

# $\lambda$ -rings: Definitions and basic properties

Darij Grinberg

Version 0.0.21, last revised January 10, 2019

## Contents

<b>1. Motivations</b>	<b>5</b>
1.1. Representation rings of groups . . . . .	5
1.2. Grothendieck rings of groups . . . . .	8
1.3. Vector bundles . . . . .	8
1.4. Exercises . . . . .	8
<b>2. <math>\lambda</math>-rings</b>	<b>9</b>
2.1. The definition . . . . .	9
2.2. An alternative characterization . . . . .	10
2.3. $\lambda$ -ideals . . . . .	12
2.4. Exercises . . . . .	13
<b>3. Examples of <math>\lambda</math>-rings</b>	<b>13</b>
3.1. Binomial $\lambda$ -rings . . . . .	13
3.2. Adjoining a polynomial variable to a $\lambda$ -ring . . . . .	15
3.3. Exercises . . . . .	17
<b>4. Intermezzo: Symmetric polynomials</b>	<b>18</b>
4.1. Symmetric polynomials are generated by the elementary symmetric ones	19
4.2. UV-symmetric polynomials are generated by the elementary symmetric ones . . . . .	21
4.3. Grothendieck's polynomials $P_k$ . . . . .	25
4.4. Grothendieck's polynomials $P_{k,j}$ . . . . .	31
4.5. Exercises . . . . .	34
<b>5. A <math>\lambda</math>-ring structure on <math>\Lambda(K) = 1 + K[[T]]^+</math></b>	<b>37</b>
5.1. Definition of the $\lambda$ -ring $\Lambda(K)$ . . . . .	37
5.2. Preparing for the proof of Theorem 5.1: introducing $1 + K[[T]]^+$ . . . . .	38
5.3. Preparing for the proof of Theorem 5.1: extending the ring to make polynomials split . . . . .	40

5.4.	Preparing for the proof of Theorem 5.1: the ring structure on $\Lambda(K)$ explained . . . . .	41
5.5.	Preparing for the proof of Theorem 5.1: the $(T)$ -topology . . . . .	46
5.6.	Proof of Theorem 5.1 . . . . .	48
5.7.	$\lambda_T : K \rightarrow \Lambda(K)$ is an additive group homomorphism . . . . .	52
5.8.	On the evaluation (substitution) map . . . . .	53
5.9.	The functor $\Lambda$ . . . . .	54
5.10.	Exercises . . . . .	55
<b>6.</b>	<b>Special <math>\lambda</math>-rings</b>	<b>56</b>
6.1.	Definition . . . . .	56
6.2.	$\Lambda(K)$ is special . . . . .	57
6.3.	Exercises . . . . .	61
<b>7.</b>	<b>Examples of special <math>\lambda</math>-rings</b>	<b>64</b>
7.1.	Binomial $\lambda$ -rings . . . . .	64
7.2.	Adjoining a polynomial variable to a $\lambda$ -ring . . . . .	65
7.3.	Exercises . . . . .	68
<b>8.</b>	<b>The <math>\lambda</math>-verification principle</b>	<b>68</b>
8.1.	$n$ -operations of special $\lambda$ -rings . . . . .	68
8.2.	A useful triviality . . . . .	69
8.3.	1-dimensional elements . . . . .	70
8.4.	The continuous splitting $\lambda$ -verification principle . . . . .	71
8.5.	$\lambda^i$ of a sum of 1-dimensional elements . . . . .	73
8.6.	Exercises . . . . .	74
<b>9.</b>	<b>Adams operations</b>	<b>74</b>
9.1.	The Hirzebruch-Newton polynomials . . . . .	74
9.2.	Definition of Adams operations . . . . .	77
9.3.	The equality $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$ for special $\lambda$ -rings . . . . .	77
9.4.	Adams operations are ring homomorphisms when the $\lambda$ -ring is special . . . . .	81
9.5.	The equality $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$ for arbitrary $\lambda$ -rings . . . . .	84
9.6.	Exercises . . . . .	93
<b>10.</b>	<b>Todd homomorphisms of power series</b>	<b>96</b>
10.1.	The universal polynomials $\text{Td}_{\varphi,j}$ . . . . .	96
10.2.	Defining the Todd homomorphism . . . . .	103
10.3.	The case when the power series is $1 + ut$ . . . . .	103
10.4.	The 0-th and 1-st coefficients of $\text{td}_{\varphi,T}(x)$ . . . . .	105
10.5.	Proof of Proposition 10.3 . . . . .	108
10.6.	The Todd homomorphism is multiplicative in $\varphi$ . . . . .	108
10.7.	$\text{td}_{\varphi,T}$ takes sums into products . . . . .	112
10.8.	The $\mathfrak{Todd}_{\varphi}$ map . . . . .	113
10.9.	Preparing for the proof of Lemma 10.17 . . . . .	117
10.10.	Proof of Lemma 10.17 . . . . .	122
10.11.	Preparing for the proof of Theorem 10.16: some trivial functoriality facts . . . . .	123
10.12.	Proof of Theorems 10.16 and 10.10 . . . . .	128

10.13	$\text{td}_{\varphi,T}$ is a homomorphism of additive groups . . . . .	128
10.14	$\text{td}_{\varphi,T}$ of a 1-dimensional element . . . . .	129
10.15	$\text{td}_{\varphi,T}$ for special $\lambda$ -rings . . . . .	132
10.16A	somewhat more general context for Todd homomorphisms . . . . .	136
10.17	Exercises . . . . .	138

**11. Hints and solutions to exercises** **141**

11.1.	To Section 1 . . . . .	141
11.2.	To Section 2 . . . . .	141
11.3.	To Section 3 . . . . .	144
11.4.	To Section 4 . . . . .	151
11.5.	To Section 5 . . . . .	161
11.6.	To Section 6 . . . . .	175
11.7.	To Section 7 . . . . .	190
11.8.	To Section 8 . . . . .	191
11.9.	To Section 9 . . . . .	193
11.10	To Section 10 . . . . .	207

This is a **BETA VERSION** and has never been systematically proofread. **Please notify me of any mistakes, typos and hard-to-understand arguments you find!**<sup>1</sup>

Thanks to Martin Brandenburg for pointing out several flaws.

At the moment, section 1 is missing a proof (namely, that the representation ring is a *special*  $\lambda$ -ring; I actually don't know this proof).

Most exercises have solutions or at least hints given at the end of this text; however, some do not.

**What is this?**

These notes try to cover some of the most important properties of  $\lambda$ -rings with proofs.

They were originally meant to accompany a talk at an undergraduate seminar, but quickly grew out of proportion to what could fit into a talk. Still they lack in anything really deep. At the moment, most of what is written here, except for the Todd homomorphism section, is also in Knutson's book [Knut73], albeit sometimes with different proofs. Part of the plan was to add some results from the Fulton/Lang book [FulLan85] with better proofs, but this is not currently my short-term objective, given that I don't understand much of [FulLan85] to begin with. Most of the notes were written independently of Yau's 2010 text [Yau10], but inevitably intersect with it.

I do not introduce, nor use, the  $\lambda$ -ring of symmetric functions (see [Knut73] and [Hazewi08b, §9, §16] for it). My avoidance of symmetric functions has no good reason<sup>2</sup>; unfortunately, it makes part of the notes (particularly, everything related to the  $\lambda$ -verification principle) unnecessarily unwieldy. This is one of the things I would have done differently if I were to rewrite these notes from scratch.

---

<sup>1</sup>my email address is A@B.com, where A=darijgrinberg and B=gmail

<sup>2</sup>Actually, the reason is that I have started writing these notes before I understood symmetric functions well.

# 0. Notation and conventions

Some notations that we will use later on:

- In the following,  $\mathbb{N}$  will denote the set  $\{0, 1, 2, \dots\}$ . The elements of this set  $\mathbb{N}$  will be called the *natural numbers*.
- When we say “ring”, we will always mean “commutative ring with unity”. A “ring homomorphism” is always supposed to send 1 to 1. When we say “ $R$ -algebra” (with  $R$  a ring), we will always mean “commutative  $R$ -algebra with unity”.
- Let  $R$  be a ring. An *extension ring* of  $R$  will mean a ring  $S$  along with a ring monomorphism  $R \rightarrow S$ . We will often sloppily identify  $R$  with a subring of  $S$  if  $S$  is an extension ring of  $R$ ; we will then also identify the polynomial ring  $R[T]$  with a subring of the polynomial ring  $S[T]$ , and so on. An extension ring  $S$  of  $R$  is called *finite-free* if and only if the  $R$ -module  $S$  is finite-free (i. e., a free  $R$ -module with a finite basis).
- We will use multisets. If  $I$  is a set, and  $u_i$  is an object for every  $i \in I$ , then we let  $[u_i \mid i \in I]$  denote the multiset formed by all the  $u_i$  where  $i$  ranges over  $I$  (this multiset will contain each object  $o$  as often as it appears as an  $u_i$  for some  $i \in I$ ). If  $I = \{1, 2, \dots, n\}$  for some  $n \in \mathbb{N}$ , then we also denote the multiset  $[u_i \mid i \in I]$  by  $[u_1, u_2, \dots, u_n]$ .
- We have not defined  $\lambda$ -rings yet, but it is important to mention some discrepancy in notation between different sources. Namely, some of the literature (including [Knut73], [Hazewi08a], [Hazewi08b] and [Yau10]) denotes as *pre- $\lambda$ -rings* what we call  $\lambda$ -rings and denotes as  *$\lambda$ -rings* what we call special  $\lambda$ -rings. Even worse, the notations in [FulLan85] are totally inconsistent<sup>3</sup>.
- When we say “monoid”, we always mean a monoid with a neutral element. (The analogous notion without a neutral element is called “semigroup”.) “Monoid homomorphisms” have to send the neutral element of the domain to the neutral element of the target.
- Most times you read an expression with a  $\sum$  or a  $\prod$  sign in mathematical literature, you know clearly what it means (e. g., the expression  $\prod_{k=1}^n \sin k$  means the product  $(\sin 1) \cdot (\sin 2) \cdot \dots \cdot (\sin n)$ ). However, some more complicated expressions with  $\sum$  and  $\prod$  signs can be ambiguous, like the expression  $\prod_{k=1}^n \sin k \cdot n$ : Does this expression mean  $\left(\prod_{k=1}^n \sin k\right) \cdot n$  or  $\prod_{k=1}^n ((\sin k) \cdot n)$ ? The answer depends on the author of the text.  
In *this* text, the following convention should be resorted to when parsing an expression with  $\sum$  or  $\prod$  signs:  
The argument of a  $\prod$  sign ends as early as reasonably possible. Here, “reasonably

---

<sup>3</sup>Often, “ $\lambda$ -ring” in [FulLan85] means “ $\lambda$ -ring with a positive structure” (such  $\lambda$ -rings are automatically special), but sometimes it simply means “ $\lambda$ -ring”.

possible” means that it cannot end before the last time the index of the product appears (e. g., the argument of  $\prod_{k=1}^n \sin k \cdot n$  cannot end before the last appearance of  $k$ ), that it cannot end inside a bracket (e. g., the argument of  $\prod_{k=1}^n ((\sin k) \cdot n)$  cannot end before the end of the  $n$ ), that it cannot end between a symbol and its exponent or index or between a function symbol or its arguments, and that the usual rules of precedence have to apply. For example, the expression  $\prod_{k=1}^n \sin k \cdot n$  has to be read as  $\left(\prod_{k=1}^n \sin k\right) \cdot n$ , and the expression  $\prod_{k=1}^n \sin k \cdot (\cos k)^2 k \cdot (n+1) kn$  has to be read as  $\left(\prod_{k=1}^n (\sin k \cdot (\cos k)^2 \cdot (n+1) k)\right) n$ . Similar rules apply to the parsing of a sum expression.

- Let  $R$  be a ring. Let  $P \in R[X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n]$  be a polynomial over  $R$  in  $m+n$  variables. Then, the *total degree* of  $P$  with respect to the variables  $X_1, X_2, \dots, X_m$  is defined as the highest  $d \in \mathbb{N}$  such that at least one monomial  $X_1^{a_1} X_2^{a_2} \dots X_m^{a_m} Y_1^{b_1} Y_2^{b_2} \dots Y_n^{b_n}$  with  $a_1 + a_2 + \dots + a_m = d$  appears in  $P$  with a nonzero coefficient. (This total degree is defined to be  $-\infty$  if  $P = 0$ .) Similarly, the total degree of  $P$  with respect to the variables  $Y_1, Y_2, \dots, Y_n$  is defined.
- The similarly-looking symbols  $\Lambda$  (a capital Lambda) and  $\wedge$  (a wedge symbol, commonly used for the logical operator “and”) will have completely different meanings. The notation  $\wedge^i V$  (where  $R$  is a ring,  $V$  is an  $R$ -module and  $i$  is a nonnegative integer) will stand for the  $i$ -th exterior power of the  $R$ -module  $V$ . On the other hand, the notation  $\Lambda(K)$  (where  $K$  is a ring) will stand for a certain ring defined in Chapter 4; this ring is **not** the exterior algebra of  $K$  (despite some authors denoting the latter by  $\Lambda(K)$ ).

## 1. Motivations

What is the point of  $\lambda$ -rings?

Fulton/Lang [FulLan85] motivate  $\lambda$ -rings through vector bundles. Here we are going for a more elementary motivation, namely through representation rings in group representation theory:

### 1.1. Representation rings of groups

Consider a finite group  $G$  and a field  $k$  of characteristic 0. In representation theory, one defines the so-called *representation ring* of the group  $G$  over the field  $k$ . This ring can be constructed as follows:

We consider only finite-dimensional representations of  $G$ .

Let  $\text{Rep}_k G$  be the set of all representations of the group  $G$  over the field  $k$ . (We disregard the set-theoretic problematics stemming from the notion of such a big set. If you wish, you can call it a class or a SET instead of a set, or restrict yourself to a smaller subset containing every representation up to isomorphism.)

Let  $\text{FRep}_k G$  be the free abelian group on the set  $\text{Rep}_k G$ . Let  $I$  be the subgroup

$$I = \langle U - V \mid U \text{ and } V \text{ are two isomorphic representations of } G \rangle \\ + \langle U \oplus V - U - V \mid U \text{ and } V \text{ are two representations of } G \rangle$$

of the free abelian group  $\text{FRep}_k G$  (written additively). Then,  $\text{FRep}_k G/I$  is an abelian group. Whenever  $U$  is a representation of  $G$ , we should denote the equivalence class of  $U \in \text{FRep}_k G$  modulo the ideal  $I$  by  $\overline{U}$ ; however, since we are going to work in  $\text{FRep}_k G/I$  throughout this Section 1 (because there is not much of interest to do in  $\text{FRep}_k G$  itself), we will simply write  $U$  for this equivalence class. This means that whenever  $U$  and  $V$  are two isomorphic representations of  $G$ , we will simply write  $U = V$ , and whenever  $U$  and  $V$  are two representations of  $G$ , we will simply write  $U + V = U \oplus V$ .

Denote by  $1$  the equivalence class of the trivial representation of  $G$  on  $k$  (with every element of  $G$  acting as identity) modulo  $I$ . We now define a ring structure on  $\text{FRep}_k G/I$  by letting  $1$  be the one of this ring, and defining the product of two representations of  $G$  as their tensor product (over  $k$ ). This is indeed a ring structure because we have isomorphisms

$$U \otimes (V \otimes W) \cong (U \otimes V) \otimes W, \\ (U \oplus V) \otimes W \cong (U \otimes W) \oplus (V \otimes W), \\ U \otimes (V \oplus W) \cong (U \otimes V) \oplus (U \otimes W), \\ U \otimes V \cong V \otimes U, \\ 1 \otimes U \cong U \otimes 1 \cong U, \\ 0 \otimes U \cong U \otimes 0 \cong 0$$

for any representations  $U$ ,  $V$  and  $W$ , and because tensor products preserve isomorphisms (this means that if  $U$ ,  $V$  and  $W$  are three representations of  $G$  such that  $V \cong W$  (as representations), then  $U \otimes V \cong U \otimes W$  and  $V \otimes U \cong W \otimes U$ ).

The ring  $\text{FRep}_k G/I$  is called the *representation ring of the group  $G$  over the field  $k$* . The elements of  $\text{FRep}_k G/I$  are called *virtual representations*.

This ring  $\text{FRep}_k G/I$  is helpful in working with representations. However, its ring structure does not yet reflect everything we can do with representations. In fact, we can build direct sums of representations (this is addition in  $\text{FRep}_k G/I$ ) and we can build tensor products (this is multiplication in  $\text{FRep}_k G/I$ ), but we can also build exterior powers of representations, and we have no idea yet what operation on  $\text{FRep}_k G/I$  this entails. So we see that the abstract notion of a ring is not enough to understand all of representation theory. We need a notion of a ring together with some operations that “behave like” taking exterior powers. What axioms should these operations satisfy?

Every representation  $V$  of a group  $G$  satisfies  $\wedge^0 V \cong 1$  and  $\wedge^1 V \cong V$ . Besides, for any two representations  $V$  and  $W$  of  $G$  and every  $k \in \mathbb{N}$ , there exists an isomorphism

$$\wedge^k (V \oplus W) \cong \bigoplus_{i=0}^k \wedge^i V \otimes \wedge^{k-i} W \quad (1)$$

(see Exercise 1.1). In the representation ring, this means

$$\wedge^k (V + W) = \sum_{i=0}^k (\wedge^i V) \cdot (\wedge^{k-i} W).$$

This already gives us three axioms for the operations that we want to introduce. If we extend these three axioms to arbitrary elements of  $\text{FRep}_k G/I$  (and not just actual representations), we can compute  $\wedge^k$  of virtual representations (and it turns out that it is well-defined), and we obtain the notion of a  $\lambda$ -ring.

We can still wonder whether these axioms are all that we can say about group representations. The answer is no: In addition to the formula (1), there exist relations of the form

$$\wedge^k (V \otimes W) = P_k (\wedge^1 V, \wedge^2 V, \dots, \wedge^k V, \wedge^1 W, \wedge^2 W, \dots, \wedge^k W)$$

for every  $k \in \mathbb{N}$  and any two representations  $V$  and  $W$  of  $G$  (2)

and

$$\wedge^k (\wedge^j (V)) = P_{k,j} (\wedge^1 V, \wedge^2 V, \dots, \wedge^{kj} V)$$

for every  $k \in \mathbb{N}$ ,  $j \in \mathbb{N}$  and any representation  $V$  of  $G$ , (3)

where  $P_k \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_k]$  and  $P_{k,j} \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_{kj}]$  are “universal” polynomials (i. e., polynomials only depending on  $k$  resp. on  $k$  and  $j$ , but not on  $V$ ,  $W$  or  $G$ ). These polynomials are rather hard to write down explicitly, so it will need some theoretical preparation to define them.<sup>4</sup>

These relations (1) and (3), generalized to arbitrary virtual representations, abstract to the notion of a *special  $\lambda$ -ring*. So  $\text{FRep}_k G/I$  is not just a  $\lambda$ -ring; it is a special  $\lambda$ -ring. However, it has even more structure than that: It is an *augmented  $\lambda$ -ring with positive structure*. “Augmented” means the existence of a ring homomorphism  $\varepsilon : \text{FRep}_k G/I \rightarrow \mathbb{Z}$  (a so-called *augmentation*) with certain properties; we will list these properties later, but let us now notice that for our representation ring  $\text{FRep}_k G/I$ , the obvious natural choice of  $\varepsilon$  is the homomorphism which maps every representation  $V$  of  $G$  to  $\dim V \in \mathbb{Z}$ . A “positive structure” is a subset of  $K$  closed under addition and multiplication and containing 1, and satisfying other properties; in our case, the best choice for a positive structure on  $\text{FRep}_k G/I$  is the subset

$$\{\bar{V} \mid V \text{ is a representation of } G\} \setminus 0 \subseteq \text{FRep}_k G/I.$$

The reader may wonder how much the ring  $\text{FRep}_k G/I$  actually tells us about representations of  $G$ . For example, if  $U$  and  $V$  are two representations of  $G$  such that  $\bar{U} = \bar{V}$  in  $\text{FRep}_k G/I$ , does this mean that  $U \cong V$ ? It turns out that this is true, thanks to the cancellative property of representation theory<sup>5</sup>; hence, abstract algebraic

---

<sup>4</sup>Note that these polynomials can have negative coefficients, so that the equality (2) does not necessarily mean an isomorphism of the kind

$$\wedge^k (V \otimes W) \cong \text{direct sum of some tensor products of some } \wedge^i V \text{ and } \wedge^j W,$$

but generally means an isomorphism of the kind

$$\begin{aligned} \wedge^k (V \otimes W) &\oplus \text{direct sum of some tensor products of some } \wedge^i V \text{ and } \wedge^j W \\ &\cong (\text{another}) \text{direct sum of some tensor products of some } \wedge^i V \text{ and } \wedge^j W, \end{aligned}$$

and similarly (3) has to be understood.

<sup>5</sup>This is the property that whenever  $U$ ,  $V$  and  $W$  are three representations of a finite group  $G$  such that  $U \oplus W \cong V \oplus W$  (where we recall once again that “representation” means “finite-dimensional representation” for us!), then  $U \cong V$ . This can be proven using the Krull-Remak-Schmidt theorem, or, when the characteristic of the field is 0, using semisimplicity of  $k[G]$ .

identities that we can prove to hold in arbitrary special  $\lambda$ -rings yield actual isomorphisms of representations of finite groups. (Of course, they only yield them once we will have proven that  $\text{FRep}_k G/I$  is a special  $\lambda$ -ring. At the moment, this is not proven in this text, although it is rather easy to show using character theory.)

## 1.2. Grothendieck rings of groups

The situation gets more complicated when the field over which we are working is not of characteristic 0. In this case, it turns out that  $\text{FRep}_k G/I$  is not necessarily a special  $\lambda$ -ring any more (although still a  $\lambda$ -ring by Exercise 1.1). If we insist on getting a special  $\lambda$ -ring, we must modify our definition of  $I$  to

$$I = \langle V - U - W \mid U, V \text{ and } W \text{ are three representations of } G \text{ such that} \\ \text{there exists an exact sequence } 0 \rightarrow U \rightarrow V \rightarrow W \rightarrow 0 \rangle.$$

The resulting ring  $\text{FRep}_k G/I$  is called the *Grothendieck ring* of representations of  $G$  over our field. A proof that it is a special  $\lambda$ -ring is sketched in [Seiler88, Example on page 95], but I do not understand it. Anyway this result is not as strong as in characteristic 0 anymore, because the equality  $\overline{U} = \overline{V}$  in the Grothendieck ring  $\text{FRep}_k G/I$  does not imply  $U \cong V$  as representations of  $G$  when  $\text{char } k \neq 0$ . So the Grothendieck ring is, in some sense, a pale shadow of the representation theory of  $G$ .

## 1.3. Vector bundles

Vector bundles over a given compact Hausdorff space are similar to representations of a given group in several ways: They are somehow “enriched” vector space structures (a vector bundle is, roughly speaking, a family of vector spaces with additional topological structure; a representation of a group is a vector space with a group action on it), so one can form direct sums, tensor products and exterior powers of both of these. Hence, it is not surprising that we can define a  $\lambda$ -ring structure on a kind of “ring of vector bundles over a space” similarly to the  $\lambda$ -ring structure on the representation ring of a group. However, just as in the case of representations of a group over nonzero characteristic, we must be careful with vector bundles, because this “ring of vector bundles over a space” actually does not consist of vector bundles, but of equivalence classes, and sometimes, different vector bundles can lie in one and the same equivalence class (just as representations of groups are no longer uniquely determined by their equivalence class in the representation ring when the characteristic of the ground field is not 0). This “ring of vector bundles” is denoted by  $K(X)$ , where  $X$  is the base space, and is the first fundamental object of study in K-theory. We will not delve into K-theory here; we will only provide some of its backbone, namely the abstract algebraic theory of  $\lambda$ -rings (which appear not only in K-theory, but also in representation theory and elsewhere).

## 1.4. Exercises

*Exercise 1.1.* Let  $G$  be a group, and let  $V$  and  $W$  be two representations of  $G$ . Let  $k \in \mathbb{N}$ . Let  $\iota_V : V \rightarrow V \oplus W$  and  $\iota_W : W \rightarrow V \oplus W$  be the canonical injections.



For every  $i \in \{0, 1, \dots, k\}$ , we can define a vector space homomorphism

$$\Phi_i : \wedge^i V \otimes \wedge^{k-i} W \rightarrow \wedge^k (V \oplus W)$$

by requiring that it sends

$$\begin{aligned} (v_1 \wedge v_2 \wedge \dots \wedge v_i) \otimes (w_1 \wedge w_2 \wedge \dots \wedge w_{k-i}) & \quad \text{to} \\ \iota_V(v_1) \wedge \iota_V(v_2) \wedge \dots \wedge \iota_V(v_i) \wedge \iota_W(w_1) \wedge \iota_W(w_2) \wedge \dots \wedge \iota_W(w_{k-i}) \end{aligned}$$

for all  $v_1, v_2, \dots, v_i \in V$  and  $w_1, w_2, \dots, w_{k-i} \in W$ .

(a) Prove that this vector space homomorphism  $\Phi_i$  is a homomorphism of representations.

(b) Prove that the vector space homomorphism

$$\bigoplus_{i=0}^k \wedge^i V \otimes \wedge^{k-i} W \rightarrow \wedge^k (V \oplus W)$$

composed of the homomorphisms  $\Phi_i$  for all  $i \in \{0, 1, \dots, k\}$  is a canonical isomorphism of representations.

## 2. $\lambda$ -rings

### 2.1. The definition

The following definition introduces our most important notions: that of a  $\lambda$ -ring, that of a  $\lambda$ -ring homomorphism, and that of a sub- $\lambda$ -ring. While these notions are rather elementary (and much easier to define than the ones in Sections 5 and later), they are the basis of our theory.

**Definition. 1)** Let  $K$  be a ring. Let  $\lambda^i : K \rightarrow K$  be a mapping<sup>6</sup> for every  $i \in \mathbb{N}$  such that

$$\lambda^0(x) = 1 \text{ and } \lambda^1(x) = x \quad \text{for every } x \in K. \quad (4)$$

Assume that

$$\lambda^k(x + y) = \sum_{i=0}^k \lambda^i(x) \lambda^{k-i}(y) \quad \text{for every } k \in \mathbb{N}, x \in K \text{ and } y \in K. \quad (5)$$

Then, we call  $(K, (\lambda^i)_{i \in \mathbb{N}})$  a  $\lambda$ -ring. We will also call  $K$  itself a  $\lambda$ -ring if there is an obvious (from the context) choice of the sequence of mappings  $(\lambda^i)_{i \in \mathbb{N}}$  which makes  $(K, (\lambda^i)_{i \in \mathbb{N}})$  a  $\lambda$ -ring.

**2)** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and  $(L, (\mu^i)_{i \in \mathbb{N}})$  be two  $\lambda$ -rings. Let  $f : K \rightarrow L$  be a map. Then,  $f$  is called a  $\lambda$ -ring homomorphism (or homomorphism of  $\lambda$ -rings) if and only if  $f$  is a ring homomorphism and satisfies  $\mu^i \circ f = f \circ \lambda^i$  for every  $i \in \mathbb{N}$ .

---

<sup>6</sup>Here, “mapping” actually means “mapping” and not “group homomorphism” or “ring homomorphism”.

3) Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $L$  be a subring of  $K$ . Then,  $L$  is said to be a *sub- $\lambda$ -ring* of  $(K, (\lambda^i)_{i \in \mathbb{N}})$  if and only if  $\lambda^i(L) \subseteq L$  for every  $i \in \mathbb{N}$ . Obviously, if  $L$  is a sub- $\lambda$ -ring of  $(K, (\lambda^i)_{i \in \mathbb{N}})$ , then  $(L, (\lambda^i|_L)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring, and the canonical inclusion  $L \rightarrow K$  is a  $\lambda$ -ring homomorphism.

## 2.2. An alternative characterization

We will now give an alternative characterization of  $\lambda$ -rings:

**Theorem 2.1.** Let  $K$  be a ring. Let  $\lambda^i : K \rightarrow K$  be a mapping<sup>7</sup> for every  $i \in \mathbb{N}$  such that  $\lambda^0(x) = 1$  and  $\lambda^1(x) = x$  for every  $x \in K$ . Consider the ring  $K[[T]]$  of formal power series in the indeterminate  $T$  over the ring  $K$ . Define a map  $\lambda_T : K \rightarrow K[[T]]$  by

$$\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \quad \text{for every } x \in K.$$

Note that the power series  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$  has the coefficient  $\lambda^0(x) = 1$  before  $T^0$ ; thus, it is invertible in  $K[[T]]$ .

(a) Then,

$$\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x + y) \quad \text{for every } x \in K \text{ and every } y \in K$$

if and only if  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring.

(b) Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Then,

$$\begin{aligned} \lambda_T(0) &= 1; \\ \lambda_T(-x) &= (\lambda_T(x))^{-1} \quad \text{for every } x \in K; \\ \lambda_T(x) \cdot \lambda_T(y) &= \lambda_T(x + y) \quad \text{for every } x \in K \text{ and every } y \in K. \end{aligned}$$

(c) Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and  $(L, (\mu^i)_{i \in \mathbb{N}})$  be two  $\lambda$ -rings. Consider the map  $\lambda_T : K \rightarrow K[[T]]$  defined above, and a similarly defined map  $\mu_T : L \rightarrow L[[T]]$  for the  $\lambda$ -ring  $L$ . Let  $f : K \rightarrow L$  be a ring homomorphism. Consider the rings  $K[[T]]$  and  $L[[T]]$ . Obviously, the homomorphism  $f$  induces a homomorphism  $f[[T]] : K[[T]] \rightarrow L[[T]]$  (defined by

$$\begin{aligned} (f[[T]]) \left( \sum_{i \in \mathbb{N}} a_i T^i \right) &= \sum_{i \in \mathbb{N}} f(a_i) T^i \\ &\quad \text{for every } \sum_{i \in \mathbb{N}} a_i T^i \in K[[T]] \text{ with } a_i \in K \end{aligned}$$

).

Then,  $f$  is a  $\lambda$ -ring homomorphism if and only if  $\mu_T \circ f = f[[T]] \circ \lambda_T$ .

(d) Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Then,  $\lambda^i(0) = 0$  for every positive integer  $i$ .

