thus $i+1 \neq 1$.

We have $i+1 \in \{2, 3, \ldots, n\} \subseteq \{1, 2, \ldots, n\}$, so that $\tau(i+1)$ is well-defined.

If we had $\tau(i+1) = \tau(1)$, then we would have $i+1 = i$ (since τ is injective), which would contradict $i+1 \neq i$. Hence, we don't have $\tau(i+1) = \tau(1)$. Thus, we have $\tau(i+1) \neq \tau(1) = m$. Since $\tau(i+1) \in \{1, 2, \ldots, n\}$ (because the target of τ is $\{1, 2, \ldots, n\}$) and $\tau(i+1) \neq m$, we must have $\tau(i+1) \in \{1, 2, \ldots, n\} \setminus \{m\}$. Thus, $\omega(\tau(i+1))$ is a well-defined element of $\{1, 2, \ldots, n-1\}$.

The definition of $\operatorname{del}_m \sigma$ yields $(\operatorname{del}_m \sigma)(b) = \omega(\tau(b+1))$. Now,

$$\omega(\tau(a+1)) = (\operatorname{del}_m \sigma)(a) = (\operatorname{del}_m \sigma)(b) = \omega(\tau(b+1)).$$

Since ω is injective, this yields $\tau(a+1) = \tau(b+1)$. Thus, $a+1 = b+1$ (since τ is injective), so that $a = b$.

Now, forget that we fixed a and b. We thus have proven that if a and b are two elements of $\{1, 2, \ldots, n-1\}$ such that $(\operatorname{del}_m \tau)(a) = (\operatorname{del}_m \tau)(b)$, then $a = b$. In other words, the map $\operatorname{del}_m \tau$ is injective.

Next, let us show that the map $\operatorname{del}_m \tau$ is surjective. In order to do so, we will show that every $j \in \{1, 2, \ldots, n-1\}$ satisfies $j \in (\operatorname{del}_m \tau)(\{1, 2, \ldots, n-1\})$.

Let $j \in \{1, 2, \ldots, n-1\}$. We are going to show that $j \in (\operatorname{del}_m \tau)(\{1, 2, \ldots, n-1\})$.

We have $j \in \{1, 2, \ldots, n-1\}$. Thus, $\eta(j)$ is a well-defined element of $\{1, 2, \ldots, n\} \setminus \{m\}$ (since η is a map $\{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n\} \setminus \{m\}$). Thus, $\eta(j) \in \{1, 2, \ldots, n\} \setminus \{m\} \subseteq \{1, 2, \ldots, n\}$, so that $\tau^{-1}(\eta(j))$ is well-defined (since $\tau^{-1} \in S_n$). Moreover, $\eta(j) \neq m$ (since $\eta(j) \in \{1, 2, \ldots, n\} \setminus \{m\}$). If we would have $\tau^{-1}(\eta(j)) = \tau^{-1}(m)$, then we would have $\eta(j) = m$ (since τ^{-1} is injective), which would contradict the fact that $\eta(j) \neq m$. Hence, we cannot have $\tau^{-1}(\eta(j)) = \tau^{-1}(m)$. Thus, we have $\tau^{-1}(\eta(j)) \neq \tau^{-1}(m) = 1$ (since $\tau(1) = m$). But $\tau^{-1}(\eta(j)) \in \{1, 2, \ldots, n\}$ (since the target of τ^{-1} is $\{1, 2, \ldots, n\}$). Combined with $\tau^{-1}(\eta(j)) \neq 1$, this yields $\tau^{-1}(\eta(j)) \in \{1, 2, \ldots, n\} \setminus \{1\} = \{2, 3, \ldots, n\}$. Hence, $\tau^{-1}(\eta(j)) - 1 \in \{1, 2, \ldots, n-1\}$. Denote the element $\tau^{-1}(\eta(j)) - 1$ of $\{1, 2, \ldots, n-1\}$ by g. Thus, $g \in \{1, 2, \ldots, n-1\}$ and

$$\tau\left(\underbrace{g}_{=\tau^{-1}(\eta(j))-1} + 1\right) = \tau\left(\underbrace{\tau^{-1}(\eta(j)) - 1 + 1}_{=\tau^{-1}(\eta(j))}\right) = \tau\left(\tau^{-1}(\eta(j))\right) = \eta(j).$$

Now, the definition of $\operatorname{del}_m \tau$ yields

$$(\operatorname{del}_m \tau)(g) = \omega\left(\underbrace{\tau(g+1)}_{=\eta(j)}\right) = \omega(\eta(j)) = \underbrace{(\omega \circ \eta)}_{\substack{=\mathrm{id} \\ \text{(since the maps } \eta \text{ and } \omega \\ \text{are mutually inverse)}}}(j) = \mathrm{id}(j) = j.$$

Thus,

$$j = (\operatorname{del}_m \tau)\left(\underbrace{g}_{\in\{1,2,\ldots,n-1\}}\right) \in (\operatorname{del}_m \tau)(\{1, 2, \ldots, n-1\}).$$

Now, forget that we fixed j. We thus have shown that every $j \in \{1, 2, \ldots, n-1\}$ satisfies $j \in (\operatorname{del}_m \tau)(\{1, 2, \ldots, n-1\})$. In other words,

$$\{1, 2, \ldots, n-1\} \subseteq (\operatorname{del}_m \tau)(\{1, 2, \ldots, n-1\}).$$

In other words, the map $\operatorname{del}_m \tau$ is surjective. Combining this with the fact that $\operatorname{del}_m \tau$ is injective, we conclude that $\operatorname{del}_m \tau$ is bijective. Thus, $\operatorname{del}_m \tau$ is a bijective map $\{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n-1\}$. In other words, $\operatorname{del}_m \tau$ is a permutation of $\{1, 2, \ldots, n-1\}$. In other words, $\operatorname{del}_m \tau$ is an element of S_{n-1}. We thus have shown that $\operatorname{del}_m \tau \in S_{n-1}$. Thus, $\operatorname{del}_m \tau$ is a well-defined element of S_{n-1}.

Now, forget that we fixed τ. We thus have proven that for every $\tau \in S_{n,m}$, the map $\operatorname{del}_m \tau$ is a well-defined element of S_{n-1}. In other words, for every $\tau \in S_{n,m}$, the right hand side of (437) is a well-defined element of S_{n-1}. Hence, the map $\pi_m : S_{n,m} \to S_{n-1}$ is well-defined (because the map $\pi_m : S_{n,m} \to S_{n-1}$ was defined by (437)). Lemma 35.5 **(g)** is thus proven.

(h) Consider the map η defined in Lemma 35.5 **(a)** and the map ω defined in Lemma 35.5 **(b)**. The maps η and ω are mutually inverse (by Lemma 35.5 **(c)**). Clearly, the compositions $\iota_m \circ \pi_m$ and $\pi_m \circ \iota_m$ are well-defined.

Consider also the notation $\operatorname{ins}_m \sigma$ (for every $\sigma \in S_{n-1}$) defined in Lemma 35.5 **(d)**, and the notation $\operatorname{del}_m \tau$ (for every $\tau \in S_{n,m}$) defined in Lemma 35.5 **(f)**.

Let us first prove that $\iota_m \circ \pi_m = \mathrm{id}$.

Indeed, let $\tau \in S_{n,m}$ be arbitrary. We have $\tau \in S_{n,m} = \{\sigma \in S_n \mid \sigma(1) = m\}$ (by the definition of $S_{n,m}$). In other words, τ is an element of S_n and satisfies $\tau(1) = m$.

Let $\tau' = (\iota_m \circ \pi_m)(\tau)$. Notice that $\tau' \in S_{n,m}$. We have

$$\tau' = (\iota_m \circ \pi_m)(\tau) = \iota_m \left(\underbrace{\pi_m(\tau)}_{\substack{=\operatorname{del}_m \tau \\ \text{(by the definition of } \pi_m\text{)}}} \right) = \iota_m(\operatorname{del}_m \tau) = \operatorname{ins}_m(\operatorname{del}_m \tau)$$

(by the definition of ι_m).

Let $i \in \{1, 2, \ldots, n\}$. We are going to prove that $\tau(i) = \tau'(i)$.

Indeed, we must be in one of the following two cases:

Case 1: We have $i = 1$.

Case 2: We have $i \neq 1$.

Let us first consider Case 1. In this case, we have $i = 1$. Since $i = 1$, we have

$$\begin{aligned}
\tau'(i) &= \underbrace{\tau'}_{=\operatorname{ins}_m(\operatorname{del}_m \tau)}(1) = (\operatorname{ins}_m(\operatorname{del}_m \tau))(1) = \begin{cases} \eta((\operatorname{del}_m \tau)(1-1)), & \text{if } 1 \neq 1; \\ m, & \text{if } 1 = 1 \end{cases} \\
&\qquad \text{(by the definition of } \operatorname{ins}_m(\operatorname{del}_m \tau)\text{)} \\
&= m \qquad \text{(since } 1 = 1\text{)} \\
&= \tau\left(\underbrace{1}_{=i}\right) \qquad \text{(since } \tau(1) = m\text{)} \\
&= \tau(i).
\end{aligned}$$

Thus, $\tau(i) = \tau'(i)$. We have thus proven $\tau(i) = \tau'(i)$ in Case 1.

Let us now consider Case 2. In this case, we have $i \neq 1$. We have

$$\underbrace{\tau'}_{=\operatorname{ins}_m(\operatorname{del}_m \tau)}(i) = (\operatorname{ins}_m(\operatorname{del}_m \tau))(i) = \begin{cases} \eta((\operatorname{del}_m \tau)(i-1)), & \text{if } i \neq 1; \\ m, & \text{if } i = 1 \end{cases}$$

$$\text{(by the definition of } \operatorname{ins}_m(\operatorname{del}_m \tau))$$

$$= \eta\left(\underbrace{(\operatorname{del}_m \tau)(i-1)}_{\substack{=\omega(\tau((i-1)+1)) \\ \text{(by the definition of } \operatorname{del}_m \tau)}}\right) \qquad (\text{since } i \neq 1)$$

$$= \eta\left(\omega\left(\tau\left(\underbrace{(i-1)+1}_{=i}\right)\right)\right) = \eta(\omega(\tau(i))) = \underbrace{(\eta \circ \omega)}_{\substack{=\mathrm{id} \\ \text{(since the maps } \eta \text{ and } \omega \\ \text{are mutually inverse)}}}(\tau(i))$$

$$= \mathrm{id}(\tau(i)) = \tau(i).$$

In other words, $\tau(i) = \tau'(i)$. We have thus proven $\tau(i) = \tau'(i)$ in Case 2.

We have therefore proven $\tau(i) = \tau'(i)$ in each of the two Cases 1 and 2. Since these two Cases cover all possibilities, this shows that $\tau(i) = \tau'(i)$ always holds.

Now, forget that we fixed i. We thus have shown that $\tau(i) = \tau'(i)$ for every $i \in \{1, 2, \ldots, n\}$. In other words, $\tau = \tau'$. Hence, $\tau = \tau' = (\iota_m \circ \pi_m)(\tau)$, so that $(\iota_m \circ \pi_m)(\tau) = \tau = \mathrm{id}(\tau)$.

Now, forget that we fixed τ. We thus have proven that $(\iota_m \circ \pi_m)(\tau) = \mathrm{id}(\tau)$ for every $\tau \in S_{n,m}$. In other words, $\iota_m \circ \pi_m = \mathrm{id}$.

Next, we will show that $\pi_m \circ \iota_m = \mathrm{id}$.

Let $\sigma \in S_{n-1}$. Let $\sigma' = (\pi_m \circ \iota_m)(\sigma)$. Notice that $\sigma' \in S_{n-1}$. We have

$$\sigma' = (\pi_m \circ \iota_m)(\sigma) = \pi_m\left(\underbrace{\iota_m(\sigma)}_{\substack{=\operatorname{ins}_m \sigma \\ \text{(by the definition of } \iota_m)}}\right) = \pi_m(\operatorname{ins}_m \sigma) = \operatorname{del}_m(\operatorname{ins}_m \sigma)$$

(by the definition of π_m).

Let $j \in \{1, 2, \ldots, n-1\}$. We are going to prove that $\sigma(j) = \sigma'(j)$. We have $j \in \{1, 2, \ldots, n-1\}$, and therefore $j+1 \in \{2, 3, \ldots, n\}$ and thus $j+1 \neq 1$. Now, the definition of $\operatorname{ins}_m \sigma$ yields

$$(\operatorname{ins}_m \sigma)(j+1) = \begin{cases} \eta(\sigma((j+1)-1)), & \text{if } j+1 \neq 1; \\ m, & \text{if } j+1 = 1 \end{cases}$$

$$= \eta\left(\sigma\left(\underbrace{(j+1)-1}_{=j}\right)\right) \qquad (\text{since } j+1 \neq 1)$$

$$= \eta(\sigma(j)).$$

Now,

$$\underbrace{\sigma'}_{=\operatorname{del}_m(\operatorname{ins}_m\sigma)}(j) = (\operatorname{del}_m(\operatorname{ins}_m\sigma))(j) = \omega\left(\underbrace{(\operatorname{ins}_m\sigma)(j+1)}_{=\eta(\sigma(j))}\right)$$

$$\text{(by the definition of } \operatorname{del}_m(\operatorname{ins}_m\sigma))$$

$$= \omega(\eta(\sigma(j))) = \underbrace{(\omega\circ\eta)}_{\substack{=\mathrm{id}\\ \text{(since the maps } \eta \text{ and } \omega\\ \text{are mutually inverse)}}}(\sigma(j))$$

$$= \mathrm{id}(\sigma(j)) = \sigma(j).$$

In other words, $\sigma(j) = \sigma'(j)$.

Now forget that we fixed j. We thus have shown that every $j \in \{1, 2, \ldots, n-1\}$ satisfies $\sigma(j) = \sigma'(j)$. In other words, $\sigma = \sigma'$. Thus, $\sigma = \sigma' = (\pi_m \circ \iota_m)(\sigma)$, so that $(\pi_m \circ \iota_m)(\sigma) = \sigma = \mathrm{id}(\sigma)$.

Now forget that we fixed σ. We thus have proven that every $\sigma \in S_{n-1}$ satisfies $(\pi_m \circ \iota_m)(\sigma) = \mathrm{id}(\sigma)$. In other words, $\pi_m \circ \iota_m = \mathrm{id}$. Combined with $\iota_m \circ \pi_m = \mathrm{id}$, this yields that the maps ι_m and π_m are mutually inverse. Lemma 35.5 **(h)** is therefore proven. □

We can now proceed to the proof of Theorem 35.1.

Proof of Theorem 35.1. **(a)** Let $s \in \{0, 1, \ldots, r-1\}$. Let a_1, a_2, ..., a_s be s elements of $\operatorname{Prim} H$. Then, $a_1 a_2 \cdots a_s \in (\operatorname{Prim} H)^s$ (since $a_i \in \operatorname{Prim} H$ for every $i \in \{1, 2, \ldots, s\}$). Hence,

$$(f_1 * f_2 * \cdots * f_r)\left(\underbrace{a_1 a_2 \cdots a_s}_{\in (\operatorname{Prim} H)^s}\right) \in (f_1 * f_2 * \cdots * f_r)\left((\operatorname{Prim} H)^s\right) = 0$$

(by Lemma 35.4). Hence, $(f_1 * f_2 * \cdots * f_r)(a_1 a_2 \cdots a_s) = 0$. This proves Theorem 35.1 **(a)**.

(b) We are going to prove Theorem 35.1 **(b)** by induction over r:

Induction base: If $r = 0$, then Theorem 35.1 **(b)** is true[222]. Hence, the induction base is complete.

Induction step: Let $n \in \mathbb{N}$ be positive. Assume that Theorem 35.1 **(b)** is proven for $r = n - 1$. We now are going to prove that Theorem 35.1 **(b)** holds for $r = n$.

Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let f_1, f_2, ..., f_n be n maps in $\mathfrak{g}(H, A)$. Let a_1, a_2, ..., a_n be n elements of $\operatorname{Prim} H$. We will prove that

$$(f_1 * f_2 * \cdots * f_n)(a_1 a_2 \cdots a_n) = \sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).$$

[222] *Proof.* Assume that $r = 0$. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let f_1, f_2, ..., f_0 be 0 maps in $\mathfrak{g}(H, A)$ (that is, no maps). Let a_1, a_2, ..., a_0 be 0 elements of $\operatorname{Prim} H$ (that is, no elements). Since $r = 0$, we have $S_r = S_0 = \{\mathrm{id}\}$. But since $r = 0$, we have $f_1 * f_2 * \cdots * f_r =$ (empty product with respect to convolution) $= e_{H,A}$. Also, since $r = 0$, we have

Let $g = f_2 * f_3 * \cdots * f_n$. Then, g is a k-linear map $H \to A$. We have

$$f_1 * f_2 * \cdots * f_n = f_1 * \underbrace{\left(f_2 * f_3 * \cdots * f_n\right)}_{=g} = f_1 * g = \mu_A \circ (f_1 \otimes g) \circ \Delta$$

(by the definition of convolution). Hence,

$$\begin{aligned}\left(f_1 * f_2 * \cdots * f_n\right)(a_1 a_2 \cdots a_n) &= \left(\mu_A \circ (f_1 \otimes g) \circ \Delta\right)(a_1 a_2 \cdots a_n) \\ &= \mu_A\left(\left(f_1 \otimes g\right)\left(\Delta\left(a_1 a_2 \cdots a_n\right)\right)\right). \qquad (440)\end{aligned}$$

We are now going to study the term $\left(f_1 \otimes g\right)\left(\Delta\left(a_1 a_2 \cdots a_n\right)\right)$ on the right hand side of this.

We have

$$\begin{aligned}&\left(f_1 \otimes g\right)\left(\begin{array}{c}\underbrace{\Delta\left(a_1 a_2 \cdots a_n\right)}_{\in \sum_{m=1}^{n} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right) + 1_H \otimes \left(a_1 a_2 \cdots a_n\right) + \sum_{\ell=0}^{n-2} H \otimes \left(\operatorname{Prim} H\right)^{\ell}} \\ \text{(by Lemma 35.2, applied to } V = \operatorname{Prim} H \text{ and } s = n\text{)}\end{array}\right) \\ &\in \left(f_1 \otimes g\right)\left(\sum_{m=1}^{n} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right) + 1_H \otimes \left(a_1 a_2 \cdots a_n\right) + \sum_{\ell=0}^{n-2} H \otimes \left(\operatorname{Prim} H\right)^{\ell}\right) \\ &\subseteq \left(f_1 \otimes g\right)\left(\sum_{m=1}^{n} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)\right) \\ &\quad + \left(f_1 \otimes g\right)\left(1_H \otimes \left(a_1 a_2 \cdots a_n\right)\right) + \left(f_1 \otimes g\right)\left(\sum_{\ell=0}^{n-2} H \otimes \left(\operatorname{Prim} H\right)^{\ell}\right). \qquad (441)\end{aligned}$$

$a_1 a_2 \cdots a_r = (\text{empty product}) = 1_H$. Thus,

$$\begin{aligned}&\underbrace{\left(f_1 * f_2 * \cdots * f_r\right)}_{=e_{H,A}}\left(\underbrace{a_1 a_2 \cdots a_r}_{=1_H}\right) \\ &= \underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_H}\left(1_H\right) = \left(\eta_A \circ \varepsilon_H\right)\left(1_H\right) = \eta_A\left(\begin{array}{c}\underbrace{\varepsilon_H\left(1_H\right)}_{=1} \\ \text{(since } H \text{ is a bialgebra)}\end{array}\right) = \eta_A(1) \\ &= 1 \cdot 1_A \qquad \text{(by the definition of } \eta_A\text{)} \\ &= 1_A\end{aligned}$$

and

$$\underbrace{\sum_{\sigma \in S_r}}_{\substack{= \sum_{\sigma \in \{\mathrm{id}\}} \\ \text{(since } S_r = \{\mathrm{id}\}\text{)}}} \underbrace{f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_r\left(a_{\sigma(r)}\right)}_{\substack{=(\text{empty product}) \\ \text{(since } r = 0\text{)}}} = \sum_{\sigma \in \{\mathrm{id}\}} \underbrace{(\text{empty product})}_{=1_A} = \sum_{\sigma \in \{\mathrm{id}\}} 1_A = 1_A.$$

Hence, $\left(f_1 * f_2 * \cdots * f_r\right)\left(a_1 a_2 \cdots a_r\right) = 1_A = \sum_{\sigma \in S_r} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_r\left(a_{\sigma(r)}\right)$. Hence, Theorem 35.1 **(b)** is true for $r = 0$, qed.

But $f_1 \in \mathfrak{g}(H, A) = \{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\}$. In other words, f_1 is an element of $\mathcal{L}(H, A)$ and satisfies $f_1(1_H) = 0$. Now,

$$(f_1 \otimes g)(1_H \otimes (a_1 a_2 \cdots a_n)) = \underbrace{f_1(1_H)}_{=0} \otimes g(a_1 a_2 \cdots a_n) = 0 \otimes g(a_1 a_2 \cdots a_n) = 0. \quad (442)$$

Furthermore, every $\ell \in \{0, 1, \ldots, (n-1)-1\}$ satisfies

$$\underbrace{g}_{=f_2 * f_3 * \cdots * f_n}\left((\operatorname{Prim} H)^{\ell}\right) = (f_2 * f_3 * \cdots * f_n)\left((\operatorname{Prim} H)^{\ell}\right) = 0 \quad (443)$$

(by Lemma 35.4, applied to $n-1$, $(f_2, f_3, \ldots, f_n)$ and ℓ instead of r, $(f_1, f_2, \ldots, f_r)$ and s). Now,

$$\begin{aligned}
&(f_1 \otimes g)\left(\sum_{\ell=0}^{n-2} H \otimes (\operatorname{Prim} H)^{\ell}\right) \\
&\subseteq \sum_{\ell=0}^{n-2} \underbrace{(f_1 \otimes g)\left(H \otimes (\operatorname{Prim} H)^{\ell}\right)}_{\subseteq f_1(H) \otimes g\left((\operatorname{Prim} H)^{\ell}\right)} \qquad \text{(since } f_1 \otimes g \text{ is a } k\text{-linear map)} \\
&\subseteq \sum_{\ell=0}^{n-2} f_1(H) \otimes \underbrace{g\left((\operatorname{Prim} H)^{\ell}\right)}_{\substack{=0 \\ \text{(by (443) (since} \\ \ell \in \{0,1,\ldots,n-2\} = \{0,1,\ldots,(n-1)-1\}))}} = \sum_{\ell=0}^{n-2} \underbrace{f_1(H) \otimes 0}_{=0} = \sum_{\ell=0}^{n-2} 0 = 0. \quad (444)
\end{aligned}$$

Now, (441) becomes

$$\begin{aligned}
&(f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_n)) \\
&\in (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right) \\
&\qquad + \underbrace{(f_1 \otimes g)(1_H \otimes (a_1 a_2 \cdots a_n))}_{\substack{=0 \\ \text{(by (442))}}} + \underbrace{(f_1 \otimes g)\left(\sum_{\ell=0}^{n-2} H \otimes (\operatorname{Prim} H)^{\ell}\right)}_{\substack{\subseteq 0 \\ \text{(by (442))}}} \\
&\subseteq (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right) + 0 + 0 \\
&= (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right).
\end{aligned}$$

In other words,

$$\begin{aligned}
&(f_1 \otimes g)\left(\Delta\left(a_1 a_2 \cdots a_n\right)\right) \\
&= (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)\right) \\
&= \sum_{m=1}^{n} \underbrace{(f_1 \otimes g)\left(a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)\right)}_{= f_1(a_m) \otimes g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)} \\
&\qquad \text{(since the map } f_1 \otimes g \text{ is } k\text{-linear)} \\
&= \sum_{m=1}^{n} f_1\left(a_m\right) \otimes g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right). \qquad (445)
\end{aligned}$$

Now, (440) becomes

$$\begin{aligned}
&\left(f_1 * f_2 * \cdots * f_n\right)\left(a_1 a_2 \cdots a_n\right) \\
&= \mu_A \left(\underbrace{(f_1 \otimes g)\left(\Delta\left(a_1 a_2 \cdots a_n\right)\right)}_{\substack{= \sum_{m=1}^{n} f_1(a_m) \otimes g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right) \\ \text{(by (445))}}} \right) \\
&= \mu_A \left(\sum_{m=1}^{n} f_1\left(a_m\right) \otimes g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)\right) \\
&= \sum_{m=1}^{n} \underbrace{\mu_A\left(f_1\left(a_m\right) \otimes g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)\right)}_{\substack{= f_1(a_m) \cdot g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right) \\ \text{(since } \mu_A \text{ is the multiplication map)}}} \\
&\qquad \text{(since the map } \mu_A \text{ is } k\text{-linear)} \\
&= \sum_{m=1}^{n} f_1\left(a_m\right) \cdot g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right). \qquad (446)
\end{aligned}$$

Now, we are going to show that every $m \in \{1, 2, \ldots, n\}$ satisfies

$$g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right) = \sum_{\substack{\sigma \in S_n; \\ \sigma(1) = m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right). \quad (447)$$

Proof of (447): Let $m \in \{1, 2, \ldots, n\}$.

We are going to use the subset $S_{n,m}$ of S_n defined in Lemma 35.5.

We are going to use the map $\eta : \{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n\} \setminus \{m\}$ defined in Lemma 35.5 **(a)**. (In particular, this means that we will not use the notation η for the unity map of a k-algebra in this proof, so as to avoid conflict of notation.) We are also going to use the map $\omega : \{1, 2, \ldots, n\} \setminus \{m\} \to \{1, 2, \ldots, n-1\}$ defined in Lemma 35.5 **(b)**. Lemma 35.5 **(c)** yields that the maps η and ω are mutually inverse. Hence, these maps η and ω are bijections.

We will use the notion of $\operatorname{del}_m \tau$ (for every $\tau \in S_{n,m}$) defined in Lemma 35.5 **(f)**. We will also use the map $\pi_m : S_{n,m} \to S_{n-1}$ defined in Lemma 35.5 **(g)**. We will furthermore use the map ι_m defined in Lemma 35.5 **(e)**. Lemma 35.5 **(h)** shows that the maps ι_m and π_m are mutually inverse. Hence, these maps ι_m and π_m are bijections.

For every $i \in \{1, 2, \ldots, n-1\}$, we know that $\eta(i)$ is a well-defined element of $\{1, 2, \ldots, n\} \setminus \{m\}$ (since η is a map $\{1, 2, \ldots, n-1\} \to \{1, 2, \ldots, n\} \setminus \{m\}$). Hence, for every $i \in \{1, 2, \ldots, n-1\}$, we have $\eta(i) \in \{1, 2, \ldots, n\} \setminus \{m\} \subseteq \{1, 2, \ldots, n\}$. Thus, for every $i \in \{1, 2, \ldots, n-1\}$, the element $a_{\eta(i)}$ is a well-defined element of $\operatorname{Prim} H$ (since a_1, a_2, ..., a_n are elements of $\operatorname{Prim} H$). Hence, we can define an $(n-1)$-tuple $(b_1, b_2, \ldots, b_{n-1}) \in (\operatorname{Prim} H)^{\times(n-1)}$ of elements of $\operatorname{Prim} H$ by setting

$$\left(b_i = a_{\eta(i)} \qquad \text{for every } i \in \{1, 2, \ldots, n-1\}\right). \tag{448}$$

Consider this $(n-1)$-tuple $(b_1, b_2, \ldots, b_{n-1})$.

It is easy to see that

$$b_1 b_2 \cdots b_{n-1} = (a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n) \tag{449}$$

[223].

[223] *Proof of (449):* Every $i \in \{1, 2, \ldots, m-1\}$ satisfies

$$\begin{aligned} \eta(i) &= \begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} && \text{(by (432))} \\ &= i && \text{(since } i < m \text{ (since } i \in \{1, 2, \ldots, m-1\})\text{)}. \end{aligned}$$

Hence, every $i \in \{1, 2, \ldots, m-1\}$ satisfies

$$\begin{aligned} b_i &= a_{\eta(i)} && \text{(by (448))} \\ &= a_i && \text{(since } \eta(i) = i\text{)}. \end{aligned}$$

Taking the product of these equalities over all $i \in \{1, 2, \ldots, m-1\}$, we obtain $b_1 b_2 \cdots b_{m-1} = a_1 a_2 \cdots a_{m-1}$.

Every $i \in \{m, m+1, \ldots, n-1\}$ satisfies

$$\begin{aligned} \eta(i) &= \begin{cases} i, & \text{if } i < m; \\ i+1, & \text{if } i \geq m \end{cases} && \text{(by (432))} \\ &= i+1 && \text{(since } i \geq m \text{ (since } i \in \{m, m+1, \ldots, n-1\})\text{)}. \end{aligned}$$

Hence, every $i \in \{m, m+1, \ldots, n-1\}$ satisfies

$$\begin{aligned} b_i &= a_{\eta(i)} && \text{(by (448))} \\ &= a_{i+1} && \text{(since } \eta(i) = i+1\text{)}. \end{aligned}$$

Taking the product of these equalities over all $i \in \{m, m+1, \ldots, n-1\}$, we obtain $b_m b_{m+1} \cdots b_{n-1} = a_{m+1} a_{(m+1)+1} \cdots a_{(n-1)+1}$.

Now,

$$\begin{aligned} b_1 b_2 \cdots b_{n-1} &= \left(\underbrace{b_1 b_2 \cdots b_{m-1}}_{= a_1 a_2 \cdots a_{m-1}} \right) \left(\underbrace{\underbrace{b_m b_{m+1} \cdots b_{n-1}}_{= a_{m+1} a_{(m+1)+1} \cdots a_{(n-1)+1}}}_{= a_{m+1} a_{m+2} \cdots a_n} \right) \\ &= (a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n). \end{aligned}$$

This proves (449).

On the other hand, we can apply Theorem 35.1 **(b)** to $n-1$, $(f_2, f_3, \ldots, f_n)$ and $(b_1, b_2, \ldots, b_{n-1})$ instead of r, $(f_1, f_2, \ldots, f_r)$ and $(a_1, a_2, \ldots, a_r)$ (because we assumed that Theorem 35.1 **(b)** holds for $r = n-1$). As a result, we obtain

$$\begin{aligned}
&\left(f_2 * f_3 * \cdots * f_n\right)\left(b_1 b_2 \cdots b_{n-1}\right) \\
&= \sum_{\sigma \in S_{n-1}} f_2\left(b_{\sigma(1)}\right) f_3\left(b_{\sigma(2)}\right) \cdots f_n\left(b_{\sigma(n-1)}\right) \\
&= \sum_{\sigma \in S_{n,m}} f_2\left(b_{(\pi_m(\sigma))(1)}\right) f_3\left(b_{(\pi_m(\sigma))(2)}\right) \cdots f_n\left(b_{(\pi_m(\sigma))(n-1)}\right) \qquad (450)
\end{aligned}$$

(here, we substituted $\pi_m(\sigma)$ for σ in the sum, because the map $\pi_m : S_{n,m} \to S_{n-1}$ is a bijection). But now,

$$\begin{aligned}
&\underbrace{g}_{=f_2 * f_3 * \cdots * f_n}\left(\underbrace{\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)}_{\substack{=b_1 b_2 \cdots b_{n-1} \\ \text{(by (449))}}}\right) \\
&= \left(f_2 * f_3 * \cdots * f_n\right)\left(b_1 b_2 \cdots b_{n-1}\right) \\
&= \sum_{\sigma \in S_{n,m}} f_2\left(b_{(\pi_m(\sigma))(1)}\right) f_3\left(b_{(\pi_m(\sigma))(2)}\right) \cdots f_n\left(b_{(\pi_m(\sigma))(n-1)}\right). \qquad (451)
\end{aligned}$$

Now, let $\sigma \in S_{n,m}$. Let $i \in \{1, 2, \ldots, n-1\}$ be arbitrary. The definition of π_m yields $\pi_m(\sigma) = \operatorname{del}_m \sigma$. Hence,

$$\left(\underbrace{\pi_m(\sigma)}_{=\operatorname{del}_m \sigma}\right)(i) = \left(\operatorname{del}_m \sigma\right)(i) = \omega\left(\sigma\left(i+1\right)\right) \qquad \text{(by the definition of } \operatorname{del}_m \sigma\text{)}.$$

Thus,

$$\begin{aligned}
b_{(\pi_m(\sigma))(i)} &= b_{\omega(\sigma(i+1))} = a_{\eta(\omega(\sigma(i+1)))} \qquad \left(\text{by the definition of } b_{\omega(\sigma(i+1))}\right) \\
&= a_{\sigma(i+1)}
\end{aligned}$$

(since $\eta\left(\omega\left(\sigma\left(i+1\right)\right)\right) = \underbrace{\left(\eta \circ \omega\right)}_{\substack{=\mathrm{id} \\ \text{(since the maps } \eta \text{ and } \omega \\ \text{are mutually inverse)}}}\left(\sigma\left(i+1\right)\right) = \mathrm{id}\left(\sigma\left(i+1\right)\right) = \sigma\left(i+1\right)$).

Hence, $f_{i+1}\left(\underbrace{b_{(\pi_m(\sigma))(i)}}_{=a_{\sigma(i+1)}}\right) = f_{i+1}\left(a_{\sigma(i+1)}\right)$.

Now, forget that we fixed i. We thus have proven the equality $f_{i+1}\left(b_{(\pi_m(\sigma))(i)}\right) = f_{i+1}\left(a_{\sigma(i+1)}\right)$ for every $i \in \{1, 2, \ldots, n-1\}$. Taking the product of these equalities over all $i \in \{1, 2, \ldots, n\}$, we obtain

$$\begin{aligned}
&f_{1+1}\left(b_{(\pi_m(\sigma))(1)}\right) f_{2+1}\left(b_{(\pi_m(\sigma))(2)}\right) \cdots f_{(n-1)+1}\left(b_{(\pi_m(\sigma))(n-1)}\right) \\
&= f_{1+1}\left(a_{\sigma(1+1)}\right) f_{2+1}\left(a_{\sigma(2+1)}\right) \cdots f_{(n-1)+1}\left(a_{\sigma((n-1)+1)}\right) \\
&= f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right).
\end{aligned}$$

Compared with

$$\begin{aligned}&f_{1+1}\left(b_{(\pi_m(\sigma))(1)}\right) f_{2+1}\left(b_{(\pi_m(\sigma))(2)}\right)\cdots f_{(n-1)+1}\left(b_{(\pi_m(\sigma))(n-1)}\right)\\&= f_2\left(b_{(\pi_m(\sigma))(1)}\right) f_3\left(b_{(\pi_m(\sigma))(2)}\right)\cdots f_n\left(b_{(\pi_m(\sigma))(n-1)}\right),\end{aligned}$$

this yields

$$\begin{aligned}&f_2\left(b_{(\pi_m(\sigma))(1)}\right) f_3\left(b_{(\pi_m(\sigma))(2)}\right)\cdots f_n\left(b_{(\pi_m(\sigma))(n-1)}\right)\\&= f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right)\cdots f_n\left(a_{\sigma(n)}\right).\end{aligned}\tag{452}$$

Now, forget that we fixed σ. We thus have shown that every $\sigma \in S_{n,m}$ satisfies (452). Hence,

$$\begin{aligned}&\sum_{\sigma\in S_{n,m}} \underbrace{f_2\left(b_{(\pi_m(\sigma))(1)}\right) f_3\left(b_{(\pi_m(\sigma))(2)}\right)\cdots f_n\left(b_{(\pi_m(\sigma))(n-1)}\right)}_{\substack{=f_2\left(b_{\sigma(2)}\right) f_3\left(b_{\sigma(3)}\right)\cdots f_n\left(b_{\sigma(n)}\right)\\ \text{(by (452))}}}\\&= \sum_{\sigma\in S_{n,m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right)\cdots f_n\left(a_{\sigma(n)}\right).\end{aligned}\tag{453}$$

Now, let us recall that $S_{n,m} = \{\sigma \in S_n \mid \sigma(1) = m\}$. Hence, we can replace the summation sign "$\sum_{\sigma\in S_{n,m}}$" by a "$\sum_{\substack{\sigma\in S_n;\\ \sigma(1)=m}}$" in $\sum_{\sigma\in S_{n,m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right)\cdots f_n\left(a_{\sigma(n)}\right)$. As a result, we obtain

$$\begin{aligned}&\sum_{\sigma\in S_{n,m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right)\cdots f_n\left(a_{\sigma(n)}\right)\\&= \sum_{\substack{\sigma\in S_n;\\ \sigma(1)=m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right)\cdots f_n\left(a_{\sigma(n)}\right).\end{aligned}\tag{454}$$

Now, (451) becomes

$$\begin{aligned}&g\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_n\right)\right)\\&= \sum_{\sigma\in S_{n,m}} f_2\left(b_{(\pi_m(\sigma))(1)}\right) f_3\left(b_{(\pi_m(\sigma))(2)}\right)\cdots f_n\left(b_{(\pi_m(\sigma))(n-1)}\right)\\&= \sum_{\sigma\in S_{n,m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right)\cdots f_n\left(a_{\sigma(n)}\right) \qquad \text{(by (453))}\\&= \sum_{\substack{\sigma\in S_n;\\ \sigma(1)=m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right)\cdots f_n\left(a_{\sigma(n)}\right) \qquad \text{(by (454))}.\end{aligned}$$

This proves (447).

Now, (446) becomes

$$
\begin{aligned}
&\left(f_1 * f_2 * \cdots * f_n\right)\left(a_1 a_2 \cdots a_n\right) \\
&= \sum_{m=1}^{n} f_1\left(a_m\right) \cdot \underbrace{g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)}_{\substack{= \sum\limits_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\ \text{(by (447))}}} \\
&= \sum_{m=1}^{n} f_1\left(a_m\right) \cdot \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(\underbrace{a_m}_{\substack{=a_{\sigma(1)} \\ \text{(since } m=\sigma(1) \\ \text{(since } \sigma(1)=m))}}\right) f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} \underbrace{f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right)}_{=f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right)} \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).
\end{aligned}
$$

Compared with

$$
\begin{aligned}
&\sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&= \underbrace{\sum_{m \in \{1,2,\ldots,n\}}}_{= \sum\limits_{m=1}^{n}} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&\qquad \text{(since every } \sigma \in S_n \text{ satisfies } \sigma(1) \in \{1,2,\ldots,n\}) \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right),
\end{aligned}
$$

this yields

$$
\left(f_1 * f_2 * \cdots * f_n\right)\left(a_1 a_2 \cdots a_n\right) = \sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).
$$

Now, forget that we fixed k, H, A, $(f_1, f_2, \ldots, f_n)$ and $(a_1, a_2, \ldots, a_n)$. We thus have shown that if k is a field, if H is a k-bialgebra, if A is a k-algebra, if f_1, f_2, …, f_n are n maps in $\mathfrak{g}(H, A)$, then every n elements a_1, a_2, …, a_n of $\operatorname{Prim} H$ satisfy

$$
\left(f_1 * f_2 * \cdots * f_n\right)\left(a_1 a_2 \cdots a_n\right) = \sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).
$$

In other words, we have shown that Theorem 35.1 **(b)** holds for $r = n$. This completes the induction step. The induction proof of Theorem 35.1 **(b)** is thus complete. $\square$

We can obtain some corollaries of Theorem 35.1. By setting f_1, f_2, ..., f_n all equal to each other, we can conclude that the following holds:

Corollary 35.6. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let $f \in \mathfrak{g}(H, A)$.

(a) Every $s \in \{0, 1, \ldots, r-1\}$ and every s elements a_1, a_2, ..., a_s of $\operatorname{Prim} H$ satisfy

$$f^{*r}(a_1 a_2 \cdots a_s) = 0.$$

(b) Every r elements a_1, a_2, ..., a_r of $\operatorname{Prim} H$ satisfy

$$f^{*r}(a_1 a_2 \cdots a_r) = \sum_{\sigma \in S_r} f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right) \cdots f\left(a_{\sigma(r)}\right)$$

(where S_r denotes the r-th symmetric group).

(c) Let a_1, a_2, ..., a_r be r elements of $\operatorname{Prim} H$. If the elements $f(a_1)$, $f(a_2)$, ..., $f(a_r)$ of A commute pairwise, then

$$f^{*r}(a_1 a_2 \cdots a_r) = r! \cdot f(a_1) f(a_2) \cdots f(a_r).$$

The proof of this corollary rests on what we already know along with the following almost trivial fact:

Lemma 35.7. Let k be a field. Let B be a k-algebra. Let $n \in \mathbb{N}$. Let b_1, b_2, ..., b_n be n elements of B which pairwise commute. Let $\sigma \in S_n$. Then,

$$b_{\sigma(1)} b_{\sigma(2)} \cdots b_{\sigma(n)} = b_1 b_2 \cdots b_n.$$

Proof of Lemma 35.7. Let $S = \{b_1, b_2, \ldots, b_n\}$. Then, $S \subseteq B$ (since b_1, b_2, ..., b_n are elements of B). Let A be the k-subalgebra of B generated by S. Then, the k-algebra A is generated by S. In particular, A contains S as a subset. That is, $S \subseteq A$.

Moreover, any two elements of S commute[224]. Thus, Proposition 11.2 yields that the k-algebra A is commutative. Hence, products in the k-algebra A are well-defined without specifying the order of the factors.

Now, every $i \in \{1, 2, \ldots, n\}$ satisfies $b_i \in \{b_1, b_2, \ldots, b_n\} = S \subseteq A$. Hence, $\prod_{i \in \{1,2,\ldots,n\}} b_i$ is a well-defined product in A (it is well-defined since the k-algebra A is commutative). Since $\sigma \in S_n$, we know that σ is a permutation of $\{1, 2, \ldots, n\}$. That is, σ is a bijection $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$. Now,

$$\begin{aligned} b_1 b_2 \cdots b_n &= \prod_{i \in \{1,2,\ldots,n\}} b_i = \prod_{i \in \{1,2,\ldots,n\}} b_{\sigma(i)} \\ &\qquad \left(\begin{array}{c} \text{here, we substituted } i \text{ for } \sigma(i) \text{ in the product,} \\ \text{since the map } \sigma : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} \text{ is a bijection} \end{array} \right) \\ &= b_{\sigma(1)} b_{\sigma(2)} \cdots b_{\sigma(n)}. \end{aligned}$$

This proves Lemma 35.7. $\square$

[224] *Proof.* The elements b_1, b_2, ..., b_n are the elements of S (because $S = \{b_1, b_2, \ldots, b_n\}$). But we also know that the elements b_1, b_2, ..., b_n pairwise commute. Since the elements b_1, b_2, ..., b_n are the elements of S, this rewrites as follows: The elements of S pairwise commute. In other words, any two elements of S commute, qed.

Proof of Corollary 35.6. **(a)** Let $s \in \{0, 1, \ldots, r-1\}$. Let a_1, a_2, ..., a_s be s elements of $\operatorname{Prim} H$. Then,

$$\underbrace{f^{*r}}_{=\underbrace{f * f * \cdots * f}_{r \text{ times}}} (a_1 a_2 \cdots a_s) = \left(\underbrace{f * f * \cdots * f}_{r \text{ times}} \right) (a_1 a_2 \cdots a_s) = 0$$

(by Theorem 35.1 **(a)**, applied to $(f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}} \right)$). This proves Corollary 35.6 **(a)**.

(b) Let a_1, a_2, ..., a_r be r elements of $\operatorname{Prim} H$. Then,

$$\underbrace{f^{*r}}_{=\underbrace{f * f * \cdots * f}_{r \text{ times}}} (a_1 a_2 \cdots a_r) = \left(\underbrace{f * f * \cdots * f}_{r \text{ times}} \right) (a_1 a_2 \cdots a_r)$$

$$= \sum_{\sigma \in S_r} f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right) \cdots f\left(a_{\sigma(r)}\right)$$

(by Theorem 35.1 **(b)**, applied to $(f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}} \right)$). This proves Corollary 35.6 **(b)**.

(c) Let a_1, a_2, ..., a_r be r elements of $\operatorname{Prim} H$. Assume that the elements $f(a_1)$, $f(a_2)$, ..., $f(a_r)$ of A commute pairwise. Thus, for every $\sigma \in S_r$, we have

$$f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right) \cdots f\left(a_{\sigma(r)}\right) = f(a_1) f(a_2) \cdots f(a_r) \tag{455}$$

(by Lemma 35.7, applied to $n = r$, $B = A$ and $b_i = f(a_i)$). Now, Corollary 35.6 **(b)** yields

$$\begin{aligned} f^{*r}(a_1 a_2 \cdots a_r) &= \sum_{\sigma \in S_r} \underbrace{f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right) \cdots f\left(a_{\sigma(r)}\right)}_{\substack{= f(a_1) f(a_2) \cdots f(a_r) \\ \text{(by (455))}}} \\ &= \sum_{\sigma \in S_r} f(a_1) f(a_2) \cdots f(a_r) = \underbrace{|S_r|}_{=r!} \cdot f(a_1) f(a_2) \cdots f(a_r) \\ &= r! \cdot f(a_1) f(a_2) \cdots f(a_r). \end{aligned}$$

This proves Corollary 35.6 **(c)**. □

We can apply Corollary 35.6 to the Eulerian idempotent:

Corollary 35.8. Let k be a field of characteristic 0. Let H be a connected filtered bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$.

(a) Every $s \in \{0, 1, \ldots, r-1\}$ and every s elements a_1, a_2, ..., a_s of $\operatorname{Prim} H$ satisfy

$$(\operatorname{Log} \mathrm{id})^{*r}(a_1 a_2 \cdots a_s) = 0.$$

(b) Every r elements a_1, a_2, ..., a_r of $\operatorname{Prim} H$ satisfy

$$(\operatorname{Log} \mathrm{id})^{*r}(a_1 a_2 \cdots a_r) = \sum_{\sigma \in S_r} a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(r)}$$

(where S_r denotes the r-th symmetric group).

Proof of Corollary 35.8. We know that $\operatorname{Log} F \in \mathfrak{g}(H, H)$ for every $F \in G(H, H)$ (this follows from the definition of Log). Applying this to $F = \mathrm{id}$, we obtain $\operatorname{Log} \mathrm{id} \in \mathfrak{g}(H, H)$. Thus, Corollary 35.8 **(a)** follows from Corollary 35.6 **(a)** (applied to $A = H$ and $f = \operatorname{Log} \mathrm{id}$).

(b) We know that H is a bialgebra, and thus a unital coalgebra. Proposition 6.2 **(c)** (applied to $A = H$ and $F = \mathrm{id}$) shows that $(\operatorname{Log} \mathrm{id})\,|_{\operatorname{Prim} H} = \mathrm{id}\,|_{\operatorname{Prim} H}$. Thus, for every $u \in \operatorname{Prim} H$, we have

$$(\operatorname{Log} \mathrm{id})(u) = \left(\underbrace{(\operatorname{Log} \mathrm{id})\,|_{\operatorname{Prim} H}}_{= \mathrm{id}|_{\operatorname{Prim} H}} \right)(u) = (\mathrm{id}\,|_{\operatorname{Prim} H})(u) = \mathrm{id}(u) = u.$$

Hence,

$$(\operatorname{Log} \mathrm{id})(u) = u \qquad \text{for every } u \in \operatorname{Prim} H. \tag{456}$$

Now, let a_1, a_2, ..., a_r be r elements of $\operatorname{Prim} H$. Let $\sigma \in S_r$. Every $i \in \{1, 2, \ldots, r\}$ satisfies $a_{\sigma(i)} \in \operatorname{Prim} H$. Hence, every $i \in \{1, 2, \ldots, r\}$ satisfies $(\operatorname{Log} \mathrm{id})\left(a_{\sigma(i)}\right) = a_{\sigma(i)}$ (by (456), applied to $u = a_{\sigma(i)}$). Multiplying these equalities over all $i \in \{1, 2, \ldots, r\}$, we obtain

$$(\operatorname{Log} \mathrm{id})\left(a_{\sigma(1)}\right) \cdot (\operatorname{Log} \mathrm{id})\left(a_{\sigma(2)}\right) \cdot \cdots \cdot (\operatorname{Log} \mathrm{id})\left(a_{\sigma(r)}\right) = a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(r)}. \tag{457}$$

Now, forget that we fixed σ. We thus have shown that (457) holds for every $\sigma \in S_r$. Now, Corollary 35.6 **(b)** (applied to $A = H$ and $f = \operatorname{Log} \mathrm{id}$) yields

$$\begin{aligned}(\operatorname{Log} \mathrm{id})^{*r}(a_1 a_2 \cdots a_r) &= \sum_{\sigma \in S_r} \underbrace{(\operatorname{Log} \mathrm{id})\left(a_{\sigma(1)}\right) \cdot (\operatorname{Log} \mathrm{id})\left(a_{\sigma(2)}\right) \cdot \cdots \cdot (\operatorname{Log} \mathrm{id})\left(a_{\sigma(r)}\right)}_{\substack{= a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(r)} \\ \text{(by (457))}}} \\ &= \sum_{\sigma \in S_r} a_{\sigma(1)} a_{\sigma(2)} \cdots a_{\sigma(r)}.\end{aligned}$$

This proves Corollary 35.8 **(b)**. □

We record a further particular case of Theorem 35.1:

Corollary 35.9. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let f_1, f_2, ..., f_r be r maps in $\mathfrak{g}(H, A)$. Let $a \in \operatorname{Prim} H$.

(a) Every $s \in \{0, 1, \ldots, r-1\}$ satisfies

$$(f_1 * f_2 * \cdots * f_r)(a^s) = 0.$$

(b) We have

$$(f_1 * f_2 * \cdots * f_r)(a^r) = r! \cdot f_1(a) f_2(a) \cdots f_r(a).$$

Proof of Corollary 35.9. **(a)** Let $s \in \{0, 1, \ldots, r-1\}$. We have

$$(f_1 * f_2 * \cdots * f_r)\left(\begin{array}{c}\underbrace{a^s}_{=\underbrace{aa\cdots a}_{s \text{ times}}}\end{array}\right) = (f_1 * f_2 * \cdots * f_r)\left(\underbrace{aa\cdots a}_{s \text{ times}}\right) = 0$$

(by Theorem 35.1 **(a)**, applied to $(a_1, a_2, \ldots, a_s) = \left(\underbrace{a, a, \ldots, a}_{s \text{ times}}\right)$). This proves Corollary 35.9 **(a)**.

(b) We have

$$\begin{aligned}(f_1 * f_2 * \cdots * f_r)\left(\begin{array}{c}\underbrace{a^r}_{=\underbrace{aa\cdots a}_{r \text{ times}}}\end{array}\right) &= (f_1 * f_2 * \cdots * f_r)\left(\underbrace{aa\cdots a}_{r \text{ times}}\right) \\ &= \sum_{\sigma \in S_r} f_1(a) f_2(a) \cdots f_r(a) \\ &\qquad \left(\begin{array}{c}\text{by Theorem 35.1 } \mathbf{(b)}\text{, applied to} \\ (a_1, a_2, \ldots, a_r) = \left(\underbrace{a, a, \ldots, a}_{r \text{ times}}\right)\end{array}\right) \\ &= \underbrace{|S_r|}_{=r!} \cdot f_1(a) f_2(a) \cdots f_r(a) = r! \cdot f_1(a) f_2(a) \cdots f_r(a).\end{aligned}$$

This proves Corollary 35.9 **(b)**. □

A further particular case involves only one map and only one primitive element:

Corollary 35.10. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let $f \in \mathfrak{g}(H, A)$. Let $a \in \operatorname{Prim} H$.

(a) Every $s \in \{0, 1, \ldots, r-1\}$ satisfies

$$f^{*r}(a^s) = 0.$$

(b) We have

$$f^{*r}(a^r) = r! \cdot (f(a))^r.$$

Proof of Corollary 35.10. **(b)** Let $s \in \{0, 1, \ldots, r-1\}$. We have

$$\underbrace{f^{*r}}_{=\underbrace{f * f * \cdots * f}_{r \text{ times}}}(a^s) = \left(\underbrace{f * f * \cdots * f}_{r \text{ times}}\right)(a^s) = 0$$

(by Corollary 35.9 **(a)**, applied to $(f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}}\right)$). This proves Corollary 35.10 **(a)**.

(b) We have

$$\underbrace{f^{*r}}_{=\underbrace{f * f * \cdots * f}_{r \text{ times}}}(a^r) = \left(\underbrace{f * f * \cdots * f}_{r \text{ times}}\right)(a^r) = r! \cdot \underbrace{\underbrace{f(a) f(a) \cdots f(a)}_{r \text{ times}}}_{=(f(a))^r}$$

$$= r! \cdot (f(a))^r \left(\begin{array}{c} \text{by Corollary 35.9 } \mathbf{(b)}\text{, applied to} \\ (f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}}\right) \end{array}\right).$$

This proves Corollary 35.10 **(b)**. □

§36. $(\varepsilon, \varepsilon)$-derivations and products

In this section, we are going to prove some results similar to those proven in §35, although not exactly analogous (in particular, they will need new proofs). However, before we start, let us record a really simple property of unital coalgebras:

Proposition 36.1. Let k be a field. Let H be a unital coalgebra. Let $x \in \operatorname{Ker}(\varepsilon_H)$. Then,

$$\Delta(x) \in x \otimes 1_H + 1_H \otimes x + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H)).$$

Proof of Proposition 36.1. The element $\Delta(x)$ is a tensor in $H \otimes H$. Hence, we can write $\Delta(x)$ in the form $\Delta(x) = \sum_{i=1}^{n} \lambda_i a_i \otimes b_i$ for some $n \in \mathbb{N}$, some elements λ_1, λ_2, …, λ_n of k, some elements a_1, a_2, …, a_n of H, and some elements b_1, b_2, …, b_n of H. Consider this n, these λ_1, λ_2, …, λ_n, these a_1, a_2, …, a_n, and these b_1, b_2, …, b_n.

From $x = \operatorname{Ker}(\varepsilon_H)$, we obtain $\varepsilon_H(x) = 0$. Thus, $\underbrace{\varepsilon}_{=\varepsilon_H}(x) = \varepsilon_H(x) = 0$.

It is now easy to see that $\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i = x$ [225] and $\sum_{i=1}^{n} \lambda_i \varepsilon(a_i) b_i = x$ [226]. Also,

[225] *Proof.* Let $\operatorname{kan} : H \to H \otimes k$ be the canonical isomorphism which sends every $y \in H$ to $y \otimes 1$. Then, by the axioms of a coalgebra, we have $(\operatorname{id} \otimes \varepsilon_H) \circ \Delta_H = \operatorname{kan}$ (since H is a coalgebra). Now,

$$\begin{aligned}
((\operatorname{id} \otimes \varepsilon_H) \circ \Delta_H)(x) &= (\operatorname{id} \otimes \varepsilon_H) \left(\underbrace{\Delta_H(x)}_{=\Delta(x)=\sum_{i=1}^{n} \lambda_i a_i \otimes b_i} \right) = (\operatorname{id} \otimes \varepsilon_H) \left(\sum_{i=1}^{n} \lambda_i a_i \otimes b_i \right) \\
&= \sum_{i=1}^{n} \lambda_i \underbrace{(\operatorname{id} \otimes \varepsilon_H)(a_i \otimes b_i)}_{=\operatorname{id}(a_i) \otimes \varepsilon_H(b_i)} \qquad \text{(since the map } \operatorname{id} \otimes \varepsilon_H \text{ is } k\text{-linear)} \\
&= \sum_{i=1}^{n} \lambda_i \underbrace{\operatorname{id}(a_i)}_{=a_i} \otimes \underbrace{\varepsilon_H(b_i)}_{=\varepsilon(b_i)=\varepsilon(b_i)1} = \sum_{i=1}^{n} \lambda_i \underbrace{a_i \otimes \varepsilon(b_i) 1}_{=\varepsilon(b_i) a_i \otimes 1} \\
&= \sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i \otimes 1 = \left(\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i \right) \otimes 1 = \operatorname{kan} \left(\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i \right)
\end{aligned}$$

(since $\operatorname{kan}\left(\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i \right) = \left(\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i \right) \otimes 1$ (by the definition of kan)). Hence,

$$\operatorname{kan} \left(\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i \right) = \left(\underbrace{(\operatorname{id} \otimes \varepsilon_H) \circ \Delta_H}_{=\operatorname{kan}} \right)(x) = \operatorname{kan}(x).$$

Since the map kan is injective (because kan is an isomorphism), this yields $\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i = x$, qed.

[226] *Proof.* Let $\operatorname{kan} : H \to k \otimes H$ be the canonical isomorphism which sends every $y \in H$ to $1 \otimes y$. Then, by the axioms of a coalgebra, we have $(\varepsilon_H \otimes \operatorname{id}) \circ \Delta_H = \operatorname{kan}$ (since H is a coalgebra). Now,

$$\begin{aligned}
((\varepsilon_H \otimes \operatorname{id}) \circ \Delta_H)(x) &= (\varepsilon_H \otimes \operatorname{id}) \left(\underbrace{\Delta_H(x)}_{=\Delta(x)=\sum_{i=1}^{n} \lambda_i a_i \otimes b_i} \right) (\varepsilon_H \otimes \operatorname{id}) \left(\sum_{i=1}^{n} \lambda_i a_i \otimes b_i \right) \\
&= \sum_{i=1}^{n} \lambda_i \underbrace{(\varepsilon_H \otimes \operatorname{id})(a_i \otimes b_i)}_{=\operatorname{id}(a_i) \otimes \varepsilon_H(b_i)} \qquad \text{(since the map } \varepsilon_H \otimes \operatorname{id} \text{ is } k\text{-linear)} \\
&= \sum_{i=1}^{n} \lambda_i \underbrace{\varepsilon_H(a_i)}_{=\varepsilon(a_i)=\varepsilon(a_i)1} \otimes \underbrace{\operatorname{id}(b_i)}_{=b_i} = \sum_{i=1}^{n} \underbrace{\lambda_i \varepsilon(a_i) 1 \otimes b_i}_{=1 \otimes \lambda_i \varepsilon(a_i) b_i} \\
&= \sum_{i=1}^{n} 1 \otimes \lambda_i \varepsilon(a_i) b_i = 1 \otimes \left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i) b_i \right) = \operatorname{kan} \left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i) b_i \right)
\end{aligned}$$

$\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,\varepsilon(b_i) = 0$ [227].

By the axioms of a unital coalgebra, we have $\varepsilon(1_H) = 1$ (since H is a unital coalgebra).

For every $i \in \{1, 2, \ldots, n\}$, define an element a_i' of H by $a_i' = a_i - \varepsilon(a_i)\,1_H$. Then, for every $i \in \{1, 2, \ldots, n\}$, we have $a_i' \in \operatorname{Ker}(\varepsilon_H)$ [228].

For every $i \in \{1, 2, \ldots, n\}$, define an element b_i' of H by $b_i' = b_i - \varepsilon(b_i)\,1_H$. Then, for every $i \in \{1, 2, \ldots, n\}$, we have $b_i' \in \operatorname{Ker}(\varepsilon_H)$ [229]. Also, $\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i' = x$ [230].

(since $\operatorname{kan}\left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i\right) = 1 \otimes \left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i\right)$ (by the definition of kan)). Hence,

$$\operatorname{kan}\left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i\right) = \left(\underbrace{(\varepsilon_H \otimes \mathrm{id}) \circ \Delta_H}_{=\operatorname{kan}}\right)(x) = \operatorname{kan}(x).$$

Since the map kan is injective (because kan is an isomorphism), this yields $\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i = x$, qed.

[227] *Proof.* We know that $\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i = x$. Applying the map ε to this equality, we obtain $\varepsilon\left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i\right) = \varepsilon(x) = 0$. Hence,

$$0 = \varepsilon\left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i\right) = \sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,\varepsilon(b_i) \qquad \text{(since the map } \varepsilon \text{ is } k\text{-linear)},$$

qed.

[228] *Proof.* Let $i \in \{1, 2, \ldots, n\}$. Applying the map ε to the equality $a_i' = a_i - \varepsilon(a_i)\,1_H$, we obtain

$$\begin{aligned}\varepsilon(a_i') &= \varepsilon(a_i - \varepsilon(a_i)\,1_H) = \varepsilon(a_i) - \varepsilon(a_i)\,\underbrace{\varepsilon(1_H)}_{=1} \qquad \text{(since the map } \varepsilon \text{ is } k\text{-linear)} \\ &= \varepsilon(a_i) - \varepsilon(a_i) = 0,\end{aligned}$$

so that $a_i' \in \operatorname{Ker}\underbrace{\varepsilon}_{=\varepsilon_H} = \operatorname{Ker}(\varepsilon_H)$, qed.

[229] *Proof.* Let $i \in \{1, 2, \ldots, n\}$. Applying the map ε to the equality $b_i' = b_i - \varepsilon(b_i)\,1_H$, we obtain

$$\begin{aligned}\varepsilon(b_i') &= \varepsilon(b_i - \varepsilon(b_i)\,1_H) = \varepsilon(b_i) - \varepsilon(b_i)\,\underbrace{\varepsilon(1_H)}_{=1} \qquad \text{(since the map } \varepsilon \text{ is } k\text{-linear)} \\ &= \varepsilon(b_i) - \varepsilon(b_i) = 0,\end{aligned}$$

so that $b_i' \in \operatorname{Ker}\underbrace{\varepsilon}_{=\varepsilon_H} = \operatorname{Ker}(\varepsilon_H)$, qed.

[230] *Proof.* We have

$$\begin{aligned}\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,\underbrace{b_i'}_{=b_i - \varepsilon(b_i)1_H} &= \sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,(b_i - \varepsilon(b_i)\,1_H) = \underbrace{\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,b_i}_{=x} - \underbrace{\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,\varepsilon(b_i)\,1_H}_{=\left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\varepsilon(b_i)\right)1_H} \\ &= x - \underbrace{\left(\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\,\varepsilon(b_i)\right)}_{=0} 1_H = x - \underbrace{0 \cdot 1_H}_{=0} = x,\end{aligned}$$

Now,

$$\begin{aligned}
\Delta(x) &= \sum_{i=1}^{n} \lambda_i a_i \otimes \underbrace{b_i}_{\substack{=b_i'+\varepsilon(b_i)1_H \\ (\text{since } b_i'=b_i-\varepsilon(b_i)1_H)}} = \sum_{i=1}^{n} \lambda_i \underbrace{a_i \otimes \left(b_i' + \varepsilon(b_i)\, 1_H\right)}_{=a_i\otimes b_i'+\varepsilon(b_i)a_i\otimes 1_H} \\
&= \sum_{i=1}^{n} \lambda_i \left(a_i \otimes b_i' + \varepsilon(b_i)\, a_i \otimes 1_H\right) \\
&= \sum_{i=1}^{n} \lambda_i \underbrace{a_i}_{\substack{=a_i'+\varepsilon(a_i)1_H \\ (\text{since } a_i'=a_i-\varepsilon(a_i)1_H)}} \otimes b_i' + \underbrace{\sum_{i=1}^{n} \lambda_i \varepsilon(b_i)\, a_i \otimes 1_H}_{=\left(\sum_{i=1}^{n} \lambda_i \varepsilon(b_i) a_i\right)\otimes 1_H} \\
&= \sum_{i=1}^{n} \lambda_i \underbrace{\left(a_i' + \varepsilon(a_i)\, 1_H\right) \otimes b_i'}_{=a_i'\otimes b_i'+\varepsilon(a_i)1_H\otimes b_i'} + \underbrace{\left(\sum_{i=1}^{n} \lambda_i \varepsilon(b_i)\, a_i\right)}_{=x} \otimes 1_H \\
&= \underbrace{\sum_{i=1}^{n} \lambda_i \left(a_i' \otimes b_i' + \varepsilon(a_i)\, 1_H \otimes b_i'\right)}_{=\sum_{i=1}^{n} \lambda_i a_i'\otimes b_i' + \sum_{i=1}^{n} \lambda_i \varepsilon(a_i) 1_H \otimes b_i'} + x \otimes 1_H \\
&= \sum_{i=1}^{n} \lambda_i \underbrace{a_i'}_{\in \operatorname{Ker}(\varepsilon_H)} \otimes \underbrace{b_i'}_{\in \operatorname{Ker}(\varepsilon_H)} + \underbrace{\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\, 1_H \otimes b_i'}_{=1_H \otimes \sum_{i=1}^{n} \lambda_i \varepsilon(a_i) b_i'} + x \otimes 1_H \\
&\in \underbrace{\sum_{i=1}^{n} \lambda_i \left(\operatorname{Ker}(\varepsilon_H)\right) \otimes \left(\operatorname{Ker}(\varepsilon_H)\right)}_{\substack{\subseteq (\operatorname{Ker}(\varepsilon_H))\otimes(\operatorname{Ker}(\varepsilon_H)) \\ (\text{since } (\operatorname{Ker}(\varepsilon_H))\otimes(\operatorname{Ker}(\varepsilon_H)) \text{ is} \\ \text{a } k\text{-vector space})}} + 1_H \otimes \underbrace{\sum_{i=1}^{n} \lambda_i \varepsilon(a_i)\, b_i'}_{=x} + x \otimes 1_H \\
&\subseteq \left(\operatorname{Ker}(\varepsilon_H)\right) \otimes \left(\operatorname{Ker}(\varepsilon_H)\right) + 1_H \otimes x + x \otimes 1_H \\
&= x \otimes 1_H + 1_H \otimes x + \left(\operatorname{Ker}(\varepsilon_H)\right) \otimes \left(\operatorname{Ker}(\varepsilon_H)\right).
\end{aligned}$$

This proves Proposition 36.1. □

The following theorem is similar to Theorem 35.1:

Theorem 36.2. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let f_1, f_2, …, f_r be r elements of $\mathcal{L}(H, A)$ such that f_1, f_2, …, f_r are $(\varepsilon_H, \varepsilon_H)$-derivations.

(a) Every $s \in \mathbb{N}$ and every s elements a_1, a_2, …, a_s of $\operatorname{Ker}(\varepsilon_H)$ such that $s > r$ satisfy

$$(f_1 * f_2 * \cdots * f_r)(a_1 a_2 \cdots a_s) = 0.$$

qed.

(b) Every r elements a_1, a_2, ..., a_r of $\operatorname{Ker}(\varepsilon_H)$ satisfy

$$(f_1 * f_2 * \cdots * f_r)(a_1 a_2 \cdots a_r) = \sum_{\sigma \in S_r} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_r\left(a_{\sigma(r)}\right)$$

(where S_r denotes the r-th symmetric group).

We prepare for the proof of this theorem by showing a fact resembling of Lemma 35.2:

Lemma 36.3. Let k be a field. Let H be a k-bialgebra. Let $s \in \mathbb{N}$. Let a_1, a_2, ..., a_s be s elements of $\operatorname{Ker}(\varepsilon_H)$. Then,

$$\Delta(a_1 a_2 \cdots a_s) \in \sum_{m=1}^{s} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_s)) + (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + H \otimes (\operatorname{Ker}(\varepsilon_H))^s$$

231

Proof of Lemma 36.3. Let us first notice that $\operatorname{Ker}(\varepsilon_H)$ is the kernel of ε_H. Thus, $\operatorname{Ker}(\varepsilon_H)$ is the kernel of an algebra homomorphism (since ε_H is an algebra homomorphism). Thus, $\operatorname{Ker}(\varepsilon_H)$ is an ideal of H (since a kernel of an algebra homomorphism is always an ideal).

We will prove that every $r \in \{0, 1, \ldots, s\}$ satisfies

$$\Delta(a_1 a_2 \cdots a_r) \in \sum_{m=1}^{r} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_r)) + 1_H \otimes (a_1 a_2 \cdots a_r) + (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^r. \tag{458}$$

Proof of (458): We will prove (458) by induction over r:

Induction base: Let $r = 0$. Then, $a_1 a_2 \cdots a_r = a_1 a_2 \cdots a_0 = (\text{empty product}) = 1_H$. Also, from $r = 0$, we obtain $(\operatorname{Ker}(\varepsilon_H))^r = (\operatorname{Ker}(\varepsilon_H))^0 = k \cdot 1_H \ni 1_H$, so that $1_H \in (\operatorname{Ker}(\varepsilon_H))^r$. Now,

$$\begin{aligned}
\Delta\left(\underbrace{a_1 a_2 \cdots a_r}_{=1_H}\right) &= \Delta(1_H) = 1_H \otimes \underbrace{1_H}_{=a_1 a_2 \cdots a_r} \qquad \text{(by the axioms of a bialgebra)} \\
&= 1_H \otimes (a_1 a_2 \cdots a_r) \\
&\subseteq \sum_{m=1}^{r} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_r)) + 1_H \otimes (a_1 a_2 \cdots a_r) \\
&\quad + (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^r.
\end{aligned}$$

Thus, (458) is proven in the case when $r = 0$. The induction base is hence complete.

Induction step: Let $R \in \{0, 1, \ldots, s-1\}$. Assume that (458) has been proven for $r = R$. We need to prove (458) for $r = R + 1$.

[231] Recall that $(\operatorname{Ker}(\varepsilon_H))^\ell$ is defined according to Convention 15.2. Hence, $(\operatorname{Ker}(\varepsilon_H))^\ell$ means the ℓ-th power of the subspace $\operatorname{Ker}(\varepsilon_H)$ of the k-algebra H for every $\ell \in \mathbb{N}$.

We know that (458) has been proven for $r = R$. In other words,

$$\Delta(a_1 a_2 \cdots a_R) \in \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_R)) + 1_H \otimes (a_1 a_2 \cdots a_R) + (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^R. \tag{459}$$

Define a k-vector subspace $\mathfrak{R}$ of $H \otimes H$ by

$$\mathfrak{R} = (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^R. \tag{460}$$

Then, (459) becomes

$$\begin{aligned}\Delta(a_1 a_2 \cdots a_R) &\in \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_R)) + 1_H \otimes (a_1 a_2 \cdots a_R) \\ &\quad + \underbrace{(\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^R}_{=\mathfrak{R}} \\ &= \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_R)) + 1_H \otimes (a_1 a_2 \cdots a_R) + \mathfrak{R}.\end{aligned} \tag{461}$$

We have $a_{R+1} \in \operatorname{Ker}(\varepsilon_H)$. Hence, Proposition 36.1 (applied to $x = a_{R+1}$) yields

$$\begin{aligned}\Delta(a_{R+1}) &\in \underbrace{a_{R+1}}_{\in \operatorname{Ker}(\varepsilon_H)} \otimes \underbrace{1_H}_{\in H} + 1_H \otimes a_{R+1} + (\operatorname{Ker}(\varepsilon_H)) \otimes \underbrace{(\operatorname{Ker}(\varepsilon_H))}_{\subseteq H} \qquad (462) \\ &\in (\operatorname{Ker}(\varepsilon_H)) \otimes H + 1_H \otimes a_{R+1} + (\operatorname{Ker}(\varepsilon_H)) \otimes H \\ &= \underbrace{(\operatorname{Ker}(\varepsilon_H)) \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes H}_{\substack{\subseteq (\operatorname{Ker}(\varepsilon_H)) \otimes H \\ \text{(since } (\operatorname{Ker}(\varepsilon_H)) \otimes H \text{ is a } k\text{-vector space)}}} + 1_H \otimes a_{R+1} \\ &\subseteq (\operatorname{Ker}(\varepsilon_H)) \otimes H + 1_H \otimes a_{R+1}. \qquad (463)\end{aligned}$$

Now, let us define a k-vector subspace $\mathfrak{R}'$ of $H \otimes H$ by

$$\mathfrak{R}' = (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^{R+1}. \tag{464}$$

It is easy to see that

$$\begin{aligned}&\left(\sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_R))\right) \cdot \Delta(a_{R+1}) \\ &\in \sum_{m=1}^{R} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_{R+1})) + \mathfrak{R}'.\end{aligned} \tag{465}$$

[232] Also,

$$\begin{aligned}&\left(1_H \otimes \left(a_1 a_2 \cdots a_R\right)\right) \cdot \Delta\left(a_{R+1}\right) \\ &\in a_{R+1} \otimes \left(a_1 a_2 \cdots a_R\right) + 1_H \otimes \left(a_1 a_2 \cdots a_{R+1}\right) + \mathfrak{R}'. \end{aligned} \tag{466}$$

[232] *Proof of (465):* Thus,

$$\begin{aligned}&\left(\sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \underbrace{\Delta\left(a_{R+1}\right)}_{\substack{\in (\operatorname{Ker}(\varepsilon_H)) \otimes H + 1_H \otimes a_{R+1} \\ \text{(by (463))}}} \\ &\in \left(\sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \\ &\qquad \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H + 1_H \otimes a_{R+1}\right) \\ &\subseteq \left(\sum_{m=1}^{R} \underbrace{a_m}_{\in \operatorname{Ker}(\varepsilon_H)} \otimes \left(\underbrace{\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)}_{\in H}\right)\right) \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right) \\ &\qquad + \underbrace{\left(\sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)}_{= \sum_{m=1}^{R} \left(a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)} \\ &\subseteq \underbrace{\left(\sum_{m=1}^{R} \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right)}_{\substack{\subseteq (\operatorname{Ker}(\varepsilon_H)) \otimes H \\ \text{(since } (\operatorname{Ker}(\varepsilon_H)) \otimes H \\ \text{is a } k\text{-vector space)}}} \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right) \\ &\qquad + \sum_{m=1}^{R} \underbrace{\left(a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right)\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)}_{= \left(a_m 1_H\right) \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_R\right) a_{R+1}\right)} \end{aligned}$$

[233] Furthermore,

$$\mathfrak{R} \cdot \Delta\left(a_{R+1}\right) \subseteq \mathfrak{R}'. \tag{467}$$

$$\begin{aligned}
&\subseteq \underbrace{\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right) \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right)}_{=\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\cdot\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right)\otimes(H\cdot H)} \\
&\qquad \text{(by Lemma 34.11, applied to } H,\ H,\ \operatorname{Ker}\left(\varepsilon_H\right),\ \operatorname{Ker}\left(\varepsilon_H\right),\ H \text{ and } H \\
&\qquad \text{instead of } U,\ V,\ A,\ C,\ B \text{ and } D) \\
&\qquad + \sum_{m=1}^{R} \underbrace{\left(a_m 1_H\right)}_{=a_m} \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right) \underbrace{\left(a_{m+1} a_{m+2} \cdots a_R\right) a_{R+1}}_{=a_{m+1}a_{m+2}\cdots a_{R+1}} \right) \\
&= \underbrace{\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \cdot \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right)}_{=\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2} \otimes \underbrace{\left(H \cdot H\right)}_{=H} \\
&\qquad + \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&= \underbrace{\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H}_{\substack{\subseteq \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{R+1} \\ = \mathfrak{R}' \\ \text{(by (464))}}} + \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&= \mathfrak{R}' + \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) \\
&= \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) + \mathfrak{R}'.
\end{aligned}$$

This proves (465).

[233] *Proof of (466):* We have

$$\begin{aligned}
&\left(1_H \otimes \left(a_1 a_2 \cdots a_R\right)\right) \cdot \underbrace{\Delta\left(a_{R+1}\right)}_{\substack{\in a_{R+1}\otimes 1_H + 1_H \otimes a_{R+1} + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\otimes\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \\ \text{(by (462))}}} \\
&\in \left(1_H \otimes \left(a_1 a_2 \cdots a_R\right)\right) \cdot \left(a_{R+1} \otimes 1_H + 1_H \otimes a_{R+1} + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right) \\
&\subseteq \underbrace{\left(1_H \otimes \left(a_1 a_2 \cdots a_R\right)\right) \cdot \left(a_{R+1} \otimes 1_H\right)}_{=\left(1_H a_{R+1}\right)\otimes\left(\left(a_1 a_2 \cdots a_R\right) 1_H\right)} \\
&\qquad + \underbrace{\left(1_H \otimes \left(a_1 a_2 \cdots a_R\right)\right) \cdot \left(1_H \otimes a_{R+1}\right)}_{=\left(1_H 1_H\right)\otimes\left(\left(a_1 a_2 \cdots a_R\right) a_{R+1}\right)} \\
&\qquad + \left(\underbrace{1_H}_{\in H} \otimes \underbrace{\left(a_1 a_2 \cdots a_R\right)}_{\substack{\in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^R \\ \text{(since } a_i \in \operatorname{Ker}\left(\varepsilon_H\right) \text{ for} \\ \text{every } i \in \{1,2,\ldots,R\}\text{)}}} \right) \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right) \\
&\subseteq \underbrace{\left(1_H a_{R+1}\right)}_{=a_{R+1}} \otimes \underbrace{\left(\left(a_1 a_2 \cdots a_R\right) 1_H\right)}_{=a_1 a_2 \cdots a_R} \\
&\qquad + \underbrace{\left(1_H 1_H\right)}_{=1_H} \otimes \underbrace{\left(\left(a_1 a_2 \cdots a_R\right) a_{R+1}\right)}_{=a_1 a_2 \cdots a_{R+1}} \\
&\qquad + \underbrace{\left(H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^R\right) \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right)}_{=\left(H\cdot\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right)\otimes\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^R\cdot\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right)} \\
&\qquad \text{(by Lemma 34.11, applied to } H,\ H,\ H,\ \operatorname{Ker}\left(\varepsilon_H\right),\ \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^R \text{ and } \operatorname{Ker}\left(\varepsilon_H\right) \\
&\qquad \text{instead of } U,\ V,\ A,\ C,\ B \text{ and } D)
\end{aligned}$$

$$
\begin{aligned}
&= a_{R+1} \otimes (a_1 a_2 \cdots a_R) \\
&\qquad + 1_H \otimes (a_1 a_2 \cdots a_{R+1}) \\
&\qquad + (H \cdot (\operatorname{Ker}(\varepsilon_H))) \otimes \left((\operatorname{Ker}(\varepsilon_H))^R \cdot (\operatorname{Ker}(\varepsilon_H)) \right) \\
&= a_{R+1} \otimes (a_1 a_2 \cdots a_R) + 1_H \otimes (a_1 a_2 \cdots a_{R+1}) + \underbrace{(H \cdot (\operatorname{Ker}(\varepsilon_H)))}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_H) \\ \text{(since } \operatorname{Ker}(\varepsilon_H) \text{ is an ideal of } H\text{)}}} \otimes \underbrace{\left((\operatorname{Ker}(\varepsilon_H))^R \cdot (\operatorname{Ker}(\varepsilon_H)) \right)}_{= (\operatorname{Ker}(\varepsilon_H))^{R+1}} \\
&\subseteq a_{R+1} \otimes (a_1 a_2 \cdots a_R) + 1_H \otimes (a_1 a_2 \cdots a_{R+1}) + \underbrace{(\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^{R+1}}_{\substack{\subseteq (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^{R+1} \\ = \mathfrak{R}' \\ \text{(by (464))}}} \\
&\subseteq a_{R+1} \otimes (a_1 a_2 \cdots a_R) + 1_H \otimes (a_1 a_2 \cdots a_{R+1}) + \mathfrak{R}',
\end{aligned}
$$

so that (466) is proven.

[234] *Proof of (467):* We have

$$
(\operatorname{Ker}(\varepsilon_H))^2 \cdot H = (\operatorname{Ker}(\varepsilon_H)) \cdot \underbrace{(\operatorname{Ker}(\varepsilon_H)) \cdot H}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_H) \\ \text{(since } \operatorname{Ker}(\varepsilon_H) \text{ is} \\ \text{an ideal of } H\text{)}}} \subseteq (\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H)) = (\operatorname{Ker}(\varepsilon_H))^2 .
$$

We have $a_{R+1} \in \operatorname{Ker}(\varepsilon_H)$ (since $a_i \in \operatorname{Ker}(\varepsilon_H)$ for every $i \in \{1, 2, \ldots, s\}$). Now,

$$
\begin{aligned}
&\underbrace{\mathfrak{R}}_{\substack{= (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^R \\ \text{(by (460))}}} \cdot \left(\underbrace{1_H}_{\in H} \otimes \underbrace{a_{R+1}}_{\in \operatorname{Ker}(\varepsilon_H)} \right) \\
&\subseteq \left((\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^R \right) \cdot (H \otimes \operatorname{Ker}(\varepsilon_H)) \\
&\subseteq \underbrace{\left((\operatorname{Ker}(\varepsilon_H))^2 \otimes H \right) \cdot (H \otimes \operatorname{Ker}(\varepsilon_H))}_{\substack{= \left((\operatorname{Ker}(\varepsilon_H))^2 \cdot H \right) \otimes (H \cdot \operatorname{Ker}(\varepsilon_H)) \\ \text{(by Lemma 34.11, applied to } H,\ H,\ (\operatorname{Ker}(\varepsilon_H))^2,\ H,\ H \text{ and } \operatorname{Ker}(\varepsilon_H) \\ \text{instead of } U,\ V,\ A,\ C,\ B \text{ and } D\text{)}}} \\
&\qquad + \underbrace{\left((\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^R \right) \cdot (H \otimes \operatorname{Ker}(\varepsilon_H))}_{\substack{= ((\operatorname{Ker}(\varepsilon_H)) \cdot H) \otimes \left((\operatorname{Ker}(\varepsilon_H))^R \cdot \operatorname{Ker}(\varepsilon_H) \right) \\ \text{(by Lemma 34.11, applied to } H,\ H,\ \operatorname{Ker}(\varepsilon_H),\ H,\ (\operatorname{Ker}(\varepsilon_H))^R \text{ and } \operatorname{Ker}(\varepsilon_H) \\ \text{instead of } U,\ V,\ A,\ C,\ B \text{ and } D\text{)}}} \\
&= \underbrace{\left((\operatorname{Ker}(\varepsilon_H))^2 \cdot H \right)}_{\subseteq (\operatorname{Ker}(\varepsilon_H))^2} \otimes \underbrace{(H \cdot \operatorname{Ker}(\varepsilon_H))}_{\subseteq H} + \underbrace{((\operatorname{Ker}(\varepsilon_H)) \cdot H)}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_H) \\ \text{(since } \operatorname{Ker}(\varepsilon_H) \text{ is an} \\ \text{ideal of } H\text{)}}} \otimes \underbrace{\left((\operatorname{Ker}(\varepsilon_H))^R \cdot \operatorname{Ker}(\varepsilon_H) \right)}_{= (\operatorname{Ker}(\varepsilon_H))^{R+1}} \\
&\subseteq (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^{R+1} = \mathfrak{R}'
\end{aligned} \tag{468}
$$

(by (464)).

We have $(\operatorname{Ker}(\varepsilon_H))^2 = (\operatorname{Ker}(\varepsilon_H)) \cdot \underbrace{(\operatorname{Ker}(\varepsilon_H))}_{\subseteq H} \subseteq (\operatorname{Ker}(\varepsilon_H)) \cdot H \subseteq \operatorname{Ker}(\varepsilon_H)$ (since $\operatorname{Ker}(\varepsilon_H)$ is an

It is also easy to find that

$$\sum_{m=1}^{R+1} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right)$$
$$= \sum_{m=1}^{R} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_{R+1}\right)\right) + a_{R+1} \otimes \left(a_1 a_2 \cdots a_R\right). \tag{469}$$

[235]

Since H is a bialgebra, the comultiplication Δ is a k-algebra homomorphism (by

---

ideal of H). Now, the definition of $\mathfrak{R}$ yields

$$\mathfrak{R} = \underbrace{\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2}_{=\operatorname{Ker}\left(\varepsilon_H\right)} \otimes H + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes \underbrace{\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^R}_{\subseteq H}$$
$$\subseteq \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H \subseteq \left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H$$

(since $\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H$ is a k-vector space). Thus,

$$\begin{aligned}
\mathfrak{R} \cdot & \underbrace{\Delta\left(a_{R+1}\right)}_{\substack{\in (\operatorname{Ker}(\varepsilon_H)) \otimes H + 1_H \otimes a_{R+1} \\ \text{(by (463))}}} \\
& \subseteq \mathfrak{R} \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H + 1_H \otimes a_{R+1}\right) \\
& \subseteq \underbrace{\mathfrak{R}}_{\subseteq (\operatorname{Ker}(\varepsilon_H)) \otimes H} \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right) + \underbrace{\mathfrak{R} \cdot \left(1_H \otimes a_{R+1}\right)}_{\substack{\subseteq \mathfrak{R}' \\ \text{(by (468))}}} \\
& \subseteq \underbrace{\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right) \cdot \left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \otimes H\right)}_{\substack{= ((\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))) \otimes (H \cdot H) \\ \text{(by Lemma 34.11, applied to } H,\ H,\ \operatorname{Ker}(\varepsilon_H),\ \operatorname{Ker}(\varepsilon_H),\ H \text{ and } H \\ \text{instead of } U,\ V,\ A,\ C,\ B \text{ and } D)}} + \mathfrak{R}' \\
& = \underbrace{\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right) \cdot \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\right)}_{=(\operatorname{Ker}(\varepsilon_H))^2} \otimes \underbrace{\left(H \cdot H\right)}_{\subseteq H} + \mathfrak{R}' \\
& \subseteq \underbrace{\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H}_{\substack{\subseteq (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + (\operatorname{Ker}(\varepsilon_H)) \otimes (\operatorname{Ker}(\varepsilon_H))^{R+1} = \mathfrak{R}' \\ \text{(by (464))}}} + \mathfrak{R}' \subseteq \mathfrak{R}' + \mathfrak{R}' \subseteq \mathfrak{R}'
\end{aligned}$$

(since $\mathfrak{R}'$ is a k-vector space). This proves (467).

[235] The proof of this is identical to the proof of (427).

the axioms of a bialgebra). We have

$$
\begin{aligned}
&\Delta\left(\underbrace{a_1a_2\cdots a_{R+1}}_{=(a_1a_2\cdots a_R)a_{R+1}}\right)\\
&=\Delta\left(\left(a_1a_2\cdots a_R\right)a_{R+1}\right)\\
&=\underbrace{\Delta\left(a_1a_2\cdots a_R\right)}_{\in\sum_{m=1}^{R}a_m\otimes((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_R))+1_H\otimes(a_1a_2\cdots a_R)+\mathfrak{R}\atop\text{(by (461))}}\cdot\Delta\left(a_{R+1}\right)\\
&\qquad\text{(since }\Delta\text{ is a }k\text{-algebra homomorphism)}\\
&\in\left(\sum_{m=1}^{R}a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_R\right)\right)+1_H\otimes\left(a_1a_2\cdots a_R\right)+\mathfrak{R}\right)\cdot\Delta\left(a_{R+1}\right)\\
&\subseteq\underbrace{\left(\sum_{m=1}^{R}a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_R\right)\right)\right)\cdot\Delta\left(a_{R+1}\right)}_{\in\sum_{m=1}^{R}a_m\otimes((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_{R+1}))+\mathfrak{R}'\atop\text{(by (465))}}\\
&\qquad+\underbrace{\left(1_H\otimes\left(a_1a_2\cdots a_R\right)\right)\cdot\Delta\left(a_{R+1}\right)}_{=a_{R+1}\otimes(a_1a_2\cdots a_R)+1_H\otimes(a_1a_2\cdots a_{R+1})+\mathfrak{R}'\atop\text{(by (466))}}+\underbrace{\mathfrak{R}\cdot\Delta\left(a_{R+1}\right)}_{\subseteq\mathfrak{R}'\atop\text{(by (467))}}\\
&\subseteq\sum_{m=1}^{R}a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_{R+1}\right)\right)+\mathfrak{R}'\\
&\qquad+a_{R+1}\otimes\left(a_1a_2\cdots a_R\right)+1_H\otimes\left(a_1a_2\cdots a_{R+1}\right)+\mathfrak{R}'+\mathfrak{R}'\\
&\qquad=\underbrace{\sum_{m=1}^{R}a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_{R+1}\right)\right)+a_{R+1}\otimes\left(a_1a_2\cdots a_R\right)}_{=\sum_{m=1}^{R+1}a_m\otimes((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_{R+1}))\atop\text{(by (469))}}\\
&\qquad\qquad+1_H\otimes\left(a_1a_2\cdots a_{R+1}\right)+\underbrace{\mathfrak{R}'+\mathfrak{R}'+\mathfrak{R}'}_{\subseteq\mathfrak{R}'\atop\text{(since }\mathfrak{R}'\text{ is a }k\text{-vector space)}}\\
&\qquad\subseteq\sum_{m=1}^{R+1}a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_{R+1}\right)\right)+1_H\otimes\left(a_1a_2\cdots a_{R+1}\right)\\
&\qquad\qquad+\underbrace{\mathfrak{R}'}_{=(\operatorname{Ker}(\varepsilon_H))^2\otimes H+(\operatorname{Ker}(\varepsilon_H))\otimes(\operatorname{Ker}(\varepsilon_H))^{R+1}\atop\text{(by the definition of }\mathfrak{R}'\text{)}}\\
&\qquad=\sum_{m=1}^{R+1}a_m\otimes\left(\left(a_1a_2\cdots a_{m-1}\right)\left(a_{m+1}a_{m+2}\cdots a_{R+1}\right)\right)+1_H\otimes\left(a_1a_2\cdots a_{R+1}\right)\\
&\qquad\qquad+\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2\otimes H+\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)\otimes\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{R+1}.
\end{aligned}
$$

In other words, (458) holds for $r = R+1$. We have thus proven (458) for $r = R+1$. The induction step is thus complete.

Hence, (458) is proven by induction. Now, applying (458) to $r = s$, we obtain

$$\begin{aligned}
\Delta\left(a_1 a_2 \cdots a_s\right) &\in \sum_{m=1}^{s} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right) + \underbrace{1_H}_{\in H} \otimes \underbrace{\left(a_1 a_2 \cdots a_s\right)}_{\substack{\in (\operatorname{Ker}(\varepsilon_H))^s \\ \text{(since } a_i \in \operatorname{Ker}(\varepsilon_H) \text{ for} \\ \text{every } i \in \{1,2,\ldots,s\}\text{)}}} \\
&\qquad + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + \underbrace{\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)}_{\subseteq H} \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s \\
&\subseteq \sum_{m=1}^{s} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right) + H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s \\
&\qquad + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s \\
&= \sum_{m=1}^{s} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right) \\
&\qquad + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + \underbrace{H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s + H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s}_{\substack{\subseteq H \otimes (\operatorname{Ker}(\varepsilon_H))^s \\ \text{(since } H \otimes (\operatorname{Ker}(\varepsilon_H))^s \text{ is a } k\text{-vector space)}}} \\
&\subseteq \sum_{m=1}^{s} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right) \\
&\qquad + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s .
\end{aligned}$$

This proves Lemma 36.3. □

From Lemma 36.3, we easily conclude the following weaker statement:

Lemma 36.4. Let k be a field. Let H be a k-bialgebra. Let $s \in \mathbb{N}$ be positive. Let a_1, a_2, …, a_s be s elements of $\operatorname{Ker}\left(\varepsilon_H\right)$. Then,

$$\Delta\left(a_1 a_2 \cdots a_s\right) \in H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1} + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s .$$

(Note that we couldn't remove the $H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1}$ term from the right hand side in Lemma 36.4; in fact, if $s = 1$, then we don't have $\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s \subseteq \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1}$, because in this case we have $\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1} = \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^0 = k \cdot 1_H \not\supseteq \operatorname{Ker}\left(\varepsilon_H\right)$.)

Proof of Lemma 36.4. Every $m \in \{1, 2, \ldots, s\}$ satisfies

$$\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right) \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1} \tag{470}$$

[236] Recall that $\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^\ell$ is defined according to Convention 15.2. Hence, $\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^\ell$ means the ℓ-th power of the subspace $\operatorname{Ker}\left(\varepsilon_H\right)$ of the k-algebra H for every $\ell \in \mathbb{N}$.

[237]. Hence,

$$\sum_{m=1}^{s} \underbrace{a_m}_{\in H} \otimes \underbrace{\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right)}_{\substack{\in (\operatorname{Ker}(\varepsilon_H))^{s-1} \\ \text{(by (470))}}} \in \sum_{m=1}^{s} H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1}$$

$$\subseteq H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1} \tag{471}$$

(since $H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1}$ is a k-vector space).

Now, Lemma 36.3 yields

$$\begin{aligned}
\Delta\left(a_1 a_2 \cdots a_s\right) &\in \underbrace{\sum_{m=1}^{s} a_m \otimes \left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_s\right)\right)}_{\in H \otimes (\operatorname{Ker}(\varepsilon_H))^{s-1}} \\
&\quad + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s \\
&\subseteq H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1} + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \otimes H + H \otimes \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s .
\end{aligned}$$

This proves Lemma 36.4. □

We are now ready to prove the following result (more or less equivalent to Theorem 36.2 **(a)**):

Lemma 36.5. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let f_1, f_2, …, f_r be r elements of $\mathcal{L}(H, A)$ such that f_1, f_2, …, f_r are $(\varepsilon_H, \varepsilon_H)$-derivations.

Every $s \in \mathbb{N}$ such that $s > r$ satisfies

$$\left(f_1 * f_2 * \cdots * f_r\right)\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^s\right) = 0.$$

[238]

Proof of Lemma 36.5. We are going to prove Lemma 36.5 by induction over r:

Induction base: If $r = 0$, then Lemma 36.5 is true[239]. Hence, the induction base is complete.

---

[237] *Proof of (470):* Let $m \in \{1, 2, \ldots, s\}$. Then, $a_1 a_2 \cdots a_{m-1} \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{m-1}$ (since $a_i \in \operatorname{Ker}\left(\varepsilon_H\right)$ for all $i \in \{1, 2, \ldots, m-1\}$) and $a_{m+1} a_{m+2} \cdots a_s \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-m}$ (since $a_i \in \operatorname{Ker}\left(\varepsilon_H\right)$ for all $i \in \{m+1, m+2, \ldots, s\}$). Now,

$$\begin{aligned}
&\underbrace{\left(a_1 a_2 \cdots a_{m-1}\right)}_{\in (\operatorname{Ker}(\varepsilon_H))^{m-1}} \underbrace{\left(a_{m+1} a_{m+2} \cdots a_s\right)}_{\in (\operatorname{Ker}(\varepsilon_H))^{s-m}} \in \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{m-1} \cdot \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-m} \\
&\qquad = \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{(m-1)+(s-m)} = \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{s-1} .
\end{aligned}$$

This proves (470).

[238] Recall that $\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{\ell}$ is defined according to Convention 15.2. Hence, $\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^{\ell}$ means the ℓ-th power of the subspace $\operatorname{Ker}\left(\varepsilon_H\right)$ of the k-algebra H for every $\ell \in \mathbb{N}$.

[239] *Proof.* Let $r = 0$. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let f_1, f_2, …, f_0 be 0 elements of $\mathcal{L}(H, A)$ (that is, no elements) such that f_1, f_2, …, f_0 are $(\varepsilon_H, \varepsilon_H)$-derivations. Let $s \in \mathbb{N}$ such that $s > r$. Recall that $\operatorname{Ker}\left(\varepsilon_H\right)$ is an ideal of H (this is proven as in the proof of

Induction step: Let $R \in \mathbb{N}$ be positive. Assume that Lemma 36.5 is proven for $r = R - 1$. We now are going to prove that Lemma 36.5 holds for $r = R$.

Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let f_1, f_2, ..., f_R be R elements of $\mathcal{L}(H, A)$ such that f_1, f_2, ..., f_R are $(\varepsilon_H, \varepsilon_H)$-derivations. Let s be an element of $\mathbb{N}$ such that $s > R$. We are going to show that

$$(f_1 * f_2 * \cdots * f_R)\left((\operatorname{Ker}(\varepsilon_H))^s\right) = 0.$$

We have $s > R \geq 0$, and thus s is positive.

Let $g = f_2 * f_3 * \cdots * f_R$. Then, g is a k-linear map $H \to A$. Let $\ell \in \mathbb{N}$ be such that $\ell > R - 1$. Thus, we can apply Lemma 36.5 to $R - 1$, $(f_2, f_3, \ldots, f_R)$ and ℓ instead of r, $(f_1, f_2, \ldots, f_r)$ and s (since we assumed that Lemma 36.5 is proven for $r = R - 1$). As a result, we obtain $(f_2 * f_3 * \cdots * f_R)\left((\operatorname{Ker}(\varepsilon_H))^\ell\right) = 0$. Thus,

$$\underbrace{g}_{=f_2*f_3*\cdots*f_R}\left((\operatorname{Ker}(\varepsilon_H))^\ell\right) = (f_2 * f_3 * \cdots * f_R)\left((\operatorname{Ker}(\varepsilon_H))^\ell\right) = 0.$$

Now, forget that we fixed ℓ. We thus have proven that

$$g\left((\operatorname{Ker}(\varepsilon_H))^\ell\right) = 0 \qquad \text{for every } \ell \in \mathbb{N} \text{ such that } \ell \geq R - 1. \tag{472}$$

Applying (472) to $\ell = s - 1$, we obtain

$$g\left((\operatorname{Ker}(\varepsilon_H))^{s-1}\right) = 0 \tag{473}$$

(since $\underbrace{s}_{>R} - 1 > R - 1$). But applying (472) to $\ell = s$, we obtain

$$g\left((\operatorname{Ker}(\varepsilon_H))^s\right) = 0 \tag{474}$$

Lemma 36.3). We have $s > r = 0$, so that $(\operatorname{Ker}(\varepsilon_H))^s = \underbrace{(\operatorname{Ker}(\varepsilon_H))^{s-1}}_{\subseteq H} \cdot (\operatorname{Ker}(\varepsilon_H)) \subseteq H \cdot (\operatorname{Ker}(\varepsilon_H)) \subseteq \operatorname{Ker}(\varepsilon_H)$ (since $\operatorname{Ker}(\varepsilon_H)$ is an ideal of H). On the other hand, $r = 0$, so that

$$\begin{aligned} f_1 * f_2 * \cdots * f_r &= f_1 * f_2 * \cdots * f_0 = (\text{empty product in } \mathcal{L}(H, A)) \\ &= e_{H,A} \qquad (\text{since the unity of the } k\text{-algebra } \mathcal{L}(H, A) \text{ is } e_{H,A}) \\ &= \eta_A \circ \varepsilon_H \qquad (\text{by the definition of } \varepsilon_H), \end{aligned}$$

so that

$$\begin{aligned} \left(\underbrace{f_1 * f_2 * \cdots * f_r}_{=\eta_A \circ \varepsilon_H}\right)\left(\underbrace{(\operatorname{Ker}(\varepsilon_H))^s}_{\subseteq \operatorname{Ker}(\varepsilon_H)}\right) &\subseteq (\eta_A \circ \varepsilon_H)(\operatorname{Ker}(\varepsilon_H)) \\ &= \eta_A\left(\underbrace{\varepsilon_H(\operatorname{Ker}(\varepsilon_H))}_{\substack{=0 \\ (\text{by the definition of a kernel})}}\right) = \eta_A(0) = 0 \end{aligned}$$

(since the map η_A is k-linear). Hence, $(f_1 * f_2 * \cdots * f_r)\left((\operatorname{Ker}(\varepsilon_H))^s\right) = 0$. Thus, Lemma 36.5 is proven under the assumption that $r = 0$, qed.

(since $s > R > R-1$).

We know that f_1 is an $(\varepsilon_H, \varepsilon_H)$-derivation. But the axioms of a k-bialgebra yield that ε_H is a k-algebra homomorphism (since H is a k-bialgebra). Hence, Theorem 15.9 (applied to $f = f_1$) yields that f_1 is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $f_1\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$. Thus, $f_1\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$ (since we know that f_1 is an $(\varepsilon_H, \varepsilon_H)$-derivation). Hence,

$$f_1\left(\underbrace{\left(\operatorname{Ker}(\varepsilon_H)\right)^2}_{\subseteq \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H}\right) \subseteq f_1\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0,$$

so that $f_1\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2\right) = 0$. Moreover,

$$f_1\left(\underbrace{1_H}_{\in k \cdot 1_H \subseteq \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H}\right) \in f_1\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0,$$

so that $f_1(1_H) = 0$.

Now, let a_1, a_2, ..., a_s be s elements of $\operatorname{Ker}(\varepsilon_H)$. We are going to prove that $(f_1 * f_2 * \cdots * f_R)(a_1 a_2 \cdots a_s) = 0$. First, we have

$$\begin{aligned}
&(f_1 \otimes g)\left(\underbrace{\Delta(a_1 a_2 \cdots a_s)}_{\substack{\in H \otimes \left(\operatorname{Ker}(\varepsilon_H)\right)^{s-1} + \left(\operatorname{Ker}(\varepsilon_H)\right)^2 \otimes H + H \otimes \left(\operatorname{Ker}(\varepsilon_H)\right)^s \\ \text{(by Lemma 36.4)}}}\right) \\
&\in \underbrace{(f_1 \otimes g)\left(H \otimes \left(\operatorname{Ker}(\varepsilon_H)\right)^{s-1}\right)}_{\subseteq f_1(H) \otimes g\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^{s-1}\right)} + \underbrace{(f_1 \otimes g)\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 \otimes H\right)}_{\subseteq f_1\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2\right) \otimes g(H)} + \underbrace{(f_1 \otimes g)\left(H \otimes \left(\operatorname{Ker}(\varepsilon_H)\right)^s\right)}_{\subseteq f_1(H) \otimes g\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^s\right)} \\
&\subseteq f_1(H) \otimes \underbrace{g\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^{s-1}\right)}_{\substack{=0 \\ \text{(by (473))}}} + \underbrace{f_1\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2\right)}_{=0} \otimes g(H) + f_1(H) \otimes \underbrace{g\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^s\right)}_{\substack{=0 \\ \text{(by (474))}}} \\
&= \underbrace{f_1(H) \otimes 0}_{=0} + \underbrace{0 \otimes g(H)}_{=0} + \underbrace{f_1(H) \otimes 0}_{=0} = 0.
\end{aligned}$$

Thus, $(f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_s)) = 0$. Now, $f_1 * f_2 * \cdots * f_R = f_1 * \underbrace{(f_2 * f_3 * \cdots * f_R)}_{=g} =$ $f_1 * g = \mu \circ (f_1 \otimes g) \circ \Delta$ (by the definition of convolution), so that

$$\begin{aligned}
&\underbrace{(f_1 * f_2 * \cdots * f_R)}_{=\mu \circ (f_1 \otimes g) \circ \Delta}(a_1 a_2 \cdots a_s) \\
&= (\mu \circ (f_1 \otimes g) \circ \Delta)(a_1 a_2 \cdots a_s) = \mu\left(\underbrace{(f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_s))}_{=0}\right) = \mu(0) \\
&= 0 \qquad \text{(since the map } \mu \text{ is } k\text{-linear)}.
\end{aligned}$$

Now, forget that we fixed a_1, a_2, ..., a_s. We thus have shown that whenever a_1, a_2, ..., a_s are s elements of $\operatorname{Ker}(\varepsilon_H)$, we have

$$(f_1 * f_2 * \cdots * f_R)(a_1 a_2 \cdots a_s) = 0. \tag{475}$$

Now, (73) yields

$$\begin{aligned}(\operatorname{Ker}(\varepsilon_H))^s &= \left\langle a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\rangle \\ &= \left\langle \left\{ a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\} \right\rangle.\end{aligned}$$

Applying the map $f_1 * f_2 * \cdots * f_R$ to both sides of this equality, we obtain

$$\begin{aligned}&(f_1 * f_2 * \cdots * f_R)\left((\operatorname{Ker}(\varepsilon_H))^s\right) \\ &= (f_1 * f_2 * \cdots * f_R)\left(\left\langle \left\{ a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\} \right\rangle\right) \\ &= \left\langle \underbrace{(f_1 * f_2 * \cdots * f_R)\left(\left\{ a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\}\right)}_{= \left\{ (f_1 * f_2 * \cdots * f_R)(a_1 a_2 \cdots a_s) \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\}} \right\rangle \\ &\qquad \left(\begin{array}{c} \text{by (165), applied to } H, A, f_1 * f_2 * \cdots * f_R \text{ and} \\ \left\{ a_1 a_2 \cdots a_s \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\} \text{ instead of } M, R, \phi \text{ and } S \end{array} \right) \\ &= \left\langle \left\{ \underbrace{(f_1 * f_2 * \cdots * f_R)(a_1 a_2 \cdots a_s)}_{\substack{=0 \\ \text{(by (475))}}} \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\} \right\rangle \\ &= \left\langle \underbrace{\left\{ 0 \ \mid \ (a_1, a_2, \ldots, a_s) \in (\operatorname{Ker}(\varepsilon_H))^{\times s} \right\}}_{\subseteq 0} \right\rangle \subseteq \langle 0 \rangle = 0.\end{aligned}$$

In other words, $(f_1 * f_2 * \cdots * f_R)\left((\operatorname{Ker}(\varepsilon_H))^s\right) = 0$.

Now, forget that we fixed k, H, A, $(f_1, f_2, \ldots, f_R)$ and s. We thus have shown that if k is a field, if H is a k-bialgebra, if A is a k-algebra, if f_1, f_2, ..., f_R be R elements of $\mathcal{L}(H, A)$ such that f_1, f_2, ..., f_R are $(\varepsilon_H, \varepsilon_H)$-derivations, then every $s \in \mathbb{N}$ satisfying $s > R$ satisfies $(f_1 * f_2 * \cdots * f_R)\left((\operatorname{Ker}(\varepsilon_H))^s\right) = 0$. In other words, we have shown that Lemma 36.5 holds for $r = R$. This completes the induction step. The induction proof of Lemma 36.5 is thus complete. □

We can now proceed to the proof of Theorem 36.2.

Proof of Theorem 36.2. **(a)** Let $s \in \mathbb{N}$ be such that $s > r$. Let a_1, a_2, ..., a_s be s elements of $\operatorname{Ker}(\varepsilon_H)$. Then, $a_1 a_2 \cdots a_s \in (\operatorname{Ker}(\varepsilon_H))^s$ (since $a_i \in \operatorname{Ker}(\varepsilon_H)$ for every $i \in \{1, 2, \ldots, s\}$). Hence,

$$(f_1 * f_2 * \cdots * f_r)\left(\underbrace{a_1 a_2 \cdots a_s}_{\in (\operatorname{Ker}(\varepsilon_H))^s}\right) \in (f_1 * f_2 * \cdots * f_r)\left((\operatorname{Ker}(\varepsilon_H))^s\right) = 0$$

(by Lemma 36.5). Hence, $(f_1 * f_2 * \cdots * f_r)(a_1 a_2 \cdots a_s) = 0$. This proves Theorem 36.2 **(a)**.

(b) We are going to prove Theorem 36.2 **(b)** by induction over r:

Induction base: If $r = 0$, then Theorem 36.2 **(b)** is true[240]. Hence, the induction base is complete.

Induction step: Let $n \in \mathbb{N}$ be positive. Assume that Theorem 36.2 **(b)** is proven for $r = n - 1$. We now are going to prove that Theorem 36.2 **(b)** holds for $r = n$.

Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let f_1, f_2, ..., f_n be n elements of $\mathcal{L}(H, A)$ such that f_1, f_2, ..., f_n are $(\varepsilon_H, \varepsilon_H)$-derivations. Let a_1, a_2, ..., a_n be n elements of $\operatorname{Ker}(\varepsilon_H)$. We will prove that

$$(f_1 * f_2 * \cdots * f_n)(a_1 a_2 \cdots a_n) = \sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).$$

Let $g = f_2 * f_3 * \cdots * f_n$. Then, g is a k-linear map $H \to A$. We have

$$f_1 * f_2 * \cdots * f_n = f_1 * \underbrace{(f_2 * f_3 * \cdots * f_n)}_{=g} = f_1 * g = \mu_A \circ (f_1 \otimes g) \circ \Delta$$

(by the definition of convolution). Hence,

$$\begin{aligned}(f_1 * f_2 * \cdots * f_n)(a_1 a_2 \cdots a_n) &= (\mu_A \circ (f_1 \otimes g) \circ \Delta)(a_1 a_2 \cdots a_n) \\ &= \mu_A((f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_n))). \end{aligned} \tag{476}$$

We are now going to study the term $(f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_n))$ on the right hand side of this.

---

[240] *Proof.* Assume that $r = 0$. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let f_1, f_2, ..., f_0 be 0 elements of $\mathcal{L}(H, A)$ (that is, no elements) such that f_1, f_2, ..., f_0 are $(\varepsilon_H, \varepsilon_H)$-derivations. Let a_1, a_2, ..., a_0 be 0 elements of $\operatorname{Ker}(\varepsilon_H)$ (that is, no elements). Since $r = 0$, we have $S_r = S_0 = \{\mathrm{id}\}$. But since $r = 0$, we have $f_1 * f_2 * \cdots * f_r =$ (empty product with respect to convolution) $= e_{H,A}$. Also, since $r = 0$, we have $a_1 a_2 \cdots a_r =$ (empty product) $= 1_H$. Thus,

$$\begin{aligned}&\underbrace{(f_1 * f_2 * \cdots * f_r)}_{=e_{H,A}}\left(\underbrace{a_1 a_2 \cdots a_r}_{=1_H}\right) \\ &= \underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_H}(1_H) = (\eta_A \circ \varepsilon_H)(1_H) = \eta_A\left(\underbrace{\varepsilon_H(1_H)}_{\substack{=1 \\ (\text{since } H \text{ is a bialgebra})}}\right) = \eta_A(1) \\ &= 1 \cdot 1_A \qquad (\text{by the definition of } \eta_A) \\ &= 1_A\end{aligned}$$

and

$$\underbrace{\sum_{\sigma \in S_r}}_{\substack{= \sum_{\sigma \in \{\mathrm{id}\}} \\ (\text{since } S_r = \{\mathrm{id}\})}} \underbrace{f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_r\left(a_{\sigma(r)}\right)}_{\substack{=(\text{empty product}) \\ (\text{since } r=0)}} = \sum_{\sigma \in \{\mathrm{id}\}} \underbrace{(\text{empty product})}_{=1_A} = \sum_{\sigma \in \{\mathrm{id}\}} 1_A = 1_A.$$

Hence, $(f_1 * f_2 * \cdots * f_r)(a_1 a_2 \cdots a_r) = 1_A = \sum_{\sigma \in S_r} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_r\left(a_{\sigma(r)}\right)$. Hence, Theorem 36.2 **(b)** is true for $r = 0$, qed.

We have

$$(f_1 \otimes g)\left(\begin{array}{c}\underbrace{\Delta(a_1a_2\cdots a_n)}\\ \in \sum_{m=1}^{n} a_m\otimes((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_n))+(\operatorname{Ker}(\varepsilon_H))^2\otimes H+H\otimes(\operatorname{Ker}(\varepsilon_H))^n\\ \text{(by Lemma 36.3, applied to } s{=}n)\end{array}\right)$$

$$\in (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_n)) + (\operatorname{Ker}(\varepsilon_H))^2 \otimes H + H \otimes (\operatorname{Ker}(\varepsilon_H))^n\right)$$

$$\subseteq (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1a_2\cdots a_{m-1})(a_{m+1}a_{m+2}\cdots a_n))\right)$$

$$+ (f_1 \otimes g)\left((\operatorname{Ker}(\varepsilon_H))^2 \otimes H\right) + (f_1 \otimes g)(H \otimes (\operatorname{Ker}(\varepsilon_H))^n). \tag{477}$$

But f_1 is an $(\varepsilon_H, \varepsilon_H)$-derivation. From this, it is easy to conclude that $f_1\left((\operatorname{Ker}(\varepsilon_H))^2\right) = 0$ [241]. Now,

$$(f_1 \otimes g)\left((\operatorname{Ker}(\varepsilon_H))^2 \otimes H\right) \subseteq \underbrace{f_1\left((\operatorname{Ker}(\varepsilon_H))^2\right)}_{=0} \otimes g(H) = 0 \otimes g(H) = 0. \tag{478}$$

Furthermore, $n > n-1$. Hence, Lemma 36.5 (applied to $n-1$, $(f_2, f_3, \ldots, f_n)$ and n instead of r, $(f_1, f_2, \ldots, f_r)$ and s) yields $(f_2 * f_3 * \cdots * f_n)((\operatorname{Ker}(\varepsilon_H))^n) = 0$. Thus,

$$\underbrace{g}_{=f_2*f_3*\cdots*f_n}((\operatorname{Ker}(\varepsilon_H))^n) = (f_2 * f_3 * \cdots * f_n)((\operatorname{Ker}(\varepsilon_H))^n) = 0. \tag{479}$$

Now,

$$(f_1 \otimes g)(H \otimes (\operatorname{Ker}(\varepsilon_H))^n) \subseteq f_1(H) \otimes \underbrace{g((\operatorname{Ker}(\varepsilon_H))^n)}_{=0} = f_1(H) \otimes 0 = 0. \tag{480}$$

[241] *Proof.* The axioms of a k-bialgebra yield that ε_H is a k-algebra homomorphism (since H is a k-bialgebra). Hence, Theorem 15.9 (applied to $f = f_1$) yields that f_1 is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $f_1\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$. Thus, $f_1\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$ (since we know that f_1 is an $(\varepsilon_H, \varepsilon_H)$-derivation). Hence,

$$f_1\left(\underbrace{(\operatorname{Ker}(\varepsilon_H))^2}_{\subseteq(\operatorname{Ker}(\varepsilon_H))^2+k\cdot 1_H}\right) \subseteq f_1\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0,$$

so that $f_1\left((\operatorname{Ker}(\varepsilon_H))^2\right) = 0$, qed.

Now, (477) becomes

$$\begin{aligned}
&(f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_n)) \\
&\in (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right) \\
&\qquad + \underbrace{(f_1 \otimes g)\left((\operatorname{Ker}(\varepsilon_H))^2 \otimes H\right)}_{\substack{\subseteq 0 \\ \text{(by (478))}}} + \underbrace{(f_1 \otimes g)(H \otimes (\operatorname{Ker}(\varepsilon_H))^n)}_{\substack{\subseteq 0 \\ \text{(by (478))}}} \\
&\subseteq (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right) + 0 + 0 \\
&= (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right).
\end{aligned}$$

In other words,

$$\begin{aligned}
&(f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_n)) \\
&= (f_1 \otimes g)\left(\sum_{m=1}^{n} a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right) \\
&= \sum_{m=1}^{n} \underbrace{(f_1 \otimes g)(a_m \otimes ((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n)))}_{= f_1(a_m) \otimes g((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))} \\
&\qquad \text{(since the map } f_1 \otimes g \text{ is } k\text{-linear)} \\
&= \sum_{m=1}^{n} f_1(a_m) \otimes g((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n)). \qquad (481)
\end{aligned}$$

Now, (476) becomes

$$\begin{aligned}
&(f_1 * f_2 * \cdots * f_n)(a_1 a_2 \cdots a_n) \\
&= \mu_A\left(\underbrace{(f_1 \otimes g)(\Delta(a_1 a_2 \cdots a_n))}_{\substack{= \sum_{m=1}^{n} f_1(a_m) \otimes g((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n)) \\ \text{(by (481))}}}\right) \\
&= \mu_A\left(\sum_{m=1}^{n} f_1(a_m) \otimes g((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n))\right) \\
&= \sum_{m=1}^{n} \underbrace{\mu_A(f_1(a_m) \otimes g((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n)))}_{\substack{= f_1(a_m) \cdot g((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n)) \\ \text{(since } \mu_A \text{ is the multiplication map)}}} \\
&\qquad \text{(since the map } \mu_A \text{ is } k\text{-linear)} \\
&= \sum_{m=1}^{n} f_1(a_m) \cdot g((a_1 a_2 \cdots a_{m-1})(a_{m+1} a_{m+2} \cdots a_n)). \qquad (482)
\end{aligned}$$

Now, we are going to show that every $m \in \{1, 2, \ldots, n\}$ satisfies

$$g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right) = \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right). \quad (483)$$

The proof of (483) proceeds exactly as the proof of (447), with the only difference that:

– every appearance of "Prim H" has to be replaced by "Ker (ε_H)";

– every reference to Theorem 35.1 has to be replaced by a reference to Theorem 36.2.

Therefore, (483) is proven.

Now, (482) becomes

$$\begin{aligned}
&\left(f_1 * f_2 * \cdots * f_n\right)\left(a_1 a_2 \cdots a_n\right) \\
&= \sum_{m=1}^{n} f_1\left(a_m\right) \cdot \underbrace{g\left(\left(a_1 a_2 \cdots a_{m-1}\right)\left(a_{m+1} a_{m+2} \cdots a_n\right)\right)}_{\substack{= \sum\limits_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\ \text{(by (483))}}} \\
&= \sum_{m=1}^{n} f_1\left(a_m\right) \cdot \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(\begin{array}{c} \underbrace{a_m}_{=a_{\sigma(1)}} \\ \text{(since } m=\sigma(1) \\ \text{(since } \sigma(1)=m)) \end{array}\right) f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} \underbrace{f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) f_3\left(a_{\sigma(3)}\right) \cdots f_n\left(a_{\sigma(n)}\right)}_{=f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right)} \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).
\end{aligned}$$

Compared with

$$\begin{aligned}
&\sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&= \underbrace{\sum_{m \in \{1,2,\ldots,n\}}}_{= \sum\limits_{m=1}^{n}} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right) \\
&\qquad \text{(since every } \sigma \in S_n \text{ satisfies } \sigma(1) \in \{1, 2, \ldots, n\}) \\
&= \sum_{m=1}^{n} \sum_{\substack{\sigma \in S_n; \\ \sigma(1)=m}} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right),
\end{aligned}$$

this yields

$$(f_1 * f_2 * \cdots * f_n)(a_1 a_2 \cdots a_n) = \sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).$$

Now, forget that we fixed H, A, $(f_1, f_2, \ldots, f_n)$ and $(a_1, a_2, \ldots, a_n)$. We thus have shown that if H is a k-bialgebra, if A is a k-algebra, if f_1, f_2, ..., f_n are n elements of $\mathcal{L}(H, A)$ such that f_1, f_2, ..., f_n are $(\varepsilon_H, \varepsilon_H)$-derivations, then every n elements a_1, a_2, ..., a_n of $\operatorname{Ker}(\varepsilon_H)$ satisfy

$$(f_1 * f_2 * \cdots * f_n)(a_1 a_2 \cdots a_n) = \sum_{\sigma \in S_n} f_1\left(a_{\sigma(1)}\right) f_2\left(a_{\sigma(2)}\right) \cdots f_n\left(a_{\sigma(n)}\right).$$

In other words, we have shown that Theorem 36.2 **(b)** holds for $r = n$. This completes the induction step. The induction proof of Theorem 36.2 **(b)** is thus complete. □

We can obtain some corollaries of Theorem 36.2. By setting f_1, f_2, ..., f_n all equal to each other, we can conclude that the following holds:

Corollary 36.6. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let $f \in \mathcal{L}(H, A)$ be such that f is an $(\varepsilon_H, \varepsilon_H)$-derivation.

(a) Every $s \in \mathbb{N}$ and every s elements a_1, a_2, ..., a_s of $\operatorname{Ker}(\varepsilon_H)$ such that $s > r$ satisfy

$$f^{*r}(a_1 a_2 \cdots a_s) = 0.$$

(b) Every r elements a_1, a_2, ..., a_r of $\operatorname{Ker}(\varepsilon_H)$ satisfy

$$f^{*r}(a_1 a_2 \cdots a_r) = \sum_{\sigma \in S_r} f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right) \cdots f\left(a_{\sigma(r)}\right)$$

(where S_r denotes the r-th symmetric group).

(c) Let a_1, a_2, ..., a_r be r elements of $\operatorname{Ker}(\varepsilon_H)$. If the elements $f(a_1)$, $f(a_2)$, ..., $f(a_r)$ of A commute pairwise, then

$$f^{*r}(a_1 a_2 \cdots a_r) = r! \cdot f(a_1) f(a_2) \cdots f(a_r).$$

Proof of Corollary 36.6. **(a)** Let $s \in \mathbb{N}$ be such that $s > r$. Let a_1, a_2, ..., a_s be s elements of $\operatorname{Ker}(\varepsilon_H)$. Then,

$$\underbrace{f^{*r}}_{=\underbrace{f * f * \cdots * f}_{r \text{ times}}}(a_1 a_2 \cdots a_s) = \left(\underbrace{f * f * \cdots * f}_{r \text{ times}}\right)(a_1 a_2 \cdots a_s) = 0$$

(by Theorem 36.2 **(a)**, applied to $(f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}}\right)$). This proves Corollary 36.6 **(a)**.

(b) Let a_1, a_2, ..., a_r be r elements of $\operatorname{Ker}(\varepsilon_H)$. Then,

$$\underbrace{f^{*r}}_{=\underbrace{f*f*\cdots*f}_{r \text{ times}}}(a_1a_2\cdots a_r) = \left(\underbrace{f*f*\cdots*f}_{r \text{ times}}\right)(a_1a_2\cdots a_r)$$

$$= \sum_{\sigma\in S_r} f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right)\cdots f\left(a_{\sigma(r)}\right)$$

(by Theorem 36.2 **(b)**, applied to $(f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}}\right)$). This proves Corollary 36.6 **(b)**.

(c) Let a_1, a_2, ..., a_r be r elements of $\operatorname{Ker}(\varepsilon_H)$. Assume that the elements $f(a_1)$, $f(a_2)$, ..., $f(a_r)$ of A commute pairwise. Thus, for every $\sigma \in S_n$, we have

$$f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right)\cdots f\left(a_{\sigma(r)}\right) = f(a_1) f(a_2)\cdots f(a_r) \tag{484}$$

(by Lemma 35.7, applied to $n = r$, $B = A$ and $b_i = f(a_i)$). Now, Corollary 36.6 **(b)** yields

$$f^{*r}(a_1a_2\cdots a_r) = \sum_{\sigma\in S_r} \underbrace{f\left(a_{\sigma(1)}\right) f\left(a_{\sigma(2)}\right)\cdots f\left(a_{\sigma(r)}\right)}_{\substack{=f(a_1)f(a_2)\cdots f(a_r) \\ \text{(by (484))}}}$$

$$= \sum_{\sigma\in S_r} f(a_1) f(a_2)\cdots f(a_r) = \underbrace{|S_r|}_{=r!}\cdot f(a_1) f(a_2)\cdots f(a_r)$$

$$= r!\cdot f(a_1) f(a_2)\cdots f(a_r).$$

This proves Corollary 36.6 **(c)**. □

We can apply Corollary 36.6 to the Eulerian idempotent:

Corollary 36.7. Let k be a field of characteristic 0. Let H be a connected filtered commutative bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$.

(a) Every $s \in \mathbb{N}$ and every s elements a_1, a_2, ..., a_s of $\operatorname{Ker}(\varepsilon_H)$ such that $s > r$ satisfy

$$(\operatorname{Log}\operatorname{id})^{*r}(a_1a_2\cdots a_s) = 0.$$

(b) Every r elements a_1, a_2, ..., a_r of $\operatorname{Ker}(\varepsilon_H)$ satisfy

$$(\operatorname{Log}\operatorname{id})^{*r}(a_1a_2\cdots a_r) = r!\cdot(\operatorname{Log}\operatorname{id})(a_1)\cdot(\operatorname{Log}\operatorname{id})(a_2)\cdot\cdots\cdot(\operatorname{Log}\operatorname{id})(a_r).$$

Notice that Corollary 36.7 generalizes an observation made in Example 3.18 of [DPR13].

Proof of Corollary 36.7. Let $f = \operatorname{Log}\operatorname{id}$. Then, f is an $(\varepsilon_H, \varepsilon_H)$-derivation (this was shown in the proof of Theorem 15.10). Hence, Corollary 36.6 **(a)** (applied to $A = H$) yields that every $s \in \mathbb{N}$ and every s elements a_1, a_2, ..., a_s of $\operatorname{Ker}(\varepsilon_H)$ such that $s > r$

satisfy $f^{*r}(a_1 a_2 \cdots a_s) = 0$. Since $f = \operatorname{Log} \mathrm{id}$, this rewrites as follows: Every $s \in \mathbb{N}$ and every s elements a_1, a_2, ..., a_s of $\operatorname{Ker}(\varepsilon_H)$ such that $s > r$ satisfy

$$(\operatorname{Log} \mathrm{id})^{*r}(a_1 a_2 \cdots a_s) = 0.$$

This proves Corollary 36.7 **(a)**.

(b) Let a_1, a_2, ..., a_r be r elements of $\operatorname{Ker}(\varepsilon_H)$. Then, the elements $f(a_1)$, $f(a_2)$, ..., $f(a_r)$ of H commute pairwise (since H is commutative). Therefore, Corollary 36.6 **(b)** (applied to $A = H$) yields that $f^{*r}(a_1 a_2 \cdots a_r) = r! \cdot f(a_1) f(a_2) \cdots f(a_r)$. Since $f = \operatorname{Log} \mathrm{id}$, this rewrites as

$$(\operatorname{Log} \mathrm{id})^{*r}(a_1 a_2 \cdots a_r) = r! \cdot (\operatorname{Log} \mathrm{id})(a_1) \cdot (\operatorname{Log} \mathrm{id})(a_2) \cdot \cdots \cdot (\operatorname{Log} \mathrm{id})(a_r).$$

This proves Corollary 36.7 **(b)**. □

We record a further particular case of Theorem 36.2:

Corollary 36.8. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let f_1, f_2, ..., f_r be r elements of $\mathcal{L}(H, A)$ such that f_1, f_2, ..., f_r are $(\varepsilon_H, \varepsilon_H)$-derivations. Let $a \in \operatorname{Ker}(\varepsilon_H)$.

(a) Every $s \in \mathbb{N}$ such that $s > r$ satisfies

$$(f_1 * f_2 * \cdots * f_r)(a^s) = 0.$$

(b) We have

$$(f_1 * f_2 * \cdots * f_r)(a^r) = r! \cdot f_1(a) f_2(a) \cdots f_r(a).$$

Proof of Corollary 36.8. **(a)** Let $s \in \mathbb{N}$ be such that $s > r$. We have

$$(f_1 * f_2 * \cdots * f_r)\left(\begin{array}{c} \underbrace{a^s}_{=\underbrace{aa\cdots a}_{s \text{ times}}} \end{array}\right) = (f_1 * f_2 * \cdots * f_r)\left(\underbrace{aa\cdots a}_{s \text{ times}}\right) = 0$$

(by Theorem 36.2 **(a)**, applied to $(a_1, a_2, \ldots, a_s) = \left(\underbrace{a, a, \ldots, a}_{s \text{ times}}\right)$). This proves Corollary 36.8 **(a)**.

(b) We have

$$\begin{aligned}(f_1 * f_2 * \cdots * f_r)\left(\begin{array}{c} \underbrace{a^r}_{=\underbrace{aa\cdots a}_{r \text{ times}}} \end{array}\right) &= (f_1 * f_2 * \cdots * f_r)\left(\underbrace{aa\cdots a}_{r \text{ times}}\right) \\ &= \sum_{\sigma \in S_r} f_1(a) f_2(a) \cdots f_r(a) \\ &\qquad \left(\begin{array}{c} \text{by Theorem 36.2 } \mathbf{(b)}\text{, applied to} \\ (a_1, a_2, \ldots, a_r) = \left(\underbrace{a, a, \ldots, a}_{r \text{ times}}\right) \end{array}\right) \\ &= \underbrace{|S_r|}_{=r!} \cdot f_1(a) f_2(a) \cdots f_r(a) = r! \cdot f_1(a) f_2(a) \cdots f_r(a).\end{aligned}$$

This proves Corollary 36.8 **(b)**. □

A further particular case involves only one map and only one element of $\operatorname{Ker}(\varepsilon_H)$:

Corollary 36.9. Let k be a field. Let H be a k-bialgebra. Let A be a k-algebra. Let $r \in \mathbb{N}$. Let $f \in \mathcal{L}(H, A)$ be such that f is an $(\varepsilon_H, \varepsilon_H)$-derivation. Let $a \in \operatorname{Ker}(\varepsilon_H)$.

(a) Every $s \in \mathbb{N}$ such that $s > r$ satisfies

$$f^{*r}(a^s) = 0.$$

(b) We have

$$f^{*r}(a^r) = r! \cdot (f(a))^r.$$

Proof of Corollary 36.9. **(b)** Let $s \in \mathbb{N}$ be such that $s > r$. We have

$$\underbrace{f^{*r}}_{=\underbrace{f * f * \cdots * f}_{r \text{ times}}}(a^s) = \left(\underbrace{f * f * \cdots * f}_{r \text{ times}}\right)(a^s) = 0$$

(by Corollary 36.8 **(a)**, applied to $(f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}}\right)$). This proves Corollary 36.9 **(a)**.