---

<sup>7</sup>Here, “mapping” actually means “mapping” and not “group homomorphism” or “ring homomorphism”.

*Proof of Theorem 2.1. (a)* Every  $x \in K$  and every  $y \in K$  satisfy

$$\begin{aligned} \lambda_T(x) \cdot \lambda_T(y) &= \left( \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \right) \cdot \left( \sum_{i \in \mathbb{N}} \lambda^i(y) T^i \right) \\ &= \left( \text{since } \lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \text{ and } \lambda_T(y) = \sum_{i \in \mathbb{N}} \lambda^i(y) T^i \right) \\ &= \sum_{k \in \mathbb{N}} \sum_{i=0}^k \lambda^i(x) \lambda^{k-i}(y) \cdot T^k \\ &\quad \text{(by the definition of the product of two formal power series)} \end{aligned}$$

and

$$\lambda_T(x+y) = \sum_{i \in \mathbb{N}} \lambda^i(x+y) T^i = \sum_{k \in \mathbb{N}} \lambda^k(x+y) T^k.$$

Hence, the equation  $\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x+y)$  is equivalent to  $\sum_{k \in \mathbb{N}} \sum_{i=0}^k \lambda^i(x) \lambda^{k-i}(y) \cdot T^k = \sum_{k \in \mathbb{N}} \lambda^k(x+y) T^k$ , which, in turn, means that every  $k \in \mathbb{N}$  satisfies  $\sum_{i=0}^k \lambda^i(x) \lambda^{k-i}(y) = \lambda^k(x+y)$ , and this is exactly the property (5) from the definition of a  $\lambda$ -ring. Thus, we have  $\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x+y)$  for every  $x \in K$  and every  $y \in K$  if and only if  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. This proves Theorem 2.1 (a).

(b) Theorem 2.1 (a) tells us that  $\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x+y)$  for every  $x \in K$  and every  $y \in K$  if and only if  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. Since we know that  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring, we thus conclude that

$$\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x+y) \quad \text{for every } x \in K \text{ and every } y \in K. \quad (6)$$

Applied to  $x = y = 0$ , this rewrites as  $\lambda_T(0) \cdot \lambda_T(0) = \lambda_T(0+0) = \lambda_T(0)$ , what yields  $\lambda_T(0) = 1$  (since  $\lambda_T(0)$  is invertible in  $K[[T]]$ ).

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

$$\begin{aligned} \lambda_T(x) \cdot \lambda_T(-x) &= \lambda_T(0) \quad \text{(by (6), applied to } y = -x) \\ &= 1, \end{aligned}$$

hence  $\lambda_T(-x) = (\lambda_T(x))^{-1}$ . Theorem 2.1 (b) is thus proven.

(c) We have  $(\mu_T \circ f)(x) = \mu_T(f(x)) = \sum_{i \in \mathbb{N}} \mu^i(f(x)) T^i$  (by the definition of  $\mu_T$ )

and  $(f[[T]] \circ \lambda_T)(x) = (f[[T]])(\lambda_T(x)) = (f[[T]]) \left( \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \right) = \sum_{i \in \mathbb{N}} f(\lambda^i(x)) T^i$  for every  $x \in K$ . Hence,  $\mu_T \circ f = f[[T]] \circ \lambda_T$  is equivalent to  $\sum_{i \in \mathbb{N}} \mu^i(f(x)) T^i = \sum_{i \in \mathbb{N}} f(\lambda^i(x)) T^i$  for every  $x \in K$ , which in turn is equivalent to  $\mu^i(f(x)) = f(\lambda^i(x))$  for every  $x \in K$  and every  $i \in \mathbb{N}$ , which in turn means that  $\mu^i \circ f = f \circ \lambda^i$  for every  $i \in \mathbb{N}$ , which in turn means that  $f$  is a  $\lambda$ -ring homomorphism. This proves Theorem 2.1 (c).

(d) Applying the equality  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$  to  $x = 0$ , we obtain  $\lambda_T(0) = \sum_{i \in \mathbb{N}} \lambda^i(0) T^i$ . But since  $\lambda_T(0) = 1$ , this rewrites as  $1 = \sum_{i \in \mathbb{N}} \lambda^i(0) T^i$ . For every positive integer  $i$ , the coefficient of  $T^i$  on the left hand side of this equality is 0, while the coefficient of  $T^i$  on the right hand side of this equality is  $\lambda^i(0)$ . Since the coefficients of  $T^i$  on the two sides of an equality must be equal, this yields  $0 = \lambda^i(0)$  for every positive integer  $i$ . This proves Theorem 2.1 (d).  $\square$

The map  $\lambda_T$  defined in Theorem 2.1 will follow us through the whole theory of  $\lambda$ -rings. It is often easier to deal with than the maps  $\lambda^i$ , since (as Theorem 2.1 (a) and (b) show)  $\lambda_T$  is a monoid homomorphism from  $(K, +)$  to  $(K[[T]], \cdot)$  when  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. Many properties of  $\lambda$ -rings are easier to write in terms of  $\lambda_T$  than in terms of the separate  $\lambda^i$ . We will later become acquainted with the notion of “special  $\lambda$ -rings”, for which  $\lambda_T$  is not only a monoid homomorphism but actually a  $\lambda$ -ring homomorphism (but not to  $K[[T]]$  but to a different  $\lambda$ -ring with a new ring structure).

### 2.3. $\lambda$ -ideals

Just as rings have ideals and Lie algebras have Lie ideals, there is a notion of  $\lambda$ -ideals defined for  $\lambda$ -rings. Here is one way to define them:

**Definition.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $I$  be an ideal of the ring  $K$ . Then,  $I$  is said to be a  $\lambda$ -ideal of  $K$  if and only if every  $t \in I$  and every positive integer  $i$  satisfy  $\lambda^i(t) \in I$ .

Just as rings can be factored by ideals to obtain new rings, and Lie algebras can be factored by Lie ideals to obtain new Lie algebras, we can factor  $\lambda$ -rings by  $\lambda$ -ideals and obtain new  $\lambda$ -rings:

**Theorem 2.2.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $I$  be a  $\lambda$ -ideal of the ring  $K$ . For every  $z \in K$ , let  $\bar{z}$  denote the residue class of  $z$  modulo  $I$ . (This  $\bar{z}$  lies in  $K/I$ .)

(a) If  $x \in K/I$  is arbitrary, and  $y \in K$  and  $z \in K$  are two elements of  $K$  satisfying  $\bar{y} = x$  and  $\bar{z} = x$ , then  $\overline{\lambda^i(y)} = \overline{\lambda^i(z)}$  for every  $i \in \mathbb{N}$ .

(b) For every  $i \in \mathbb{N}$ , define a map  $\tilde{\lambda}^i : K/I \rightarrow K/I$  as follows: For every  $x \in K/I$ , let  $\tilde{\lambda}^i(x)$  be defined as  $\overline{\lambda^i(w)}$ , where  $w$  is an element of  $K$  satisfying  $\bar{w} = x$ . (This is well-defined because the value of  $\overline{\lambda^i(w)}$  does not depend on the choice of  $w$  <sup>8</sup>.)

Then,  $(K/I, (\tilde{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring.

(c) The canonical projection  $K \rightarrow K/I$  is a  $\lambda$ -ring homomorphism.

The proof of Theorem 2.2 is given in the solution of Exercise 2.3. Along with Theorem 2.2 comes the following result:

**Theorem 2.3.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and  $(L, (\mu^i)_{i \in \mathbb{N}})$  be two  $\lambda$ -rings. Let  $f : K \rightarrow L$  be a  $\lambda$ -ring homomorphism. Then,  $\text{Ker } f$  is a  $\lambda$ -ideal.

The proof of Theorem 2.3 is given in the solution of Exercise 2.4.

---

<sup>8</sup>In fact, any two choices of  $w$  lead to the same value of  $\overline{\lambda^i(w)}$  (this follows from Theorem 2.2 (a)).

## 2.4. Exercises

*Exercise 2.1.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and  $(L, (\mu^i)_{i \in \mathbb{N}})$  be two  $\lambda$ -rings. Let  $f : K \rightarrow L$  be a ring homomorphism. Let  $E$  be a generating set of the  $\mathbb{Z}$ -module  $K$ .

(a) Prove that  $f$  is a  $\lambda$ -ring homomorphism if and only if every  $e \in E$  satisfies  $(\mu_T \circ f)(e) = (f \circ [\lambda_T]) \circ \lambda_T(e)$ .

(b) Prove that  $f$  is a  $\lambda$ -ring homomorphism if and only if every  $e \in E$  satisfies  $(\mu^i \circ f)(e) = (f \circ \lambda^i)(e)$  for every  $i \in \mathbb{N}$ .

*Exercise 2.2.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $L$  be a subset of  $K$  which is closed under addition, multiplication and the maps  $\lambda^i$ . Assume that  $0 \in L$  and  $1 \in L$ . Then, the subset  $L - L$  of  $K$  (this subset  $L - L$  is defined by  $L - L = \{\ell - \ell' \mid \ell \in L, \ell' \in L\}$ ) is a sub- $\lambda$ -ring of  $K$ .

*Exercise 2.3.* Prove Theorem 2.2.

*Exercise 2.4.* Prove Theorem 2.3.

## 3. Examples of $\lambda$ -rings

### 3.1. Binomial $\lambda$ -rings

Before we go deeper into the theory, it is time for some examples.

Obviously, the trivial ring  $0$  (the ring satisfying  $0 = 1$ ) along with the trivial maps  $\lambda^i : 0 \rightarrow 0$  is a  $\lambda$ -ring. Let us move on to more surprising examples:

**Theorem 3.1.** For every  $i \in \mathbb{N}$ , define a map  $\lambda^i : \mathbb{Z} \rightarrow \mathbb{Z}$  by  $\lambda^i(x) = \binom{x}{i}$  for every  $x \in \mathbb{Z}$ .<sup>9</sup> Then,  $(\mathbb{Z}, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring.

*Proof of Theorem 3.1.* Trivially,  $\lambda^0(x) = 1$  and  $\lambda^1(x) = x$  for every  $x \in \mathbb{Z}$ . The only challenge, if there is a challenge in this proof, is to verify the identity (5) for  $K = \mathbb{Z}$ . In other words, we have to prove that

$$\binom{x+y}{k} = \sum_{i=0}^k \binom{x}{i} \binom{y}{k-i} \quad (7)$$

for every  $k \in \mathbb{N}$ ,  $x \in \mathbb{Z}$  and  $y \in \mathbb{Z}$ . This is the so-called *Vandermonde convolution identity*, and various proofs of it can easily be found in the literature<sup>10</sup>. Probably the shortest proof of (7) is the following: If we fix  $k \in \mathbb{N}$ , then (7) is a polynomial identity in both  $x$  and  $y$  (indeed, both sides of (7) are polynomials in  $x$  and  $y$  with rational coefficients), and thus it is enough to prove it for all natural  $x$  and  $y$  (because a polynomial identity holding for all natural variables must hold everywhere). But for

<sup>9</sup>Note that  $\binom{x}{i}$  is defined to be  $\frac{x \cdot (x-1) \cdot \dots \cdot (x-i+1)}{i!}$  for every  $x \in \mathbb{R}$  and  $i \in \mathbb{N}$ .

<sup>10</sup>For example, it follows immediately from [Grin-detn, Theorem 3.29].

$x$  and  $y$  natural, we have

$$\begin{aligned} \sum_{k=0}^{x+y} \sum_{i=0}^k \binom{x}{i} \binom{y}{k-i} T^k &= \underbrace{\sum_{i=0}^x \binom{x}{i} T^i}_{=(1+T)^x \text{ (by the binomial formula)}} \cdot \underbrace{\sum_{j=0}^y \binom{y}{j} T^j}_{=(1+T)^y \text{ (by the binomial formula)}} \\ &= (1+T)^x \cdot (1+T)^y = (1+T)^{x+y} = \sum_{k=0}^{x+y} \binom{x+y}{k} T^k \\ &\quad \text{(by the binomial formula)} \end{aligned}$$

in the polynomial ring  $\mathbb{Z}[T]$ . Comparing coefficients before  $T^k$  in this equality, we quickly conclude that (7) holds for each  $k \in \mathbb{N}$ . Thus, (7) is proven.<sup>11</sup> This proves Theorem 3.1.  $\square$

Our next example is a generalization of Theorem 3.1:

**Definition.** Let  $K$  be a ring. We call  $K$  a *binomial ring* if and only if none of the elements  $1, 2, 3, \dots$  is a zero-divisor in  $K$ , and  $n! \mid x \cdot (x-1) \cdot \dots \cdot (x-i+1)$  for every  $x \in K$  and every  $n \in \mathbb{N}$ .

**Theorem 3.2.** Let  $K$  be a binomial ring. For every  $i \in \mathbb{N}$ , define a map  $\lambda^i : K \rightarrow K$  by  $\lambda^i(x) = \binom{x}{i}$  for every  $x \in K$  (where, again,  $\binom{x}{i}$  is defined to be  $\frac{x \cdot (x-1) \cdot \dots \cdot (x-i+1)}{i!}$ ). Then,  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring.

Such  $\lambda$ -rings  $K$  are called *binomial  $\lambda$ -rings*.

*Proof of Theorem 3.2.* Obviously,  $\lambda^0(x) = 1$  and  $\lambda^1(x) = x$  for every  $x \in K$ , so it only remains to show that (5) is satisfied. This means proving (7) for every  $k \in \mathbb{N}$ ,  $x \in K$  and  $y \in K$ . But this is easy now: Fix  $k \in \mathbb{N}$ . Then, (7) is a polynomial identity in both  $x$  and  $y$ , and since we know that it holds for every  $x \in \mathbb{Z}$  and every  $y \in \mathbb{Z}$  (as we have seen in the proof of Theorem 3.1), it follows that it holds for every  $x \in K$  and every  $y \in K$  (since a polynomial identity holding for all integer variables must hold everywhere). This completes the proof of Theorem 3.2.  $\square$

Obviously, the  $\lambda$ -ring  $(\mathbb{Z}, (\lambda^i)_{i \in \mathbb{N}})$  defined in Theorem 3.1 is a binomial  $\lambda$ -ring. For other examples of binomial  $\lambda$ -rings, see Exercise 3.1. Of course, every  $\mathbb{Q}$ -algebra is a binomial ring as well.

---

<sup>11</sup>*Remark.* It is tempting to apply this argument to the general case (where  $x$  and  $y$  are not required to be natural), because the binomial formula holds for negative exponents as well (of course, this requires working in the formal power series ring  $\mathbb{Z}[[T]]$  rather than in the polynomial ring  $\mathbb{Z}[T]$ ), but I am not sure whether this argument is free of circular reasoning because it is not at all obvious that  $(1+T)^x (1+T)^y = (1+T)^{x+y}$  in  $\mathbb{Z}[[T]]$  for negative  $x$  and  $y$ , and I even fear that this is usually proven using (7).

### 3.2. Adjoining a polynomial variable to a $\lambda$ -ring

Binomial  $\lambda$ -rings are not the main examples of  $\lambda$ -rings. We will see an important example of  $\lambda$ -rings in Theorem 5.1 and Exercise 6.1. Another simple way to construct new examples from known ones is the following one:

**Definition.** Let  $K$  be a ring. Let  $L$  be a  $K$ -algebra. Consider the ring  $K[[T]]$  of formal power series in the indeterminate  $T$  over the ring  $K$ , and the ring  $L[[T]]$  of formal power series in the indeterminate  $T$  over the ring  $L$ . For every  $\mu \in L$ , we can define a  $K$ -algebra homomorphism  $\text{ev}_{\mu T} : K[[T]] \rightarrow L[[T]]$  by setting  $\text{ev}_{\mu T} \left( \sum_{i \in \mathbb{N}} a_i T^i \right) = \sum_{i \in \mathbb{N}} a_i \mu^i T^i$  for every power series  $\sum_{i \in \mathbb{N}} a_i T^i \in K[[T]]$  (which satisfies  $a_i \in K$  for every  $i \in \mathbb{N}$ ). (In other words,  $\text{ev}_{\mu T}$  is the map that takes any power series in  $T$  and replaces every  $T$  in this power series by  $\mu T$ .)

**Theorem 3.3.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Consider the polynomial ring  $K[S]$ . For every  $i \in \mathbb{N}$ , define a map  $\bar{\lambda}^i : K[S] \rightarrow K[S]$  as follows: For every  $\sum_{j \in \mathbb{N}} a_j S^j \in K[S]$  (with  $a_j \in K$  for every  $j \in \mathbb{N}$ ), let  $\bar{\lambda}^i \left( \sum_{j \in \mathbb{N}} a_j S^j \right)$  be the coefficient of the power series  $\prod_{j \in \mathbb{N}} \lambda_{S^j T}(a_j) \in (K[S])[[T]]$  before  $T^i$ , where the power series  $\lambda_{S^j T}(a_j) \in (K[S])[[T]]$  is defined as  $\text{ev}_{S^j T}(\lambda_T(a_j))$ .

(a) Then,  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. The ring  $K$  is a sub- $\lambda$ -ring of  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$ .

(b) For every  $a \in K$  and  $\alpha \in \mathbb{N}$ , we have  $\bar{\lambda}^i(aS^\alpha) = \lambda^i(a)S^{\alpha i}$  for every  $i \in \mathbb{N}$ .

*Proof of Theorem 3.3.* For every  $x \in K$ , we have

$$\begin{aligned}
 \lambda_{S^j T}(x) &= \sum_{i \in \mathbb{N}} \lambda^i(x) (S^j T)^i && \left( \text{since } \lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \right) \\
 &= \underbrace{\lambda^0(x)}_{=1} \underbrace{(S^j T)^0}_{=1} + \underbrace{\lambda^1(x)}_{=x} \underbrace{(S^j T)^1}_{=S^j T} + \sum_{i \geq 2} \lambda^i(x) \underbrace{(S^j T)^i}_{=S^{ji} T^i} \\
 &= 1 + xS^j T + \underbrace{\sum_{i \geq 2} \lambda^i(x) S^{ji} T^i}_{\substack{= (\text{sum of terms divisible by } T^2) \\ (\text{since } T^2 | T^i \text{ for every } i \geq 2)}} \\
 &= 1 + xS^j T + (\text{sum of terms divisible by } T^2). \tag{8}
 \end{aligned}$$

(a) Define a map  $\bar{\lambda}_T : K[S] \rightarrow (K[S])[[T]]$  by

$$\bar{\lambda}_T(u) = \sum_{i \in \mathbb{N}} \bar{\lambda}^i(u) T^i \quad \text{for every } u \in K[S]. \tag{9}$$

Then, according to the definition of the maps  $\bar{\lambda}^i$ , we have

$$\bar{\lambda}_T \left( \sum_{j \in \mathbb{N}} a_j S^j \right) = \prod_{j \in \mathbb{N}} \lambda_{S^j T}(a_j) \in (K[S])[[T]] \quad (10)$$

for every  $\sum_{j \in \mathbb{N}} a_j S^j \in K[S]$  (with  $a_j \in K$  for every  $j \in \mathbb{N}$ ). Hence, for every  $u \in K[S]$ , we have

$$\sum_{i \in \mathbb{N}} \bar{\lambda}^i(u) T^i = 1 + uT + (\text{sum of terms divisible by } T^2) \quad (11)$$

in  $(K[S])[[T]]$ <sup>12</sup>. Hence, for every  $u \in K[S]$ , we have  $\bar{\lambda}^0(u) = 1$  (this is obtained by comparing coefficients before  $T^0$  in the equality (11)) and  $\bar{\lambda}^1(u) = u$  (this is obtained by comparing coefficients before  $T^1$  in the equality (11)). Renaming  $u$  as  $x$  in this sentence, we obtain the following: For every  $x \in K[S]$ , we have  $\bar{\lambda}^0(x) = 1$  and  $\bar{\lambda}^1(x) = x$ .

Thus, we can apply Theorem 2.1 (a) to  $K[S]$ ,  $(\bar{\lambda}^i)_{i \in \mathbb{N}}$  and  $\bar{\lambda}_T$  instead of  $K$ ,  $\lambda^i$  and  $\lambda_T$ . As a result, we see that

$$\bar{\lambda}_T(x) \cdot \bar{\lambda}_T(y) = \bar{\lambda}_T(x + y) \quad \text{for every } x \in K[S] \text{ and every } y \in K[S] \quad (12)$$

if and only if  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. Therefore, proving that  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring boils down to verifying (12). Let us therefore verify (12):

*Proof of (12):* Let  $x \in K[S]$  and  $y \in K[S]$ . Write  $x$  in the form  $x = \sum_{j \in \mathbb{N}} a_j S^j$  for some family  $(a_j)_{j \in \mathbb{N}} \in K^{\mathbb{N}}$ . Write  $y$  in the form  $y = \sum_{j \in \mathbb{N}} b_j S^j$  for some family  $(b_j)_{j \in \mathbb{N}} \in K^{\mathbb{N}}$ . Adding the equalities  $x = \sum_{j \in \mathbb{N}} a_j S^j$  and  $y = \sum_{j \in \mathbb{N}} b_j S^j$ , we obtain  $x + y = \sum_{j \in \mathbb{N}} a_j S^j + \sum_{j \in \mathbb{N}} b_j S^j = \sum_{j \in \mathbb{N}} (a_j + b_j) S^j$ . Applying the map  $\bar{\lambda}_T$  to both sides of this equality,

<sup>12</sup>*Proof of (11):* Let  $u \in K[S]$ . Write  $u$  in the form  $u = \sum_{j \in \mathbb{N}} a_j S^j$ , where  $a_j \in K$  for every  $j \in \mathbb{N}$ .

Then, (9) yields

$$\begin{aligned} \sum_{i \in \mathbb{N}} \bar{\lambda}^i(u) T^i &= \bar{\lambda}_T \left( \underbrace{\sum_{j \in \mathbb{N}} a_j S^j}_u \right) = \bar{\lambda}_T \left( \sum_{j \in \mathbb{N}} a_j S^j \right) = \prod_{j \in \mathbb{N}} \underbrace{\lambda_{S^j T}(a_j)}_{=1+a_j S^j T + (\text{sum of terms divisible by } T^2)} \\ &= \prod_{j \in \mathbb{N}} (1 + a_j S^j T + (\text{sum of terms divisible by } T^2)) \\ &= 1 + \underbrace{\left( \sum_{j \in \mathbb{N}} a_j S^j \right)}_{=u} T + (\text{sum of terms divisible by } T^2) \\ &= 1 + uT + (\text{sum of terms divisible by } T^2). \end{aligned}$$

This proves (11).



we find

$$\begin{aligned}
\bar{\lambda}_T(x+y) &= \bar{\lambda}_T\left(\sum_{j \in \mathbb{N}} (a_j + b_j) S^j\right) = \prod_{j \in \mathbb{N}} \underbrace{\lambda_{S^j T}(a_j + b_j)}_{\substack{= \lambda_{S^j T}(a_j) \cdot \lambda_{S^j T}(b_j) \\ \text{(since } \lambda_T(a_j + b_j) = \lambda_T(a_j) \cdot \lambda_T(b_j) \\ \text{by Theorem 2.1 (a))}}} \\
&\quad \text{(by (10), applied to } a_j + b_j \text{ instead of } a_j) \\
&= \prod_{j \in \mathbb{N}} \underbrace{\lambda_{S^j T}(a_j)}_{= \bar{\lambda}_T\left(\sum_{j \in \mathbb{N}} a_j S^j\right)} \cdot \prod_{j \in \mathbb{N}} \underbrace{\lambda_{S^j T}(b_j)}_{= \bar{\lambda}_T\left(\sum_{j \in \mathbb{N}} b_j S^j\right)} \\
&\quad \text{(by (10))} \quad \text{(by (10), applied to } b_j \text{ instead of } a_j) \\
&= \bar{\lambda}_T\left(\underbrace{\sum_{j \in \mathbb{N}} a_j S^j}_{=x}\right) \cdot \bar{\lambda}_T\left(\underbrace{\sum_{j \in \mathbb{N}} b_j S^j}_{=y}\right) = \bar{\lambda}_T(x) \cdot \bar{\lambda}_T(y).
\end{aligned}$$

Thus, (12) is proven.

As we said, (12) shows that  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. The rest of Theorem 3.3 (a) is yet easier to verify.

(b) We have  $\bar{\lambda}_T(aS^\alpha) = \lambda_{S^\alpha T}(a)$  as a particular case of (10). The equation  $\bar{\lambda}^i(aS^\alpha) = \lambda^i(a)S^{\alpha i}$  for every  $i \in \mathbb{N}$  follows by comparing coefficients before  $T^i$  in the equality  $\bar{\lambda}_T(aS^\alpha) = \lambda_{S^\alpha T}(a)$ . Thus, Theorem 3.3 (b) is proven.  $\square$

The exercises below give some more examples.

### 3.3. Exercises

*Exercise 3.1.* Let  $p \in \mathbb{N}$  be a prime. Prove that the localization  $\{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  of the ring  $\mathbb{Z}$  at the multiplicative subset  $\{1, p, p^2, \dots\}$  is a binomial ring.

*Exercise 3.2.* Let  $K$  be a ring where none of the elements  $1, 2, 3, \dots$  is a zero-divisor. Let  $E$  be a subset of  $K$  that generates  $K$  as a ring. Assume that  $n! \mid x \cdot (x-1) \cdot \dots \cdot (x-n+1)$  for every  $x \in E$  and every  $n \in \mathbb{N}$ . Prove that  $K$  is a binomial ring.

*Exercise 3.3. (a)* Let  $K$  be a binomial ring. Let  $p \in K[[T]]$  be a formal power series with coefficient 1 before  $T^0$  (we will later denote the set of such power series by  $1 + K[[T]]^+$ ). For every  $i \in \mathbb{N}$ , define a map  $\lambda^i : K \rightarrow K$  as follows: For every  $x \in K$ , let  $\lambda^i(x)$  be the coefficient of the formal power series  $(1 + pT)^x$  (which is defined as  $\sum_{k \in \mathbb{N}} \binom{x}{k} (pT)^k$ <sup>13</sup>) before  $T^i$ . Prove that  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring.

<sup>13</sup>If  $K$  is a  $\mathbb{Q}$ -algebra, then this power series also equals  $\exp(x \log(1 + pT))$ , where  $\log(1 + T)$  is the power series  $\log(1 + T) = \sum_{i \in \mathbb{N} \setminus \{0\}} \frac{(-1)^{i-1}}{i} T^i$ .

(b) If  $p = 1$ , prove that this  $\lambda$ -ring is the one defined in Theorem 3.2.

*Exercise 3.4.* Let  $M$  be a commutative monoid, written multiplicatively (this means, in particular, that we denote the neutral element of  $M$  as 1). Define a  $\mathbb{Z}$ -algebra  $\mathbb{Z}[M]$  as follows:

As a  $\mathbb{Z}$ -module, let  $\mathbb{Z}[M]$  be the free  $\mathbb{Z}$ -module with the basis  $M$ . Let the multiplication on  $\mathbb{Z}[M]$  be the  $\mathbb{Z}$ -linear extension of the multiplication on the monoid  $M$ .

For every  $i \in \mathbb{N}$ , define a map  $\lambda^i : \mathbb{Z}[M] \rightarrow \mathbb{Z}[M]$  as follows: For every  $\sum_{m \in M} \alpha_m m \in \mathbb{Z}[M]$  (with  $\alpha_m \in \mathbb{Z}$  for every  $m \in M$ ), let  $\lambda^i \left( \sum_{m \in M} \alpha_m m \right)$  be the coefficient of the power series  $\prod_{m \in M} (1 + mT)^{\alpha_m} \in (\mathbb{Z}[M])[[T]]$  before  $T^i$ .

Prove that  $(\mathbb{Z}[M], (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring.

*Exercise 3.5. (a)* Let  $M$  be a commutative monoid, written multiplicatively (this means, in particular, that we denote the neutral element of  $M$  as 1). Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring.

Define a  $K$ -algebra  $K[M]$  as follows:

As a  $K$ -module, let  $K[M]$  be the free  $K$ -module with the basis  $M$ . Let the multiplication on  $K[M]$  be the  $K$ -linear extension of the multiplication on the monoid  $M$ .

For every  $i \in \mathbb{N}$ , define a map  $\bar{\lambda}^i : K[M] \rightarrow K[M]$  as follows: For every  $\sum_{m \in M} \alpha_m m \in K[M]$  (with  $\alpha_m \in K$  for every  $m \in M$ ), let  $\bar{\lambda}^i \left( \sum_{m \in M} \alpha_m m \right)$  be the coefficient of the power series  $\prod_{m \in M} \lambda_{mT}(\alpha_m) \in (K[M])[[T]]$  before  $T^i$ , where the power series  $\lambda_{mT}(\alpha_m) \in (K[M])[[T]]$  is defined as  $\text{ev}_{mT}(\lambda_T(\alpha_m))$ .

Prove that  $(K[M], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. The ring  $K$  is a sub- $\lambda$ -ring of  $(K[M], (\bar{\lambda}^i)_{i \in \mathbb{N}})$ . For every  $a \in K$  and  $m \in M$ , we have  $\bar{\lambda}^i(am) = \lambda^i(a) m^i$  for every  $i \in \mathbb{N}$ .

(b) Show that Exercise 3.4 is a particular case of (a) for  $K = \mathbb{Z}$ , and that Theorem 3.3 is a particular case of (a) for  $M \cong \mathbb{N}$  (where  $\mathbb{N}$  denotes the *additive* monoid  $\mathbb{N}$ ).

## 4. Intermezzo: Symmetric polynomials

Our next plan is to introduce a rather general example of  $\lambda$ -rings that we will use as a prototype to the notion of *special  $\lambda$ -rings*. Before we do this, we need some rather clumsy theory of symmetric polynomials. In case you can take the proofs for granted, you don't need to read much of this paragraph - you only need to know Theorems 4.3 and 4.4 and the preceding definitions (only the goals of the definitions; not the actual constructions of the polynomials  $P_k$  and  $P_{k,j}$ ).

## 4.1. Symmetric polynomials are generated by the elementary symmetric ones

**Theorem 4.1 (characterization of symmetric polynomials).** Let  $K$  be a ring. Let  $m \in \mathbb{N}$ . Consider the ring  $K[U_1, U_2, \dots, U_m]$  (the polynomial ring in  $m$  indeterminates  $U_1, U_2, \dots, U_m$  over the ring  $K$ ). For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the so-called  *$i$ -th elementary symmetric polynomial* in the variables  $U_1, U_2, \dots, U_m$ . (In particular,  $X_0 = 1$  and  $X_i = 0$  for every  $i > m$ .)