(b) We have

$$\underbrace{f^{*r}}_{=\underbrace{f * f * \cdots * f}_{r \text{ times}}}(a^r) = \left(\underbrace{f * f * \cdots * f}_{r \text{ times}}\right)(a^r) = r! \cdot \underbrace{\underbrace{f(a) f(a) \cdots f(a)}_{r \text{ times}}}_{=(f(a))^r}$$

$$\left(\begin{array}{c}\text{by Corollary 36.8 } \textbf{(b)}\text{, applied to} \\ (f_1, f_2, \ldots, f_r) = \left(\underbrace{f, f, \ldots, f}_{r \text{ times}}\right)\end{array}\right)$$

$$= r! \cdot (f(a))^r.$$

This proves Corollary 36.9 **(b)**. □

§37. An invertibility criterion for coalgebra homomorphisms

We next prove a fact which comes handy when one desires to show that certain coalgebra maps are invertible:

Theorem 37.1. Let k be a field. Let C be a connected filtered k-coalgebra. As we know, C thus becomes a unital coalgebra. Let $f : C \to C$ be a k-coalgebra homomorphism satisfying $f(1_C) = 1_C$. Assume that

$$f(x) = x \qquad \text{for every primitive element } x \text{ of } C. \tag{485}$$

(a) We have $(\mathrm{id}_C - f)^n (C_{\leq n}) = 0$ for every integer $n \geq 1$.

(b) The map f is a k-coalgebra isomorphism.

Note that f is not required to satisfy $f(C_{\leq n}) \subseteq C_{\leq n}$ in Theorem 37.1.

Before we prove Theorem 37.1, we are going to show some lemmas. First, here is a very basic invertibility criterion for linear maps:

Lemma 37.2. Let k be a field. Let V be a k-vector space. Let $f : V \to V$ be a k-linear map. Let $(V_1, V_2, V_3, \ldots)$ be a sequence of k-vector subspaces of V such that $V = \bigcup_{n \geq 1} V_n$. Assume that $(\mathrm{id}_V - f)^n (V_n) = 0$ for every integer $n \geq 1$. Then, the map f is invertible.

Proof of Lemma 37.2. Clearly, the elements f and id_V of $\operatorname{End} V$ commute (since $f \circ \mathrm{id}_V = f = \mathrm{id}_V \circ f$). Let $\mathfrak{H}$ be the k-subalgebra of $\operatorname{End} V$ generated by the elements f and id_V. [242] Then, the k-algebra $\mathfrak{H}$ is commutative (by Corollary 11.3, applied to $A = \operatorname{End} V$ and $g = \mathrm{id}_V$). Therefore, we can apply the binomial theorem in this k-algebra $\mathfrak{H}$. Since f and id_V both belong to $\mathfrak{H}$ (because $\mathfrak{H}$ is generated by f and id_V), the binomial theorem thus yields

$$\begin{aligned}
(\mathrm{id}_V - f)^n &= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \underbrace{\mathrm{id}_V^i}_{=\mathrm{id}_V} \circ f^{n-i} = \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} \underbrace{\mathrm{id}_V \circ f^{n-i}}_{=f^{n-i}} \\
&= \sum_{i=0}^{n} (-1)^{n-i} \binom{n}{i} f^{n-i} = \underbrace{(-1)^{n-n}}_{=(-1)^0=1} \underbrace{\binom{n}{n}}_{=1} \underbrace{f^{n-n}}_{=f^0=\mathrm{id}_V} + \sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} \underbrace{f^{n-i}}_{=f^{(n-i-1)+1}} \\
&= \mathrm{id}_V + \sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} \underbrace{f^{(n-i-1)+1}}_{\substack{=f \circ f^{n-i-1} \\ (\text{since } n-i-1 \geq 0 \text{ (because } i \leq n-1))}} \qquad (486) \\
&= \mathrm{id}_V + \underbrace{\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f \circ f^{n-i-1}}_{\substack{= f \circ \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) \\ (\text{since composition of } k\text{-linear maps is } k\text{-bilinear})}} \\
&= \mathrm{id}_V + f \circ \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) \qquad (487)
\end{aligned}$$

[242] Of course, this $\mathfrak{H}$ is also the k-subalgebra of $\operatorname{End} V$ generated by the element f alone (because the element id_V is the unity of the k-algebra $\operatorname{End} V$, and thus lies in any k-subalgebra of $\operatorname{End} V$). But we will not need this.

for each $n \in \mathbb{N}$.

Let us now show that the map f is surjective.

Indeed, let $v \in V$ be arbitrary. Then, $v \in V = \bigcup_{n \geq 1} V_n$. Hence, there exists an integer $n \geq 1$ such that $v \in V_n$. Consider this n.

Since $v \in V_n$, we have $\left(\mathrm{id}_V - f\right)^n \left(\underbrace{v}_{\in V_n} \right) \in \left(\mathrm{id}_V - f\right)^n (V_n) = 0$, and thus $\left(\mathrm{id}_V - f\right)^n (v) = 0$.

Now, recall that $\left(\mathrm{id}_V - f\right)^n (v) = 0$, so that

$$\begin{aligned} 0 &= \underbrace{\left(\mathrm{id}_V - f\right)^n}_{= \mathrm{id}_V + f \circ \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) \text{ (by (487))}} (v) = \left(\mathrm{id}_V + f \circ \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) \right) (v) \\ &= \underbrace{\mathrm{id}_V (v)}_{=v} + \left(f \circ \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) \right) (v) \\ &= v + \left(f \circ \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) \right) (v) . \end{aligned}$$

Subtracting v from this equality, we obtain

$$\begin{aligned} -v &= \left(f \circ \left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) \right) (v) \\ &= f \left(\underbrace{\left(\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \right) (v)}_{\in V} \right) \in f(V) . \end{aligned}$$

Thus, $v = -\underbrace{(-v)}_{\in f(V)} \in -f(V) \subseteq f(V)$ (since $f(V)$ is a k-vector space).

Now, forget that we fixed v. We thus have proven that every $v \in V$ satisfies $v \in f(V)$. In other words, $V \subseteq f(V)$. In other words, the map f is surjective.

Now, let $v \in \operatorname{Ker} f$ be arbitrary. Then, $f(v) = 0$. But on the other hand, $v \in \operatorname{Ker} f \subseteq V = \bigcup_{n \geq 1} V_n$. Hence, there exists an integer $n \geq 1$ such that $v \in V_n$. Consider this n.

Since $v \in V_n$, we have $\left(\mathrm{id}_V - f\right)^n \left(\underbrace{v}_{\in V_n} \right) \in \left(\mathrm{id}_V - f\right)^n (V_n) = 0$, and thus $\left(\mathrm{id}_V - f\right)^n (v) =$

0. Thus,

$$
\begin{aligned}
0 = & \underbrace{\left(\mathrm{id}_V - f\right)^n}_{=\mathrm{id}_V + \sum\limits_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{(n-i-1)+1} \ \text{(by (486))}} (v) \\
&= \left(\mathrm{id}_V + \sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{(n-i-1)+1} \right) (v) \\
&= \underbrace{\mathrm{id}_V (v)}_{=v} + \sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} \underbrace{f^{(n-i-1)+1}}_{=f^{n-i-1} \circ f \ \text{(since } n-i-1 \geq 0 \text{ (because } i \leq n-1))} (v) \\
&= v + \sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} \underbrace{\left(f^{n-i-1} \circ f\right)(v)}_{=f^{n-i-1}(f(v))} \\
&= v + \sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} f^{n-i-1} \left(\underbrace{f(v)}_{=0} \right) = v + \sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} \underbrace{f^{n-i-1}(0)}_{=0 \ \text{(since } f^{n-i-1} \text{ is } k\text{-linear)}} \\
&= v + \underbrace{\sum_{i=0}^{n-1} (-1)^{n-i} \binom{n}{i} 0}_{=0} = v,
\end{aligned}
$$

so that $v = 0$.

Now, forget that we fixed v. We thus have proven that every $v \in \operatorname{Ker} f$ satisfies $v = 0$. In other words, $\operatorname{Ker} f = 0$. Thus, the k-linear map f is injective. Combined with the fact that f is surjective, this yields that f is bijective. Hence, f is invertible. This proves Lemma 37.2. □

Let us show a simple property of connected filtered k-coalgebras:

Proposition 37.3. Let k be a field. Let C be a connected filtered k-coalgebra. As we know, C thus becomes a unital coalgebra. Let $x \in C_{\leq 1}$. Then, $x - \varepsilon(x) \cdot 1_C$ is a primitive element of C.

Proof of Proposition 37.3. By the axioms of a unital coalgebra, we have $\varepsilon(1_C) = 1$ (since C is a unital coalgebra).

Let $y = x - \varepsilon(x) \cdot 1_C$. We have

$$
\begin{aligned}
\varepsilon \left(\underbrace{y}_{=x-\varepsilon(x)\cdot 1_C} \right) &= \varepsilon\left(x - \varepsilon(x) \cdot 1_C\right) = \varepsilon(x) - \varepsilon(x) \cdot \underbrace{\varepsilon(1_C)}_{=1} \qquad \text{(since the map } \varepsilon \text{ is } k\text{-linear)} \\
&= \varepsilon(x) - \varepsilon(x) = 0.
\end{aligned}
$$

Thus, $y \in \operatorname{Ker} \varepsilon$. Combined with $y \in C_{\leq 1}$, this yields $y \in C_{\leq 1} \cap \operatorname{Ker} \varepsilon$. Thus, Proposi-

tion 17.9 (applied to 1 and y instead of ℓ and x) yields

$$\Delta_C(y) \in y \otimes 1_C + 1_C \otimes y + \underbrace{\sum_{u=1}^{1-1} C_{\leq u} \otimes C_{\leq 1-u}}_{=(\text{empty sum})=0} = y \otimes 1_C + 1_C \otimes y.$$

In other words, $\Delta_C(y) = y \otimes 1_C + 1_C \otimes y$. In other words, y is primitive. In other words, $x - \varepsilon(x) \cdot 1_C$ is primitive (since $y = x - \varepsilon(x) \cdot 1_C$). This proves Proposition 37.3. $\square$

Next, we state two lemmas from linear algebra:

Lemma 37.4. Let k be a field. Let V and V' be two k-vector spaces. Let $\beta \in \operatorname{End} V$ and $\beta' \in \operatorname{End}(V')$. Then,

$$\beta^i \otimes (\beta')^i = (\beta \otimes \beta')^i \tag{488}$$

for every $i \in \mathbb{N}$.

Proof of Lemma 37.4. We shall prove (488) by induction over i:

Induction base: If $i = 0$, then

$$\begin{aligned}\beta^i \otimes (\beta')^i &= \underbrace{\beta^0}_{=\mathrm{id}_V} \otimes \underbrace{(\beta')^0}_{=\mathrm{id}_{V'}} = \mathrm{id}_V \otimes \mathrm{id}_{V'} = \mathrm{id}_{V \otimes V'} = (\beta \otimes \beta')^0 \\ &\qquad \left(\text{since } (\beta \otimes \beta')^0 = \mathrm{id}_{V \otimes V'}\right) \\ &= (\beta \otimes \beta')^i \qquad (\text{since } 0 = i \text{ (because } i = 0)).\end{aligned}$$

Thus, (488) is proven for $i = 0$. This completes the induction base.

Induction step: Let $K \in \mathbb{N}$. Assume that (488) holds for $i = K$. We need to show that (488) holds for $i = K + 1$.

We know that (488) holds for $i = K$. In other words, $\beta^K \otimes (\beta')^K = (\beta \otimes \beta')^K$. Now,

$$\underbrace{\beta^{K+1}}_{=\beta^K \circ \beta} \otimes \underbrace{(\beta')^{K+1}}_{=(\beta')^K \circ \beta'} = \left(\beta^K \circ \beta\right) \otimes \left((\beta')^K \circ \beta'\right) = \left(\beta^K \otimes (\beta')^K\right) \circ (\beta \otimes \beta')$$

(by (21), applied to V, V, V, V', V', V', β, β^K, β' and $(\beta')^K$ instead of U, V, W, U', V', W', α, β, α' and β'). Thus,

$$\beta^{K+1} \otimes (\beta')^{K+1} = \underbrace{\left(\beta^K \otimes (\beta')^K\right)}_{=(\beta \otimes \beta')^K} \circ (\beta \otimes \beta') = (\beta \otimes \beta')^K \circ (\beta \otimes \beta') = (\beta \otimes \beta')^{K+1}.$$

In other words, (488) holds for $i = K + 1$. This completes the induction step. Thus, (488) is proven by induction. Hence, Lemma 37.4 is proven. $\square$

Lemma 37.5. Let k be a field. Let V be a k-vector space. Let $f \in \operatorname{End} V$. Let $n \in \mathbb{N}$. Then,

$$(\mathrm{id}_V \otimes \mathrm{id}_V - f \otimes f)^n = \sum_{i=0}^{n} \binom{n}{i} (\mathrm{id}_V - f)^{n-i} \otimes \left(f^{n-i} \circ (\mathrm{id}_V - f)^i\right).$$

Proof of Lemma 37.5. First of all, it is easy to see that

$$(\mathrm{id}_V - f)^i \circ f^{n-i} = f^{n-i} \circ (\mathrm{id}_V - f)^i \qquad \text{for every } i \in \{0, 1, \ldots, n\}. \tag{489}$$

[243]

Also,

$$\begin{aligned}(\mathrm{id}_V - f) \circ f &= \underbrace{\mathrm{id}_V \circ f}_{= f = f \circ \mathrm{id}_V} - f \circ f \qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} \\ &= f \circ \mathrm{id}_V - f \circ f \\ &= f \circ (\mathrm{id}_V - f) \qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)}.\end{aligned}$$

Now, (21) (applied to V, V, V, V, V, V, $\mathrm{id}_V - f$, id_V, f and $\mathrm{id}_V - f$ instead of U, V, W, U', V', W', α, β, α' and β') yields

$$(\mathrm{id}_V \circ (\mathrm{id}_V - f)) \otimes ((\mathrm{id}_V - f) \circ f) = (\mathrm{id}_V \otimes (\mathrm{id}_V - f)) \circ ((\mathrm{id}_V - f) \otimes f),$$

so that

$$\begin{aligned}&(\mathrm{id}_V \otimes (\mathrm{id}_V - f)) \circ ((\mathrm{id}_V - f) \otimes f) \\ &= \left(\underbrace{\mathrm{id}_V \circ (\mathrm{id}_V - f)}_{= \mathrm{id}_V - f = (\mathrm{id}_V - f) \circ \mathrm{id}_V} \right) \otimes \left(\underbrace{(\mathrm{id}_V - f) \circ f}_{= f \circ (\mathrm{id}_V - f)} \right) \\ &= ((\mathrm{id}_V - f) \circ \mathrm{id}_V) \otimes (f \circ (\mathrm{id}_V - f)) \\ &= ((\mathrm{id}_V - f) \otimes f) \circ (\mathrm{id}_V \otimes (\mathrm{id}_V - f))\end{aligned}$$

(by (21), applied to V, V, V, V, V, V, $\mathrm{id}_V - f$, id_V, $\mathrm{id}_V - f$ and f instead of U, V, W, U', V', W', α, β, α' and β'). In other words, the elements $\mathrm{id}_V \otimes (\mathrm{id}_V - f)$ and $(\mathrm{id}_V - f) \otimes f$ of $\mathrm{End}\,(V \otimes V)$ commute.

Now, let $\mathfrak{H}$ be the the k-subalgebra of $\mathrm{End}\,(V \otimes V)$ generated by the elements $\mathrm{id}_V \otimes (\mathrm{id}_V - f)$ and $(\mathrm{id}_V - f) \otimes f$. Then, the k-algebra $\mathfrak{H}$ is commutative (by Corollary 11.3, applied to $\mathrm{End}\,(V \otimes V)$, $\mathrm{id}_V \otimes (\mathrm{id}_V - f)$ and $(\mathrm{id}_V - f) \otimes f$ instead of A, f and g). Therefore, we can apply the binomial theorem in this k-algebra $\mathfrak{H}$. Since $\mathrm{id}_V \otimes (\mathrm{id}_V - f)$ and $(\mathrm{id}_V - f) \otimes f$ both belong to $\mathfrak{H}$ (because $\mathfrak{H}$ is generated by $\mathrm{id}_V \otimes (\mathrm{id}_V - f)$

[243] *Proof of (489):* Let $i \in \{0, 1, \ldots, n\}$. The elements f and id_V of $\mathrm{End}\, V$ clearly commute (since $f \circ \mathrm{id}_V = f = \mathrm{id}_V \circ f$). Let $\mathfrak{G}$ be the k-subalgebra of $\mathrm{End}\, V$ generated by the elements f and id_V. Then, the k-algebra $\mathfrak{G}$ is commutative (by Corollary 11.3, applied to $A = \mathrm{End}\, V$, $g = \mathrm{id}_V$ and $\mathfrak{H} = \mathfrak{G}$). But the elements f and id_V belong to $\mathfrak{G}$ (because the k-algebra $\mathfrak{G}$ is generated by f and id_V). Thus, f^{n-i} and $(\mathrm{id}_V - f)^i$ belong to $\mathfrak{G}$. As a consequence, $f^{n-i} \circ (\mathrm{id}_V - f)^i = (\mathrm{id}_V - f)^i \circ f^{n-i}$ in $\mathfrak{G}$ (since $\mathfrak{G}$ is commutative). This proves (489).

and $(\mathrm{id}_V - f) \otimes f$), the binomial theorem thus yields

$$
\begin{aligned}
&(\mathrm{id}_V \otimes (\mathrm{id}_V - f) + (\mathrm{id}_V - f) \otimes f)^n \\
&= \sum_{i=0}^{n} \binom{n}{i} \underbrace{(\mathrm{id}_V \otimes (\mathrm{id}_V - f))^i}_{\substack{= \mathrm{id}_V^i \otimes (\mathrm{id}_V - f)^i \\ \text{(because Lemma 37.4 (applied to } V,\ \mathrm{id}_V \text{ and } \mathrm{id}_V - f \\ \text{instead of } V',\ \beta \text{ and } \beta') \text{ yields} \\ \mathrm{id}_V^i \otimes (\mathrm{id}_V - f)^i = (\mathrm{id}_V \otimes (\mathrm{id}_V - f))^i)}} \circ \underbrace{((\mathrm{id}_V - f) \otimes f)^{n-i}}_{\substack{= (\mathrm{id}_V - f)^{n-i} \otimes f^{n-i} \\ \text{(because Lemma 37.4 (applied to } V,\ \mathrm{id}_V - f,\ f \text{ and } n-i \\ \text{instead of } V',\ \beta,\ \beta' \text{ and } i) \text{ yields} \\ (\mathrm{id}_V - f)^{n-i} \otimes f^{n-i} = ((\mathrm{id}_V - f) \otimes f)^{n-i})}} \\
&= \sum_{i=0}^{n} \binom{n}{i} \underbrace{\left(\mathrm{id}_V^i \otimes (\mathrm{id}_V - f)^i\right) \circ \left((\mathrm{id}_V - f)^{n-i} \otimes f^{n-i}\right)}_{\substack{= \left(\mathrm{id}_V^i \circ (\mathrm{id}_V - f)^{n-i}\right) \otimes \left((\mathrm{id}_V - f)^i \circ f^{n-i}\right) \\ \text{(since (21) (applied to } V,\ V,\ V,\ V,\ V,\ V, \\ (\mathrm{id}_V - f)^{n-i},\ \mathrm{id}_V^i,\ f^{n-i} \text{ and } (\mathrm{id}_V - f)^i \text{ instead of} \\ U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha' \text{ and } \beta') \text{ yields} \\ \left(\mathrm{id}_V^i \circ (\mathrm{id}_V - f)^{n-i}\right) \otimes \left((\mathrm{id}_V - f)^i \circ f^{n-i}\right) \\ = \left(\mathrm{id}_V^i \otimes (\mathrm{id}_V - f)^i\right) \circ \left((\mathrm{id}_V - f)^{n-i} \otimes f^{n-i}\right))}} \\
&= \sum_{i=0}^{n} \binom{n}{i} \left(\underbrace{\mathrm{id}_V^i}_{= \mathrm{id}_V} \circ (\mathrm{id}_V - f)^{n-i}\right) \otimes \left(\underbrace{(\mathrm{id}_V - f)^i \circ f^{n-i}}_{\substack{= f^{n-i} \circ (\mathrm{id}_V - f)^i \\ \text{(by (489))}}}\right) \\
&= \sum_{i=0}^{n} \binom{n}{i} \underbrace{\left(\mathrm{id}_V \circ (\mathrm{id}_V - f)^{n-i}\right)}_{= (\mathrm{id}_V - f)^{n-i}} \otimes \left(f^{n-i} \circ (\mathrm{id}_V - f)^i\right) \\
&= \sum_{i=0}^{n} \binom{n}{i} (\mathrm{id}_V - f)^{n-i} \otimes \left(f^{n-i} \circ (\mathrm{id}_V - f)^i\right).
\end{aligned}
$$

This proves Lemma 37.5. □

Here comes another little lemma about coalgebras:

Lemma 37.6. Let k be a field. Let C be a k-coalgebra. Let $f : C \to C$ and $g : C \to C$ be two k-coalgebra homomorphisms. Then,

$$(f \otimes f - g \otimes g)^n \circ \Delta_C = \Delta_C \circ (f - g)^n \tag{490}$$

for every $n \in \mathbb{N}$.

Proof of Lemma 37.6. We will prove Lemma 37.6 by induction over n:

Induction base: If $n = 0$, then (490) holds.[244] This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that (490) holds for $n = N$. We now must show that (490) also holds for $n = N + 1$.

[244] *Proof.* Assume that $n = 0$. Then,

$$
\begin{aligned}
(f \otimes f - g \otimes g)^n \circ \Delta_C &= \underbrace{(f \otimes f - g \otimes g)^0}_{= \mathrm{id}_{C \otimes C}} \circ \Delta_C \qquad \text{(since } n = 0\text{)} \\
&= \Delta_C.
\end{aligned}
$$

We know that (490) holds for $n = N$. In other words, we have

$$(f \otimes f - g \otimes g)^N \circ \Delta_C = \Delta_C \circ (f - g)^N .$$

Since f is a k-coalgebra homomorphism, we have $\Delta_C \circ f = (f \otimes f) \circ \Delta_C$ and $\varepsilon_C \circ f = \varepsilon_C$. Since g is a k-coalgebra homomorphism, we have $\Delta_C \circ g = (g \otimes g) \circ \Delta_C$ and $\varepsilon_C \circ g = \varepsilon_C$.

Since composition of k-linear maps is k-bilinear, we have

$$\begin{aligned}\Delta_C \circ (f - g) &= \underbrace{\Delta_C \circ f}_{=(f\otimes f)\circ\Delta_C} - \underbrace{\Delta_C \circ g}_{=(g\otimes g)\circ\Delta_C} = (f \otimes f) \circ \Delta_C - (g \otimes g) \circ \Delta_C \\ &= (f \otimes f - g \otimes g) \circ \Delta_C \qquad \text{(since composition of } k\text{-linear maps is } k\text{-bilinear)} .\end{aligned}$$

Thus,

$$(f \otimes f - g \otimes g) \circ \Delta_C = \Delta_C \circ (f - g) .$$

But now,

$$\begin{aligned}&\underbrace{(f \otimes f - g \otimes g)^{N+1}}_{=(f\otimes f-g\otimes g)\circ(f\otimes f-g\otimes g)^N} \circ \Delta_C \\ &= (f \otimes f - g \otimes g) \circ \underbrace{(f \otimes f - g \otimes g)^N \circ \Delta_C}_{=\Delta_C\circ(f-g)^N} \\ &= \underbrace{(f \otimes f - g \otimes g) \circ \Delta_C}_{=\Delta_C\circ(f-g)} \circ (f - g)^N = \Delta_C \circ \underbrace{(f - g) \circ (f - g)^N}_{=(f-g)^{N+1}} = \Delta_C \circ (f - g)^{N+1} .\end{aligned}$$

In other words, (490) holds for $n = N + 1$. This completes the induction step. The induction proof of (490) is thus complete. Hence, Lemma 37.6 is proven. □

We will now finally prove Theorem 37.1.

Proof of Theorem 37.1. **(a)** We need to prove that

$$(\mathrm{id}_C - f)^n (C_{\leq n}) = 0 \qquad \text{for every integer } n \geq 1. \tag{491}$$

Proof of (491): We will prove (491) by strong induction over n:

Induction step:[245] Let N be an integer ≥ 1. We assume that (491) holds whenever $n < N$. We now need to prove that (491) holds for $n = N$.

We have assumed that (491) holds whenever $n < N$. In other words,

$$(\mathrm{id}_C - f)^n (C_{\leq n}) = 0 \qquad \text{for every integer } n \geq 1 \text{ satisfying } n < N. \tag{492}$$

Compared with

$$\begin{aligned}\Delta_C \circ (f - g)^n &= \Delta_C \circ \underbrace{(f - g)^0}_{=\mathrm{id}_C} \qquad \text{(since } n = 0\text{)} \\ &= \Delta_C,\end{aligned}$$

this yields $(f \otimes f - g \otimes g)^n \circ \Delta_C = \Delta_C \circ (f - g)^n$. Thus, (490) holds if $n = 0$, qed.

[245] A strong induction needs no induction base.

Now, let $x \in C_{\leq N}$ be arbitrary. Let $y = x - \varepsilon(x) \cdot 1_C$. Then, it is easy to see that $y \in C_{\leq N} \cap \operatorname{Ker} \varepsilon$ [246]. Hence, Proposition 17.9 (applied to N and y instead of ℓ and x) yields

$$\Delta_C(y) \in y \otimes 1_C + 1_C \otimes y + \sum_{u=1}^{N-1} C_{\leq u} \otimes C_{\leq N-u}. \tag{493}$$

But Lemma 37.6 (applied to id_C, f and $N-1$ instead of f, g and n) yields

$$(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1} \circ \Delta_C = \Delta_C \circ (\mathrm{id}_C - f)^{N-1}. \tag{494}$$

Now, define an element $z \in C$ by $z = (\mathrm{id}_C - f)^{N-1}(y)$. Then,

$$\begin{aligned}
\Delta_C\left(\underbrace{z}_{=(\mathrm{id}_C - f)^{N-1}(y)}\right) &= \Delta_C\left((\mathrm{id}_C - f)^{N-1}(y)\right) = \left(\underbrace{\Delta_C \circ (\mathrm{id}_C - f)^{N-1}}_{\substack{=(\mathrm{id}_C \otimes \mathrm{id}_C - f\otimes f)^{N-1}\circ\Delta_C \\ \text{(by (494))}}}\right)(y) \\
&= \left((\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1} \circ \Delta_C\right)(y) \\
&= (\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1} \left(\underbrace{\Delta_C(y)}_{\substack{\in y\otimes 1_C + 1_C \otimes y + \sum_{u=1}^{N-1} C_{\leq u}\otimes C_{\leq N-u} \\ \text{(by (493))}}}\right) \\
&\in (\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1} \left(y \otimes 1_C + 1_C \otimes y + \sum_{u=1}^{N-1} C_{\leq u} \otimes C_{\leq N-u}\right) \\
&\subseteq (\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}(y \otimes 1_C) \\
&\quad + (\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}(1_C \otimes y) \\
&\quad + (\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1} \left(\sum_{u=1}^{N-1} C_{\leq u} \otimes C_{\leq N-u}\right)
\end{aligned} \tag{495}$$

(since the map $(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}$ is k-linear).

[246] *Proof.* By the axioms of a connected filtered k-coalgebra, we have $1_C \in C_{\leq 0}$ (since C is a connected filtered k-coalgebra). But $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$ (since C is a filtered k-coalgebra), hence $C_{\leq 0} \subseteq C_{\leq N}$. Thus, $1_C \in C_{\leq 0} \subseteq C_{\leq N}$. Now, $y = \underbrace{x}_{\in C_{\leq N}} - \varepsilon(x) \cdot \underbrace{1_C}_{\in C_{\leq N}} \in C_{\leq N} - \varepsilon(x) \cdot C_{\leq N} \subseteq C_{\leq N}$ (since $C_{\leq N}$ is a k-vector space).

By the axioms of a unital coalgebra, we have $\varepsilon(1_C) = 1$ (since C is a unital coalgebra).

Also,

$$\begin{aligned}
\varepsilon\left(\underbrace{y}_{=x-\varepsilon(x)\cdot 1_C}\right) &= \varepsilon(x - \varepsilon(x) \cdot 1_C) = \varepsilon(x) - \varepsilon(x) \cdot \underbrace{\varepsilon(1_C)}_{=1} \qquad \text{(since the map } \varepsilon \text{ is } k\text{-linear)} \\
&= \varepsilon(x) - \varepsilon(x) = 0.
\end{aligned}$$

Thus, $y \in \operatorname{Ker} \varepsilon$. Combined with $y \in C_{\leq N}$, this yields $y \in C_{\leq N} \cap \operatorname{Ker} \varepsilon$, qed.

Recall that $N \geq 1$, hence $N-1 \geq 0$. Thus, $N-1 \in \mathbb{N}$. But Lemma 37.5 (applied to $V = C$ and $n = N-1$) yields

$$\begin{aligned} & \left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1} \\ &= \sum_{i=0}^{N-1} \binom{N-1}{i} \left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right). \end{aligned} \tag{496}$$

Also, we have

$$\left(\mathrm{id}_C - f\right)^\ell (1_C) = 0 \qquad \text{for every integer } \ell \geq 1. \tag{497}$$

[247] Moreover,

$$f^\ell (1_C) = 1_C \qquad \text{for every } \ell \in \mathbb{N}. \tag{498}$$

[248]

Now,

$$\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1} (y \otimes 1_C) = z \otimes 1_C \tag{499}$$

[249] and

$$\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1} (1_C \otimes y) = 1_C \otimes z \tag{501}$$

---

[247] *Proof of (497):* Let ℓ be an integer ≥ 1. Then, $\left(\mathrm{id}_C - f\right)^\ell = \left(\mathrm{id}_C - f\right)^{\ell-1} \circ \left(\mathrm{id}_C - f\right)$. But $f(1_C) = 1_C$, so that $\left(\mathrm{id}_C - f\right)(1_C) = \underbrace{\mathrm{id}_C(1_C)}_{=1_C} - \underbrace{f(1_C)}_{=1_C} = 1_C - 1_C = 0$ and

$$\underbrace{\left(\mathrm{id}_C - f\right)^\ell}_{=\left(\mathrm{id}_C - f\right)^{\ell-1} \circ \left(\mathrm{id}_C - f\right)} (1_C) = \left(\left(\mathrm{id}_C - f\right)^{\ell-1} \circ \left(\mathrm{id}_C - f\right)\right)(1_C)$$

$$= \left(\mathrm{id}_C - f\right)^{\ell-1} \left(\underbrace{\left(\mathrm{id}_C - f\right)(1_C)}_{=0}\right) = \left(\mathrm{id}_C - f\right)^{\ell-1}(0) = 0$$

(since the map $\left(\mathrm{id}_C - f\right)^{\ell-1}$ is k-linear). This proves (497).

[248] *Proof of (498):* We will prove (498) by induction over ℓ:

Induction base: For $\ell = 0$, we have $f^\ell (1_C) = \underbrace{f^0}_{=\mathrm{id}_C} (1_C) = \mathrm{id}_C (1_C) = 1_C$. Hence, (498) is proven for $\ell = 0$. This completes the induction base.

Induction step: Let $L \in \mathbb{N}$. Assume that (498) holds for $\ell = L$. We need to prove that (498) holds for $\ell = L+1$.

We know that (498) holds for $\ell = L$. In other words, $f^L (1_C) = 1_C$. Now, $\underbrace{f^{L+1}}_{=f \circ f^L} (1_C) = \left(f \circ f^L\right)(1_C) = f\left(\underbrace{f^L (1_C)}_{=1_C}\right) = f(1_C) = 1_C$. In other words, (498) holds for $\ell = L+1$. This completes the induction step. The induction proof of (498) is thus complete.

[249] *Proof of (499):* Every $i \in \{1, 2, \ldots, N-1\}$ satisfies $i \geq 1$. Hence, every $i \in \{1, 2, \ldots, N-1\}$ satisfies $\left(\mathrm{id}_C - f\right)^i (1_C) = 0$ (by (497) (applied to $\ell = i$)). Thus, every $i \in \{1, 2, \ldots, N-1\}$ satisfies

$$\left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right)(1_C) = f^{N-1-i}\left(\underbrace{\left(\mathrm{id}_C - f\right)^i (1_C)}_{=0}\right) = f^{N-1-i}(0) = 0 \tag{500}$$

[250]. Furthermore, every $u \in \{1,2,\ldots,N-1\}$ and every $i \in \{0,1,\ldots,N-1\}$ satisfy

$$\left(\mathrm{id}_C - f\right)^{N-1-i}\left(C_{\leq u}\right) \otimes f^{N-1-i}\left(\left(\mathrm{id}_C - f\right)^{i}\left(C_{\leq N-u}\right)\right) = 0. \tag{503}$$

(since f^{N-1-i} is k-linear). Now,

$$\begin{aligned}
&\underbrace{\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1}}_{=\sum_{i=0}^{N-1}\binom{N-1}{i}\left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^{i}\right) \text{ (by (496))}} \qquad (y \otimes 1_C) \\
&= \left(\sum_{i=0}^{N-1} \binom{N-1}{i} \left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^{i}\right)\right)(y \otimes 1_C) \\
&= \sum_{i=0}^{N-1} \binom{N-1}{i} \underbrace{\left(\left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^{i}\right)\right)(y \otimes 1_C)}_{=\left(\mathrm{id}_C - f\right)^{N-1-i}(y) \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^{i}\right)(1_C)} \\
&= \sum_{i=0}^{N-1} \binom{N-1}{i} \left(\mathrm{id}_C - f\right)^{N-1-i}(y) \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^{i}\right)(1_C) \\
&= \sum_{i=1}^{N-1} \binom{N-1}{i} \left(\mathrm{id}_C - f\right)^{N-1-i}(y) \otimes \underbrace{\left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^{i}\right)(1_C)}_{=0 \text{ (by (500))}} \\
&\quad + \underbrace{\binom{N-1}{0}}_{=1} \underbrace{\left(\mathrm{id}_C - f\right)^{N-1-0}}_{=\left(\mathrm{id}_C - f\right)^{N-1}}(y) \otimes \left(\underbrace{f^{N-1-0}}_{=f^{N-1}} \circ \underbrace{\left(\mathrm{id}_C - f\right)^{0}}_{=\mathrm{id}_C}\right)(1_C) \\
&= \sum_{i=1}^{N-1} \binom{N-1}{i} \underbrace{\left(\mathrm{id}_C - f\right)^{N-1-i}(y) \otimes 0}_{=0} + \underbrace{1\left(\mathrm{id}_C - f\right)^{N-1}(y)}_{\substack{=\left(\mathrm{id}_C - f\right)^{N-1}(y)=z \\ \text{(since } z=\left(\mathrm{id}_C - f\right)^{N-1}(y)\text{)}}} \otimes \underbrace{\left(f^{N-1} \circ \mathrm{id}_C\right)}_{=f^{N-1}}(1_C) \\
&= \underbrace{\sum_{i=1}^{N-1} \binom{N-1}{i} 0}_{=0} + z \otimes f^{N-1}(1_C) = z \otimes \underbrace{f^{N-1}(1_C)}_{\substack{=1_C \\ \text{(by (498), applied to } \ell=N-1\text{)}}} = z \otimes 1_C.
\end{aligned}$$

This proves (499).

[250] *Proof of (501):* Every $i \in \{0,1,\ldots,N-2\}$ satisfies $N-1-i \geq 1$ (since every $i \in \{0,1,\ldots,N-2\}$ satisfies $i \leq N-2$ and thus $N-1-\underbrace{i}_{\leq N-2} \geq N-1-(N-2)=1$). Hence, every $i \in \{0,1,\ldots,N-2\}$ satisfies

$$\left(\mathrm{id}_C - f\right)^{N-1-i}(1_C) = 0 \tag{502}$$

[251]. Every $u \in \{1,2,\ldots,N-1\}$ satisfies

$$\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1} \left(C_{\leq u} \otimes C_{\leq N-u}\right) = 0. \tag{504}$$

(by (497) (applied to $\ell = N-1-i$)). Now,

$$\begin{aligned}
&\underbrace{\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1}}_{\substack{=\sum_{i=0}^{N-1} \binom{N-1}{i} (\mathrm{id}_C - f)^{N-1-i} \otimes \left(f^{N-1-i} \circ (\mathrm{id}_C - f)^i\right) \\ \text{(by (496))}}} (1_C \otimes y) \\
&= \left(\sum_{i=0}^{N-1} \binom{N-1}{i} (\mathrm{id}_C - f)^{N-1-i} \otimes \left(f^{N-1-i} \circ (\mathrm{id}_C - f)^i\right)\right) (1_C \otimes y) \\
&= \sum_{i=0}^{N-1} \binom{N-1}{i} \underbrace{\left((\mathrm{id}_C - f)^{N-1-i} \otimes \left(f^{N-1-i} \circ (\mathrm{id}_C - f)^i\right)\right) (1_C \otimes y)}_{= (\mathrm{id}_C - f)^{N-1-i}(1_C) \otimes \left(f^{N-1-i} \circ (\mathrm{id}_C - f)^i\right)(y)} \\
&= \sum_{i=0}^{N-1} \binom{N-1}{i} (\mathrm{id}_C - f)^{N-1-i} (1_C) \otimes \left(f^{N-1-i} \circ (\mathrm{id}_C - f)^i\right) (y) \\
&= \sum_{i=0}^{N-2} \binom{N-1}{i} \underbrace{(\mathrm{id}_C - f)^{N-1-i} (1_C)}_{\substack{=0 \\ \text{(by (502))}}} \otimes \left(f^{N-1-i} \circ (\mathrm{id}_C - f)^i\right) (y) \\
&\qquad + \underbrace{\binom{N-1}{N-1}}_{=1} \underbrace{(\mathrm{id}_C - f)^{N-1-(N-1)}}_{=(\mathrm{id}_C - f)^0 = \mathrm{id}_C} (1_C) \otimes \left(\underbrace{f^{N-1-(N-1)}}_{=f^0=\mathrm{id}_C} \circ (\mathrm{id}_C - f)^{N-1}\right) (y) \\
&= \sum_{i=0}^{N-2} \binom{N-1}{i} \underbrace{0 \otimes \left(f^{N-1-i} \circ (\mathrm{id}_C - f)^i\right) (y)}_{=0} + \underbrace{1 \mathrm{id}_C (1_C)}_{=\mathrm{id}_C(1_C)=1_C} \otimes \underbrace{\left(\mathrm{id}_C \circ (\mathrm{id}_C - f)^{N-1}\right)}_{=(\mathrm{id}_C - f)^{N-1}} (y) \\
&= \underbrace{\sum_{i=0}^{N-2} \binom{N-1}{i} 0}_{=0} + 1_C \otimes (\mathrm{id}_C - f)^{N-1} (y) = 1_C \otimes \underbrace{(\mathrm{id}_C - f)^{N-1} (y)}_{\substack{=z \\ \text{(since } z = (\mathrm{id}_C - f)^{N-1}(y)\text{)}}} = 1_C \otimes z.
\end{aligned}$$

This proves (501).

[251] *Proof of (503):* Let $u \in \{1,2,\ldots,N-1\}$ and $i \in \{0,1,\ldots,N-1\}$. Notice that $1 \leq u \leq N-1$ (since $u \in \{1,2,\ldots,N-1\}$), hence $u \geq 1$ and $u \leq N-1 < N$. Hence, (492) (applied to $n = u$) yields $(\mathrm{id}_C - f)^u (C_{\leq u}) = 0$. On the other hand, $N - \underbrace{u}_{\leq N-1} \geq N - (N-1) = 1$ and $N - \underbrace{u}_{\geq 1} \leq N-1 < N$; therefore, (492) (applied to $n = N-u$) yields $(\mathrm{id}_C - f)^{N-u} (C_{\leq N-u}) = 0$.

We want to prove (503). We must be in one of the following two cases:

Case 1: We have $u \leq N-1-i$.

Case 2: We have $u > N-1-i$.

Let us first consider Case 1. In this case, we have $u \leq N-1-i$. Thus, $N-1-i \geq u$, so that $(N-1-i)-u$ is a nonnegative integer. Denote this nonnegative integer by γ. Thus, $(N-1-i)-u = \gamma$, so that $N-1-i = \gamma+u$ and therefore

$$(\mathrm{id}_C - f)^{N-1-i} = (\mathrm{id}_C - f)^{\gamma+u} = (\mathrm{id}_C - f)^{\gamma} \circ (\mathrm{id}_C - f)^u,$$

and thus

$$\underbrace{\left(\mathrm{id}_C - f\right)^{N-1-i}}_{=\left(\mathrm{id}_C - f\right)^{\gamma} \circ \left(\mathrm{id}_C - f\right)^{u}} \left(C_{\leq u}\right) = \left(\left(\mathrm{id}_C - f\right)^{\gamma} \circ \left(\mathrm{id}_C - f\right)^{u}\right)\left(C_{\leq u}\right)$$

$$= \left(\mathrm{id}_C - f\right)^{\gamma}\left(\underbrace{\left(\mathrm{id}_C - f\right)^{u}\left(C_{\leq u}\right)}_{=0}\right) = \left(\mathrm{id}_C - f\right)^{\gamma}(0) = 0$$

(since the map $\left(\mathrm{id}_C - f\right)^{\gamma}$ is k-linear). Hence,

$$\underbrace{\left(\mathrm{id}_C - f\right)^{N-1-i}\left(C_{\leq u}\right)}_{=0} \otimes f^{N-1-i}\left(\left(\mathrm{id}_C - f\right)^{i}\left(C_{\leq N-u}\right)\right) = 0 \otimes f^{N-1-i}\left(\left(\mathrm{id}_C - f\right)^{i}\left(C_{\leq N-u}\right)\right) = 0.$$

Therefore, (503) is proven in Case 1.

Let us now consider Case 2. In this case, we have $u > N-1-i$. Since u and $N-1-i$ are integers, this yields $u \geq (N-1-i)+1 = N-i$. Thus, $u+i \geq N$, so that $i \geq N-u$. In other words, $i-(N-u)$ is a nonnegative integer. Denote this nonnegative integer by γ. Thus, $i-(N-u) = \gamma$, so that $i = \gamma + (N-u)$ and therefore

$$\left(\mathrm{id}_C - f\right)^{i} = \left(\mathrm{id}_C - f\right)^{\gamma+(N-u)} = \left(\mathrm{id}_C - f\right)^{\gamma} \circ \left(\mathrm{id}_C - f\right)^{N-u},$$

and thus

$$\underbrace{\left(\mathrm{id}_C - f\right)^{i}}_{=\left(\mathrm{id}_C - f\right)^{\gamma} \circ \left(\mathrm{id}_C - f\right)^{N-u}} \left(C_{\leq N-u}\right) = \left(\left(\mathrm{id}_C - f\right)^{\gamma} \circ \left(\mathrm{id}_C - f\right)^{N-u}\right)\left(C_{\leq N-u}\right)$$

$$= \left(\mathrm{id}_C - f\right)^{\gamma}\left(\underbrace{\left(\mathrm{id}_C - f\right)^{N-u}\left(C_{\leq N-u}\right)}_{=0}\right) = \left(\mathrm{id}_C - f\right)^{\gamma}(0) = 0$$

(since the map $\left(\mathrm{id}_C - f\right)^{\gamma}$ is k-linear). Thus,

$$\left(\mathrm{id}_C - f\right)^{N-1-i}\left(C_{\leq u}\right) \otimes f^{N-1-i}\left(\underbrace{\left(\mathrm{id}_C - f\right)^{i}\left(C_{\leq N-u}\right)}_{=0}\right)$$

$$= \left(\mathrm{id}_C - f\right)^{N-1-i}\left(C_{\leq u}\right) \otimes \underbrace{f^{N-1-i}(0)}_{\substack{=0 \\ \text{(since } f^{N-1-i} \text{ is } k\text{-linear)}}} = \left(\mathrm{id}_C - f\right)^{N-1-i}\left(C_{\leq u}\right) \otimes 0 = 0.$$

Thus, (503) is proven in Case 2.

We have now proven (503) in both Cases 1 and 2. Since these two Cases cover all possibilities, this yields that (503) always holds. The proof of (503) is thus complete.

[252] Thus,

$$\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1} \left(\sum_{u=1}^{N-1} C_{\leq u} \otimes C_{\leq N-u} \right) = 0. \tag{505}$$

[252] *Proof of (504):* Let $u \in \{1, 2, \ldots, N-1\}$. Then, $1 \leq u \leq N-1$. Now,

$$\begin{aligned}
&\underbrace{\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1}}_{} \qquad (C_{\leq u} \otimes C_{\leq N-u}) \\
&= \sum_{i=0}^{N-1} \binom{N-1}{i} \underbrace{\left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right)}_{\text{(by (496))}} \\
&= \left(\sum_{i=0}^{N-1} \binom{N-1}{i} \left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right) \right) \left(C_{\leq u} \otimes C_{\leq N-u}\right) \\
&\subseteq \sum_{i=0}^{N-1} \underbrace{\binom{N-1}{i} \left(\left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right) \right) \left(C_{\leq u} \otimes C_{\leq N-u}\right)}_{\substack{\subseteq \left(\left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right)\right)\left(C_{\leq u} \otimes C_{\leq N-u}\right) \\ \text{(since } \left(\left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right)\right)\left(C_{\leq u} \otimes C_{\leq N-u}\right) \\ \text{is a } k\text{-vector space)}}} \\
&\subseteq \sum_{i=0}^{N-1} \underbrace{\left(\left(\mathrm{id}_C - f\right)^{N-1-i} \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right) \right) \left(C_{\leq u} \otimes C_{\leq N-u}\right)}_{\subseteq \left(\mathrm{id}_C - f\right)^{N-1-i}\left(C_{\leq u}\right) \otimes \left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right)\left(C_{\leq N-u}\right)} \\
&\subseteq \sum_{i=0}^{N-1} \left(\mathrm{id}_C - f\right)^{N-1-i} \left(C_{\leq u}\right) \otimes \underbrace{\left(f^{N-1-i} \circ \left(\mathrm{id}_C - f\right)^i\right) \left(C_{\leq N-u}\right)}_{= f^{N-1-i}\left(\left(\mathrm{id}_C - f\right)^i\left(C_{\leq N-u}\right)\right)} \\
&= \sum_{i=0}^{N-1} \underbrace{\left(\mathrm{id}_C - f\right)^{N-1-i} \left(C_{\leq u}\right) \otimes f^{N-1-i} \left(\left(\mathrm{id}_C - f\right)^i \left(C_{\leq N-u}\right) \right)}_{\substack{=0 \\ \text{(by (503))}}} \\
&= \sum_{i=0}^{N-1} 0 = 0.
\end{aligned}$$

In other words, $\left(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f\right)^{N-1} \left(C_{\leq u} \otimes C_{\leq N-u}\right) = 0$. This proves (504).

[253] Now, (495) becomes

$$\begin{aligned}\Delta_C(z) \in & \underbrace{(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}(y \otimes 1_C)}_{\substack{=z\otimes 1_C \\ \text{(by (499))}}} \\ & + \underbrace{(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}(1_C \otimes y)}_{\substack{=1_C\otimes z \\ \text{(by (501))}}} \\ & + \underbrace{(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}\left(\sum_{u=1}^{N-1} C_{\leq u} \otimes C_{\leq N-u}\right)}_{\substack{=0 \\ \text{(by (505))}}} \\ = & \, z \otimes 1_C + 1_C \otimes z + 0 = z \otimes 1_C + 1_C \otimes z.\end{aligned}$$

In other words, $\Delta_C(z) = z \otimes 1_C + 1_C \otimes z$. In other words, the element z of C is primitive (because the definition of "primitive" yields that the element z of C is primitive if and only if $\Delta_C(z) = z \otimes 1_C + 1_C \otimes z$). Hence, (485) (applied to z instead of x) yields

$$f(z) = z. \tag{506}$$

Now,

$$\begin{aligned}\underbrace{(\mathrm{id}_C - f)^N}_{=(\mathrm{id}_C - f)\circ(\mathrm{id}_C - f)^{N-1}}(y) &= \left((\mathrm{id}_C - f) \circ (\mathrm{id}_C - f)^{N-1}\right)(y) = (\mathrm{id}_C - f)\left(\underbrace{(\mathrm{id}_C - f)^{N-1}(y)}_{\substack{=z \\ \text{(since } z=(\mathrm{id}_C - f)^{N-1}(y)\text{)}}}\right) \\ &= (\mathrm{id}_C - f)(z) = \underbrace{\mathrm{id}_C(z)}_{=z} - \underbrace{f(z)}_{\substack{=z \\ \text{(by (506))}}} = z - z = 0.\end{aligned}$$

But recall that $y = x - \varepsilon(x) \cdot 1_C$, so that $x = y + \varepsilon(x) \cdot 1_C$. Applying the map

[253] *Proof of (505):* The map $(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}$ is k-linear. Thus,

$$\begin{aligned}&(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}\left(\sum_{u=1}^{N-1} C_{\leq u} \otimes C_{\leq N-u}\right) \\ &\subseteq \sum_{u=1}^{N-1} \underbrace{(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}(C_{\leq u} \otimes C_{\leq N-u})}_{\substack{=0 \\ \text{(by (505))}}} = \sum_{u=1}^{N-1} 0 = 0.\end{aligned}$$

Therefore, $(\mathrm{id}_C \otimes \mathrm{id}_C - f \otimes f)^{N-1}\left(\sum_{u=1}^{N-1} C_{\leq u} \otimes C_{\leq N-u}\right) = 0$. This proves (505).

$(\mathrm{id}_C - f)^N$ to both sides of this equality, we obtain

$$\begin{aligned}
&(\mathrm{id}_C - f)^N (x) \\
&= (\mathrm{id}_C - f)^N (y + \varepsilon(x) \cdot 1_C) \\
&= \underbrace{(\mathrm{id}_C - f)^N (y)}_{=0} + \varepsilon(x) \cdot \underbrace{(\mathrm{id}_C - f)^N (1_C)}_{\substack{=0 \\ \text{(by (497), applied to } \ell = N\text{)}}} \\
&\qquad \Big(\text{since the map } (\mathrm{id}_C - f)^N \text{ is } k\text{-linear}\Big) \\
&= 0 + \varepsilon(x) \cdot 0 = 0.
\end{aligned}$$

In other words, $x \in \mathrm{Ker}\left((\mathrm{id}_C - f)^N\right)$.

Now, forget that we fixed x. We thus have proven that every $x \in C_{\leq N}$ satisfies $x \in \mathrm{Ker}\left((\mathrm{id}_C - f)^N\right)$. In other words, $C_{\leq N} \subseteq \mathrm{Ker}\left((\mathrm{id}_C - f)^N\right)$. Hence,

$$(\mathrm{id}_C - f)^N \left(\underbrace{C_{\leq N}}_{\subseteq \mathrm{Ker}\left((\mathrm{id}_C - f)^N\right)} \right) \subseteq (\mathrm{id}_C - f)^N \left(\mathrm{Ker}\left((\mathrm{id}_C - f)^N\right) \right) = 0.$$

In other words, (491) holds for $n = N$. This completes the induction step. Thus, the induction proof of (491) is complete.

Now, we have proven that (491) holds for every integer $n \geq 1$. In other words, Theorem 37.1 **(a)** is proven.

(b) We have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$ (since C is filtered), so that $C_{\leq 0} \subseteq C_{\leq 1} \subseteq \bigcup_{n \geq 1} C_{\leq n}$ (because $C_{\leq 1}$ is a term in the union $\bigcup_{n \geq 1} C_{\leq n}$). Now, since C is filtered, we have

$$C = \bigcup_{n \geq 0} C_{\leq n} = \underbrace{C_{\leq 0}}_{\subseteq \bigcup_{n \geq 1} C_{\leq n}} \cup \left(\bigcup_{n \geq 1} C_{\leq n} \right) \subseteq \left(\bigcup_{n \geq 1} C_{\leq n} \right) \cup \left(\bigcup_{n \geq 1} C_{\leq n} \right) = \bigcup_{n \geq 1} C_{\leq n}.$$

Combined with $\bigcup_{n \geq 1} C_{\leq n} \subseteq C$ (this is obvious), this yields $C = \bigcup_{n \geq 1} C_{\leq n}$. Moreover, Theorem 37.1 **(a)** yields that $(\mathrm{id}_C - f)^n (C_{\leq n}) = 0$ for every integer $n \geq 1$. Hence, Lemma 37.2 (applied to $V = C$ and $V_i = C_{\leq i}$) yields that the map f is invertible. Thus, f is an invertible k-coalgebra homomorphism. Therefore, Proposition 34.13 (applied to $D = C$) yields that f is a k-coalgebra isomorphism. This proves Theorem 37.1 **(b)**. □

As a consequence of Theorem 37.1, we can obtain the curious fact that the antipode of a connected filtered k-Hopf algebra is invertible, and somewhat more:

Theorem 37.7. Let k be a field. Let H be a connected filtered k-Hopf algebra. Let S be the antipode of H.

(a) We have $(\mathrm{id}_H - S^2)^n (H_{\leq n}) = 0$ for every integer $n \geq 1$.

(b) The map S is invertible.

We notice that Theorem 37.7 generalizes a result of Aguiar and Lauve ([AguLau14, Corollary 5])[254].

Before we prove Theorem 37.7, let us show a lemma concerning arbitrary Hopf algebras:

Lemma 37.8. Let k be a field. Let H be a k-Hopf algebra. Let S be the antipode of H.

(a) The map $S^2 : H \to H$ is a k-coalgebra homomorphism.

(b) We have $S^2(1_H) = 1_H$.

(c) We have $S^2(x) = x$ for every primitive element x of H.

Proof of Lemma 37.8. **(a)** Recall that the coopposite coalgebra H^{cop} of H is defined as the k-coalgebra $(H, \tau_{H,H} \circ \Delta_H, \varepsilon_H)$. Thus, $\Delta_{H^{\mathrm{cop}}} = \tau_{H,H} \circ \Delta_H$ and $\varepsilon_{H^{\mathrm{cop}}} = \varepsilon_H$.

Proposition 25.4 yields that the antipode of H is a k-coalgebra homomorphism $H^{\mathrm{cop}} \to H$. In other words, S is a k-coalgebra homomorphism $H^{\mathrm{cop}} \to H$ (since S is the antipode of H). Thus, $\Delta_H \circ S = (S \otimes S) \circ \Delta_{H^{\mathrm{cop}}}$ and $\varepsilon_H \circ S = \varepsilon_{H^{\mathrm{cop}}}$.

Clearly, (21) (applied to $U = H$, $V = H$, $W = H$, $U' = H$, $V' = H$, $W' = H$, $\alpha = S$, $\beta = S$, $\alpha' = S$ and $\beta' = S$) yields $(S \circ S) \otimes (S \circ S) = (S \otimes S) \circ (S \otimes S)$. Hence,

$$(S \otimes S) \circ (S \otimes S) = \underbrace{(S \circ S)}_{=S^2} \otimes \underbrace{(S \circ S)}_{=S^2} = S^2 \otimes S^2.$$

A very basic property of the flip maps says that if V and W are two k-vector spaces, then $\tau_{W,V} \circ \tau_{V,W} = \mathrm{id}_{V \otimes W}$. Applying this to $V = H$ and $W = H$, we obtain $\tau_{H,H} \circ \tau_{H,H} = \mathrm{id}_{H \otimes H}$. Now,

$$\begin{aligned}
\Delta_H \circ \underbrace{S^2}_{=S \circ S} &= \underbrace{\Delta_H \circ S}_{=(S \otimes S) \circ \Delta_{H^{\mathrm{cop}}}} \circ S = (S \otimes S) \circ \underbrace{\Delta_{H^{\mathrm{cop}}}}_{=\tau_{H,H} \circ \Delta_H} \circ S \\
&= (S \otimes S) \circ \tau_{H,H} \circ \underbrace{\Delta_H \circ S}_{=(S \otimes S) \circ \Delta_{H^{\mathrm{cop}}}} = (S \otimes S) \circ \tau_{H,H} \circ (S \otimes S) \circ \underbrace{\Delta_{H^{\mathrm{cop}}}}_{=\tau_{H,H} \circ \Delta_H} \\
&= (S \otimes S) \circ \tau_{H,H} \circ \underbrace{(S \otimes S) \circ \tau_{H,H}}_{\substack{=\tau_{H,H} \circ (S \otimes S) \\ \text{(by Proposition 9.3 (a),} \\ \text{applied to } V=H,\ W=H,\ V'=H,\ W'=H, \\ f=S \text{ and } g=S)}} \circ \Delta_H \\
&= (S \otimes S) \circ \underbrace{\tau_{H,H} \circ \tau_{H,H}}_{=\mathrm{id}_{H \otimes H}} \circ (S \otimes S) \circ \Delta_H \\
&= \underbrace{(S \otimes S) \circ (S \otimes S)}_{=S^2 \otimes S^2} \circ \Delta_H = \left(S^2 \otimes S^2\right) \circ \Delta_H.
\end{aligned}$$

[254] Here are the details:

If k is a field, and H is a connected filtered k-Hopf algebra, then Theorem 37.7 **(a)** shows that the only possible eigenvalue of S^2 on $H_{\leq n}$ is 1, whence the only possible eigenvalues of S on $H_{\leq n}$ are 1 and -1. This readily yields [AguLau14, Corollary 5], but is itself a more general result. (Note also that the paper [AguLau14] works entirely over a field of characteristic 0, and does use this assumption in the proof; in contrast, what we are doing makes sense over any commutative ring k.)

Combined with

$$\varepsilon_H \circ \underbrace{S^2}_{=S\circ S} = \underbrace{\varepsilon_H \circ S}_{=\varepsilon_{H^{\mathrm{cop}}}=\varepsilon_H} \circ S = \varepsilon_H \circ S = \varepsilon_{H^{\mathrm{cop}}} = \varepsilon_H,$$

this yields that $S^2 : H \to H$ is a k-coalgebra homomorphism. This proves Lemma 37.8 **(a)**.

(b) Just as in the proof of Corollary 28.10, we can show that $S(1_H) = 1_H$. Hence, $\underbrace{S^2}_{=S\circ S}(1_H) = (S \circ S)(1_H) = S\left(\underbrace{S(1_H)}_{=1_H}\right) = S(1_H) = 1_H$. This proves Lemma 37.8 **(b)**.

(c) Let x be a primitive element of H. Then, x belongs to the set of all primitive elements of H. In other words, x belongs to $\operatorname{Prim} H$ (since $\operatorname{Prim} H$ is the set of all primitive elements of H). In other words, $x \in \operatorname{Prim} H$. Hence, Proposition 28.18 yields $S(x) = -x$. Thus,

$$\underbrace{S^2}_{=S\circ S}(x) = (S \circ S)(x) = S\left(\underbrace{S(x)}_{=-x}\right) = S(-x) = -\underbrace{S(x)}_{=-x} \qquad \text{(since the map } S \text{ is } k\text{-linear)}$$
$$= -(-x) = x.$$

This proves Lemma 37.8 **(c)**. □

Proof of Theorem 37.7. Lemma 37.8 **(a)** shows that the map $S^2 : H \to H$ is a k-coalgebra homomorphism.

Lemma 37.8 **(b)** yields $S^2(1_H) = 1_H$.

Moreover, Lemma 37.8 **(c)** shows that

$$S^2(x) = x \qquad \text{for every primitive element } x \text{ of } H.$$

Hence, we can apply Theorem 37.1 to $C = H$ and $f = S^2$.

(a) Theorem 37.1 **(a)** (applied to $C = H$ and $f = S^2$) yields that we have $(\mathrm{id}_H - S^2)^n (H_{\leq n}) = 0$ for every integer $n \geq 1$. This proves Theorem 37.7 **(a)**.

(b) Theorem 37.1 **(b)** (applied to $C = H$ and $f = S^2$) yields that the map S^2 is a k-coalgebra isomorphism. In particular, the map S^2 is invertible. In other words, there exists a map $T : H \to H$ satisfying $S^2 \circ T = \mathrm{id}_H$ and $T \circ S^2 = \mathrm{id}_H$. Consider this map T. We have

$$S \circ (S \circ T) = \underbrace{(S \circ S)}_{=S^2} \circ T = S^2 \circ T = \mathrm{id}_H;$$

therefore, the map S is right-invertible. Also,

$$(T \circ S) \circ S = T \circ \underbrace{(S \circ S)}_{=S^2} = T \circ S^2 = \mathrm{id}_H;$$

therefore, the map S is left-invertible. Any map which is both left-invertible and right-invertible must be invertible. Applying this to the map S, we conclude that the map S is invertible (since we know that the map S is both left-invertible and right-invertible). This proves Theorem 37.7 **(b)**. □

§38. Leray's theorem for the Eulerian idempotent

Our next goal is to prove (one form of) Leray's theorem. We first introduce some notation:

Definition 38.1. Let V be any k-vector space. We use the notation $\operatorname{Sym} V$ for the symmetric algebra of V. For every $n \in \mathbb{N}$, we denote by $\operatorname{Sym}^n V$ the n-th symmetric power of V. Thus, $\operatorname{Sym} V = \bigoplus_{n \in \mathbb{N}} \operatorname{Sym}^n V$. Thus, $\operatorname{Sym}^1 V \subseteq \operatorname{Sym} V$.

There is a canonical injection $V \to \operatorname{Sym} V$ of vector spaces (obtained by composing the canonical isomorphism $V \to \operatorname{Sym}^1 V$ with the canonical inclusion $\operatorname{Sym}^1 V \to \operatorname{Sym} V$). We denote this injection by syminc_V. We will often identify V with a k-vector subspace of $\operatorname{Sym} V$ along this injection (whenever this does not cause misunderstandings).

The universal property of $\operatorname{Sym} V$ says that if A is any commutative k-algebra and if $\varphi : V \to A$ is any k-linear map, then there exists a unique k-algebra homomorphism $\Phi : \operatorname{Sym} V \to A$ satisfying $\Phi \circ \operatorname{syminc}_V = \varphi$. This homomorphism Φ will be denoted by $\operatorname{symlift} \varphi$. It can be explicitly computed by the formula

$$(\operatorname{symlift} \varphi)(v_1 v_2 \cdots v_n) = \varphi(v_1)\,\varphi(v_2) \cdots \varphi(v_n) \qquad (507)$$
$$\text{for any } n \in \mathbb{N} \text{ and } (v_1, v_2, \ldots, v_n) \in V^{\times n}.$$

(Here, $v_1 v_2 \cdots v_n$ denotes the projection of the tensor $v_1 \otimes v_2 \otimes \cdots \otimes v_n \in V^{\otimes n}$ onto the n-th symmetric power $\operatorname{Sym}^n V$, or, equivalently, the product of the elements v_1, v_2, …, v_n of $\operatorname{Sym} V$.)

Theorem 38.2. Let k be a field of characteristic 0. Let H be a connected filtered commutative bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. Let $\mathfrak{e}$ denote the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$.

(a) The map $\mathfrak{e}$ is a projection.

(b) We have $\operatorname{Ker} \mathfrak{e} = (\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H$. [255]

(c) The map $\mathfrak{e}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation.

(d) Let $\mathfrak{j}$ denote the inclusion map $\mathfrak{e}(H) \to H$. Define a map $\mathfrak{e}' : H \to \mathfrak{e}(H)$ by

$$(\mathfrak{e}'(h) = \mathfrak{e}(h) \qquad \text{for every } h \in H).$$

[256] This map $\mathfrak{e}'$ is clearly k-linear[257]. Define a k-linear map $\mathfrak{q} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ by $\mathfrak{q} = \operatorname{syminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'$. Then, the two k-linear maps $\operatorname{symlift} \mathfrak{j} : \operatorname{Sym}(\mathfrak{e}(H)) \to H$ and $e^{*\mathfrak{q}} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ are well-defined k-algebra homomorphisms and mutually inverse.

(e) We have $\operatorname{Sym}(\mathfrak{e}(H)) \cong H$ as k-algebras.

[255] Recall that $(\operatorname{Ker}(\varepsilon_H))^2$ is to be understood according to Convention 15.2. Thus, $(\operatorname{Ker}(\varepsilon_H))^2$ means the subspace $(\operatorname{Ker}(\varepsilon_H)) \cdot (\operatorname{Ker}(\varepsilon_H))$ of H.

[256] This is well-defined, since $\mathfrak{e}(h) \in \mathfrak{e}(H)$ for every $h \in H$.

[257] In fact, this map $\mathfrak{e}'$ is obtained from the k-linear map $\mathfrak{e}$ by changing the target to $\mathfrak{e}(H)$.

Much of Theorem 38.2 has already been proven (e.g., parts **(a)** and **(b)** follow readily from Theorem 15.3). It is part **(d)**, and its consequence part **(e)**, which are the most important for us. Theorem 38.2 **(e)** is more or less a generalization of Theorem 3.8.3 in [Cartie06][258].

Before we step to proving Theorem 38.2, let us show a general fact about convolution:[259]

Proposition 38.3. Let k be a field. Let C be a k-coalgebra. Let A and B be two k-algebras. Let $p : A \to B$ be a k-algebra homomorphism.

(a) We have $p \circ e_{C,A} = e_{C,B}$. (Here, the maps $e_{C,A} : C \to A$ and $e_{C,B} : C \to B$ are defined in the same way as the map $e_{H,A} : H \to A$ in Definition 1.12.)

(b) For every $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$, we have $p \circ (f * g) = (p \circ f) * (p \circ g)$.

(c) For every $f \in \mathcal{L}(C, A)$ and $n \in \mathbb{N}$, we have $p \circ (f^{*n}) = (p \circ f)^{*n}$.

(d) Assume that the field k has characteristic 0. Assume also that C is a connected filtered k-coalgebra. Let $f \in \mathfrak{g}(C, A)$. (See Definition 3.1 for the meaning of $\mathfrak{g}(C, A)$.) Then, $p \circ f \in \mathfrak{g}(C, B)$ and $p \circ e^{*f} = e^{*(p \circ f)}$.

Proof of Proposition 38.3. We know that p is a k-algebra homomorphism if and only if it satisfies $p \circ \eta_A = \eta_B$ and $p \circ \mu_A = \mu_B \circ (p \otimes p)$ (due to the definition of k-algebra homomorphisms using arrows). Thus, p satisfies $p \circ \eta_A = \eta_B$ and $p \circ \mu_A = \mu_B \circ (p \otimes p)$ (since we know that p is a k-algebra homomorphism).

By the definition of $\mathfrak{g}(C, A)$, we have

$$\mathfrak{g}(C, A) = \{f \in \mathcal{L}(C, A) \mid f(1_C) = 0\} = \{h \in \mathcal{L}(C, A) \mid h(1_C) = 0\}$$

(here we renamed f as h). By the definition of $\mathfrak{g}(C, B)$, we have

$$\mathfrak{g}(C, B) = \{f \in \mathcal{L}(C, B) \mid f(1_C) = 0\} = \{h \in \mathcal{L}(C, B) \mid h(1_C) = 0\}$$

(here we renamed f as h).

(a) The definition of $e_{C,A}$ yields $e_{C,A} = \eta_A \circ \varepsilon_C$. The definition of $e_{C,B}$ yields $e_{C,B} = \eta_B \circ \varepsilon_C$. Now, $p \circ \underbrace{e_{C,A}}_{=\eta_A \circ \varepsilon_C} = \underbrace{p \circ \eta_A}_{=\eta_B} \circ \varepsilon_C = \eta_B \circ \varepsilon_C = e_{C,B}$. This proves Proposition 38.3 **(a)**.

[258] It is not exactly a generalization of Theorem 3.8.3 in [Cartie06], since [Cartie06] works with graded k-algebras, and consequently assumes H to be graded and claims $\operatorname{Sym}(\mathfrak{e}(H))$ to be isomorphic to H as **graded** k-algebra. But this can also be easily derived from our Theorem 38.2 **(d)**, since one can easily show that $\mathfrak{e}(H)$ is a homogeneous k-vector subspace of H and that the k-linear map symlift $\mathfrak{j}$ is graded (with the appropriate grading on $\operatorname{Sym}(\mathfrak{e}(H))$).

[259] I have now realized that Proposition 38.3 is just a repetition of parts **(a)**, **(b)**, **(c)** and **(d)** of Proposition 31.2 (with ψ renamed as p).

(b) Let $f \in \mathcal{L}(C, A)$ and $g \in \mathcal{L}(C, A)$. The definition of convolution yields

$$(p \circ f) * (p \circ g) = \mu_B \circ \underbrace{((p \circ f) \otimes (p \circ g))}_{\substack{=(p \otimes p) \circ (f \otimes g) \\ \text{(by (21), applied to } C,\ A,\ B,\ C,\ A,\ B,\ f,\ p,\ g \text{ and } p \\ \text{instead of } U,\ V,\ W,\ U',\ V',\ W',\ \alpha,\ \beta,\ \alpha' \text{ and } \beta')}} \circ \Delta_C$$

$$= \underbrace{\mu_B \circ (p \otimes p)}_{\substack{=p \circ \mu_A \\ (\text{since } p \circ \mu_A = \mu_B \circ (p \otimes p))}} \circ (f \otimes g) \circ \Delta_C = p \circ \underbrace{\mu_A \circ (f \otimes g) \circ \Delta_C}_{\substack{=f * g \\ (\text{since } f * g = \mu_A \circ (f \otimes g) \circ \Delta_C \\ \text{(by the definition of convolution))}}}$$

$$= p \circ (f * g).$$

This proves Proposition 38.3 **(b)**.

(c) Let $f \in \mathcal{L}(C, A)$. We need to show that

$$p \circ (f^{*n}) = (p \circ f)^{*n} \qquad \text{for every } n \in \mathbb{N}. \tag{508}$$

Proof of (508): We shall prove (508) by induction over n:

Induction base: We have $p \circ \underbrace{\left(f^{*0}\right)}_{=e_{C,A}} = p \circ e_{C,A} = e_{C,B}$ (according to Proposition 38.3 **(a)**) and $(p \circ f)^{*0} = e_{C,B}$. Hence, $p \circ (f^{*0}) = e_{C,B} = (p \circ f)^{*0}$. In other words, (508) holds for $n = 0$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that (508) holds for $n = N$. We now need to show that (508) holds for $n = N + 1$.

We know that (508) holds for $n = N$. In other words, we have $p \circ \left(f^{*N}\right) = (p \circ f)^{*N}$. Now,

$$p \circ \underbrace{\left(f^{*(N+1)}\right)}_{=f^{*N} \circ f} = p \circ \left(f^{*N} \circ f\right) = \underbrace{\left(p \circ f^{*N}\right)}_{=(p \circ f)^{*N}} * (p \circ f)$$

$$\left(\text{by Proposition 38.3 } \mathbf{(b)}, \text{ applied to } f^{*N} \text{ and } f \text{ instead of } f \text{ and } g\right)$$

$$= (p \circ f)^{*N} * (p \circ f) = (p \circ f)^{*(N+1)}.$$

In other words, (508) holds for $n = N + 1$. This completes the induction step.

Thus, the induction proof of (508) is complete. In other words, Proposition 38.3 **(c)** is proven.

(d) We have $f \in \mathfrak{g}(C, A) = \{h \in \mathcal{L}(C, A) \mid h(1_C) = 0\}$. In other words, f is an element of $\mathcal{L}(C, A)$ and satisfies $f(1_C) = 0$. Now, $(p \circ f)(1_C) = p\left(\underbrace{f(1_C)}_{=0}\right) = p(0) =$ 0 (since the map p is k-linear). Thus, $p \circ f$ is an element of $\mathcal{L}(C, B)$ and satisfies $(p \circ f)(1_C) = 0$. In other words, $p \circ f \in \{h \in \mathcal{L}(C, B) \mid h(1_C) = 0\} = \mathfrak{g}(C, B)$ (since $\mathfrak{g}(C, B) = \{h \in \mathcal{L}(C, B) \mid h(1_C) = 0\}$). Thus, $e^{*(p \circ f)}$ is a well-defined k-linear map $C \to B$.

Now, let $x \in C$. Then, the definition of $e^{*(p \circ f)}(x)$ yields $e^{*(p \circ f)}(x) = \sum_{i \geq 0} \dfrac{(p \circ f)^{*i}(x)}{i!}$.

On the other hand, the definition of $e^{*f}(x)$ yields

$$e^{*f}(x) = \sum_{i \geq 0} \frac{f^{*i}(x)}{i!} = \sum_{i \geq 0} \frac{1}{i!} f^{*i}(x). \tag{509}$$

Notice that the sum $\sum_{i\geq 0}\frac{1}{i!}f^{*i}(x)$ converges with respect to the discrete topology.

Applying the map p to both sides of the equality (509), we obtain

$$p\left(e^{*f}(x)\right) = p\left(\sum_{i\geq 0}\frac{1}{i!}f^{*i}(x)\right) = \sum_{i\geq 0}\frac{1}{i!}\underbrace{p\left(f^{*i}(x)\right)}_{=(p\circ(f^{*i}))(x)}$$

$$\left(\begin{array}{c}\text{since the map } p \text{ is } k\text{-linear, and since the}\\ \text{sum } \sum_{i\geq 0}\frac{1}{i!}f^{*i}(x) \text{ converges}\\ \text{with respect to the discrete topology}\end{array}\right)$$

$$= \sum_{i\geq 0}\frac{1}{i!}\underbrace{\left(p\circ\left(f^{*i}\right)\right)}_{\substack{=(p\circ f)^{*i}\\ \text{(by Proposition 38.3 (c),}\\ \text{applied to } n=i)}}(x) = \sum_{i\geq 0}\frac{1}{i!}(p\circ f)^{*i}(x) = \sum_{i\geq 0}\frac{(p\circ f)^{*i}(x)}{i!}$$

$$= e^{*(p\circ f)}(x) \qquad \left(\text{since } e^{*(p\circ f)}(x) = \sum_{i\geq 0}\frac{(p\circ f)^{*i}(x)}{i!}\right).$$

Thus, $e^{*(p\circ f)}(x) = p\left(e^{*f}(x)\right) = \left(p\circ e^{*f}\right)(x)$.

Now, let us forget that we fixed x. We thus have shown that $e^{*(p\circ f)}(x) = \left(p\circ e^{*f}\right)(x)$ for every $x\in C$. In other words, $e^{*(p\circ f)} = p\circ e^{*f}$. This proves Proposition 38.3 **(d)**. $\square$

The following proposition neatly complements Proposition 38.3:[260]

Proposition 38.4. Let k be a field of characteristic 0. Let C be a connected filtered k-coalgebra. Let A and B be two k-algebras. Let $p: A\to B$ be a k-algebra homomorphism. Let $F\in G(C,A)$. (See Definition 3.1 for the meaning of $G(C,A)$.) Then, $p\circ F\in G(C,B)$ and $p\circ \operatorname{Log} F = \operatorname{Log}(p\circ F)$.

Proof of Proposition 38.4. By the definition of $G(C,A)$, we have

$$G(C,A) = \{f\in\mathcal{L}(C,A) \mid f(1_C) = 1_A\}.$$

By the definition of $G(C,B)$, we have

$$G(C,B) = \{f\in\mathcal{L}(C,B) \mid f(1_C) = 1_B\}.$$

We have $F\in G(C,A) = \{f\in\mathcal{L}(C,A) \mid f(1_C)=1_A\}$. In other words, F is an element $f\in\mathcal{L}(C,A)$ satisfying $f(1_C)=1_A$. In other words, F is an element of $\mathcal{L}(C,A)$ and satisfies $F(1_C)=1_A$.

But p is a k-algebra homomorphism, and therefore satisfies $p(1_A)=1_B$. Now, $(p\circ F)(1_C) = p\left(\underbrace{F(1_C)}_{=1_A}\right) = p(1_A) = 1_B$. Hence, $p\circ F$ is an element of $\mathcal{L}(C,B)$ and

[260] I have now realized that Proposition 38.4 is just a repetition of Proposition 31.2 **(e)** (with ψ renamed as p).

satisfies $(p \circ F)(1_C) = 1_B$. In other words, $p \circ F$ is an element $f \in \mathcal{L}(C, B)$ satisfying $f(1_C) = 1_B$. In other words,

$$p \circ F \in \{f \in \mathcal{L}(C, B) \mid f(1_C) = 1_B\} = G(C, B)$$

(since $G(C, B) = \{f \in \mathcal{L}(C, B) \mid f(1_C) = 1_B\}$). Thus, $\operatorname{Log}(p \circ F)$ is a well-defined k-linear map $C \to B$.

Consider the maps $e_{C,A} : C \to A$ and $e_{C,B} : C \to B$ that are defined in the same way as the map $e_{H,A} : H \to A$ in Definition 1.12.

The definition of $\operatorname{Log}(p \circ F)$ yields $\operatorname{Log}(p \circ F) = \operatorname{Log}_1(p \circ F - e_{C,B})$. Thus, $\operatorname{Log}_1(p \circ F - e_{C,B})$ is well-defined; hence, $p \circ F - e_{C,B} \in \mathfrak{g}(C, B)$ (since $\operatorname{Log}_1 f$ is well-defined for an $f \in \mathcal{L}(C, B)$ only when $f \in \mathfrak{g}(C, B)$).

The definition of $\operatorname{Log} F$ yields $\operatorname{Log} F = \operatorname{Log}_1(F - e_{C,A})$. Thus, $\operatorname{Log}_1(F - e_{C,A})$ is well-defined; hence, $F - e_{C,A} \in \mathfrak{g}(C, A)$ (since $\operatorname{Log}_1 f$ is well-defined for an $f \in \mathcal{L}(C, A)$ only when $f \in \mathfrak{g}(C, A)$).

Define an $f \in \mathcal{L}(C, A)$ by $f = F - e_{C,A}$. Then, $f = F - e_{C,A} \in \mathfrak{g}(C, A)$. Also,

$$\begin{aligned} p \circ \underbrace{f}_{=F-e_{C,A}} &= p \circ (F - e_{C,A}) = p \circ F - \underbrace{p \circ e_{C,A}}_{\substack{=e_{C,B} \\ \text{(by Proposition 38.3 (a))}}} = p \circ F - e_{C,B} \\ &\in \mathfrak{g}(C, B). \end{aligned}$$

Now let $x \in C$. Then, the definition of $\operatorname{Log}_1 f$ yields

$$(\operatorname{Log}_1 f)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) \qquad (\text{since } f \in \mathfrak{g}(C, A)). \tag{510}$$

In particular, the sum $\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ converges with respect to the discrete topology. Applying the map p to both sides of the equality (510), we find

$$p((\operatorname{Log}_1 f)(x)) = p\left(\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)\right) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} p\left(f^{*i}(x)\right) \tag{511}$$

(since the map p is k-linear, and since the sum $\sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x)$ converges with respect to the discrete topology). Also, the definition of $\operatorname{Log}_1(p \circ f)$ yields

$$\begin{aligned} (\operatorname{Log}_1(p \circ f))(x) &= \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} \underbrace{(p \circ f)^{*i}}_{\substack{=p \circ \left(f^{*i}\right) \\ \left(\text{since } p \circ \left(f^{*i}\right) = (p \circ f)^{*i} \text{ (by Proposition 38.3 (c), applied to } n=i\right)\right)}} (x) \qquad (\text{since } p \circ f \in \mathfrak{g}(C, B)) \\ &= \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} \underbrace{\left(p \circ \left(f^{*i}\right)\right)(x)}_{=p(f^{*i}(x))} = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} p\left(f^{*i}(x)\right) \\ &= p((\operatorname{Log}_1 f)(x)) \qquad (\text{by (511)}) \\ &= (p \circ (\operatorname{Log}_1 f))(x). \end{aligned}$$

Now, forget that we fixed x. We thus have shown that $\left(\operatorname{Log}_1\left(p\circ f\right)\right)(x) = \left(p\circ\left(\operatorname{Log}_1 f\right)\right)(x)$ for each $x\in C$. In other words, $\operatorname{Log}_1\left(p\circ f\right) = p\circ\left(\operatorname{Log}_1 f\right)$. Hence, $p\circ\left(\operatorname{Log}_1 f\right) = \operatorname{Log}_1\left(p\circ f\right)$. But

$$p\circ\left(\underbrace{\operatorname{Log} F}_{=\operatorname{Log}_1\left(F-e_{C,A}\right)}\right) = p\circ\left(\operatorname{Log}_1\left(\underbrace{F-e_{C,A}}_{=f}\right)\right) = p\circ\left(\operatorname{Log}_1 f\right) = \operatorname{Log}_1\left(\underbrace{p\circ f}_{=p\circ F-e_{C,B}}\right)$$
$$= \operatorname{Log}_1\left(p\circ F-e_{C,B}\right) = \operatorname{Log}\left(p\circ F\right)$$

(since we have shown that $\operatorname{Log}\left(p\circ F\right) = \operatorname{Log}_1\left(p\circ F-e_{C,B}\right)$). This completes the proof of Proposition 38.4 (since $p\circ F\in G\left(C,B\right)$ has already been shown). □

The next proposition can be regarded as an addendum to Proposition 17.8:

Proposition 38.5. Let k be a field of characteristic 0. Let C be a connected filtered k-coalgebra. Let A be a filtered k-algebra.

Let $F\in G\left(C,A\right)$ be a k-linear map respecting the filtration. Then, the k-linear map $\operatorname{Log} F$ also respects the filtration.

Proof of Proposition 38.5. We know that the map F respects the filtration. In other words,

$$F\left(C_{\leq n}\right)\subseteq A_{\leq n} \qquad \text{for each } n\in\mathbb{N}. \tag{512}$$

On the other hand, Proposition 17.8 **(a)** shows that the map $e_{C,A}: C\to A$ respects the filtration. In other words,

$$e_{C,A}\left(C_{\leq n}\right)\subseteq A_{\leq n} \qquad \text{for each } n\in\mathbb{N}. \tag{513}$$

The definition of $\operatorname{Log} F$ yields $\operatorname{Log} F = \operatorname{Log}_1\left(F-e_{C,A}\right)$. In particular, $\operatorname{Log}_1\left(F-e_{C,A}\right)$ is well-defined; thus, $F-e_{C,A}\in\mathfrak{g}\left(C,A\right)$ (since $\operatorname{Log}_1 f$ is well-defined for an $f\in\mathcal{L}\left(C,A\right)$ only when $f\in\mathfrak{g}\left(C,A\right)$). Thus, we can define a k-linear map $f\in\mathfrak{g}\left(C,A\right)$ by $f = F-e_{C,A}$. Consider this f. We have $\operatorname{Log} F = \operatorname{Log}_1\underbrace{\left(F-e_{C,A}\right)}_{=f} = \operatorname{Log}_1 f$.

We have $f\left(C_{\leq n}\right)\subseteq A_{\leq n}$ for each $n\in\mathbb{N}$ [261]. In other words, the map $f: C\to A$ respects the filtration.

Now, fix $i\in\mathbb{N}$. Thus, i is a nonnegative integer. Recall that the map $f: C\to A$ respects the filtration. Hence, Proposition 17.8 **(c)** (applied to $n=i$) shows that f^{*i} also respects the filtration. In other words,

$$f^{*i}\left(C_{\leq n}\right)\subseteq A_{\leq n} \qquad \text{for each } n\in\mathbb{N}. \tag{514}$$

[261] *Proof.* Let $n\in\mathbb{N}$. Then,

$$\underbrace{f}_{=F-e_{C,A}}\left(C_{\leq n}\right) = \left(F-e_{C,A}\right)\left(C_{\leq n}\right)\subseteq \underbrace{F\left(C_{\leq n}\right)}_{\substack{\subseteq A_{\leq n}\\ \text{(by (512))}}} - \underbrace{e_{C,A}\left(C_{\leq n}\right)}_{\substack{\subseteq A_{\leq n}\\ \text{(by (513))}}}\subseteq A_{\leq n}-A_{\leq n}$$
$$\subseteq A_{\leq n} \qquad \left(\text{since } A_{\leq n} \text{ is a } k\text{-vector space}\right).$$

Qed.

Now, forget that we fixed i. We thus have proven (514) for each $i \in \mathbb{N}$.

Fix $n \in \mathbb{N}$. Let $x \in C_{\leq n}$. Then, each integer $i > n$ satisfies

$$f^{*i}(x) = 0 \tag{515}$$

[262]. Now,

$$\begin{aligned}
\underbrace{(\operatorname{Log} F)}_{=\operatorname{Log}_1 f}(x) &= (\operatorname{Log}_1 f)(x) = \sum_{i \geq 1} \frac{(-1)^{i-1}}{i} f^{*i}(x) \qquad \text{(by (8))} \\
&= \underbrace{\sum_{\substack{i \geq 1; \\ i \leq n}}}_{=\sum_{i=1}^{n}} \frac{(-1)^{i-1}}{i} f^{*i}\left(\underbrace{x}_{\in C_{\leq n}}\right) + \sum_{\substack{i \geq 1; \\ i > n}} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(x)}_{\substack{=0 \\ \text{(by (515))}}} \\
&\in \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} f^{*i}(C_{\leq n}) + \underbrace{\sum_{\substack{i \geq 1; \\ i > n}} \frac{(-1)^{i-1}}{i} 0}_{=0} = \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} \underbrace{f^{*i}(C_{\leq n})}_{\substack{\subseteq A_{\leq n} \\ \text{(by (514))}}} \\
&\subseteq \sum_{i=1}^{n} \frac{(-1)^{i-1}}{i} A_{\leq n} \subseteq A_{\leq n} \qquad \text{(since } A_{\leq n} \text{ is a } k\text{-vector space)}.
\end{aligned}$$

Now, forget that we fixed x. We thus have proven that $(\operatorname{Log} F)(x) \in A_{\leq n}$ for each $x \in C_{\leq n}$. In other words, $(\operatorname{Log} F)(C_{\leq n}) \subseteq A_{\leq n}$.

Now, forget that we fixed n. We thus have shown that $(\operatorname{Log} F)(C_{\leq n}) \subseteq A_{\leq n}$ for each $n \in \mathbb{N}$. In other words, the map $\operatorname{Log} F$ respects the filtration. This proves Proposition 38.5. □

Proposition 38.6. Let k be a field of characteristic 0. Let H be a connected filtered commutative bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. Let $\mathfrak{e}$ denote the map $\operatorname{Log} \mathrm{id} \in \mathcal{L}(H, H)$.

(a) We have $\mathrm{id}^{*n} \circ \mathfrak{e} = n\mathfrak{e}$ for each $n \in \mathbb{N}$.

(b) We have $\mathfrak{e}^{*n} \circ \mathfrak{e} = \delta_{n,1}\mathfrak{e}$ for each $n \in \mathbb{N}$. Here, we are using the *Kronecker delta notation* (i.e., whenever u and v are two objects, we set $\delta_{u,v} = \begin{cases} 1, & \text{if } u = v; \\ 0, & \text{if } u \neq v \end{cases}$).

Proof of Proposition 38.6. Recall that $\operatorname{Log} F \in \mathfrak{g}(H, H)$ for each $F \in G(H, H)$ (by the definition of $\operatorname{Log} F$). Applying this to $F = \mathrm{id}$, we obtain $\operatorname{Log} \mathrm{id} \in \mathfrak{g}(H, H)$. Thus, $\mathfrak{e} = \operatorname{Log} \mathrm{id} \in \mathfrak{g}(H, H)$. Hence, $\mathfrak{e}(1_H) = 0$ [263].

[262] *Proof of (515):* Let $i > n$ be an integer. Then, Remark 3.5 (applied to $H = C$) yields $f^{*i}(C_{\leq n}) = 0$ (since $i > n$). But from $x \in C_{\leq n}$, we obtain $f^{*i}(x) \in f^{*i}(C_{\leq n}) = 0$, thus $f^{*i}(x) = 0$. This proves (515).

[263] *Proof.* We have $\mathfrak{e} \in \mathfrak{g}(H, H) = \{f \in \mathcal{L}(H, H) \mid f(1_H) = 0\}$ (by the definition of $\mathfrak{g}(H, H)$). In other words, $\mathfrak{e}$ is an element $f \in \mathcal{L}(H, H)$ satisfying $f(1_H) = 0$. In other words, $\mathfrak{e}$ is an element of $\mathcal{L}(H, H)$ and satisfies $\mathfrak{e}(1_H) = 0$. Qed.

Proposition 5.13 **(b)** (applied to $A = H$ and $F = \mathrm{id}$) yields $e^{*(\operatorname{Log}\mathrm{id})} = \mathrm{id}$. Since $\mathfrak{e} = \operatorname{Log}\mathrm{id}$, this rewrites as $e^{*\mathfrak{e}} = \mathrm{id}$.

(a) Let $n \in \mathbb{N}$. Clearly, $\mathrm{id} : H \to H$ is a k-algebra homomorphism. Hence, Corollary 15.16 (applied to $A = H$ and $f = \mathrm{id}$) shows that $\mathrm{id}^{*n} : H \to H$ is a k-algebra homomorphism.

Also, $\mathrm{id} : H \to H$ is an element of $G(H, H)$.

But H is a connected filtered k-coalgebra (since H is a connected filtered bialgebra over k). Hence, Proposition 38.4 (applied to $C = H$, $A = H$, $B = H$, $p = \mathrm{id}^{*n}$ and $F = \mathrm{id}$) shows that $\mathrm{id}^{*n} \circ \mathrm{id} \in G(H, H)$ and $\mathrm{id}^{*n} \circ \operatorname{Log}\mathrm{id} = \operatorname{Log}(\mathrm{id}^{*n} \circ \mathrm{id})$. Thus,

$$\mathrm{id}^{*n} \circ \underbrace{\mathfrak{e}}_{=\operatorname{Log}\mathrm{id}} = \mathrm{id}^{*n} \circ \operatorname{Log}\mathrm{id} = \operatorname{Log}\left(\underbrace{\mathrm{id}^{*n} \circ \mathrm{id}}_{=\mathrm{id}^{*n}}\right) = \operatorname{Log}\left(\mathrm{id}^{*n}\right). \tag{516}$$

On the other hand, $n \underbrace{\mathfrak{e}}_{\in \mathfrak{g}(H,H)} \in n\mathfrak{g}(H, H) \subseteq \mathfrak{g}(H, H)$ (since $\mathfrak{g}(H, H)$ is a k-vector space).

Recall that $\mathfrak{e} \in \mathfrak{g}(H, H)$. Thus, Corollary 11.4 (applied to $C = H$ and $f = \mathfrak{e}$) yields $e^{*(n\mathfrak{e})} = (e^{*\mathfrak{e}})^{*n} = \mathrm{id}^{*n}$ (since $e^{*\mathfrak{e}} = \mathrm{id}$). Thus, $\operatorname{Log}\left(\underbrace{e^{*(n\mathfrak{e})}}_{=\mathrm{id}^{*n}}\right) = \operatorname{Log}\left(\mathrm{id}^{*n}\right) = \mathrm{id}^{*n} \circ \mathfrak{e}$ (by (516)). But Proposition 5.13 **(a)** (applied to $A = H$ and $f = n\mathfrak{e}$) yields $\operatorname{Log}\left(e^{*(n\mathfrak{e})}\right) = n\mathfrak{e}$ (since $n\mathfrak{e} \in \mathfrak{g}(H, H)$). Comparing this with $\operatorname{Log}\left(e^{*(n\mathfrak{e})}\right) = \mathrm{id}^{*n} \circ \mathfrak{e}$, we obtain $\mathrm{id}^{*n} \circ \mathfrak{e} = n\mathfrak{e}$. This proves Proposition 38.6 **(a)**.

(b) For each $n \in \mathbb{N}$, we define a k-linear map $g_n : H \to H$ by $g_n = \mathfrak{e}^{*n} \circ \mathfrak{e} - \delta_{n,1}\mathfrak{e}$. Then, $g_n(H_{\leq n-1}) = 0$ for each $n \in \mathbb{N}$ [264].

For each $n \in \mathbb{N}$, define a k-linear map $h_n : H \to H$ by $h_n = \dfrac{1}{n!} g_n$. Then,

---

[264] *Proof.* Let $n \in \mathbb{N}$. We must show that $g_n(H_{\leq n-1}) = 0$.

We have $n \in \mathbb{N}$. Hence, we are in one of the following three cases:

Case 1: We have $n = 0$.

Case 2: We have $n = 1$.

Case 3: We have $n > 1$.

Let us first consider Case 1. In this case, we have $n = 0$. Thus, $H_{\leq n-1} = H_{\leq 0-1} = H_{\leq -1} = 0$. Hence, $g_n\left(\underbrace{H_{\leq n-1}}_{=0}\right) = g_n(0) = 0$ (since the map g_n is k-linear). Thus, $g_n(H_{\leq n-1}) = 0$ is proven in Case 1.

Let us now consider Case 2. In this case, we have $n = 1$. Thus, $H_{\leq n-1} = H_{\leq 1-1} = H_{\leq 0}$.

But the filtered k-bialgebra H is connected if and only if $H_{\leq 0} = k \cdot 1_H$ (by Remark 2.12). Thus, $H_{\leq 0} = k \cdot 1_H$ (since the k-bialgebra H is connected). Hence, $H_{\leq n-1} = H_{\leq 0} = k \cdot 1_H$.

Now,

$$\underbrace{g_n}_{=\mathfrak{e}^{*n}\circ\mathfrak{e}-\delta_{n,1}\circ\mathfrak{e}}(1_H) = \left(\mathfrak{e}^{*n} \circ \mathfrak{e} - \delta_{n,1} \circ \mathfrak{e}\right)(1_H) = \underbrace{\left(\mathfrak{e}^{*n} \circ \mathfrak{e}\right)(1_H)}_{=\mathfrak{e}^{*n}(\mathfrak{e}(1_H))} - \delta_{n,1}\underbrace{\mathfrak{e}(1_H)}_{=0}$$

$$= \mathfrak{e}^{*n}(\mathfrak{e}(1_H)) - \underbrace{\delta_{n,1}0}_{=0} = \mathfrak{e}^{*n}\left(\underbrace{\mathfrak{e}(1_H)}_{=0}\right) = \mathfrak{e}^{*n}(0) = 0$$

$h_n\left(H_{\leq n-1}\right) = 0$ for each $n \in \mathbb{N}$ [265].

For each $i \in \mathbb{N}$, we have

$$h_i = \frac{1}{i!} \underbrace{g_i}_{\substack{=\mathfrak{e}^{*i}\circ\mathfrak{e}-\delta_{i,1}\mathfrak{e} \\ \text{(by the definition of } g_i\text{)}}} \qquad \text{(by the definition of } h_i\text{)}$$

$$= \frac{1}{i!}\left(\mathfrak{e}^{*i}\circ\mathfrak{e} - \delta_{i,1}\mathfrak{e}\right). \tag{517}$$

Now, let $t \in \mathbb{N}$. Recall that $\mathfrak{e} \in \mathfrak{g}\left(H,H\right)$. Thus, Corollary 11.4 (applied to $C = H$, $n = t$ and $f = \mathfrak{e}$) yields $e^{*(t\mathfrak{e})} = \left(e^{*\mathfrak{e}}\right)^{*t} = \mathrm{id}^{*t}$ (since $e^{*\mathfrak{e}} = \mathrm{id}$).

On the other hand, $t \underbrace{\mathfrak{e}}_{\in\mathfrak{g}(H,H)} \in t\mathfrak{g}\left(H,H\right) \subseteq \mathfrak{g}\left(H,H\right)$ (since $\mathfrak{g}\left(H,H\right)$ is a k-vector space).

Let $x \in H$. Set $y = \mathfrak{e}\left(x\right)$. Proposition 38.6 **(a)** (applied to $n = t$) yields $\mathrm{id}^{*t}\circ\mathfrak{e} = t\mathfrak{e}$. Thus,

$$\left(\mathrm{id}^{*t}\circ\mathfrak{e}\right)\left(x\right) = \left(t\mathfrak{e}\right)\left(x\right) = t\underbrace{\mathfrak{e}\left(x\right)}_{=y} = ty,$$

(since the map $\mathfrak{e}^{*n}$ is k-linear). Finally,

$$g_n\left(\underbrace{H_{\leq n-1}}_{=k\cdot 1_H}\right) = g_n\left(k\cdot 1_H\right) = k\cdot\underbrace{g_n\left(1_H\right)}_{=0} \qquad \text{(since the map } g_n \text{ is } k\text{-linear)}$$

$$= 0.$$

Thus, $g_n\left(H_{\leq n-1}\right) = 0$ is proven in Case 2.

Let us finally consider Case 3. In this case, we have $n > 1$. Thus, $n \geq 2$ (since $n \in \mathbb{N}$), so that $n-1 \geq 1$ and thus $n-1 \in \mathbb{N}$. Now, Remark 3.5 (applied to H, n, $n-1$ and $\mathfrak{e}$ instead of A, i, n and f) shows that $\mathfrak{e}^{*n}\left(H_{\leq n-1}\right) = 0$ (since $\mathfrak{e} \in \mathfrak{g}\left(H,H\right)$ and $n > n-1$). Also, $n \neq 1$ (since $n > 1$) and thus $\delta_{n,1} = 0$.

Furthermore, the map $\mathrm{id} \in G\left(H,H\right)$ is a k-linear map respecting the filtration. Hence, Proposition 38.5 (applied to $C = H$, $A = H$ and $F = \mathrm{id}$) shows that the k-linear map $\mathrm{Log}\,\mathrm{id}$ also respects the filtration. In other words, the k-linear map $\mathfrak{e}$ respects the filtration (since $\mathfrak{e} = \mathrm{Log}\,\mathrm{id}$). In other words, $\mathfrak{e}\left(H_{\leq m}\right) \subseteq H_{\leq m}$ for each $m \in \mathbb{N}$. Applying this to $m = n-1$, we find $\mathfrak{e}\left(H_{\leq n-1}\right) \subseteq H_{\leq n-1}$.

Now,

$$\underbrace{g_n}_{=\mathfrak{e}^{*n}\circ\mathfrak{e}-\delta_{n,1}\circ\mathfrak{e}}\left(H_{\leq n-1}\right) = \left(\mathfrak{e}^{*n}\circ\mathfrak{e} - \delta_{n,1}\circ\mathfrak{e}\right)\left(H_{\leq n-1}\right) \subseteq \underbrace{\left(\mathfrak{e}^{*n}\circ\mathfrak{e}\right)\left(H_{\leq n-1}\right)}_{=\mathfrak{e}^{*n}\left(\mathfrak{e}\left(H_{\leq n-1}\right)\right)} - \underbrace{\left(\delta_{n,1}\circ\mathfrak{e}\right)\left(H_{\leq n-1}\right)}_{=\delta_{n,1}\mathfrak{e}\left(H_{\leq n-1}\right)}$$

$$= \mathfrak{e}^{*n}\left(\underbrace{\mathfrak{e}\left(H_{\leq n-1}\right)}_{\subseteq H_{\leq n-1}}\right) - \underbrace{\delta_{n,1}}_{=0}\mathfrak{e}\left(H_{\leq n-1}\right) \subseteq \underbrace{\mathfrak{e}^{*n}\left(H_{\leq n-1}\right)}_{=0} - \underbrace{0\mathfrak{e}\left(H_{\leq n-1}\right)}_{=0} = 0 - 0 = 0.$$

Thus, $g_n\left(H_{\leq n-1}\right) = 0$ is proven in Case 3.

We have now proven $g_n\left(H_{\leq n-1}\right) = 0$ in all three Cases 1, 2 and 3. Since these three Cases cover all possibilities, we therefore conclude that $g_n\left(H_{\leq n-1}\right) = 0$ always holds. Qed.

[265] *Proof.* We have previously shown that $g_n\left(H_{\leq n-1}\right) = 0$ for each $n \in \mathbb{N}$. Now, for each $n \in \mathbb{N}$, we have

$$\underbrace{h_n}_{=\frac{1}{n!}g_n}\left(H_{\leq n-1}\right) = \left(\frac{1}{n!}g_n\right)\left(H_{\leq n-1}\right) = \frac{1}{n!}\underbrace{g_n\left(H_{\leq n-1}\right)}_{=0} = 0.$$

Qed.

so that

$$\begin{aligned} ty &= \left(\mathrm{id}^{*t} \circ \mathfrak{e}\right)(x) = \underbrace{\mathrm{id}^{*t}}_{=e^{*(t\mathfrak{e})}}\left(\underbrace{\mathfrak{e}(x)}_{=y}\right) = e^{*(t\mathfrak{e})}(y) \\ &= \sum_{i\geq 0} \frac{(t\mathfrak{e})^{*i}(y)}{i!} \qquad \text{(by (6), applied to } t\mathfrak{e} \text{ and } y \text{ instead of } f \text{ and } x\text{)} \\ &= \sum_{i\geq 0} \frac{1}{i!} \underbrace{(t\mathfrak{e})^{*i}}_{=t^i\mathfrak{e}^{*i}}(y) = \sum_{i\geq 0} \frac{1}{i!} \underbrace{\left(t^i\mathfrak{e}^{*i}\right)(y)}_{=t^i\mathfrak{e}^{*i}(y)} = \sum_{i\geq 0} \frac{1}{i!} t^i \mathfrak{e}^{*i}\left(\underbrace{y}_{=\mathfrak{e}(x)}\right) \\ &= \sum_{i\geq 0} \frac{1}{i!} t^i \underbrace{\mathfrak{e}^{*i}(\mathfrak{e}(x))}_{=(\mathfrak{e}^{*i}\circ\mathfrak{e})(x)} = \sum_{i\geq 0} \frac{1}{i!} t^i \left(\mathfrak{e}^{*i} \circ \mathfrak{e}\right)(x). \end{aligned} \tag{518}$$

On the other hand, all but finitely many $i \in \mathbb{N}$ satisfy $\frac{1}{i!}t^i\delta_{i,1}\mathfrak{e}(x) = 0$ [266]. Hence, the infinite sum $\sum_{i\geq 0} \frac{1}{i!}t^i\delta_{i,1}\mathfrak{e}(x)$ converges. This infinite sum rewrites as follows:

$$\begin{aligned} \sum_{i\geq 0} \frac{1}{i!}t^i\delta_{i,1}\mathfrak{e}(x) &= \sum_{\substack{i\geq 0;\\ i\neq 1}} \frac{1}{i!}t^i \underbrace{\delta_{i,1}}_{\substack{=0\\ (\text{since } i\neq 1)}} \mathfrak{e}(x) + \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1} \underbrace{t^1}_{=t} \underbrace{\delta_{1,1}}_{\substack{=1\\ (\text{since } 1=1)}} \underbrace{\mathfrak{e}(x)}_{=y} \\ &\qquad \text{(here, we have split off the addend for } i=1 \text{ from the sum)} \\ &= \underbrace{\sum_{\substack{i\geq 0;\\ i\neq 1}} \frac{1}{i!}t^i 0\mathfrak{e}(x)}_{=0} + ty = ty \\ &= \sum_{i\geq 0} \frac{1}{i!}t^i \left(\mathfrak{e}^{*i} \circ \mathfrak{e}\right)(x) \qquad \text{(by (518))}. \end{aligned}$$

[266] *Proof.* Each $i \in \mathbb{N}$ satisfying $i \neq 1$ satisfies $\frac{1}{i!}t^i \underbrace{\delta_{i,1}}_{\substack{=0\\ (\text{since } i\neq 1)}} \mathfrak{e}(x) = 0$. Hence, all but finitely many $i \in \mathbb{N}$ satisfy $\frac{1}{i!}t^i\delta_{i,1}\mathfrak{e}(x) = 0$ (since all but finitely many $i \in \mathbb{N}$ satisfy $i \neq 1$).

Hence,

$$0 = \sum_{i\geq 0} \frac{1}{i!} t^i \left(\mathfrak{e}^{*i} \circ \mathfrak{e}\right)(x) - \sum_{i\geq 0} \frac{1}{i!} t^i \delta_{i,1} \mathfrak{e}(x) = \sum_{i\geq 0} \underbrace{\frac{1}{i!} t^i}_{= t^i \cdot \frac{1}{i!}} \underbrace{\left(\left(\mathfrak{e}^{*i} \circ \mathfrak{e}\right)(x) - \delta_{i,1}\mathfrak{e}(x)\right)}_{= (\mathfrak{e}^{*i} \circ \mathfrak{e} - \delta_{i,1}\mathfrak{e})(x)}$$

$$= \sum_{i\geq 0} t^i \cdot \underbrace{\frac{1}{i!}\left(\mathfrak{e}^{*i} \circ \mathfrak{e} - \delta_{i,1}\mathfrak{e}\right)(x)}_{= \left(\frac{1}{i!}(\mathfrak{e}^{*i} \circ \mathfrak{e} - \delta_{i,1}\mathfrak{e})\right)(x)} = \sum_{i\geq 0} t^i \cdot \underbrace{\left(\frac{1}{i!}\left(\mathfrak{e}^{*i} \circ \mathfrak{e} - \delta_{i,1}\mathfrak{e}\right)\right)}_{= h_i \text{ (by (517))}}(x)$$

$$= \sum_{i\geq 0} t^i h_i(x).$$

In other words, $\sum_{i\geq 0} t^i h_i(x) = 0$.

Now, forget that we fixed x and t. We thus have shown that every $x \in H$ and every $t \in \mathbb{N}$ satisfy $\sum_{i\geq 0} t^i h_i(x) = 0$. Hence, Proposition 12.1 **(b)** shows that

$$h_n = 0 \qquad \text{for every } n \in \mathbb{N} \tag{519}$$

(since we already have proven that $h_n(H_{\leq n-1}) = 0$ for each $n \in \mathbb{N}$).

Now, fix $n \in \mathbb{N}$. From (519), we obtain $h_n = 0$. But the definition of h_n yields $h_n = \frac{1}{n!} g_n$, so that $g_n = n! \underbrace{h_n}_{=0} = 0$. Furthermore, the definition of g_n yields $g_n = \mathfrak{e}^{*n} \circ \mathfrak{e} - \delta_{n,1}\mathfrak{e}$, so that $\mathfrak{e}^{*n} \circ \mathfrak{e} - \delta_{n,1}\mathfrak{e} = g_n = 0$, and thus $\mathfrak{e}^{*n} \circ \mathfrak{e} = \delta_{n,1}\mathfrak{e}$. This proves Proposition 38.6 **(b)**. □

Proposition 38.7. Let k be a field of characteristic 0. Let H be a connected filtered bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. Let $\mathfrak{e}$ denote the map $\operatorname{Log}\operatorname{id} \in \mathcal{L}(H, H)$. Then, the image $\mathfrak{e}(H)$ generates the k-algebra H.

Proof of Proposition 38.7. Let $\mathfrak{E}$ be the k-vector subspace $\mathfrak{e}(H)$ of H.

Recall Convention 16.19. For every $\ell \in \mathbb{N}$, Proposition 17.4 yields

$$H_{\leq \ell} \subseteq \sum_{i=0}^{\ell} \underbrace{\mathfrak{E}^i}_{\subseteq \operatorname{AlgGen}_k \mathfrak{E}} \subseteq \sum_{i=0}^{\ell} \operatorname{AlgGen}_k \mathfrak{E} \subseteq \operatorname{AlgGen}_k \mathfrak{E}$$

(since $\operatorname{AlgGen}_k \mathfrak{E}$ is a k-vector space). Since H is filtered, we have

$$H = \bigcup_{\ell \in \mathbb{N}} \underbrace{H_{\leq \ell}}_{\subseteq \operatorname{AlgGen}_k \mathfrak{E}} \subseteq \bigcup_{\ell \in \mathbb{N}} \operatorname{AlgGen}_k \mathfrak{E} = \operatorname{AlgGen}_k \mathfrak{E}.$$

Combined with $\operatorname{AlgGen}_k \mathfrak{E} \subseteq H$ (which is trivial), this yields $H = \operatorname{AlgGen}_k \mathfrak{E}$. In other words, H is the k-subalgebra of H generated by $\mathfrak{E}$ (since $\operatorname{AlgGen}_k \mathfrak{E}$ is the k-subalgebra of H generated by $\mathfrak{E}$). In other words, the subset $\mathfrak{E}$ of H generates the k-algebra H. Since $\mathfrak{E} = \mathfrak{e}(H)$, this rewrites as follows: The subset $\mathfrak{e}(H)$ of H generates the k-algebra H. This proves Proposition 38.7. □

Lemma 38.8. Let k be a field. Let V be any k-vector space. Recall the notations introduced in Definition 38.1.

Let A be a commutative k-algebra. Let $\varphi : V \to A$ be a k-linear map.

(a) If the image $\varphi(V)$ generates the k-algebra A, then the k-algebra homomorphism $\operatorname{symlift}\varphi : \operatorname{Sym} V \to A$ is surjective.

(b) Let $\rho : A \to \operatorname{Sym} V$ be a k-algebra homomorphism such that $\rho \circ \varphi = \operatorname{syminc}_V$. Then, $\rho \circ (\operatorname{symlift}\varphi) = \operatorname{id}_{\operatorname{Sym} V}$.

(c) Let $\rho : A \to \operatorname{Sym} V$ be a k-algebra homomorphism such that $\rho \circ \varphi = \operatorname{syminc}_V$. Assume furthermore that the image $\varphi(V)$ generates the k-algebra A. Then, the two k-algebra homomorphisms $\operatorname{symlift}\varphi : \operatorname{Sym} V \to A$ and $\rho : A \to \operatorname{Sym} V$ are mutually inverse.

Proof of Lemma 38.8. Recall that $\operatorname{symlift}\varphi$ is the unique k-algebra homomorphism $\Phi : \operatorname{Sym} V \to A$ satisfying $\Phi \circ \operatorname{syminc}_V = \varphi$. Hence, $\operatorname{symlift}\varphi$ is a k-algebra homomorphism $\operatorname{Sym} V \to A$ and satisfies $(\operatorname{symlift}\varphi) \circ \operatorname{syminc}_V = \varphi$.

(a) Assume that the image $\varphi(V)$ generates the k-algebra A. In other words, the k-subalgebra of A generated by $\varphi(V)$ is A.

Let S denote the image $\varphi(V)$.

Recall that the k-subalgebra of A generated by $\varphi(V)$ is A. In other words, the k-subalgebra of A generated by S is A (since $S = \varphi(V)$). In other words, A is the k-subalgebra of A generated by S. In other words, A is the smallest k-subalgebra of A which contains S as a subset (because the k-subalgebra of A generated by S is the smallest k-subalgebra of A which contains S as a subset). Hence,

$$\left(\begin{array}{c} \text{whenever } U \text{ is a } k\text{-subalgebra of } A \text{ which contains } S \text{ as} \\ \text{a subset, we must necessarily have } A \subseteq U \end{array} \right). \tag{520}$$

But the map $\operatorname{symlift}\varphi : \operatorname{Sym} V \to A$ is a k-algebra homomorphism. Thus, its image $(\operatorname{symlift}\varphi)(\operatorname{Sym} V)$ is a k-subalgebra of A. Furthermore, this k-subalgebra $(\operatorname{symlift}\varphi)(\operatorname{Sym} V)$ contains S as a subset[267]. Hence, (520) (applied to $U = (\operatorname{symlift}\varphi)(\operatorname{Sym} V)$) shows that $A \subseteq (\operatorname{symlift}\varphi)(\operatorname{Sym} V)$. Combined with $(\operatorname{symlift}\varphi)(\operatorname{Sym} V) \subseteq A$ (which is obvious), this yields $A = (\operatorname{symlift}\varphi)(\operatorname{Sym} V)$. In other words, the map $\operatorname{symlift}\varphi$ is surjective. This proves Lemma 38.8 **(a)**.

(b) The k-algebra $\operatorname{Sym} V$ is commutative, and the map $\operatorname{syminc}_V : V \to \operatorname{Sym} V$ is a k-linear map. Hence, a k-algebra homomorphism $\operatorname{symlift}(\operatorname{syminc}_V) : \operatorname{Sym} V \to \operatorname{Sym} V$ is well-defined. The definition of this homomorphism shows that $\operatorname{symlift}(\operatorname{syminc}_V)$ is the unique k-algebra homomorphism $\Phi : \operatorname{Sym} V \to \operatorname{Sym} V$ satisfying $\Phi \circ \operatorname{syminc}_V = \operatorname{syminc}_V$. In particular, this shows that there exists **at most one** k-algebra homomorphism $\Phi : \operatorname{Sym} V \to \operatorname{Sym} V$ satisfying $\Phi \circ \operatorname{syminc}_V = \operatorname{syminc}_V$ (namely, the

[267] *Proof.* We have

$$S = \underbrace{\varphi}_{=(\operatorname{symlift}\varphi)\circ\operatorname{syminc}_V}(V) = ((\operatorname{symlift}\varphi)\circ\operatorname{syminc}_V)(V) = (\operatorname{symlift}\varphi)\left(\underbrace{\operatorname{syminc}_V(V)}_{\subseteq \operatorname{Sym} V}\right) \subseteq (\operatorname{symlift}\varphi)(\operatorname{Sym} V).$$

In other words, $(\operatorname{symlift}\varphi)(\operatorname{Sym} V)$ contains S as a subset.

homomorphism symlift $(\operatorname{syminc}_V)$). In other words, if Φ_1 and Φ_2 are two k-algebra homomorphisms $\Phi : \operatorname{Sym} V \to \operatorname{Sym} V$ satisfying $\Phi \circ \operatorname{syminc}_V = \operatorname{syminc}_V$, then

$$\Phi_1 = \Phi_2. \tag{521}$$

Now, $\mathrm{id}_{\operatorname{Sym} V}$ is a k-algebra homomorphism $\operatorname{Sym} V \to \operatorname{Sym} V$ satisfying $\mathrm{id}_{\operatorname{Sym} V} \circ \operatorname{syminc}_V = \operatorname{syminc}_V$. In other words, $\mathrm{id}_{\operatorname{Sym} V}$ is a k-algebra homomorphism $\Phi : \operatorname{Sym} V \to \operatorname{Sym} V$ satisfying $\Phi \circ \operatorname{syminc}_V = \operatorname{syminc}_V$.

On the other hand, ρ and $\operatorname{symlift} \varphi$ are k-algebra homomorphisms. Thus, their composition $\rho \circ (\operatorname{symlift} \varphi)$ is also a k-algebra homomorphism (since the composition of two k-algebra homomorphisms is always a k-algebra homomorphism). Hence, $\rho \circ (\operatorname{symlift} \varphi)$ is a k-algebra homomorphism $\operatorname{Sym} V \to \operatorname{Sym} V$ satisfying

$$(\rho \circ (\operatorname{symlift} \varphi)) \circ \operatorname{syminc}_V = \rho \circ \underbrace{(\operatorname{symlift} \varphi) \circ \operatorname{syminc}_V}_{=\varphi} = \rho \circ \varphi = \operatorname{syminc}_V .$$

In other words, $\rho \circ (\operatorname{symlift} \varphi)$ is a k-algebra homomorphism $\Phi : \operatorname{Sym} V \to \operatorname{Sym} V$ satisfying $\Phi \circ \operatorname{syminc}_V = \operatorname{syminc}_V$.

Thus, (521) (applied to $\Phi_1 = \rho \circ (\operatorname{symlift} \varphi)$ and $\Phi_2 = \mathrm{id}_{\operatorname{Sym} V}$) shows that $\rho \circ (\operatorname{symlift} \varphi) = \mathrm{id}_{\operatorname{Sym} V}$. This proves Lemma 38.8 **(b)**.

(c) Lemma 38.8 **(a)** shows that the k-algebra homomorphism $\operatorname{symlift} \varphi : \operatorname{Sym} V \to A$ is surjective. Lemma 38.8 **(b)** shows that $\rho \circ (\operatorname{symlift} \varphi) = \mathrm{id}_{\operatorname{Sym} V}$. Hence, $(\operatorname{symlift} \varphi) \circ \rho = \mathrm{id}_A$ [268]. Combining this with $\rho \circ (\operatorname{symlift} \varphi) = \mathrm{id}_{\operatorname{Sym} V}$, we conclude that the maps $\operatorname{symlift} \varphi : \operatorname{Sym} V \to A$ and $\rho : A \to \operatorname{Sym} V$ are mutually inverse. This proves Lemma 38.8 **(c)**. □

The following lemma just recapitulates some trivial observations:

Lemma 38.9. Let k be a field. Let A be a k-algebra. Let C be a connected filtered k-coalgebra. Let $h \in \mathfrak{g}(C, A)$.

(a) We have $h(1_C) = 0$.

(b) We have $h(C_{\leq 0}) = 0$.

(c) Assume that the field k has characteristic 0. Then, $e^{*h}(1_C) = 1_A$.

Proof of Lemma 38.9. We have $h \in \mathfrak{g}(C, A) = \{f \in \mathcal{L}(C, A) \mid f(1_C) = 0\}$ (by the definition of $\mathfrak{g}(C, A)$). In other words, h is an element $f \in \mathcal{L}(C, A)$ satisfying $f(1_C) =$

[268] *Proof.* Let $a \in A$. Then, $a \in A = (\operatorname{symlift} \varphi)(\operatorname{Sym} V)$ (since the homomorphism $\operatorname{symlift} \varphi$ is surjective). In other words, there exists some $b \in \operatorname{Sym} V$ such that $a = (\operatorname{symlift} \varphi)(b)$. Consider this b. Now, $\underbrace{(\rho \circ (\operatorname{symlift} \varphi))}_{=\mathrm{id}_{\operatorname{Sym} V}}(b) = \mathrm{id}_{\operatorname{Sym} V}(b) = b$, so that $b = (\rho \circ (\operatorname{symlift} \varphi))(b) = \rho\left(\underbrace{(\operatorname{symlift} \varphi)(b)}_{=a}\right) = \rho(a)$. Hence, $\rho(a) = b$.

Now,

$$((\operatorname{symlift} \varphi) \circ \rho)(a) = (\operatorname{symlift} \varphi)\left(\underbrace{\rho(a)}_{=b}\right) = (\operatorname{symlift} \varphi)(b) = a = \mathrm{id}_A(a).$$

Now, forget that we fixed a. We thus have shown that $((\operatorname{symlift} \varphi) \circ \rho)(a) = \mathrm{id}_A(a)$ for each $a \in A$. In other words, $(\operatorname{symlift} \varphi) \circ \rho = \mathrm{id}_A$.

0. In other words, h is an element of $\mathcal{L}(C, A)$ and satisfies $h(1_C) = 0$. Thus, Lemma 38.9 **(a)** is proven.

(b) Remark 2.11 gives $C_{\leq 0} = k \cdot 1_C$. Thus,

$$h\left(\underbrace{C_{\leq 0}}_{=k\cdot 1_C}\right) = h(k \cdot 1_C) = k \cdot \underbrace{h(1_C)}_{=0} \qquad \text{(since } h \text{ is } k\text{-linear)}$$
$$= k \cdot 0 = 0.$$

This proves Lemma 38.9 **(b)**.

(c) In Definition 3.6, it was shown that if H is a connected filtered k-coalgebra, and if $f \in \mathfrak{g}(H, A)$, then $e^{*f} \in G(H, A)$. Applying this to $H = C$ and $f = h$, we obtain $e^{*h} \in G(C, A) = \{f \in \mathcal{L}(C, A) \mid f(1_C) = 1_A\}$ (by the definition of $G(C, A)$). In other words, e^{*h} is an element $f \in \mathcal{L}(C, A)$ satisfying $f(1_C) = 1_A$. In other words, e^{*h} is an element of $\mathcal{L}(C, A)$ and satisfies $e^{*h}(1_C) = 1_A$. Thus, Lemma 38.9 **(c)** is proven. □

Next, we state a lemma which is somewhat similar to Lemma 16.27:

Lemma 38.10. Let k be a field. Let A be a k-algebra. Let V be a filtered k-vector space. Let $\alpha : V \to A$ and $\beta : V \to A$ be two k-linear maps. Assume that each $i \in \mathbb{N}$ satisfies

$$(\alpha - \beta)(V_{\leq i}) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq i-1})). \tag{522}$$

Then:

(a) For each $n \in \{-1, 0, 1, \ldots\}$, we have $\operatorname{AlgGen}_k(\alpha(V_{\leq n})) = \operatorname{AlgGen}_k(\beta(V_{\leq n}))$.

(b) We have $\operatorname{AlgGen}_k(\alpha(V)) = \operatorname{AlgGen}_k(\beta(V))$.

Proof of Lemma 38.10. **(a)** Let us prove Lemma 38.10 **(a)** by induction over n:

Induction base: We have $\alpha(V_{\leq -1}) = \beta(V_{\leq -1})$ [269] and thus $\operatorname{AlgGen}_k\left(\underbrace{\alpha(V_{\leq -1})}_{=\beta(V_{\leq -1})}\right) = \operatorname{AlgGen}_k(\beta(V_{\leq -1}))$. In other words, Lemma 38.10 **(a)** holds for $n = -1$. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume that Lemma 38.10 **(a)** holds for $n = N - 1$. We now must prove that Lemma 38.10 **(a)** also holds for $n = N$.

The assumption (522) (applied to $n = N$) yields

$$(\alpha - \beta)(V_{\leq N}) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N-1})). \tag{523}$$

Since Lemma 38.10 **(a)** holds for $n = N - 1$, we have $\operatorname{AlgGen}_k(\alpha(V_{\leq N-1})) = \operatorname{AlgGen}_k(\beta(V_{\leq N-1}))$. Thus, (523) becomes

$$(\alpha - \beta)(V_{\leq N}) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N-1})) = \operatorname{AlgGen}_k(\alpha(V_{\leq N-1})).$$

[269] *Proof.* We have $V_{\leq -1} = 0$ and thus $\alpha(V_{\leq -1}) = \alpha(0) = 0$ (since the map α is k-linear). The same argument (applied to β instead of α) shows that $\beta(V_{\leq -1}) = 0$. Thus, $\alpha(V_{\leq -1}) = 0 = \beta(V_{\leq -1})$.

Hence,

$$\underbrace{(\beta-\alpha)}_{=-(\alpha-\beta)}(V_{\leq N}) = (-(\alpha-\beta))(V_{\leq N}) = -\underbrace{(\alpha-\beta)(V_{\leq N})}_{\subseteq \operatorname{AlgGen}_k(\alpha(V_{\leq N-1}))}$$
$$\subseteq -\operatorname{AlgGen}_k(\alpha(V_{\leq N-1})) \subseteq \operatorname{AlgGen}_k(\alpha(V_{\leq N-1})) \tag{524}$$

(since $\operatorname{AlgGen}_k(\alpha(V_{\leq N-1}))$ is a k-vector space).

We have $V_{\leq N-1} \subseteq V_{\leq N}$ [270].

Applying (116) to $S = \beta(V_{\leq N})$, we obtain $\beta(V_{\leq N}) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N}))$.

Now, define a k-linear map $\xi : V \to A$ by $\xi = \alpha - \beta$. Then,

$$\underbrace{\xi}_{=\alpha-\beta}(V_{\leq N}) = (\alpha-\beta)(V_{\leq N}) \subseteq \operatorname{AlgGen}_k\left(\beta\left(\underbrace{V_{\leq N-1}}_{\subseteq V_{\leq N}}\right)\right) \qquad \text{(by (523))}$$
$$= \operatorname{AlgGen}_k(\beta(V_{\leq N})).$$

But $\alpha = \xi + \beta$ (since $\xi = \alpha - \beta$). Now,

$$\underbrace{\alpha}_{=\xi+\beta}(V_{\leq N}) = (\xi+\beta)(V_{\leq N}) \subseteq \underbrace{\xi(V_{\leq N})}_{\subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N}))} + \underbrace{\beta(V_{\leq N})}_{\subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N}))}$$
$$\subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N})) + \operatorname{AlgGen}_k(\beta(V_{\leq N})) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N}))$$

(since $\operatorname{AlgGen}_k(\beta(V_{\leq N}))$ is a k-vector space). In other words, $\operatorname{AlgGen}_k(\beta(V_{\leq N}))$ contains $\alpha(V_{\leq N})$ as a subset. Hence, $\operatorname{AlgGen}_k(\beta(V_{\leq N}))$ is a k-subalgebra of A containing $\alpha(V_{\leq N})$ as a subset[271].

But we know that $\operatorname{AlgGen}_k(\alpha(V_{\leq N}))$ is the smallest k-subalgebra of A containing $\alpha(V_{\leq N})$ as a subset. This means that whenever U is a k-subalgebra of A containing $\alpha(V_{\leq N})$ as a subset, we must necessarily have $\operatorname{AlgGen}_k(\alpha(V_{\leq N})) \subseteq U$. Applied to $U = \operatorname{AlgGen}_k(\beta(V_{\leq N}))$, this yields that $\operatorname{AlgGen}_k(\alpha(V_{\leq N})) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N}))$.

So we have proven $\operatorname{AlgGen}_k(\alpha(V_{\leq N})) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N}))$. But the same argument, with the maps α and β interchanged (and using the equality (524) instead of (523)), shows that $\operatorname{AlgGen}_k(\beta(V_{\leq N})) \subseteq \operatorname{AlgGen}_k(\alpha(V_{\leq N}))$.

Combining $\operatorname{AlgGen}_k(\alpha(V_{\leq N})) \subseteq \operatorname{AlgGen}_k(\beta(V_{\leq N}))$ and $\operatorname{AlgGen}_k(\beta(V_{\leq N})) \subseteq \operatorname{AlgGen}_k(\alpha(V_{\leq N}))$, we obtain $\operatorname{AlgGen}_k(\alpha(V_{\leq N})) = \operatorname{AlgGen}_k(\beta(V_{\leq N}))$. In other words, Lemma 38.10 **(a)** holds for $n = N$. This completes the induction step.

Thus, the induction proof of Lemma 38.10 **(a)** is complete.

(b) For every $n \in \mathbb{N}$, we have

$$\alpha(V_{\leq n}) \subseteq \operatorname{AlgGen}_k(\alpha(V_{\leq n})) \qquad \text{(by (116), applied to } S = \alpha(V_{\leq n}))$$
$$= \operatorname{AlgGen}_k\left(\beta\left(\underbrace{V_{\leq n}}_{\subseteq V}\right)\right) \qquad \text{(by Lemma 38.10 (a))}$$
$$\subseteq \operatorname{AlgGen}_k(\beta(V)). \tag{525}$$

[270] *Proof.* If $N = 0$, then $V_{\leq N-1} \subseteq V_{\leq N}$ holds (because if $N = 0$, then $V_{\leq N-1} = V_{\leq 0-1} = V_{\leq -1} = 0 \subseteq V_{\leq N}$). Hence, for the rest of this proof, we can WLOG assume that we don't have $N = 0$. Assume this. We have $N \neq 0$ (since we don't have $N = 0$), and thus $N \geq 1$ (since $N \in \mathbb{N}$). Hence, $N - 1 \in \mathbb{N}$.

But since V is a filtered k-algebra, we have $V_{\leq 0} \subseteq V_{\leq 1} \subseteq V_{\leq 2} \subseteq \cdots$. Hence, $V_{\leq N-1} \subseteq V_{\leq N}$ (since $N - 1 \in \mathbb{N}$). Qed.

[271] since $\operatorname{AlgGen}_k(\beta(V_{\leq N}))$ is clearly a k-subalgebra of A

But V is a filtered k-vector space. Hence, $V = \bigcup\limits_{n \in \mathbb{N}} V_{\leq n}$. Applying the map α to this equality, we obtain

$$\alpha(V) = \alpha\left(\bigcup_{n \in \mathbb{N}} V_{\leq n}\right) = \bigcup_{n \in \mathbb{N}} \underbrace{\alpha\left(V_{\leq n}\right)}_{\substack{\subseteq \operatorname{AlgGen}_k(\beta(V)) \\ \text{(by (525))}}}$$
$$\subseteq \bigcup_{n \in \mathbb{N}} \operatorname{AlgGen}_k(\beta(V)) = \operatorname{AlgGen}_k(\beta(V)).$$

In other words, $\operatorname{AlgGen}_k(\beta(V))$ contains $\alpha(V)$ as a subset. Hence, $\operatorname{AlgGen}_k(\beta(V))$ is a k-subalgebra of A containing $\alpha(V)$ as a subset[272].

But we know that $\operatorname{AlgGen}_k(\alpha(V))$ is the smallest k-subalgebra of A containing $\alpha(V)$ as a subset. This means that whenever U is a k-subalgebra of A containing $\alpha(V)$ as a subset, we must necessarily have $\operatorname{AlgGen}_k(\alpha(V)) \subseteq U$. Applied to $U = \operatorname{AlgGen}_k(\beta(V))$, this yields that $\operatorname{AlgGen}_k(\alpha(V)) \subseteq \operatorname{AlgGen}_k(\beta(V))$.

So we have proven $\operatorname{AlgGen}_k(\alpha(V)) \subseteq \operatorname{AlgGen}_k(\beta(V))$. But the same argument, with the maps α and β interchanged, shows that $\operatorname{AlgGen}_k(\beta(V)) \subseteq \operatorname{AlgGen}_k(\alpha(V))$.