A polynomial  $P \in K[U_1, U_2, \dots, U_m]$  is called *symmetric* if it satisfies  $P(U_1, U_2, \dots, U_m) = P(U_{\pi(1)}, U_{\pi(2)}, \dots, U_{\pi(m)})$  for every permutation  $\pi$  of the set  $\{1, 2, \dots, m\}$ .

(a) Let  $P \in K[U_1, U_2, \dots, U_m]$  be a symmetric polynomial. Then, there exists one and only one polynomial  $Q \in \underbrace{K[\alpha_1, \alpha_2, \dots, \alpha_m]}_{\text{polynomial ring}}$  such that  $P(U_1, U_2, \dots, U_m) =$

$$Q(X_1, X_2, \dots, X_m). \quad {}^{14}$$

(b) Let  $\ell \in \mathbb{N}$ . Assume, moreover, that  $P \in K[U_1, U_2, \dots, U_m]$  is a symmetric polynomial of total degree  $\leq \ell$  in the variables  $U_1, U_2, \dots, U_m$ . Consider the unique polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  from Theorem 4.1 (a). Then, the variables  $\alpha_i$  for  $i > \ell$  do not appear in the polynomial  $Q$ .

There is a canonical homomorphism  $K[\alpha_1, \alpha_2, \dots, \alpha_m] \rightarrow K[\alpha_1, \alpha_2, \dots, \alpha_\ell]$  (which maps every  $\alpha_i$  to  $\begin{cases} \alpha_i, & \text{if } i \leq \ell; \\ 0, & \text{if } i > \ell \end{cases}$ )<sup>15</sup>. If we denote by  $Q_\ell$  the image of  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  under this homomorphism, then,  $P(U_1, U_2, \dots, U_m) = Q(X_1, X_2, \dots, X_m) = Q_\ell(X_1, X_2, \dots, X_\ell)$ .

We are not going to prove Theorem 4.1 here, since it is a fairly well-known fact<sup>16</sup>. But we are going to extend it to two sets of indeterminates:

<sup>14</sup>In other words, the  $K$ -subalgebra

$$\{P \in K[U_1, U_2, \dots, U_m] \mid P \text{ is symmetric}\}$$

of the polynomial ring  $K[U_1, U_2, \dots, U_m]$  is generated by the elements  $X_1, X_2, \dots, X_m$ . Moreover, these elements  $X_1, X_2, \dots, X_m$  are algebraically independent; in other words, the  $K$ -algebra homomorphism

$$\underbrace{K[\alpha_1, \alpha_2, \dots, \alpha_m]}_{\text{polynomial ring}} \rightarrow \{P \in K[U_1, U_2, \dots, U_m] \mid P \text{ is symmetric}\}$$

which maps every  $\alpha_i$  to  $X_i$  is injective. Hence, this homomorphism is an isomorphism.

<sup>15</sup>This homomorphism is a surjection if  $\ell \leq m$  and an injection if  $\ell \geq m$ .

<sup>16</sup>Proofs of Theorem 4.1 (a) can be found in [BluCos16, proof of Theorem 1], in [Dumas08, Theorem 1.2.1], in [MiRiRu88, Chapter II, Theorem 8.1], in [Neusel07, Remark 4.16], in [Smith95, §1.1] or in [CoLiOS15, Chapter 7, §1, proof of Theorem 3]. (Some of these sources only state the result in the case when  $K$  is a field, or when  $K = \mathbb{C}$ ; but the same proof applies more generally for any ring  $K$ .) Various other sources give proofs of Theorem 4.1 (a) under the condition that  $K$  is a field (or that  $K = \mathbb{C}$ ), but they can easily be modified so that they become complete proofs of Theorem 4.1 (a) for any commutative ring  $K$ . (For instance, in order to make a complete proof of Theorem 4.1 (a) out of [DraGij09, proof of Theorem 2.1.1], it suffices to replace every occurrence of  $\mathbb{C}$  by  $K$ , and to add the extra condition “the leading monomial of  $f$  has coefficient 1 in  $f$ ” to [DraGij09,

Let us state one piece of Theorem 4.1 **(a)** separately, to facilitate its later use:

**Corollary 4.1a.** Let  $K$  be a ring. Let  $m \in \mathbb{N}$ . Consider the ring  $K[U_1, U_2, \dots, U_m]$  (the polynomial ring in  $m$  indeterminates  $U_1, U_2, \dots, U_m$  over the ring  $K$ ). For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the so-

Exercise 2.1.2].) Also, various textbooks make claims which are easily seen to be equivalent to Theorem 4.1 **(a)** (for example, [Newman12, Theorems 3.4 and 3.5]). Note that I am not saying that all these proofs are distinct; in fact, many of them are essentially identical (although written up in slightly different fashions and with varying levels of detail and constructiveness). Beware of texts that use Galois theory to prove Theorem 4.1 **(a)** in the case when  $K$  is a field; such proofs usually don't generalize to the case when  $K$  is an arbitrary commutative ring (although they, too, can be salvaged with a bit of work: it is not too hard to derive the general case from the case when  $K$  is a field).

Various sources prove a result that is easily seen to be equivalent to Theorem 4.1 **(a)**. Namely, they prove the following result:

**Theorem 4.1'.** Let  $K, m, (U_1, U_2, \dots, U_m)$  and  $X_i$  be as in Theorem 4.1. Let  $\mathcal{S}$  be the  $K$ -module consisting of all symmetric polynomials  $P \in K[U_1, U_2, \dots, U_m]$ . Then, the family  $(X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m})_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m}$  is a basis of the  $K$ -module  $\mathcal{S}$ .

For example, Theorem 4.1' is [LLPT95, (5.10) in Chapter SYM].

Let us briefly explain how Theorem 4.1 **(a)** follows from Theorem 4.1':

[Proof of Theorem 4.1 **(a)** using Theorem 4.1': A family  $(k_g)_{g \in G} \in K^G$  of elements of  $K$  (where  $G$  is an arbitrary set) is said to be *finitely supported* if all but finitely many  $g \in G$  satisfy  $k_g = 0$ .

Notice that the finitely supported families  $(k_{(i_1, i_2, \dots, i_m)})_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \in K^{\mathbb{N}^m}$  of elements of  $K$  are in bijection with the polynomials in the polynomial ring  $K[\alpha_1, \alpha_2, \dots, \alpha_m]$ . Indeed, the bijection maps each finitely supported family  $(k_{(i_1, i_2, \dots, i_m)})_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m}$  to the polynomial

$$\sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} k_{(i_1, i_2, \dots, i_m)} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_m^{i_m}.$$

We know that  $P$  is a symmetric polynomial in  $K[U_1, U_2, \dots, U_m]$ . In other words,  $P \in \mathcal{S}$  (by the definition of  $\mathcal{S}$ ).

But Theorem 4.1' shows that the family  $(X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m})_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m}$  is a basis of the  $K$ -module  $\mathcal{S}$ . Hence,  $P$  can be uniquely written as a  $K$ -linear combination of the elements of the family  $(X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m})_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m}$  (since  $P \in \mathcal{S}$ ). In other words, there is a unique finitely supported family  $(k_{(i_1, i_2, \dots, i_m)})_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \in K^{\mathbb{N}^m}$  of elements of  $K$  satisfying  $P =$

$$\sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} k_{(i_1, i_2, \dots, i_m)} X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m}.$$

In other words, there is a unique polynomial  $\sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} k_{(i_1, i_2, \dots, i_m)} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_m^{i_m} \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  satisfying  $P = \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} k_{(i_1, i_2, \dots, i_m)} X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m}$  (because the finitely supported families  $(k_{(i_1, i_2, \dots, i_m)})_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \in K^{\mathbb{N}^m}$  of elements of  $K$  are in bijection with the polynomials in  $K[\alpha_1, \alpha_2, \dots, \alpha_m]$ ).

Renaming the polynomial  $\sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} k_{(i_1, i_2, \dots, i_m)} \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_m^{i_m}$  as  $Q$  in this statement, we obtain the following: There is a unique polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  satisfying  $P = Q(X_1, X_2, \dots, X_m)$ . In other words, there is a unique polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  satisfying  $P(U_1, U_2, \dots, U_m) = Q(X_1, X_2, \dots, X_m)$  (since  $P(U_1, U_2, \dots, U_m) = P$ ). This proves Theorem 4.1 **(a)**.]

The first claim of Theorem 4.1 **(b)** (namely, that the variables  $\alpha_i$  for  $i > \ell$  do not appear in the polynomial  $Q$ ) can easily be obtained from the proof of Theorem 4.1 **(a)**: In fact, each of the above-mentioned proofs of Theorem 4.1 **(a)** provides an actual algorithm to find the polynomial  $Q$ , and this algorithm does not ever increase the total degree of  $P$  in the process. Thus, the first

called *i*-th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$ . (In particular,  $X_0 = 1$  and  $X_i = 0$  for every  $i > m$ .)

Then, the elements  $X_1, X_2, \dots, X_m$  of  $K[U_1, U_2, \dots, U_m]$  are algebraically independent (over  $K$ ).

## 4.2. UV-symmetric polynomials are generated by the elementary symmetric ones

**Theorem 4.2 (characterization of UV-symmetric polynomials).**

Let  $K$  be a ring. Let  $m \in \mathbb{N}$  and  $n \in \mathbb{N}$ . Consider the ring  $K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  (the polynomial ring in  $m + n$  indeterminates  $U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n$  over the ring  $K$ ). For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the

*i*-th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$ . For every  $j \in \mathbb{N}$ , let  $Y_j = \sum_{\substack{S \subseteq \{1, 2, \dots, n\}; \\ |S|=j}} \prod_{k \in S} V_k$  be the *j*-th elementary symmetric

polynomial in the variables  $V_1, V_2, \dots, V_n$ .

A polynomial  $P \in K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  is called *UV-symmetric* if it satisfies

$$P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) = P(U_{\pi(1)}, U_{\pi(2)}, \dots, U_{\pi(m)}, V_{\sigma(1)}, V_{\sigma(2)}, \dots, V_{\sigma(n)})$$

for every permutation  $\pi$  of the set  $\{1, 2, \dots, m\}$  and every permutation  $\sigma$  of the set  $\{1, 2, \dots, n\}$ .

**(a)** Let  $P \in K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  be a UV-symmetric polynomial.

Then, there exists one and only one polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  such that  $P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) = Q(X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n)$ .

17

claim of Theorem 4.1 **(b)** follows. The second claim of Theorem 4.1 **(b)** follows from the first (indeed, we have  $Q(X_1, X_2, \dots, X_m) = Q_\ell(X_1, X_2, \dots, X_\ell)$ , because the variables  $\alpha_i$  for  $i > \ell$  do not appear in the polynomial  $Q$ ).

[*Remark:* Theorem 4.1 **(b)** can be strengthened: Namely, we can replace the assumption that  $P$  has total degree  $\leq \ell$  by the (weaker) assumption that  $P$  is a  $K$ -linear combination of monomials of the form  $U_1^{a_1} U_2^{a_2} \cdots U_m^{a_m}$  where each  $a_i$  is  $\leq \ell$ . This stronger version, again, can be easily derived from the classical proofs of Theorem 4.1 **(a)**.]

<sup>17</sup>In other words, the  $K$ -subalgebra

$$\{P \in K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n] \mid P \text{ is UV-symmetric}\}$$

of the polynomial ring  $K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  is generated by the elements  $X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n$ . Moreover, these elements  $X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n$  are algebraically independent; in other words, the  $K$ -algebra homomorphism

$$\underbrace{K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]}_{\text{polynomial ring}} \rightarrow \{P \in K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n] \mid P \text{ is UV-symmetric}\}$$

which maps every  $\alpha_i$  to  $X_i$  and every  $\beta_j$  to  $Y_j$  is injective. Hence, this homomorphism is an isomorphism.

(b) Let  $\ell \in \mathbb{N}$  and  $k \in \mathbb{N}$ . Assume, moreover, that  $P \in K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  is a UV-symmetric polynomial of total degree  $\leq \ell$  in the variables  $U_1, U_2, \dots, U_m$  and of total degree  $\leq k$  in the variables  $V_1, V_2, \dots, V_n$ . Consider the unique polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  from Theorem 4.2 (a). Then, neither the variables  $\alpha_i$  for  $i > \ell$  nor the variables  $\beta_j$  for  $j > k$  ever appear in the polynomial  $Q$ .

There is a canonical homomorphism

$$K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n] \rightarrow K[\alpha_1, \alpha_2, \dots, \alpha_\ell, \beta_1, \beta_2, \dots, \beta_k]$$

(which maps every  $\alpha_i$  to  $\begin{cases} \alpha_i, & \text{if } i \leq \ell; \\ 0, & \text{if } i > \ell \end{cases}$  and every  $\beta_j$  to  $\begin{cases} \beta_j, & \text{if } j \leq k; \\ 0, & \text{if } j > k \end{cases}$ ).

If we denote by  $Q_{\ell,k}$  the image of  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  under this homomorphism, then

$$P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) = Q_{\ell,k}(X_1, X_2, \dots, X_\ell, Y_1, Y_2, \dots, Y_k).$$

*Proof of Theorem 4.2. (a)* Consider  $P$  as a polynomial in the indeterminates  $V_1, V_2, \dots, V_n$  over the ring  $K[U_1, U_2, \dots, U_m]$ . Then,  $P$  is a symmetric polynomial in these indeterminates  $V_1, V_2, \dots, V_n$  (since  $P$  is UV-symmetric), so Theorem 4.1 (a) (applied to  $n, K[U_1, U_2, \dots, U_m], (V_1, V_2, \dots, V_n), Y_i, (\beta_1, \beta_2, \dots, \beta_n)$  and  $\widehat{Q}$  instead of  $m, K, (U_1, U_2, \dots, U_m), X_i, (\alpha_1, \alpha_2, \dots, \alpha_m)$  and  $Q$ ) yields the existence of one and only one polynomial  $\widehat{Q} \in \underbrace{(K[U_1, U_2, \dots, U_m])}_{\text{polynomial ring}}[\beta_1, \beta_2, \dots, \beta_n]$  such that  $P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) =$

$\widehat{Q}(Y_1, Y_2, \dots, Y_n)$ . Consider this  $\widehat{Q}$ .

For every  $n$ -tuple  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$ , let  $Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} \in K[U_1, U_2, \dots, U_m]$  be the coefficient of this polynomial  $\widehat{Q}$  before  $\beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}$ . Thus,

$$\widehat{Q} = \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}. \quad (13)$$

Now,

$$\begin{aligned} P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) \\ = \widehat{Q}(Y_1, Y_2, \dots, Y_n) = \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} Y_1^{\lambda_1} Y_2^{\lambda_2} \dots Y_n^{\lambda_n} \end{aligned} \quad (14)$$

(this follows by evaluating both sides of (13) at  $(\beta_1, \beta_2, \dots, \beta_n) = (Y_1, Y_2, \dots, Y_n)$ ).

Now, for every  $n$ -tuple  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$ , the polynomial  $Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}$  is a symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$ <sup>18</sup>. Hence, by Theorem 4.1

<sup>18</sup>*Proof.* Let  $\sigma \in S_m$ . If we substitute  $U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}, V_1, V_2, \dots, V_n$  for  $U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n$  on both sides of the equality (14), then we obtain

$$\begin{aligned} P(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}, V_1, V_2, \dots, V_n) \\ = \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}) Y_1^{\lambda_1} Y_2^{\lambda_2} \dots Y_n^{\lambda_n} \end{aligned}$$

(indeed, the polynomials  $Y_1, Y_2, \dots, Y_n$  stay the same under this substitution, since they are built

(a) (applied to  $Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}$  instead of  $P$ ), there exists one and only one polynomial  $R_{(\lambda_1, \lambda_2, \dots, \lambda_n)} \in \underbrace{K[\alpha_1, \alpha_2, \dots, \alpha_m]}_{\text{polynomial ring}}$  such that

$$Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(X_1, X_2, \dots, X_m).$$

Consider this  $R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}$ . Now, (14) becomes

$$\begin{aligned} & P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) \\ &= \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} \underbrace{Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}}_{=R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(X_1, X_2, \dots, X_m)} Y_1^{\lambda_1} Y_2^{\lambda_2} \dots Y_n^{\lambda_n} \\ &= \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(X_1, X_2, \dots, X_m) Y_1^{\lambda_1} Y_2^{\lambda_2} \dots Y_n^{\lambda_n}. \end{aligned}$$

Thus, the polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  defined by

$$Q = \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(\alpha_1, \alpha_2, \dots, \alpha_m) \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n} \quad (17)$$

satisfies  $P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) = Q(X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n)$ . It only remains to prove that this is the only such polynomial. This amounts to showing that  $X_1,$

---

of the variables  $V_1, V_2, \dots, V_n$ . Hence,

$$\begin{aligned} & \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}) Y_1^{\lambda_1} Y_2^{\lambda_2} \dots Y_n^{\lambda_n} \\ &= P(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}, V_1, V_2, \dots, V_n) \\ &= P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) \quad (\text{since } P \text{ is UV-symmetric}) \\ &= \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} Y_1^{\lambda_1} Y_2^{\lambda_2} \dots Y_n^{\lambda_n} \quad (\text{by (14)}). \end{aligned}$$

Subtracting the right hand side of this equation from the left, we obtain

$$\begin{aligned} & \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} (Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}) - Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}) Y_1^{\lambda_1} Y_2^{\lambda_2} \dots Y_n^{\lambda_n} \\ &= 0. \end{aligned} \quad (15)$$

But  $Y_1, Y_2, \dots, Y_n$  are algebraically independent over  $K[U_1, U_2, \dots, U_m]$  (as we can see by applying Corollary 4.1a to  $n, K[U_1, U_2, \dots, U_m], (V_1, V_2, \dots, V_n)$  and  $Y_i$  instead of  $m, K, (U_1, U_2, \dots, U_m)$  and  $X_i$ ). Hence, (15) entails that

$$Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}) - Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = 0$$

for every  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$ . In other words,

$$Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)}) = Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} \quad (16)$$

for every  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$ .

Now, forget that we fixed  $\sigma$ . We thus have shown that (16) holds for every  $\sigma \in S_m$  and every  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$ .

Now, fix  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$ . As we know, (16) holds for every  $\sigma \in S_m$ . Hence,

$$Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(U_1, U_2, \dots, U_m) = Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(U_{\sigma(1)}, U_{\sigma(2)}, \dots, U_{\sigma(m)})$$

(by (16)) holds for every  $\sigma \in S_m$ . In other words, the polynomial  $Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}$  is symmetric. Qed.

$X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n$  are algebraically independent over  $K$ . But this is clear (from Exercise 4.3, applied to  $S = K[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$ ,  $T = K[U_1, U_2, \dots, U_m]$ ,  $p_i = X_i$  and  $q_j = Y_j$ ), since  $X_1, X_2, \dots, X_m$  are algebraically independent over  $K$  (by Corollary 4.1a) and since  $Y_1, Y_2, \dots, Y_n$  are algebraically independent over  $K[U_1, U_2, \dots, U_m]$  (by Corollary 4.1a, applied to  $n, K[U_1, U_2, \dots, U_m], (V_1, V_2, \dots, V_n)$  and  $Y_i$  instead of  $m, K, (U_1, U_2, \dots, U_m)$  and  $X_i$ ).

**(b)** Consider the polynomials  $\widehat{Q}, Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}, R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}$  and  $Q$  defined in our proof of Theorem 4.2 **(a)**.

The first claim of Theorem 4.1 **(b)** (applied to  $n, K[U_1, U_2, \dots, U_m], (V_1, V_2, \dots, V_n), Y_i, (\beta_1, \beta_2, \dots, \beta_n), \widehat{Q}$  and  $k$  instead of  $m, K, (U_1, U_2, \dots, U_m), X_i, (\alpha_1, \alpha_2, \dots, \alpha_m), Q$  and  $\ell$ ) yields that the variables  $\beta_j$  for  $j > k$  do not appear in the polynomial  $\widehat{Q}$ . Hence, the coefficient of the polynomial  $\widehat{Q}$  before any monomial  $\beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}$  is 0 unless this monomial satisfies  $\lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0$ . Since this coefficient has been denoted by  $Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)}$ , we can rewrite this as follows: We have

$$Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = 0 \tag{18}$$

for every  $n$ -tuple  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$  that fails to satisfy  $\lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0$ . From this, we obtain

$$R_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = 0 \tag{19}$$

for every  $n$ -tuple  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$  that fails to satisfy  $\lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0$ .

Consider the polynomial ring  $K[\alpha_1, \alpha_2, \alpha_3, \dots, \beta_1, \beta_2, \beta_3, \dots]$  in the infinitely many variables  $\alpha_i$  (for  $i \in \{1, 2, 3, \dots\}$ ) and  $\beta_j$  (for  $j \in \{1, 2, 3, \dots\}$ ). For any  $u \in \mathbb{N}$  and  $v \in \mathbb{N}$ , we shall consider the polynomial ring  $K[\alpha_1, \alpha_2, \dots, \alpha_u, \beta_1, \beta_2, \dots, \beta_v]$  as a subring of  $K[\alpha_1, \alpha_2, \alpha_3, \dots, \beta_1, \beta_2, \beta_3, \dots]$  (by abuse of notation).

---

<sup>19</sup>*Proof.* Fix some  $(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n$  that fails to satisfy  $\lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0$ . We must show that  $R_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = 0$ .

Recall that  $Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(X_1, X_2, \dots, X_m)$ . Hence,  $R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(X_1, X_2, \dots, X_m) = Q_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = 0$  (by (18)). Since  $X_1, X_2, \dots, X_m$  are algebraically independent over  $K$  (by Corollary 4.1a), this entails that  $R_{(\lambda_1, \lambda_2, \dots, \lambda_n)} = 0$ . This proves (19).



Now, recall how  $Q$  has been defined in (17). Thus,<sup>20</sup>

$$\begin{aligned}
Q &= \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(\alpha_1, \alpha_2, \dots, \alpha_m) \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n} \\
&= \sum_{\substack{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n; \\ \lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0}} R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(\alpha_1, \alpha_2, \dots, \alpha_m) \underbrace{\beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}}_{= \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_k^{\lambda_k}} \\
&\quad \text{(since } \lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0\text{)} \\
&\quad + \sum_{\substack{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n; \\ \text{not } \lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0}} \underbrace{R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(\alpha_1, \alpha_2, \dots, \alpha_m)}_{=0} \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n} \\
&\quad \text{(by (19))} \\
&= \underbrace{\sum_{\substack{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n; \\ \lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0}} R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(\alpha_1, \alpha_2, \dots, \alpha_m) \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_k^{\lambda_k}}_{\in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_k]} \\
&\quad + \underbrace{\sum_{\substack{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n; \\ \text{not } \lambda_{k+1} = \lambda_{k+2} = \dots = \lambda_n = 0}} 0 \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}}_{=0} \\
&\in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_k].
\end{aligned}$$

Hence, the variables  $\beta_j$  for  $j > k$  do not appear in the polynomial  $Q$ . A similar argument (but in which the roles of  $m$ , of  $U_i$ , of  $X_i$ , of  $\alpha_i$  and of  $\ell$  are switched with the roles of  $n$ , of  $V_i$ , of  $Y_i$ , of  $\beta_i$  and of  $k$ ) shows that the variables  $\alpha_i$  for  $i > \ell$  do not appear in the polynomial  $Q$ . Thus, we know that neither the variables  $\alpha_i$  for  $i > \ell$  nor the variables  $\beta_j$  for  $j > k$  ever appear in the polynomial  $Q$ . Therefore, the variables which do appear in the polynomial  $Q$  remain unchanged under the homomorphism which sends  $Q$  to  $Q_{\ell, k}$ . Therefore,  $Q_{\ell, k} = Q$ . Therefore,

$$Q_{\ell, k}(X_1, X_2, \dots, X_\ell, Y_1, Y_2, \dots, Y_k) = Q(X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n).$$

Hence,

$$\begin{aligned}
P(U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n) &= Q(X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n) \\
&= Q_{\ell, k}(X_1, X_2, \dots, X_\ell, Y_1, Y_2, \dots, Y_k).
\end{aligned}$$

This completes the proof of Theorem 4.2 (b).  $\square$

Note that in the following, we are going to use Theorems 4.1 and 4.2 for  $K = \mathbb{Z}$  only, until Section 10 where we actually get to use them for general  $K$ .

### 4.3. Grothendieck's polynomials $P_k$

Theorem 4.2 allows us to make the following definition:

<sup>20</sup>In the following computation, we are WLOG assuming that  $k \leq n$ . Indeed, this assumption is legitimate, because in the case when  $k > n$ , the result of the computation (namely, the claim that  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_k]$ ) is obvious anyway.

**Definition.** Let  $k \in \mathbb{N}$ . Our goal now is to define a polynomial  $P_k \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_k]$  such that

$$\sum_{\substack{S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = P_k(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) \quad (20)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  for every  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ , where  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  is the  $i$ -th elementary symmetric

polynomial in the variables  $U_1, U_2, \dots, U_m$  for every  $i \in \mathbb{N}$ , and  $Y_j = \sum_{\substack{S \subseteq \{1, 2, \dots, n\}; \\ |S|=j}} \prod_{k \in S} V_k$  is the  $j$ -th elementary symmetric polynomial in the variables  $V_1, V_2, \dots, V_n$  for every  $j \in \mathbb{N}$ .

In order to do this, we first fix some  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ . The polynomial

$$\sum_{\substack{S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j \in \mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$$

is UV-symmetric. Thus, Theorem 4.2 (a) yields that there exists one and only one polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  such that

$$\sum_{\substack{S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = Q(X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n)$$

in  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$ . Since the polynomial  $\sum_{\substack{S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j$

has total degree  $\leq k$  in the variables  $U_1, U_2, \dots, U_m$  and of total degree  $\leq k$  in the variables  $V_1, V_2, \dots, V_n$ , Theorem 4.2 (b) yields that

$$\sum_{\substack{S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = Q_{k,k}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k),$$

where  $Q_{k,k}$  is the image of the polynomial  $Q$  under the canonical homomorphism  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n] \rightarrow \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_k]$ . However, this polynomial  $Q_{k,k}$  is not independent of  $n$  and  $m$  yet (as the polynomial  $P_k$  that we intend to construct should be), so we call it  $Q_{k,k,[n,m]}$  rather than just  $Q_{k,k}$ .

Now we forget that we fixed  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ . We have learnt that

$$\sum_{\substack{S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = Q_{k,k,[n,m]}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  for every  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ . Now, define a polynomial  $P_k \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_k]$  by  $P_k = Q_{k,k,[k,k]}$ .

**Theorem 4.3. (a)** The polynomial  $P_k$  just defined satisfies the equation (20) in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  for every  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ . (Hence, the goal mentioned above in the definition is actually achieved.)

**(b)** For every  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ , we have

$$\prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + U_i V_j T) = \sum_{k \in \mathbb{N}} P_k(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) T^k \quad (21)$$

in the ring  $(\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n])[[T]]$ . (Note that the right hand side of this equation is a power series with coefficient 1 before  $T^0$ , since  $P_0 = 1$ .)

*Proof of Theorem 4.3. (a) 1st Step:* Fix  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$  such that  $n \geq k$  and  $m \geq k$ . Then, we claim that  $Q_{k,k,[n,m]} = P_k$ .

*Proof.* The definition of  $Q_{k,k,[n,m]}$  yields

$$\sum_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = Q_{k,k,[n,m]}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$ . Applying the canonical ring epimorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n] \rightarrow \mathbb{Z}[U_1, U_2, \dots, U_k, V_1, V_2, \dots, V_k]$  (which maps every  $U_i$  to  $\begin{cases} U_i, & \text{if } i \leq k; \\ 0, & \text{if } i > k \end{cases}$  and every  $V_j$  to  $\begin{cases} V_j, & \text{if } j \leq k; \\ 0, & \text{if } j > k \end{cases}$ ) to this equation (and noticing that this epimorphism maps every  $X_i$  with  $i \geq 1$  to the corresponding  $X_i$  of the image ring and every  $Y_j$  with  $j \geq 1$  to the corresponding  $Y_j$  of the image ring!), we obtain

$$\sum_{\substack{S \subseteq \{1,2,\dots,k\} \times \{1,2,\dots,k\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = Q_{k,k,[n,m]}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_k, V_1, V_2, \dots, V_k]$ . On the other hand, the definition of  $Q_{k,k,[k,k]}$  yields

$$\sum_{\substack{S \subseteq \{1,2,\dots,k\} \times \{1,2,\dots,k\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = Q_{k,k,[k,k]}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$$

in the same ring. These two equations yield

$$Q_{k,k,[n,m]}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) = Q_{k,k,[k,k]}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k).$$

Since the elements  $X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k$  of  $\mathbb{Z}[U_1, U_2, \dots, U_k, V_1, V_2, \dots, V_k]$  are algebraically independent (by Theorem 4.2 (a)), this yields  $Q_{k,k,[n,m]} = Q_{k,k,[k,k]}$ . In other words,  $Q_{k,k,[n,m]} = P_k$ , and the 1st Step is proven.

*2nd Step:* For every  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ , the equation (20) is satisfied in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$ .

*Proof.* Let  $n' \in \mathbb{N}$  be such that  $n' \geq n$  and  $n' \geq k$  (such an  $n'$  clearly exists). Let  $m' \in \mathbb{N}$  be such that  $m' \geq m$  and  $m' \geq k$  (such an  $m'$  clearly exists). Then, the 1st Step (applied to  $n'$  and  $m'$  instead of  $n$  and  $m$ ) yields that  $Q_{k,k,[n',m']} = P_k$ .