Combining $\operatorname{AlgGen}_k(\alpha(V)) \subseteq \operatorname{AlgGen}_k(\beta(V))$ and $\operatorname{AlgGen}_k(\beta(V)) \subseteq \operatorname{AlgGen}_k(\alpha(V))$, we obtain $\operatorname{AlgGen}_k(\alpha(V)) = \operatorname{AlgGen}_k(\beta(V))$. This proves Lemma 38.10 **(b)**. □

Proposition 38.11. Let k be a field. Let C be a connected filtered k-coalgebra. Let A be a k-algebra. Let $f \in \mathfrak{g}(C, A)$. Then:

(a) For each $n \in \mathbb{N}$ and $i \in \mathbb{N}$, we have

$$f^{*i}(C_{\leq n}) \subseteq \operatorname{AlgGen}_k(f(C_{\leq n})).$$

(b) For each $n \in \mathbb{N}$ and $i \in \mathbb{N}$ satisfying $i \geq 2$, we have

$$f^{*i}(C_{\leq n}) \subseteq \operatorname{AlgGen}_k(f(C_{\leq n-1})).$$

Proof of Proposition 38.11. **(a)** We shall prove Proposition 38.11 **(a)** by induction on i:

Induction base: For each $n \in \mathbb{N}$, we have $f^{*0}(C_{\leq n}) \subseteq \operatorname{AlgGen}_k(f(C_{\leq n}))$ [273]. In other words, Proposition 38.11 **(a)** holds for $i = 0$. This completes the induction base.

Induction step: Let j be a positive integer. Assume that Proposition 38.11 **(a)** holds for $i = j - 1$. We must then show that Proposition 38.11 **(a)** holds for $i = j$.

---

[272] since $\operatorname{AlgGen}_k(\beta(V))$ is clearly a k-subalgebra of A

[273] *Proof.* Let $n \in \mathbb{N}$. The set $\operatorname{AlgGen}_k(f(C_{\leq n}))$ is a k-subalgebra of A, and thus contains the element 1_A. In other words, $1_A \in \operatorname{AlgGen}_k(f(C_{\leq n}))$.

But $f^{*0} = e_{C,A} = \eta_A \circ \varepsilon_C$ (by the definition of $e_{C,A}$). Hence, each $x \in C_{\leq n}$ satisfies

$$\underbrace{f^{*0}}_{=\eta_A \circ \varepsilon_C}(x) = (\eta_A \circ \varepsilon_C)(x) = \eta_A(\varepsilon_C(x)) = \varepsilon_C(x) \cdot \underbrace{1_A}_{\in \operatorname{AlgGen}_k(f(C_{\leq n}))} \quad \text{(by the definition of } \eta_A\text{)}$$
$$\in \varepsilon_C(x) \cdot \operatorname{AlgGen}_k(f(C_{\leq n})) \subseteq \operatorname{AlgGen}_k(f(C_{\leq n}))$$

(since $\operatorname{AlgGen}_k(f(C_{\leq n}))$ is a k-vector space). In other words, $f^{*0}(C_{\leq n}) \subseteq \operatorname{AlgGen}_k(f(C_{\leq n}))$. Qed.

We have assumed that Proposition 38.11 **(a)** holds for $i = j - 1$. In other words, whenever k, C, A and f are as in Proposition 38.11 **(a)**, we have

$$f^{*(j-1)}\left(C_{\leq n}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right) \tag{526}$$

for each $n \in \mathbb{N}$.

Now, we must prove that Proposition 38.11 **(a)** holds for $i = j$. So let k, C, A and f be as in Proposition 38.11 **(a)**. Let $n \in \mathbb{N}$.

Let $\mathfrak{A}$ be the k-subalgebra $\operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right)$ of A. Thus, $\mathfrak{A} = \operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right)$.

Each $u \in \{0, 1, \ldots, n\}$ satisfies

$$f\left(C_{\leq u}\right) \subseteq \mathfrak{A} \tag{527}$$

[274] and

$$f^{*(j-1)}\left(C_{\leq n-u}\right) \subseteq \mathfrak{A} \tag{528}$$

[275].

Since j is a positive integer, we have $f^{*j} = f * f^{*(j-1)} = \mu_A \circ \left(f \otimes f^{*(j-1)}\right) \circ \Delta_C$ (by

[274] *Proof of (527):* Let $u \in \{0, 1, \ldots, n\}$. Then, $u \in \mathbb{N}$ and $u \leq n$.

Applying (116) to $S = f\left(C_{\leq n}\right)$, we obtain $f\left(C_{\leq n}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right) = \mathfrak{A}$.

Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$. In other words, $C_{\leq x} \subseteq C_{\leq y}$ whenever x and y are two elements of $\mathbb{N}$ satisfying $x \leq y$. Applying this to $x = u$ and $y = n$, we obtain $C_{\leq u} \subseteq C_{\leq n}$ (since $u \leq n$). Thus, $f\left(\underbrace{C_{\leq u}}_{\subseteq C_{\leq n}}\right) \subseteq f\left(C_{\leq n}\right) \subseteq \mathfrak{A}$. This proves (527).

[275] *Proof of (528):* Let $u \in \{0, 1, \ldots, n\}$. Then, $n - u \in \{0, 1, \ldots, n\} \subseteq \mathbb{N}$. But $u \in \{0, 1, \ldots, n\}$ shows that $u \geq 0$ and thus $n - \underbrace{u}_{\geq 0} \leq n$.

Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$. In other words, $C_{\leq x} \subseteq C_{\leq y}$ whenever x and y are two elements of $\mathbb{N}$ satisfying $x \leq y$. Applying this to $x = n - u$ and $y = n$, we obtain $C_{\leq n-u} \subseteq C_{\leq n}$ (since $n - u \leq n$). Thus,

$$\begin{aligned} f^{*(j-1)}\left(\underbrace{C_{\leq n-u}}_{\subseteq C_{\leq n}}\right) &\subseteq f^{*(j-1)}\left(C_{\leq n}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right) \qquad \text{(by (526))} \\ &= \mathfrak{A}. \end{aligned}$$

This proves (528).

the definition of convolution). Hence,

$$
\begin{aligned}
&\underbrace{f^{*j}}_{=\mu_A\circ\left(f\otimes f^{*(j-1)}\right)\circ\Delta_C}\left(C_{\leq n}\right) \\
&= \left(\mu_A \circ \left(f \otimes f^{*(j-1)}\right) \circ \Delta_C\right)\left(C_{\leq n}\right) \\
&= \mu_A\left(\left(f \otimes f^{*(j-1)}\right)\left(\underbrace{\Delta_C\left(C_{\leq n}\right)}_{\substack{\subseteq \sum_{u=0}^{n} C_{\leq u}\otimes C_{\leq n-u} \\ \text{(since } C \text{ is a filtered } k\text{-coalgebra)}}}\right)\right) \\
&\subseteq \mu_A\left(\underbrace{\left(f \otimes f^{*(j-1)}\right)\left(\sum_{u=0}^{n} C_{\leq u} \otimes C_{\leq n-u}\right)}_{\substack{\subseteq \sum_{u=0}^{n}\left(f\otimes f^{*(j-1)}\right)\left(C_{\leq u}\otimes C_{\leq n-u}\right) \\ \text{(since the map } f\otimes f^{*(j-1)} \text{ is } k\text{-linear)}}}\right) \\
&\subseteq \mu_A\left(\sum_{u=0}^{n} \underbrace{\left(f \otimes f^{*(j-1)}\right)\left(C_{\leq u} \otimes C_{\leq n-u}\right)}_{\subseteq f\left(C_{\leq u}\right)\otimes f^{*(j-1)}\left(C_{\leq n-u}\right)}\right) \subseteq \mu_A\left(\sum_{u=0}^{n} \underbrace{f\left(C_{\leq u}\right)}_{\substack{\subseteq \mathfrak{A} \\ \text{(by (527))}}} \otimes \underbrace{f^{*(j-1)}\left(C_{\leq n-u}\right)}_{\substack{\subseteq \mathfrak{A} \\ \text{(by (528))}}}\right) \\
&\subseteq \mu_A\left(\underbrace{\sum_{u=0}^{n} \mathfrak{A} \otimes \mathfrak{A}}_{\substack{\subseteq \mathfrak{A}\otimes\mathfrak{A} \\ \text{(since } \mathfrak{A}\otimes\mathfrak{A} \text{ is a } k\text{-vector space)}}}\right) \subseteq \mu_A\left(\mathfrak{A} \otimes \mathfrak{A}\right) \\
&= \mathfrak{A}\mathfrak{A} \qquad \text{(by (74), applied to } U = \mathfrak{A} \text{ and } V = \mathfrak{A}) \\
&\subseteq \mathfrak{A} \qquad \text{(since } \mathfrak{A} \text{ is a } k\text{-algebra)} \\
&= \operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right).
\end{aligned}
$$

Now, forget that we fixed n. We thus have proven that $f^{*j}\left(C_{\leq n}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right)$ for each $n \in \mathbb{N}$.

Now, forget that we fixed k, C, A and f. We thus have shown that if k, C, A and f are as in Proposition 38.11 **(a)**, then we have $f^{*j}\left(C_{\leq n}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n}\right)\right)$ for each $n \in \mathbb{N}$. In other words, Proposition 38.11 **(a)** holds for $i = j$. This completes the induction step. Thus, the induction proof of Proposition 38.11 **(a)** is complete.

(b) Let $n \in \mathbb{N}$ and $i \in \mathbb{N}$ be such that $i \geq 2$.

From $i \geq 2 \geq 1$, we conclude that i is positive. Hence, Lemma 17.10 (applied to C and f instead of H and h) yields $f^{*i} \in \mathfrak{g}\left(C, A\right)$. Hence, Lemma 38.9 **(b)** (applied to f^{*i} instead of h) yields

$$
f^{*i}\left(C_{\leq 0}\right) = 0 \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq 0-1}\right)\right)
$$

(since $\operatorname{AlgGen}_k\left(f\left(C_{\leq 0-1}\right)\right)$ is a k-subalgebra of A). In other words, Proposition 38.11 **(b)** holds if $n=0$. Thus, for the rest of this proof, we can WLOG assume that we don't have $n=0$. Assume this.

We have $n \neq 0$ (since we don't have $n=0$). Thus, n is a positive integer (since $n \in \mathbb{N}$). Hence, $n-1 \in \mathbb{N}$. Also, $i-1 \in \mathbb{N}$ (since i is a positive integer).

Let $\mathfrak{A}$ be the k-subalgebra $\operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)$ of A. Thus, $\mathfrak{A}=\operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)$.

For each $u \in\{1,2, \ldots, n-1\}$, we have

$$f\left(C_{\leq u}\right) \subseteq \mathfrak{A} \tag{529}$$

[276] and

$$f^{*(i-1)}\left(C_{\leq n-u}\right) \subseteq \mathfrak{A} \tag{530}$$

[277].

From $i \geq 2$, we obtain $i-1 \geq 1$. Thus, $i-1$ is a positive element of $\mathbb{N}$. Hence, Lemma 17.10 (applied to C, f and $i-1$ instead of H, h and i) yields $f^{*(i-1)} \in \mathfrak{g}(C, A)$. Thus, Proposition 17.7 (applied to $g=f^{*(i-1)}$ and $\ell=n$) yields

$$\left(f * f^{*(i-1)}\right)\left(C_{\leq n}\right) \subseteq \sum_{u=1}^{n-1} \underbrace{f\left(C_{\leq u}\right)}_{\substack{\subseteq \mathfrak{A} \\ \text{(by (529))}}} \underbrace{f^{*(i-1)}\left(C_{\leq n-u}\right)}_{\substack{\subseteq \mathfrak{A} \\ \text{(by (530))}}} \subseteq \sum_{u=1}^{n-1} \mathfrak{A} \mathfrak{A} \subseteq \mathfrak{A}$$

(since $\mathfrak{A}$ is a k-subalgebra of A). Now,

$$\underbrace{f^{*i}}_{=f * f^{*(i-1)}}\left(C_{\leq n}\right)=\left(f * f^{*(i-1)}\right)\left(C_{\leq n}\right) \subseteq \mathfrak{A}=\operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right).$$

This proves Proposition 38.11 **(b)**. □

[276] *Proof of (529):* Let $u \in\{1,2, \ldots, n-1\}$. Then, $1 \leq u \leq n-1$.

Applying (116) to $S=f\left(C_{\leq n-1}\right)$, we obtain $f\left(C_{\leq n-1}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)=\mathfrak{A}$.

Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$. In other words, $C_{\leq x} \subseteq C_{\leq y}$ whenever x and y are two elements of $\mathbb{N}$ satisfying $x \leq y$. Applying this to $x=u$ and $y=n-1$, we obtain $C_{\leq u} \subseteq C_{\leq n-1}$ (since $u \leq n-1$). Thus, $f\left(\underbrace{C_{\leq u}}_{\subseteq C_{\leq n-1}}\right) \subseteq f\left(C_{\leq n-1}\right) \subseteq \mathfrak{A}$. This proves (529).

[277] *Proof of (530):* Let $u \in\{1,2, \ldots, n-1\}$. Then, $n-u \in\{1,2, \ldots, n-1\} \subseteq \mathbb{N}$. Also, from $u \in\{1,2, \ldots, n-1\}$, we obtain $1 \leq u \leq n-1$. Thus, $n-\underbrace{u}_{\geq 1} \leq n-1$.

Since C is filtered, we have $C_{\leq 0} \subseteq C_{\leq 1} \subseteq C_{\leq 2} \subseteq \cdots$. In other words, $C_{\leq x} \subseteq C_{\leq y}$ whenever x and y are two elements of $\mathbb{N}$ satisfying $x \leq y$. Applying this to $x=n-u$ and $y=n-1$, we obtain $C_{\leq n-u} \subseteq C_{\leq n-1}$ (since $n-u \leq n-1$). Thus,

$$f^{*(i-1)}\left(\underbrace{C_{\leq n-u}}_{\subseteq C_{\leq n-1}}\right) \subseteq f^{*(i-1)}\left(C_{\leq n-1}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)$$

(by Proposition 38.11 **(a)**, applied to $n-1$ and $i-1$ instead of n and i)

$$=\mathfrak{A}.$$

This proves (530).

Proposition 38.12. Let k be a field of characteristic 0. Let C be a connected filtered k-coalgebra. Let A be a k-algebra. Let $f \in \mathfrak{g}(C, A)$. Then:

(a) Each $i \in \mathbb{N}$ satisfies

$$\left(e^{*f} - f\right)\left(C_{\leq i}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right).$$

(b) We have $\operatorname{AlgGen}_k\left(e^{*f}\left(C\right)\right) = \operatorname{AlgGen}_k\left(f\left(C\right)\right)$.

Proof of Proposition 38.12. **(a)** Let n be a positive integer. We shall prove that

$$\left(e^{*f} - f\right)\left(C_{\leq n}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right). \tag{531}$$

Indeed, let $x \in C_{\leq n}$ be arbitrary. Then,

$$f^{*i}\left(x\right) = 0 \qquad \text{for every integer } i > n \tag{532}$$

[278].

Let $\mathfrak{A}$ denote the k-subalgebra $\operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)$ of A. Then, $1_A \in \mathfrak{A}$ (since $\mathfrak{A}$ is a k-subalgebra of A).

We have

$$f^{*i}\left(x\right) \in \mathfrak{A} \qquad \text{for each integer } i \geq 2 \tag{533}$$

[279].

On the other hand, $n \geq 1$ (since n is a positive integer). Furthermore, $f^{*0} = e_{C,A} = \eta_A \circ \varepsilon_C$ (by the definition of $e_{C,A}$) and thus

$$\underbrace{f^{*0}}_{=\eta_A \circ \varepsilon_C}\left(x\right) = \left(\eta_A \circ \varepsilon_C\right)\left(x\right) = \eta_A\left(\varepsilon_C\left(x\right)\right) = \varepsilon_C\left(x\right) \cdot \underbrace{1_A}_{\in \mathfrak{A}} \qquad \text{(by the definition of } \eta_A\text{)}$$
$$\in \varepsilon_C\left(x\right) \cdot \mathfrak{A} \subseteq \mathfrak{A}$$

(since $\mathfrak{A}$ is a k-vector space).

---

[278] *Proof of (532):* Let $i > n$ be an integer. Thus, $i > n \geq 0$, so that $i \in \mathbb{N}$. Now, Remark 3.5 (applied to $H = C$) yields $f^{*i}\left(C_{\leq n}\right) = 0$ (since $i > n$). But $x \in C_{\leq n}$ yields $f^{*i}\left(x\right) \in f^{*i}\left(C_{\leq n}\right) = 0$, thus $f^{*i}\left(x\right) = 0$. This proves (532).

[279] *Proof of (533):* Let $i \geq 2$ be an integer. Thus, $i \in \mathbb{N}$. Now, Proposition 38.11 **(b)** yields $f^{*i}\left(C_{\leq n}\right) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right) = \mathfrak{A}$ (since $\mathfrak{A} = \operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)$). But $f^{*i}\left(\underbrace{x}_{\in C_{\leq n}}\right) \in f^{*i}\left(C_{\leq n}\right) \subseteq \mathfrak{A}$. This proves (533).

But the definition of e^{*f} yields

$$\begin{aligned}
e^{*f}(x) &= \sum_{i\geq 0} \underbrace{\frac{f^{*i}(x)}{i!}}_{=\frac{1}{i!}f^{*i}(x)} = \sum_{i\geq 0} \frac{1}{i!} f^{*i}(x) \\
&= \underbrace{\sum_{\substack{i\geq 0;\\ i\leq n}} \frac{1}{i!} f^{*i}(x)}_{=\sum_{i=0}^{n}} + \sum_{\substack{i\geq 0;\\ i>n}} \frac{1}{i!} \underbrace{f^{*i}(x)}_{\substack{=0\\ \text{(by (532))}}} \\
&= \sum_{i=0}^{n} \frac{1}{i!} f^{*i}(x) + \underbrace{\sum_{\substack{i\geq 0;\\ i>n}} \frac{1}{i!} 0}_{=0} = \sum_{i=0}^{n} \frac{1}{i!} f^{*i}(x) \\
&= \underbrace{\frac{1}{0!}}_{=\frac{1}{1}=1} f^{*0}(x) + \underbrace{\sum_{i=1}^{n} \frac{1}{i!} f^{*i}(x)}_{\substack{=\frac{1}{1!}f^{*1}(x)+\sum_{i=2}^{n}\frac{1}{i!}f^{*i}(x)\\ \text{(here, we have split off the addend}\\ \text{for } i=1 \text{ from the sum (since } n\geq 1))}} \\
&\qquad \left(\begin{array}{c} \text{here, we have split off the addend for } i=0 \\ \text{from the sum (because } n \geq 1 \geq 0) \end{array} \right) \\
&= f^{*0}(x) + \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1} \underbrace{f^{*1}}_{=f}(x) + \sum_{i=2}^{n} \frac{1}{i!} f^{*i}(x) \\
&= f^{*0}(x) + f(x) + \sum_{i=2}^{n} \frac{1}{i!} f^{*i}(x).
\end{aligned}$$

Subtracting $f(x)$ from both sides of this equality, we obtain

$$\begin{aligned}
e^{*f}(x) - f(x) &= \underbrace{f^{*0}(x)}_{\in \mathfrak{A}} + \sum_{i=2}^{n} \frac{1}{i!} \underbrace{f^{*i}(x)}_{\substack{\in \mathfrak{A}\\ \text{(by (533))}}} \in \mathfrak{A} + \underbrace{\sum_{i=2}^{n} \frac{1}{i!} \mathfrak{A}}_{\substack{\subseteq \mathfrak{A}\\ \text{(since } \mathfrak{A} \text{ is a } k\text{-vector space)}}} \\
&\subseteq \mathfrak{A} + \mathfrak{A} \subseteq \mathfrak{A} \qquad \text{(since } \mathfrak{A} \text{ is a } k\text{-vector space)}.
\end{aligned}$$

Now, $\left(e^{*f} - f\right)(x) = e^{*f}(x) - f(x) \in \mathfrak{A}$.

Now, let us forget that we fixed x. We thus have proven that $\left(e^{*f} - f\right)(x) \in \mathfrak{A}$ for each $x \in C_{\leq n}$. In other words, $\left(e^{*f} - f\right)(C_{\leq n}) \subseteq \mathfrak{A}$. This rewrites as $\left(e^{*f} - f\right)(C_{\leq n}) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)$ (since $\mathfrak{A} = \operatorname{AlgGen}_k\left(f\left(C_{\leq n-1}\right)\right)$). Thus, (531) is proven.

Now, let us forget that we fixed n. We thus have proven that (531) holds for each positive integer n.

Now, let $i \in \mathbb{N}$. We must prove that $\left(e^{*f} - f\right)(C_{\leq i}) \subseteq \operatorname{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right)$. If i is a positive integer, then this follows immediately from (531) (applied to $n = i$). Hence,

for the rest of this proof, we can WLOG assume that i is not a positive integer. Assume this.

We have $i \notin \{1, 2, 3, \ldots\}$ (since i is not a positive integer). Combining this with $i \in \mathbb{N}$, we obtain $i \in \mathbb{N} \setminus \{1, 2, 3, \ldots\} = \{0\}$. In other words, $i = 0$. Hence, $C_{\leq i} = C_{\leq 0} = k \cdot 1_C$ (by Remark 2.11).

But

$$\left(e^{*f} - f\right)(1_C) = \underbrace{e^{*f}(1_C)}_{\substack{=1_A \\ \text{(by Lemma 38.9 (c),} \\ \text{applied to } h=f)}} - \underbrace{f(1_C)}_{\substack{=0 \\ \text{(by Lemma 38.9 (a),} \\ \text{applied to } h=f)}} = 1_A - 0 = 1_A.$$

Now,

$$\begin{aligned}
\left(e^{*f} - f\right)\left(\underbrace{C_{\leq i}}_{=k\cdot 1_C}\right) &= \left(e^{*f} - f\right)(k \cdot 1_C) \\
&= k \cdot \underbrace{\left(e^{*f} - f\right)(1_C)}_{=1_A} \qquad \left(\text{since the map } e^{*f} - f \text{ is } k\text{-linear}\right) \\
&= k \cdot \underbrace{1_A}_{\substack{\in \mathrm{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right) \\ \left(\text{since } \mathrm{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right)\right. \\ \left.\text{is a } k\text{-subalgebra of } A\right)}} \qquad \subseteq k \cdot \mathrm{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right) \\
&\subseteq \mathrm{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right)
\end{aligned}$$

(since $\mathrm{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right)$ is a k-vector subspace of A). Thus, $\left(e^{*f} - f\right)(C_{\leq i}) \subseteq \mathrm{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right)$ is proven. The proof of Proposition 38.12 **(a)** is thus complete.

(b) Proposition 38.12 **(a)** says that each $i \in \mathbb{N}$ satisfies $\left(e^{*f} - f\right)(C_{\leq i}) \subseteq \mathrm{AlgGen}_k\left(f\left(C_{\leq i-1}\right)\right)$. Hence, Lemma 38.10 **(b)** (applied to $V = C$, $\alpha = e^{*f}$ and $\beta = f$) shows that $\mathrm{AlgGen}_k\left(e^{*f}(C)\right) = \mathrm{AlgGen}_k\left(f(C)\right)$. This proves Proposition 38.12 **(b)**. □

Corollary 38.13. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a k-algebra. Let $f \in \mathfrak{g}(H, A)$ be an $(\varepsilon_H, \varepsilon_H)$-derivation. Assume that the subset $f(H)$ of A generates the k-algebra A. Then, the map $e^{*f} : H \to A$ is a surjective k-algebra homomorphism.

Proof of Corollary 38.13. Lemma 15.11 yields that e^{*f} is a k-algebra homomorphism. It remains to show that this homomorphism e^{*f} is surjective.

The subset $f(H)$ of A generates the k-algebra A. In other words, the k-subalgebra of A generated by $f(H)$ is A. In other words, $\mathrm{AlgGen}_k(f(H))$ is A (since $\mathrm{AlgGen}_k(f(H))$ is the k-subalgebra of A generated by $f(H)$). In other words, $\mathrm{AlgGen}_k(f(H)) = A$.

Proposition 38.12 (applied to $C = H$) yields $\mathrm{AlgGen}_k\left(e^{*f}(H)\right) = \mathrm{AlgGen}_k(f(H)) = A$.

The image $e^{*f}(H)$ is a k-subalgebra of A (since $e^{*f} : H \to A$ is a k-algebra homomorphism).

Let S denote the image $e^{*f}(H)$. Then, $S = e^{*f}(H)$. Hence, $\operatorname{AlgGen}_k \underbrace{S}_{=e^{*f}(H)} = \operatorname{AlgGen}_k \left(e^{*f}(H)\right) = A$.

But $S = e^{*f}(H)$. Hence, S is a k-subalgebra of A (since $e^{*f}(H)$ is a k-subalgebra of A).

The k-subalgebra of A generated by S is $\operatorname{AlgGen}_k S = A$. In other words, A is the k-subalgebra of A generated by S. In other words, A is the smallest k-subalgebra of A which contains S as a subset (because the k-subalgebra of A generated by S is the smallest k-subalgebra of A which contains S as a subset). Hence,

$$\left(\begin{array}{c} \text{whenever } U \text{ is a } k\text{-subalgebra of } A \text{ which contains } S \text{ as} \\ \text{a subset, we must necessarily have } A \subseteq U \end{array} \right).$$

Applying this to $U = S$, we conclude that $A \subseteq S$ (since S is a k-subalgebra of A that contains S as a subset). Combined with $S \subseteq A$ (which is obvious), this yields $A = S$. Thus, $A = S = e^{*f}(H)$. In other words, the map e^{*f} is surjective. This completes the proof of Corollary 38.13. □

Proposition 38.14. Let k be a field. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a k-algebra. Let $h : H \to A$ be an $(\varepsilon_H, \varepsilon_H)$-derivation. Then, $h \in \mathfrak{g}(H, A)$.

Proof of Proposition 38.14. Theorem 15.9 (applied to $f = h$) shows that h is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $h\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$. Thus, $h\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$ (since h is an $(\varepsilon_H, \varepsilon_H)$-derivation).

But $1_H = \underbrace{1}_{\in k} \cdot 1_H \in k \cdot 1_H \subseteq \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$. Hence,

$$h\left(\underbrace{1_H}_{\in \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H}\right) \subseteq h\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0.$$

Thus, $h(1_H) = 0$.

Recall that $\mathfrak{g}(H, A) = \{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\}$ (by the definition of $\mathfrak{g}(H, A)$). Now, h is an element $f \in \mathcal{L}(H, A)$ satisfying $f(1_H) = 0$ (since $h \in \mathcal{L}(H, A)$ and $h(1_H) = 0$). In other words, $h \in \{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\}$. This rewrites as $h \in \mathfrak{g}(H, A)$ (since $\mathfrak{g}(H, A) = \{f \in \mathcal{L}(H, A) \mid f(1_H) = 0\}$). This proves Proposition 38.14. □

Finally, having collected all the pieces of the puzzle, we can prove Theorem 38.2:

Proof of Theorem 38.2. Theorem 15.3 shows that the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$ is a projection such that $\operatorname{Ker}(\operatorname{Log} \operatorname{id}) = \left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H$. [280]

But $\mathfrak{e} = \operatorname{Log} \operatorname{id}$ (by the definition of $\mathfrak{e}$). Hence, the map $\mathfrak{e}$ is a projection (since the map $\operatorname{Log} \operatorname{id}$ is a projection). This proves Theorem 38.2 **(a)**.

[280] Recall that $\left(\operatorname{Ker}(\varepsilon_H)\right)^2$ is to be understood according to Convention 15.2. Thus, $\left(\operatorname{Ker}(\varepsilon_H)\right)^2$ means the subspace $\left(\operatorname{Ker}(\varepsilon_H)\right) \cdot \left(\operatorname{Ker}(\varepsilon_H)\right)$ of H.

From $\mathfrak{e} = \operatorname{Log} \mathrm{id}$, we obtain $\operatorname{Ker} \mathfrak{e} = \operatorname{Ker} (\operatorname{Log} \mathrm{id}) = (\operatorname{Ker} (\varepsilon_H))^2 + k \cdot 1_H$. This proves Theorem 38.2 **(b)**.

We have $\mathfrak{e} = \operatorname{Log} \mathrm{id} \in \mathfrak{g}(H, H)$ (because $\operatorname{Log} F \in \mathfrak{g}(H, H)$ for every $F \in G(H, H)$). Besides, $\mathfrak{e} = \operatorname{Log} \mathrm{id}$ yields $e^{*\mathfrak{e}} = e^{*(\operatorname{Log} \mathrm{id})} = \mathrm{id}$ (by Proposition 5.13 **(b)**, applied to $F = \mathrm{id}$ and $A = H$). Hence, $e^{*\mathfrak{e}}$ is a k-algebra homomorphism (since id is a k-algebra homomorphism). By Lemma 15.12 (applied to $A = H$ and $f = \mathfrak{e}$), this yields that $\mathfrak{e}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation. This proves Theorem 38.2 **(c)**.

Definition 15.7 (applied to $A = H$ and $f = \mathfrak{e}$) shows that the map $\mathfrak{e}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if every $(a, b) \in H \times H$ satisfies $\mathfrak{e}(ab) = \mathfrak{e}(a)\, \varepsilon_H(b) + \varepsilon_H(a)\, \mathfrak{e}(b)$. Thus, every $(a, b) \in H \times H$ satisfies

$$\mathfrak{e}(ab) = \mathfrak{e}(a)\, \varepsilon_H(b) + \varepsilon_H(a)\, \mathfrak{e}(b) \tag{534}$$

(since the map $\mathfrak{e}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation). Hence, every $(a, b) \in H \times H$ satisfies

$$\mathfrak{q}(ab) = \mathfrak{q}(a)\, \varepsilon_H(b) + \varepsilon_H(a)\, \mathfrak{q}(b) \tag{535}$$

[281].

Definition 15.7 (applied to $A = \operatorname{Sym}(\mathfrak{e}(H))$ and $f = \mathfrak{q}$) shows that the map $\mathfrak{q}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if every $(a, b) \in H \times H$ satisfies $\mathfrak{q}(ab) = \mathfrak{q}(a)\, \varepsilon_H(b) + \varepsilon_H(a)\, \mathfrak{q}(b)$. Thus, the map $\mathfrak{q}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation (since every $(a, b) \in H \times H$ satisfies $\mathfrak{q}(ab) = \mathfrak{q}(a)\, \varepsilon_H(b) + \varepsilon_H(a)\, \mathfrak{q}(b)$). Therefore, Proposition 38.14 (applied to $A = \operatorname{Sym}(\mathfrak{e}(H))$ and $h = \mathfrak{q}$) yields $\mathfrak{q} \in \mathfrak{g}(H, \operatorname{Sym}(\mathfrak{e}(H)))$. Hence, the map $e^{*\mathfrak{q}} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ is well-defined.

---

[281] *Proof of (535):* Let $(a, b) \in H \times H$. The definition of the map $\mathfrak{e}'$ yields $\mathfrak{e}'(ab) = \mathfrak{e}(ab)$ and $\mathfrak{e}'(a) = \mathfrak{e}(a)$ and $\mathfrak{e}'(b) = \mathfrak{e}(b)$. But recall that $\mathfrak{q} = \operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'$. Hence,

$$\underbrace{\mathfrak{q}}_{= \operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'}(a) = \left(\operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'\right)(a) = \operatorname{symminc}_{\mathfrak{e}(H)} \left(\underbrace{\mathfrak{e}'(a)}_{= \mathfrak{e}(a)} \right) = \operatorname{symminc}_{\mathfrak{e}(H)} (\mathfrak{e}(a)). \tag{536}$$

The same argument (applied to b instead of a) shows that

$$\mathfrak{q}(b) = \operatorname{symminc}_{\mathfrak{e}(H)} (\mathfrak{e}(b)). \tag{537}$$

Finally,

$$\begin{aligned}
\underbrace{\mathfrak{q}}_{= \operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'}(ab) &= \left(\operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'\right)(ab) = \operatorname{symminc}_{\mathfrak{e}(H)} \left(\underbrace{\mathfrak{e}'(ab)}_{= \mathfrak{e}(ab)} \right) = \operatorname{symminc}_{\mathfrak{e}(H)} \left(\underbrace{\mathfrak{e}(ab)}_{\substack{= \mathfrak{e}(a)\varepsilon_H(b) + \varepsilon_H(a)\mathfrak{e}(b) \\ (\text{by (534)})}} \right) \\
&= \operatorname{symminc}_{\mathfrak{e}(H)} (\mathfrak{e}(a)\, \varepsilon_H(b) + \varepsilon_H(a)\, \mathfrak{e}(b)) \\
&= \underbrace{\operatorname{symminc}_{\mathfrak{e}(H)} (\mathfrak{e}(a))}_{\substack{= \mathfrak{q}(a) \\ (\text{by (536)})}} \varepsilon_H(b) + \varepsilon_H(a) \underbrace{\operatorname{symminc}_{\mathfrak{e}(H)} (\mathfrak{e}(b))}_{\substack{= \mathfrak{q}(b) \\ (\text{by (537)})}} \\
&\qquad \left(\text{since the map } \operatorname{symminc}_{\mathfrak{e}(H)} \text{ is } k\text{-linear}\right) \\
&= \mathfrak{q}(a)\, \varepsilon_H(b) + \varepsilon_H(a)\, \mathfrak{q}(b).
\end{aligned}$$

This proves (535).

Furthermore, the subset $\mathfrak{q}(H)$ of $\operatorname{Sym}(\mathfrak{e}(H))$ generates the k-algebra $\operatorname{Sym}(\mathfrak{e}(H))$ [282]. Hence, Corollary 38.13 (applied to $A = \operatorname{Sym}(\mathfrak{e}(H))$ and $f = \mathfrak{q}$) shows that the map $e^{*\mathfrak{q}} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ is a surjective k-algebra homomorphism.

On the other hand, symlift $\mathfrak{j}$ is the unique k-algebra homomorphism $\Phi : \operatorname{Sym}(\mathfrak{e}(H)) \to H$ satisfying $\Phi \circ \operatorname{syminc}_{\mathfrak{e}(H)} = \mathfrak{j}$ (by the definition of symlift $\mathfrak{j}$). Thus, symlift $\mathfrak{j}$ is a k-algebra homomorphism $\operatorname{Sym}(\mathfrak{e}(H)) \to H$ and satisfies $(\operatorname{symlift}\mathfrak{j}) \circ \operatorname{syminc}_{\mathfrak{e}(H)} = \mathfrak{j}$. Therefore, $(\operatorname{symlift}\mathfrak{j}) \circ \mathfrak{q} = \mathfrak{e}$ [283].

Now, Proposition 38.3 **(d)** (applied to $C = H$, $A = \operatorname{Sym}(\mathfrak{e}(H))$, $B = H$, $p = \operatorname{symlift}\mathfrak{j}$ and $f = \mathfrak{q}$) shows that $(\operatorname{symlift}\mathfrak{j}) \circ \mathfrak{q} \in \mathfrak{g}(H, \operatorname{Sym}(\mathfrak{e}(H)))$ and $(\operatorname{symlift}\mathfrak{j}) \circ e^{*\mathfrak{q}} = e^{*((\operatorname{symlift}\mathfrak{j})\circ\mathfrak{q})}$.

Now,

$$\begin{aligned}(\operatorname{symlift}\mathfrak{j}) \circ e^{*\mathfrak{q}} &= e^{*((\operatorname{symlift}\mathfrak{j})\circ\mathfrak{q})} = e^{*\mathfrak{e}} \qquad (\text{since } (\operatorname{symlift}\mathfrak{j}) \circ \mathfrak{q} = \mathfrak{e}) \\ &= \operatorname{id}.\end{aligned}$$

Since $e^{*\mathfrak{q}}$ is surjective, we can thus easily obtain $e^{*\mathfrak{q}} \circ (\operatorname{symlift}\mathfrak{j}) = \operatorname{id}$ [284].

We now have shown the two equalities $(\operatorname{symlift}\mathfrak{j}) \circ e^{*\mathfrak{q}} = \operatorname{id}$ and $e^{*\mathfrak{q}} \circ (\operatorname{symlift}\mathfrak{j}) = \operatorname{id}$. Combining these equalities, we conclude that the maps $\operatorname{symlift}\mathfrak{j} : \operatorname{Sym}(\mathfrak{e}(H)) \to$

---

[282] *Proof.* We have

$$\mathfrak{e}'(H) = \left\{ \underbrace{\mathfrak{e}'(h)}_{\substack{=\mathfrak{e}(h) \\ (\text{by the definition of } \mathfrak{e}')}} \;\middle|\; h \in H \right\} = \{\mathfrak{e}(h) \mid h \in H\} = \mathfrak{e}(H).$$

On the other hand, the definition of $\mathfrak{q}$ yields $\mathfrak{q} = \operatorname{syminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'$. Hence,

$$\begin{aligned}\underbrace{\mathfrak{q}}_{=\operatorname{syminc}_{\mathfrak{e}(H)}\circ\mathfrak{e}'}(H) &= \left(\operatorname{syminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'\right)(H) = \operatorname{syminc}_{\mathfrak{e}(H)}(\mathfrak{e}'(H)) = \mathfrak{e}'(H) \\ &\qquad \left(\text{since } \operatorname{syminc}_{\mathfrak{e}(H)} \text{ is merely an inclusion map}\right) \\ &= \mathfrak{e}(H).\end{aligned}$$

It is well-known that if V is a k-vector space, then the subset V of $\operatorname{Sym} V$ generates the k-algebra $\operatorname{Sym} V$. Applying this to $V = \mathfrak{e}(H)$, we conclude that the subset $\mathfrak{e}(H)$ of $\operatorname{Sym}(\mathfrak{e}(H))$ generates the k-algebra $\operatorname{Sym}(\mathfrak{e}(H))$. In other words, the subset $\mathfrak{q}(H)$ of $\operatorname{Sym}(\mathfrak{e}(H))$ generates the k-algebra $\operatorname{Sym}(\mathfrak{e}(H))$ (since $\mathfrak{q}(H) = \mathfrak{e}(H)$).

[283] *Proof.* Each $h \in H$ satisfies

$$\begin{aligned}(\mathfrak{j} \circ \mathfrak{e}')(h) = \mathfrak{j}(\mathfrak{e}'(h)) &= \mathfrak{e}'(h) \qquad (\text{since } \mathfrak{j} \text{ is just an inclusion map}) \\ &= \mathfrak{e}(h) \qquad (\text{by the definition of } \mathfrak{e}).\end{aligned}$$

Thus, $\mathfrak{j} \circ \mathfrak{e}' = \mathfrak{e}$ (since both $\mathfrak{j} \circ \mathfrak{e}'$ and $\mathfrak{e}$ are maps from H to H). Now,

$$(\operatorname{symlift}\mathfrak{j}) \circ \underbrace{\mathfrak{q}}_{=\operatorname{syminc}_{\mathfrak{e}(H)}\circ\mathfrak{e}'} = \underbrace{(\operatorname{symlift}\mathfrak{j}) \circ \operatorname{syminc}_{\mathfrak{e}(H)}}_{=\mathfrak{j}} \circ \mathfrak{e}' = \mathfrak{j} \circ \mathfrak{e}' = \mathfrak{e}.$$

[284] *Proof.* Let $x \in \operatorname{Sym}(\mathfrak{e}(H))$. Thus, $x \in \operatorname{Sym}(\mathfrak{e}(H)) = e^{*\mathfrak{q}}(H)$ (since the map $e^{*\mathfrak{q}}$ is surjective). In other words, there exists some $y \in H$ such that $x = e^{*\mathfrak{q}}(y)$. Consider this y. Now, $((\operatorname{symlift}\mathfrak{j}) \circ e^{*\mathfrak{q}})(y) = (\operatorname{symlift}\mathfrak{j})\left(\underbrace{e^{*\mathfrak{q}}(y)}_{=x}\right) = (\operatorname{symlift}\mathfrak{j})(x)$, so that $(\operatorname{symlift}\mathfrak{j})(x) =$

H and $e^{*\mathfrak{q}} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ are mutually inverse. Furthermore, we have already shown that these two maps are k-algebra homomorphisms. This completes the proof of Theorem 38.2 **(d)**.

(e) Theorem 38.2 **(d)** shows that the two k-algebra homomorphisms $\operatorname{symlift}\mathfrak{j} : \operatorname{Sym}(\mathfrak{e}(H)) \to H$ and $e^{*\mathfrak{q}} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ are mutually inverse. Hence, these two k-algebra homomorphisms are invertible, and thus are k-algebra isomorphisms. In particular, $\operatorname{symlift}\mathfrak{j} : \operatorname{Sym}(\mathfrak{e}(H)) \to H$ is a k-algebra isomorphism. Thus, $\operatorname{Sym}(\mathfrak{e}(H)) \cong H$ as k-algebras. This proves Theorem 38.2 **(e).** □

Remark 38.15. It is possible to slightly improve Theorem 38.2: Namely, the symmetric algebra $\operatorname{Sym}(\mathfrak{e}(H))$ canonically becomes a filtered k-algebra[285]. With respect to this filtration, the isomorphism $\operatorname{Sym}(\mathfrak{e}(H)) \cong H$ claimed in Theorem 38.2 **(e)** is actually an isomorphism of **filtered** algebras, since both homomorphisms $\operatorname{symlift}\mathfrak{j} : \operatorname{Sym}(\mathfrak{e}(H)) \to H$ and $e^{*\mathfrak{q}} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ respect the filtration. Proving this is not too difficult (it is mostly an issue of bookkeeping).

§39. More on symmetric algebras

Next, we shall show some more properties of the symmetric algebra $\operatorname{Sym} V$ of a k-vector space V. We begin with the following fact:

Lemma 39.1. Let k be a field of characteristic 0. Let V and W be two k-vector spaces. Let $f : \operatorname{Sym} V \to W$ and $g : \operatorname{Sym} V \to W$ be two k-linear maps. Assume that

$$f(a^n) = g(a^n) \qquad \text{for each } a \in \operatorname{syminc}_V(V) \text{ and } n \in \mathbb{N}. \tag{538}$$

[286] Then, $f = g$.

Proof of Lemma 39.1. Let A be the k-algebra $\operatorname{Sym} V$. Recall that syminc_V is a k-linear map $V \to \operatorname{Sym} V$. In other words, syminc_V is a k-linear map $V \to A$ (since $\operatorname{Sym} V = A$).

$\underbrace{((\operatorname{symlift}\mathfrak{j}) \circ e^{*\mathfrak{q}})}_{=\mathrm{id}}(y) = \mathrm{id}(y) = y$. Now,

$$(e^{*\mathfrak{q}} \circ (\operatorname{symlift}\mathfrak{j}))(x) = e^{*\mathfrak{q}}\left(\underbrace{(\operatorname{symlift}\mathfrak{j})(x)}_{=y}\right) = e^{*\mathfrak{q}}(y) = x = \mathrm{id}(x).$$

Now, forget that we fixed x. We thus have shown that $(e^{*\mathfrak{q}} \circ (\operatorname{symlift}\mathfrak{j}))(x) = \mathrm{id}(x)$ for each $x \in \operatorname{Sym}(\mathfrak{e}(H))$. In other words, $e^{*\mathfrak{q}} \circ (\operatorname{symlift}\mathfrak{j}) = \mathrm{id}$.

[285] Indeed, whenever V is a filtered k-vector space, its symmetric algebra $\operatorname{Sym} V$ becomes a filtered k-algebra. In our situation, we can apply this to $V = \mathfrak{e}(H)$ (indeed, the vector space $\mathfrak{e}(H)$ becomes filtered by virtue of being a subspace of H), and thus conclude that $\operatorname{Sym}(\mathfrak{e}(H))$ canonically becomes a filtered k-algebra.

[286] See Definition 38.1 for the definition of the map $\operatorname{syminc}_V : V \to \operatorname{Sym} V$.

Let $U = \operatorname{syminc}_V(V)$. Then, U is a k-vector subspace of A (since syminc_V is a k-linear map $V \to A$). Also, $xy - yx \in U$ for any $x \in U$ and $y \in U$ [287].

Consider the tensor algebra $\otimes V$. We identify V with a k-vector subspace of $\otimes V$ by viewing V as the addend $V^{\otimes 1}$ in the direct sum $\bigoplus_{n \in \mathbb{N}} V^{\otimes n} = \otimes V$. Thus, the canonical injection $V \to \otimes V$ becomes an inclusion map.

Recall that the symmetric algebra $\operatorname{Sym} V$ is defined as a quotient algebra of $\otimes V$. Let π be the canonical projection $\otimes V \to \operatorname{Sym} V$. Then, π is a surjective k-algebra homomorphism.

The canonical map $\operatorname{syminc}_V : V \to \operatorname{Sym} V$ factors through the projection $\pi : \otimes V \to \operatorname{Sym} V$. More precisely, $\operatorname{syminc}_V(x) = \pi(x)$ for every $x \in V$ (this follows from the definition of syminc_V). Now,

$$U = \operatorname{syminc}_V(V) = \left\{ \underbrace{\operatorname{syminc}_V(x)}_{=\pi(x)} \mid x \in V \right\} = \{\pi(x) \mid x \in V\}$$
$$= \pi(V). \tag{539}$$

By the definition of the tensor algebra, we have $\otimes V = \bigoplus_{n \in \mathbb{N}} V^{\otimes n}$. Thus, $\otimes V = \bigoplus_{n \in \mathbb{N}} V^{\otimes n} = \sum_{n \in \mathbb{N}} V^{\otimes n}$ (since direct sums are sums).

For every $n \in \mathbb{N}$, we have $V^{\otimes n} = V^n$ as k-vector subspaces of $\otimes V$ (where V^n means $\underbrace{V \cdot V \cdot \cdots \cdot V}_{n \text{ times}}$, as usual) [288]. Hence, $\sum_{n \in \mathbb{N}} V^{\otimes n} = \sum_{n \in \mathbb{N}} V^n$. Thus, $\otimes V = \sum_{n \in \mathbb{N}} V^{\otimes n} = \sum_{n \in \mathbb{N}} V^n$.

Now, the map π is surjective (since it is a projection). Hence,

$$A = \pi\left(\underbrace{\otimes V}_{=\sum_{n \in \mathbb{N}} V^n} \right) = \pi\left(\sum_{n \in \mathbb{N}} V^n \right) = \sum_{n \in \mathbb{N}} \left(\underbrace{\pi(V)}_{\substack{=U \\ \text{(by (539))}}} \right)^n \qquad \text{(since } \pi \text{ is a } k\text{-algebra homomorphism)}$$
$$= \sum_{n \in \mathbb{N}} U^n.$$

[287] *Proof.* Let $x \in U$ and $y \in U$. Then, $x \in U \subseteq A$ and $y \in U \subseteq A$. But the k-algebra A is commutative (since $A = \operatorname{Sym} V$ is the symmetric algebra of a k-vector space). Hence, $xy = yx$ (since $x \in A$ and $y \in A$). Thus, $xy - yx = 0 \in U$ (since U is a k-vector subspace of A). Qed.

[288] *Proof.* Let $n \in \mathbb{N}$. The n-th tensor power $V^{\otimes n}$ is spanned by all pure tensors. In other words,

$$V^{\otimes n} = \left\langle \underbrace{v_1 \otimes v_2 \otimes \cdots \otimes v_n}_{\substack{=v_1 v_2 \cdots v_n \\ \text{(because the multiplication on } \otimes V \text{ is the} \\ \text{tensor product, so we have} \\ v_1 v_2 \cdots v_n = v_1 \otimes v_2 \otimes \cdots \otimes v_n)}} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle$$
$$= \left\langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle.$$

Compared with

$$V^n = \left\langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle,$$

this yields $V^{\otimes n} = V^n$, qed.

Recall that $f : \operatorname{Sym} V \to W$ and $g : \operatorname{Sym} V \to W$ are two k-linear maps. In other words, $f : A \to W$ and $g : A \to W$ are two k-linear maps (since $A = \operatorname{Sym} V$).

We have $f(v^n) = g(v^n)$ for every $v \in U$ and $n \in \mathbb{N}$ [289]. Hence, Corollary 32.7 (applied to U instead of V) yields that $f = g$. This proves Lemma 39.1. $\square$

An easy corollary of Lemma 39.1 (somewhat more suited to certain applications) is the following fact:

Lemma 39.2. Let k be a field of characteristic 0. Let V and W be two k-vector spaces. Let $f : \operatorname{Sym} V \to W$ and $g : \operatorname{Sym} V \to W$ be two k-linear maps. Assume that

$$f(a^n) = g(a^n) \tag{540}$$

for each $a \in \operatorname{syminc}_V(V)$ [290] and each positive integer $n \in \mathbb{N}$. Assume further that $f(1) = g(1)$. Then, $f = g$.

Proof of Lemma 39.2. We have $f(a^n) = g(a^n)$ for each $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$ [291]. Thus, Lemma 39.1 shows that $f = g$. This proves Lemma 39.2. $\square$

Next, we recall the notion of a *symmetric* map:

Definition 39.3. Let V and W be two sets. Let $n \in \mathbb{N}$. A map $f : V^{\times n} \to W$ is said to be *symmetric* if each $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ and each $\gamma \in S_n$ satisfy $f\left(v_{\gamma(1)}, v_{\gamma(2)}, \ldots, v_{\gamma(n)}\right) = f(v_1, v_2, \ldots, v_n)$. (Recall that S_n denotes the n-th symmetric group.)

Now, we can state the well-known universal property of the n-th symmetric power:

Proposition 39.4. Let k be a field. Let V be a k-vector space. Let $n \in \mathbb{N}$. Let π_n be the canonical projection $V^{\otimes n} \to \operatorname{Sym}^n V$. Let W be any k-vector space. Let $f : V^{\times n} \to W$ be any symmetric k-multilinear map. Then, there exists a unique k-linear map $f_{\operatorname{Sym}} : \operatorname{Sym}^n V \to W$ such that every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies $f_{\operatorname{Sym}}(\pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)) = f(v_1, v_2, \ldots, v_n)$.

Proof of Proposition 39.4. Proposition 39.4 is precisely [Grinbe15, Corollary 95] (in the particular case where k is a field)[292]. $\square$

We are now ready for a general construction:

---

[289] *Proof.* Let $v \in U$ and $n \in \mathbb{N}$. Then, $v \in U = \operatorname{syminc}_V(V)$. Hence, (538) (applied to $a = v$) yields $f(v^n) = g(v^n)$. Qed.

[290] See Definition 38.1 for the definition of the map $\operatorname{syminc}_V : V \to \operatorname{Sym} V$.

[291] *Proof.* Let $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$. We must show that $f(a^n) = g(a^n)$.

Clearly, n is an integer. If n is positive, then $f(a^n) = g(a^n)$ follows immediately from (540). Thus, for the rest of this proof, we can WLOG assume that n is not positive. Assume this.

We have $n \leq 0$ (since n is not positive). Hence, $n = 0$ (since $n \in \mathbb{N}$). Thus, $a^n = a^0 = 1$. Hence, $f\left(\underbrace{a^n}_{=1}\right) = f(1) = g\left(\underbrace{1}_{=a^n}\right) = g(a^n)$. Qed.

[292] Notice that the projection that we denote by π_n has been called $\operatorname{sym}_{V,n}$ in [Grinbe15, Corollary 95].

Proposition 39.5. Let k be a field of characteristic 0. Let A be a k-algebra. Let V be a k-vector subspace of A. Then, there exists a unique k-linear map $\operatorname{spr} : \operatorname{Sym} V \to A$ such that every $n \in \mathbb{N}$ and every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfy

$$\begin{aligned} &\operatorname{spr}\left(\operatorname{syminc}_V(v_1)\operatorname{syminc}_V(v_2)\cdots\operatorname{syminc}_V(v_n)\right) \\ &= \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)}. \end{aligned} \tag{541}$$

Before we prove Proposition 39.5, let us recall the universal property of direct sums of vector spaces:

Proposition 39.6. Let k be a field. Let T be a set. Let $(U_t)_{t\in T}$ be a family of k-vector spaces. For each $t \in T$, let $\iota_t : U_t \to \bigoplus_{s\in T} U_s$ be the canonical inclusion of the addend U_t into the direct sum $\bigoplus_{s\in T} U_s$.

Let W be a k-vector space. For each $t \in T$, let $f_t : U_t \to W$ be a k-linear map. Then, there exists a unique k-linear map $f : \bigoplus_{s\in T} U_s \to W$ such that each $t \in T$ satisfies $f_t = f \circ \iota_t$.

Proof of Proposition 39.5. Let $n \in \mathbb{N}$. Let π_n be the canonical projection $V^{\otimes n} \to \operatorname{Sym}^n V$. This projection π_n is k-linear and surjective (since it is a projection).

Let us define a map $\varphi_n : V^{\times n} \to A$ by

$$\left(\varphi_n(v_1, v_2, \ldots, v_n) = \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \qquad \text{for every } (v_1, v_2, \ldots, v_n) \in V^{\times n}\right).$$

Then, this map φ_n is clearly n-multilinear. Moreover, this map φ_n is symmetric[293]. Hence, Proposition 39.4 (applied to $W = A$ and $f = \varphi_n$) shows that there exists a

[293] *Proof.* Let $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ and $\gamma \in S_n$.

Recall that S_n is a group. Hence, the map $S_n \to S_n,\ \sigma \mapsto \gamma\circ\sigma$ is a bijection (since $\gamma \in S_n$). But the definition of φ_n yields

$$\begin{aligned} \varphi_n\left(v_{\gamma(1)}, v_{\gamma(2)}, \ldots, v_{\gamma(n)}\right) &= \frac{1}{n!}\sum_{\sigma\in S_n} \underbrace{v_{\gamma(\sigma(1))}v_{\gamma(\sigma(2))}\cdots v_{\gamma(\sigma(n))}}_{\substack{=v_{(\gamma\circ\sigma)(1)}v_{(\gamma\circ\sigma)(2)}\cdots v_{(\gamma\circ\sigma)(n)} \\ \text{(since } v_{\gamma(\sigma(i))}=v_{(\gamma\circ\sigma)(i)} \text{ for each } i\in\{1,2,\ldots,n\}\text{)}}} \\ &= \frac{1}{n!}\sum_{\sigma\in S_n} v_{(\gamma\circ\sigma)(1)}v_{(\gamma\circ\sigma)(2)}\cdots v_{(\gamma\circ\sigma)(n)} = \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \end{aligned}$$

(here, we have substituted σ for $\gamma\circ\sigma$ in the sum, since the map $S_n \to S_n,\ \sigma \mapsto \gamma\circ\sigma$ is a bijection). Comparing this with

$$\varphi_n(v_1, v_2, \ldots, v_n) = \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)} \qquad \text{(by the definition of } \varphi_n\text{)},$$

we obtain $\varphi_n\left(v_{\gamma(1)}, v_{\gamma(2)}, \ldots, v_{\gamma(n)}\right) = \varphi_n(v_1, v_2, \ldots, v_n)$.

Now, forget that we fixed $(v_1, v_2, \ldots, v_n)$ and γ. We thus have shown that each $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ and each $\gamma \in S_n$ satisfy $\varphi_n\left(v_{\gamma(1)}, v_{\gamma(2)}, \ldots, v_{\gamma(n)}\right) = \varphi_n(v_1, v_2, \ldots, v_n)$. In other words, the map φ_n is symmetric (since the map φ_n is symmetric if and only if each $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ and each $\gamma \in S_n$ satisfy $\varphi_n\left(v_{\gamma(1)}, v_{\gamma(2)}, \ldots, v_{\gamma(n)}\right) = \varphi_n(v_1, v_2, \ldots, v_n)$ (by the definition of "symmetric")).

unique k-linear map $f_{\mathrm{Sym}} : \mathrm{Sym}^n V \to A$ such that every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies $f_{\mathrm{Sym}}(\pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)) = \varphi_n(v_1, v_2, \ldots, v_n)$. Consider this map f_{Sym}, and denote it by ψ_n.

Thus, ψ_n is a k-linear map $f_{\mathrm{Sym}} : \mathrm{Sym}^n V \to A$ such that every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies $f_{\mathrm{Sym}}(\pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)) = \varphi_n(v_1, v_2, \ldots, v_n)$. In other words, ψ_n is a k-linear map $\mathrm{Sym}^n V \to A$ and has the property that every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies

$$\psi_n(\pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)) = \varphi_n(v_1, v_2, \ldots, v_n). \tag{542}$$

Now, each $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies

$$\mathrm{syminc}_V(v_1)\,\mathrm{syminc}_V(v_2)\cdots\mathrm{syminc}_V(v_n) = \pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n) \tag{543}$$

[294] and

$$\psi_n(\pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)) = \frac{1}{n!}\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \tag{546}$$

[295].

---

[294] *Proof of (543):* Let $(v_1, v_2, \ldots, v_n) \in V^{\times n}$.

Consider the tensor algebra $\otimes V$. We identify V with a k-vector subspace of $\otimes V$ by viewing V as the addend $V^{\otimes 1}$ in the direct sum $\bigoplus_{n \in \mathbb{N}} V^{\otimes n} = \otimes V$. Thus, the canonical injection $V \to \otimes V$ becomes an inclusion map.

Recall that the symmetric algebra $\mathrm{Sym}\, V$ is defined as a quotient algebra of $\otimes V$. Let π be the canonical projection $\otimes V \to \mathrm{Sym}\, V$. Then, π is a surjective k-algebra homomorphism.

The projection $\pi_n : V^{\otimes n} \to \mathrm{Sym}^n V$ is a restriction of the projection $\pi : \otimes V \to \mathrm{Sym}\, V$ (provided that we regard $V^{\otimes n}$ and $\mathrm{Sym}^n V$ as k-vector subspaces of $\otimes V$ and $\mathrm{Sym}\, V$, respectively). Thus,

$$\pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = \pi(v_1 \otimes v_2 \otimes \cdots \otimes v_n). \tag{544}$$

The canonical map $\mathrm{syminc}_V : V \to \mathrm{Sym}\, V$ factors through the projection $\pi : \otimes V \to \mathrm{Sym}\, V$. More precisely,

$$\mathrm{syminc}_V(x) = \pi(x) \qquad \text{for each } x \in V \tag{545}$$

(this follows from the definition of syminc_V). Now, each $i \in \{1, 2, \ldots, n\}$ satisfies the equality $\mathrm{syminc}_V(v_i) = \pi(v_i)$ (by (545), applied to $x = v_i$). Multiplying these equalities for all $i \in \{1, 2, \ldots, n\}$, we obtain

$$\begin{aligned}
&\mathrm{syminc}_V(v_1)\,\mathrm{syminc}_V(v_2)\cdots\mathrm{syminc}_V(v_n) \\
&= \pi(v_1)\,\pi(v_2)\cdots\pi(v_n) \\
&= \pi\left(\underbrace{v_1 v_2 \cdots v_n}_{\substack{= v_1 \otimes v_2 \otimes \cdots \otimes v_n \\ \text{(since the multiplication in the} \\ \text{algebra } \otimes V \text{ is the tensor product)}}}\right) \qquad \text{(since } \pi \text{ is a } k\text{-algebra homomorphism)} \\
&= \pi(v_1 \otimes v_2 \otimes \cdots \otimes v_n) = \pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)
\end{aligned}$$

(by (544)). This proves (543).

[295] *Proof of (546):* Let $(v_1, v_2, \ldots, v_n) \in V^{\times n}$. Then, (542) yields

$$\psi_n(\pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)) = \varphi_n(v_1, v_2, \ldots, v_n) = \frac{1}{n!}\sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}$$

(by the definition of φ_n). This proves (546).

Now, forget that we fixed n. Thus, for each $n \in \mathbb{N}$, we have constructed a k-linear map $\psi_n : \operatorname{Sym}^n V \to A$, and we have shown that each $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies (543) and (546).

Recall that $\operatorname{Sym} V = \bigoplus_{n \in \mathbb{N}} \operatorname{Sym}^n V = \bigoplus_{s \in \mathbb{N}} \operatorname{Sym}^s V$ (here, we have renamed the index n as s). For each $t \in \mathbb{N}$, let $\iota_t : \operatorname{Sym}^t V \to \bigoplus_{s \in \mathbb{N}} \operatorname{Sym}^s V$ be the canonical inclusion of the addend $\operatorname{Sym}^t V$ into the direct sum $\bigoplus_{s \in \mathbb{N}} \operatorname{Sym}^s V$. We shall use this inclusion to identify $\operatorname{Sym}^t V$ with a subspace of $\bigoplus_{s \in \mathbb{N}} \operatorname{Sym}^s V = \operatorname{Sym} V$. Thus,

$$\iota_t(q) = q \qquad \text{for each } t \in \mathbb{N} \text{ and } q \in \operatorname{Sym}^t V. \tag{547}$$

Proposition 39.6 (applied to $T = \mathbb{N}$, $(U_t)_{t \in T} = \left(\operatorname{Sym}^t V\right)_{t \in \mathbb{N}}$, $W = A$ and $f_t = \psi_t$) shows that there exists a unique k-linear map $f : \bigoplus_{s \in \mathbb{N}} \operatorname{Sym}^s V \to A$ such that each $t \in \mathbb{N}$ satisfies $\psi_t = f \circ \iota_t$. Consider this f.

We know that f is a k-linear map $\bigoplus_{s \in \mathbb{N}} \operatorname{Sym}^s V \to A$. In other words, f is a k-linear map $\operatorname{Sym} V \to A$ (since $\operatorname{Sym} V = \bigoplus_{s \in \mathbb{N}} \operatorname{Sym}^s V$).

Every $n \in \mathbb{N}$ and every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfy

$$\begin{aligned} & f\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right) \\ &= \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \end{aligned} \tag{548}$$

[296]. Hence, there exists **at least one** k-linear map $\operatorname{spr} : \operatorname{Sym} V \to A$ such that every $n \in \mathbb{N}$ and every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfy (541) (namely, $\operatorname{spr} = f$).

Next, I shall show the following claim:

Claim 1: Let $\operatorname{spr} : \operatorname{Sym} V \to A$ be a k-linear map such that every $n \in \mathbb{N}$ and every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfy (541). Then, $\operatorname{spr} = f$.

[*Proof of Claim 1:* The maps spr and f are k-linear. Thus, their difference $\operatorname{spr} - f$ is k-linear as well. Hence, $\operatorname{Ker}(\operatorname{spr} - f)$ is a k-vector subspace of $\operatorname{Sym} V$.

[296] *Proof of (548):* Let $n \in \mathbb{N}$ and $(v_1, v_2, \ldots, v_n) \in V^{\times n}$. We must prove (548).

Recall that each $t \in \mathbb{N}$ satisfies $\psi_t = f \circ \iota_t$. Applying this to $t = n$, we obtain $\psi_n = f \circ \iota_n$.

But (543) yields $\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n) = \pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n) \in \operatorname{Sym}^n V$. Thus, (547) (applied to $t = n$ and $q = \operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)$) yields

$$\iota_n\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right) = \operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n).$$

Now,

$$\begin{aligned} & \underbrace{\psi_n}_{= f \circ \iota_n}\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right) \\ &= (f \circ \iota_n)\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right) \\ &= f\left(\underbrace{\iota_n\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right)}_{= \operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)}\right) \\ &= f\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right). \end{aligned}$$

Fix $n \in \mathbb{N}$. The k-vector space $V^{\otimes n}$ is spanned by its pure tensors. In other words,

$$V^{\otimes n} = \left\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle.$$

Thus,

$$\begin{aligned} V^{\otimes n} &= \left\langle v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\ &= \left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle. \end{aligned}$$

Applying the map π_n to both sides of this equality, we obtain

$$\begin{aligned} \pi_n\left(V^{\otimes n}\right) &= \pi_n\left(\left\langle \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle\right) \\ &= \left\langle \underbrace{\pi_n\left(\left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}\right)}_{= \left\{ \pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n) \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}} \right\rangle \\ &\qquad \left(\begin{array}{c} \text{by (165), applied to } M = V^{\otimes n},\ R = \operatorname{Sym}^n V,\ \phi = \pi_n \text{ and} \\ S = \left\{ v_1 \otimes v_2 \otimes \cdots \otimes v_n \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \end{array} \right) \\ &= \left\langle \left\{ \pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle. \end{aligned}$$

Comparing this with $\pi_n\left(V^{\otimes n}\right) = \operatorname{Sym}^n V$ (since the map π_n is surjective), we obtain

$$\operatorname{Sym}^n V = \left\langle \left\{ \pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle. \tag{549}$$

Each $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies

$$\begin{aligned} &(\operatorname{spr} - f)\left(\underbrace{\pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right)}_{\substack{= \operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n) \\ \text{(by (543))}}} \right) \\ &= (\operatorname{spr} - f)\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right) \\ &= \underbrace{\operatorname{spr}\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right)}_{\substack{= \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \\ \text{(by (541))}}} \\ &\qquad - \underbrace{f\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right)}_{\substack{= \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \\ \text{(by (548))}}} \\ &= \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} - \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} = 0 \end{aligned}$$

Hence,

$$\begin{aligned} &f\left(\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)\right) \\ &= \psi_n\left(\underbrace{\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)}_{= \pi_n(v_1 \otimes v_2 \otimes \cdots \otimes v_n)} \right) \\ &= \psi_n\left(\pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right)\right) = \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)}. \end{aligned}$$

This proves (548).

and therefore

$$\pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \in \operatorname{Ker}\left(\operatorname{spr} - f\right).$$

In other words, we have

$$\left\{\pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \;\mid\; \left(v_1, v_2, \ldots, v_n\right) \in V^{\times n}\right\} \subseteq \operatorname{Ker}\left(\operatorname{spr} - f\right).$$

Hence, (154) (applied to $\operatorname{Sym} V$, $\{\pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \mid \left(v_1, v_2, \ldots, v_n\right) \in V^{\times n}\}$ and $\operatorname{Ker}\left(\operatorname{spr} - f\right)$ instead of M, S and Q) yields

$$\left\langle\left\{\pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \;\mid\; \left(v_1, v_2, \ldots, v_n\right) \in V^{\times n}\right\}\right\rangle \subseteq \operatorname{Ker}\left(\operatorname{spr} - f\right).$$

Now, (549) becomes

$$\begin{aligned}\operatorname{Sym}^n V &= \left\langle\left\{\pi_n\left(v_1 \otimes v_2 \otimes \cdots \otimes v_n\right) \;\mid\; \left(v_1, v_2, \ldots, v_n\right) \in V^{\times n}\right\}\right\rangle \\ &\subseteq \operatorname{Ker}\left(\operatorname{spr} - f\right).\end{aligned}$$

Now, forget that we fixed n. We thus have shown that $\operatorname{Sym}^n V \subseteq \operatorname{Ker}\left(\operatorname{spr} - f\right)$ for each $n \in \mathbb{N}$. Hence,

$$\sum_{n \in \mathbb{N}} \underbrace{\operatorname{Sym}^n V}_{\subseteq \operatorname{Ker}(\operatorname{spr} - f)} \subseteq \sum_{n \in \mathbb{N}} \operatorname{Ker}\left(\operatorname{spr} - f\right) \subseteq \operatorname{Ker}\left(\operatorname{spr} - f\right)$$

(since $\operatorname{Ker}\left(\operatorname{spr} - f\right)$ is a k-vector space).

But

$$\begin{aligned}\operatorname{Sym} V &= \bigoplus_{n \in \mathbb{N}} \operatorname{Sym}^n V = \sum_{n \in \mathbb{N}} \operatorname{Sym}^n V \qquad \text{(since direct sums are sums)} \\ &\subseteq \operatorname{Ker}\left(\operatorname{spr} - f\right).\end{aligned}$$

Hence, $\operatorname{spr} - f = 0$. Thus, $\operatorname{spr} = f$. This proves Claim 1.]

Now, we contrast the following two facts:

- There exists **at least one** k-linear map $\operatorname{spr} : \operatorname{Sym} V \to A$ such that every $n \in \mathbb{N}$ and every $\left(v_1, v_2, \ldots, v_n\right) \in V^{\times n}$ satisfy (541).[297]
- There exists **at most one** k-linear map $\operatorname{spr} : \operatorname{Sym} V \to A$ such that every $n \in \mathbb{N}$ and every $\left(v_1, v_2, \ldots, v_n\right) \in V^{\times n}$ satisfy (541).[298]

Combining these two facts, we conclude that there exists **a unique** k-linear map $\operatorname{spr} : \operatorname{Sym} V \to A$ such that every $n \in \mathbb{N}$ and every $\left(v_1, v_2, \ldots, v_n\right) \in V^{\times n}$ satisfy (541). This proves Proposition 39.5. □

Next, let us introduce a Hopf algebra structure on the symmetric algebra $\operatorname{Sym} V$ of any k-vector space V:

[297] Indeed, this has been proven above.

[298] This is because each such map spr must be equal to f (by Claim 1).

Theorem 39.7. Let k be a field. Let V be a k-vector space.

Then, there exists a unique k-bialgebra structure on the k-algebra $\operatorname{Sym} V$ whose comultiplication $\Delta_{\operatorname{Sym} V}$ and counity $\varepsilon_{\operatorname{Sym} V}$ satisfy

$$\left(\begin{array}{ll} \Delta_{\operatorname{Sym} V}(v) = v \otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V} \otimes v & \text{and} \quad \varepsilon_{\operatorname{Sym} V}(v) = 0 \\ & \text{for every } v \in \operatorname{syminc}_V(V) \end{array} \right).$$

Definition 39.8. Let k be a field. Let V be a k-vector space.

Then, when we speak of the "k-bialgebra $\operatorname{Sym} V$", we mean the symmetric algebra $\operatorname{Sym} V$ endowed with the unique k-bialgebra structure whose comultiplication $\Delta_{\operatorname{Sym} V}$ and counity $\varepsilon_{\operatorname{Sym} V}$ satisfy

$$\left(\begin{array}{ll} \Delta_{\operatorname{Sym} V}(v) = v \otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V} \otimes v & \text{and} \quad \varepsilon_{\operatorname{Sym} V}(v) = 0 \\ & \text{for every } v \in \operatorname{syminc}_V(V) \end{array} \right).$$

(This is well-defined due to Theorem 39.7.)

Notice that Theorem 39.7 can be viewed as a particular case of Theorem 34.7, because the symmetric algebra $\operatorname{Sym} V$ is the universal enveloping algebra $U(\mathfrak{g})$ for $\mathfrak{g}$ being the abelian Lie algebra on V [299]. Thus, the k-bialgebra $\operatorname{Sym} V$ (where V is a k-vector space) is a particular case of the k-bialgebra $U(\mathfrak{g})$ (where $\mathfrak{g}$ is a Lie algebra).

We observe a simple property of primitive elements in bialgebras:

Proposition 39.9. Let k be a field. Let H be a bialgebra over k. Let $a \in \operatorname{Prim} H$ and $n \in \mathbb{N}$. Then,

$$\Delta_H(a^n) = \sum_{j=0}^{n} \binom{n}{j} a^j \otimes a^{n-j}.$$

Proof of Proposition 39.9. We have $a \in \operatorname{Prim} H =$ (the set of all primitive elements of H). In other words, the element a of H is primitive. In other words, $\Delta(a) = a \otimes 1_H + 1_H \otimes a$ (by the definition of "primitive").

By the axioms of a bialgebra, we know that Δ_H and ε_H are k-algebra homomorphisms (since H is a k-bialgebra).

Define two elements f and g of $H \otimes H$ by $f = a \otimes 1_H$ and $g = 1_H \otimes a$. Then,

$$\underbrace{f}_{=a\otimes 1_H}\,\underbrace{g}_{=1_H\otimes a} = (a \otimes 1_H)(1_H \otimes a) = \underbrace{a1_H}_{=a} \otimes \underbrace{1_H a}_{=a} = a \otimes a.$$

Comparing this with

$$\underbrace{g}_{=1_H\otimes a}\,\underbrace{f}_{=a\otimes 1_H} = (1_H \otimes a)(a \otimes 1_H) = \underbrace{1_H a}_{=a} \otimes \underbrace{a1_H}_{=a} = a \otimes a,$$

we obtain $fg = gf$. In other words, the two elements f and g of $H \otimes H$ commute. Now, let $\mathfrak{H}$ be the k-subalgebra of $H \otimes H$ generated by f and g. Then, the k-algebra $\mathfrak{H}$ is commutative (by Corollary 11.3, applied to $A = H \otimes H$). Hence, we can calculate

[299] The *abelian Lie algebra* on a k-vector space V is defined to be the Lie algebra whose underlying vector space is V, and whose Lie bracket is identically 0.

inside $\mathfrak{H}$ as in any commutative algebra. In particular, we can thus apply the binomial formula to f and g. We thus obtain $(f+g)^i = \sum_{j=0}^{i} \binom{i}{j} f^j g^{i-j}$ for every $i \in \mathbb{N}$. Applying this to $i = n$, we find

$$\begin{aligned}
(f+g)^n &= \sum_{j=0}^{n} \binom{n}{j} \underbrace{f^j}_{\substack{=(a\otimes 1_H)^j \\ (\text{since } f = a\otimes 1_H)}} \underbrace{g^{n-j}}_{\substack{=(1_H\otimes a)^{n-j} \\ (\text{since } g = 1_H\otimes a)}} = \sum_{j=0}^{n} \binom{n}{j} \underbrace{(a\otimes 1_H)^j}_{=a^j\otimes 1_H} \underbrace{(1_H\otimes a)^{n-j}}_{=1_H\otimes a^{n-j}} \\
&= \sum_{j=0}^{n} \binom{n}{j} \underbrace{\left(a^j\otimes 1_H\right)\left(1_H\otimes a^{n-j}\right)}_{=(a^j 1_H)\otimes(1_H a^{n-j})} \\
&= \sum_{j=0}^{n} \binom{n}{j} \underbrace{\left(a^j 1_H\right)}_{=a^j} \otimes \underbrace{\left(1_H a^{n-j}\right)}_{=a^{n-j}} = \sum_{j=0}^{n} \binom{n}{j} a^j \otimes a^{n-j}.
\end{aligned}$$

But recall that Δ_H is a k-algebra homomorphism. Thus,

$$\begin{aligned}
\Delta_H\left(a^n\right) &= \left(\underbrace{\Delta_H(a)}_{=a\otimes 1_H + 1_H\otimes a}\right)^n = \left(\underbrace{a\otimes 1_H}_{=f} + \underbrace{1_H\otimes a}_{=g}\right)^n \\
&= (f+g)^n = \sum_{j=0}^{n} \binom{n}{j} a^j \otimes a^{n-j}.
\end{aligned}$$

This proves Proposition 39.9. □

As a consequence of Proposition 39.9, we obtain the following formula holding in symmetric algebras:

Corollary 39.10. Let k be a field. Let V be a k-vector space. Let $a \in \operatorname{sym}\operatorname{inc}_V(V)$ and $n \in \mathbb{N}$. Then, the comultiplication $\Delta_{\operatorname{Sym} V}$ of the bialgebra $\operatorname{Sym} V$ satisfies

$$\Delta_{\operatorname{Sym} V}\left(a^n\right) = \sum_{j=0}^{n} \binom{n}{j} a^j \otimes a^{n-j}.$$

Proof of Corollary 39.10. Let us first recall that $\Delta_{\operatorname{Sym} V}(v) = v \otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V} \otimes v$ for every $v \in \operatorname{sym}\operatorname{inc}_V(V)$ (by the definition of $\Delta_{\operatorname{Sym} V}$). Applying this to $v = a$, we obtain $\Delta_{\operatorname{Sym} V}(a) = a \otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V} \otimes a$. In other words, the element a of $\operatorname{Sym} V$ is primitive (by the definition of "primitive"). Thus,

$$a \in (\text{the set of all primitive elements of } \operatorname{Sym} V) = \operatorname{Prim}(\operatorname{Sym} V).$$

Hence, Proposition 39.9 (applied to $H = \operatorname{Sym} V$) yields $\Delta_{\operatorname{Sym} V}\left(a^n\right) = \sum_{j=0}^{n} \binom{n}{j} a^j \otimes a^{n-j}$. This proves Corollary 39.10. □

Next, we apply Proposition 39.5 to the situation of a cocommutative filtered bialgebra. It turns out that in this situation, we can say more:

Proposition 39.11. Let k be a field of characteristic 0. Let H be a bialgebra over k. Let V denote the k-vector subspace $\operatorname{Prim} H$ of H. Proposition 39.5 (applied to $A = H$) yields that there exists a unique k-linear map $\operatorname{spr} : \operatorname{Sym} V \to H$ such that every $n \in \mathbb{N}$ and every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfy

$$\begin{aligned} &\operatorname{spr}\left(\operatorname{syminc}_V(v_1)\operatorname{syminc}_V(v_2)\cdots\operatorname{syminc}_V(v_n)\right) \\ &= \frac{1}{n!}\sum_{\sigma\in S_n} v_{\sigma(1)}v_{\sigma(2)}\cdots v_{\sigma(n)}. \end{aligned} \tag{550}$$

Consider this spr.

The map spr is a k-coalgebra homomorphism.

Proof of Proposition 39.11. Let $a \in \operatorname{syminc}_V(V)$. We are going to show that each $n \in \mathbb{N}$ satisfies

$$\left((\operatorname{spr}\otimes\operatorname{spr})\circ\Delta_{\operatorname{Sym} V}\right)(a^n) = \left(\Delta_H\circ\operatorname{spr}\right)(a^n) \tag{551}$$

and

$$\varepsilon_{\operatorname{Sym} V}(a^n) = \left(\varepsilon_H\circ\operatorname{spr}\right)(a^n). \tag{552}$$

First, let us however make some preliminary work.

Recall that $\Delta_{\operatorname{Sym} V}(v) = v\otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V}\otimes v$ for every $v \in \operatorname{syminc}_V(V)$ (by the definition of $\Delta_{\operatorname{Sym} V}$). Applying this to $v = a$, we obtain $\Delta_{\operatorname{Sym} V}(a) = a\otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V}\otimes a$.

Recall that $\varepsilon_{\operatorname{Sym} V}(v) = 0$ for every $v \in \operatorname{syminc}_V(V)$ (by the definition of $\varepsilon_{\operatorname{Sym} V}$). Applying this to $v = a$, we obtain $\varepsilon_{\operatorname{Sym} V}(a) = 0$.

By the axioms of a bialgebra, we know that $\Delta_{\operatorname{Sym} V}$ and $\varepsilon_{\operatorname{Sym} V}$ are k-algebra homomorphisms (since $\operatorname{Sym} V$ is a k-bialgebra).

By the axioms of a bialgebra, we know that Δ_H and ε_H are k-algebra homomorphisms (since H is a k-bialgebra).

We know that $a \in \operatorname{syminc}_V(V)$. In other words, there exists some $w \in V$ such that $a = \operatorname{syminc}_V(w)$. Consider this w.

The equality (550) (applied to 1 and (w) instead of n and $(v_1, v_2, \ldots, v_n)$) yields

$$\begin{aligned} \operatorname{spr}\left(\operatorname{syminc}_V(w)\right) &= \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1}\sum_{\sigma\in S_1} w = \sum_{\sigma\in S_1} w = \sum_{\sigma\in\{\mathrm{id}\}} w \qquad (\text{since } S_1 = \{\mathrm{id}\}) \\ &= w. \end{aligned}$$

Thus, $w = \operatorname{spr}\left(\underbrace{\operatorname{syminc}_V(w)}_{=a}\right) = \operatorname{spr} a$.

Let $n \in \mathbb{N}$. The equality (550) (applied to $(w, w, \ldots, w)$ instead of $(v_1, v_2, \ldots, v_n)$)

yields

$$\operatorname{spr}\left(\underbrace{\operatorname{symincc}_V(w)\operatorname{symincc}_V(w)\cdots\operatorname{symincc}_V(w)}_{n \text{ times } \operatorname{symincc}_V(w)}\right)$$
$$= \frac{1}{n!}\sum_{\sigma\in S_n}\underbrace{\underbrace{ww\cdots w}_{n \text{ times } w}}_{=|S_n|\cdot\underbrace{ww\cdots w}_{n \text{ times } w}} = \frac{1}{n!}\underbrace{|S_n|}_{=n!}\cdot\underbrace{\underbrace{ww\cdots w}_{n \text{ times } w}}_{=w^n} = \frac{1}{n!}n!\cdot w^n = w^n.$$

In view of $\underbrace{\operatorname{symincc}_V(w)\operatorname{symincc}_V(w)\cdots\operatorname{symincc}_V(w)}_{n \text{ times } \operatorname{symincc}_V(w)} = \left(\underbrace{\operatorname{symincc}_V(w)}_{=a}\right)^n = a^n$, this rewrites as

$$\operatorname{spr}(a^n) = w^n. \tag{553}$$

Let us forget that we fixed n. We thus have proven (553) for every $n \in \mathbb{N}$.

Let $n \in \mathbb{N}$. We have $w \in V = \operatorname{Prim} H$. Hence, Proposition 39.9 (applied to w instead of a) yields

$$\Delta_H(w^n) = \sum_{j=0}^{n}\binom{n}{j}w^j \otimes w^{n-j}. \tag{554}$$

But Corollary 39.10 yields

$$\Delta_{\operatorname{Sym} V}(a^n) = \sum_{j=0}^{n}\binom{n}{j}a^j \otimes a^{n-j}.$$

Hence,

$$
\begin{aligned}
&((\operatorname{spr}\otimes\operatorname{spr})\circ\Delta_{\operatorname{Sym}V})(a^n)\\
&=(\operatorname{spr}\otimes\operatorname{spr})\left(\underbrace{\Delta_{\operatorname{Sym}V}(a^n)}_{=\sum_{j=0}^{n}\binom{n}{j}a^j\otimes a^{n-j}}\right)\\
&=(\operatorname{spr}\otimes\operatorname{spr})\left(\sum_{j=0}^{n}\binom{n}{j}a^j\otimes a^{n-j}\right)=\sum_{j=0}^{n}\binom{n}{j}\underbrace{(\operatorname{spr}\otimes\operatorname{spr})\left(a^j\otimes a^{n-j}\right)}_{=\operatorname{spr}(a^j)\otimes\operatorname{spr}(a^{n-j})}\\
&\qquad\text{(since the map } \operatorname{spr}\otimes\operatorname{spr} \text{ is } k\text{-linear)}\\
&=\sum_{j=0}^{n}\binom{n}{j}\underbrace{\operatorname{spr}\left(a^j\right)}_{\substack{=w^j\\ \text{(by (553)}\\ \text{(applied to } j \text{ instead of } n\text{))}}}\otimes\underbrace{\operatorname{spr}\left(a^{n-j}\right)}_{\substack{=w^{n-j}\\ \text{(by (553)}\\ \text{(applied to } n-j \text{ instead of } n\text{))}}}\\
&=\sum_{j=0}^{n}\binom{n}{j}w^j\otimes w^{n-j}=\Delta_H\left(\underbrace{w^n}_{\substack{=\operatorname{spr}(a^n)\\ \text{(by (553))}}}\right)\qquad\text{(by (554))}\\
&=\Delta_H(\operatorname{spr}(a^n))=(\Delta_H\circ\operatorname{spr})(a^n).
\end{aligned}
$$

In other words, (551) holds.

We have $w\in V=\operatorname{Prim}H$. Thus, Remark 6.3 (applied to $x=w$) shows that $\varepsilon(w)=0$. Thus, $\underbrace{\varepsilon_H}_{=\varepsilon}(w)=\varepsilon(w)=0$.

Recall that $\varepsilon_{\operatorname{Sym}V}$ is a k-algebra homomorphism. Thus, $\varepsilon_{\operatorname{Sym}V}(a^n)=\left(\underbrace{\varepsilon_{\operatorname{Sym}V}(a)}_{=0}\right)^n=0^n$.

On the other hand,

$$
\begin{aligned}
(\varepsilon_H\circ\operatorname{spr})(a^n)&=\varepsilon_H\left(\underbrace{\operatorname{spr}(a^n)}_{\substack{=w^n\\ \text{(by (553))}}}\right)=\varepsilon_H(w^n)\\
&=\left(\underbrace{\varepsilon_H(w)}_{=0}\right)^n\qquad\text{(since } \varepsilon_H \text{ is a } k\text{-algebra homomorphism)}\\
&=0^n.
\end{aligned}
$$

Comparing this with $\varepsilon_{\operatorname{Sym}V}(a^n)=0$, we find $\varepsilon_{\operatorname{Sym}V}(a^n)=(\varepsilon_H\circ\operatorname{spr})(a^n)$. In other words, (552) holds.

We have now proven that (551) and (552) hold.

Now, forget that we fixed n. We thus have proven that (551) and (552) hold for each $n \in \mathbb{N}$.

Now, forget that we fixed a. We thus have proven that (551) and (552) hold for each $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$.

In particular, (551) holds for each $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$. In other words, $((\operatorname{spr} \otimes \operatorname{spr}) \circ \Delta_{\operatorname{Sym} V})(a^n) = (\Delta_H \circ \operatorname{spr})(a^n)$ for each $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$. Hence, Lemma 39.1 (applied to $W = H \otimes H$, $f = (\operatorname{spr} \otimes \operatorname{spr}) \circ \Delta_{\operatorname{Sym} V}$ and $g = \Delta_H \circ \operatorname{spr}$) shows that $(\operatorname{spr} \otimes \operatorname{spr}) \circ \Delta_{\operatorname{Sym} V} = \Delta_H \circ \operatorname{spr}$. In other words, $\Delta_H \circ \operatorname{spr} = (\operatorname{spr} \otimes \operatorname{spr}) \circ \Delta_{\operatorname{Sym} V}$.

Also, (552) holds for each $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$. In other words, $\varepsilon_{\operatorname{Sym} V}(a^n) = (\varepsilon_H \circ \operatorname{spr})(a^n)$ for each $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$. Hence, Lemma 39.1 (applied to $W = k$, $f = \varepsilon_{\operatorname{Sym} V}$ and $g = \varepsilon_H \circ \operatorname{spr}$) shows that $\varepsilon_{\operatorname{Sym} V} = \varepsilon_H \circ \operatorname{spr}$. In other words, $\varepsilon_H \circ \operatorname{spr} = \varepsilon_{\operatorname{Sym} V}$.

The two equalities $\Delta_H \circ \operatorname{spr} = (\operatorname{spr} \otimes \operatorname{spr}) \circ \Delta_{\operatorname{Sym} V}$ and $\varepsilon_H \circ \operatorname{spr} = \varepsilon_{\operatorname{Sym} V}$ (combined) show that spr is a k-coalgebra homomorphism (by the definition of a k-coalgebra homomorphism). This proves Proposition 39.11. $\square$

Proposition 39.12. Let k be a field of characteristic 0. Let H be a connected filtered cocommutative bialgebra over k. Let V denote the k-vector subspace $\operatorname{Prim} H$ of H. Define the k-linear map $\operatorname{spr} : \operatorname{Sym} V \to H$ as in Proposition 39.11.

The map spr is surjective.

Proof of Proposition 39.12. Theorem 17.12 yields

$$H = \sum_{i \in \mathbb{N}} \operatorname{symp}_i \left(\underbrace{\operatorname{Prim} H}_{=V} \right) = \sum_{i \in \mathbb{N}} \operatorname{symp}_i V = \sum_{n \in \mathbb{N}} \operatorname{symp}_n V$$

(here, we have renamed the summation index i as n).

The set $\operatorname{spr}(\operatorname{Sym} V)$ is a k-vector subspace of H (since spr is a k-linear map).

But every $n \in \mathbb{N}$ satisfies $\operatorname{symp}_n V \subseteq \operatorname{spr}(\operatorname{Sym} V)$ [300]. Thus, $\sum_{n \in \mathbb{N}} \underbrace{\operatorname{symp}_n V}_{\subseteq \operatorname{spr}(\operatorname{Sym} V)} \subseteq \sum_{n \in \mathbb{N}} \operatorname{spr}(\operatorname{Sym} V) \subseteq \operatorname{spr}(\operatorname{Sym} V)$ (since $\operatorname{spr}(\operatorname{Sym} V)$ is a k-vector space). Thus, $H = \operatorname{spr}(\operatorname{Sym} V)$.

[300] *Proof.* Let $n \in \mathbb{N}$. Then, every $(v_1, v_2, \ldots, v_n) \in V^{\times n}$ satisfies

$$\frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} = \operatorname{spr}\left(\underbrace{\operatorname{syminc}_V(v_1) \operatorname{syminc}_V(v_2) \cdots \operatorname{syminc}_V(v_n)}_{\in \operatorname{Sym} V} \right) \qquad \text{(by (550))}$$
$$\in \operatorname{spr}(\operatorname{Sym} V).$$

In other words,

$$\left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \subseteq \operatorname{spr}(\operatorname{Sym} V).$$

Hence, (154) (applied to H, $\left\{ \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\}$ and $\operatorname{spr}(\operatorname{Sym} V)$

$\sum_{n\in\mathbb{N}} \operatorname{symp}_n V \subseteq \operatorname{spr}(\operatorname{Sym} V)$. In other words, the map spr is surjective. This proves Proposition 39.12. $\square$

Let us now state some further properties of the k-bialgebra $\operatorname{Sym} V$:

Theorem 39.13. Let k be a field. Let V be a k-vector space.

(a) We have $\operatorname{Sym} V = \sum_{n\in\mathbb{N}} \left(\operatorname{syminc}_V (V)\right)^n$.

(b) The family $\left(\sum_{n=0}^{i} \left(\operatorname{syminc}_V (V)\right)^n\right)_{i\in\mathbb{N}}$ is a filtration of the k-vector space $\operatorname{Sym} V$.

(c) The k-bialgebra $\operatorname{Sym} V$ endowed with the filtration $\left(\sum_{n=0}^{i} \left(\operatorname{syminc}_V (V)\right)^n\right)_{i\in\mathbb{N}}$ is a connected filtered k-bialgebra.

(d) We have $\operatorname{syminc}_V (V) \subseteq \operatorname{Prim}(\operatorname{Sym} V)$.

(e) The k-bialgebra $\operatorname{Sym} V$ is cocommutative.

(f) The k-bialgebra $\operatorname{Sym} V$ is a Hopf algebra.

Notice that Theorem 39.13 can also be viewed as a particular case of Theorem 34.9 (since the k-bialgebra $\operatorname{Sym} V$ (where V is a k-vector space) is a particular case of the k-bialgebra $U(\mathfrak{g})$ (where $\mathfrak{g}$ is a Lie algebra)). However, we shall give a self-contained proof of the parts of Theorem 39.13 that we will need:

Partial proof of Theorem 39.13. Recall that

$$\Delta_{\operatorname{Sym} V}(v) = v \otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V} \otimes v \qquad \text{for every } v \in \operatorname{syminc}_V (V) \tag{555}$$

(by the definition of the map $\Delta_{\operatorname{Sym} V}$).

We have $\operatorname{syminc}_V (V) \subseteq \operatorname{Prim}(\operatorname{Sym} V)$ [301]. This proves Theorem 39.13 **(d)**.

---

instead of M, S and Q) yields

$$\left\langle \left\{ \frac{1}{n!} \sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle \subseteq \operatorname{spr}(\operatorname{Sym} V).$$

Now, the definition of $\operatorname{symp}_n V$ yields

$$\begin{aligned} \operatorname{symp}_n V &= \left\langle \frac{1}{n!} \sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle \\ &= \left\langle \left\{ \frac{1}{n!} \sum_{\sigma\in S_n} v_{\sigma(1)} v_{\sigma(2)} \cdots v_{\sigma(n)} \;\mid\; (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\} \right\rangle \\ &\subseteq \operatorname{spr}(\operatorname{Sym} V). \end{aligned}$$

Qed.

[301] *Proof.* Let $v \in \operatorname{syminc}_V (V)$. Then, $\Delta_{\operatorname{Sym} V}(v) = v \otimes 1_{\operatorname{Sym} V} + 1_{\operatorname{Sym} V} \otimes v$ (according to (555)). In other words, the element v of $\operatorname{Sym} V$ is primitive (by the definition of "primitive"). In other words, $v \in \operatorname{Prim}(\operatorname{Sym} V)$ (since $\operatorname{Prim}(\operatorname{Sym} V)$ is the set of all primitive elements of $\operatorname{Sym} V$).

Now, forget that we fixed v. We thus have shown that every $v \in \operatorname{syminc}_V (V)$ satisfies $v \in \operatorname{Prim}(\operatorname{Sym} V)$. In other words, $\operatorname{syminc}_V (V) \subseteq \operatorname{Prim}(\operatorname{Sym} V)$, qed.

Let π be the canonical projection $\otimes V \to \operatorname{Sym} V$. Then, π is a surjective k-algebra homomorphism. [Actually, π is a k-bialgebra homomorphism, but we don't need to know this.]

The canonical map syminc_V from V to $\operatorname{Sym} V$ factors through the projection $\pi : \otimes V \to \operatorname{Sym} V$. More precisely, $\operatorname{syminc}_V(x) = \pi(x)$ for every $x \in V$ (this follows from the definition of syminc_V). Thus,

$$\operatorname{syminc}_V(V) = \left\{ \underbrace{\operatorname{syminc}_V(x)}_{=\pi(x)} \mid x \in V \right\} = \{\pi(x) \mid x \in V\} = \pi(V). \tag{556}$$

By the definition of the tensor algebra, we have $\otimes V = \bigoplus_{n \in \mathbb{N}} V^{\otimes n}$. Thus, $\otimes V = \bigoplus_{n \in \mathbb{N}} V^{\otimes n} = \sum_{n \in \mathbb{N}} V^{\otimes n}$ (since direct sums are sums).

For every $n \in \mathbb{N}$, we have $V^{\otimes n} = V^n$ as k-vector subspaces of $\otimes V$ (where V^n means $\underbrace{V \cdot V \cdot \cdots \cdot V}_{n \text{ times}}$, as usual) [302]. Hence, $\sum_{n \in \mathbb{N}} V^{\otimes n} = \sum_{n \in \mathbb{N}} V^n$.

Now, $\otimes V = \sum_{n \in \mathbb{N}} V^{\otimes n} = \sum_{n \in \mathbb{N}} V^n$. Applying the map π to this equality, we obtain

$$\pi(\otimes V) = \pi\left(\sum_{n \in \mathbb{N}} V^n\right) = \sum_{n \in \mathbb{N}} \left(\underbrace{\pi(V)}_{\substack{=\operatorname{syminc}_V(V) \\ \text{(by (556))}}} \right)^n \qquad \text{(since } \pi \text{ is a } k\text{-algebra homomorphism)}$$

$$= \sum_{n \in \mathbb{N}} (\operatorname{syminc}_V(V))^n.$$

Since $\pi(\otimes V) = \operatorname{Sym} V$ (because π is surjective), this rewrites as $\operatorname{Sym} V = \sum_{n \in \mathbb{N}} (\operatorname{syminc}_V(V))^n$. Thus, Theorem 39.13 **(a)** is proven.

We have

$$\Delta_{\operatorname{Sym} V}(\operatorname{syminc}_V(V)) \subseteq \operatorname{syminc}_V(V) \otimes (k \cdot 1_{\operatorname{Sym} V}) + (k \cdot 1_{\operatorname{Sym} V}) \otimes \operatorname{syminc}_V(V).$$

[303] Combining this with the equality $\operatorname{Sym} V = \sum_{n \in \mathbb{N}} (\operatorname{syminc}_V(V))^n$, we see that we can

---

[302] *Proof.* Let $n \in \mathbb{N}$. The n-th tensor power $V^{\otimes n}$ is spanned by all pure tensors. In other words,

$$V^{\otimes n} = \left\langle \underbrace{v_1 \otimes v_2 \otimes \cdots \otimes v_n}_{\substack{=v_1 v_2 \cdots v_n \\ \text{(because the multiplication on } \otimes V \text{ is the} \\ \text{tensor product, so we have} \\ v_1 v_2 \cdots v_n = v_1 \otimes v_2 \otimes \cdots \otimes v_n)}} \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle$$

$$= \left\langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle.$$

Compared with

$$V^n = \left\langle v_1 v_2 \cdots v_n \mid (v_1, v_2, \ldots, v_n) \in V^{\times n} \right\rangle,$$

this yields $V^{\otimes n} = V^n$, qed.

[303] *Proof.* Every $v \in \operatorname{syminc}_V(V)$ satisfies

$$\Delta_{\operatorname{Sym} V}(v) = \underbrace{v}_{\in \operatorname{syminc}_V(V)} \otimes \underbrace{1_{\operatorname{Sym} V}}_{\in k \cdot 1_{\operatorname{Sym} V}} + \underbrace{1_{\operatorname{Sym} V}}_{\in k \cdot 1_{\operatorname{Sym} V}} \otimes \underbrace{v}_{\in \operatorname{syminc}_V(V)} \qquad \text{(according to (555))}$$

$$\in \operatorname{syminc}_V(V) \otimes (k \cdot 1_{\operatorname{Sym} V}) + (k \cdot 1_{\operatorname{Sym} V}) \otimes \operatorname{syminc}_V(V).$$

apply Proposition 34.10 to $H = \operatorname{Sym} V$ and $V = \operatorname{syminc}_V(V)$.

Proposition 34.10 **(a)** (applied to $H = \operatorname{Sym} V$ and $V = \operatorname{syminc}_V(V)$) yields that the family $\left(\sum_{n=0}^{i} (\operatorname{syminc}_V(V))^n\right)_{i \in \mathbb{N}}$ is a filtration of the k-vector space $\operatorname{Sym} V$. This proves Theorem 39.13 **(b)**.

Proposition 34.10 **(b)** (applied to $H = \operatorname{Sym} V$ and $V = \operatorname{syminc}_V(V)$) yields that the k-bialgebra $\operatorname{Sym} V$ endowed with the filtration $\left(\sum_{n=0}^{i} (\operatorname{syminc}_V(V))^n\right)_{i \in \mathbb{N}}$ is a connected filtered k-bialgebra. This proves Theorem 39.13 **(c)**.

Finally, Proposition 34.10 **(c)** (applied to $H = \operatorname{Sym} V$ and $V = \operatorname{syminc}_V(V)$) yields that the k-bialgebra $\operatorname{Sym} V$ is cocommutative (since $\operatorname{syminc}_V(V) \subseteq \operatorname{Prim}(\operatorname{Sym} V)$). This proves Theorem 39.13 **(e)**.

We are not going to prove Theorem 39.13 **(f)** (as we are not going to need it). □

Next, let us show a slight extension of Theorem 33.1:

Corollary 39.14. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let $v \in \operatorname{Prim} H$ and $n \in \mathbb{N}$. Then,

$$(\operatorname{Log} \operatorname{id})(v^n) = \delta_{n,1} v.$$

Here, we are using the *Kronecker delta notation* (i.e., whenever u and v are two objects, we set $\delta_{u,v} = \begin{cases} 1, & \text{if } u = v; \\ 0, & \text{if } u \neq v \end{cases}$).

Proof of Corollary 39.14. Recall that $\operatorname{id} \in G(H,H)$. Thus, $\operatorname{Log} \operatorname{id} \in \mathfrak{g}(H,H)$ (because $\operatorname{Log} F \in \mathfrak{g}(H,H)$ for every $F \in G(H,H)$). Hence,

$$\operatorname{Log} \operatorname{id} \in \mathfrak{g}(H,H) = \{f \in \mathcal{L}(H,H) \mid f(1_H) = 0\}$$

(by the definition of $\mathfrak{g}(H,H)$). In other words, $\operatorname{Log} \operatorname{id}$ is an element $f \in \mathcal{L}(H,H)$ satisfying $f(1_H) = 0$. In other words, $\operatorname{Log} \operatorname{id}$ is an element of $\mathcal{L}(H,H)$ and satisfies $(\operatorname{Log} \operatorname{id})(1_H) = 0$.

We are in one of the following three cases:

Case 1: We have $n = 0$.

Case 2: We have $n = 1$.

Case 3: We have neither $n = 0$ nor $n = 1$.

Let us first consider Case 1. In this case, we have $n = 0$. Hence, $v^n = v^0 = 1_H$. Applying the map $\operatorname{Log} \operatorname{id}$ to both sides of this equality, we obtain $(\operatorname{Log} \operatorname{id})(v^n) = (\operatorname{Log} \operatorname{id})(1_H) = 0$. Comparing this with $\underbrace{\delta_{n,1}}_{\substack{=0 \\ (\text{since } n=0 \neq 1)}} v = 0$, we obtain $(\operatorname{Log} \operatorname{id})(v^n) = \delta_{n,1} v$. Thus, Corollary 39.14 is proven in Case 1.

Let us now consider Case 2. In this case, we have $n = 1$. Hence, $v^n = v^1 = v$. But Proposition 6.2 **(c)** (applied to $A = H$ and $F = \operatorname{id}$) shows that $(\operatorname{Log} \operatorname{id})|_{\operatorname{Prim} H} = \operatorname{id}|_{\operatorname{Prim} H}$. But $v \in \operatorname{Prim} H$. Thus,

$$(\operatorname{Log} \operatorname{id})(v) = \underbrace{((\operatorname{Log} \operatorname{id})|_{\operatorname{Prim} H})}_{= \operatorname{id}|_{\operatorname{Prim} H}}(v) = (\operatorname{id}|_{\operatorname{Prim} H})(v) = \operatorname{id}(v) = v.$$

In other words, $\Delta_{\operatorname{Sym} V}(\operatorname{syminc}_V(V)) \subseteq \operatorname{syminc}_V(V) \otimes (k \cdot 1_{\operatorname{Sym} V}) + (k \cdot 1_{\operatorname{Sym} V}) \otimes \operatorname{syminc}_V(V)$, qed.

Now, $(\operatorname{Log}\operatorname{id})\left(\underbrace{v^n}_{=v}\right) = (\operatorname{Log}\operatorname{id})(v) = v$. Comparing this with $\underbrace{\delta_{n,1}}_{\substack{=1 \\ (\text{since } n=1)}} v = v$, we obtain $(\operatorname{Log}\operatorname{id})(v^n) = \delta_{n,1} v$. Thus, Corollary 39.14 is proven in Case 2.

Now, let us consider Case 3. In this case, we have neither $n = 0$ nor $n = 1$. Thus, $n \notin \{0, 1\}$. Combining $n \in \mathbb{N}$ with $n \in \{0, 1\}$, we find $n \in \mathbb{N} \setminus \{0, 1\} = \{2, 3, 4, \ldots\}$, so that $n \geq 2 > 1$. Thus, Theorem 33.1 shows that $(\operatorname{Log}\operatorname{id})(v^n) = 0$. But $n > 1$ and thus $n \neq 1$. Hence, $\delta_{n,1} = 0$. Comparing $(\operatorname{Log}\operatorname{id})(v^n) = 0$ with $\underbrace{\delta_{n,1}}_{=0} v = 0$, we obtain $(\operatorname{Log}\operatorname{id})(v^n) = \delta_{n,1} v$. Thus, Corollary 39.14 is proven in Case 3.

We now have proven Corollary 39.14 in each of the three Cases 1, 2 and 3. Thus, Corollary 39.14 is proven (since these three Cases cover all possibilities). □

Next, we shall show a result that resembles Theorem 38.2 but concerns cocommutative bialgebras rather than commutative bialgebras:

Lemma 39.15. Let k be a field of characteristic 0. Let H be a connected filtered cocommutative bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. Let $\mathfrak{e}$ denote the map $\operatorname{Log}\operatorname{id} \in \mathcal{L}(H, H)$.

Let $\mathfrak{j}$ denote the inclusion map $\mathfrak{e}(H) \to H$. Define a map $\mathfrak{e}' : H \to \mathfrak{e}(H)$ by

$$(\mathfrak{e}'(h) = \mathfrak{e}(h) \qquad \text{for every } h \in H).$$

[304] This map $\mathfrak{e}'$ is clearly k-linear[305]. Define a k-linear map $\mathfrak{q} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ by $\mathfrak{q} = \operatorname{syminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'$.

Let V denote the k-vector subspace $\operatorname{Prim} H$ of H. Define the k-linear map $\operatorname{spr} : \operatorname{Sym} V \to H$ as in Proposition 39.11.

Recall that $\operatorname{Sym} V$ is a connected filtered k-bialgebra (according to Theorem 39.13 **(c)**). Hence, a k-linear map $\operatorname{Log}\operatorname{id}_{\operatorname{Sym} V} : \operatorname{Sym} V \to \operatorname{Sym} V$ is defined for this k-bialgebra $\operatorname{Sym} V$ (in the same way as the k-linear map $\operatorname{Log}\operatorname{id} : H \to H$ is defined for the k-bialgebra H).

(a) We have $\mathfrak{e}(H) = V$. Thus, $\mathfrak{q}$ is a k-linear map $H \to \operatorname{Sym} V$, and the map $\mathfrak{q} \circ \operatorname{spr} : \operatorname{Sym} V \to \operatorname{Sym} V$ is well-defined.

(b) We have $\mathfrak{q} \circ \operatorname{spr} = \operatorname{Log}\operatorname{id}_{\operatorname{Sym} V}$.

Proof of Lemma 39.15. Theorem 4.1 shows that the map $\operatorname{Log}\operatorname{id} \in \mathcal{L}(H, H)$ is a projection from H to the subspace $\operatorname{Prim} H$ of all primitive elements of H. Thus, $(\operatorname{Log}\operatorname{id})(H) = \operatorname{Prim} H$. Now, $\underbrace{\mathfrak{e}}_{=\operatorname{Log}\operatorname{id}}(H) = (\operatorname{Log}\operatorname{id})(H) = \operatorname{Prim} H = V$.

Recall that $\mathfrak{q}$ is a k-linear map $H \to \operatorname{Sym}(\mathfrak{e}(H))$. In other words, $\mathfrak{q}$ is a k-linear map $H \to \operatorname{Sym} V$ (since $\mathfrak{e}(H) = V$). Hence, the map $\mathfrak{q} \circ \operatorname{spr} : \operatorname{Sym} V \to \operatorname{Sym} V$ is well-defined (since spr is a k-linear map $\operatorname{Sym} V \to H$). Altogether, we thus have proven Lemma 39.15 **(a)**.

(b) In the following, the symbol "id" (without subscript) shall always mean the identity map $\operatorname{id}_H : H \to H$ (not the identity map $\operatorname{id}_{\operatorname{Sym} V} : \operatorname{Sym} V \to \operatorname{Sym} V$).

[304] This is well-defined, since $\mathfrak{e}(h) \in \mathfrak{e}(H)$ for every $h \in H$.

[305] In fact, this map $\mathfrak{e}'$ is obtained from the k-linear map $\mathfrak{e}$ by changing the target to $\mathfrak{e}(H)$.

We know that the map $\mathfrak{q} \circ \operatorname{spr} : \operatorname{Sym} V \to \operatorname{Sym} V$ is well-defined. Denote this map by f. Thus, $f = \mathfrak{q} \circ \operatorname{spr}$ is a map from $\operatorname{Sym} V$ to $\operatorname{Sym} V$.

We have $f = \mathfrak{q} \circ \operatorname{spr}$. Hence, f is the composition of two k-linear maps (since the two maps $\mathfrak{q}$ and spr are k-linear). Thus, f itself is k-linear.

Define a k-linear map $g : \operatorname{Sym} V \to \operatorname{Sym} V$ by $g = \operatorname{Log} \operatorname{id}_{\operatorname{Sym} V}$.

In the following, we shall use the *Kronecker delta notation* (i.e., whenever u and v are two objects, we set $\delta_{u,v} = \begin{cases} 1, & \text{if } u = v; \\ 0, & \text{if } u \neq v \end{cases}$).

Let $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$. We shall show that $f(a^n) = g(a^n)$.

We have $a \in \operatorname{syminc}_V(V) \subseteq \operatorname{Prim}(\operatorname{Sym} V)$ (by Theorem 39.13 **(d)**). Hence, Corollary 39.14 (applied to $\operatorname{Sym} V$ and a instead of H and v) shows that $(\operatorname{Log} \operatorname{id}_{\operatorname{Sym} V})(a^n) = \delta_{n,1} a$. Thus, $\underbrace{g}_{=\operatorname{Log} \operatorname{id}_{\operatorname{Sym} V}}(a^n) = (\operatorname{Log} \operatorname{id}_{\operatorname{Sym} V})(a^n) = \delta_{n,1} a$.

We know that $a \in \operatorname{syminc}_V(V)$. In other words, there exists some $w \in V$ such that $a = \operatorname{syminc}_V(w)$. Consider this w.

We have $\operatorname{spr}(a^n) = w^n$. (Indeed, this is the equality (553) from the proof of Proposition 39.11, and has already been shown during the proof of Proposition 39.11.)

We have $w \in V = \operatorname{Prim} H$. Hence, Corollary 39.14 (applied to $v = w$) shows that $(\operatorname{Log} \operatorname{id})(w^n) = \delta_{n,1} w$.

The definition of $\mathfrak{e}'$ yields $\mathfrak{e}'(w^n) = \underbrace{\mathfrak{e}}_{=\operatorname{Log} \operatorname{id}}(w^n) = (\operatorname{Log} \operatorname{id})(w^n) = \delta_{n,1} w$.

Now,

$$\underbrace{f}_{=\mathfrak{q} \circ \operatorname{spr}}(a^n) = (\mathfrak{q} \circ \operatorname{spr})(a^n) = \underbrace{\mathfrak{q}}_{=\operatorname{syminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'}\left(\underbrace{\operatorname{spr}(a^n)}_{=w^n}\right) = \left(\operatorname{syminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'\right)(w^n)$$

$$= \underbrace{\operatorname{syminc}_{\mathfrak{e}(H)}}_{\substack{=\operatorname{syminc}_V \\ (\text{since } \mathfrak{e}(H) = V)}}\left(\underbrace{\mathfrak{e}'(w^n)}_{=\delta_{n,1} w}\right) = \operatorname{syminc}_V(\delta_{n,1} w)$$

$$= \delta_{n,1} \underbrace{\operatorname{syminc}_V(w)}_{=a} \qquad (\text{since the map } \operatorname{syminc}_V \text{ is } k\text{-linear})$$

$$= \delta_{n,1} a.$$

Comparing this with $g(a^n) = \delta_{n,1} a$, we obtain $f(a^n) = g(a^n)$.

Now, forget that we fixed a. We thus have shown that $f(a^n) = g(a^n)$ for each $a \in \operatorname{syminc}_V(V)$ and $n \in \mathbb{N}$. Thus, Lemma 39.1 (applied to $W = \operatorname{Sym} V$) shows that $f = g$. Comparing this with $f = \mathfrak{q} \circ \operatorname{spr}$, we obtain $\mathfrak{q} \circ \operatorname{spr} = f = g = \operatorname{Log} \operatorname{id}_{\operatorname{Sym} V}$. This proves Lemma 39.15 **(b)**. □

Theorem 39.16. Let k be a field of characteristic 0. Let H be a connected filtered cocommutative bialgebra over k. Consider the convolution algebra $\mathcal{L}(H, H)$. Let $\mathfrak{e}$ denote the map $\operatorname{Log} \operatorname{id} \in \mathcal{L}(H, H)$.

Let $\mathfrak{j}$ denote the inclusion map $\mathfrak{e}(H) \to H$. Define a map $\mathfrak{e}' : H \to \mathfrak{e}(H)$ by

$$(\mathfrak{e}'(h) = \mathfrak{e}(h) \qquad \text{for every } h \in H).$$

[306] This map $\mathfrak{e}'$ is clearly k-linear[307]. Define a k-linear map $\mathfrak{q} : H \to \operatorname{Sym}(\mathfrak{e}(H))$ by $\mathfrak{q} = \operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'$.

Let V denote the k-vector subspace $\operatorname{Prim} H$ of H. Define the k-linear map $\operatorname{spr} : \operatorname{Sym} V \to H$ as in Proposition 39.11.

From Lemma 39.15 **(a)**, we know that $\mathfrak{e}(H) = V$. Thus, $\mathfrak{q}$ is a k-linear map $H \to \operatorname{Sym} V$.

Recall that $\operatorname{Sym} V$ is a connected filtered k-bialgebra (according to Theorem 39.13 **(c)**).

The maps $e^{*\mathfrak{q}} : H \to \operatorname{Sym} V$ and $\operatorname{spr} : \operatorname{Sym} V \to H$ are mutually inverse k-coalgebra isomorphisms.

Proof of Theorem 39.16. Recall that $\mathfrak{q}$ is a k-linear map $H \to \operatorname{Sym}(\mathfrak{e}(H))$. In other words, $\mathfrak{q}$ is a k-linear map $H \to \operatorname{Sym} V$ (since $\mathfrak{e}(H) = V$).

The map $\operatorname{spr} : \operatorname{Sym} V \to H$ is a k-coalgebra homomorphism (by Proposition 39.11) and is surjective (by Proposition 39.12).

We have $\mathfrak{q} \in \mathfrak{g}(H, \operatorname{Sym} V)$ [308]. Hence, the map $e^{*\mathfrak{q}} : H \to \operatorname{Sym} V$ is well-defined.

Recall that $\operatorname{spr} : \operatorname{Sym} V \to H$ is a k-coalgebra homomorphism. Also $\operatorname{spr}(1_{\operatorname{Sym} V}) = 1_H$ [309].

Hence, Proposition 31.1 **(e)** (applied to H, $\operatorname{Sym} V$, $\operatorname{Sym} V$ and spr instead of C, D, A and φ) shows that every $f \in \mathfrak{g}(H, \operatorname{Sym} V)$ satisfies $f \circ \operatorname{spr} \in \mathfrak{g}(\operatorname{Sym} V, \operatorname{Sym} V)$ and $e^{*(f \circ \operatorname{spr})} = e^{*f} \circ \operatorname{spr}$. Applying this to $f = \mathfrak{q}$, we obtain $\mathfrak{q} \circ \operatorname{spr} \in \mathfrak{g}(\operatorname{Sym} V, \operatorname{Sym} V)$ and $e^{*(\mathfrak{q} \circ \operatorname{spr})} = e^{*\mathfrak{q}} \circ \operatorname{spr}$.

---

[306] This is well-defined, since $\mathfrak{e}(h) \in \mathfrak{e}(H)$ for every $h \in H$.

[307] In fact, this map $\mathfrak{e}'$ is obtained from the k-linear map $\mathfrak{e}$ by changing the target to $\mathfrak{e}(H)$.

[308] *Proof.* We have $(\operatorname{Log} \operatorname{id})(1_H) = 0$. (This has already been proven in the proof of Corollary 39.14). Now, the definition of $\mathfrak{e}'$ yields $\mathfrak{e}'(1_H) = \underbrace{\mathfrak{e}}_{=\operatorname{Log} \operatorname{id}}(1_H) = (\operatorname{Log} \operatorname{id})(1_H) = 0$. Furthermore, $\underbrace{\mathfrak{q}}_{=\operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'}(1_H) = \left(\operatorname{symminc}_{\mathfrak{e}(H)} \circ \mathfrak{e}'\right)(1_H) = \operatorname{symminc}_{\mathfrak{e}(H)}\left(\underbrace{\mathfrak{e}'(1_H)}_{=0}\right) = \operatorname{symminc}_{\mathfrak{e}(H)}(0) = 0$ (since the map $\operatorname{symminc}_{\mathfrak{e}(H)}$ is k-linear).

But $\mathfrak{q}$ is a k-linear map $H \to \operatorname{Sym} V$. In other words, $\mathfrak{q} \in \mathcal{L}(H, \operatorname{Sym} V)$.

Thus, $\mathfrak{q}$ is an $f \in \mathcal{L}(H, \operatorname{Sym} V)$ satisfying $f(1_H) = 0$ (since $\mathfrak{q}(1_H) = 0$). In other words, $\mathfrak{q} \in \{f \in \mathcal{L}(H, \operatorname{Sym} V) \mid f(1_H) = 0\}$.

But the definition of $\mathfrak{g}(H, \operatorname{Sym} V)$ yields $\mathfrak{g}(H, \operatorname{Sym} V) = \{f \in \mathcal{L}(H, \operatorname{Sym} V) \mid f(1_H) = 0\}$. Thus, $\mathfrak{q} \in \{f \in \mathcal{L}(H, \operatorname{Sym} V) \mid f(1_H) = 0\} = \mathfrak{g}(H, \operatorname{Sym} V)$.

[309] *Proof.* The equality (550) (applied to $n = 0$ and $(v_1, v_2, \ldots, v_n) = ()$) yields

$$\operatorname{spr}((\text{empty product in } \operatorname{Sym} V)) = \underbrace{\frac{1}{0!}}_{=\frac{1}{1}=1} \sum_{\sigma \in S_0} \underbrace{(\text{empty product in } H)}_{=1_H} = \sum_{\sigma \in S_0} 1_H = \underbrace{|S_0|}_{=0!=1} \cdot 1_H = 1_H.$$

Comparing this with $\operatorname{spr}\left(\underbrace{(\text{empty product in } \operatorname{Sym} V)}_{=1_{\operatorname{Sym} V}}\right) = \operatorname{spr}(1_{\operatorname{Sym} V})$, we obtain $\operatorname{spr}(1_{\operatorname{Sym} V}) = 1_H$.

We have $\mathrm{id}_{\mathrm{Sym}\, V} \in G(\mathrm{Sym}\, V, \mathrm{Sym}\, V)$ (since $\mathrm{id}_B \in G(B, B)$ for every k-bialgebra B). Thus, Proposition 5.13 **(b)** (applied to $\mathrm{Sym}\, V$, $\mathrm{Sym}\, V$ and $\mathrm{id}_{\mathrm{Sym}\, V}$ instead of A, H and F) yields $e^{*\left(\mathrm{Log}\, \mathrm{id}_{\mathrm{Sym}\, V}\right)} = \mathrm{id}_{\mathrm{Sym}\, V}$.

Lemma 39.15 **(b)** yields $\mathfrak{q} \circ \mathrm{spr} = \mathrm{Log}\, \mathrm{id}_{\mathrm{Sym}\, V}$. Thus, $e^{*(\mathfrak{q} \circ \mathrm{spr})} = e^{*\left(\mathrm{Log}\, \mathrm{id}_{\mathrm{Sym}\, V}\right)} = \mathrm{id}_{\mathrm{Sym}\, V}$. Comparing this with $e^{*(\mathfrak{q} \circ \mathrm{spr})} = e^{*\mathfrak{q}} \circ \mathrm{spr}$, we obtain $e^{*\mathfrak{q}} \circ \mathrm{spr} = \mathrm{id}_{\mathrm{Sym}\, V}$.

Using the surjectivity of spr, it is now easy to conclude that $\mathrm{spr} \circ e^{*\mathfrak{q}} = \mathrm{id}_H$ [310].

Combining the equalities $e^{*\mathfrak{q}} \circ \mathrm{spr} = \mathrm{id}_{\mathrm{Sym}\, V}$ and $\mathrm{spr} \circ e^{*\mathfrak{q}} = \mathrm{id}_H$, we conclude that the maps $e^{*\mathfrak{q}} : H \to \mathrm{Sym}\, V$ and $\mathrm{spr} : \mathrm{Sym}\, V \to H$ are mutually inverse. Thus, these maps are invertible. Furthermore, the inverse of spr is $\mathrm{spr}^{-1} = e^{*\mathfrak{q}}$ (since the maps $e^{*\mathfrak{q}} : H \to \mathrm{Sym}\, V$ and $\mathrm{spr} : \mathrm{Sym}\, V \to H$ are mutually inverse).

The map spr is a k-coalgebra isomorphism (since it is invertible and it is a k-coalgebra homomorphism). Hence, its inverse spr^{-1} is a k-coalgebra isomorphism as well. Since $\mathrm{spr}^{-1} = e^{*\mathfrak{q}}$, this rewrites as follows: The map $e^{*\mathfrak{q}}$ is a k-coalgebra isomorphism. Altogether, we thus have shown that the maps $e^{*\mathfrak{q}} : H \to \mathrm{Sym}\, V$ and $\mathrm{spr} : \mathrm{Sym}\, V \to H$ are mutually inverse k-coalgebra isomorphisms. This proves Theorem 39.16. □

Corollary 39.17. Let k be a field of characteristic 0. Let H be a connected filtered cocommutative bialgebra over k. Let V denote the k-vector subspace $\mathrm{Prim}\, H$ of H. Define the k-linear map $\mathrm{spr} : \mathrm{Sym}\, V \to H$ as in Proposition 39.11. Then, spr is a k-coalgebra isomorphism.

Proof of Corollary 39.17. We shall use the notations introduced in Theorem 39.16.

Theorem 39.16 shows that the maps $e^{*\mathfrak{q}} : H \to \mathrm{Sym}\, V$ and $\mathrm{spr} : \mathrm{Sym}\, V \to H$ are mutually inverse k-coalgebra isomorphisms. Thus, in particular, spr is a k-coalgebra isomorphism. This proves Corollary 39.17. □

We notice that Corollary 39.17 is closely related to [PatReu98, Corollary 4.4]. Indeed, the "canonical map" in the corrected version of [PatReu98, Corollary 4.4][311] (applied to $A = H$) is more or less our map $e^{*\mathfrak{q}} : H \to \mathrm{Sym}\, V$, at least if we identify the invariant space $\bigoplus_{n \in \mathbb{N}} \left((\mathrm{Prim}\, H)^{\otimes n}\right)^{S_n} \subseteq \otimes\, \mathrm{Prim}\, H$ with the symmetric algebra $\mathrm{Sym}\,(\mathrm{Prim}\, H)$.

Remark 39.18. Again, it is possible to slightly improve Theorem 39.16 and Corollary 39.17: Namely, the symmetric algebra $\mathrm{Sym}\, V$ canonically

[310] *Proof.* Let $h \in H$. Then, $h \in H = \mathrm{spr}\,(\mathrm{Sym}\, V)$ (since the map spr is surjective). In other words, there exists some $a \in \mathrm{Sym}\, V$ such that $h = \mathrm{spr}\, a$. Consider this a.

We have $\underbrace{\left(e^{*\mathfrak{q}} \circ \mathrm{spr}\right)}_{=\mathrm{id}_{\mathrm{Sym}\, V}}(a) = \mathrm{id}_{\mathrm{Sym}\, V}(a) = a$, so that $a = \left(e^{*\mathfrak{q}} \circ \mathrm{spr}\right)(a) = e^{*\mathfrak{q}}\left(\underbrace{\mathrm{spr}\, a}_{=h}\right) = e^{*\mathfrak{q}}(h)$. Now,

$$\left(\mathrm{spr} \circ e^{*\mathfrak{q}}\right)(h) = \mathrm{spr}\left(\underbrace{e^{*\mathfrak{q}}(h)}_{=a}\right) = \mathrm{spr}\, a = h = \mathrm{id}_H(h).$$

Now, forget that we fixed h. We thus have shown that $\left(\mathrm{spr} \circ e^{*\mathfrak{q}}\right)(h) = \mathrm{id}_H(h)$ for each $h \in H$. In other words, $\mathrm{spr} \circ e^{*\mathfrak{q}} = \mathrm{id}_H$.

[311] The definition of the "canonical map" in [PatReu98, Corollary 4.4] is slightly wrong: The "$\bigoplus_{n \in \mathbf{N}} \iota^{\otimes n} \circ \Delta_n$" should be replaced by "$\bigoplus_{n \in \mathbf{N}} \frac{1}{n!} \iota^{\otimes n} \circ \Delta_n$".

becomes a filtered k-algebra[312]. With respect to this filtration, the maps $e^{*\mathfrak{q}} : H \to \operatorname{Sym} V$ and $\operatorname{spr} : \operatorname{Sym} V \to H$ in Theorem 39.16 are actually isomorphisms of **filtered** k-coalgebras. Proving this is not too difficult (it is mostly an issue of bookkeeping).

§40. Graded versions of Leray's theorem

The notion of "Leray's theorem" does (to my knowledge) not refer to any particular fact; rather, it stands for a group of results, each of which claims that a commutative bialgebra satisfying certain conditions (e.g., connected filtered or connected graded) must be isomorphic **as an algebra** to a symmetric algebra of a certain vector space. Theorem 38.2 is one of these results; but there are others. To derive one other such result, let us first prepare by analyzing properties of graded vector spaces.

Lemma 40.1. Let k be a field. Let V be a graded k-vector space. For each $m \in \mathbb{N}$, we define a k-vector subspace $V_{>m}$ of V by $V_{>m} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g > m}} V_g$.

Let $f : V \to V$ be a k-linear map.[313] Assume that

$$f(V_n) \subseteq V_{>n} \qquad \text{for each } n \in \mathbb{N}. \tag{557}$$

Then, the map $\mathrm{id}_V - f$ is injective.

Proof of Lemma 40.1. We shall use the notations introduced in Remark 16.15 and in Definition 16.16.

If $n \in \mathbb{N}$ and $m \in \mathbb{N}$ satisfy $m \leq n$, then

$$p_{m,V}(V_{>n}) = 0 \tag{558}$$

[314].

[312] Indeed, V is a filtered k-vector space (by virtue of being a subspace of the filtered k-vector space H), and thus its symmetric algebra $\operatorname{Sym} V$ becomes a filtered k-algebra.

[313] We do not require f to be graded.

[314] *Proof of (558):* Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$ be such that $m \leq n$. The definition of $V_{>n}$ yields $V_{>n} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g > n}} V_g$.

Let $g \in \mathbb{N}$ be such that $g > n$. Then, $g > n \geq m$ (since $m \leq n$). Hence, $g \neq m$. Thus, (111) (applied to m and g instead of n and m) yields $p_{m,V} \mid_{V_g} = 0$. Thus, $\underbrace{\left(p_{m,V} \mid_{V_g}\right)}_{=0}(V_g) = 0(V_g) = 0$. Comparing this with $\left(p_{m,V} \mid_{V_g}\right)(V_g) = p_{m,V}(V_g)$, we obtain $p_{m,V}(V_g) = 0$.

Now, forget that we fixed g. We thus have shown that $p_{m,V}(V_g) = 0$ for each $g \in \mathbb{N}$ satisfying $g > n$. Hence, $\sum\limits_{\substack{g \in \mathbb{N}; \\ g > n}} \underbrace{p_{m,V}(V_g)}_{=0} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g > n}} 0 = 0$.

But recall that $V_{>n} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g > n}} V_g$. Applying the map $p_{m,V}$ to both sides of this equality, we find

$$p_{m,V}(V_{>n}) = p_{m,V}\left(\sum_{\substack{g \in \mathbb{N}; \\ g > n}} V_g\right) = \sum_{\substack{g \in \mathbb{N}; \\ g > n}} p_{m,V}(V_g) \qquad \text{(since the map } p_{m,V} \text{ is } k\text{-linear)}$$
$$= 0.$$

This proves (558).

Each $m \in \mathbb{N}$ satisfies

$$p_{m,V}\left(\sum_{\substack{g \in \mathbb{N}; \\ g \geq m}} f\left(V_g\right)\right) = 0 \tag{559}$$

[315].

Now, let $x \in \operatorname{Ker}\left(\mathrm{id}_V - f\right)$ be arbitrary. We shall prove that $x = 0$.

We have $x \in \operatorname{Ker}\left(\mathrm{id}_V - f\right)$. In other words, x is an element of V satisfying $\left(\mathrm{id}_V - f\right)(x) = 0$. Comparing $\left(\mathrm{id}_V - f\right)(x) = 0$ with $\left(\mathrm{id}_V - f\right)(x) = \underbrace{\mathrm{id}_V(x)}_{=x} - f(x) = x - f(x)$, we obtain $x - f(x) = 0$. In other words, $x = f(x)$.

But (114) (applied to $v = x$) yields

$$x = \sum_{\ell \in \mathbb{N}} p_{\ell,V}(x) = \sum_{g \in \mathbb{N}} p_{g,V}(x) \tag{561}$$

(here, we have renamed the summation index ℓ as g).

Next, we claim that every $g \in \mathbb{N}$ satisfies

$$p_{g,V}(x) = 0. \tag{562}$$

[*Proof of (562):* We will prove (562) by strong induction over g:

Induction step: Let $m \in \mathbb{N}$. Assume that (562) holds for every $g < m$. We must then prove that (562) holds for $g = m$.

We have assumed that (562) holds for every $g < m$. In other words, for every $g \in \mathbb{N}$ satisfying $g < m$, we have

$$p_{g,V}(x) = 0. \tag{563}$$

[315] *Proof of (559):* Let $m \in \mathbb{N}$. Let $g \in \mathbb{N}$ be such that $g \geq m$. Hence, $m \leq g$. But (557) (applied to $n = g$) yields $f\left(V_g\right) \subseteq V_{>g}$. Hence, $p_{m,V}\left(\underbrace{f\left(V_g\right)}_{\subseteq V_{>g}}\right) \subseteq p_{m,V}\left(V_{>g}\right) = 0$ (by (558) (applied to $n = g$)). Hence, $p_{m,V}\left(f\left(V_g\right)\right) = 0$.

Now, forget that we fixed g. We thus have shown that

$$p_{m,V}\left(f\left(V_g\right)\right) = 0 \qquad \text{for each } g \in \mathbb{N} \text{ satisfying } g \geq m. \tag{560}$$

Now, the map $p_{m,V}$ is k-linear. Hence,

$$p_{m,V}\left(\sum_{\substack{g \in \mathbb{N}; \\ g \geq m}} f\left(V_g\right)\right) = \sum_{\substack{g \in \mathbb{N}; \\ g \geq m}} \underbrace{p_{m,V}\left(f\left(V_g\right)\right)}_{\substack{=0 \\ \text{(by (560))}}} = \sum_{\substack{g \in \mathbb{N}; \\ g \geq m}} 0 = 0.$$

This proves (559).