The definition of  $Q_{k,k,[n',m']}$  yields

$$\sum_{\substack{S \subseteq \{1,2,\dots,m'\} \times \{1,2,\dots,n'\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j = Q_{k,k,[n',m']} (X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_{m'}, V_1, V_2, \dots, V_{n'}]$ . Applying the canonical ring epimorphism  $\mathbb{Z}[U_1, U_2, \dots, U_{m'}, V_1, V_2, \dots, V_{n'}] \rightarrow \mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  (which maps every  $U_i$  to  $\begin{cases} U_i, & \text{if } i \leq m; \\ 0, & \text{if } i > m \end{cases}$  and every  $V_j$  to  $\begin{cases} V_j, & \text{if } j \leq n; \\ 0, & \text{if } j > n \end{cases}$ ) to this equation (and noticing that this epimorphism maps every  $X_i$  with  $i \geq 1$  to the corresponding  $X_i$  of the image ring and every  $Y_j$  with  $j \geq 1$  to the corresponding  $Y_j$  of the image ring!), we obtain

$$\begin{aligned} \sum_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j &= \underbrace{Q_{k,k,[n',m']}}_{=P_k} (X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) \\ &= P_k (X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) \end{aligned}$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$ . Hence, the equation (20) is satisfied in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$ . This completes the 2nd Step and proves Theorem 4.3 (a).

(b) We have

$$\begin{aligned} \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + U_i V_j T) &= \sum_{k \in \mathbb{N}} \underbrace{\sum_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j T^k}_{=P_k(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) \text{ (according to (20))}} \\ &\quad \left( \begin{array}{l} \text{by Exercise 4.2 (d), applied to} \\ Q = \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}, \\ A = (\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n])[[T]], \\ t = T \text{ and } \alpha_{(i,j)} = U_i V_j \end{array} \right) \\ &= \sum_{k \in \mathbb{N}} P_k (X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) T^k. \end{aligned}$$

This proves Theorem 4.3 (b).  $\square$

**Example.** The above definition of the polynomials  $P_k$  was rather abstract. Let us sketch an example of how these polynomials are computed - namely, let us compute  $P_2$ .

While our definition of  $P_k$  was somewhat indirect (we constructed  $P_k$  in multiple steps; while each of these steps is constructive, this still is a rather long way to  $P_k$ ), the important thing about  $P_k$  is that it satisfies (20). In fact, for every  $m \geq k$  and

$n \geq k$ , the polynomial  $P_k$  is uniquely determined by the equation (20)<sup>21</sup>, so that we only need (20) to find  $P_k$ .

Since we want to compute  $P_2$ , let us pick  $k = 2$ . Now we need to pick some  $m \geq k$  and  $n \geq k$ ; the best choice is  $m = n = 2$  (choosing greater  $m$  or  $n$  would lead to the same polynomial  $P_k$  in the end, but the computations required to obtain it would involve some longer terms). So let  $m = n = 2$ . Then, the left hand side of (20) is

$$\begin{aligned}
& \sum_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \prod_{(i,j) \in S} U_i V_j \\
&= \sum_{\substack{S \subseteq \{1,2\} \times \{1,2\}; \\ |S|=2}} \prod_{(i,j) \in S} U_i V_j \\
&= \prod_{(i,j) \in \{(1,1), (1,2)\}} U_i V_j + \prod_{(i,j) \in \{(1,1), (2,1)\}} U_i V_j + \prod_{(i,j) \in \{(1,1), (2,2)\}} U_i V_j \\
&\quad + \prod_{(i,j) \in \{(1,2), (2,1)\}} U_i V_j + \prod_{(i,j) \in \{(1,2), (2,2)\}} U_i V_j + \prod_{(i,j) \in \{(2,1), (2,2)\}} U_i V_j \\
&= U_1^2 V_1 V_2 + U_1 U_2 V_1^2 + 2U_1 U_2 V_1 V_2 + U_1 U_2 V_2^2 + U_2^2 V_1 V_2,
\end{aligned}$$

while the right hand side is

$$P_k(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) = P_2(X_1, X_2, Y_1, Y_2).$$

Thus our polynomial  $P_2$  must satisfy

$$U_1^2 V_1 V_2 + U_1 U_2 V_1^2 + 2U_1 U_2 V_1 V_2 + U_1 U_2 V_2^2 + U_2^2 V_1 V_2 = P_2(X_1, X_2, Y_1, Y_2)$$

in  $\mathbb{Z}[U_1, U_2, V_1, V_2]$ . According to Theorem 4.2 (a), the polynomial  $P_2$  is uniquely determined by this condition, but in order to actually compute it, we need to recall how Theorem 4.2 (a) was proven. In other words, we need to recall how to write a UV-symmetric polynomial as a polynomial in the elementary symmetric polynomials  $X_1, X_2, \dots$  and  $Y_1, Y_2, \dots$ .

Let us look what we did in our proof of Theorem 4.2 (a) above, in the particular case of the UV-symmetric polynomial

$$U_1^2 V_1 V_2 + U_1 U_2 V_1^2 + 2U_1 U_2 V_1 V_2 + U_1 U_2 V_2^2 + U_2^2 V_1 V_2.$$

In this case, the proof begins by considering  $U_1^2 V_1 V_2 + 2U_1 U_2 V_1^2 + U_1 U_2 V_1 V_2 + U_1 U_2 V_2^2 + U_2^2 V_1 V_2$  as a polynomial in the indeterminates  $V_1, V_2$  over the ring  $\mathbb{Z}[U_1, U_2]$ . This is a symmetric polynomial in these indeterminates  $V_1, V_2$ . Thus, Theorem 4.1 (a) yields the existence of one and only one polynomial  $\widehat{Q} \in (K[U_1, U_2])[\beta_1, \beta_2]$  such that

$$U_1^2 V_1 V_2 + U_1 U_2 V_1^2 + 2U_1 U_2 V_1 V_2 + U_1 U_2 V_2^2 + U_2^2 V_1 V_2 = \widehat{Q}(Y_1, Y_2).$$

---

<sup>21</sup>*Proof.* Theorem 4.2 (a) yields that the elements  $X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n$  of the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  are algebraically independent. Since  $m \geq k$  and  $n \geq k$ , this yields that the elements  $X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k$  of the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  are algebraically independent. Hence, a polynomial  $\mathbf{p} \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_k, \beta_1, \beta_2, \dots, \beta_k]$  is uniquely determined by the value  $\mathbf{p}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$ . Thus, the polynomial  $P_k$  is uniquely determined by the equation (20) (because the equation (20) determines the value  $P_k(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$ ).

This polynomial  $\widehat{Q}$  can be obtained by any algorithm which writes a symmetric polynomial as a polynomial in the elementary symmetric polynomials; I assume that you know such an algorithm (if not, read it up; most proofs of Theorem 4.1 **(a)** give such an algorithm). Applying this algorithm, we get

$$U_1^2 V_1 V_2 + U_1 U_2 V_1^2 + 2U_1 U_2 V_1 V_2 + U_1 U_2 V_2^2 + U_2^2 V_1 V_2 = (U_1^2 + U_2^2) Y_2 + U_1 U_2 Y_1^2,$$

so that  $\widehat{Q} = (U_1^2 + U_2^2) \beta_2 + U_1 U_2 \beta_1^2$ .

Now, for every 2-tuple  $(\lambda_1, \lambda_2) \in \mathbb{N}^2$ , the coefficient  $Q_{(\lambda_1, \lambda_2)}$  of this polynomial  $\widehat{Q}$  before the monomial  $\beta_1^{\lambda_1} \beta_2^{\lambda_2}$  is a symmetric polynomial in the variables  $U_1, U_2$ . Hence, by Theorem 4.1 **(a)**, there exists a polynomial  $R_{(\lambda_1, \lambda_2)} \in \mathbb{Z}[\alpha_1, \alpha_2]$  such that this coefficient is  $R_{(\lambda_1, \lambda_2)}(X_1, X_2)$ . This  $R_{(\lambda_1, \lambda_2)}$  can generally be computed by any algorithm which writes a symmetric polynomial as a polynomial in the elementary symmetric polynomials. In our case, the polynomial  $\widehat{Q}$  has only two nonzero coefficients: the coefficient  $U_1^2 + U_2^2$  before  $\beta_2$  and the coefficient  $U_1 U_2$  before  $\beta_1^2$ . So we get two polynomials  $R_{(0,1)}$  and  $R_{(2,0)}$ , whereas all the other  $R_{(\lambda_1, \lambda_2)}$  are zero. More concretely, in order to obtain  $R_{(0,1)}$ , we write the symmetric polynomial  $Q_{(0,1)} = U_1^2 + U_2^2$  (which is the coefficient of  $\widehat{Q}$  before  $\beta_1^0 \beta_2^1 = \beta_2$ ) as a polynomial in the elementary symmetric polynomials; this gives us  $U_1^2 + U_2^2 = X_1^2 - 2X_2$ , so that  $R_{(0,1)} = \alpha_1^2 - 2\alpha_2$ . Similarly,  $R_{(2,0)} = \alpha_2$ .

Now, according to the proof of Theorem 4.2 **(a)**, a polynomial  $P_2$  satisfying  $U_1 V_1 + U_1 V_2 + U_2 V_1 + U_2 V_2 = P_2(X_1, X_2, Y_1, Y_2)$  can be defined by the equation

$$P_2 = \sum_{(\lambda_1, \lambda_2, \dots, \lambda_n) \in \mathbb{N}^n} R_{(\lambda_1, \lambda_2, \dots, \lambda_n)}(\alpha_1, \alpha_2, \dots, \alpha_m) \beta_1^{\lambda_1} \beta_2^{\lambda_2} \dots \beta_n^{\lambda_n}.$$

In our case, this simplifies to

$$P_2 = \underbrace{R_{(0,1)}(\alpha_1, \alpha_2)}_{=\alpha_1^2 - 2\alpha_2} \beta_1^0 \beta_2^1 + \underbrace{R_{(2,0)}(\alpha_1, \alpha_2)}_{=\alpha_2} \beta_1^2 \beta_2^0 = (\alpha_1^2 - 2\alpha_2) \beta_2 + \alpha_2 \beta_1^2 = \alpha_1^2 \beta_2 + \alpha_2 \beta_1^2 - 2\alpha_2 \beta_2.$$

So we have found  $P_2$ . Similarly we can compute  $P_k$  for all  $k \in \mathbb{N}$ , even though the computations get longer with increasing  $k$  very rapidly. Here are the values for small  $k$ :

$$P_0 = 1;$$

$$P_1 = \alpha_1 \beta_1;$$

$$P_2 = \alpha_1^2 \beta_2 + \alpha_2 \beta_1^2 - 2\alpha_2 \beta_2;$$

$$P_3 = \alpha_1^3 \beta_3 + \alpha_3 \beta_1^3 + \alpha_1 \alpha_2 \beta_1 \beta_2 - 3\alpha_1 \alpha_2 \beta_3 - 3\alpha_3 \beta_1 \beta_2 + 3\alpha_3 \beta_3;$$

$$P_4 = \alpha_4 \beta_1^4 + \alpha_1 \alpha_3 \beta_1^2 \beta_2 + \alpha_1^2 \alpha_2 \beta_1 \beta_3 + \alpha_1^4 \beta_4 - 4\alpha_4 \beta_1^2 \beta_2 + \alpha_2^2 \beta_2^2 - 2\alpha_1 \alpha_3 \beta_2^2 - 2\alpha_2^2 \beta_1 \beta_3 - \alpha_1 \alpha_3 \beta_1 \beta_3 - 4\alpha_1^2 \alpha_2 \beta_4 + 2\alpha_4 \beta_2^2 + 4\alpha_4 \beta_1 \beta_3 + 2\alpha_2^2 \beta_4 + 4\alpha_1 \alpha_3 \beta_4 - 4\alpha_4 \beta_4;$$

$$P_5 = \alpha_5 \beta_1^5 + \alpha_1 \alpha_4 \beta_1^3 \beta_2 + \alpha_1^2 \alpha_3 \beta_1^2 \beta_3 + \alpha_1^3 \alpha_2 \beta_1 \beta_4 + \alpha_1^5 \beta_5 - 5\alpha_5 \beta_1^3 \beta_2 + \alpha_2 \alpha_3 \beta_1 \beta_2^2 - 3\alpha_1 \alpha_4 \beta_1 \beta_2^2 - 2\alpha_2 \alpha_3 \beta_1^2 \beta_3 - \alpha_1 \alpha_4 \beta_1^2 \beta_3 + \alpha_1 \alpha_2^2 \beta_2 \beta_3 - 2\alpha_1^2 \alpha_3 \beta_2 \beta_3 - 3\alpha_1 \alpha_2^2 \beta_1 \beta_4 - \alpha_1^2 \alpha_3 \beta_1 \beta_4 - 5\alpha_1^3 \alpha_2 \beta_5 + 5\alpha_5 \beta_1 \beta_2^2 + 5\alpha_5 \beta_1^2 \beta_3 - \alpha_2 \alpha_3 \beta_2 \beta_3 + 5\alpha_1 \alpha_4 \beta_2 \beta_3 + 5\alpha_2 \alpha_3 \beta_1 \beta_4 + \alpha_1 \alpha_4 \beta_1 \beta_4 + 5\alpha_1 \alpha_2^2 \beta_5 + 5\alpha_1^2 \alpha_3 \beta_5 - 5\alpha_5 \beta_2 \beta_3 - 5\alpha_5 \beta_1 \beta_4 - 5\alpha_2 \alpha_3 \beta_5 - 5\alpha_1 \alpha_4 \beta_5 + 5\alpha_5 \beta_5.$$

Now, let us return to the general case.

#### 4.4. Grothendieck's polynomials $P_{k,j}$

Just as our above definition of the polynomials  $P_k$  and Theorem 4.3 based upon Theorem 4.2, we can make another definition basing upon Theorem 4.1:

**Definition.** For every set  $H$  and every  $j \in \mathbb{N}$ , let us denote by  $\mathcal{P}_j(H)$  the set of all  $j$ -element subsets of  $H$ . (This is also often denoted as  $\binom{H}{j}$ .)

Let  $j \in \mathbb{N}$ . Let  $k \in \mathbb{N}$ . Our goal now is to define a polynomial  $P_{k,j} \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_{kj}]$  such that

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = P_{k,j}(X_1, X_2, \dots, X_{kj}) \quad (22)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ , where  $X_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k$  is the  $i$ -th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$  for every  $i \in \mathbb{N}$ .

In order to do this, we first fix some  $m \in \mathbb{N}$ . The polynomial

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i \in \mathbb{Z}[U_1, U_2, \dots, U_m]$$

is symmetric. Thus, Theorem 4.1 (a) yields that there exists one and only one polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  such that

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = Q(X_1, X_2, \dots, X_m).$$

Since the polynomial  $\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i$  has total degree  $\leq kj$  in the variables  $U_1, U_2, \dots, U_m$ , Theorem 4.1 (b) yields that

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = Q_{k,j}(X_1, X_2, \dots, X_{kj}),$$

where  $Q_{k,j}$  is the image of the polynomial  $Q$  under the canonical homomorphism  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m] \rightarrow \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_{kj}]$ . However, this polynomial  $Q_{k,j}$  is not independent of  $m$  yet (as the polynomial  $P_{k,j}$  that we intend to construct should be), so we call it  $Q_{k,j,[m]}$  rather than just  $Q_{k,j}$ .

Now we forget that we fixed  $m \in \mathbb{N}$ . We have learnt that

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = Q_{k,j,[m]}(X_1, X_2, \dots, X_{kj})$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ . Now, define a polynomial  $P_{k,j} \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_{kj}]$  by  $P_{k,j} = Q_{k,j,[kj]}$ .

**Theorem 4.4. (a)** The polynomial  $P_{k,j}$  just defined satisfies the equation (22) in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ . (Hence, the goal mentioned above in the definition is actually achieved.)

(b) For every  $m \in \mathbb{N}$  and  $j \in \mathbb{N}$ , we have

$$\prod_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \left( 1 + \prod_{i \in I} U_i \cdot T \right) = \sum_{k \in \mathbb{N}} P_{k,j}(X_1, X_2, \dots, X_{kj}) T^k \quad (23)$$

in the ring  $(\mathbb{Z}[U_1, U_2, \dots, U_m])[[T]]$ . (Note that the right hand side of this equation is a power series with coefficient 1 before  $T^0$ , since  $P_{0,j} = 1$ .)

*Proof of Theorem 4.4. (a) 1st Step:* Fix  $m \in \mathbb{N}$  such that  $m \geq kj$ . Then, we claim that  $Q_{k,j,[m]} = P_{k,j}$ .

*Proof.* The definition of  $Q_{k,j,[m]}$  yields

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = Q_{k,j,[m]}(X_1, X_2, \dots, X_{kj})$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ . Applying the canonical ring epimorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m] \rightarrow \mathbb{Z}[U_1, U_2, \dots, U_{kj}]$  (which maps every  $U_i$  to  $\begin{cases} U_i, & \text{if } i \leq kj; \\ 0, & \text{if } i > kj \end{cases}$ ) to this equation (and noticing that this epimorphism maps every  $X_i$  with  $i \geq 1$  to the corresponding  $X_i$  of the image ring!), we obtain

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,kj\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = Q_{k,j,[m]}(X_1, X_2, \dots, X_{kj})$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_{kj}]$ . On the other hand, the definition of  $Q_{k,j,[kj]}$  yields

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,kj\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = Q_{k,j,[kj]}(X_1, X_2, \dots, X_{kj})$$

in the same ring. These two equations yield

$$Q_{k,j,[m]}(X_1, X_2, \dots, X_{kj}) = Q_{k,j,[kj]}(X_1, X_2, \dots, X_{kj}).$$

Since the elements  $X_1, X_2, \dots, X_{kj}$  of  $\mathbb{Z}[U_1, U_2, \dots, U_{kj}]$  are algebraically independent (by Theorem 4.1 (a)), this yields  $Q_{k,j,[m]} = Q_{k,j,[kj]}$ . In other words,  $Q_{k,j,[m]} = P_{k,j}$ , and the 1st Step is proven.

*2nd Step:* For every  $m \in \mathbb{N}$ , the equation (22) is satisfied in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ .

*Proof.* Let  $m' \in \mathbb{N}$  be such that  $m' \geq m$  and  $m' \geq kj$  (such an  $m'$  clearly exists). Then, the 1st Step (applied to  $m'$  instead of  $m$ ) yields that  $Q_{k,j,[m']} = P_{k,j}$ .



The definition of  $Q_{k,j,[m']}$  yields

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m'\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i = Q_{k,j,[m']} (X_1, X_2, \dots, X_{kj})$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_{m'}]$ . Applying the canonical ring epimorphism  $\mathbb{Z}[U_1, U_2, \dots, U_{m'}] \rightarrow \mathbb{Z}[U_1, U_2, \dots, U_m]$  (which maps every  $U_i$  to  $\begin{cases} U_i, & \text{if } i \leq m; \\ 0, & \text{if } i > m \end{cases}$ ) to this equation (and noticing that this epimorphism maps every  $X_i$  with  $i \geq 1$  to the corresponding  $X_i$  of the image ring!), we obtain

$$\begin{aligned} \sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i &= \underbrace{Q_{k,j,[m']}}_{=P_{k,j}} (X_1, X_2, \dots, X_{kj}) \\ &= P_{k,j} (X_1, X_2, \dots, X_{kj}) \end{aligned}$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ . This means that the equation (22) is satisfied in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ . This completes the 2nd Step and proves Theorem 4.4 (a).

(b) We have

$$\begin{aligned} & \prod_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \left( 1 + \prod_{i \in I} U_i \cdot T \right) \\ &= \sum_{k \in \mathbb{N}} \underbrace{\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \prod_{I \in S} \prod_{i \in I} U_i T^k}_{=P_{k,j}(X_1, X_2, \dots, X_{kj}) \text{ (according to (22))}} \\ & \quad \left( \begin{array}{c} \text{by Exercise 4.2 (d), applied to} \\ Q = \mathcal{P}_j(\{1, 2, \dots, m\}), A = (\mathbb{Z}[U_1, U_2, \dots, U_m])[[T]], \\ t = T \text{ and } \alpha_I = \prod_{i \in I} U_i \end{array} \right) \\ &= \sum_{k \in \mathbb{N}} P_{k,j} (X_1, X_2, \dots, X_{kj}) T^k. \end{aligned}$$

This proves Theorem 4.4 (b). □

**Example.** Computing the polynomials  $P_{k,j}$  can be done by retracing their definition, just as in the case of  $P_k$ . It is even easier than computing  $P_k$ , because the definition of  $P_k$  made use of Theorem 4.2 (a), while that of  $P_{k,j}$  did not. Thus all we need is (22) and an algorithm to write a symmetric polynomial as a polynomial in the elementary symmetric ones. I am not doing any example computations for this here,

but here are some results:

$$\begin{aligned}
P_{0,j} &= 1 && \text{for all } j \in \mathbb{N}; \\
P_{1,0} &= 1; \\
P_{1,j} &= \alpha_j && \text{for all positive } j \in \mathbb{N}; \\
P_{k,0} &= 0 && \text{for all integers } k \geq 2; \\
P_{k,1} &= \alpha_k && \text{for all positive } k \in \mathbb{N}; \\
P_{2,2} &= \alpha_1\alpha_3 - \alpha_4; \\
P_{2,3} &= \alpha_6 - \alpha_1\alpha_5 + \alpha_2\alpha_4; \\
P_{3,2} &= \alpha_6 + \alpha_1^2\alpha_4 - 2\alpha_2\alpha_4 - \alpha_1\alpha_5 + \alpha_3^2; \\
P_{3,3} &= \alpha_1\alpha_4^2 + \alpha_2^2\alpha_5 - 2\alpha_1\alpha_3\alpha_5 - \alpha_1\alpha_2\alpha_6 + \alpha_1^2\alpha_7 - \alpha_4\alpha_5 + 3\alpha_3\alpha_6 - \alpha_2\alpha_7 - \alpha_1\alpha_8 + \alpha_9; \\
P_{4,2} &= \alpha_1^3\alpha_5 + \alpha_1\alpha_3\alpha_4 - 3\alpha_1\alpha_2\alpha_5 - \alpha_1^2\alpha_6 - \alpha_4^2 + \alpha_3\alpha_5 + 2\alpha_2\alpha_6 + \alpha_1\alpha_7 - \alpha_8.
\end{aligned}$$

Do you see the pattern in the  $P_{2,j}$ ? See Exercise 4.4 for the answer.

## 4.5. Exercises

*Exercise 4.1. (Computing  $P_k$  and  $P_{k,j}$  as coefficients of determinants.)*

The definitions of the polynomials  $P_k$  and  $P_{k,j}$  provide a possibility to recursively compute them for given values of  $k$  and  $j$  (at least if one knows the constructive proof of Theorem 4.1, which is fortunately the one given in most books). In this exercise, we will show another way to compute explicit formulas for  $P_k$  and  $P_{k,j}$ :

(a) Let  $m \in \mathbb{N}$ . In the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ , let  $X_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the  $i$ -th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$  for every  $i \in \mathbb{N}$ .

Define a matrix  $F_U \in (\mathbb{Z}[X_1, X_2, \dots, X_m])^{m \times m}$  by

$$F_U = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ (-1)^{m-1} X_m & (-1)^{m-2} X_{m-1} & (-1)^{m-3} X_{m-2} & (-1)^{m-4} X_{m-3} & \cdots & (-1)^0 X_1 \end{pmatrix}.$$

Prove that the polynomial

$$\det(TF_U + I_m) \in (\mathbb{Z}[X_1, X_2, \dots, X_m])[T]$$

equals  $\prod_{i=1}^m (1 + U_i T)$ .

(b) Let  $m \in \mathbb{N}$  and  $n \in \mathbb{N}$ . In the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$ , let  $X_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the  $i$ -th elementary symmetric polynomial in

the variables  $U_1, U_2, \dots, U_m$  for every  $i \in \mathbb{N}$ , and  $Y_j = \sum_{\substack{S \subseteq \{1, 2, \dots, n\}; \\ |S|=j}} \prod_{k \in S} V_k$  be

the  $j$ -th elementary symmetric polynomial in the variables  $V_1, V_2, \dots, V_n$  for every  $j \in \mathbb{N}$ .

Similarly to the matrix  $F_U$  defined in part (a), we can define a matrix  $F_V \in (\mathbb{Z}[Y_1, Y_2, \dots, Y_n])^{n \times n}$  by

$$F_V = \begin{pmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ (-1)^{n-1} Y_n & (-1)^{n-2} Y_{n-1} & (-1)^{n-3} Y_{n-2} & (-1)^{n-4} Y_{n-3} & \cdots & (-1)^0 Y_1 \end{pmatrix}.$$

Also, define a matrix  $F_U \in (\mathbb{Z}[X_1, X_2, \dots, X_m])^{m \times m}$  as in part (a). Let  $\mathcal{R}$  be the ring  $\mathbb{Z}[X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n]$ . We can thus regard both  $F_U$  and  $F_V$  as matrices over the ring  $\mathcal{R}$ : namely,  $F_U \in \mathcal{R}^{m \times m}$  and  $F_V \in \mathcal{R}^{n \times n}$ . Hence, the tensor product  $F_U \otimes F_V$  of these two matrices is defined<sup>22</sup>; it is an  $mn \times mn$ -matrix over  $\mathcal{R}$ . Prove that the polynomial

$$\det(-T(F_U \otimes F_V) + I_{mn}) \in (\mathbb{Z}[X_1, X_2, \dots, X_m, Y_1, Y_2, \dots, Y_n])[T]$$

equals  $\prod_{(i,j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}} (1 + U_i V_j T)$ . Conclude that the coefficient of this polynomial before  $T^k$  equals the  $Q_{k,k,[n,m]}(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k)$  defined in the definition of  $P_k$ . How to compute  $P_k$  now? (Don't forget to choose  $n$  and  $m$  such that  $n \geq k$  and  $m \geq k$ .)

(c) Let  $m \in \mathbb{N}$  and  $j \in \mathbb{N}$ . Define the polynomials  $X_i$  and an  $m \times m$ -matrix  $F_U$  as in part (a). Then, an  $\binom{m}{j} \times \binom{m}{j}$ -matrix  $\wedge^j F_U$  over the ring  $\mathbb{Z}[X_1, X_2, \dots, X_m]$  is defined<sup>23</sup>. Prove that the polynomial

$$\det \left( (-1)^j T (\wedge^j F_U) + I_{\binom{m}{j}} \right) \in (\mathbb{Z}[X_1, X_2, \dots, X_m])[T]$$

<sup>22</sup>It is defined as follows: The  $m \times m$ -matrix  $F_U$  induces an endomorphism of the free  $\mathcal{R}$ -module  $\mathcal{R}^m$ , whereas the  $n \times n$ -matrix  $F_V$  induces an endomorphism of the free  $\mathcal{R}$ -module  $\mathcal{R}^n$ . The tensor product of these two endomorphisms is an endomorphism of the free  $\mathcal{R}$ -module  $\mathcal{R}^n \otimes_{\mathcal{R}} \mathcal{R}^m$ . This latter endomorphism can be represented by an  $mn \times mn$ -matrix once we have chosen a basis of the free  $\mathcal{R}$ -module  $\mathcal{R}^n \otimes_{\mathcal{R}} \mathcal{R}^m$ . For the purposes of this exercise, it makes no matter which basis we choose, as long as we do choose a basis. Anyway, we have thus obtained an  $mn \times mn$ -matrix; this matrix is called  $F_U \otimes F_V$ .

<sup>23</sup>It is defined as follows: Let  $\mathcal{M}$  be the ring  $\mathbb{Z}[X_1, X_2, \dots, X_m]$ . The  $m \times m$ -matrix  $F_U$  induces an endomorphism of the free  $\mathcal{R}$ -module  $\mathcal{R}^m$ . The  $j$ -th exterior power of this endomorphism is an endomorphism of the free  $\mathcal{R}$ -module  $\wedge^j \mathcal{R}^m$ . This latter endomorphism can be represented by an  $\binom{m}{j} \times \binom{m}{j}$ -matrix once we have chosen a basis of the free  $\mathcal{R}$ -module  $\wedge^j \mathcal{R}^m$ . For the purposes of this exercise, it makes no matter which basis we choose, as long as we do choose a basis. Anyway, we have thus obtained an  $\wedge^j \mathcal{R}^m$ -matrix; this matrix is called  $\wedge^j F_U$ .

equals  $\prod_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \left(1 + \prod_{i \in I} U_i \cdot T\right)$ . Conclude that the coefficient of this polynomial before  $T^k$  equals the  $Q_{k,j,[m]}(X_1, X_2, \dots, X_{kj})$  defined in the definition of  $P_{k,j}$ . How to compute  $P_{k,j}$  now? (Don't forget to choose  $m$  such that  $m \geq kj$ .)

*Exercise 4.2.*

(a) Let  $\alpha_1, \alpha_2, \dots, \alpha_m$  be any elements of a commutative ring  $A$ . Prove that

$$\prod_{i=1}^m (1 + \alpha_i) = \sum_{S \subseteq \{1,2,\dots,m\}} \prod_{k \in S} \alpha_k.$$

(b) Let  $\alpha_1, \alpha_2, \dots, \alpha_m$  and  $t$  be any elements of a commutative ring  $A$ . Then, prove that

$$\prod_{i=1}^m (1 + \alpha_i t) = \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k t^i.$$

24

(c) Let  $\alpha_1, \alpha_2, \dots, \alpha_m$  and  $t$  be any elements of a commutative ring  $A$ . Then, prove that

$$\prod_{i=1}^m (1 - \alpha_i t) = \sum_{i \in \mathbb{N}} (-1)^i \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k t^i.$$

(d) Let  $Q$  be a finite set, and let  $A$  be a commutative ring. Let  $\alpha_q$  be an element of  $A$  for every  $q \in Q$ . Let  $t \in A$ . Then, prove that

$$\prod_{q \in Q} (1 + \alpha_q t) = \sum_{k \in \mathbb{N}} \sum_{\substack{S \subseteq Q; \\ |S|=k}} \prod_{q \in S} \alpha_q t^k.$$

(These are four variants of one and the same identity, which is very easy but basic and used in much of the theory of symmetric polynomials.)

*Exercise 4.3.* Let  $K$  be a ring. Let  $S$  be a  $K$ -algebra. Let  $T$  be a  $K$ -subalgebra of  $S$ . Let  $p_1, p_2, \dots, p_m$  be  $m$  elements of  $T$ , and let  $q_1, q_2, \dots, q_n$  be  $n$  elements of  $S$ . Assume that the elements  $p_1, p_2, \dots, p_m$  are algebraically independent over  $K$ , and that the elements  $q_1, q_2, \dots, q_n$  are algebraically independent over  $T$ . Prove that the  $m+n$  elements  $p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n$  are algebraically independent over  $K$ .

*Exercise 4.4.* Prove that  $P_{2,j} = \sum_{i=0}^{j-1} (-1)^{i+j-1} \alpha_i \alpha_{2j-i}$  for every  $j \in \mathbb{N}$ , where  $\alpha_0$  has to be interpreted as 1.

---

<sup>24</sup>Note that a product of the form  $\prod_{k \in S} \alpha_k t^i$  has to be read as  $\left(\prod_{k \in S} \alpha_k\right) t^i$ , rather than as  $\prod_{k \in S} (\alpha_k t^i)$ .

This is a particular case of the general convention about parsing product expressions that we made in Section 0.

[The result of Exercise 4.4 is a result by John Hopkinson ([Hopkin06, Proposition 2.1]). His proof is different from the one I give in the solutions. He also gives a similar, even if more complicated formula for  $P_{3,j}$ : see [Hopkin06, Proposition 2.2].]

## 5. A $\lambda$ -ring structure on $\Lambda(K) = 1 + K[[T]]^+$

### 5.1. Definition of the $\lambda$ -ring $\Lambda(K)$

Now we are going to introduce a  $\lambda$ -ring structure on a particular set defined for any given ring  $K$ .

**Definition.** Let  $K$  be a ring. Consider the ring  $K[[T]]$  of formal power series in the variable  $T$  over  $K$ . Let  $K[[T]]^+$  denote the subset

$$\begin{aligned} TK[[T]] &= \left\{ \sum_{i \in \mathbb{N}} a_i T^i \in K[[T]] \mid a_i \in K \text{ for all } i, \text{ and } a_0 = 0 \right\} \\ &= \{p \in K[[T]] \mid p \text{ is a power series with constant term } 0\} \end{aligned}$$

of the ring  $K[[T]]$ . We are going to define a ring structure on the set

$$\begin{aligned} 1 + K[[T]]^+ &= \{1 + u \mid u \in K[[T]]^+\} \\ &= \{p \in K[[T]] \mid p \text{ is a power series with constant term } 1\}. \end{aligned}$$

First, we define an Abelian group structure on this set:

Define an addition  $\hat{+}$  on the set  $1 + K[[T]]^+$  by  $u \hat{+} v = uv$  for every  $u \in 1 + K[[T]]^+$  and  $v \in 1 + K[[T]]^+$ . In other words, addition on  $1 + K[[T]]^+$  is defined as multiplication of power series. The zero of  $1 + K[[T]]^+$  will be 1. The subtraction  $\hat{-}$  on the set  $1 + K[[T]]^+$  is given by  $u \hat{-} v = \frac{u}{v}$  for every  $u \in 1 + K[[T]]^+$  and  $v \in 1 + K[[T]]^+$  (since every  $v \in 1 + K[[T]]^+$  is an invertible power series).

Then, clearly,  $(1 + K[[T]]^+, \hat{+})$  is an Abelian group with zero 1.

Now, define a multiplication  $\hat{\cdot}$  on the set  $1 + K[[T]]^+$  by

$$\left( \sum_{i \in \mathbb{N}} a_i T^i \right) \hat{\cdot} \left( \sum_{i \in \mathbb{N}} b_i T^i \right) = \sum_{k \in \mathbb{N}} P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k) T^k$$

<sup>25</sup> for any two power series  $\sum_{i \in \mathbb{N}} a_i T^i \in 1 + K[[T]]^+$  and  $\sum_{i \in \mathbb{N}} b_i T^i \in 1 + K[[T]]^+$  (where  $a_i$  and  $b_i$  lie in  $K$  for every  $i \in \mathbb{N}$ ). <sup>26</sup>

The multiplicative unity of the ring  $1 + K[[T]]^+$  will be  $1 + T$ .

<sup>25</sup>Here, the  $\sum_{k \in \mathbb{N}}$  sign means addition in  $K[[T]]$ , not in  $1 + K[[T]]^+$ . The same holds for the  $\sum_{i \in \mathbb{N}}$  sign.

<sup>26</sup>Of course, it is not obvious that this multiplication  $\hat{\cdot}$  is associative. See Theorem 5.1 (a) for the proof of this.

Also, for every  $j \in \mathbb{N}$ , define a mapping  $\widehat{\lambda}^j : 1 + K[[T]]^+ \rightarrow 1 + K[[T]]^+$  by

$$\widehat{\lambda}^j \left( \sum_{i \in \mathbb{N}} a_i T^i \right) = \sum_{k \in \mathbb{N}} P_{k,j}(a_1, a_2, \dots, a_{k_j}) T^k$$

for every power series  $\sum_{i \in \mathbb{N}} a_i T^i \in 1 + K[[T]]^+$  (where  $a_i \in K$  for every  $i \in \mathbb{N}$ ).

Note that we have denoted the newly-defined addition, subtraction and multiplication on the set  $1 + K[[T]]^+$  by  $\widehat{+}$ ,  $\widehat{-}$  and  $\widehat{\cdot}$  in order to distinguish them from the addition  $+$ , subtraction  $-$  and multiplication  $\cdot$  inherited from  $K[[T]]$ . We will later continue in this spirit (for instance, we will denote a finite sum with respect to the addition  $\widehat{+}$  by the sign  $\widehat{\sum}$ , while a finite sum with respect to the addition  $+$  will be written using the normal  $\sum$  sign).<sup>27</sup>

**Theorem 5.1. (a)** The multiplication  $\widehat{\cdot}$  just defined makes  $(1 + K[[T]]^+, \widehat{+}, \widehat{\cdot})$  a ring with multiplicative unity  $1 + T$ . We will call this ring  $\Lambda(K)$ .

**(b)** The above defined maps  $\widehat{\lambda}^j$  make  $(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  a  $\lambda$ -ring.

We repeat again that the notation  $\Lambda(K)$  has nothing to do with exterior algebras, even though some authors use it for them.

Before we prove this Theorem 5.1, we will have to do some preparatory work: We will introduce a subset  $1 + K[T]^+$  of  $1 + K[[T]]^+$  which consists of polynomials with constant term 1. We will show (Theorem 5.2) how we can factorize such polynomials into linear factors in an extension of our ring  $K$  (similarly to Galois theory, but easier, because we don't have to worry about the extension not being a field). Then, we will see how the operations  $\widehat{+}$ ,  $\widehat{\cdot}$  and  $\widehat{\lambda}^j$  act on factorized linear polynomials (Theorem 5.3). Then, with the help of some very basic point-set topology, we will see that the subset  $1 + K[T]^+$  is dense in an appropriate topology on  $1 + K[[T]]^+$  (Theorem 5.5 **(a)**), that this topology is Hausdorff (Theorem 5.5 **(e)**), and that the operations  $\widehat{+}$ ,  $\widehat{\cdot}$  and  $\widehat{\lambda}^j$  are continuous with respect to it (Theorem 5.5 **(d)**); hence, in order to prove the ring and  $\lambda$ -ring axioms for  $\Lambda(K)$ , we only need to prove them on elements of this dense subset  $1 + K[T]^+$ . This will then be done using Theorems 5.2 and 5.3.

Even if you are willing to believe me that Theorem 5.1 holds, you are advised to read this proof, since the ideas and notions it uses will be reused several times (e. g., in Sections 9 and 10).

## 5.2. Preparing for the proof of Theorem 5.1: introducing

$$1 + K[T]^+$$

Before we prove this Theorem 5.1, we try to motivate the above definition of  $\Lambda(K)$ :

<sup>27</sup>In [Knut73], Knutson writes " + ", " - " and " \cdot " (with quotation marks) instead of  $\widehat{+}$ ,  $\widehat{-}$  and  $\widehat{\cdot}$  for the newly-defined operations. In [FulLan85], Fulton and Lang simply write  $+$ ,  $-$  and  $\cdot$  for  $\widehat{+}$ ,  $\widehat{-}$  and  $\widehat{\cdot}$ , approving the danger of confusion with the "old" operations  $+$ ,  $-$  and  $\cdot$  inherited from  $K[[T]]$ .

**Definition.** Let  $K$  be a ring. Let  $K[T]^+$  be the subset of the polynomial ring  $K[T]$  defined by

$$K[T]^+ = TK[T] = \left\{ \sum_{i \in \mathbb{N}} a_i T^i \in K[T] \mid a_i \in K \text{ for all } i, \text{ and } a_0 = 0 \right\} \\ = \{p \in K[T] \mid p \text{ is a polynomial with constant term } 0\}.$$

Then, the set  $1 + K[T]^+$  is a subset of  $1 + K[[T]]^+$ . The elements of  $1 + K[T]^+$  are polynomials.

So  $1 + K[T]^+$  is the set of all polynomials  $p \in K[T]$  with constant term 1. Loosely speaking, this means that the elements of  $1 + K[T]^+$  are monic polynomials “turned upside down” (in the sense that if  $\sum_{i=0}^n a_i T^i$  is a polynomial in  $1 + K[T]^+$  of degree  $n$  (with  $a_i \in K$  for every  $i$ ), then  $\sum_{i=0}^n a_{n-i} T^i$  is a monic polynomial of degree  $n$ , and conversely). This allows us to take some properties of monic polynomials and use them to derive similar properties for polynomials in  $1 + K[T]^+$ . For example, we can take Exercise 5.1 (which says that whenever  $P$  is a monic polynomial of degree  $n$  over a ring  $K$ , we can find a finite-free extension ring of  $K$  over which the polynomial  $P$  factors into a product of monic linear polynomials), and “turn it upside down”, obtaining the following fact about polynomials in  $1 + K[T]^+$ :

**Theorem 5.2.** Let  $K$  be a ring. For every element  $p \in 1 + K[T]^+$ , there exists an integer  $n$  (the degree of the polynomial  $p$ ), a finite-free extension ring  $K_p$  of the ring  $K$  and  $n$  elements  $p_1, p_2, \dots, p_n$  of this extension ring  $K_p$  such that  $p = \prod_{i=1}^n (1 + p_i T)$  in  $K_p[T]$ .

*Proof of Theorem 5.2.* Write the polynomial  $p$  in the form  $p = \sum_{i=0}^n a_i T^i$ , where  $n = \deg p$ . Then,  $a_0 = 1$  (since  $p \in 1 + K[T]^+$ ).

Define a new polynomial  $\tilde{p} = \sum_{i=0}^n a_{n-i} T^i \in K[T]$ . Then, the polynomial  $\tilde{p}$  is monic (since  $a_0 = 1$ ) and satisfies  $n = \deg \tilde{p}$ . Hence, by Exercise 5.1 (applied to  $P = \tilde{p}$ ), there exists a finite-free extension ring  $K_{\tilde{p}}$  of the ring  $K$  and  $n$  elements  $\tilde{p}_1, \tilde{p}_2, \dots, \tilde{p}_n$  of this extension ring  $K_{\tilde{p}}$  such that  $\tilde{p} = \prod_{i=1}^n (T - \tilde{p}_i)$  in  $K_{\tilde{p}}[T]$ .

Consider this ring  $K_{\tilde{p}}$  and these  $n$  elements  $\tilde{p}_1, \tilde{p}_2, \dots, \tilde{p}_n$ . Let  $K_p$  be the extension ring  $K_{\tilde{p}}$ , and let  $p_i$  be the element  $-\tilde{p}_i \in K_p$  for every  $i \in \{1, 2, \dots, n\}$ . Then,

$$\sum_{i=0}^n a_{n-i} T^i = \tilde{p} = \prod_{i=1}^n (T - \tilde{p}_i) = \prod_{i=1}^n \left( T + \underbrace{(-\tilde{p}_i)}_{=p_i} \right) = \prod_{i=1}^n (T + p_i) = \prod_{i=1}^n (p_i + T).$$

Therefore, Exercise 5.2 (a) (applied to  $L = K_p$ ) yields that  $\sum_{i=0}^n a_i T^i = \prod_{i=1}^n (1 + p_i T)$ .

Since  $p = \sum_{i=0}^n a_i T^i$ , this rewrites as  $p = \prod_{i=1}^n (1 + p_i T)$ . Thus, Theorem 5.2 is proven.  $\square$

### 5.3. Preparing for the proof of Theorem 5.1: extending the ring to make polynomials split

Theorem 5.2 shows us that we can split every polynomial  $p \in 1 + K[T]^+$  into linear factors in a suitably large (but finite-free) extension ring of  $K$ . This is a rather useful fact: Whenever we have to prove some facts about polynomials in  $1 + K[T]^+$ , it allows us to “adjoin roots of these polynomials” to  $K$ . In this sense it is a partial replacement of the fundamental theorem of algebra for arbitrary commutative rings. Of course, its use is limited by the fact that we don’t know much about the extension ring of  $K$  in which  $p$  factors, but the fact that it is finite-free is enough for many things!

To make systematic use of Theorem 5.2, let us introduce some notation again:

**Definition.** Let  $S$  be a set. Let  $J_s$  be a set for each  $s \in S$ . Then  $\dot{\bigcup}_{s \in S} J_s$  (the so-called *disjoint union* of the sets  $J_s$  over all  $s \in S$ ) is defined to be the set of all pairs  $(s, j)$  with  $s \in S$  and  $j \in J_s$ . In other words,  $\dot{\bigcup}_{s \in S} J_s = \bigcup_{s \in S} \{s\} \times J_s$ .

**Definition.** For every set  $H$ , let  $\mathcal{P}_{\text{fin}}^*(H)$  denote the set of all finite multisets which consist of elements of  $H$ . Also, we recall that we denote the multiset formed by the elements  $u_1, u_2, \dots, u_n$  (with multiplicity) by  $[u_1, u_2, \dots, u_n]$ .

For our ring  $K$ , let  $\text{Exten } K$  be the set of all finite-free extension rings of  $K$ . (Again, this is not a set, but a proper class. Again, we don’t care. Basically it is enough to consider all finite-free extension rings of the form  $K[X_1, X_2, \dots, X_n]/I$  with  $I$  being an ideal of  $K[X_1, X_2, \dots, X_n]$ , and *these* extension rings do form a set.)

Let  $K^{\text{int}}$  be the subset<sup>28</sup>

$$\left\{ \left( \tilde{K}, [u_1, u_2, \dots, u_n] \right) \in \dot{\bigcup}_{K' \in \text{Exten } K} \mathcal{P}_{\text{fin}}^*(K') \mid \prod_{i=1}^n (1 + u_i T) \in K[T] \right\}$$

of  $\dot{\bigcup}_{K' \in \text{Exten } K} \mathcal{P}_{\text{fin}}^*(K')$ . We then define a map

$$\Pi : K^{\text{int}} \rightarrow 1 + K[T]^+$$

through

$$\Pi \left( \tilde{K}, [u_1, u_2, \dots, u_n] \right) = \prod_{i=1}^n (1 + u_i T) \in 1 + K[T]^+$$

for every  $\left( \tilde{K}, [u_1, u_2, \dots, u_n] \right) \in K^{\text{int}}$ .

---

<sup>28</sup>Recall that  $\dot{\bigcup}_{K' \in \text{Exten } K} \mathcal{P}_{\text{fin}}^*(K')$  denotes the disjoint union of the sets  $\mathcal{P}_{\text{fin}}^*(K')$  over all  $K' \in \text{Exten } K$ ;

it is defined by  $\dot{\bigcup}_{K' \in \text{Exten } K} \mathcal{P}_{\text{fin}}^*(K') = \bigcup_{K' \in \text{Exten } K} \{K'\} \times \mathcal{P}_{\text{fin}}^*(K')$ .



Every polynomial  $p \in 1+K[T]^+$  can be written as  $p = \Pi\left(\tilde{K}, [u_1, u_2, \dots, u_n]\right)$  for some  $\left(\tilde{K}, [u_1, u_2, \dots, u_n]\right) \in K^{\text{int}}$ <sup>30</sup>. In other words, the map  $\Pi$  is surjective.

The surjectivity of the map  $\Pi$  should remind you of the correspondence between polynomials over a field and their roots over extensions of that field (and the proof of Theorem 5.2 explains why); it will help us understand  $\hat{+}$ ,  $\hat{\cdot}$  and  $\hat{\lambda}^j$  better.

#### 5.4. Preparing for the proof of Theorem 5.1: the ring structure on $\Lambda(K)$ explained

In fact, the following fact how the ring operations  $\hat{+}$  and  $\hat{\cdot}$  and the  $\lambda$ -operations  $\hat{\lambda}^j$  on  $1+K[T]^+$  act on images under the map  $\Pi$ :

**Theorem 5.3.** Let  $K$  be a ring.

Let  $u \in 1+K[T]^+$  and  $v \in 1+K[T]^+$ . Assume that  $u = \Pi\left(\tilde{K}_u, [u_1, u_2, \dots, u_m]\right)$  for some  $\left(\tilde{K}_u, [u_1, u_2, \dots, u_m]\right) \in K^{\text{int}}$ , and that  $v = \Pi\left(\tilde{K}_v, [v_1, v_2, \dots, v_n]\right)$  for some  $\left(\tilde{K}_v, [v_1, v_2, \dots, v_n]\right) \in K^{\text{int}}$ . This, in particular, implies that  $\tilde{K}_u$  and  $\tilde{K}_v$  are finite-free extension rings of  $K$ . Let  $\tilde{K}_{u,v}$  be a finite-free extension ring of  $K$  which contains both  $\tilde{K}_u$  and  $\tilde{K}_v$  as subrings.

(a) Such a ring  $\tilde{K}_{u,v}$  always exists. For instance,<sup>31</sup>  $\tilde{K}_u \otimes \tilde{K}_v$  is a finite-free extension ring of  $K$ , and we can canonically identify  $\tilde{K}_u$  with the subring  $\tilde{K}_u \otimes 1$  of  $\tilde{K}_u \otimes \tilde{K}_v$ , and identify  $\tilde{K}_v$  with the subring  $1 \otimes \tilde{K}_v$  of  $\tilde{K}_u \otimes \tilde{K}_v$ ; hence, we can set  $\tilde{K}_{u,v} = \tilde{K}_u \otimes \tilde{K}_v$ .

---

<sup>29</sup>This map is well-defined, because every  $\left(\tilde{K}, [u_1, u_2, \dots, u_n]\right) \in K^{\text{int}}$  satisfies  $\prod_{i=1}^n (1 + u_i T) \in K[T]$  and therefore  $\prod_{i=1}^n (1 + u_i T) \in 1 + K[T]^+$  (since the polynomial  $\prod_{i=1}^n (1 + u_i T)$  clearly has constant term 1).

<sup>30</sup>*Proof.* Let  $p \in 1 + K[T]^+$  be a polynomial. Then, Theorem 5.2 shows that there exists an integer  $n$  (the degree of the polynomial  $p$ ), a finite-free extension ring  $K_p$  of the ring  $K$  and  $n$  elements  $p_1, p_2, \dots, p_n$  of this extension ring  $K_p$  such that  $p = \prod_{i=1}^n (1 + p_i T)$  in  $K_p[T]$ . Consider these  $n$  and  $K_p$  and these  $p_1, p_2, \dots, p_n$ . Then,  $(K_p, [p_1, p_2, \dots, p_n]) \in K^{\text{int}}$  (since  $\prod_{i=1}^n (1 + p_i T) = p \in K[T]$ ). Moreover, the definition of  $\Pi$  yields

$$\Pi(K_p, [p_1, p_2, \dots, p_n]) = \prod_{i=1}^n (1 + p_i T) = p.$$

Hence,  $p$  can be written as  $p = \Pi\left(\tilde{K}, [u_1, u_2, \dots, u_n]\right)$  for some  $\left(\tilde{K}, [u_1, u_2, \dots, u_n]\right) \in K^{\text{int}}$  (namely, for  $\left(\tilde{K}, [u_1, u_2, \dots, u_n]\right) = (K_p, [p_1, p_2, \dots, p_n])$ ). Qed.

<sup>31</sup>In the following, the  $\otimes$  sign always means  $\otimes_K$  until stated otherwise.

(b) We have  $u\widehat{+}v = \Pi\left(\widetilde{K}_{u,v}, [u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n]\right)$ .

(c) Also,  $u\widehat{\cdot}v = \Pi\left(\widetilde{K}_{u,v}, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}]\right)$ .

(d) Let  $j \in \mathbb{N}$ . Then,  $\widehat{\lambda}^j(u) = \Pi\left(\widetilde{K}_u, \left[\prod_{i \in I} u_i \mid I \in \mathcal{P}_j(\{1, 2, \dots, m\})\right]\right)$ .

*Proof of Theorem 5.3.* The assumption that  $u = \Pi\left(\widetilde{K}_u, [u_1, u_2, \dots, u_m]\right)$  is just a different way to say that  $u = \prod_{i=1}^m (1 + u_i T)$ . Similarly,  $v = \prod_{j=1}^n (1 + v_j T)$ . Write the polynomials  $u$  and  $v$  in the forms  $u = \sum_{i \in \mathbb{N}} a_i T^i$  (with  $a_i \in K$ ) and  $v = \sum_{i \in \mathbb{N}} b_i T^i$  (with  $b_i \in K$ ).

Recall that  $\sum_{i \in \mathbb{N}} a_i T^i = u = \prod_{i=1}^m (1 + u_i T)$ . Hence, for every  $i \in \mathbb{N}$ , the element  $a_i$  is the  $i$ -th elementary symmetric polynomial applied to  $u_1, u_2, \dots, u_m$  (that is, we have  $a_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; k \in S \\ |S|=i}} \prod u_k$ ).

Similarly, for every  $j \in \mathbb{N}$ , the element  $b_j$  is the  $j$ -th elementary symmetric polynomial applied to  $v_1, v_2, \dots, v_n$  (that is, we have  $b_j = \sum_{\substack{S \subseteq \{1, 2, \dots, n\}; k \in S \\ |S|=j}} \prod v_k$ ).

(a) The  $K$ -module  $\widetilde{K}_u \otimes \widetilde{K}_v$  is finite-free (being the tensor product of two finite-free  $K$ -modules). The embedding  $K \rightarrow \widetilde{K}_v$  is injective; hence, the map  $\widetilde{K}_u \otimes K \rightarrow \widetilde{K}_u \otimes \widetilde{K}_v$  it induces must also be injective (since  $\widetilde{K}_u$  is finite-free, and hence tensoring with  $\widetilde{K}_u$  is an exact functor). Thus, we can canonically identify  $\widetilde{K}_u$  with the subring  $\widetilde{K}_u \otimes K = \widetilde{K}_u \otimes 1$  of  $\widetilde{K}_u \otimes \widetilde{K}_v$ . Similarly, we can canonically identify  $\widetilde{K}_v$  with the subring  $1 \otimes \widetilde{K}_v$  of  $\widetilde{K}_u \otimes \widetilde{K}_v$ . These two identifications are “compatible at  $K$ ” (that is, they lead to one and the same embedding of  $K$  into  $\widetilde{K}_u \otimes \widetilde{K}_v$ ). As a consequence,  $\widetilde{K}_u \otimes \widetilde{K}_v$  is an extension ring of  $K$ . This proves Theorem 5.3 (a).

(b) We have

$$\begin{aligned} u\widehat{+}v &= uv = \prod_{i=1}^m (1 + u_i T) \prod_{j=1}^n (1 + v_j T) \\ &\left( \text{since } u = \prod_{i=1}^m (1 + u_i T) \text{ and } v = \prod_{j=1}^n (1 + v_j T) \right) \\ &= \Pi\left(\widetilde{K}_{u,v}, [u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n]\right) \end{aligned}$$

(by the definition of  $\Pi\left(\widetilde{K}_{u,v}, [u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n]\right)$ ). This proves Theorem 5.3 (b).

(c) Consider the ring  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n]$  (the polynomial ring in  $m + n$  indeterminates  $U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n$  over the ring  $\mathbb{Z}$ ). For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; k \in S \\ |S|=i}} \prod U_k$  be the  $i$ -th elementary symmetric polynomial in the variables

$U_1, U_2, \dots, U_m$ . For every  $j \in \mathbb{N}$ , let  $Y_j = \sum_{\substack{S \subseteq \{1, 2, \dots, n\}; \\ |S|=j}} \prod_{k \in S} V_k$  be the  $j$ -th elementary symmetric polynomial in the variables  $V_1, V_2, \dots, V_n$ .

There exists a ring homomorphism

$$\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n] \rightarrow \tilde{K}_{u,v}$$

which maps  $U_i$  to  $u_i$  for every  $i \in \{1, 2, \dots, m\}$  and  $V_j$  to  $v_j$  for every  $j \in \{1, 2, \dots, n\}$ . This homomorphism maps  $X_i$  to  $a_i$  for every  $i \in \mathbb{N}$  (because  $a_i$  is the  $i$ -th elementary symmetric polynomial applied to  $u_1, u_2, \dots, u_m$ ) and  $Y_j$  to  $b_j$  for every  $j \in \mathbb{N}$  (for a similar reason). Hence, applying this homomorphism (or, rather, the ring homomorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n][T] \rightarrow \tilde{K}_{u,v}[T]$  that it induces) to (21), we obtain

$$\prod_{(i,j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}} (1 + u_i v_j T) = \sum_{k \in \mathbb{N}} P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k) T^k.$$

But

$$\sum_{k \in \mathbb{N}} P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k) T^k = \left( \sum_{i \in \mathbb{N}} a_i T^i \right) \hat{\cdot} \left( \sum_{i \in \mathbb{N}} b_i T^i \right) = \hat{u} \hat{v},$$

so this becomes

$$\prod_{(i,j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}} (1 + u_i v_j T) = \hat{u} \hat{v},$$

and thus

$$\begin{aligned} \hat{u} \hat{v} &= \prod_{(i,j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}} (1 + u_i v_j T) \\ &= \Pi \left( \tilde{K}_{u,v}, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}] \right) \end{aligned}$$

(by the definition of  $\Pi \left( \tilde{K}_{u,v}, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}] \right)$ ). This proves Theorem 5.3 (c).

(d) Consider the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ . For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the  $i$ -th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$ .

There exists a ring homomorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m] \rightarrow \tilde{K}_u$  which maps  $U_i$  to  $u_i$  for every  $i \in \{1, 2, \dots, m\}$ . This homomorphism maps  $X_i$  to  $a_i$  for every  $i \in \mathbb{N}$  (because  $a_i$  is the  $i$ -th elementary symmetric polynomial applied to  $u_1, u_2, \dots, u_m$ ). Hence, applying this homomorphism (or, rather, the ring homomorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m][T] \rightarrow \tilde{K}_u[T]$  that it induces) to (23), we obtain

$$\prod_{I \in \mathcal{P}_j(\{1, 2, \dots, m\})} \left( 1 + \prod_{i \in I} u_i \cdot T \right) = \sum_{k \in \mathbb{N}} P_{k,j}(a_1, a_2, \dots, a_{kj}) T^k.$$

But

$$\sum_{k \in \mathbb{N}} P_{k,j}(a_1, a_2, \dots, a_{kj}) T^k = \hat{\lambda}^j \left( \sum_{i \in \mathbb{N}} a_i T^i \right) = \hat{\lambda}^j(u),$$

so this becomes

$$\prod_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \left( 1 + \prod_{i \in I} u_i \cdot T \right) = \widehat{\lambda}^j(u),$$

and thus

$$\widehat{\lambda}^j(u) = \prod_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \left( 1 + \prod_{i \in I} u_i \cdot T \right) = \Pi \left( \widetilde{K}_u, \left[ \prod_{i \in I} u_i \mid I \in \mathcal{P}_j(\{1,2,\dots,m\}) \right] \right)$$

(by the definition of  $\Pi \left( \widetilde{K}_u, \left[ \prod_{i \in I} u_i \mid I \in \mathcal{P}_j(\{1,2,\dots,m\}) \right] \right)$ ). This proves Theorem 5.3 (d).  $\square$

**Corollary 5.4.** Let  $K$  be a ring. Let  $\widetilde{K}$  be a finite-free extension ring of  $K$ . Let  $I$  be some finite set, and let  $T_i$  be a finite set for every  $i \in I$ . Let  $u_{i,j}$  be an element of  $\widetilde{K}$  for every  $i \in I$  and every  $j \in T_i$ . We will write  $[u_{i,j} \mid i \in I \text{ and } j \in T_i]$  for the multiset formed by all these  $u_{i,j}$  (where each element occurs as often as it occurs among these  $u_{i,j}$ ).

(a) Then,

$$\widehat{\sum}_{i \in I} \Pi \left( \widetilde{K}, [u_{i,j} \mid j \in T_i] \right) = \Pi \left( \widetilde{K}, [u_{i,j} \mid i \in I \text{ and } j \in T_i] \right).$$

Here, the sign  $\widehat{\sum}_{i \in I}$  means a finite sum based on the addition  $\widehat{+}$  of the ring  $\Lambda(K)$  (for instance,  $\widehat{\sum}_{i \in \{1,2,3\}} a_i$  means  $a_1 \widehat{+} a_2 \widehat{+} a_3$  and not  $a_1 + a_2 + a_3$ ).

(b) Also,

$$\widehat{\prod}_{i \in I} \Pi \left( \widetilde{K}, [u_{i,j} \mid j \in T_i] \right) = \Pi \left( \widetilde{K}, \left[ \prod_{i \in I} u_{i,j_i} \mid (j_i)_{i \in I} \in \prod_{i \in I} T_i \right] \right).$$

Here, the sign  $\widehat{\prod}_{i \in I}$  means a finite product based on the multiplication  $\widehat{\cdot}$  of the ring  $\Lambda(K)$  (for instance,  $\widehat{\prod}_{i \in \{1,2,3\}} a_i$  means  $a_1 \widehat{\cdot} a_2 \widehat{\cdot} a_3$  and not  $a_1 \cdot a_2 \cdot a_3$ ).

*Proof of Corollary 5.4.* Part (a) follows by induction from Theorem 5.3 (b), and part (b) follows by induction from Theorem 5.3 (c).  $\square$

For later use, we restate parts (b), (c) and (d) of Theorem 5.3 in somewhat more flexible notations (and in a slightly extended form). First, let us deal with Theorem 5.3 (b):

**Theorem 5.3' (b).** Let  $K$  be a ring. Let  $u \in 1+K[T]^+$  and  $v \in 1+K[T]^+$ . Assume that  $u = \Pi \left( \widetilde{K}_u, [u_i \mid i \in I] \right)$  for some  $\left( \widetilde{K}_u, [u_i \mid i \in I] \right) \in K^{\text{int}}$ , and

that  $v = \Pi \left( \tilde{K}_v, [v_j \mid j \in J] \right)$  for some  $\left( \tilde{K}_v, [v_j \mid j \in J] \right) \in K^{\text{int}}$ . Let  $\tilde{K}$  be a finite-free extension ring of  $K$  such that  $\tilde{K}_u$  and  $\tilde{K}_v$  are subrings of  $\tilde{K}$ .