Now, (561) becomes

$$x = \sum_{g\in\mathbb{N}} p_{g,V}(x) = \sum_{\substack{g\in\mathbb{N};\\ g<m}} \underbrace{p_{g,V}(x)}_{\substack{=0\\ \text{(by (563))}}} + \sum_{\substack{g\in\mathbb{N};\\ g\geq m}} p_{g,V}(x) = \underbrace{\sum_{\substack{g\in\mathbb{N};\\ g<m}} 0}_{=0} + \sum_{\substack{g\in\mathbb{N};\\ g\geq m}} p_{g,V}(x)$$

$$= \sum_{\substack{g\in\mathbb{N};\\ g\geq m}} p_{g,V}\left(\underbrace{x}_{\in V}\right)$$

$$\in \sum_{\substack{g\in\mathbb{N};\\ g\geq m}} \underbrace{p_{g,V}(V)}_{\substack{=V_g\\ \text{(by (112) (applied to } n=g))}} = \sum_{\substack{g\in\mathbb{N};\\ g\geq m}} V_g.$$

But recall that

$$x = f\left(\underbrace{x}_{\in \sum\limits_{\substack{g\in\mathbb{N};\\ g\geq m}} V_g}\right) \in f\left(\sum_{\substack{g\in\mathbb{N};\\ g\geq m}} V_g\right) = \sum_{\substack{g\in\mathbb{N};\\ g\geq m}} f(V_g)$$

(since the map f is k-linear). Applying the map $p_{m,V}$ to both sides of this relation, we obtain

$$p_{m,V}(x) \in p_{m,V}\left(\sum_{\substack{g\in\mathbb{N};\\ g\geq m}} f(V_g)\right) = 0 \qquad \text{(by (559))}.$$

In other words, $p_{m,V}(x) = 0$. In other words, (562) holds for $g = m$. This completes the induction step. Thus, the proof of (562) by induction is complete.]

Now, (561) becomes

$$x = \sum_{g\in\mathbb{N}} \underbrace{p_{g,V}(x)}_{\substack{=0\\ \text{(by (562))}}} = \sum_{g\in\mathbb{N}} 0 = 0.$$

Now, forget that we fixed x. We thus have proven that $x = 0$ for each $x \in \operatorname{Ker}(\mathrm{id}_V - f)$. In other words, $\operatorname{Ker}(\mathrm{id}_V - f) \subseteq 0$. Thus, $\operatorname{Ker}(\mathrm{id}_V - f) = 0$. Hence, the map $\mathrm{id}_V - f$ is injective (since this map is k-linear (since the maps id_V and f are k-linear)). This proves Lemma 40.1. □

Our next few lemmas will rely on the notations introduced in Convention 16.19.

Lemma 40.2. Let k be a field. Let V be a graded k-vector space. Let U be a subset of V. Let $n \in \mathbb{N}$.

Consider the map $p_{n,V} : V \to V$ defined in Definition 16.16.

(a) If $U \subseteq V_n$, then $p_{n,V}(U) = U$.

(b) Let $m \in \mathbb{N}$ be such that $m \neq n$. If $U \subseteq V_m$, then $p_{n,V}(U) = 0$.

Proof of Lemma 40.2. **(a)** Assume that $U \subseteq V_n$. The equality (110) yields $p_{n,V}\mid_{V_n} = \mathrm{id}_V\mid_{V_n}$.

But each $x \in U$ satisfies

$$p_{n,V}(x) = \underbrace{\left(p_{n,V} \mid_{V_n}\right)}_{=\mathrm{id}_V \mid_{V_n}}(x) \qquad (\text{since } x \in U \subseteq V_n)$$
$$= \left(\mathrm{id}_V \mid_{V_n}\right)(x) = \mathrm{id}_V(x) = x. \tag{564}$$

Now,

$$p_{n,V}(U) = \left\{ \underbrace{p_{n,V}(x)}_{\substack{=x \\ (\text{by (564)})}} \mid x \in U \right\} = \{x \mid x \in U\} = U.$$

This proves Lemma 40.2 **(a)**.

(b) Assume that $U \subseteq V_m$. But recall that $m \neq n$. Thus, $n \neq m$. Hence, (111) yields $p_{n,V} \mid_{V_m} = 0$. But

$$p_{n,V}\left(\underbrace{U}_{\subseteq V_m}\right) \subseteq p_{n,V}(V_m) = \underbrace{\left(p_{n,V} \mid_{V_m}\right)}_{=0}(V_m) \qquad (\text{since } \left(p_{n,V} \mid_{V_m}\right)(V_m) = p_{n,V}(V_m))$$
$$= 0(V_m) = 0.$$

In other words, $p_{n,V}(U) = 0$. This proves Lemma 40.2 **(b)**. □

Lemma 40.3. Let k be a field. Let A be a graded k-algebra.

(a) Each $n \in \mathbb{N}$ satisfies $(A_1)^n \subseteq A_n$.

(b) Assume that $A = \mathrm{AlgGen}_k(A_1)$. Then, each $n \in \mathbb{N}$ satisfies $A_n = (A_1)^n$.

Proof of Lemma 40.3. **(a)** Since A is a graded k-algebra, we have

$$A_\ell A_m \subseteq A_{\ell+m} \qquad \text{for any } \ell \in \mathbb{N} \text{ and } m \in \mathbb{N}. \tag{565}$$

Each $n \in \mathbb{N}$ satisfies

$$(A_1)^n \subseteq A_n \tag{566}$$

[316]. This proves Lemma 40.3 **(a)**.

[316] *Proof of (566):* We shall prove (566) by induction over n:

Induction base: We have $1_A \in A_0$ (since A is a graded k-algebra). Now, $(A_1)^0 = k \cdot \underbrace{1_A}_{\in A_0} \subseteq k \cdot A_0 \subseteq A_0$ (since A_0 is a k-vector subspace of A). In other words, (566) holds for $n = 0$. This completes the induction base.

Induction step: Let N be a positive integer. Assume that (566) holds for $n = N - 1$. We must prove that (566) holds for $n = N$.

We know that $N - 1 \in \mathbb{N}$ (since N is a positive integer). Hence, (565) (applied to $\ell = N - 1$ and $m = 1$) yields $A_{N-1}A_1 \subseteq A_{(N-1)+1} = A_N$ (since $(N-1)+1 = N$).

But we have assumed that (566) holds for $n = N - 1$. In other words, we have $(A_1)^{N-1} \subseteq A_{N-1}$. Now,

$$(A_1)^N = \underbrace{(A_1)^{N-1}}_{\subseteq A_{N-1}} A_1 \subseteq A_{N-1}A_1 \subseteq A_N.$$

In other words, (566) holds for $n = N$. This completes the induction step.

Thus, the induction proof of (566) is complete.

(b) Recall the following basic fact (recorded in Convention 16.19): If S is a subset of the k-algebra A, then the k-subalgebra of A generated by S is the k-vector subspace $\sum_{\ell \in \mathbb{N}} \langle S \rangle^\ell$ of A. In other words, if S is a subset of the k-algebra A, then

$$(\text{the } k\text{-subalgebra of } A \text{ generated by } S) = \sum_{\ell \in \mathbb{N}} \langle S \rangle^\ell .$$

Applying this to $S = A_1$, we obtain

$$(\text{the } k\text{-subalgebra of } A \text{ generated by } A_1) = \sum_{\ell \in \mathbb{N}} \langle A_1 \rangle^\ell .$$

On the other hand, if W is a k-vector space, and if S is a k-vector subspace of W, then $\langle S \rangle = S$. [317] Applying this to $W = A$ and $S = A_1$, we obtain $\langle A_1 \rangle = A_1$ (since A_1 is a k-vector subspace of A).

But $\operatorname{AlgGen}_k(A_1)$ is defined as the k-subalgebra of A generated by A_1. Hence,

$$\operatorname{AlgGen}_k(A_1) = (\text{the } k\text{-subalgebra of } A \text{ generated by } A_1) = \sum_{\ell \in \mathbb{N}} \underbrace{\langle A_1 \rangle^\ell}_{\substack{=(A_1)^\ell \\ (\text{since } \langle A_1 \rangle = A_1)}}$$

$$= \sum_{\ell \in \mathbb{N}} (A_1)^\ell .$$

The assumptions of Lemma 40.3 now yield

$$A = \operatorname{AlgGen}_k(A_1) = \sum_{\ell \in \mathbb{N}} (A_1)^\ell . \tag{567}$$

We shall use the notations introduced in Remark 16.15 and in Definition 16.16.

Now, fix $n \in \mathbb{N}$. For each $\ell \in \mathbb{N}$ satisfying $\ell \neq n$, we have

$$p_{n,A}\left((A_1)^\ell\right) = 0 \tag{568}$$

[318]. On the other hand,

$$p_{n,A}\left((A_1)^n\right) = (A_1)^n \tag{569}$$

[319].

[317] This is an elementary fact from linear algebra.

[318] *Proof of (568):* Let $\ell \in \mathbb{N}$ satisfy $\ell \neq n$. But (566) (applied to ℓ instead of n) shows that $(A_1)^\ell \subseteq A_\ell$. Hence, Lemma 40.2 **(b)** (applied to A, $(A_1)^\ell$ and ℓ instead of V, U and m) yields $p_{n,A}\left((A_1)^\ell\right) = 0$. This proves (568).

[319] *Proof of (569):* The relation (566) yields $(A_1)^n \subseteq A_n$. Hence, Lemma 40.2 **(a)** (applied to A and $(A_1)^n$ instead of V and U) yields $p_{n,A}\left((A_1)^n\right) = (A_1)^n$. This proves (569).

Applying the map $p_{n,A}$ to both sides of the equality (567), we obtain

$$\begin{aligned}
p_{n,A}(A) &= p_{n,A}\left(\sum_{\ell\in\mathbb{N}} (A_1)^{\ell}\right) = \sum_{\ell\in\mathbb{N}} p_{n,A}\left((A_1)^{\ell}\right) \qquad \text{(since the map } p_{n,A} \text{ is } k\text{-linear)} \\
&= \underbrace{p_{n,A}\left((A_1)^{n}\right)}_{\substack{=(A_1)^n \\ \text{(by (569))}}} + \sum_{\substack{\ell\in\mathbb{N}; \\ \ell\neq n}} \underbrace{p_{n,A}\left((A_1)^{\ell}\right)}_{\substack{=0 \\ \text{(by (568))}}} \\
&\qquad \text{(here, we have split off the addend for } \ell = n \text{ from the sum)} \\
&= (A_1)^n + \underbrace{\sum_{\substack{\ell\in\mathbb{N}; \\ \ell\neq n}} 0}_{=0} = (A_1)^n .
\end{aligned}$$

Thus, $(A_1)^n = p_{n,A}(A) = A_n$ (by (112) (applied to $V = A$)). In other words, $A_n = (A_1)^n$. This proves Lemma 40.3 **(b)**. □

Lemma 40.4. Let k be a field. Let A and B be k-algebras. Let $f : A \to B$ and $g : A \to B$ be two k-algebra homomorphisms. Let U and V be two k-vector subspaces of A. Then,

$$(g-f)(UV) \subseteq ((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V)) .$$

Proof of Lemma 40.4. The map $g - f$ is k-linear (since the maps g and f are k-linear). Hence, $(g-f)(U)$ and $(g-f)(V)$ are k-vector subspaces of B. Also, $g(V)$ is a k-vector subspace of B (since the map g is k-linear), and $f(U)$ is a k-vector subspace of B (since the map f is k-linear). Hence,

$$((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V))$$

is a k-vector subspace of B.

Each $(u, v) \in U \times V$ satisfies

$$(g-f)(uv) \in ((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V)) \tag{570}$$

[320]. In other words,

$$\begin{aligned}&\{(g-f)(uv) \mid (u,v) \in U \times V\}\\ &\subseteq ((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V)).\end{aligned}$$

Thus, (154) (applied to B, $\{(g-f)(uv) \mid (u,v) \in U \times V\}$ and $((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V))$ instead of M, S and Q) shows that

$$\begin{aligned}&\langle \{(g-f)(uv) \mid (u,v) \in U \times V\} \rangle\\ &\subseteq ((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V)).\end{aligned} \tag{571}$$

The definition of UV yields

$$UV = \langle uv \mid (u,v) \in U \times V \rangle = \langle \{uv \mid (u,v) \in U \times V\} \rangle. \tag{572}$$

Thus, (165) (applied to A, B, $g-f$ and $\{uv \mid (u,v) \in U \times V\}$ instead of M, R, ϕ and S) yields

$$\begin{aligned}(g-f)(\langle \{uv \mid (u,v) \in U \times V\} \rangle) &= \langle \{(g-f)(uv) \mid (u,v) \in U \times V\} \rangle\\ &\subseteq ((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V))\end{aligned} \tag{573}$$

(by (571)).

Now, applying the map $g-f$ to both sides of the equality (572), we obtain

$$\begin{aligned}(g-f)(UV) &= (g-f)(\langle \{uv \mid (u,v) \in U \times V\} \rangle)\\ &\subseteq ((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V))\end{aligned}$$

(by (573)). This proves Lemma 40.4. □

As an application of the above lemmata, we can show a criterion for endomorphisms of a graded algebra to be injective:

[320] *Proof of (570):* Let $(u,v) \in U \times V$. Thus, $u \in U$ and $v \in V$.

Now,

$$\begin{aligned}(g-f)(uv) &= \underbrace{g(uv)}_{\substack{=g(u)g(v)\\ \text{(since } g \text{ is a } k\text{-algebra}\\ \text{homomorphism)}}} - \underbrace{f(uv)}_{\substack{=f(u)f(v)\\ \text{(since } f \text{ is a } k\text{-algebra}\\ \text{homomorphism)}}} = g(u)g(v) - f(u)f(v)\\ &= \underbrace{(g(u)g(v) - f(u)g(v))}_{=(g(u)-f(u))\cdot g(v)} + \underbrace{(f(u)g(v) - f(u)f(v))}_{=f(u)\cdot(g(v)-f(v))}\\ &= \underbrace{(g(u)-f(u))}_{=(g-f)(u)} \cdot g(v) + f(u) \cdot \underbrace{(g(v)-f(v))}_{=(g-f)(v)}\\ &= (g-f)\left(\underbrace{u}_{\in U}\right) \cdot g\left(\underbrace{v}_{\in V}\right) + f\left(\underbrace{u}_{\in U}\right) \cdot (g-f)\left(\underbrace{v}_{\in V}\right)\\ &\in ((g-f)(U)) \cdot g(V) + f(U) \cdot ((g-f)(V)).\end{aligned}$$

This proves (570).

Lemma 40.5. Let k be a field. Let A be a graded k-algebra. For each $m \in \mathbb{N}$, we define a k-vector subspace $A_{>m}$ of A by $A_{>m} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g > m}} A_g$.

Let $f : A \to A$ be a k-algebra homomorphism.[321] Assume that each $x \in A_1$ satisfies

$$f(x) - x \in A_{>1}. \tag{574}$$

(a) We have $(\mathrm{id}_A - f)\left((A_1)^n\right) \subseteq A_{>n}$ for each $n \in \mathbb{N}$.

(b) Assume that $A = \mathrm{AlgGen}_k(A_1)$. Then, the map f is injective.

Proof of Lemma 40.5. The map $\mathrm{id}_A - f$ is k-linear (since both maps id_A and f are k-linear). Notice that

$$(\mathrm{id}_A - f)(A_1) \subseteq A_{>1} \tag{575}$$

[322].

Since A is a graded k-algebra, we have

$$A_\ell A_m \subseteq A_{\ell+m} \qquad \text{for any } \ell \in \mathbb{N} \text{ and } m \in \mathbb{N}. \tag{576}$$

Thus, each positive integer N satisfies

$$A_{>1} \cdot A_{N-1} \subseteq A_{>N} \tag{577}$$

[323].

Also,

$$f(A_1) \subseteq A_{>0} \tag{578}$$

[321] We do not require f to be graded.

[322] *Proof of (575):* Each $x \in A_1$ satisfies

$$(\mathrm{id}_A - f)(x) = \underbrace{\mathrm{id}_A(x)}_{=x} - f(x) = x - f(x) = -\underbrace{(f(x) - x)}_{\substack{\in A_{>1} \\ \text{(by (574))}}} \in -A_{>1} \subseteq A_{>1}$$

(since $A_{>1}$ is a k-vector subspace of A).

In other words, $\{(\mathrm{id}_A - f)(x) \mid x \in A_1\} \subseteq A_{>1}$. But $(\mathrm{id}_A - f)(A_1) = \{(\mathrm{id}_A - f)(x) \mid x \in A_1\} \subseteq A_{>1}$. This proves (575).

[323] *Proof of (577):* Let N be a positive integer. Thus, $N - 1 \in \mathbb{N}$. The definition of $A_{>N}$ yields $A_{>N} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g > N}} A_g$.

[324]. Furthermore, every positive integer h satisfies

$$A_h \cdot A_{>N-1} \subseteq A_{>N} \tag{579}$$

[325]. Thus,

$$A_{>0} \cdot A_{>N-1} \subseteq A_{>N} \tag{580}$$

But the definition of $A_{>1}$ yields $A_{>1} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g>1}} A_g$. Hence,

$$\begin{aligned}
\underbrace{A_{>1}}_{= \sum\limits_{\substack{g \in \mathbb{N}; \\ g>1}} A_g} \cdot A_{N-1} &= \left(\sum_{\substack{g \in \mathbb{N}; \\ g>1}} A_g \right) \cdot A_{N-1} = \sum_{\substack{g \in \mathbb{N}; \\ g>1}} \underbrace{A_g A_{N-1}}_{\substack{\subseteq A_{g+(N-1)} \\ \text{(by (576)} \\ \text{(applied to } \ell = g \text{ and } m = N-1))}} \\
&\subseteq \sum_{\substack{g \in \mathbb{N}; \\ g>1}} A_{g+(N-1)} \\
&= \sum_{\substack{g \in \mathbb{N}; \\ g>1+(N-1)}} A_g \qquad \text{(here, we have substituted } g+(N-1) \text{ for } g \text{ in the sum)} \\
&= \sum_{\substack{g \in \mathbb{N}; \\ g>N}} A_g \qquad \text{(since } 1+(N-1) = N\text{)} \\
&= A_{>N} \qquad \left(\text{since } A_{>N} = \sum_{\substack{g \in \mathbb{N}; \\ g>N}} A_g \right).
\end{aligned}$$

This proves (577).

[324] *Proof of (578):* Let $y \in f(A_1)$. Thus, there exists some $x \in A_1$ such that $y = f(x)$. Consider this y.

From (574), we obtain $f(x) - x \in A_{>1}$, so that $f(x) \in x + A_{>1}$.

But the definition of $A_{>1}$ yields $A_{>1} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g>1}} A_g$. Meanwhile, the definition of $A_{>0}$ yields

$$A_{>0} = \sum_{\substack{g \in \mathbb{N}; \\ g>0}} A_g = A_1 + A_2 + A_3 + \cdots = A_1 + \underbrace{(A_2 + A_3 + A_4 + \cdots)}_{= \sum\limits_{\substack{g \in \mathbb{N}; \\ g>1}} A_g = A_{>1}} = A_1 + A_{>1}.$$

But $y = f(x) \in \underbrace{x}_{\in A_1} + A_{>1} \in A_1 + A_{>1} = A_{>0}$.

Now, forget that we fixed y. We thus have proven that $y \in A_{>0}$ for each $y \in f(A_1)$. In other words, $f(A_1) \subseteq A_{>0}$. This proves (578).

[325] *Proof of (579):* Let h be a positive integer. The definition of $A_{>N-1}$ yields $A_{>N-1} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g>N-1}} A_g$. But the definition of $A_{>N}$ yields $A_{>N} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g>N}} A_g$.

But $h \geq 1$ (since h is a positive integer) and thus $(N-1) + \underbrace{h}_{\geq 1} \geq (N-1) + 1 = N$. Hence, every $g \in \mathbb{N}$ satisfying $g > (N-1) + h$ also satisfies $g > N$ (since $g > (N-1) + h \geq N$). Thus, the sum $\sum\limits_{\substack{g \in \mathbb{N}; \\ g>(N-1)+h}} A_g$ is a subsum of the sum $\sum\limits_{\substack{g \in \mathbb{N}; \\ g>N}} A_g$. Hence, $\sum\limits_{\substack{g \in \mathbb{N}; \\ g>(N-1)+h}} A_g \subseteq \sum\limits_{\substack{g \in \mathbb{N}; \\ g>N}} A_g = A_{>N}$.

[326].

(a) We shall prove Lemma 40.5 **(a)** by induction over n:

Induction base: We have $(\mathrm{id}_A - f)\left((A_1)^0\right) = 0$ [327]. Hence, $(\mathrm{id}_A - f)\left((A_1)^0\right) = 0 \subseteq A_{>0}$ (since $A_{>0}$ is a k-vector space). In other words, Lemma 40.5 **(a)** holds for $n = 0$. This completes the induction base.

Induction step: Let N be a positive integer. Assume that Lemma 40.5 **(a)** holds for $n = N-1$. We must show that Lemma 40.5 **(a)** holds for $n = N$.

We have $N - 1 \in \mathbb{N}$ (since N is a positive integer). Thus, Lemma 40.3 **(a)** (applied to $n = N-1$) yields $(A_1)^{N-1} \subseteq A_{N-1}$.

Also, recall that Lemma 40.5 **(a)** holds for $n = N-1$. In other words, we have

---

Now,

$$\begin{aligned} A_h \cdot \underbrace{A_{>N-1}}_{= \sum\limits_{\substack{g \in \mathbb{N}; \\ g > N-1}} A_g} &= A_h \cdot \left(\sum_{\substack{g \in \mathbb{N}; \\ g > N-1}} A_g \right) = \sum_{\substack{g \in \mathbb{N}; \\ g > N-1}} \underbrace{A_h A_g}_{\substack{\subseteq A_{h+g} \\ \text{(by (576)} \\ \text{(applied to } \ell = h \text{ and } m = g))}} \\ &\subseteq \sum_{\substack{g \in \mathbb{N}; \\ g > N-1}} \underbrace{A_{h+g}}_{= A_{g+h}} = \sum_{\substack{g \in \mathbb{N}; \\ g > N-1}} A_{g+h} \\ &= \sum_{\substack{g \in \mathbb{N}; \\ g > (N-1)+h}} A_g \qquad \text{(here, we have substituted } g+h \text{ for } g \text{ in the sum)} \\ &\subseteq A_{>N}. \end{aligned}$$

This proves (579).

[326] *Proof of (580):* The definition of $A_{>0}$ yields

$$A_{>0} = \sum_{\substack{g \in \mathbb{N}; \\ g > 0}} A_g = \sum_{\substack{h \in \mathbb{N}; \\ h > 0}} A_h$$

(here, we have renamed the summation index g as h). Thus,

$$\underbrace{A_{>0}}_{= \sum\limits_{\substack{h \in \mathbb{N}; \\ h > 0}} A_h} \cdot A_{>N-1} = \left(\sum_{\substack{h \in \mathbb{N}; \\ h > 0}} A_h \right) \cdot A_{>N-1} = \sum_{\substack{h \in \mathbb{N}; \\ h > 0}} \underbrace{A_h \cdot A_{>N-1}}_{\substack{\subseteq A_{>N} \\ \text{(by (579))}}} \subseteq \sum_{\substack{h \in \mathbb{N}; \\ h > 0}} A_{>N} \subseteq A_{>N}$$

(since $A_{>N}$ is a k-vector subspace of A). This proves (580).

[327] *Proof.* Recall that f is a k-algebra homomorphism. Hence, $f(1_A) = 1_A$. Now,

$$(\mathrm{id}_A - f)(1_A) = \underbrace{\mathrm{id}_A(1_A)}_{= 1_A} - \underbrace{f(1_A)}_{= 1_A} = 1_A - 1_A = 0.$$

Now,

$$\begin{aligned} (\mathrm{id}_A - f)\left(\underbrace{(A_1)^0}_{= k \cdot 1_A} \right) &= (\mathrm{id}_A - f)(k \cdot 1_A) = k \cdot \underbrace{(\mathrm{id}_A - f)(1_A)}_{=0} \qquad \text{(since the map } \mathrm{id}_A - f \text{ is } k\text{-linear)} \\ &= k \cdot 0 = 0, \end{aligned}$$

qed.

$(\mathrm{id}_A - f)\left((A_1)^{N-1}\right) \subseteq A_{>N-1}$.

Now, both $\mathrm{id}_A : A \to A$ and $f : A \to A$ are k-algebra homomorphisms. Thus, Lemma 40.4 (applied to $B = A$, $U = A_1$ and $V = (A_1)^{N-1}$) shows that

$$\begin{aligned}(\mathrm{id}_A - f)\left(A_1 (A_1)^{N-1}\right) &\subseteq \underbrace{((\mathrm{id}_A - f)(A_1))}_{\substack{\subseteq A_{>1} \\ \text{(by (575))}}} \cdot \underbrace{\mathrm{id}_A\left((A_1)^{N-1}\right)}_{=(A_1)^{N-1} \subseteq A_{N-1}} + \underbrace{f(A_1)}_{\substack{\subseteq A_{>0} \\ \text{(by (578))}}} \cdot \underbrace{\left((\mathrm{id}_A - f)\left((A_1)^{N-1}\right)\right)}_{\subseteq A_{>N-1}} \\ &\subseteq \underbrace{A_{>1} \cdot A_{N-1}}_{\substack{\subseteq A_{>N} \\ \text{(by (577))}}} + \underbrace{A_{>0} \cdot A_{>N-1}}_{\substack{\subseteq A_{>N} \\ \text{(by (580))}}} \\ &\subseteq A_{>N} + A_{>N} \subseteq A_{>N} \qquad \text{(since } A_{>N} \text{ is a } k\text{-vector space)}.\end{aligned}$$

Since $A_1 (A_1)^{N-1} = (A_1)^N$, this rewrites as $(\mathrm{id}_A - f)\left((A_1)^N\right) \subseteq A_{>N}$. In other words, Lemma 40.5 **(a)** holds for $n = N$. This completes the induction step. Thus, Lemma 40.5 **(a)** is proven by induction.

(b) For each $n \in \mathbb{N}$, we have

$$(\mathrm{id}_A - f)\left(\underbrace{A_n}_{\substack{=(A_1)^n \\ \text{(by Lemma 40.3 (b))}}}\right) = (\mathrm{id}_A - f)\left((A_1)^n\right) \subseteq A_{>n}$$

(by Lemma 40.5 **(a)**). Thus, Lemma 40.1 (applied to A and $\mathrm{id}_A - f$ instead of V and f) shows that the map $\mathrm{id}_A - (\mathrm{id}_A - f)$ is injective. Since $\mathrm{id}_A - (\mathrm{id}_A - f) = f$, this rewrites as follows: The map f is injective. This proves Lemma 40.5 **(b)**. □

We shall now prove a simple lemma about homogeneous subspaces:

Lemma 40.6. Let k be a field. Let V be a graded k-vector space. Let W be a homogeneous subspace of V. Then, $p_{n,V}(W) = W \cap V_n$ for any $n \in \mathbb{N}$. (Here, the map $p_{n,V} : V \to V$ is defined as in Definition 16.16.)

Proof of Lemma 40.6. Recall that W is a homogeneous subspace of V if and only if $W = \bigoplus_{n \in \mathbb{N}} (W \cap V_n)$ (by the definition of a "homogeneous subspace"). Hence, $W = \bigoplus_{n \in \mathbb{N}} (W \cap V_n)$ (since W is a homogeneous subspace of V). Thus,

$$\begin{aligned}W &= \bigoplus_{n \in \mathbb{N}} (W \cap V_n) = \sum_{n \in \mathbb{N}} (W \cap V_n) \qquad \text{(since direct sums are sums)} \\ &= \sum_{m \in \mathbb{N}} (W \cap V_m) \qquad (581)\end{aligned}$$

(here, we renamed the summation index n as m).

Let $n \in \mathbb{N}$. For any $m \in \mathbb{N}$ satisfying $m \neq n$, we have

$$p_{n,V}(W \cap V_m) = 0 \qquad (582)$$

[328]. But

$$p_{n,V}\left(W \cap V_n\right) = W \cap V_n \tag{583}$$

[329].

Applying the map $p_{n,V}$ to both sides of the equality (581), we obtain

$$\begin{aligned} p_{n,V}\left(W\right) &= p_{n,V}\left(\sum_{m\in\mathbb{N}} \left(W \cap V_m\right)\right) = \sum_{m\in\mathbb{N}} p_{n,V}\left(W \cap V_m\right) \qquad \text{(since the map } p_{n,V} \text{ is } k\text{-linear)} \\ &= \underbrace{p_{n,V}\left(W \cap V_n\right)}_{\substack{=W\cap V_n \\ \text{(by (583))}}} + \sum_{\substack{m\in\mathbb{N}; \\ m\neq n}} \underbrace{p_{n,V}\left(W \cap V_m\right)}_{\substack{=0 \\ \text{(by (582))}}} \\ &\qquad \text{(here, we have split off the addend for } m = n \text{ from the sum)} \\ &= \left(W \cap V_n\right) + \underbrace{\sum_{\substack{m\in\mathbb{N}; \\ m\neq n}} 0}_{=0} = W \cap V_n. \end{aligned}$$

This proves Lemma 40.6. □

Next, we shall show a criterion for generating sets of graded algebras:

Lemma 40.7. Let k be a field. Let A be a graded k-algebra such that $A_0 = k \cdot 1_A$. For each $m \in \mathbb{N}$, we define a k-vector subspace $A_{>m}$ of A by $A_{>m} = \sum_{\substack{g\in\mathbb{N}; \\ g>m}} A_g$.

Let V be a homogeneous subspace of A such that $A_{>0} = V + \left(A_{>0}\right)^2$. Then:

(a) Every positive integer n satisfies $A_n \subseteq \left(V \cap A_n\right) + \sum_{g=1}^{n-1} A_g A_{n-g}$.

(b) We have $A = \operatorname{AlgGen}_k V$.

Proof of Lemma 40.7. **(a)** We shall use the notations introduced in Remark 16.15 and in Definition 16.16.

Since A is a graded k-algebra, we have

$$A_\ell A_m \subseteq A_{\ell+m} \qquad \text{for any } \ell \in \mathbb{N} \text{ and } m \in \mathbb{N}. \tag{584}$$

Let n be a positive integer. Define a k-vector subspace Q of A by $Q = \sum_{g=1}^{n-1} A_g A_{n-g}$. Then, every two positive integers ℓ and m satisfy

$$p_{n,A}\left(A_\ell A_m\right) \subseteq Q \tag{585}$$

[330]. Hence,

$$p_{n,A}\left(\left(A_{>0}\right)^2\right) \subseteq Q \tag{586}$$

[328] *Proof of (582):* Let $m \in \mathbb{N}$ be such that $m \neq n$. Thus, Lemma 40.2 **(b)** (applied to $W \cap V_m$ instead of U) yields $p_{n,V}\left(W \cap V_m\right) = 0$ (since $W \cap V_m \subseteq V_m$). This proves (582).

[329] *Proof of (583):* Lemma 40.2 **(a)** (applied to $U = W \cap V_n$) yields $p_{n,V}\left(W \cap V_n\right) = W \cap V_n$ (since $W \cap V_n \subseteq V_n$). This proves (583).

[330] *Proof of (585):* Let ℓ and m be two positive integers. We are in one of the following two cases:

[331].

Lemma 40.6 (applied to A and V instead of V and W) yields $p_{n,A}(V) = V \cap A_n$.

Case 1: We have $\ell + m = n$.

Case 2: We have $\ell + m \neq n$.

Let us first consider Case 1. In this case, we have $\ell + m = n$. Thus, $m = n - \ell$. Also, $\ell > 0$ (since ℓ is a positive integer) and $m > 0$ (since m is a positive integer). Also, $n = \ell + \underbrace{m}_{>0} > \ell$, so that $\ell < n$. Combining this with $\ell > 0$, we obtain $\ell \in \{1, 2, \ldots, n-1\}$ (since ℓ is a positive integer). Hence, $A_\ell A_{n-\ell}$ is an addend of the sum $\sum_{g=1}^{n-1} A_g A_{n-g}$. Thus, $A_\ell A_{n-\ell} \subseteq \sum_{g=1}^{n-1} A_g A_{n-g} = Q$.

Now, (584) yields $A_\ell A_m \subseteq A_{\ell+m} = A_n$ (since $\ell + m = n$). Hence, Lemma 40.2 **(a)** (applied to A and $A_\ell A_m$ instead of V and U) shows that $p_{n,A}(A_\ell A_m) = A_\ell A_m = A_\ell A_{n-\ell}$ (since $m = n - \ell$). Hence, $p_{n,A}(A_\ell A_m) = A_\ell A_{n-\ell} \subseteq Q$. Thus, (585) is proven in Case 1.

Let us now consider Case 2. In this case, we have $\ell + m \neq n$. Now, (584) yields $A_\ell A_m \subseteq A_{\ell+m}$. Hence, Lemma 40.2 **(b)** (applied to A, $A_\ell A_m$ and $\ell + m$ instead of V, U and m) shows that $p_{n,A}(A_\ell A_m) = 0$ (since $\ell + m \neq n$). Thus, $p_{n,A}(A_\ell A_m) = 0 \subseteq Q$ (since Q is a k-vector space). Thus, (585) is proven in Case 2.

We have now proven (585) in each of the two Cases 1 and 2. Since these two Cases cover all possibilities, we thus conclude that (585) always holds.

[331] *Proof of (586):* The definition of $A_{>0}$ yields $A_{>0} = \sum_{\substack{g \in \mathbb{N}; \\ g>0}} A_g = \sum_{\substack{m \in \mathbb{N}; \\ m>0}} A_m$ (here, we have renamed the summation index g as m). Now,

$$\begin{aligned}
\left(A_{>0}\right)^2 &= \underbrace{A_{>0}}_{= \sum_{\substack{g \in \mathbb{N}; \\ g>0}} A_g} \underbrace{A_{>0}}_{= \sum_{\substack{m \in \mathbb{N}; \\ m>0}} A_m} = \left(\sum_{\substack{g \in \mathbb{N}; \\ g>0}} A_g \right) \left(\sum_{\substack{m \in \mathbb{N}; \\ m>0}} A_m \right) \\
&= \sum_{\substack{g \in \mathbb{N}; \\ g>0}} \sum_{\substack{m \in \mathbb{N}; \\ m>0}} A_g A_m .
\end{aligned}$$

Applying the map $p_{n,A}$ to both sides of this relation, we obtain

$$\begin{aligned}
p_{n,A}\left(\left(A_{>0}\right)^2\right) &= p_{n,A}\left(\sum_{\substack{g \in \mathbb{N}; \\ g>0}} \sum_{\substack{m \in \mathbb{N}; \\ m>0}} A_g A_m \right) = \sum_{\substack{g \in \mathbb{N}; \\ g>0}} \underbrace{p_{n,A}\left(\sum_{\substack{m \in \mathbb{N}; \\ m>0}} A_g A_m \right)}_{= \sum_{\substack{m \in \mathbb{N}; \\ m>0}} p_{n,A}(A_g A_m)} \\
&\qquad \text{(since the map } p_{n,A} \text{ is } k\text{-linear)} \qquad \text{(since the map } p_{n,A} \text{ is } k\text{-linear)} \\
&= \sum_{\substack{g \in \mathbb{N}; \\ g>0}} \sum_{\substack{m \in \mathbb{N}; \\ m>0}} \underbrace{p_{n,A}\left(A_g A_m\right)}_{\subseteq Q} \subseteq \sum_{\substack{g \in \mathbb{N}; \\ g>0}} \underbrace{\sum_{\substack{m \in \mathbb{N}; \\ m>0}} Q}_{\subseteq Q} \\
&\qquad \text{(by (585) (applied to } \ell = g)) \qquad \text{(since } Q \text{ is a } k\text{-vector space)} \\
&\subseteq \sum_{\substack{g \in \mathbb{N}; \\ g>0}} Q \subseteq Q \qquad \text{(since } Q \text{ is a } k\text{-vector space)} .
\end{aligned}$$

But $A_n \subseteq p_{n,A}\left(A_{>0}\right)$ [332]. Hence,

$$A_n \subseteq p_{n,A}\left(\underbrace{A_{>0}}_{=V+(A_{>0})^2}\right) = p_{n,A}\left(V + (A_{>0})^2\right) = \underbrace{p_{n,A}\left(V\right)}_{=V\cap A_n} + \underbrace{p_{n,A}\left((A_{>0})^2\right)}_{\substack{\subseteq Q \\ \text{(by (586))}}}$$

(since the map $p_{n,A}$ is k-linear)

$$\subseteq (V \cap A_n) + \underbrace{Q}_{=\sum\limits_{g=1}^{n-1} A_g A_{n-g}} = (V \cap A_n) + \sum_{g=1}^{n-1} A_g A_{n-g}.$$

This proves Lemma 40.7 **(a)**.

(b) Let $R = \operatorname{AlgGen}_k V$. Then, R is a k-subalgebra of A (since $\operatorname{AlgGen}_k V$ is a k-subalgebra of A), and thus a k-vector subspace of A.

Lemma 16.20 (applied to $S = V$) yields $V \subseteq \operatorname{AlgGen}_k V = R$.

Now, we are going to prove that

$$A_n \subseteq R \qquad \text{for each } n \in \mathbb{N}. \tag{587}$$

[*Proof of (587):* We shall prove (587) by strong induction over n:

Induction step: Let $N \in \mathbb{N}$. Assume that (587) holds for every $n < N$. We must now show that (587) holds for $n = N$.

If $N = 0$, then this is obvious[333]. Hence, for the rest of this proof, we can WLOG assume that we don't have $N = 0$. Assume this.

We have $N \neq 0$ (since we don't have $N = 0$). Combining this with $N \in \mathbb{N}$, we obtain $N \in \mathbb{N} \setminus \{0\} = \{1, 2, 3, \ldots\}$. In other words, N is a positive integer. Hence, Lemma 40.7 **(a)** (applied to $n = N$) yields

$$A_N \subseteq (V \cap A_N) + \sum_{g=1}^{N-1} A_g A_{N-g}. \tag{588}$$

But we have assumed that (587) holds for every $n < N$. In other words, for each $n \in \mathbb{N}$ satisfying $n < N$, we have

$$A_n \subseteq R. \tag{589}$$

[332] *Proof.* The definition of $A_{>0}$ yields $A_{>0} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g>0}} A_g$. But n is a positive integer; thus, $n \in \mathbb{N}$ and $n > 0$. Hence, A_n is an addend of the sum $\sum\limits_{\substack{g \in \mathbb{N}; \\ g>0}} A_g$ (namely, the addend for $g = n$). Thus, $A_n \subseteq \sum\limits_{\substack{g \in \mathbb{N}; \\ g>0}} A_g = A_{>0}$. Hence, $p_{n,A}\left(\underbrace{A_n}_{\subseteq A_{>0}}\right) \subseteq p_{n,A}\left(A_{>0}\right)$.

But Lemma 40.2 **(a)** (applied to A and A_n instead of V and U) shows that $p_{n,A}\left(A_n\right) = A_n$ (since $A_n \subseteq A_n$). Thus, $A_n = p_{n,A}\left(A_n\right) \subseteq p_{n,A}\left(A_{>0}\right)$.

[333] *Proof.* Assume that $N = 0$. Thus, $A_N = A_0 = k \cdot 1_A$. But R is a k-subalgebra of A; thus, $1_A \in R$. Also, R is a k-vector subspace of A (since R is a k-subalgebra of A); thus, $k \cdot R \subseteq R$. Now, $A_N = k \cdot \underbrace{1_A}_{\in R} \subseteq k \cdot R \subseteq R$. In other words, (587) holds for $n = N$. Qed.

Now, each $g \in \{1, 2, \ldots, N-1\}$ satisfies

$$A_g A_{N-g} \subseteq R \tag{590}$$

[334]. Finally, (588) becomes

$$A_N \subseteq \underbrace{(V \cap A_N)}_{\subseteq V \subseteq R} + \sum_{g=1}^{N-1} \underbrace{A_g A_{N-g}}_{\substack{\subseteq R \\ \text{(by (590))}}} \subseteq R + \underbrace{\sum_{g=1}^{N-1} R}_{\substack{\subseteq R \\ \text{(since } R \text{ is a } k\text{-vector subspace of } A\text{)}}}$$

$$\subseteq R + R \subseteq R \qquad \text{(since } R \text{ is a } k\text{-vector subspace of } A\text{)}.$$

In other words, (587) holds for $n = N$. Thus, the induction step is complete. This completes the induction proof of (587).]

Now recall that A is a graded k-algebra. Hence, $A = \bigoplus_{n \in \mathbb{N}} A_n = \sum_{n \in \mathbb{N}} A_n$ (since direct sums are sums). Hence,

$$A = \sum_{n \in \mathbb{N}} \underbrace{A_n}_{\substack{\subseteq R \\ \text{(by (587))}}} \subseteq \sum_{n \in \mathbb{N}} R \subseteq R$$

(since R is a k-vector subspace of A). Combined with $R \subseteq A$, this yields $A = R$. Thus, $A = R = \operatorname{AlgGen}_k V$. This proves Lemma 40.7 **(b)**. □

Lemma 40.8. Let k be a field. Let V be a k-vector space. The k-algebra $\operatorname{Sym} V$ is generated by its subset $\operatorname{syminc}_V(V)$ [335].

Proof of Lemma 40.8. Let R be the k-subalgebra of $\operatorname{Sym} V$ generated by $\operatorname{syminc}_V(V)$. Then, clearly, R is a k-subalgebra of $\operatorname{Sym} V$ and contains $\operatorname{syminc}_V(V)$ as a subset. But Theorem 39.13 **(a)** yields

$$\operatorname{Sym} V = \sum_{n \in \mathbb{N}} \left(\underbrace{\operatorname{syminc}_V(V)}_{\substack{\subseteq R \\ \text{(since } R \text{ contains } \operatorname{syminc}_V(V) \\ \text{as a subset)}}} \right)^n \subseteq \sum_{n \in \mathbb{N}} \underbrace{R^n}_{\substack{\subseteq R \\ \text{(since } R \text{ is a } k\text{-algebra)}}} \subseteq \sum_{n \in \mathbb{N}} R \subseteq R$$

(since R is a k-vector subspace of $\operatorname{Sym} V$ (since R is a k-subalgebra of $\operatorname{Sym} V$)). Combining this with the obvious relation $R \subseteq \operatorname{Sym} V$, we obtain $\operatorname{Sym} V = R$.

[334] *Proof of (590):* Let $g \in \{1, 2, \ldots, N-1\}$. Thus, $g \leq N-1 < N$. Also, $g \in \{1, 2, \ldots, N-1\} \subseteq \mathbb{N}$. Hence, (589) (applied to $n = g$) yields $A_g \subseteq R$. But we also have $g > 0$ (since $g \in \{1, 2, \ldots, N-1\}$) and thus $N - \underbrace{g}_{>0} < N$. On the other hand, from $g < N$, we obtain $N - g > 0$, so that $N - g \in \mathbb{N}$. Thus, (589) (applied to $n = N - g$) yields $A_{N-g} \subseteq R$. Now,

$$\underbrace{A_g}_{\subseteq R} \underbrace{A_{N-g}}_{\subseteq R} \subseteq RR \subseteq R \qquad \text{(since } R \text{ is a } k\text{-subalgebra of } A\text{)}.$$

This proves (590).

[335] We are using the notations introduced in Definition 38.1.

Now, recall that R is the k-subalgebra of $\operatorname{Sym} V$ generated by $\operatorname{syminc}_V(V)$. In other words, $\operatorname{Sym} V$ is the k-subalgebra of $\operatorname{Sym} V$ generated by $\operatorname{syminc}_V(V)$ (since $\operatorname{Sym} V = R$). In other words, the k-algebra $\operatorname{Sym} V$ is generated by its subset $\operatorname{syminc}_V(V)$. This proves Lemma 40.8. $\square$

After these basic facts, let us again return to coalgebras and exponentials:

Lemma 40.9. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra. Let A be a graded k-algebra. For each $m \in \mathbb{N}$, we define a k-vector subspace $A_{>m}$ of A by $A_{>m} = \sum_{\substack{g \in \mathbb{N}; \\ g > m}} A_g$.

Let $\mathfrak{a} \in \mathfrak{g}(H, A)$ be such that $\mathfrak{a}(H) \subseteq A_1$. Notice that the k-linear map $e^{*\mathfrak{a}} : H \to A$ is well-defined (since $\mathfrak{a} \in \mathfrak{g}(H, A)$).

We have $e^{*\mathfrak{a}}(x) - \mathfrak{a}(x) \in A_{>1}$ for each $x \in \operatorname{Ker}(\varepsilon_H)$.

Proof of Lemma 40.9. Remark 2.10 (applied to $C = H$) yields that H is a unital coalgebra with unity $1_H = \left(\varepsilon_H \mid_{H_{\leq 0}}\right)^{-1}(1)$. In other words, $(H, 1_H)$ is a unital coalgebra, where $1_H = \left(\varepsilon_H \mid_{H_{\leq 0}}\right)^{-1}(1)$. In other words, H is a k-coalgebra and 1_H is an element of H satisfying $\Delta_H(1_H) = 1_H \otimes 1_H$ and $\varepsilon_H(1_H) = 1$ (by the definition of a "unital coalgebra").

Since A is a graded k-algebra, we have

$$A_\ell A_m \subseteq A_{\ell+m} \qquad \text{for any } \ell \in \mathbb{N} \text{ and } m \in \mathbb{N}. \tag{591}$$

Each $i \in \mathbb{N}$ satisfies

$$\mathfrak{a}^{*i}(H) \subseteq A_i \tag{592}$$

[336]. Thus, every integer $i > 1$ satisfies

$$\mathfrak{a}^{*i}(H) \subseteq A_{>1} \tag{593}$$

[336] *Proof of (592):* We shall prove (592) by induction over i:

Induction base: Recall the map $e_{H,A}$ defined in Definition 1.12. Its definition yields $e_{H,A} = \eta_A \circ \varepsilon_H$. Thus, each $h \in H$ satisfies

$$\underbrace{e_{H,A}}_{=\eta_A \circ \varepsilon_H}(h) = (\eta_A \circ \varepsilon_H)(h) = \eta_A(\varepsilon_H(h)) = \varepsilon_H(h) \cdot \underbrace{1_A}_{\substack{\in A_0 \\ \text{(since } A \\ \text{is a graded } k\text{-algebra)}}} \qquad \text{(by the definition of the map } \eta_A\text{)}$$

$$\in \varepsilon_H(h) \cdot A_0 \subseteq A_0 \qquad \text{(since } A_0 \text{ is a } k\text{-vector subspace of } A\text{)}.$$

In other words, $e_{H,A}(H) \subseteq A_0$. Now, $\underbrace{\mathfrak{a}^{*0}}_{=e_{H,A}}(H) = e_{H,A}(H) \subseteq A_0$. In other words, (592) holds for $i = 0$. This completes the induction base.

Induction step: Let $j \in \mathbb{N}$. Assume that (592) holds for $i = j$. We must prove that (592) holds for $i = j + 1$.

We have assumed that (592) holds for $i = j$. In other words, we have $\mathfrak{a}^{*j}(H) \subseteq A_j$. But

$$\mathfrak{a}^{*(j+1)} = \mathfrak{a} * \mathfrak{a}^{*j} = \mu_A \circ \left(\mathfrak{a} \otimes \mathfrak{a}^{\otimes j}\right) \circ \Delta_H \qquad \text{(by the definition of convolution)}.$$

[337].

Now, let $x \in \operatorname{Ker}(\varepsilon_H)$. Thus,

$$x \in \operatorname{Ker}(\varepsilon_H) \subseteq H = \bigcup_{n \in \mathbb{N}} H_{\leq n} \qquad \text{(since } H \text{ is filtered)}.$$

In other words, there exists some $n \in \mathbb{N}$ satisfying $x \in H_{\leq n}$. Consider this x. Each integer $i > n+1$ satisfies

$$\mathfrak{a}^{*i}(x) = 0 \tag{594}$$

[338]. Also,

$$\mathfrak{a}^{*0}(x) = 0 \tag{595}$$

[339]. Note that $\underbrace{n}_{\geq 0} + 1 \geq 1$.

Thus,

$$\begin{aligned}
&\underbrace{\mathfrak{a}^{*(j+1)}}_{=\mu_A \circ (\mathfrak{a} \otimes \mathfrak{a}^{\otimes j}) \circ \Delta_H}(H) \\
&= \left(\mu_A \circ \left(\mathfrak{a} \otimes \mathfrak{a}^{\otimes j}\right) \circ \Delta_H\right)(H) = \mu_A\left(\left(\mathfrak{a} \otimes \mathfrak{a}^{\otimes j}\right)\left(\underbrace{\Delta_H(H)}_{\subseteq H \otimes H}\right)\right) \\
&\subseteq \mu_A\left(\underbrace{\left(\mathfrak{a} \otimes \mathfrak{a}^{\otimes j}\right)(H \otimes H)}_{\subseteq \mathfrak{a}(H) \otimes \mathfrak{a}^{\otimes j}(H)}\right) \subseteq \mu_A\left(\mathfrak{a}(H) \otimes \mathfrak{a}^{\otimes j}(H)\right) \\
&= \underbrace{\mathfrak{a}(H)}_{\subseteq A_1} \cdot \underbrace{\mathfrak{a}^{\otimes j}(H)}_{\subseteq A_j} \qquad \left(\text{by Lemma 15.5 (applied to } U = \mathfrak{a}(H) \text{ and } V = \mathfrak{a}^{\otimes j}(H)\right)\text{)} \\
&\subseteq A_1 A_j \subseteq A_{1+j} \qquad \text{(by (591) (applied to } \ell = 1 \text{ and } m = j)) \\
&= A_{j+1} \qquad \text{(since } 1 + j = j + 1).
\end{aligned}$$

In other words, (592) holds for $i = j+1$. This completes the induction step. Thus, the induction proof of (592) is complete.

[337] *Proof of (593):* Let $i > 1$ be an integer. Thus, $i \in \mathbb{N}$. Hence, (592) yields $\mathfrak{a}^{*i}(H) \subseteq A_i$.

But the definition of $A_{>1}$ yields $A_{>1} = \sum_{\substack{g \in \mathbb{N}; \\ g > 1}} A_g$.

Now, $i \in \mathbb{N}$ satisfies $i > 1$. Hence, A_i is an addend of the sum $\sum_{\substack{g \in \mathbb{N}; \\ g > 1}} A_g$ (namely, the addend for $g = i$). Hence, $A_i \subseteq \sum_{\substack{g \in \mathbb{N}; \\ g > 1}} A_g = A_{>1}$. Now, $\mathfrak{a}^{*i}(H) \subseteq A_i \subseteq A_{>1}$. This proves (593).

[338] *Proof of (594):* Let i be an integer such that $i > n+1$. Then, $i > n+1 > n \geq 0$, so that $i \in \mathbb{N}$. Thus, Remark 3.5 (applied to $f = \mathfrak{a}$) yields $\mathfrak{a}^{*i}(H_{\leq n}) = 0$. Now, $x \in H_{\leq n}$, so that $\mathfrak{a}^{*i}\left(\underbrace{x}_{\in H_{\leq n}}\right) \in \mathfrak{a}^{*i}(H_{\leq n}) = 0$. In other words, $\mathfrak{a}^{*i}(x) = 0$. This proves (594).

[339] *Proof of (595):* Recall the map $e_{H,A}$ defined in Definition 1.12. Its definition yields $e_{H,A} = \eta_A \circ \varepsilon_H$. But

$$\underbrace{\mathfrak{a}^{*0}}_{=e_{H,A}=\eta_A \circ \varepsilon_H}(x) = (\eta_A \circ \varepsilon_H)(x) = \eta_A\left(\underbrace{\varepsilon_H(x)}_{\substack{=0 \\ (\text{since } x \in \operatorname{Ker}(\varepsilon_H))}}\right) = \eta_A(0) = 0$$

(since η_A is a k-linear map).

The definition of $e^{*\mathfrak{a}}$ yields

$$e^{*\mathfrak{a}}(x) = \sum_{i\geq 0} \underbrace{\frac{\mathfrak{a}^{*i}(x)}{i!}}_{=\frac{1}{i!}\mathfrak{a}^{*i}(x)} = \sum_{i\geq 0} \frac{1}{i!}\mathfrak{a}^{*i}(x) = \underbrace{\sum_{\substack{i\geq 0;\\ i\leq n+1}} \frac{1}{i!}\mathfrak{a}^{*i}(x)}_{=\sum_{i=0}^{n+1}} + \sum_{\substack{i\geq 0;\\ i>n+1}} \frac{1}{i!} \underbrace{\mathfrak{a}^{*i}(x)}_{\substack{=0\\ \text{(by (594))}}}$$

(since each $i \geq 0$ satisfies either $i \leq n+1$ or $i > n+1$ (but not both))

$$= \sum_{i=0}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}(x) + \underbrace{\sum_{\substack{i\geq 0;\\ i>n+1}} \frac{1}{i!}0}_{=0} = \sum_{i=0}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}(x) = \frac{1}{0!}\underbrace{\mathfrak{a}^{*0}(x)}_{\substack{=0\\ \text{(by (595))}}} + \sum_{i=1}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}(x)$$

(here, we have split off the addend for $i = 0$ from the sum)

$$= \underbrace{\frac{1}{0!}0}_{=0} + \sum_{i=1}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}(x) = \sum_{i=1}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}(x) = \underbrace{\frac{1}{1!}}_{=\frac{1}{1}=1} \underbrace{\mathfrak{a}^{*1}}_{=\mathfrak{a}}(x) + \sum_{i=2}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}(x)$$

$$\left(\begin{array}{c}\text{here, we have split off the addend for } i=0 \text{ from the sum}\\ \text{(this is allowed since } n+1 \geq 1)\end{array}\right)$$

$$= \mathfrak{a}(x) + \sum_{i=2}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}(x).$$

Subtracting $\mathfrak{a}(x)$ from both sides of this equality, we find

$$e^{*\mathfrak{a}}(x) - \mathfrak{a}(x) = \sum_{i=2}^{n+1} \frac{1}{i!}\mathfrak{a}^{*i}\left(\underbrace{x}_{\in H}\right) \in \sum_{i=2}^{n+1} \frac{1}{i!} \underbrace{\mathfrak{a}^{*i}(H)}_{\substack{\subseteq A_{>1}\\ \text{(by (593))}}} \subseteq \sum_{i=2}^{n+1} \frac{1}{i!} A_{>1} \subseteq A_{>1}$$

(since $A_{>1}$ is a k-vector subspace of A). This proves Lemma 40.9. □

Lemma 40.10. Let k be a field of characteristic 0. Let H be a connected filtered k-coalgebra and, at the same time, a k-bialgebra with the same underlying k-coalgebra structure. Let A be a commutative graded k-algebra satisfying $A = \operatorname{AlgGen}_k(A_1)$.

Let $\mathfrak{b} : A \to H$ be a k-algebra homomorphism satisfying $\mathfrak{b}(A_1) \subseteq \operatorname{Ker}(\varepsilon_H)$. Let $\mathfrak{a} \in \mathfrak{g}(H, A)$ be an $(\varepsilon_H, \varepsilon_H)$-derivation satisfying $\mathfrak{a}(H) \subseteq A_1$. Notice that the k-linear map $e^{*\mathfrak{a}} : H \to A$ is well-defined (since $\mathfrak{a} \in \mathfrak{g}(H, A)$).

Assume further that

$$(\mathfrak{a} \circ \mathfrak{b})(x) = x \qquad \text{for each } x \in A_1. \tag{596}$$

Then, both maps $e^{*\mathfrak{a}} \circ \mathfrak{b} : A \to A$ and $\mathfrak{b} : A \to H$ are injective.

Proof of Lemma 40.10. Lemma 15.11 (applied to $f = \mathfrak{a}$) yields that $e^{*\mathfrak{a}}$ is a k-algebra homomorphism.

The two maps $e^{*\mathfrak{a}}$ and $\mathfrak{b}$ are k-algebra homomorphisms. Hence, their composition $e^{*\mathfrak{a}} \circ \mathfrak{b} : A \to A$ is a k-algebra homomorphism as well (since the composition of two k-algebra homomorphisms always is a k-algebra homomorphism).

For each $m \in \mathbb{N}$, we define a k-vector subspace $A_{>m}$ of A by $A_{>m} = \sum_{\substack{g \in \mathbb{N}; \\ g > m}} A_g$.

Each $x \in A_1$ satisfies $\left(e^{*\mathfrak{a}} \circ \mathfrak{b}\right)(x) - x \in A_{>1}$ [340]. Thus, Lemma 40.5 **(b)** (applied to $f = e^{*\mathfrak{a}} \circ \mathfrak{b}$) shows that the map $e^{*\mathfrak{a}} \circ \mathfrak{b}$ is injective.

Next, let us recall the following basic fact about maps: If X, Y and Z are three sets, and if $\alpha : X \to Y$ and $\beta : Y \to Z$ are two maps such that $\beta \circ \alpha$ is injective, then the map α is injective.[341] Applying this to $X = A$, $Y = H$, $Z = A$, $\alpha = \mathfrak{b}$ and $\beta = e^{*\mathfrak{a}}$, we conclude that the map $\mathfrak{b}$ is injective (since the map $e^{*\mathfrak{a}} \circ \mathfrak{b}$ is injective).

We thus have shown that both maps $e^{*\mathfrak{a}} \circ \mathfrak{b} : A \to A$ and $\mathfrak{b} : A \to H$ are injective. This proves Lemma 40.10. □

Lemma 40.11. Let k be a field. Let C be a graded k-coalgebra. For each $m \in \mathbb{N}$, we define a k-vector subspace $C_{>m}$ of C by $C_{>m} = \sum_{\substack{g \in \mathbb{N}; \\ g > m}} C_g$. Then:

(a) We have $C_{>0} \subseteq \operatorname{Ker}(\varepsilon_C)$.

(b) Assume that the graded k-coalgebra C is connected. Then, $C_{>0} = \operatorname{Ker}(\varepsilon_C)$.

Proof of Lemma 40.11. The map ε_C is k-linear. Hence, its kernel $\operatorname{Ker}(\varepsilon_C)$ is a k-vector subspace of C.

Each positive integer g satisfies

$$C_g \subseteq \operatorname{Ker}(\varepsilon_C) \tag{597}$$

[342].

---

[340] *Proof.* Let $x \in A_1$. Then, (596) yields $(\mathfrak{a} \circ \mathfrak{b})(x) = x$. Hence, $x = (\mathfrak{a} \circ \mathfrak{b})(x) = \mathfrak{a}(\mathfrak{b}(x))$.

But $\mathfrak{b}\left(\underbrace{x}_{\in A_1}\right) \in \mathfrak{b}(A_1) \subseteq \operatorname{Ker}(\varepsilon_H)$. Thus, Lemma 40.9 (applied to $\mathfrak{b}(x)$ instead of x) yields $e^{*\mathfrak{a}}(\mathfrak{b}(x)) - \mathfrak{a}(\mathfrak{b}(x)) \in A_{>1}$. Thus,

$$\underbrace{\left(e^{*\mathfrak{a}} \circ \mathfrak{b}\right)(x)}_{=e^{*\mathfrak{a}}(\mathfrak{b}(x))} - \underbrace{x}_{=\mathfrak{a}(\mathfrak{b}(x))} = e^{*\mathfrak{a}}(\mathfrak{b}(x)) - \mathfrak{a}(\mathfrak{b}(x)) \in A_{>1}.$$

Qed.

[341] *Proof.* Let X, Y and Z be three sets. Let $\alpha : X \to Y$ and $\beta : Y \to Z$ be two maps such that $\beta \circ \alpha$ is injective. We must show that the map α is injective.

Let u and v be two elements of X such that $\alpha(u) = \alpha(v)$. Then, $(\beta \circ \alpha)(u) = \beta\left(\underbrace{\alpha(u)}_{=\alpha(v)}\right) = \beta(\alpha(v)) = (\beta \circ \alpha)(v)$. Since the map $\beta \circ \alpha$ is injective, we obtain $u = v$ from this.

Now, forget that we fixed u and v. We thus have shown that if u and v are two elements of X such that $\alpha(u) = \alpha(v)$, then $u = v$. In other words, the map α is injective. Qed.

[342] *Proof of (597):* Let g be a positive integer. Hence, $g \in \mathbb{N}$.

Let us give k the usual grading (the one where $k_0 = k$ and $k_n = 0$ for all positive $n \in \mathbb{N}$).

Recall that C is a graded k-coalgebra. Thus, its counity map $\varepsilon_C : C \to k$ is graded. In other words, $\varepsilon_C(C_n) \subseteq k_n$ for every $n \in \mathbb{N}$. Applying this to $n = g$, we obtain $\varepsilon_C(C_g) \subseteq k_g$.

Now, the definition of $C_{>0}$ yields

$$C_{>0} = \sum_{\substack{g \in \mathbb{N}; \\ g>0}} \underbrace{C_g}_{\substack{\subseteq \operatorname{Ker}(\varepsilon_C) \\ \text{(by (597))}}} \subseteq \sum_{\substack{g \in \mathbb{N}; \\ g>0}} \operatorname{Ker}(\varepsilon_C) \subseteq \operatorname{Ker}(\varepsilon_C) \tag{598}$$

(since $\operatorname{Ker}(\varepsilon_C)$ is a k-vector subspace of C). This proves Lemma 40.11 **(a)**.

(b) We know that C is a graded k-coalgebra. Thus, Proposition 16.6 shows that $\left(C, (C_{\leq n})_{n \geq 0}\right)$ is a filtered k-coalgebra. As usual, we shall refer to this filtered k-coalgebra $\left(C, (C_{\leq n})_{n \geq 0}\right)$ simply as "the filtered k-coalgebra C".

Remark 16.11 shows that the graded k-coalgebra C is connected if and only if the filtered k-coalgebra C is connected. Thus, the filtered k-coalgebra C is connected (since the graded k-coalgebra C is connected).

Remark 2.10 yields that C is a unital coalgebra with unity $1_C = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$. In other words, $(C, 1_C)$ is a unital coalgebra, where $1_C = \left(\varepsilon_C \mid_{C_{\leq 0}}\right)^{-1}(1)$. In other words, C is a k-coalgebra and 1_C is an element of C satisfying $\Delta_C(1_C) = 1_C \otimes 1_C$ and $\varepsilon_C(1_C) = 1$ (by the definition of a "unital coalgebra").

Remark 2.12 yields that C is connected if and only if $C_{\leq 0} = k \cdot 1_C$. Thus, $C_{\leq 0} = k \cdot 1_C$ (since C is connected). By the definition of $C_{\leq 0}$, we have $C_{\leq 0} = \bigoplus_{\ell=0}^{0} C_\ell = C_0$. Thus, $C_0 = C_{\leq 0} = k \cdot 1_C$.

Now, C is graded; thus,

$$C = \bigoplus_{g \in \mathbb{N}} C_g = C_0 \oplus \underbrace{\left(\bigoplus_{\substack{g \in \mathbb{N}; \\ g>0}} C_g\right)}_{\substack{= \sum\limits_{\substack{g \in \mathbb{N}; \\ g>0}} C_g \\ \text{(since direct sums are sums)}}} \qquad \left(\begin{array}{c}\text{here, we have split off the addend} \\ \text{for } g = 0 \text{ from the direct sum}\end{array}\right)$$

$$= C_0 \oplus \underbrace{\left(\sum_{\substack{g \in \mathbb{N}; \\ g>0}} C_g\right)}_{\substack{= C_{>0} \\ \text{(by (598))}}} = C_0 \oplus C_{>0}.$$

Now, let $x \in \operatorname{Ker}(\varepsilon_C)$. Then, $x \in \operatorname{Ker}(\varepsilon_C) \subseteq C = C_0 \oplus C_{>0} = C_0 + C_{>0}$ (since direct sums are sums). In other words, there exist $y \in C_0$ and $z \in C_{>0}$ such that $x = y + z$. Consider these y and z.

We have $y \in C_0 = k \cdot 1_C$. Thus, there exists some $\lambda \in k$ such that $y = \lambda \cdot 1_C$. Consider this λ.

But recall that $k_n = 0$ for all positive $n \in \mathbb{N}$ (by the definition of the grading on k). Applying this to $n = g$, we conclude that $k_g = 0$. Thus, $\varepsilon_C(C_g) \subseteq k_g = 0$, so that $\varepsilon_C(C_g) = 0$ and thus $C_g \subseteq \operatorname{Ker}(\varepsilon_C)$. This proves (597).