We have  $u \hat{+} v = \Pi \left( \tilde{K}, [u_i \mid i \in I] \cup [v_j \mid j \in J] \right)$ . Here, for any two multi-sets  $X$  and  $Y$ , we let  $X \cup Y$  denote the multiset such that every object  $z$  satisfies

$$\begin{aligned} & \text{(the multiplicity of } z \text{ in } X \cup Y) \\ &= \text{(the multiplicity of } z \text{ in } X) + \text{(the multiplicity of } z \text{ in } Y). \end{aligned}$$

*Proof of Theorem 5.3' (b).* The set  $I$  is a finite set used merely for labelling. Hence, we can WLOG assume that  $I = \{1, 2, \dots, m\}$  for some  $m \in \mathbb{N}$ . Assume this; thus,  $[u_i \mid i \in I] = [u_1, u_2, \dots, u_m]$ . Hence,  $u = \Pi \left( \tilde{K}_u, [u_i \mid i \in I] \right)$  rewrites as

$$u = \Pi \left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right).$$

The set  $J$  is a finite set used merely for labelling. Hence, we can WLOG assume that  $J = \{1, 2, \dots, n\}$  for some  $n \in \mathbb{N}$ . Assume this; thus,  $[v_j \mid j \in J] = [v_1, v_2, \dots, v_n]$ . Hence,  $v = \Pi \left( \tilde{K}_v, [v_j \mid j \in J] \right)$  rewrites as  $v = \Pi \left( \tilde{K}_v, [v_1, v_2, \dots, v_n] \right)$ .

From  $[u_i \mid i \in I] = [u_1, u_2, \dots, u_m]$  and  $[v_j \mid j \in J] = [v_1, v_2, \dots, v_n]$ , we obtain

$$\begin{aligned} [u_i \mid i \in I] \cup [v_j \mid j \in J] &= [u_1, u_2, \dots, u_m] \cup [v_1, v_2, \dots, v_n] \\ &= [u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n]. \end{aligned} \tag{24}$$

But Theorem 5.3 (b) shows that  $u \hat{+} v = \Pi \left( \tilde{K}, [u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n] \right)$ . In view of (24), this rewrites as  $u \hat{+} v = \Pi \left( \tilde{K}, [u_i \mid i \in I] \cup [v_j \mid j \in J] \right)$ . This proves Theorem 5.3' (b).  $\square$

**Theorem 5.3' (c).** Let  $K$  be a ring. Let  $u \in 1 + K[T]^+$  and  $v \in 1 + K[T]^+$ . Assume that  $u = \Pi \left( \tilde{K}_u, [u_i \mid i \in I] \right)$  for some  $\left( \tilde{K}_u, [u_i \mid i \in I] \right) \in K^{\text{int}}$ , and that  $v = \Pi \left( \tilde{K}_v, [v_j \mid j \in J] \right)$  for some  $\left( \tilde{K}_v, [v_j \mid j \in J] \right) \in K^{\text{int}}$ . Let  $\tilde{K}$  be a finite-free extension ring of  $K$  such that  $\tilde{K}_u$  and  $\tilde{K}_v$  are subrings of  $\tilde{K}$ .

We have  $u \hat{v} = \Pi \left( \tilde{K}, [u_i v_j \mid (i, j) \in I \times J] \right)$

*Proof of Theorem 5.3' (c).* We can derive Theorem 5.3' (c) from Theorem 5.3 (c) in the same way as Theorem 5.3' (b) was derived from Theorem 5.3 (b).  $\square$

Finally, let us restate Theorem 5.3 (d):

**Theorem 5.3' (d).** Let  $K$  be a ring. Let  $w \in 1 + K[T]^+$ . Assume that  $w = \Pi \left( \tilde{K}, [w_\ell \mid \ell \in L] \right)$  for some  $\left( \tilde{K}, [w_\ell \mid \ell \in L] \right) \in K^{\text{int}}$ . Let  $k \in \mathbb{N}$ . Then,

$$\hat{\lambda}^k(w) = \Pi \left( \tilde{K}, \left[ \prod_{\ell \in S} w_\ell \mid S \in \mathcal{P}_k(L) \right] \right).$$

*Proof of Theorem 5.3' (d).* Since  $L$  is a finite set used only for labelling, we can WLOG assume that  $L = \{1, 2, \dots, m\}$  for some  $m \in \mathbb{N}$ . Thus,  $w = \Pi \left( \tilde{K}, [w_\ell \mid \ell \in L] \right)$  rewrites as  $w = \Pi \left( \tilde{K}, [w_\ell \mid \ell \in \{1, 2, \dots, m\}] \right) = \Pi \left( \tilde{K}, [w_1, w_2, \dots, w_m] \right)$ . Hence, we can apply Theorem 5.3 (d) to  $u = w$ ,  $j = k$ ,  $\tilde{K}_u = \tilde{K}$ , and  $u_\ell = w_\ell$ <sup>32</sup>, and obtain

$$\begin{aligned} \hat{\lambda}^k(w) &= \Pi \left( \tilde{K}, \left[ \prod_{i \in I} w_i \mid I \in \mathcal{P}_k \left( \underbrace{\{1, 2, \dots, m\}}_{=L} \right) \right] \right) = \Pi \left( \tilde{K}, \left[ \prod_{i \in I} w_i \mid I \in \mathcal{P}_k(L) \right] \right) \\ &= \Pi \left( \tilde{K}, \left[ \prod_{\ell \in S} w_\ell \mid S \in \mathcal{P}_k(L) \right] \right) \end{aligned}$$

(here, we renamed  $i$  and  $I$  as  $\ell$  and  $S$ ). This proves Theorem 5.3' (d).  $\square$

## 5.5. Preparing for the proof of Theorem 5.1: the $(T)$ -topology

We are approaching the proof of Theorem 5.1. The idea of the proof is: We have to show some identities for elements of  $1 + K[[T]]^+$  (such as associativity of multiplication). Computing with elements of  $1 + K[[T]]^+$  can be difficult, but computing with elements of  $1 + K[T]^+$  is rather easy thanks to Theorem 5.3. Hence, we are going to reduce Theorem 5.1 to the case when our elements are in  $1 + K[T]^+$ . The reader is encouraged to try doing this on his own. In practice, it is a matter of noticing that for every  $k \in \mathbb{N}$ , only the first so and so many coefficients of the power series  $u$  and  $v$  matter when computing the  $k$ -th coefficient of  $u \hat{\cdot} v$  (for instance), and thus we can truncate the power series at these coefficients, thus turning it into a polynomial. The abstract algebraical way to formulate this argument is by introducing the so-called  $(T)$ -topology (also called the  $(T)$ -adic topology) on  $K[[T]]$ :

**Definition.** Let  $K$  be a ring. As a  $K$ -module,  $K[[T]] = \prod_{k \in \mathbb{N}} KT^k$ . Now, we define the so-called  $(T)$ -topology on the ring  $K[[T]]$  as the topology generated by

$$\{u + T^N K[[T]] \mid u \in K[[T]] \text{ and } N \in \mathbb{N}\}.$$

In other words, the open sets of this topology should be all translates<sup>33</sup> of the  $K$ -submodules  $T^N K[[T]]$  for  $N \in \mathbb{N}$ , as well as the unions of these translates<sup>34</sup>. (Note that, for each  $N \in \mathbb{N}$ , the set  $T^N K[[T]]$  is actually an

<sup>32</sup>To be fully precise, we also need to specify  $v$ ,  $\left( \tilde{K}_v, [v_1, v_2, \dots, v_n] \right)$  and  $\tilde{K}_{u,v}$  in order to apply Theorem 5.3 (d). But  $v$  and  $\left( \tilde{K}_v, [v_1, v_2, \dots, v_n] \right)$  have not been used in the proof of Theorem 5.3 (d), and  $\tilde{K}_{u,v}$  can just be taken to be  $\tilde{K}$ .

<sup>33</sup>The notion of a “translate” is defined as follows: If  $A$  is an additive group and  $B$  is a subset of  $A$ , then a *translate* of  $B$  (in  $A$ ) means a subset of  $A$  having the form

$$a + B = \{a + b \mid b \in B\}$$

for some  $a \in A$ .

<sup>34</sup>This includes the empty union, which is  $\emptyset$ .

ideal of  $K[[T]]$ , and consists of all power series  $f \in K[[T]]$  whose coefficients before  $T^0, T^1, \dots, T^{N-1}$  all vanish. This ideal  $T^N K[[T]]$  can also be described as the  $N$ -th power of the ideal  $TK[[T]]$ ; therefore, the  $(T)$ -topology on  $K[[T]]$  is precisely the so-called  $TK[[T]]$ -adic topology. Also note that every translate of the submodule  $T^N K[[T]]$  for  $N \in \mathbb{N}$  actually has the form  $p + T^N K[[T]]$  for a polynomial  $p \in K[T]$  of degree  $< N$ , and this polynomial is uniquely determined.) It is well-known that the  $(T)$ -topology makes  $K[[T]]$  into a topological ring.

This  $(T)$ -topology is a particular case of several known constructions; for example, a similar way exists to define a topology on the completion of any graded ring, or on a ring with a given ideal, or on the ring with a given sequence of ideals satisfying certain properties. We will need only the  $(T)$ -topology, however.

Now, an easy fact:

**Theorem 5.5.** Let  $K$  be a ring. The  $(T)$ -topology on the ring  $K[[T]]$  restricts to a topology on its subset  $1 + K[[T]]^+$ ; we call this topology the  $(T)$ -topology again. Whenever we say “open”, “continuous”, “dense”, etc., we are referring to this topology.

(a) The subset  $1 + K[T]^+$  is dense in  $1 + K[[T]]^+$ .

(b) Let  $f : 1 + K[[T]]^+ \rightarrow 1 + K[[T]]^+$  be a map such that for every  $n \in \mathbb{N}$  there exists some  $N \in \mathbb{N}$  such that the first  $n$  coefficients of the image of a formal power series under  $f$  depend only on the first  $N$  coefficients of the series itself (and not on the remaining ones). Then,  $f$  is continuous.

(c) Let  $g : (1 + K[[T]]^+) \times (1 + K[[T]]^+) \rightarrow 1 + K[[T]]^+$  be a map such that for every  $n \in \mathbb{N}$  there exists some  $N \in \mathbb{N}$  such that the first  $n$  coefficients of the image of a pair of formal power series under  $f$  depend only on the first  $N$  coefficients of the two series itself (and not on the remaining ones). Then,  $g$  is continuous.

(d) The map

$$\begin{aligned} (1 + K[[T]]^+) \times (1 + K[[T]]^+) &\rightarrow 1 + K[[T]]^+, \\ (u, v) &\mapsto u \widehat{+} v, \end{aligned}$$

the map

$$\begin{aligned} (1 + K[[T]]^+) \times (1 + K[[T]]^+) &\rightarrow 1 + K[[T]]^+, \\ (u, v) &\mapsto u \widehat{-} v, \end{aligned}$$

the map

$$\begin{aligned} (1 + K[[T]]^+) \times (1 + K[[T]]^+) &\rightarrow 1 + K[[T]]^+, \\ (u, v) &\mapsto \widehat{u} \cdot v, \end{aligned}$$

and the map  $\widehat{\lambda}^j : 1 + K[[T]]^+ \rightarrow 1 + K[[T]]^+$  for every  $j \in \mathbb{N}$  are continuous.

(e) The topological spaces  $K[[T]]$  and  $1 + K[[T]]^+$  are Hausdorff spaces.

Note that Theorem 5.5 **(d)** yields that any finite compositions of the maps  $\widehat{+}$ ,  $\widehat{-}$ ,  $\widehat{\cdot}$  and  $\widehat{\lambda}^j$  are continuous (since finite compositions of continuous functions are continuous). In particular, any polynomial with integral coefficients acts on  $1 + K[[T]]^+$  as a continuous map.

*Proof of Theorem 5.5.* **(a)** and **(e)** are done in any commutative algebra book such as [AtiMac69, Chapter 10].

**(b)** and **(c)** are basic exercises in topology.

**(d)** follows from **(b)** and **(c)** together with the definitions of  $\widehat{+}$ ,  $\widehat{\cdot}$  and  $\widehat{\lambda}^j$ .  $\square$

## 5.6. Proof of Theorem 5.1

Now it comes:

*Proof of Theorem 5.1.* **(a)** We have to prove the ring axioms for  $(1 + K[[T]]^+, \widehat{+}, \widehat{\cdot})$  (including the unity axiom for  $1 + T$ ). There are several axioms to be checked, but the idea is always the same, so we will only check the associativity of  $\widehat{\cdot}$  and leave the rest to the reader.

In order to prove that the operation  $\widehat{\cdot}$  is associative, we must show that  $u\widehat{\cdot}(v\widehat{\cdot}w) = (u\widehat{\cdot}v)\widehat{\cdot}w$  for all  $u, v, w \in 1 + K[[T]]^+$ . Since the operation  $\widehat{\cdot}$  is continuous (by Theorem 5.5 **(d)**), and since  $1 + K[T]^+$  is a dense subset of  $1 + K[[T]]^+$  (by Theorem 5.5 **(a)**), this needs only to be shown for all  $u, v, w \in 1 + K[T]^+$ .<sup>35</sup> So let us assume that  $u, v, w \in 1 + K[T]^+$ . Recall that the map  $\Pi$  is surjective. Hence, there exist

- some  $(\widetilde{K}_u, [u_1, u_2, \dots, u_m]) \in K^{\text{int}}$  such that  $u = \Pi(\widetilde{K}_u, [u_1, u_2, \dots, u_m])$ ,
- some  $(\widetilde{K}_v, [v_1, v_2, \dots, v_n]) \in K^{\text{int}}$  such that  $v = \Pi(\widetilde{K}_v, [v_1, v_2, \dots, v_n])$ ,
- some  $(\widetilde{K}_w, [w_1, w_2, \dots, w_\ell]) \in K^{\text{int}}$  such that  $w = \Pi(\widetilde{K}_w, [w_1, w_2, \dots, w_\ell])$ .

Consider these elements of  $K^{\text{int}}$ . Notice that

$$u = \Pi\left(\widetilde{K}_u, \underbrace{[u_1, u_2, \dots, u_m]}_{=[u_i | i \in \{1, 2, \dots, m\}]}\right) = \Pi\left(\widetilde{K}_u, [u_i \mid i \in \{1, 2, \dots, m\}]\right)$$

and

$$w = \Pi\left(\widetilde{K}_w, \underbrace{[w_1, w_2, \dots, w_\ell]}_{=[w_k | k \in \{1, 2, \dots, \ell\}]}\right) = \Pi\left(\widetilde{K}_w, [w_k \mid k \in \{1, 2, \dots, \ell\}]\right).$$

Let  $L = \widetilde{K}_u \otimes \widetilde{K}_v \otimes \widetilde{K}_w$ . Clearly,  $L$  is a finite-free  $K$ -module (since it is the tensor product of the finite-free  $K$ -modules  $\widetilde{K}_u, \widetilde{K}_v, \widetilde{K}_w$ ). We identify the rings  $\widetilde{K}_u, \widetilde{K}_v, \widetilde{K}_w$  with the subrings  $\widetilde{K}_u \otimes 1 \otimes 1, 1 \otimes \widetilde{K}_v \otimes 1, 1 \otimes 1 \otimes \widetilde{K}_w$  of the ring  $L = \widetilde{K}_u \otimes \widetilde{K}_v \otimes \widetilde{K}_w$ ,

<sup>35</sup>At this point, we are actually also using Theorem 5.5 **(e)**. In fact, what we are using is the fact that if two continuous maps from a topological space  $\mathfrak{P}$  to a Hausdorff topological space  $\mathfrak{Q}$  are equal to each other on a dense subset of  $\mathfrak{P}$ , then they are equal to each other on the whole  $\mathfrak{P}$ .



respectively<sup>36</sup>. This way,  $L$  becomes a finite-free extension ring of  $K$  which contains all three rings  $\tilde{K}_u, \tilde{K}_v, \tilde{K}_w$  as subrings. Now, Theorem 5.3 (c) yields

$$u\hat{v} = \Pi(L, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}]).$$

Hence, Theorem 5.3' (c) (applied to  $u\hat{v}, w, L, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}], \tilde{K}_w, [w_k \mid k \in \{1, 2, \dots, \ell\}]$  and  $L$  instead of  $u, v, \tilde{K}_u, [u_i \mid i \in I], \tilde{K}_v, [v_j \mid j \in J]$  and  $\tilde{K}$ ) yields

$$(u\hat{v})\hat{w} = \Pi(L, [(u_i v_j) w_k \mid ((i, j), k) \in (\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}) \times \{1, 2, \dots, \ell\}]).$$

Also, Theorem 5.3 (c) (applied to  $v, w, \tilde{K}_v, [v_1, v_2, \dots, v_n], \tilde{K}_w, [w_1, w_2, \dots, w_\ell]$  and  $L$  instead of  $u, v, \tilde{K}_u, [u_1, u_2, \dots, u_m], \tilde{K}_v, [v_1, v_2, \dots, v_n]$  and  $\tilde{K}_{u,v}$ ) yields

$$v\hat{w} = \Pi(L, [v_j w_k \mid (j, k) \in \{1, 2, \dots, n\} \times \{1, 2, \dots, \ell\}]).$$

Hence, Theorem 5.3' (c) (applied to  $u, v\hat{w}, \tilde{K}_u, [u_i \mid i \in I], L, [v_j w_k \mid (j, k) \in \{1, 2, \dots, n\} \times \{1, 2, \dots, \ell\}]$  and  $L$  instead of  $u, v, \tilde{K}_u, [u_i \mid i \in I], \tilde{K}_v, [v_j \mid j \in J]$  and  $\tilde{K}$ ) yields

$$u\hat{(v\hat{w})} = \Pi(L, [u_i (v_j w_k) \mid (i, (j, k)) \in \{1, 2, \dots, m\} \times (\{1, 2, \dots, n\} \times \{1, 2, \dots, \ell\})]).$$

But there is a canonical isomorphism of sets

$$(\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}) \times \{1, 2, \dots, \ell\} \rightarrow \{1, 2, \dots, m\} \times (\{1, 2, \dots, n\} \times \{1, 2, \dots, \ell\}),$$

mapping every  $((i, j), k)$  to  $(i, (j, k))$ . Hence,

$$\begin{aligned} & \Pi(L, [(u_i v_j) w_k \mid ((i, j), k) \in (\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}) \times \{1, 2, \dots, \ell\}]) \\ &= \Pi \left( L, \left[ \underbrace{(u_i v_j) w_k}_{=u_i(v_j w_k)} \mid (i, (j, k)) \in \{1, 2, \dots, m\} \times (\{1, 2, \dots, n\} \times \{1, 2, \dots, \ell\}) \right] \right) \\ &= \Pi(L, [u_i (v_j w_k) \mid (i, (j, k)) \in \{1, 2, \dots, m\} \times (\{1, 2, \dots, n\} \times \{1, 2, \dots, \ell\})]). \end{aligned}$$

Thus,

$$\begin{aligned} (u\hat{v})\hat{w} &= \Pi(L, [(u_i v_j) w_k \mid ((i, j), k) \in (\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}) \times \{1, 2, \dots, \ell\}]) \\ &= \Pi(L, [u_i (v_j w_k) \mid (i, (j, k)) \in \{1, 2, \dots, m\} \times (\{1, 2, \dots, n\} \times \{1, 2, \dots, \ell\})]) \\ &= u\hat{(v\hat{w})}. \end{aligned}$$

This proves the associativity of the operation  $\hat{\cdot}$ . As I said above, the other ring axioms can be proven similarly, so we can consider Theorem 5.1 (a) as proven.

(b) It is easy to see that

$$\hat{\lambda}^0(x) = 1 + T = (\text{the multiplicative unity of the ring } (1 + K[[T]]^+, \hat{+}, \hat{\cdot}))$$

<sup>36</sup>This is legitimate, because the canonical ring homomorphisms  $\tilde{K}_u \otimes 1 \otimes 1 \rightarrow \tilde{K}_u \otimes \tilde{K}_v \otimes \tilde{K}_w$ ,  $1 \otimes \tilde{K}_v \otimes 1 \rightarrow \tilde{K}_u \otimes \tilde{K}_v \otimes \tilde{K}_w$  and  $1 \otimes 1 \otimes \tilde{K}_w \rightarrow \tilde{K}_u \otimes \tilde{K}_v \otimes \tilde{K}_w$  are injective (indeed, the  $K$ -modules  $\tilde{K}_u, \tilde{K}_v$  and  $\tilde{K}_w$  are finite free, and therefore tensoring with each of these  $K$ -modules is an exact functor).

and

$$\widehat{\lambda}^1(x) = x$$

for every  $x \in \Lambda(K)$ . It now remains to prove that

$$\widehat{\lambda}^j(u \widehat{+} v) = \widehat{\sum_{i=0}^j \widehat{\lambda}^i(u) \widehat{\cdot} \widehat{\lambda}^{j-i}(v)} \quad (25)$$

for every  $j \in \mathbb{N}$ ,  $u \in \Lambda(K)$  and  $v \in \Lambda(K)$ . Here, the sign  $\widehat{\sum_{i=0}^j}$  means that the summation is based on the addition  $\widehat{+}$  of the ring  $\Lambda(K)$ .

Let us fix some  $j \in \mathbb{N}$ . Since the addition  $\widehat{+}$ , the multiplication  $\widehat{\cdot}$  and the map  $\widehat{\lambda}^i$  for every  $i \in \mathbb{N}$  are continuous (by Theorem 5.5 **(d)**), and since  $1 + K[T]^+$  is a dense subset of  $1 + K[[T]]^+$  (by Theorem 5.5 **(a)**), we only need to check (25) for all  $u, v \in 1 + K[T]^+$ . So let us assume that  $u, v \in 1 + K[T]^+$ . Then, there exist some  $(\widetilde{K}_u, [u_1, u_2, \dots, u_m]) \in K^{\text{int}}$  such that  $u = \Pi(\widetilde{K}_u, [u_1, u_2, \dots, u_m])$ , and some  $(\widetilde{K}_v, [v_1, v_2, \dots, v_n]) \in K^{\text{int}}$  such that  $v = \Pi(\widetilde{K}_v, [v_1, v_2, \dots, v_n])$ . Let  $\widetilde{K}_{u,v}$  be a finite-free extension ring of  $K$  which contains both  $\widetilde{K}_u$  and  $\widetilde{K}_v$  as subrings. (Such an extension ring exists, as was proven in Theorem 5.3 **(a)**.) Theorem 5.3 **(b)** yields

$$u \widehat{+} v = \Pi(\widetilde{K}_{u,v}, [u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n]).$$

In other words, if we define  $m + n$  elements  $w_1, w_2, \dots, w_{m+n}$  by

$$w_i = \begin{cases} u_i, & \text{if } i \leq m; \\ v_{i-m}, & \text{if } i > m \end{cases} \quad \text{for every } i \in \{1, 2, \dots, m+n\},$$

then

$$u \widehat{+} v = \Pi(\widetilde{K}_{u,v}, [w_1, w_2, \dots, w_{m+n}]).$$

Thus, Theorem 5.3 **(d)** yields

$$\widehat{\lambda}^j(u \widehat{+} v) = \Pi\left(\widetilde{K}_{u,v}, \left[\prod_{i \in I} w_i \mid I \in \mathcal{P}_j(\{1, 2, \dots, m+n\})\right]\right).$$

But since

$$\begin{aligned}
& \left[ \prod_{i \in I} w_i \mid I \in \mathcal{P}_j(\{1, 2, \dots, m+n\}) \right] \\
&= \left[ \prod_{\gamma \in I} w_\gamma \mid I \in \mathcal{P}_j(\{1, 2, \dots, m+n\}) \right] \\
&= \left[ \prod_{\gamma \in J \cup K'} w_\gamma \mid i \in \{0, 1, \dots, j\}, J \in \mathcal{P}_i(\{1, 2, \dots, m\}), K' \in \mathcal{P}_{j-i}(\{m+1, m+2, \dots, m+n\}) \right] \\
&\quad \left( \begin{array}{l} \text{because every set } I \in \mathcal{P}_j(\{1, 2, \dots, m+n\}) \text{ can be uniquely} \\ \text{written as a union } J \cup K' \text{ of two sets } J \in \mathcal{P}_i(\{1, 2, \dots, m\}) \text{ and} \\ K' \in \mathcal{P}_{j-i}(\{m+1, m+2, \dots, m+n\}) \text{ for some } i \in \{0, 1, \dots, j\} \\ \text{(namely, these two sets are } J = I \cap \{1, 2, \dots, m\} \text{ and} \\ K' = I \cap \{m+1, m+2, \dots, m+n\}, \text{ and } i \text{ is the cardinality of } J) \end{array} \right) \\
&= \left[ \prod_{\alpha \in J} w_\alpha \prod_{\beta \in K'} w_\beta \mid i \in \{0, 1, \dots, j\}, J \in \mathcal{P}_i(\{1, 2, \dots, m\}), K' \in \mathcal{P}_{j-i}(\{m+1, m+2, \dots, m+n\}) \right] \\
&\quad \left( \text{since } \prod_{\gamma \in J \cup K'} w_\gamma = \prod_{\alpha \in J} w_\alpha \prod_{\beta \in K'} w_\beta \text{ (because } J \cap K' = \emptyset) \right) \\
&= \left[ \prod_{\alpha \in J} w_\alpha \prod_{\beta \in M} w_{m+\beta} \mid i \in \{0, 1, \dots, j\}, J \in \mathcal{P}_i(\{1, 2, \dots, m\}), M \in \mathcal{P}_{j-i}(\{1, 2, \dots, n\}) \right] \\
&\quad \text{(here, we have substituted } M = \{u - m \mid u \in K'\} \text{ for } K') \\
&= \left[ \prod_{\alpha \in J} u_\alpha \prod_{\beta \in M} v_\beta \mid i \in \{0, 1, \dots, j\}, J \in \mathcal{P}_i(\{1, 2, \dots, m\}), M \in \mathcal{P}_{j-i}(\{1, 2, \dots, n\}) \right] \\
&\quad \left( \text{since } w_i = \begin{cases} u_i, & \text{if } i \leq m; \\ v_{i-m}, & \text{if } i > m \end{cases} \right),
\end{aligned}$$

this becomes

$$\begin{aligned}
& \widehat{\lambda}^j (u \widehat{+} v) \\
&= \Pi \left( \widetilde{K}_{u,v}, \left[ \prod_{\alpha \in J} u_\alpha \prod_{\beta \in M} v_\beta \mid i \in \{0, 1, \dots, j\}, J \in \mathcal{P}_i(\{1, 2, \dots, m\}), M \in \mathcal{P}_{j-i}(\{1, 2, \dots, n\}) \right] \right) \\
&= \sum_{i=0}^{\widehat{j}} \underbrace{\Pi \left( \widetilde{K}_{u,v}, \left[ \prod_{\alpha \in J} u_\alpha \prod_{\beta \in M} v_\beta \mid J \in \mathcal{P}_i(\{1, 2, \dots, m\}), M \in \mathcal{P}_{j-i}(\{1, 2, \dots, n\}) \right] \right)}_{= \Pi \left( \widetilde{K}_u, \left[ \prod_{\alpha \in J} u_\alpha \mid J \in \mathcal{P}_i(\{1, 2, \dots, m\}) \right] \right) \widehat{\cdot} \Pi \left( \widetilde{K}_v, \left[ \prod_{\beta \in M} v_\beta \mid M \in \mathcal{P}_{j-i}(\{1, 2, \dots, n\}) \right] \right)} \\
&\quad \text{(by Theorem 5.3' (c))} \\
&\quad \text{(by Corollary 5.4 (a))} \\
&= \sum_{i=0}^{\widehat{j}} \underbrace{\Pi \left( \widetilde{K}_u, \left[ \prod_{\alpha \in J} u_\alpha \mid J \in \mathcal{P}_i(\{1, 2, \dots, m\}) \right] \right)}_{= \widehat{\lambda}^i(u)} \widehat{\cdot} \underbrace{\Pi \left( \widetilde{K}_v, \left[ \prod_{\beta \in M} v_\beta \mid M \in \mathcal{P}_{j-i}(\{1, 2, \dots, n\}) \right] \right)}_{= \widehat{\lambda}^{j-i}(v)} \\
&\quad \text{(by Theorem 5.3 (d))} \quad \text{(by Theorem 5.3 (d))} \\
&= \sum_{i=0}^{\widehat{j}} \widehat{\lambda}^i (u) \widehat{\cdot} \widehat{\lambda}^{j-i} (v),
\end{aligned}$$

proving (25). Theorem 5.1 (b) is proven.  $\square$

## 5.7. $\lambda_T : K \rightarrow \Lambda(K)$ is an additive group homomorphism

The following trivial fact is a foreshadowing of the notion of “special  $\lambda$ -rings”:

**Theorem 5.6.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Consider the map  $\lambda_T : K \rightarrow \Lambda(K)$  defined by

$$\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \quad \text{for every } x \in K.$$

Then,  $\lambda_T$  is an additive group homomorphism (where the additive group structure on  $\Lambda(K)$  is given by  $\widehat{+}$ ).

*Proof of Theorem 5.6.* The map  $\lambda_T$  is well-defined (i. e. every  $x \in K$  satisfies  $\sum_{i \in \mathbb{N}} \lambda^i(x) T^i \in \Lambda(K)$ ) because  $\lambda^0(x) = 1$  for every  $x \in K$ . The assertion that  $\lambda_T$  is an additive group homomorphism follows from Theorem 2.1 (b) (because as an additive group,  $\Lambda(K) = (\Lambda(K), \widehat{+}) = (\Lambda(K), \cdot)$ ). Theorem 5.6 is thus proven.  $\square$

While Theorem 5.6 says that  $\lambda_T$  is an additive group homomorphism, it is not in general a ring homomorphism. But for many  $\lambda$ -rings  $K$ , it is one - and even a  $\lambda$ -ring homomorphism. These  $\lambda$ -rings will be studied in the next Section.

## 5.8. On the evaluation (substitution) map

The following properties of the map  $\text{ev}$  defined in Section 3 will turn out useful to us later:

**Theorem 5.7.** Let  $K$  be a ring.

(a) For every  $\mu \in K$ , the map  $\text{ev}_{\mu T} : K[[T]] \rightarrow K[[T]]$  is continuous (with respect to the  $(T)$ -topology).

(b) Let  $u \in 1 + K[[T]]^+$ . Assume that  $u = \Pi \left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right)$  for some  $\left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right) \in K^{\text{int}}$ . Let  $\mu \in K$ . Then,  $\text{ev}_{\mu T}(u) = \Pi \left( \tilde{K}_u, [\mu u_1, \mu u_2, \dots, \mu u_m] \right) = \Pi \left( \tilde{K}_u, [\mu u_i \mid i \in \{1, 2, \dots, m\}] \right)$ .

(c) Let  $u \in \Lambda(K)$  and  $v \in \Lambda(K)$ . Let  $\mu \in K$ . Then,  $\text{ev}_{\mu T}(u) \hat{+} \text{ev}_{\mu T}(v) = \text{ev}_{\mu T}(u \hat{+} v)$ .

(d) Let  $u \in \Lambda(K)$  and  $v \in \Lambda(K)$ . Let  $\mu \in K$  and  $\nu \in K$ . Then,  $\text{ev}_{\mu T}(u) \hat{\cdot} \text{ev}_{\nu T}(v) = \text{ev}_{\mu\nu T}(u \hat{\cdot} v)$ .

(e) Let  $u \in \Lambda(K)$ . Let  $\mu \in K$ . Let  $k \in \mathbb{N}$ . Then,  $\hat{\lambda}^k(\text{ev}_{\mu T}(u)) = \text{ev}_{\mu^k T}(\hat{\lambda}^k(u))$ .

*Proof of Theorem 5.7.* (a) Obvious from Theorem 5.5 (b) (or, more precisely, from the assertion you get if you replace  $1 + K[[T]]^+$  by  $K[[T]]$  in Theorem 5.5 (b)); but this assertion is proven in the same way as Theorem 5.5 (b)).

(b) By assumption,  $u = \Pi \left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right) = \prod_{i=1}^m (1 + u_i T)$ , so that

$$\text{ev}_{\mu T}(u) = \prod_{i=1}^m (1 + u_i \mu T) = \prod_{i=1}^m (1 + \mu u_i T) = \Pi \left( \tilde{K}_u, [\mu u_1, \mu u_2, \dots, \mu u_m] \right),$$

and Theorem 5.7 (b) is proven.

(d) Since the operation  $\hat{\cdot}$  and the maps  $\text{ev}_{\mu T}$ ,  $\text{ev}_{\nu T}$  and  $\text{ev}_{\mu\nu T}$  are continuous (by Theorem 5.5 (d) and Theorem 5.7 (a)), and  $1 + K[[T]]^+$  is a dense subset of  $1 + K[[T]]^+$  (by Theorem 5.5 (a)), this needs only to be shown for all  $u, v \in 1 + K[[T]]^+$ . So let us assume that  $u, v \in 1 + K[[T]]^+$ . Then, there exist some  $\left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right) \in K^{\text{int}}$  such that  $u = \Pi \left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right)$ , and some  $\left( \tilde{K}_v, [v_1, v_2, \dots, v_n] \right) \in K^{\text{int}}$  such that  $v = \Pi \left( \tilde{K}_v, [v_1, v_2, \dots, v_n] \right)$ . Theorem 5.3 (a) says that there exists an extension ring  $\tilde{K}_{u,v}$  containing both  $\tilde{K}_u$  and  $\tilde{K}_v$  as subrings. Now, Theorem 5.3 (c) yields  $u \hat{\cdot} v = \Pi \left( \tilde{K}_{u,v}, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}] \right)$ , so that Theorem 5.7 (b) gives us

$$\begin{aligned} \text{ev}_{\mu\nu T}(u \hat{\cdot} v) &= \Pi \left( \tilde{K}_{u,v}, [\mu\nu u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}] \right) \\ &= \Pi \left( \tilde{K}_{u,v}, [\mu u_i \cdot \nu v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}] \right). \end{aligned}$$

On the other hand, Theorem 5.7 (b) yields  $\text{ev}_{\mu T}(u) = \Pi\left(\tilde{K}_u, [\mu u_1, \mu u_2, \dots, \mu u_m]\right)$  and (similarly)  $\text{ev}_{\nu T}(v) = \Pi\left(\tilde{K}_v, [\nu v_1, \nu v_2, \dots, \nu v_n]\right)$ . Thus, Theorem 5.3 (c) yields

$$\text{ev}_{\mu T}(u) \hat{\cdot} \text{ev}_{\nu T}(v) = \Pi\left(\tilde{K}_{u,v}, [\mu u_i \cdot \nu v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}]\right).$$

Hence,  $\text{ev}_{\mu T}(u) \hat{\cdot} \text{ev}_{\nu T}(v) = \text{ev}_{\mu\nu T}(u \hat{\cdot} v)$ . This proves Theorem 5.7 (d).

(c) We can prove Theorem 5.7 (c) similarly to our above proof of Theorem 5.7 (d). However, there is also a much simpler proof of Theorem 5.7 (c): Since  $\text{ev}_{\mu T}$  is a ring homomorphism, we have  $\text{ev}_{\mu T}(u) \cdot \text{ev}_{\nu T}(v) = \text{ev}_{\mu T}(u \cdot v)$ . Since  $\hat{\cdot}$  is the multiplication on  $1 + K[[T]]^+$ , this rewrites as  $\text{ev}_{\mu T}(u) \hat{\cdot} \text{ev}_{\nu T}(v) = \text{ev}_{\mu T}(u \hat{\cdot} v)$ . This proves Theorem 5.7 (c).

(e) Since the maps  $\hat{\lambda}^k$  and  $\text{ev}_{\mu T}$  and  $\text{ev}_{\mu^k T}$  are continuous (by Theorem 5.5 (d) and Theorem 5.7 (a)), and  $1 + K[[T]]^+$  is a dense subset of  $1 + K[[T]]^+$  (by Theorem 5.5 (a)), this needs only to be shown for all  $u \in 1 + K[[T]]^+$ . So, from now on we assume that  $u \in 1 + K[[T]]^+$ . Then, there exists some  $(\tilde{K}_u, [u_1, u_2, \dots, u_m]) \in K^{\text{int}}$  such that  $u = \Pi\left(\tilde{K}_u, [u_1, u_2, \dots, u_m]\right)$ . Theorem 5.3 (d) then yields

$$\hat{\lambda}^k(u) = \Pi\left(\tilde{K}_u, \left[\prod_{i \in I} u_i \mid I \in \mathcal{P}_k(\{1, 2, \dots, m\})\right]\right) = \prod_{I \in \mathcal{P}_k(\{1, 2, \dots, m\})} \left(1 + \prod_{i \in I} u_i \cdot T\right),$$

so that

$$\begin{aligned} \text{ev}_{\mu^k T}(\hat{\lambda}^k(u)) &= \prod_{I \in \mathcal{P}_k(\{1, 2, \dots, m\})} \left(1 + \prod_{i \in I} u_i \cdot \mu^k T\right) = \prod_{I \in \mathcal{P}_k(\{1, 2, \dots, m\})} \left(1 + \prod_{i \in I} (\mu u_i) \cdot T\right) \\ &= \Pi\left(\tilde{K}_u, \left[\prod_{i \in I} (\mu u_i) \mid I \in \mathcal{P}_k(\{1, 2, \dots, m\})\right]\right). \end{aligned}$$

On the other hand, Theorem 5.7 (b) yields  $\text{ev}_{\mu T}(u) = \Pi\left(\tilde{K}_u, [\mu u_1, \mu u_2, \dots, \mu u_m]\right)$  and thus, by Theorem 5.3 (d) again,

$$\hat{\lambda}^k(\text{ev}_{\mu T}(u)) = \Pi\left(\tilde{K}_u, \left[\prod_{i \in I} (\mu u_i) \mid I \in \mathcal{P}_k(\{1, 2, \dots, m\})\right]\right),$$

so that we conclude  $\hat{\lambda}^k(\text{ev}_{\mu T}(u)) = \text{ev}_{\mu^k T}(\hat{\lambda}^k(u))$ , and Theorem 5.7 (e) is proven.  $\square$

## 5.9. The functor $\Lambda$

Finally, a small definition that turns  $\Lambda$  into a functor:

**Definition.** Every homomorphism  $\varphi : K \rightarrow L$  of rings canonically induces a  $\lambda$ -ring homomorphism  $\Lambda(K) \rightarrow \Lambda(L)$  (which sends every  $\sum_{i \in \mathbb{N}} a_i T^i \in \Lambda(K)$  to  $\sum_{i \in \mathbb{N}} \varphi(a_i) T^i \in \Lambda(L)$ ). This homomorphism  $\Lambda(K) \rightarrow \Lambda(L)$  will be denoted by  $\Lambda(\varphi)$ .

It is easy to see that this  $\Lambda(\varphi)$  indeed is a  $\lambda$ -ring homomorphism.<sup>37</sup> Besides, it has some obvious properties: If  $\varphi$  is surjective, then so is  $\Lambda(\varphi)$ . If  $\varphi$  is injective, then  $\Lambda(\varphi)$  is injective as well; thus, if  $L$  is an extension ring of  $K$ , then  $\Lambda(L)$  can be canonically considered an extension ring of  $\Lambda(K)$ .

## 5.10. Exercises

*Exercise 5.1.* Let  $K$  be a ring. For every monic polynomial  $P \in K[T]$ , there exists a finite-free extension ring  $K_P$  of the ring  $K$  and  $n$  elements  $p_1, p_2, \dots, p_n$  of this extension ring  $K_P$  such that  $P = \prod_{i=1}^n (T - p_i)$  in  $K_P[T]$ , where  $n = \deg P$ .

[This exercise is a particular case of [Laksov09, Theorem 5.5], and (more generally) a simple corollary of Laksov's theory of splitting algebras.]

*Exercise 5.2.* Let  $L$  be a ring. Let  $n \in \mathbb{N}$ , let  $a_0, a_1, \dots, a_n$  be some elements of  $L$ , and let  $p_1, p_2, \dots, p_n$  be some elements of  $L$ .

(a) If  $\sum_{i=0}^n a_{n-i}T^i = \prod_{i=1}^n (p_i + T)$  in the polynomial ring  $L[T]$ , then prove that  $\sum_{i=0}^n a_iT^i = \prod_{i=1}^n (1 + p_iT)$ .

(b) If  $\sum_{i=0}^n a_iT^i = \prod_{i=1}^n (1 + p_iT)$  in the polynomial ring  $L[T]$ , then prove that  $\sum_{i=0}^n a_{n-i}T^i = \prod_{i=1}^n (p_i + T)$ .

*Exercise 5.3.* Let  $K$  be a ring. Let  $p$  be an element of  $K$ . Let  $P \in K[T]$  be a monic polynomial such that  $P(p) = 0$ . Let  $n = \deg P$ . Then, there exists a finite-free extension ring  $K'_P$  of the ring  $K$  and  $n$  elements  $p_1, p_2, \dots, p_n$  of this extension ring  $K'_P$  such that  $P = \prod_{i=1}^n (T - p_i)$  in  $K'_P[T]$  and such that  $p = p_n$ .

*Exercise 5.4.* Let  $K$  be a ring, and  $L$  an extension ring of  $K$ . For some  $n \in \mathbb{N}$ , an element  $u$  of  $L$  is said to be  $n$ -integral over  $K$  if there exists a monic polynomial  $P \in K[T]$  such that  $\deg P = n$  and  $P(u) = 0$ .

Let  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ . Let  $\alpha$  and  $\beta$  be two elements of  $L$  such that  $\alpha$  is  $n$ -integral over  $K$  and  $\beta$  is  $m$ -integral over  $K$ . Prove that  $\alpha\beta$  is  $nm$ -integral over  $K$ .

[This is a known fact, but it turns out to also be a corollary of our construction of the polynomials  $P_k$  further above.]

*Exercise 5.5.* Let  $K$  be a ring, and  $I$  be an ideal of  $K$ . Let  $I[[T]]$  denote the  $K$ -submodule

$$\left\{ \sum_{i \in \mathbb{N}} a_i T^i \in K[[T]] \mid a_i \in I \text{ for all } i \right\} \\ = \{p \in K[[T]] \mid p \text{ is a power series with all its coefficients lying in } I\}$$

<sup>37</sup>Basically, this is because the  $P_k$  and  $P_{k,j}$  are polynomials, and polynomials commute with ring homomorphisms.

of  $K[[T]]$ . Let  $I[[T]]^+$  denote the subset

$$TI[[T]] = \left\{ \sum_{i \in \mathbb{N}} a_i T^i \in I[[T]] \mid a_i \in I \text{ for all } i, \text{ and } a_0 = 0 \right\}$$

$$= \{p \in I[[T]] \mid p \text{ is a power series with constant term } 0\}$$

of  $I[[T]]$ . Consider the subset  $1 + I[[T]]^+$  of  $1 + K[[T]]^+ = \Lambda(K)$ .<sup>38</sup>  
Prove the following:

(a) We have  $1 + I[[T]]^+ = \text{Ker}(\Lambda(\pi))$ , where  $\pi$  is the canonical projection  $K \rightarrow K/I$ .

(b) The set  $1 + I[[T]]^+$  is a  $\lambda$ -ideal of the  $\lambda$ -ring  $\Lambda(K)$ .

## 6. Special $\lambda$ -rings

### 6.1. Definition

Now we will define a particular subclass of  $\lambda$ -rings that we will be interested in from now on:

**Definition. 1)** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. The map  $\lambda_T$  defined in Theorem 5.6 is an additive group homomorphism (by Theorem 5.6). We call  $(K, (\lambda^i)_{i \in \mathbb{N}})$  a *special  $\lambda$ -ring* if this map  $\lambda_T : (K, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism.

**2)** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $L$  be a sub- $\lambda$ -ring of  $K$ . If  $(L, (\lambda^i|_L)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring, then we call  $L$  a *special sub- $\lambda$ -ring* of  $K$ .

A different, more down-to-earth characterization of special  $\lambda$ -rings:

**Theorem 6.1.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring.

Then,  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring if and only if

$$\lambda^k(xy) = P_k(\lambda^1(x), \lambda^2(x), \dots, \lambda^k(x), \lambda^1(y), \lambda^2(y), \dots, \lambda^k(y))$$

for every  $k \in \mathbb{N}$ ,  $x \in K$  and  $y \in K$  (26)

and

$$\lambda^k(\lambda^j(x)) = P_{k,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^{kj}(x))$$

for every  $k \in \mathbb{N}$ ,  $j \in \mathbb{N}$  and  $x \in K$ . (27)

*Proof of Theorem 6.1.* According to the preceding definition,  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring if and only if the map  $\lambda_T$  is a  $\lambda$ -ring homomorphism. This map is always an

---

<sup>38</sup>Notice that  $I[[T]]^+ \neq I \cdot (K[[T]]^+)$  in general!



additive group homomorphism (by Theorem 5.6); hence, it is a  $\lambda$ -ring homomorphism if and only if it satisfies the three conditions

$$\begin{aligned} \lambda_T(xy) &= \lambda_T(x) \widehat{\cdot} \lambda_T(y) && \text{for every } x \in K \text{ and } y \in K, \\ \lambda_T(1) &= 1 + T, && \text{and} \\ \lambda_T(\lambda^j(x)) &= \widehat{\lambda}^j(\lambda_T(x)) && \text{for every } j \in \mathbb{N} \text{ and } x \in K \end{aligned}$$

(note that  $1 + T$  is the multiplicative unity of  $\Lambda(K)$ ). The second of these three conditions actually follows from the third one (since  $\lambda_T(\lambda^j(x)) = \widehat{\lambda}^j(\lambda_T(x))$ , applied to  $j = 0$ , yields  $\lambda_T(1) = 1 + T$ ), so we see that the map  $\lambda_T$  is a  $\lambda$ -ring homomorphism if and only if it satisfies the two conditions

$$\begin{aligned} \lambda_T(xy) &= \lambda_T(x) \widehat{\cdot} \lambda_T(y) && \text{for every } x \in K \text{ and } y \in K, && \text{and} \\ \lambda_T(\lambda^j(x)) &= \widehat{\lambda}^j(\lambda_T(x)) && \text{for every } j \in \mathbb{N} \text{ and } x \in K. \end{aligned}$$

But these two conditions are equivalent to (26) and (27), respectively (because of the definitions of  $\widehat{\cdot}$  and  $\widehat{\lambda}^j$  and because two formal power series are equal if and only if their respective coefficients are equal). This proves Theorem 6.1.  $\square$

## 6.2. $\Lambda(K)$ is special

**Theorem 6.2 (Grothendieck).** Let  $K$  be a ring. Then,  $\left(\Lambda(K), \left(\widehat{\lambda}^i\right)_{i \in \mathbb{N}}\right)$  is a special  $\lambda$ -ring.

*Proof of Theorem 6.2.* According to Theorem 6.1, we only have to prove that

$$\begin{aligned} \widehat{\lambda}^k(u \widehat{\cdot} v) &= \widehat{P}_k \left( \widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^k(u), \widehat{\lambda}^1(v), \widehat{\lambda}^2(v), \dots, \widehat{\lambda}^k(v) \right) \\ &\text{for every } k \in \mathbb{N}, u \in \Lambda(K) \text{ and } v \in \Lambda(K), \end{aligned} \tag{28}$$

and

$$\begin{aligned} \widehat{\lambda}^k \left( \widehat{\lambda}^j(u) \right) &= \widehat{P}_{k,j} \left( \widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^{kj}(u) \right) \\ &\text{for every } k \in \mathbb{N}, j \in \mathbb{N} \text{ and } u \in \Lambda(K). \end{aligned} \tag{29}$$

Here, we are using the following *notation*: If  $S \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_{kj}]$  is a polynomial, then  $\widehat{S} \left( \widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^{kj}(u) \right)$  denotes the polynomial  $S$  applied to  $\widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^{kj}(u)$  as elements of the ring  $\Lambda(K)$  (and not as elements of the ring  $K[[T]]$ ). For instance, if  $S = \alpha_1 + \alpha_2 + \dots + \alpha_{kj}$ , then  $\widehat{S} \left( \widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^{kj}(u) \right)$  means  $\widehat{\lambda}^1(u) \widehat{+} \widehat{\lambda}^2(u) \widehat{+} \dots \widehat{+} \widehat{\lambda}^{kj}(u)$  (and not  $\widehat{\lambda}^1(u) + \widehat{\lambda}^2(u) + \dots + \widehat{\lambda}^{kj}(u)$ , where  $+$  denotes the addition in the ring  $K[[T]]$ ). This explains how the right hand sides of the equations (28) and (29) should be understood.

Let us first prove (28): Since the subset  $1 + K[T]^+$  is dense in  $1 + K[[T]]^+ = \Lambda(K)$  (by Theorem 5.5 (a)), and since  $\widehat{\cdot}$  and  $\widehat{\lambda}^i$  are continuous (by Theorem 5.5 (d)), it will be enough to verify (28) for  $u \in 1 + K[T]^+$  and  $v \in 1 + K[T]^+$ . Then, there exist some  $\left( \widetilde{K}_u, [u_1, u_2, \dots, u_m] \right) \in K^{\text{int}}$  such that  $u = \Pi \left( \widetilde{K}, [u_1, u_2, \dots, u_m] \right)$ , and some

$(\tilde{K}_v, [v_1, v_2, \dots, v_n]) \in K^{\text{int}}$  such that  $v = \Pi(\tilde{K}, [v_1, v_2, \dots, v_n])$ . By Theorem 5.3 (a), there exists a finite-free extension ring  $\tilde{K}_{u,v}$  of  $K$  which contains both  $\tilde{K}_u$  and  $\tilde{K}_v$  as subrings. We replace  $K$  by  $\tilde{K}_{u,v}$  now (silently using the obvious fact that the injection  $K \rightarrow \tilde{K}_{u,v}$  canonically yields an injection  $\Lambda(K) \rightarrow \Lambda(\tilde{K}_{u,v})$ ). Hence, we can now assume that  $u_1, u_2, \dots, u_m, v_1, v_2, \dots, v_n$  all lie in  $K$ . Theorem 5.3 (c) yields  $u\hat{v} = \Pi(\tilde{K}_{u,v}, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}])$ . Since we identified  $\tilde{K}_{u,v}$  with  $K$ , this becomes

$$u\hat{v} = \Pi(K, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}]).$$

Thus, Theorem 5.3' (d) (applied to  $w = u\hat{v}$ ,  $\tilde{K} = K$ ,  $L = \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}$  and  $w_{(i,j)} = u_i v_j$ ) yields

$$\hat{\lambda}^k(u\hat{v}) = \Pi\left(K, \left[ \prod_{(i,j) \in S} u_i v_j \mid S \in \mathcal{P}_k(\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}) \right]\right).$$

There exists a ring homomorphism

$$\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n] \rightarrow \Lambda(K)$$

which maps  $U_i$  to  $1 + u_i T$  for every  $i$  and  $V_j$  to  $1 + v_j T$  for every  $j$ . This homomorphism maps  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  to

$$\begin{aligned} \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \widehat{\prod_{k \in S} (1 + u_k T)} &= \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \widehat{\prod_{k \in S} \Pi(K, [u_k])} = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \Pi\left(K, \left[ \prod_{k \in S} u_k \right]\right) \\ &= \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \Pi\left(K, \left[ \prod_{k \in S} u_k \right]\right) \\ &\quad \text{according to Corollary 5.4 (b)} \\ &= \Pi\left(K, \left[ \prod_{k \in S} u_k \mid S \subseteq \{1, 2, \dots, m\}; |S| = i \right]\right) \\ &= \Pi\left(K, \left[ \prod_{k \in S} u_k \mid S \in \mathcal{P}_i(\{1, 2, \dots, m\}) \right]\right) \\ &= \hat{\lambda}^i(u) \quad (\text{after Theorem 5.3 (d)}) \end{aligned}$$

and  $Y_j$  to  $\hat{\lambda}^j(v)$  for every  $j \in \mathbb{N}$  (according to a similar argument). Hence, applying this homomorphism to (20), we obtain

$$\begin{aligned} &\sum_{\substack{S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; \\ |S|=k}} \widehat{\prod_{(i,j) \in S} (1 + u_i T) \hat{\cdot} (1 + v_j T)} \\ &= \widehat{P}_k(\hat{\lambda}^1(u), \hat{\lambda}^2(u), \dots, \hat{\lambda}^k(u), \hat{\lambda}^1(v), \hat{\lambda}^2(v), \dots, \hat{\lambda}^k(v)). \end{aligned}$$

But combined with

$$\begin{aligned}
& \widehat{\sum}_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \widehat{\prod}_{(i,j) \in S} \underbrace{(1 + u_i T) \widehat{\cdot} (1 + v_j T)}_{\substack{= \Pi(K, [u_i]) \cdot \Pi(K, [v_j]) \\ = \Pi(K, [u_i v_j]) \text{ after} \\ \text{Theorem 5.3 (c)}}}} = \widehat{\sum}_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \underbrace{\widehat{\prod}_{(i,j) \in S} \Pi(K, [u_i v_j])}_{= \Pi\left(K, \left[ \prod_{(i,j) \in S} u_i v_j \right]\right)} \\
& = \widehat{\sum}_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \Pi\left(K, \left[ \prod_{(i,j) \in S} u_i v_j \right]\right) \\
& = \Pi\left(K, \left[ \prod_{(i,j) \in S} u_i v_j \mid S \subseteq \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}; |S| = k \right]\right) \\
& \quad \text{(after Corollary 5.4 (a))} \\
& = \Pi\left(K, \left[ \prod_{(i,j) \in S} u_i v_j \mid S \in \mathcal{P}_k(\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}) \right]\right) \\
& = \widehat{\lambda}^k(u \widehat{\cdot} v),
\end{aligned}$$

this yields

$$\widehat{\lambda}^k(u \widehat{\cdot} v) = \widehat{P}_k\left(\widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^k(u), \widehat{\lambda}^1(v), \widehat{\lambda}^2(v), \dots, \widehat{\lambda}^k(v)\right).$$

Thus, (28) is proven.

Next we are going to prove (29) (the argument will be similar to the above proof of (28)):

Since the subset  $1 + K[T]^+$  is dense in  $1 + K[[T]]^+ = \Lambda(K)$  (by Theorem 5.5 (a)), and since all the  $\widehat{\lambda}^i$  are continuous (by Theorem 5.5 (d)), it will be enough to verify (29) for the case  $u \in 1 + K[T]^+$ . But in this case, there exists some  $(\widetilde{K}_u, [u_1, u_2, \dots, u_m]) \in K^{\text{int}}$  such that  $u = \Pi(\widetilde{K}, [u_1, u_2, \dots, u_m])$ . By definition,  $\widetilde{K}_u$  is a finite-free extension of  $K$ .

We replace  $K$  by  $\widetilde{K}_u$  now (silently using the obvious fact that the injection  $K \rightarrow \widetilde{K}_u$  canonically yields an injection  $\Lambda(K) \rightarrow \Lambda(\widetilde{K}_u)$ ). Hence, we can now assume that  $u_1, u_2, \dots, u_m$  all lie in  $K$ . Theorem 5.3 (d) yields  $\widehat{\lambda}^j(u) = \Pi\left(\widetilde{K}_u, \left[ \prod_{i \in I} u_i \mid I \in \mathcal{P}_j(\{1, 2, \dots, m\}) \right]\right)$ .

Since we identified  $\widetilde{K}_{u,v}$  with  $K$ , this becomes

$$\widehat{\lambda}^j(u) = \Pi\left(K, \left[ \prod_{i \in I} u_i \mid I \in \mathcal{P}_j(\{1, 2, \dots, m\}) \right]\right).$$

Thus, Theorem 5.3' (d) (applied to  $w = \widehat{\lambda}^j(u)$ ,  $\widetilde{K} = K$ ,  $L = \mathcal{P}_j(\{1, 2, \dots, m\})$  and  $w_I = \prod_{i \in I} u_i$ ) yields

$$\widehat{\lambda}^k(\widehat{\lambda}^j(u)) = \Pi\left(K, \left[ \prod_{I \in S} \prod_{i \in I} u_i \mid S \in \mathcal{P}_k(\mathcal{P}_j(\{1, 2, \dots, m\})) \right]\right).$$

There exists a ring homomorphism

$$\mathbb{Z}[U_1, U_2, \dots, U_m] \rightarrow \Lambda(K)$$

which maps  $U_i$  to  $1+u_iT$  for every  $i$ . This homomorphism maps  $X_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k$

to  $\widehat{\lambda}^i(u)$ <sup>39</sup>. Hence, applying this homomorphism to (22), we obtain

$$\sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \widehat{\prod_{i \in S} \prod_{i \in I} (1+u_iT)} = \widehat{P_{k,j}}(\widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^{kj}(u)).$$

But combined with

$$\begin{aligned} \sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \widehat{\prod_{I \in S} \prod_{i \in I} (1+u_iT)} &= \sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \widehat{\prod_{I \in S} \Pi \left( K, \left[ \prod_{i \in I} u_i \right] \right)} \\ &= \sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \widehat{\prod_{I \in S} \Pi \left( K, \left[ \prod_{i \in S} \prod_{i \in I} u_i \right] \right)} \\ &= \sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=k}} \widehat{\Pi \left( K, \left[ \prod_{I \in S} \prod_{i \in I} u_i \right] \right)} \\ &= \widehat{\Pi \left( K, \left[ \prod_{I \in S} \prod_{i \in I} u_i \mid S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); |S|=k \right] \right)} \\ &\quad \text{(after Corollary 5.4 (a))} \\ &= \widehat{\Pi \left( K, \left[ \prod_{I \in S} \prod_{i \in I} u_i \mid S \in \mathcal{P}_k(\mathcal{P}_j(\{1,2,\dots,m\})) \right] \right)} \\ &= \widehat{\lambda}^k(\widehat{\lambda}^j(u)), \end{aligned}$$

this becomes

$$\widehat{\lambda}^k(\widehat{\lambda}^j(u)) = \widehat{P_{k,j}}(\widehat{\lambda}^1(u), \widehat{\lambda}^2(u), \dots, \widehat{\lambda}^{kj}(u)).$$

Thus, we have verified (29). Theorem 6.2 is thus proven.  $\square$

Theorem 6.1 gives us an alternative definition of special  $\lambda$ -rings via the polynomials  $P_k$  and  $P_{k,j}$ . Why, then, did we define the notion of special  $\lambda$ -rings via the map  $\lambda_T : (K, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  rather than using Theorem 6.1? The reason is that while Theorem 6.1 provides an easy-to-formulate definition of special  $\lambda$ -rings, it is

<sup>39</sup>This can be proven exactly in the same way as we have showed, during the proof of (28), that the ring homomorphism

$$\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n] \rightarrow \Lambda(K)$$

which maps  $U_i$  to  $1+u_iT$  for every  $i$  and  $V_j$  to  $1+v_jT$  for every  $j$  must map  $X_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k$

to  $\widehat{\lambda}^i(u)$  (where the notations are the ones we introduced in our above proof of (28)).

rather hard to work with. In order to check that some given ring is a special  $\lambda$ -ring using Theorem 6.1, we would have to prove the identities (26) and (27), which is a difficult task since the polynomials  $P_k$  and  $P_{k,j}$  are very hard to compute explicitly. Using the definition that we gave, we would instead have to check that  $\lambda_T : (K, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism, and this is often easier since Exercise 2.1 reduces this to checking some identity at  $\mathbb{Z}$ -module generators of  $K$ .

### 6.3. Exercises

*Exercise 6.1.* Let  $K$  be a ring. Consider the localization  $(1 + K[T]^+)^{-1} K[T]$  of the polynomial ring  $K[T]$  at the multiplicatively closed subset  $1 + K[T]^+$ .

<sup>40</sup> This localization  $(1 + K[T]^+)^{-1} K[T]$  can be considered a subring of  $K[[T]]$  (since  $K[T] \subseteq K[[T]]$ , and every element of  $1 + K[T]^+$  is invertible in  $K[[T]]$ ). Prove that the set  $(1 + K[T]^+)^{-1} K[T] \cap \Lambda(K)$  is a special sub- $\lambda$ -ring of  $\Lambda(K)$ .

*Exercise 6.2.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring. Then, prove that:

(a) Every  $n \in \mathbb{Z}$  and  $i \in \mathbb{N}$  satisfy  $\lambda^i(n \cdot 1) = \binom{n}{i} \cdot 1$ , where 1 denotes the unity of the ring  $K$ .