We have $z \in C_{>0} \subseteq \operatorname{Ker}(\varepsilon_C)$ (by Lemma 40.11 **(a)**) and thus $\varepsilon_C(z) = 0$. Also, $\varepsilon_C(x) = 0$ (since $x \in \operatorname{Ker}(\varepsilon_C)$). Thus,

$$0 = \varepsilon_C\left(\underbrace{x}_{=y+z}\right) = \varepsilon_C(y+z) = \varepsilon_C(y) + \underbrace{\varepsilon_C(z)}_{=0} \qquad \text{(since the map } \varepsilon_C \text{ is } k\text{-linear)}$$

$$= \varepsilon_C\left(\underbrace{y}_{=\lambda\cdot 1_C}\right) = \varepsilon_C(\lambda \cdot 1_C) = \lambda \cdot \underbrace{\varepsilon_C(1_C)}_{=1} \qquad \text{(since the map } \varepsilon_C \text{ is } k\text{-linear)}$$

$$= \lambda.$$

Thus, $\lambda = 0$, so that $y = \underbrace{\lambda}_{=0} \cdot 1_C = 0$. Hence, $x = \underbrace{y}_{=0} + z = z \in C_{>0}$.

Now, forget that we fixed x. We thus have proven that $x \in C_{>0}$ for each $x \in \operatorname{Ker}(\varepsilon_C)$. In other words, $\operatorname{Ker}(\varepsilon_C) \subseteq C_{>0}$. But Lemma 40.11 **(a)** yields $C_{>0} \subseteq \operatorname{Ker}(\varepsilon_C)$. Combining this with $\operatorname{Ker}(\varepsilon_C) \subseteq C_{>0}$, we obtain $C_{>0} = \operatorname{Ker}(\varepsilon_C)$. This proves Lemma 40.11 **(b)**. □

Lemma 40.12. Let k be a field. Let C be a unital coalgebra. Let V and W be two k-vector subspaces of C such that $\operatorname{Ker}(\varepsilon_C) = V \oplus W$. Then, there exists a k-linear map $\alpha : C \to V$ that satisfies $\alpha(W + k \cdot 1_C) = 0$ and $\alpha|_V = \mathrm{id}_V$.

Proof of Lemma 40.12. Recall that $\operatorname{Ker}(\varepsilon_C) = V \oplus W$. In particular, $V \oplus W$ is a well-defined internal direct sum. Let $\mathfrak{p} : V \oplus W \to V$ be the canonical projection from this direct sum to its first addend V. Thus, $\mathfrak{p}|_V = \mathrm{id}_V$ and $\mathfrak{p}|_W = 0$.

The map $\mathfrak{p}$ is a k-linear map $V \oplus W \to V$ (since it is a canonical projection from a direct sum to one of its addends). In other words, the map $\mathfrak{p}$ is a k-linear map $\operatorname{Ker}(\varepsilon_C) \to V$ (since $C_{>0} = V \oplus W$).

We know that $(C, 1_C)$ is a unital coalgebra. In other words, C is a k-coalgebra and 1_C is an element of C satisfying $\Delta_C(1_C) = 1_C \otimes 1_C$ and $\varepsilon_C(1_C) = 1$ (by the definition of a "unital coalgebra").

Consider the k-linear map $e_{C,C} : C \to C$. (Here, we are using the notation introduced in Definition 2.14.)

Define a k-linear map $\xi : C \to C$ by $\xi = \mathrm{id}_C - e_{C,C}$. [343] Then, each $c \in C$ satisfies $\xi(c) \in \operatorname{Ker}(\varepsilon_C)$ [344]. Hence, we can define a map $\xi' : C \to \operatorname{Ker}(\varepsilon_C)$ by

$$(\xi'(c) = \xi(c) \qquad \text{for every } c \in C).$$

Consider this map ξ'. This map ξ' is obtained from ξ by restricting the codomain to $\operatorname{Ker}(\varepsilon_C)$ (since $\xi'(c) = \xi(c)$ for every $c \in C$). Hence, this map ξ' is k-linear (since the map ξ is k-linear).

Thus, ξ' is a k-linear map $C \to \operatorname{Ker}(\varepsilon_C)$, whereas $\mathfrak{p}$ is a k-linear map $\operatorname{Ker}(\varepsilon_C) \to V$. Hence, the composition $\mathfrak{p} \circ \xi'$ of these two maps is a k-linear map $C \to V$.

[343] This is indeed a k-linear map, since both maps id_C and $e_{C,C}$ are k-linear.

[344] *Proof.* Let $c \in C$. Then, the definition of $e_{C,C}$ yields $e_{C,C} = \eta_C \circ \varepsilon_C$, so that

$$\underbrace{e_{C,C}}_{=\eta_C\circ\varepsilon_C}(c) = (\eta_C \circ \varepsilon_C)(c) = \eta_C(\varepsilon_C(c)) = \varepsilon_C(c) \cdot 1_C \qquad \text{(by the definition of } \eta_C).$$

Furthermore,

$$\xi'(x) = x \qquad \text{for each } x \in \operatorname{Ker}(\varepsilon_C) \tag{599}$$

[345]. Hence, $(\mathfrak{p} \circ \xi')(W) = 0$ [346] and $(\mathfrak{p} \circ \xi')(k \cdot 1_C) = 0$ [347]. Hence, $(\mathfrak{p} \circ \xi')(W + k \cdot 1_C) =$

Now,

$$\begin{aligned}
\varepsilon_C\left(\underbrace{\xi}_{=\mathrm{id}_C - e_{C,C}}(c)\right) &= \varepsilon_C\left(\underbrace{(\mathrm{id}_C - e_{C,C})(c)}_{=\mathrm{id}_C(c) - e_{C,C}(c)}\right) = \varepsilon_C\left(\underbrace{\mathrm{id}_C(c)}_{=c} - \underbrace{e_{C,C}(c)}_{=\varepsilon_C(c)\cdot 1_C}\right) \\
&= \varepsilon_C(c) - \underbrace{\varepsilon_C(\varepsilon_C(c)\cdot 1_C)}_{\substack{=\varepsilon_C(c)\cdot\varepsilon_C(1_C) \\ \text{(since the map } \varepsilon_C \text{ is } k\text{-linear)}}} = \varepsilon_C(c) - \varepsilon_C(c)\cdot\underbrace{\varepsilon_C(1_C)}_{=1} \\
&= \varepsilon_C(c) - \varepsilon_C(c) = 0.
\end{aligned}$$

In other words, $\xi(c) \in \operatorname{Ker}(\varepsilon_C)$. Qed.

[345] *Proof of (599):* Let $x \in \operatorname{Ker}(\varepsilon_C)$. Thus, $x \in C$ and $\varepsilon_C(x) = 0$.

But the definition of $e_{C,C}$ yields $e_{C,C} = \eta_C \circ \varepsilon_C$, so that

$$\underbrace{e_{C,C}}_{=\eta_C\circ\varepsilon_C}(x) = (\eta_C \circ \varepsilon_C)(x) = \eta_C\left(\underbrace{\varepsilon_C(x)}_{=0}\right) = \eta_C(0) = 0$$

(since the map η_C is k-linear). Now, the definition of ξ' yields

$$\xi'(x) = \underbrace{\xi}_{=\mathrm{id}_C - e_{C,C}}(x) = (\mathrm{id}_C - e_{C,C})(x) = \underbrace{\mathrm{id}_C(x)}_{=x} - \underbrace{e_{C,C}(x)}_{=0} = x.$$

Qed.

[346] *Proof.* Let $x \in W$. Then, $x \in W \subseteq V \oplus W = \operatorname{Ker}(\varepsilon_C)$. Thus, (599) shows that $\xi'(x) = x$. But $x \in W$; therefore, $(\mathfrak{p}\mid_W)(x)$ is well-defined. We have $\underbrace{(\mathfrak{p}\mid_W)}_{=0}(x) = 0(x) = 0$. Comparing this with $(\mathfrak{p}\mid_W)(x) = \mathfrak{p}(x)$, we obtain $\mathfrak{p}(x) = 0$.

Now, $(\mathfrak{p} \circ \xi')(x) = \mathfrak{p}\left(\underbrace{\xi'(x)}_{=x}\right) = \mathfrak{p}(x) = 0$. Hence, $x \in \operatorname{Ker}(\mathfrak{p} \circ \xi')$.

Let us now forget that we fixed x. We thus have proven that $x \in \operatorname{Ker}(\mathfrak{p} \circ \xi')$ for each $x \in W$. In other words, $W \subseteq \operatorname{Ker}(\mathfrak{p} \circ \xi')$. In other words, $(\mathfrak{p} \circ \xi')(W) = 0$.

[347] *Proof.* The definition of $e_{C,C}$ yields $e_{C,C} = \eta_C \circ \varepsilon_C$, so that

$$\begin{aligned}
\underbrace{e_{C,C}}_{=\eta_C\circ\varepsilon_C}(1_C) &= (\eta_C \circ \varepsilon_C)(1_C) = \eta_C\left(\underbrace{\varepsilon_C(1_C)}_{=1}\right) = \eta_C(1) \\
&= 1 \cdot 1_C \qquad \text{(by the definition of the map } \eta_C\text{)} \\
&= 1_C.
\end{aligned}$$

Now, the definition of ξ' yields

$$\xi'(1_C) = \underbrace{\xi}_{=\mathrm{id}_C - e_{C,C}}(1_C) = (\mathrm{id}_C - e_{C,C})(1_C) = \underbrace{\mathrm{id}_C(1_C)}_{=1_C} - \underbrace{e_{C,C}(1_C)}_{=1_C} = 1_C - 1_C = 0.$$

Since the map ξ' is k-linear, we have $\xi'(k \cdot 1_C) = k \cdot \underbrace{\xi'(1_C)}_{=0} = k \cdot 0 = 0$. Now, $(\mathfrak{p} \circ \xi')(k \cdot 1_C) =$

0 [348]. Furthermore, $(\mathfrak{p} \circ \xi')\,|_V = \mathrm{id}_V$ [349]. Hence, there exists a k-linear map $\alpha : C \to V$ that satisfies $\alpha(W + k \cdot 1_C) = 0$ and $\alpha\,|_V = \mathrm{id}_V$ (namely, $\alpha = \mathfrak{p} \circ \xi'$). This proves Lemma 40.12. $\square$

We are now ready to prove another form of Leray's theorem:

Theorem 40.13. Let k be a field of characteristic 0. Let H be a connected graded commutative bialgebra over k. For each $m \in \mathbb{N}$, we define a k-vector subspace $H_{>m}$ of H by $H_{>m} = \sum_{\substack{g \in \mathbb{N}; \\ g > m}} H_g$. Let V be a homogeneous subspace of H such that $H_{>0} = V \oplus (H_{>0})^2$.

Let $\mathfrak{i}$ denote the inclusion map $V \to H$. Let $\mathfrak{b}$ denote the k-algebra homomorphism $\operatorname{symlift} \mathfrak{i} : \operatorname{Sym} V \to H$ [350].

(a) This map $\mathfrak{b}$ is a k-algebra isomorphism.

(b) Let $\alpha : H \to V$ be a k-linear map that satisfies $\alpha\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$ and $\alpha\,|_V = \mathrm{id}_V$. Define a k-linear map $\mathfrak{a} : H \to \operatorname{Sym} V$ by $\mathfrak{a} = \operatorname{symin}\mathrm{c}_V \circ \alpha$. Then, $\mathfrak{a} \in \mathfrak{g}(H, \operatorname{Sym} V)$, and thus the k-linear map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is well-defined. This map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is a k-algebra isomorphism.[351]

Proof of Theorem 40.13. Recall that H is a k-bialgebra. Thus, $\varepsilon_H : H \to k$ is a k-algebra homomorphism (by the axioms of a k-bialgebra).

We know that H is a graded k-bialgebra. Thus, Proposition 16.8 shows that $\left(H, (H_{\leq n})_{n \geq 0}\right)$ is a filtered k-bialgebra. As usual, we shall refer to this filtered k-bialgebra $\left(H, (H_{\leq n})_{n \geq 0}\right)$ simply as "the filtered k-bialgebra H".

Remark 16.11 (applied to $C = H$) shows that the graded k-coalgebra H is connected if and only if the filtered k-coalgebra H is connected. Thus, the filtered k-coalgebra H is connected (since the graded k-coalgebra H is connected).

$\mathfrak{p}\left(\underbrace{\xi'(k \cdot 1_C)}_{=0}\right) = \mathfrak{p}(0) = 0$ (since the map $\mathfrak{p}$ is k-linear).

[348] *Proof.* The map $\mathfrak{p} \circ \xi'$ is k-linear. Thus,

$$(\mathfrak{p} \circ \xi')(W + k \cdot 1_C) = \underbrace{(\mathfrak{p} \circ \xi')(W)}_{=0} + \underbrace{(\mathfrak{p} \circ \xi')(k \cdot 1_C)}_{=0} = 0 + 0 = 0.$$

[349] *Proof.* Let $x \in V$. Then, $x \in V \subseteq V \oplus W = \operatorname{Ker}(\varepsilon_C)$. Thus, (599) shows that $\xi'(x) = x$. But $x \in V$; thus, the element $(\mathfrak{p}\,|_V)(x)$ is well-defined. Hence, $\underbrace{(\mathfrak{p}\,|_V)}_{=\mathrm{id}_V}(x) = \mathrm{id}_V(x) = x$, so that $x = (\mathfrak{p}\,|_V)(x) = \mathfrak{p}(x)$. Hence, $\mathfrak{p}(x) = x$.

Now,

$$((\mathfrak{p} \circ \xi')\,|_V)(x) = (\mathfrak{p} \circ \xi')(x) = \mathfrak{p}\left(\underbrace{\xi'(x)}_{=x}\right) = \mathfrak{p}(x) = x = \mathrm{id}_V(x).$$

Now, forget that we fixed x. We thus have shown that $((\mathfrak{p} \circ \xi')\,|_V)(x) = \mathrm{id}_V(x)$ for each $x \in V$. In other words, $(\mathfrak{p} \circ \xi')\,|_V = \mathrm{id}_V$.

[350] We are using the notations introduced in Definition 38.1.

[351] The maps $\mathfrak{b}$ and $e^{*\mathfrak{a}}$ are not mutually inverse in general.

Remark 2.10 (applied to $C = H$) yields that H is a unital coalgebra with unity $1_H = \left(\varepsilon_H \mid_{H_{\leq 0}}\right)^{-1}(1)$. In other words, $(H, 1_H)$ is a unital coalgebra, where $1_H = \left(\varepsilon_H \mid_{H_{\leq 0}}\right)^{-1}(1)$.

(b) We have $\mathfrak{a}\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$ [352]. But Theorem 15.9 (applied to $A = \operatorname{Sym} V$) shows that $\mathfrak{a}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation if and only if $\mathfrak{a}\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$. Hence, $\mathfrak{a}$ is an $(\varepsilon_H, \varepsilon_H)$-derivation (since $\mathfrak{a}\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = 0$). Hence, Proposition 38.14 (applied to $A = \operatorname{Sym} V$ and $h = \mathfrak{a}$) shows that $\mathfrak{a} \in \mathfrak{g}(H, \operatorname{Sym} V)$. Thus, the k-linear map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is well-defined.

We have $\mathfrak{a} \mid_V = \operatorname{syminc}_V$ [353]. Also, $\mathfrak{a}(H) = \operatorname{syminc}_V(V)$ [354].

Lemma 40.8 yields that the k-algebra $\operatorname{Sym} V$ is generated by its subset $\operatorname{syminc}_V(V)$. In other words, the k-algebra $\operatorname{Sym} V$ is generated by its subset $\mathfrak{a}(H)$ (since $\mathfrak{a}(H) = \operatorname{syminc}_V(V)$). In other words, the subset $\mathfrak{a}(H)$ of $\operatorname{Sym} V$ generates the k-algebra $\operatorname{Sym} V$. Hence, Corollary 38.13 (applied to $A = \operatorname{Sym} V$ and $f = \mathfrak{a}$) shows that the map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is a surjective k-algebra homomorphism.

It is well-known that $\operatorname{Sym} V$ is a graded k-algebra, with grading given by

$$(\operatorname{Sym} V)_n = \operatorname{Sym}^n V \qquad \text{for each } n \in \mathbb{N}.$$

[355] In particular, $(\operatorname{Sym} V)_1 = \operatorname{Sym}^1 V = \operatorname{syminc}_V(V)$.

We have $\mathfrak{b} \circ \operatorname{syminc}_V = \mathfrak{i}$ [356].

---

[352] *Proof.* We have

$$\underbrace{\mathfrak{a}}_{=\operatorname{syminc}_V \circ \alpha}\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right) = (\operatorname{syminc}_V \circ \alpha)\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right)$$

$$= \operatorname{syminc}_V\left(\underbrace{\alpha\left(\left(\operatorname{Ker}(\varepsilon_H)\right)^2 + k \cdot 1_H\right)}_{=0}\right) = \operatorname{syminc}_V(0) = 0$$

(since the map syminc_V is k-linear).

[353] *Proof.* Let $v \in V$. Then, $(\mathfrak{a} \mid_V)(v) = \underbrace{\mathfrak{a}}_{=\operatorname{syminc}_V \circ \alpha}(v) = (\operatorname{syminc}_V \circ \alpha)(v) = \operatorname{syminc}_V(\alpha(v))$. But from $v \in V$, we obtain $(\alpha \mid_V)(v) = \alpha(v)$, so that $\alpha(v) = \underbrace{(\alpha \mid_V)}_{=\mathrm{id}_V}(v) = \mathrm{id}_V(v) = v$. Thus, $(\mathfrak{a} \mid_V)(v) = \operatorname{syminc}_V\left(\underbrace{\alpha(v)}_{=v}\right) = \operatorname{syminc}_V(v)$.

Now, forget that we fixed v. We thus have proven that $(\mathfrak{a} \mid_V)(v) = \operatorname{syminc}_V(v)$ for each $v \in V$. In other words, $\mathfrak{a} \mid_V = \operatorname{syminc}_V$.

[354] *Proof.* Recall that $\alpha \mid_V = \mathrm{id}_V$; that is, $\mathrm{id}_V = \alpha \mid_V$.

Now, each $v \in V$ satisfies $v = \underbrace{\mathrm{id}_V}_{=\alpha \mid_V}(v) = (\alpha \mid_V)(v) = \alpha\left(\underbrace{v}_{\in V \subseteq H}\right) \in \alpha(H)$. Thus, $V \subseteq \alpha(H)$. Combining this with $\alpha(H) \subseteq V$ (which is obvious, since α is a map $H \to V$), we obtain $V = \alpha(H)$. Thus, $\alpha(H) = V$.

But $\underbrace{\mathfrak{a}}_{=\operatorname{syminc}_V \circ \alpha}(H) = (\operatorname{syminc}_V \circ \alpha)(H) = \operatorname{syminc}_V\left(\underbrace{\alpha(H)}_{=V}\right) = \operatorname{syminc}_V(V)$.

[355] Notice that this grading has **nothing** to do with the grading on H.

[356] *Proof.* Recall that symlift $\mathfrak{i}$ is the unique k-algebra homomorphism $\Phi : \operatorname{Sym} V \to H$ satisfying $\Phi \circ$

Recall that the k-algebra $\operatorname{Sym} V$ is generated by its subset $\operatorname{syminc}_V(V)$. In other words, the k-subalgebra of $\operatorname{Sym} V$ generated by $\operatorname{syminc}_V(V)$ is $\operatorname{Sym} V$. In other words, $\operatorname{AlgGen}_k(\operatorname{syminc}_V(V))$ is $\operatorname{Sym} V$ [357]. In other words, $\operatorname{AlgGen}_k(\operatorname{syminc}_V(V)) = \operatorname{Sym} V$. Thus,

$$\operatorname{Sym} V = \operatorname{AlgGen}_k\left(\underbrace{\operatorname{syminc}_V(V)}_{=(\operatorname{Sym} V)_1}\right) = \operatorname{AlgGen}_k\left((\operatorname{Sym} V)_1\right).$$

Moreover, it is well-known that the k-algebra $\operatorname{Sym} V$ is commutative.

The k-algebra homomorphism $\mathfrak{b} : \operatorname{Sym} V \to H$ satisfies $\mathfrak{b}\left((\operatorname{Sym} V)_1\right) \subseteq \operatorname{Ker}(\varepsilon_H)$ [358]. The $(\varepsilon_H, \varepsilon_H)$-derivation $\mathfrak{a} \in \mathfrak{g}(H, \operatorname{Sym} V)$ satisfies $\mathfrak{a}(H) \subseteq (\operatorname{Sym} V)_1$ [359]. Furthermore, we have

$$(\mathfrak{a} \circ \mathfrak{b})(x) = x \qquad \text{for each } x \in (\operatorname{Sym} V)_1$$

[360]. Hence, Lemma 40.10 (applied to $A = \operatorname{Sym} V$) shows that both maps $e^{*\mathfrak{a}} \circ \mathfrak{b} : \operatorname{Sym} V \to \operatorname{Sym} V$ and $\mathfrak{b} : A \to \operatorname{Sym} V$ are injective.

$\operatorname{syminc}_V = \mathfrak{i}$ (because this is how $\operatorname{symlift} \mathfrak{i}$ was defined). Thus, $\operatorname{symlift} \mathfrak{i}$ is a k-algebra homomorphism $\operatorname{Sym} V \to H$ and satisfies $(\operatorname{symlift} \mathfrak{i}) \circ \operatorname{syminc}_V = \mathfrak{i}$.

Now, $\underbrace{\mathfrak{b}}_{=\operatorname{symlift} \mathfrak{i}} \circ \operatorname{syminc}_V = (\operatorname{symlift} \mathfrak{i}) \circ \operatorname{syminc}_V = \mathfrak{i}$.

[357] since $\operatorname{AlgGen}_k(\operatorname{syminc}_V(V))$ is the k-subalgebra of $\operatorname{Sym} V$ generated by $\operatorname{syminc}_V(V)$ (by the definition of $\operatorname{AlgGen}_k(\operatorname{syminc}_V(V))$)

[358] *Proof.* We have

$$\mathfrak{b}\left(\underbrace{(\operatorname{Sym} V)_1}_{=\operatorname{syminc}_V(V)}\right) = \mathfrak{b}(\operatorname{syminc}_V(V)) = \underbrace{(\mathfrak{b} \circ \operatorname{syminc}_V)}_{=\mathfrak{i}}(V) = \mathfrak{i}(V) = V$$

(since $\mathfrak{i}$ is an inclusion map).

Lemma 40.11 **(a)** (applied to $C = H$) shows that $H_{>0} \subseteq \operatorname{Ker}(\varepsilon_H)$.

But recall that $H_{>0} = V \oplus (H_{>0})^2 \supseteq V$, so that $V \subseteq H_{>0} \subseteq \operatorname{Ker}(\varepsilon_H)$. Thus, $\mathfrak{b}\left((\operatorname{Sym} V)_1\right) = V \subseteq \operatorname{Ker}(\varepsilon_H)$.

[359] *Proof.* We have $\underbrace{\mathfrak{a}}_{=\operatorname{syminc}_V \circ \alpha}(H) = (\operatorname{syminc}_V \circ \alpha)(H) = \operatorname{syminc}_V\left(\underbrace{\alpha(H)}_{\subseteq V}\right) \subseteq \operatorname{syminc}_V(V) = (\operatorname{Sym} V)_1$.

[360] *Proof.* Let $x \in (\operatorname{Sym} V)_1$. Then, $x \in (\operatorname{Sym} V)_1 = \operatorname{syminc}_V(V)$. In other words, there exists some $w \in V$ such that $x = \operatorname{syminc}_V(w)$. Consider this w.

From $w \in V$, we obtain $\alpha(w) = \underbrace{(\alpha\mid_V)}_{=\mathrm{id}_V}(w) = \mathrm{id}_V(w) = w$.

Applying the map $\mathfrak{b}$ to both sides of the equality $x = \operatorname{syminc}_V(w)$, we find

$$\mathfrak{b}(x) = \mathfrak{b}(\operatorname{syminc}_V(w)) = \underbrace{(\mathfrak{b} \circ \operatorname{syminc}_V)}_{=\mathfrak{i}}(w) = \mathfrak{i}(w) = w$$

(since $\mathfrak{i}$ is merely an inclusion map). Now,

$$(\mathfrak{a} \circ \mathfrak{b})(x) = \underbrace{\mathfrak{a}}_{=\operatorname{syminc}_V \circ \alpha}\left(\underbrace{\mathfrak{b}(x)}_{=w}\right) = (\operatorname{syminc}_V \circ \alpha)(w) = \operatorname{syminc}_V\left(\underbrace{\alpha(w)}_{=w}\right) = \operatorname{syminc}_V(w) = x.$$

Qed.

On the other hand, $H_{>0} = V \oplus (H_{>0})^2 = V + (H_{>0})^2$ (since direct sums are sums). Furthermore, $H_0 = k \cdot 1_H$ (by Proposition 29.14). Thus, Lemma 40.7 **(b)** (applied to $A = H$) yields $H = \operatorname{AlgGen}_k V$.

Now, $V = \mathfrak{i}(V)$ [361]. Hence, $H = \operatorname{AlgGen}_k \underbrace{V}_{=\mathfrak{i}(V)} = \operatorname{AlgGen}_k (\mathfrak{i}(V))$.

Now, recall that $\operatorname{AlgGen}_k (\mathfrak{i}(V))$ is the k-subalgebra of H generated by $\mathfrak{i}(V)$ (by the definition of $\operatorname{AlgGen}_k (\mathfrak{i}(V))$). In other words, H is the k-subalgebra of H generated by $\mathfrak{i}(V)$ (since $H = \operatorname{AlgGen}_k (\mathfrak{i}(V))$). In other words, the image $\mathfrak{i}(V)$ generates the k-algebra H. Hence, Lemma 38.8 **(a)** (applied to $A = H$ and $\varphi = \mathfrak{i}$) shows that the k-algebra homomorphism $\operatorname{symlift} \mathfrak{i} : \operatorname{Sym} V \to H$ is surjective. In other words, the k-algebra homomorphism $\mathfrak{b} : \operatorname{Sym} V \to H$ is surjective (since $\mathfrak{b} = \operatorname{symlift} \mathfrak{i}$).

We now know that the map $\mathfrak{b}$ is both injective and surjective. Hence, $\mathfrak{b}$ is bijective. Thus, $\mathfrak{b}$ is invertible. Therefore,

$$\mathfrak{b} \text{ is a } k\text{-algebra isomorphism} \tag{600}$$

(since $\mathfrak{b}$ is an invertible k-algebra homomorphism). Hence, the inverse $\mathfrak{b}^{-1}$ of $\mathfrak{b}$ is well-defined, and also is a k-algebra isomorphism. This map $\mathfrak{b}^{-1}$ is invertible (since it is a k-algebra isomorphism), thus bijective, thus injective.

Recall that the map $e^{*\mathfrak{a}} \circ \mathfrak{b}$ is surjective. Thus, both maps $e^{*\mathfrak{a}} \circ \mathfrak{b}$ and $\mathfrak{b}^{-1}$ are injective. Therefore, their composition $(e^{*\mathfrak{a}} \circ \mathfrak{b}) \circ \mathfrak{b}^{-1}$ is also injective (since the composition of any two injective maps is injective). In other words, the map $e^{*\mathfrak{a}}$ is injective (since $(e^{*\mathfrak{a}} \circ \mathfrak{b}) \circ \mathfrak{b}^{-1} = e^{*\mathfrak{a}} \circ \underbrace{\mathfrak{b} \circ \mathfrak{b}^{-1}}_{=\mathrm{id}} = e^{*\mathfrak{a}}$).

We now know that the map $e^{*\mathfrak{a}}$ is both injective and surjective. Thus, $e^{*\mathfrak{a}}$ is bijective. Hence, $e^{*\mathfrak{a}}$ is invertible. Thus, $e^{*\mathfrak{a}}$ is a k-algebra isomorphism (since $e^{*\mathfrak{a}}$ is an invertible k-algebra homomorphism). This proves Theorem 40.13 **(b)**.

(a) We are going to apply the fact (600), which we have proven during our above proof of Theorem 40.13 **(b)**. However, in order to do this, we must ensure that we are in the situation of Theorem 40.13 **(b)**; that is, we must construct a k-linear map $\alpha : H \to V$ with the properties that $\alpha\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$ and $\alpha|_V = \mathrm{id}_V$.

However, this is easy: Lemma 40.11 **(b)** (applied to $C = H$) shows that $H_{>0} = \operatorname{Ker}(\varepsilon_H)$. Hence, $\operatorname{Ker}(\varepsilon_H) = H_{>0} = V \oplus (H_{>0})^2$. Thus, Lemma 40.12 (applied to $C = H$ and $W = (H_{>0})^2$) shows that there exists a k-linear map $\alpha : H \to V$ that satisfies $\alpha\left((H_{>0})^2 + k \cdot 1_H\right) = 0$ and $\alpha|_V = \mathrm{id}_V$. Consider this α. We have $\alpha\left((H_{>0})^2 + k \cdot 1_H\right) = 0$. Since $H_{>0} = \operatorname{Ker}(\varepsilon_H)$, this rewrites as $\alpha\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$. Thus, we now know that α is a k-linear map $H \to V$ satisfying $\alpha\left((\operatorname{Ker}(\varepsilon_H))^2 + k \cdot 1_H\right) = 0$ and $\alpha|_V = \mathrm{id}_V$. Therefore, the hypotheses of Theorem 40.13 **(b)** are satisfied. Thus, the fact (600) shows that $\mathfrak{b}$ is a k-algebra isomorphism. This proves Theorem 40.13 **(a)**. □

Remark 40.14. Consider the situation of Theorem 40.13. We can say slightly more: Namely, the k-algebra isomorphism $\mathfrak{b} : \operatorname{Sym} V \to H$ is graded, provided that the k-algebra $\operatorname{Sym} V$ has been equipped with the appropriate grading. (To equip $\operatorname{Sym} V$ with the appropriate grading, we have to regard V as a graded k-vector space[362], and extend this grading to

[361] *Proof.* Recall that $\mathfrak{i}$ is merely an inclusion map. Hence, $\mathfrak{i}(V) = V$, so that $V = \mathfrak{i}(V)$.

[362] Indeed, V is canonically graded, since it is a homogeneous subspace of the graded k-vector space H.

$\operatorname{Sym} V$. Note that this is **not** the grading on $\operatorname{Sym} V$ that was used in the proof of Theorem 40.13.)

The proof of this fact is left to the reader; it is fairly straightforward. Similarly, in the situation of Theorem 40.13 **(b)**, the k-algebra isomorphism $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is graded as well (where, again, $\operatorname{Sym} V$ is equipped with the appropriate grading).

We shall next transform Theorem 40.13 into a form more suited for applications. But first, let us prove a simple property of graded maps, similar in spirit to Remark 18.2:

Remark 40.15. Let k be a field. Let U and V be two graded k-vector spaces. Let $f : U \to V$ be a graded k-linear map. Then, $f(U)$ is a homogeneous subspace of V.

Proof of Remark 40.15. If W is any k-vector subspace of V, then the internal direct sum $\bigoplus_{n \in \mathbb{N}} (W \cap V_n)$ is always well-defined[363]. Applying this to $W = f(U)$, we conclude that the internal direct sum $\bigoplus_{n \in \mathbb{N}} (f(U) \cap V_n)$ is well-defined.

But U is graded. Thus, $U = \bigoplus_{n \in \mathbb{N}} U_n = \sum_{n \in \mathbb{N}} U_n$ (since direct sums are sums).

Also, the map f is graded. In other words, every $n \in \mathbb{N}$ satisfies

$$f(U_n) \subseteq V_n \tag{601}$$

(by the definition of a graded map). Hence, every $n \in \mathbb{N}$ satisfies

$$f(U_n) \subseteq f(U) \cap V_n \tag{602}$$

[364].

Applying the map f to both sides of the equality $U = \sum_{n \in \mathbb{N}} U_n$, we obtain

$$\begin{aligned} f(U) &= f\left(\sum_{n \in \mathbb{N}} U_n \right) = \sum_{n \in \mathbb{N}} \underbrace{f(U_n)}_{\substack{\subseteq f(U) \cap V_n \\ \text{(by (602))}}} \qquad \text{(since the map } f \text{ is } k\text{-linear)} \\ &\subseteq \sum_{n \in \mathbb{N}} (f(U) \cap V_n). \end{aligned}$$

Combining this with

$$\sum_{n \in \mathbb{N}} \underbrace{(f(U) \cap V_n)}_{\subseteq f(U)} \subseteq \sum_{n \in \mathbb{N}} f(U) \subseteq f(U) \qquad \text{(since } f(U) \text{ is a } k\text{-vector space)},$$

we obtain

$$f(U) = \sum_{n \in \mathbb{N}} (f(U) \cap V_n). \tag{603}$$

[363] This was proven during Definition 18.1.

[364] *Proof of (602):* Let $n \in \mathbb{N}$. Then, (601) yields $f(U) \subseteq V_n$. Combining $f\left(\underbrace{U_n}_{\subseteq U} \right) \subseteq f(U)$ with $f(U) \subseteq V_n$, we obtain $f(U_n) \subseteq f(U) \cap V_n$. This proves (602).

But recall that the internal direct sum $\bigoplus_{n\in\mathbb{N}} (f(U)\cap V_n)$ is well-defined. It satisfies

$$\begin{aligned}\bigoplus_{n\in\mathbb{N}} (f(U)\cap V_n) &= \sum_{n\in\mathbb{N}} (f(U)\cap V_n) \qquad \text{(since direct sums are sums)}\\ &= f(U) \qquad \text{(by (603))}.\end{aligned}$$

Thus, $f(U) = \bigoplus_{n\in\mathbb{N}} (f(U)\cap V_n)$.

But $f(U)$ is a k-vector subspace of V (since $f: U\to V$ is a k-linear map). Hence, $f(U)$ is a homogeneous subspace of V if and only if $f(U) = \bigoplus_{n\in\mathbb{N}} (f(U)\cap V_n)$ (by the definition of a "homogeneous subspace"). Thus, $f(U)$ is a homogeneous subspace of V (since we know that $f(U) = \bigoplus_{n\in\mathbb{N}} (f(U)\cap V_n)$). This proves Remark 40.15. □

We can now re-package Theorem 40.13 into the following corollary:

Corollary 40.16. Let k be a field of characteristic 0. Let H be a connected graded commutative bialgebra over k.

Let $\mathfrak{d}: H\to H$ be a graded k-linear map that is a projection (i.e., it satisfies $\mathfrak{d}\circ\mathfrak{d} = \mathfrak{d}$) and satisfies $\operatorname{Ker}\mathfrak{d} = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$.

Let $V = \mathfrak{d}(H)$. Let $\mathfrak{i}$ denote the inclusion map $V\to H$. Let $\mathfrak{b}$ denote the k-algebra homomorphism $\operatorname{symlift}\mathfrak{i}: \operatorname{Sym}V\to H$ [365].

(a) This map $\mathfrak{b}$ is a k-algebra isomorphism.

(b) Let $\alpha: H\to V$ be the map defined by $(\alpha(x) = \mathfrak{d}(x)$ for each $x\in H)$. It is easy to see that this map α is well-defined and k-linear. Define a k-linear map $\mathfrak{a}: H\to \operatorname{Sym}V$ by $\mathfrak{a} = \operatorname{syminc}_V\circ\alpha$. Then, $\mathfrak{a}\in\mathfrak{g}(H, \operatorname{Sym}V)$, and thus the k-linear map $e^{*\mathfrak{a}}: H\to\operatorname{Sym}V$ is well-defined. This map $e^{*\mathfrak{a}}: H\to\operatorname{Sym}V$ is a k-algebra isomorphism.[366]

Proof of Corollary 40.16. For each $m\in\mathbb{N}$, we define a k-vector subspace $H_{>m}$ of H by $H_{>m} = \sum_{\substack{g\in\mathbb{N};\\ g>m}} H_g$. Notice that $H = H_0 + H_{>0}$ [367].

Proposition 29.14 yields $H_0 = k\cdot 1_H$.

[365] We are using the notations introduced in Definition 38.1.

[366] The maps $\mathfrak{b}$ and $e^{*\mathfrak{a}}$ are not mutually inverse in general.

[367] *Proof.* The k-vector space H is graded. Hence, $H = \bigoplus_{g\in\mathbb{N}} H_g = \sum_{g\in\mathbb{N}} H_g$ (since direct sums are sums).

The definition of $H_{>0}$ yields $H_{>0} = \sum_{\substack{g\in\mathbb{N};\\ g>0}} H_g$. But

$$\begin{aligned}H &= \sum_{g\in\mathbb{N}} H_g = H_0 + \underbrace{\sum_{\substack{g\in\mathbb{N};\\ g>0}} H_g}_{=H_{>0}} \qquad \left(\begin{array}{c}\text{here, we have split off the addend}\\ \text{for } g=0 \text{ from the sum}\end{array}\right)\\ &= H_0 + H_{>0}.\end{aligned}$$

Remark 40.15 (applied to H, H and $\mathfrak{d}$ instead of U, V and f) shows that $\mathfrak{d}(H)$ is a homogeneous subspace of H. In other words, V is a homogeneous subspace of H (since $V = \mathfrak{d}(H)$).

Lemma 40.11 **(b)** (applied to $C = H$) shows that $H_{>0} = \operatorname{Ker}(\varepsilon_H)$. Also, $(H_{>0})^2 \subseteq H_{>0}$ [368].

Recall that the map $\mathfrak{d}$ is graded. Hence,

$$\mathfrak{d}(H_{>0}) \subseteq H_{>0} \tag{604}$$

[369].

Recall that $\mathfrak{d}$ is a projection. In other words, $\mathfrak{d} \circ \mathfrak{d} = \mathfrak{d}$.

---

[368] *Proof.* Recall that H is a k-bialgebra. Thus, the map ε_H is a k-algebra homomorphism (by the axioms of a k-bialgebra). Hence, its kernel $\operatorname{Ker}(\varepsilon_H)$ is an ideal of H. In other words, $H_{>0}$ is an ideal of H (since $H_{>0} = \operatorname{Ker}(\varepsilon_H)$). Hence, $HH_{>0} \subseteq H_{>0}$ and $H_{>0}H \subseteq H_{>0}$. Now, $(H_{>0})^2 = H_{>0} \underbrace{H_{>0}}_{\subseteq H} \subseteq H_{>0}H \subseteq H_{>0}$.

[369] *Proof.* The map $\mathfrak{d}$ is graded. In other words, every $n \in \mathbb{N}$ satisfies

$$\mathfrak{d}(H_n) \subseteq H_n \tag{605}$$

(by the definition of a graded map). Now, the definition of $H_{>0}$ yields $H_{>0} = \sum\limits_{\substack{g \in \mathbb{N}; \\ g>0}} H_g$. Applying the map $\mathfrak{d}$ to both sides of this equality, we obtain

$$\begin{aligned}
\mathfrak{d}(H_{>0}) &= \mathfrak{d}\left(\sum_{\substack{g \in \mathbb{N}; \\ g>0}} H_g\right) = \sum_{\substack{g \in \mathbb{N}; \\ g>0}} \underbrace{\mathfrak{d}(H_g)}_{\substack{\subseteq H_g \\ \text{(by (605)} \\ \text{(applied to } n=g))}} \qquad \text{(since the map } \mathfrak{d} \text{ is } k\text{-linear)} \\
&\subseteq \sum_{\substack{g \in \mathbb{N}; \\ g>0}} H_g = H_{>0}.
\end{aligned}$$

Now, it is easy to see that $H_{>0} \subseteq V + (H_{>0})^2$ [370] and $V + (H_{>0})^2 \subseteq H_{>0}$ [371]. Combining these two relations, we obtain $H_{>0} = V + (H_{>0})^2$.

---

[370] *Proof.* Let $x \in H_{>0}$. The map $\mathfrak{d}$ is k-linear; thus, we have

$$\mathfrak{d}(x - \mathfrak{d}(x)) = \mathfrak{d}(x) - \underbrace{\mathfrak{d}(\mathfrak{d}(x))}_{=(\mathfrak{d}\circ\mathfrak{d})(x)} = \mathfrak{d}(x) - \underbrace{(\mathfrak{d}\circ\mathfrak{d})}_{=\mathfrak{d}}(x) = \mathfrak{d}(x) - \mathfrak{d}(x) = 0.$$

In other words, $x - \mathfrak{d}(x) \in \operatorname{Ker}\mathfrak{d}$. In light of $\operatorname{Ker}\mathfrak{d} = H_0 + \left(\underbrace{\operatorname{Ker}(\varepsilon_H)}_{=H_{>0}}\right)^2 = H_0 + (H_{>0})^2$, this rewrites as $x - \mathfrak{d}(x) \in H_0 + (H_{>0})^2$. In other words, there exist $y \in H_0$ and $z \in (H_{>0})^2$ such that $x - \mathfrak{d}(x) = y + z$. Consider these y and z.

We shall show that $y = 0$. Indeed, we have $y \in H_0 = k \cdot 1_H$; thus, there exists some $\lambda \in k$ such that $y = \lambda \cdot 1_H$. Consider this λ.

We have $z \in (H_{>0})^2 \subseteq H_{>0} = \operatorname{Ker}(\varepsilon_H)$ and thus $\varepsilon_H(z) = 0$.

Recall that H is a k-bialgebra. Hence, $\varepsilon_H(1_H) = 1$ (by the axioms of a k-bialgebra). Now,

$$\varepsilon_H\left(\underbrace{y}_{=\lambda\cdot 1_H}\right) = \varepsilon_H(\lambda \cdot 1_H) = \lambda \cdot \underbrace{\varepsilon_H(1_H)}_{=1} \qquad \text{(since the map } \varepsilon_H \text{ is } k\text{-linear)}$$
$$= \lambda.$$

We have $\mathfrak{d}\left(\underbrace{x}_{\in H_{>0}}\right) \subseteq \mathfrak{d}(H_{>0}) \subseteq H_{>0}$ (by (604)). Thus, $\mathfrak{d}(x) \in H_{>0} = \operatorname{Ker}(\varepsilon_H)$, so that $\varepsilon_H(\mathfrak{d}(x)) = 0$. Now, let us apply the map ε_H to both sides of the equality $x - \mathfrak{d}(x) = y + z$. We thus obtain

$$\varepsilon_H(x - \mathfrak{d}(x)) = \varepsilon_H(y + z) = \underbrace{\varepsilon_H(y)}_{=\lambda} + \underbrace{\varepsilon_H(z)}_{=0} \qquad \text{(since the map } \varepsilon \text{ is } k\text{-linear)}$$
$$= \lambda.$$

Hence,

$$\lambda = \varepsilon_H(x - \mathfrak{d}(x)) = \underbrace{\varepsilon_H(x)}_{\substack{=0 \\ (\text{since } x \in H_{>0} = \operatorname{Ker}(\varepsilon_H))}} - \underbrace{\varepsilon_H(\mathfrak{d}(x))}_{=0} = 0.$$

Hence, $y = \underbrace{\lambda}_{=0} \cdot 1_H = 0$. Thus, $x - \mathfrak{d}(x) = \underbrace{y}_{=0} + z = z$, so that $x = \mathfrak{d}\left(\underbrace{x}_{\in H}\right) + \underbrace{z}_{\in (H_{>0})^2} \in \underbrace{\mathfrak{d}(H)}_{=V} + (H_{>0})^2 = V + (H_{>0})^2$.

Now, forget that we fixed x. We thus have shown that each $x \in H_{>0}$ satisfies $x \in V + (H_{>0})^2$. In other words, $H_{>0} \subseteq V + (H_{>0})^2$.

[371] *Proof.* We have $H_0 \subseteq H_0 + (\operatorname{Ker}(\varepsilon_H))^2 = \operatorname{Ker}\mathfrak{d}$ and thus $\mathfrak{d}(H_0) = 0$.

But $V \cap \left(H_{>0}\right)^2 = 0$ [372]. Hence, the internal direct sum $V \oplus \left(H_{>0}\right)^2$ is well-defined. This internal direct sum satisfies $V \oplus \left(H_{>0}\right)^2 = V + \left(H_{>0}\right)^2$. Comparing this with $H_{>0} = V + \left(H_{>0}\right)^2$, we obtain $H_{>0} = V \oplus \left(H_{>0}\right)^2$. Theorem 40.13 **(a)** thus yields that the map $\mathfrak{b}$ is a k-algebra isomorphism. This proves Corollary 40.16 **(a)**.

(b) Let us first prove that the map α is well-defined and k-linear.

Every $x \in H$ satisfies $\mathfrak{d}\left(\underbrace{x}_{\in H}\right) \in \mathfrak{d}\left(H\right) = V$. Thus, the map $\alpha : H \to V$ is well-defined (since this map is defined by $\left(\alpha\left(x\right) = \mathfrak{d}\left(x\right) \text{ for each } x \in H\right)$). Furthermore, the map α is k-linear[373].

Now, it remains to show that $\mathfrak{a} \in \mathfrak{g}\left(H, \operatorname{Sym} V\right)$, and that the map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is a k-algebra isomorphism.

For every subset T of H, we have

$$\alpha\left(T\right) = \left\{ \underbrace{\alpha\left(x\right)}_{\substack{=\mathfrak{d}(x) \\ \text{(by the definition of } \alpha\text{)}}} \;\middle|\; x \in T \right\} = \left\{ \mathfrak{d}\left(x\right) \;\middle|\; x \in T \right\} = \mathfrak{d}\left(T\right).$$

Applying this to $T = \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H$, we obtain

$$\begin{aligned} \alpha\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + k \cdot 1_H\right) &= \mathfrak{d}\left(\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + \underbrace{k \cdot 1_H}_{=H_0}\right) = \mathfrak{d}\left(\underbrace{\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 + H_0}_{=H_0+\left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 = \operatorname{Ker}\mathfrak{d}}\right) \\ &= \mathfrak{d}\left(\operatorname{Ker}\mathfrak{d}\right) = 0. \end{aligned}$$

But

$$\begin{aligned} V &= \mathfrak{d}\left(\underbrace{H}_{=H_0+H_{>0}}\right) = \mathfrak{d}\left(H_0 + H_{>0}\right) = \underbrace{\mathfrak{d}\left(H_0\right)}_{=0} + \mathfrak{d}\left(H_{>0}\right) \qquad \text{(since the map } \mathfrak{d} \text{ is } k\text{-linear)} \\ &= \mathfrak{d}\left(H_{>0}\right) \subseteq H_{>0} \qquad \text{(by (604))}. \end{aligned}$$

Now,

$$\underbrace{V}_{\subseteq H_{>0}} + \underbrace{\left(H_{>0}\right)^2}_{\subseteq H_{>0}} \subseteq H_{>0} + H_{>0} \subseteq H_{>0} \qquad \text{(since } H_{>0} \text{ is a } k\text{-vector space)}.$$

[372] *Proof.* Let $x \in V \cap \left(H_{>0}\right)^2$. Then, $x \in V \cap \left(H_{>0}\right)^2 \subseteq V = \mathfrak{d}\left(H\right)$. Thus, there exists some $y \in H$ such that $x = \mathfrak{d}\left(y\right)$. Consider this y.

Now, $\mathfrak{d}\left(\underbrace{x}_{=\mathfrak{d}(y)}\right) = \mathfrak{d}\left(\mathfrak{d}\left(y\right)\right) = \underbrace{\left(\mathfrak{d} \circ \mathfrak{d}\right)}_{=\mathfrak{d}}\left(y\right) = \mathfrak{d}\left(y\right) = x.$

But $x \in V \cap \left(H_{>0}\right)^2 \subseteq \left(\underbrace{H_{>0}}_{=\operatorname{Ker}\left(\varepsilon_H\right)}\right)^2 = \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 \subseteq H_0 + \left(\operatorname{Ker}\left(\varepsilon_H\right)\right)^2 = \operatorname{Ker}\mathfrak{d}$, so that $\mathfrak{d}\left(x\right) = 0$. Comparing this with $\mathfrak{d}\left(x\right) = x$, we obtain $x = 0$.

Now, forget that we fixed x. We thus have shown that every $x \in V \cap \left(H_{>0}\right)^2$ satisfies $x = 0$. In other words, $V \cap \left(H_{>0}\right)^2 = 0$.

[373] *Proof.* This map α is obtained from $\mathfrak{d}$ by restricting the codomain to V (since $\alpha\left(x\right) = \mathfrak{d}\left(x\right)$ for every $x \in H$). Hence, this map α is k-linear (since the map $\mathfrak{d}$ is k-linear).

Moreover, $\alpha\mid_V = \mathrm{id}_V$ [374]. Theorem 40.13 **(b)** thus shows that $\mathfrak{a} \in \mathfrak{g}(H, \operatorname{Sym} V)$, and that the map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is a k-algebra isomorphism. This proves Corollary 40.16 **(b)**. □

Corollary 40.16 can be applied to various choices of the map $\mathfrak{d}$. One obvious choice is the Eulerian idempotent $\operatorname{Log} \mathrm{id}$; however, this results in nothing new, but just a weaker version of Theorem 38.2 **(d)**[375]. However, we can also apply it to the Dynkin idempotents, and then we obtain something new. Actually, let us first extend Theorem 29.17:

Theorem 40.17. Let k be a field of characteristic 0. Let H be a commutative graded k-bialgebra. Let E_H be defined according to Definition 27.1.

Let $P : H \to H$ and $Q : H \to H$ be two graded k-algebra homomorphisms satisfying $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$ and $P * \mathrm{id}_H * Q = e_{H,H}$. Here, the map $e_{H,H}$ is defined to be the map $\eta_H \circ \varepsilon_H : H \to H$ (this definition of the map $e_{H,H}$ is identical with the definition of the map $e_{H,A}$ in Definition 1.12).

Let $\mathfrak{d}$ be the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q) : H \to H$.

(a) The map $\mathfrak{d}$ is a projection (i.e., it satisfies $\mathfrak{d} \circ \mathfrak{d} = \mathfrak{d}$) and satisfies $\operatorname{Ker} \mathfrak{d} = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$.

(b) The map $\mathfrak{d}$ is graded.

Let $V = \mathfrak{d}(H)$. Let $\mathfrak{i}$ denote the inclusion map $V \to H$. Let $\mathfrak{b}$ denote the k-algebra homomorphism $\operatorname{symlift} \mathfrak{i} : \operatorname{Sym} V \to H$ [376].

(c) This map $\mathfrak{b}$ is a k-algebra isomorphism.

(d) Let $\alpha : H \to V$ be the map defined by $(\alpha(x) = \mathfrak{d}(x)$ for each $x \in H)$. It is easy to see that this map α is well-defined and k-linear. Define a k-linear map $\mathfrak{a} : H \to \operatorname{Sym} V$ by $\mathfrak{a} = \operatorname{syminc}_V \circ \alpha$. Then, $\mathfrak{a} \in \mathfrak{g}(H, \operatorname{Sym} V)$, and thus the k-linear map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is well-defined. This map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is a k-algebra isomorphism.[377]

Proof of Theorem 40.17. Theorem 29.17 shows that the map $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ is a projection such that $\operatorname{Ker}\left(E_H^{\mathrm{inv}} \circ (P * E_H * Q)\right) = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$. Since $E_H^{\mathrm{inv}} \circ (P * E_H * Q) = \mathfrak{d}$ (because $\mathfrak{d}$ was defined to be $E_H^{\mathrm{inv}} \circ (P * E_H * Q)$), this rewrites as follows: The map $\mathfrak{d}$ is a projection such that $\operatorname{Ker} \mathfrak{d} = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$. This proves Theorem 40.17 **(a)**.

---

[374] *Proof.* Let $x \in V$. The definition of α yields $\alpha(x) = \mathfrak{d}(x)$.

But $x \in V = \mathfrak{d}(H)$. Thus, there exists some $y \in H$ such that $x = \mathfrak{d}(y)$. Consider this y.

Now, $\mathfrak{d}\left(\underbrace{x}_{=\mathfrak{d}(y)}\right) = \mathfrak{d}(\mathfrak{d}(y)) = \underbrace{(\mathfrak{d} \circ \mathfrak{d})}_{=\mathfrak{d}}(y) = \mathfrak{d}(y) = x$. Hence, $\alpha(x) = \mathfrak{d}(x) = x$.

Finally, $x \in V$, so that $(\alpha\mid_V)(x) = \alpha(x) = x = \mathrm{id}_V(x)$.

Now, forget that we fixed x. We thus have shown that $(\alpha\mid_V)(x) = \mathrm{id}_V(x)$ for each $x \in V$. In other words, $\alpha\mid_V = \mathrm{id}_V$.

[375] It is a weaker version for two reasons: Firstly, it requires H to be graded (not just filtered); secondly, it does not prove that the maps $\operatorname{symlift} \mathfrak{j}$ and $e^{*\mathfrak{q}}$ are mutually inverse.

[376] We are using the notations introduced in Definition 38.1.

[377] The maps $\mathfrak{b}$ and $e^{*\mathfrak{a}}$ are not mutually inverse in general.

In the proof of Theorem 29.12, we have shown that the map $P * E_H * Q$ is graded. Furthermore, Corollary 27.12 **(c)** (applied to H instead of V) shows that the map E_H^{inv} is graded.

Now, recall that $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (P * E_H * Q)$. Hence, the map $\mathfrak{d}$ is the composition of the two graded maps E_H^{inv} and $P * E_H * Q$ (since we know that both maps E_H^{inv} and $P * E_H * Q$ are graded), and therefore itself is a graded map (since any composition of two graded maps must be a graded map). This proves Theorem 40.17 **(b)**.

We thus conclude that the hypotheses of Corollary 40.16 are satisfied.

(c) Thus, Corollary 40.16 **(a)** shows that the map $\mathfrak{b}$ is a k-algebra isomorphism. This proves Theorem 40.17 **(c)**.

(d) Furthermore, Corollary 40.16 **(b)** shows that the map α is well-defined and k-linear, and that $\mathfrak{a} \in \mathfrak{g}(H, \operatorname{Sym} V)$, and that the map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is a k-algebra isomorphism. This proves Theorem 40.17 **(d)**. □

Let us now specialize Theorem 40.17 to the actual Dynkin idempotents:

Corollary 40.18. Let k be a field of characteristic 0. Let H be a commutative graded k-Hopf algebra. Let S be the antipode of H. Define a map $E_H : H \to H$ according to Definition 27.1. Define a map $E_H^{\mathrm{inv}} : H \to H$ according to Definition 27.9.

Let $\mathfrak{d} : H \to H$ be one of the two maps $E_H^{\mathrm{inv}} \circ (E_H * S)$ and $E_H^{\mathrm{inv}} \circ (S * E_H)$.

(a) The map $\mathfrak{d}$ is a projection (i.e., it satisfies $\mathfrak{d} \circ \mathfrak{d} = \mathfrak{d}$) and satisfies $\operatorname{Ker} \mathfrak{d} = H_0 + (\operatorname{Ker}(\varepsilon_H))^2$.

(b) The map $\mathfrak{d}$ is graded.

Let $V = \mathfrak{d}(H)$. Let $\mathfrak{i}$ denote the inclusion map $V \to H$. Let $\mathfrak{b}$ denote the k-algebra homomorphism $\operatorname{symlift} \mathfrak{i} : \operatorname{Sym} V \to H$ [378].

(c) This map $\mathfrak{b}$ is a k-algebra isomorphism.

(d) Let $\alpha : H \to V$ be the map defined by $(\alpha(x) = \mathfrak{d}(x)$ for each $x \in H)$. It is easy to see that this map α is well-defined and k-linear. Define a k-linear map $\mathfrak{a} : H \to \operatorname{Sym} V$ by $\mathfrak{a} = \operatorname{syminc}_V \circ \alpha$. Then, $\mathfrak{a} \in \mathfrak{g}(H, \operatorname{Sym} V)$, and thus the k-linear map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is well-defined. This map $e^{*\mathfrak{a}} : H \to \operatorname{Sym} V$ is a k-algebra isomorphism.[379]

Proof of Corollary 40.18. Just as in the proof of Corollary 29.8, we can prove the following facts:

- The map S is a k-algebra homomorphism from H to H.
- The map $e_{H,H}$ is a k-algebra homomorphism (where $e_{H,H}$ is defined as according to Definition 1.12).
- We have $S = \mathrm{id}_H^{*(-1)}$.
- We have $S * \mathrm{id}_H * e_{H,H} = e_{H,H}$ and $e_{H,H} * \mathrm{id}_H * S = e_{H,H}$.

[378] We are using the notations introduced in Definition 38.1.

[379] The maps $\mathfrak{b}$ and $e^{*\mathfrak{a}}$ are not mutually inverse in general.

Just as in the proof of Corollary 29.13, we can prove the following facts:

- We have $\varepsilon_H \circ e_{H,H} = \varepsilon_H$ and $\varepsilon_H \circ S = \varepsilon_H$.
- The maps $e_{H,H}$ and S are graded.

Now,

$$\left(\begin{array}{c} \text{there exist two graded } k\text{-algebra homomorphisms } P : H \to H \\ \text{and } Q : H \to H \text{ satisfying } \varepsilon_H \circ P = \varepsilon_H,\ \varepsilon_H \circ Q = \varepsilon_H, \\ P * \mathrm{id}_H * Q = e_{H,H} \text{ and } \mathfrak{d} = E_H^{\mathrm{inv}} \circ (P * E_H * Q) \end{array} \right) \tag{606}$$

[380]. Consider these P and Q. Thus, the hypotheses of Theorem 40.17 are satisfied. Hence, the four parts of Corollary 40.18 follow immediately from the corresponding four parts of Theorem 40.17. □

§41. A final remark on commutative rings

Let us make one final remark about generalizing the preceding results:

In §14, we noticed that most of the results in §1-§13, and most of the proofs, do not require k to be a field; only minor modifications are required to make them work when k is just a commutative ring with unity. Something similar can be said about the results of §15-§40: All theorems stated in §15-§40 still hold if k is just a commutative ring with unity, as long as the following replacements are made:

---

[380] *Proof of (606):* Recall that $e_{H,H}$ is the unity of the convolution algebra $\mathcal{L}(H,H)$. Thus, $e_{H,H} * E_H = E_H$ and $E_H * e_{H,H} = E_H$.

We know that $\mathfrak{d}$ is one of the two maps $E_H^{\mathrm{inv}} \circ (E_H * S)$ and $E_H^{\mathrm{inv}} \circ (S * E_H)$. Thus, we are in one of the following two cases:

Case 1: We have $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (E_H * S)$.

Case 2: We have $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (S * E_H)$.

Let us first consider Case 1. In this case, we have $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (E_H * S)$. Thus, $\mathfrak{d} = E_H^{\mathrm{inv}} \circ \left(\underbrace{E_H}_{=e_{H,H} * E_H} * S \right) = E_H^{\mathrm{inv}} \circ (e_{H,H} * E_H * S)$.

Altogether, we thus know that $e_{H,H} : H \to H$ and $S : H \to H$ are two graded k-algebra homomorphisms satisfying $\varepsilon_H \circ e_{H,H} = \varepsilon_H$, $\varepsilon_H \circ S = \varepsilon_H$, $e_{H,H} * \mathrm{id}_H * S = e_{H,H}$ and $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (e_{H,H} * E_H * S)$. Hence, there exist two graded k-algebra homomorphisms $P : H \to H$ and $Q : H \to H$ satisfying $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$, $P * \mathrm{id}_H * Q = e_{H,H}$ and $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ (namely, $P = e_{H,H}$ and $Q = S$). Thus, (606) is proven in Case 1.

Let us now consider Case 2. In this case, we have $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (S * E_H)$. Thus, $\mathfrak{d} = E_H^{\mathrm{inv}} \circ \left(S * \underbrace{E_H}_{=E_H * e_{H,H}} \right) = E_H^{\mathrm{inv}} \circ (S * E_H * e_{H,H})$.

Altogether, we thus know that $S : H \to H$ and $e_{H,H} : H \to H$ are two graded k-algebra homomorphisms satisfying $\varepsilon_H \circ S = \varepsilon_H$, $\varepsilon_H \circ e_{H,H} = \varepsilon_H$, $S * \mathrm{id}_H * e_{H,H} = e_{H,H}$ and $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (S * E_H * e_{H,H})$. Hence, there exist two graded k-algebra homomorphisms $P : H \to H$ and $Q : H \to H$ satisfying $\varepsilon_H \circ P = \varepsilon_H$, $\varepsilon_H \circ Q = \varepsilon_H$, $P * \mathrm{id}_H * Q = e_{H,H}$ and $\mathfrak{d} = E_H^{\mathrm{inv}} \circ (P * E_H * Q)$ (namely, $P = S$ and $Q = e_{H,H}$). Thus, (606) is proven in Case 2.

We have thus proven (606) in each of the two Cases 1 and 2. Since these two Cases cover all possibilities, we thus conclude that (606) always holds.

- Any occurrence of "k-vector space" must be replaced by "k-module".
- Any requirement that k be a field of characteristic 0 must be replaced by a requirement that k be a commutative $\mathbb{Q}$-algebra.
- The definition of the notion of a "filtered k-coalgebra" has to be replaced by the Definition 14.1.

Moreover, all of the proofs in §15-§40 can be easily adjusted to the general case when k is just a commutative ring with unity. The meaning of the word "adjust" here (i. e., the exact changes that have to be made to the proofs) is the same as the one explained in §14.

Note that, while the notion of a "filtered k-coalgebra" took a little bit of thinking to be adjusted to the case when k is a ring, the notion of a "graded k-coalgebra" generalizes in the most obvious way, since direct sums commute with tensor products over arbitrary rings (not only over fields).

References

[Mancho06] Dominique Manchon, *Hopf algebras, from basics to applications to renormalization*, Revised and updated version, may 2006, arXiv:math/0408405v2.
http://arxiv.org/abs/math/0408405v2

[PatReu98] Frédéric Patras and Christophe Reutenauer, *Higher Lie idempotents*, November 18, 1998.
http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.25.1416

[QEDMO09] *6th QEDMO 2009, Problem 4 (the Cauchy identity)*, with Solution by Darij Grinberg.
http://www.cip.ifi.lmu.de/~grinberg/QEDMO6P4long.pdf

[PatReu00] Frédéric Patras and Christophe Reutenauer, *On Dynkin and Klyacho idempotents in graded bialgebras*.
http://www-irma.u-strasbg.fr/annexes/publications/pdf/01029.pdf

[DMTCN13] Gérard Henry Edmond Duchamp, Vincel Hoang Ngoc Minh, Christophe Tollu, Bùi Chiên, Nguyen Hoang Nghia, *Combinatorics of deformed shuffle Hopf algebras*, arXiv:1302.5391v7.
http://arxiv.org/abs/1302.5391v7

[EGHLSVY] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina, *Introduction to representation theory*, arXiv:0901.0827v5.
http://arxiv.org/abs/0901.0827v5

[Grinbe08] Darij Grinberg, *St. Petersburg 2003: An alternating sum of zero-sum subset numbers*, version 14 March 2008.
http://www.cip.ifi.lmu.de/~grinberg/StPeters2003.pdf

[DPR13] Persi Diaconis, C. Y. Amy Pang, Arun Ram, *Hopf algebras and Markov chains: Two examples and a theory*, version of 30 December 2014.
https://amypang.github.io/papers/hpmc.pdf

[Cartie06] Pierre Cartier, *A Primer of Hopf algebras*, September 2006, IHES/M/06/40.
http://preprints.ihes.fr/2006/M/M-06-40.pdf

[AguLau14] Marcelo Aguiar, Aaron Lauve, *The characteristic polynomial of the Adams operators on graded connected Hopf algebras*, Algebra Number Theory 9 (2015), pp. 547–583. A preprint is available at arXiv:1403.7584v2.

[Grinbe17] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, Version of 25 May 2021.
http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf
The numbering of theorems and formulas in this link might shift when the project gets updated; for a "frozen" version whose numbering is guaranteed to match that in the citations above, see https://github.com/darijgr/detnotes/releases/tag/2021-05-25 or arXiv:2008.09862v2.

[Grinbe15] Darij Grinberg, *A few classical results on tensor, symmetric and exterior powers*, version 0.3 (June 13, 2017).
http://www.cip.ifi.lmu.de/~grinberg/algebra/tensorext.pdf

[Schnei15] Hans-Jürgen Schneider, *Hopfalgebren* (lecture notes taken by Darij Grinberg).
https://sites.google.com/site/darijgrinberg/hopfalgebren