(b) None of the elements 1, 2, 3, ... of the ring  $K$  equals zero in  $K$ , unless  $K$  is the trivial ring.

*Exercise 6.3.* Consider the ring  $\mathbb{Z}[X] / (X^2, 2X) = \mathbb{Z}[x]$ , where  $x$  denotes the residue class of  $X$  modulo the ideal  $(X^2, 2X)$ .

Define a map  $\lambda_T : \mathbb{Z}[x] \rightarrow (\mathbb{Z}[x])[[T]]$  by  $\lambda_T(a + bx) = (1 + T)^a (1 + xT)^b$  for every  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}$ .

Define a map  $\lambda^i : \mathbb{Z}[x] \rightarrow \mathbb{Z}[x]$  for every  $i \in \mathbb{N}$  through the condition  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$  for every  $x \in \mathbb{Z}[x]$ .

Prove that  $(\mathbb{Z}[x], (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring. [This way, we see that the additive group of a special  $\lambda$ -ring needs not be torsion-free.]

*Exercise 6.4.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $E$  be a generating set of the  $\mathbb{Z}$ -module  $K$ .

Prove that the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special if and only if it satisfies

$$\lambda^k(xy) = P_k(\lambda^1(x), \lambda^2(x), \dots, \lambda^k(x), \lambda^1(y), \lambda^2(y), \dots, \lambda^k(y))$$

for every  $k \in \mathbb{N}$ ,  $x \in E$  and  $y \in E$  (30)

---

<sup>40</sup>When  $K$  is a field, this localization is simply the (local) ring of the (so-called) rational functions in one variable over  $K$  which have no pole at 0. (Note that the term “rational function” is being used here for an element of the quotient field  $\text{Quot}(K[T])$ . This is the standard meaning that the term “rational function” has in modern literature. This meaning is somewhat confusing: In fact, rational functions are not functions in the standard meaning of this word; they *induce* functions (although no functions on  $K$ , but instead only functions on an open subset of  $K$ ), but even these induced functions don’t determine them uniquely, so the word “function” in “rational function” should not be taken literally. However, lacking a better word, everybody keeps calling the elements of  $\text{Quot}(K[T])$  “rational functions”, and so do I.)

and

$$\begin{aligned} \lambda^k(\lambda^j(x)) &= P_{k,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^{kj}(x)) \\ &\text{for every } k \in \mathbb{N}, j \in \mathbb{N} \text{ and } x \in E. \end{aligned} \quad (31)$$

*Exercise 6.5.* Let  $K$  be a ring. Let  $i \in \mathbb{N}$ . Define a mapping  $\text{coeff}_i : \Lambda(K) \rightarrow K$  by setting

$$\left( \begin{array}{l} \text{coeff}_i \left( \sum_{j \in \mathbb{N}} a_j T^j \right) = a_i \\ \text{for every } \sum_{j \in \mathbb{N}} a_j T^j \in \Lambda(K) \text{ (with } a_j \in K \text{ for every } j \in \mathbb{N}) \end{array} \right).$$

(In other words,  $\text{coeff}_i$  is the mapping that takes a power series and returns its coefficient before  $T^i$ .)

Prove that

$$\text{coeff}_i(u) = \text{coeff}_1(\widehat{\lambda}^i(u)) \quad \text{for every } u \in \Lambda(K).$$

*Exercise 6.6.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring, and  $A$  be a ring. Let  $\varphi : K \rightarrow A$  be a ring homomorphism, and let  $\text{coeff}_1^A : \Lambda(A) \rightarrow A$  be the mapping defined by  $\text{coeff}_1^A \left( \sum_{j \in \mathbb{N}} a_j T^j \right) = a_1$  for every  $\sum_{j \in \mathbb{N}} a_j T^j \in \Lambda(A)$  (with  $a_j \in A$  for every  $j \in \mathbb{N}$ ). (In other words,  $\text{coeff}_1^A$  is the mapping that takes a power series and returns its coefficient before  $T^1$ .)

As Theorem 5.1 (b) states,  $(\Lambda(A), (\widehat{\lambda}_A^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring, where the maps  $\widehat{\lambda}_A^i : \Lambda(A) \rightarrow \Lambda(A)$  are defined in the same way as the maps  $\widehat{\lambda}^i : \Lambda(K) \rightarrow \Lambda(K)$  (which we have defined in Section 5) but for the ring  $A$  instead of  $K$ .

Prove that there exists one and only one  $\lambda$ -ring homomorphism  $\widetilde{\varphi} : K \rightarrow \Lambda(A)$  such that  $\text{coeff}_1^A \circ \widetilde{\varphi} = \varphi$ .

*Exercise 6.7.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring, and  $I$  be an ideal of  $K$ . Let  $S$  be a subset of  $I$  which generates the ideal  $I$ . Assume that every  $s \in S$  and every positive integer  $i$  satisfy  $\lambda^i(s) \in I$ . Then, prove that  $I$  is a  $\lambda$ -ideal of  $K$ .

*Exercise 6.8.* Let  $K$  be a ring. For every  $i \in \mathbb{N}$ , we define a mapping  $\text{Coeff}_i : K[[T]] \rightarrow K$  by setting

$$\left( \begin{array}{l} \text{Coeff}_i(P) = (\text{the coefficient of } P \text{ before } T^i) \\ \text{for every power series } P \in K[[T]] \end{array} \right)$$

<sup>41</sup>. (In other words,  $\text{Coeff}_i$  is the mapping that takes a power series and returns its coefficient before  $T^i$ .) <sup>42</sup>

<sup>41</sup>Equivalently,  $\text{Coeff}_i \left( \sum_{j \in \mathbb{N}} a_j T^j \right) = a_i$  for every  $\sum_{j \in \mathbb{N}} a_j T^j \in K[[T]]$  (with  $a_j \in K$  for every  $j \in \mathbb{N}$ ).

<sup>42</sup>Note that we are denoting this mapping by  $\text{Coeff}_i$  with a capital ‘‘C’’ to distinguish it from the mapping  $\text{coeff}_i$  defined in Exercise 6.5. This distinction is necessary because these two mappings have different domains (namely, the map  $\text{Coeff}_i$  is defined on all of  $K[[T]]$ , whereas the map  $\text{coeff}_i$  is defined only on  $\Lambda(K)$ ).

Let  $m \in \mathbb{N}$ . For every  $i \in \{1, 2, \dots, m\}$ , let  $\Phi_i \in K[[T]]$  be a power series.

(a) We have  $\text{Coeff}_0 \left( \prod_{i=1}^m \Phi_i \right) = \prod_{i=1}^m \text{Coeff}_0(\Phi_i)$ .

(b) Assume that  $\text{Coeff}_0(\Phi_i) = 1$  for every  $i \in \{1, 2, \dots, m\}$ . Then,  $\text{Coeff}_0 \left( \prod_{i=1}^m \Phi_i \right) = 1$  and  $\text{Coeff}_1 \left( \prod_{i=1}^m \Phi_i \right) = \sum_{i=1}^m \text{Coeff}_1(\Phi_i)$ .

*Exercise 6.9.* Let  $K$  be a ring. For each  $i \in \mathbb{N}$ , define the mapping  $\text{coeff}_i : \Lambda(K) \rightarrow K$  as in Exercise 6.5. Then, show that  $\text{coeff}_1 : \Lambda(K) \rightarrow K$  is a ring homomorphism<sup>43</sup>.

*Exercise 6.10.* In this exercise, the  $\otimes$  sign shall always mean  $\otimes_{\mathbb{Z}}$ . Let  $A$ ,  $B$  and  $C$  be three rings. Let  $\iota_1 : A \rightarrow A \otimes B$  be the ring homomorphism sending each  $a \in A$  to  $a \otimes 1 \in A \otimes B$ . Let  $\iota_2 : B \rightarrow A \otimes B$  be the ring homomorphism sending each  $b \in B$  to  $1 \otimes b \in A \otimes B$ . Let  $\alpha : A \rightarrow C$  and  $\beta : B \rightarrow C$  be two  $\mathbb{Z}$ -module homomorphisms.

(a) There exists a unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow C$  satisfying

$$(\phi(a \otimes b) = \alpha(a) \beta(b) \quad \text{for every } (a, b) \in A \times B).$$

(b) Assume that  $\alpha$  and  $\beta$  are ring homomorphisms. Consider the unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow C$  constructed in Exercise 6.10 (a). Then, this  $\phi$  is a ring homomorphism and satisfies  $\phi \circ \iota_1 = \alpha$  and  $\phi \circ \iota_2 = \beta$ .

[This exercise is not directly related to  $\lambda$ -rings; it is just a mostly trivial fact that will be cited in the next exercise.]

*Exercise 6.11.* In this exercise, the  $\otimes$  sign shall always mean  $\otimes_{\mathbb{Z}}$ . Let  $(A, (\lambda^i)_{i \in \mathbb{N}})$  and  $(B, (\mu^i)_{i \in \mathbb{N}})$  be two  $\lambda$ -rings. Define a map  $\lambda_T : A \rightarrow \Lambda(A)$  by

$$\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \quad \text{for every } x \in A.$$

Define a map  $\mu_T : B \rightarrow \Lambda(B)$  by

$$\mu_T(x) = \sum_{i \in \mathbb{N}} \mu^i(x) T^i \quad \text{for every } x \in B.$$

Notice that  $\lambda_T$  is an additive group homomorphism from  $A$  to  $\Lambda(A)$  (by Theorem 5.6, applied to  $A$  instead of  $K$ ), and thus a  $\mathbb{Z}$ -module homomorphism. Similarly,  $\mu_T$  is a  $\mathbb{Z}$ -module homomorphism.

Let  $\iota_1 : A \rightarrow A \otimes B$  be the ring homomorphism sending each  $a \in A$  to  $a \otimes 1 \in A \otimes B$ . Let  $\iota_2 : B \rightarrow A \otimes B$  be the ring homomorphism sending each  $b \in B$  to  $1 \otimes b \in A \otimes B$ . The ring homomorphisms  $\iota_1 : A \rightarrow A \otimes B$  and  $\iota_2 : B \rightarrow A \otimes B$  canonically induce  $\lambda$ -ring homomorphisms  $\Lambda(\iota_1) : \Lambda(A) \rightarrow \Lambda(A \otimes B)$  and  $\Lambda(\iota_2) : \Lambda(B) \rightarrow \Lambda(A \otimes B)$  (since  $\Lambda$  is a functor). Exercise 6.10 (a) (applied to  $C = \Lambda(A \otimes B)$ ,  $\alpha = \Lambda(\iota_1) \circ \lambda_T$  and  $\beta = \Lambda(\iota_2) \circ \mu_T$ ) thus yields that there exists a unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow \Lambda(A \otimes B)$  satisfying

$$\left( \begin{array}{l} \phi(a \otimes b) = (\Lambda(\iota_1) \circ \lambda_T)(a) \widehat{\cdot} (\Lambda(\iota_2) \circ \mu_T)(b) \\ \text{for every } (a, b) \in A \times B \end{array} \right).$$

---

<sup>43</sup>but, generally, not a  $\lambda$ -ring homomorphism, even when  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring!

Let us denote this  $\phi$  by  $\tau_T$ . For every  $i \in \mathbb{N}$ , we define a map  $\tau^i : A \otimes B \rightarrow A \otimes B$  as follows: For every  $c \in A \otimes B$ , let  $\tau^i(c)$  be the coefficient of the power series  $\tau_T(c) \in \Lambda(A \otimes B) \subseteq (A \otimes B)[[T]]$  before  $T^i$ . Prove the following facts:

(a) The pair  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring.

(b) If  $(C, (\nu^i)_{i \in \mathbb{N}})$  is a **special**  $\lambda$ -ring, and if  $\alpha : (A, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (C, (\nu^i)_{i \in \mathbb{N}})$  and  $\beta : (B, (\mu^i)_{i \in \mathbb{N}}) \rightarrow (C, (\nu^i)_{i \in \mathbb{N}})$  are two  $\lambda$ -ring homomorphisms, then the unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow C$  constructed in Exercise 6.10 (a) is a  $\lambda$ -ring homomorphism  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}}) \rightarrow (C, (\nu^i)_{i \in \mathbb{N}})$ .

(c) Assume that the  $\lambda$ -rings  $(A, (\lambda^i)_{i \in \mathbb{N}})$  and  $(B, (\mu^i)_{i \in \mathbb{N}})$  are special. Then, the map  $\iota_1$  is a  $\lambda$ -ring homomorphism from  $(A, (\lambda^i)_{i \in \mathbb{N}})$  to  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$ , and the map  $\iota_2$  is a  $\lambda$ -ring homomorphism from  $(B, (\mu^i)_{i \in \mathbb{N}})$  to  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$ .

(d) Assume that the  $\lambda$ -rings  $(A, (\lambda^i)_{i \in \mathbb{N}})$  and  $(B, (\mu^i)_{i \in \mathbb{N}})$  are special. Then, the  $\lambda$ -ring  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$  is special.

## 7. Examples of special $\lambda$ -rings

### 7.1. Binomial $\lambda$ -rings

We have learned a lot of examples for  $\lambda$ -rings, but which of them are special? Of course, the trivial ring  $0$  with the trivial maps  $\lambda^i : 0 \rightarrow 0$  is a special  $\lambda$ -ring. Also, we know a vast class of special  $\lambda$ -rings from Theorem 6.2. Obviously, every sub- $\lambda$ -ring of a special  $\lambda$ -ring is special. On the other hand, the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  defined in Exercise 3.3 (a) is not special unless  $p = 1$ . What happens to the other examples from Section 3?

**Theorem 7.1.** The  $\lambda$ -ring  $(\mathbb{Z}, (\lambda^i)_{i \in \mathbb{N}})$  defined in Theorem 3.1 is special.

*Proof of Theorem 7.1.* According to Theorem 6.1, we just have to verify the identities (26) and (27) for  $K = \mathbb{Z}$ . In other words, we have to prove that

$$\binom{xy}{k} = P_k \left( \binom{x}{1}, \binom{x}{2}, \dots, \binom{x}{k}, \binom{y}{1}, \binom{y}{2}, \dots, \binom{y}{k} \right) \quad (32)$$

for every  $k \in \mathbb{N}$ ,  $x \in \mathbb{Z}$  and  $y \in \mathbb{Z}$  and

$$\binom{\binom{x}{j}}{k} = P_{k,j} \left( \binom{x}{1}, \binom{x}{2}, \dots, \binom{x}{kj} \right) \quad (33)$$

for every  $k \in \mathbb{N}$ ,  $j \in \mathbb{N}$  and  $x \in \mathbb{Z}$ .

Let us prove (32): Fix  $k \in \mathbb{N}$ . Then, (32) is a polynomial identity in  $x$  and in  $y$ . Hence, (for the same reason as in the proof of Theorem 3.1) it is enough to prove (32) for all natural  $x$  and  $y$ . In this case, let  $m = x$  and  $n = y$ . There exists a ring homomorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m, V_1, V_2, \dots, V_n] \rightarrow \mathbb{Z}$  mapping every  $U_i$  to 1 and every  $V_j$  to 1. This homomorphism maps  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  to

$$\sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{\substack{k \in S \\ =1}} 1 = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} 1 = \sum_{S \in \mathcal{P}_i(\{1, 2, \dots, m\})} 1 = |\mathcal{P}_i(\{1, 2, \dots, m\})| = \binom{m}{i}$$



for every  $i \in \mathbb{N}$ , and (for similar reasons) maps  $Y_j$  to  $\binom{n}{j}$  for every  $j \in \mathbb{N}$ . Thus, applying this homomorphism to the polynomial identity (20), we obtain

$$\sum_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \prod_{(i,j) \in S} 1 \cdot 1 = P_k \left( \binom{m}{1}, \binom{m}{2}, \dots, \binom{m}{k}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{k} \right).$$

Since  $m = x$ ,  $n = y$  and

$$\begin{aligned} \sum_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} \underbrace{\prod_{(i,j) \in S} 1 \cdot 1}_{=1} &= \sum_{\substack{S \subseteq \{1,2,\dots,m\} \times \{1,2,\dots,n\}; \\ |S|=k}} 1 = \sum_{S \in \mathcal{P}_k(\{1,2,\dots,m\} \times \{1,2,\dots,n\})} 1 \\ &= |\mathcal{P}_k(\{1,2,\dots,m\} \times \{1,2,\dots,n\})| = \binom{mn}{k} = \binom{xy}{k}, \end{aligned}$$

this equality transforms into (32). Hence, (32) is proven (since, as we said, once (32) is proven for natural  $x$  and  $y$ , it follows that (32) holds for all integers  $x$  and  $y$ ). Just as we have derived (32) from (20), we can derive (33) from (22), and Theorem 7.1 is proven.  $\square$

Theorem 7.1 generalizes to the following fact:

**Theorem 7.2.** Let  $K$  be a binomial ring. The  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  defined in Theorem 3.2 is special.

*Proof of Theorem 7.2.* This follows from our proof of Theorem 7.1 in the same way as Theorem 3.2 followed from our proof of Theorem 3.1. To be more precise: According to Theorem 6.1, the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special if it satisfies the identities (26) and (27). This means (32) for every  $k \in \mathbb{N}$ ,  $x \in K$  and  $y \in K$  and (33) for every  $k \in \mathbb{N}$ ,  $j \in \mathbb{N}$  and  $x \in K$ . In the proof of Theorem 7.1, we have proven these identities for all  $x \in \mathbb{Z}$  and  $y \in \mathbb{Z}$ ; but being polynomial identities (for fixed  $k$  and  $j$ ), these identities therefore also hold for every  $x \in K$  and  $y \in K$ , and Theorem 7.2 is proven.  $\square$

## 7.2. Adjoining a polynomial variable to a $\lambda$ -ring

Theorem 3.3 has a special version as well:

**Theorem 7.3.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring. Then, the  $\lambda$ -ring  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  defined in Theorem 3.3 is special.

*Proof of Theorem 7.3.* As in the proof of Theorem 3.3, we can define a map  $\bar{\lambda}_T : K[S] \rightarrow (K[S])[T]$  by

$$\bar{\lambda}_T(u) = \sum_{i \in \mathbb{N}} \bar{\lambda}^i(u) T^i \quad \text{for every } u \in K[S].$$

Noting that  $\bar{\lambda}_T(u) \in \Lambda(K[S])$  for every  $u \in K[S]$  (since  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring), we see that we can actually consider  $\bar{\lambda}_T$  as a map  $K[S] \rightarrow \Lambda(K[S])$ .

Theorem 5.6 (applied to  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  and  $\bar{\lambda}_T$  instead of  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and  $\lambda_T$ ) yields that the map  $\bar{\lambda}_T$  is an additive group homomorphism. In order to show that the  $\lambda$ -ring  $(K[S], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  is special, we must prove that this map  $\bar{\lambda}_T$  is a  $\lambda$ -ring homomorphism.

Observe that  $\lambda_T$  is a  $\lambda$ -ring homomorphism (as  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring). In particular,  $\lambda_T$  is a ring homomorphism. Thus,  $\lambda_T$  maps the unity 1 of the ring  $K$  to the unity  $1 + T$  of the ring  $\Lambda(K)$ . In other words,  $\lambda_T(1) = 1 + T$ .

Let  $E = \{aS^\alpha \mid a \in K, \alpha \in \mathbb{N}\}$ . Obviously,  $E$  is a generating set of the  $\mathbb{Z}$ -module  $K[S]$ . Notice that

$$\bar{\lambda}_T(aS^\alpha) = \lambda_{S^\alpha T}(a) \quad (34)$$

for every  $a \in K$  and  $\alpha \in \mathbb{N}$  (as shown in the proof of Theorem 3.3 (b)). Applying this to  $a = 1$  and  $\alpha = 0$ , we obtain

$$\bar{\lambda}_T(1S^0) = \lambda_{S^0 T}(1) = \lambda_T(1) = 1 + T.$$

In other words,  $\bar{\lambda}_T(1) = 1 + T$  (since  $1S^0 = 1$ ).

For every  $a \in K$ ,  $\alpha \in \mathbb{N}$ ,  $b \in K$  and  $\beta \in \mathbb{N}$ , we have

$$\begin{aligned} & \underbrace{\bar{\lambda}_T(aS^\alpha)}_{\substack{= \lambda_{S^\alpha T}(a) \\ \text{(by (34))}}} \hat{\cdot} \underbrace{\bar{\lambda}_T(bS^\beta)}_{\substack{= \lambda_{S^\beta T}(b) \\ \text{(by (34), applied to} \\ \text{b and } \beta \text{ instead of a and } \alpha)}} \\ &= \underbrace{\lambda_{S^\alpha T}(a)}_{= \text{ev}_{S^\alpha T}(\lambda_T(a))} \hat{\cdot} \underbrace{\lambda_{S^\beta T}(b)}_{= \text{ev}_{S^\beta T}(\lambda_T(b))} \\ & \quad \left( \text{since } \bar{\lambda}_T(aS^\alpha) = \lambda_{S^\alpha T}(a) \text{ and similarly } \bar{\lambda}_T(bS^\beta) = \lambda_{S^\beta T}(b) \right) \\ &= \text{ev}_{S^\alpha T}(\lambda_T(a)) \hat{\cdot} \text{ev}_{S^\beta T}(\lambda_T(b)) = \text{ev}_{S^\alpha S^\beta T} \left( \underbrace{\lambda_T(a) \hat{\cdot} \lambda_T(b)}_{\substack{= \lambda_T(ab) \\ \text{(since } \lambda_T \text{ is a ring} \\ \text{homomorphism)}}} \right) \\ & \quad \left( \text{by Theorem 5.7 (d), applied to } K[S], \lambda_T(a), \lambda_T(b), S^\alpha \text{ and } S^\beta \right. \\ & \quad \left. \text{instead of } K, u, v, \mu \text{ and } \nu \right) \\ &= \text{ev}_{S^\alpha S^\beta T}(\lambda_T(ab)) = \lambda_{S^\alpha S^\beta T}(ab) = \lambda_{S^{\alpha+\beta} T}(ab) = \bar{\lambda}_T \left( \underbrace{ab \cdot S^{\alpha+\beta}}_{= aS^\alpha \cdot bS^\beta} \right) \\ & \quad \left( \text{since } \bar{\lambda}_T(ab \cdot S^{\alpha+\beta}) = \lambda_{S^{\alpha+\beta} T}(ab) \text{ (by (34), applied to} \right. \\ & \quad \left. ab \text{ and } \alpha + \beta \text{ instead of } a \text{ and } b) \right) \\ &= \bar{\lambda}_T(aS^\alpha \cdot bS^\beta). \end{aligned}$$

In other words,  $\bar{\lambda}_T(e) \hat{\cdot} \bar{\lambda}_T(f) = \bar{\lambda}_T(e f)$  for any two elements  $e$  and  $f$  of  $E$ . Since  $E$  is a generating set of the  $\mathbb{Z}$ -module  $K[S]$ , and since  $\bar{\lambda}_T$  is already known to be an additive group homomorphism, it thus follows that  $\bar{\lambda}_T(x) \hat{\cdot} \bar{\lambda}_T(y) = \bar{\lambda}_T(xy)$  for any two elements  $x$  and  $y$  of  $K[S]$ . Since  $\bar{\lambda}_T$  also maps the multiplicative unity 1 of  $K[S]$

to the multiplicative unity  $1 + T$  of  $\Lambda(K[S])$  (because  $\bar{\lambda}_T(1) = 1 + T$ ), it thus follows that  $\bar{\lambda}_T : K[S] \rightarrow \Lambda(K[S])$  is a ring homomorphism.

Now, for every  $i \in \mathbb{N}$ , let us define a map  $\widehat{\bar{\lambda}}^i : \Lambda(K[S]) \rightarrow \Lambda(K[S])$  in the same way as the map  $\widehat{\lambda}^i : \Lambda(K) \rightarrow \Lambda(K)$  was defined in Section 5 (but with  $K$  replaced by  $K[S]$ ). Then, the diagram

$$\begin{array}{ccc} \Lambda(K) & \xrightarrow{\widehat{\lambda}^i} & \Lambda(K) \\ \downarrow & & \downarrow \\ \Lambda(K[S]) & \xrightarrow{\widehat{\bar{\lambda}}^i} & \Lambda(K[S]) \end{array} \quad (35)$$

(where the vertical arrows are induced by the canonical inclusion  $K \rightarrow K[S]$ ) is commutative (since the maps  $\widehat{\lambda}^i : \Lambda(K) \rightarrow \Lambda(K)$  and  $\widehat{\bar{\lambda}}^i : \Lambda(K[S]) \rightarrow \Lambda(K[S])$  were defined in the same natural way).

For every  $a \in K$  and  $\alpha \in \mathbb{N}$ , we have

$$\begin{aligned} & \left( \widehat{\bar{\lambda}}^i \circ \bar{\lambda}_T \right) (aS^\alpha) = \widehat{\bar{\lambda}}^i (\bar{\lambda}_T (aS^\alpha)) \\ &= \widehat{\bar{\lambda}}^i (\text{ev}_{S^\alpha T} (\lambda_T (a))) \quad \left( \text{since } \bar{\lambda}_T (aS^\alpha) = \lambda_{S^\alpha T} (a) = \text{ev}_{S^\alpha T} (\lambda_T (a)) \right) \\ &= \text{ev}_{(S^\alpha)^i T} \left( \widehat{\bar{\lambda}}^i (\lambda_T (a)) \right) \\ & \quad \left( \text{by Theorem 5.7 (e), applied to } K[S], \lambda_T (a), S^\alpha \text{ and } i \text{ instead of } K, u, \mu \text{ and } k \right) \\ &= \text{ev}_{(S^\alpha)^i T} \left( \widehat{\lambda}^i (\lambda_T (a)) \right) \quad \left( \begin{array}{l} \text{because the commutative diagram (35)} \\ \text{shows that } \widehat{\bar{\lambda}}^i (\lambda_T (a)) = \widehat{\lambda}^i (\lambda_T (a)) \end{array} \right) \\ &= \text{ev}_{(S^\alpha)^i T} (\lambda_T (\lambda^i (a))) \\ & \quad \left( \begin{array}{l} \text{since } \widehat{\lambda}^i \circ \lambda_T = \lambda_T \circ \lambda^i \text{ (because } \lambda_T \text{ is a } \lambda\text{-ring homomorphism)} \\ \text{and thus } \widehat{\lambda}^i (\lambda_T (a)) = \lambda_T (\lambda^i (a)) \end{array} \right) \\ &= \lambda_{(S^\alpha)^i T} (\lambda^i (a)) = \lambda_{S^{\alpha i} T} (\lambda^i (a)) = \bar{\lambda}_T \left( \underbrace{\lambda^i (a) S^{\alpha i}}_{= \bar{\lambda}^i (aS^\alpha)} \right) \\ & \quad \left( \begin{array}{l} \text{since } \bar{\lambda}_T (\lambda^i (a) S^{\alpha i}) = \lambda_{S^{\alpha i} T} (\lambda^i (a)) \text{ (by (34), applied to)} \\ \lambda^i (a) \text{ and } \alpha i \text{ instead of } a \text{ and } b \end{array} \right) \\ &= \bar{\lambda}_T (\bar{\lambda}^i (aS^\alpha)) = (\bar{\lambda}_T \circ \bar{\lambda}^i) (aS^\alpha) \end{aligned}$$

for every  $i \in \mathbb{N}$ . In other words, every  $e \in E$  satisfies  $\left( \widehat{\bar{\lambda}}^i \circ \bar{\lambda}_T \right) (e) = (\bar{\lambda}_T \circ \bar{\lambda}^i) (e)$  for every  $i \in \mathbb{N}$ .

Altogether, we now know that  $\bar{\lambda}_T : K[S] \rightarrow \Lambda(K[S])$  is a ring homomorphism, that  $E$  is a generating set of the  $\mathbb{Z}$ -module  $K[S]$ , and that every  $e \in E$  satisfies

$(\widehat{\lambda}^i \circ \bar{\lambda}_T)(e) = (\bar{\lambda}_T \circ \bar{\lambda}^i)(e)$  for every  $i \in \mathbb{N}$ . Thus, by Exercise 2.1 (b), it follows that  $\bar{\lambda}_T$  is a  $\lambda$ -ring homomorphism. This proves Theorem 7.3.  $\square$

### 7.3. Exercises

*Exercise 7.1.* Let  $M$  be a commutative monoid. Prove that the  $\lambda$ -ring  $(\mathbb{Z}[M], (\lambda^i)_{i \in \mathbb{N}})$  defined in Exercise 3.4 is special.

*Exercise 7.2.* Let  $M$  be a commutative monoid. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring. Prove that the  $\lambda$ -ring  $(K[M], (\bar{\lambda}^i)_{i \in \mathbb{N}})$  defined in Exercise 3.5 (a) is special.

## 8. The $\lambda$ -verification principle

### 8.1. $n$ -operations of special $\lambda$ -rings

In Section 5, we have constructed a family of  $\lambda$ -rings  $\Lambda(K)$  which are (comparatively) easy to work with due to the following property: If you want to prove an identity involving the ring structure of  $\Lambda(K)$  (the addition  $\widehat{+}$ , the corresponding subtraction  $\widehat{-}$ , the zero 1, the multiplication  $\widehat{\cdot}$ , and the multiplicative unity  $1+T$ ) and the mappings  $\widehat{\lambda}^i$ , then it is enough to verify it for elements of  $1+K[T]^+$  only (by continuity, according to Theorem 5.5); and this is usually much easier since we know what  $\widehat{+}$ ,  $\widehat{\cdot}$  and  $\widehat{\lambda}^i$  mean for elements of  $1+K[T]^+$  (this is what Theorem 5.3 is for).

As a consequence of this, it is no wonder that often an identity is more easily proven in  $\Lambda(K)$  than in arbitrary  $\lambda$ -rings. However, it turns out that if an identity can be proven in  $\Lambda(K)$ , then it automatically holds for arbitrary special  $\lambda$ -rings! This is one of the so-called  *$\lambda$ -verification principles*<sup>44</sup>. Before we formulate this principle, let us first formally define what kind of identities it will hold for:

**Definition.** Let  $\text{Rng}^{\text{SA}}$  denote the so-called *category of special  $\lambda$ -rings*, which is defined as the category whose objects are the special  $\lambda$ -rings and whose morphisms are  $\lambda$ -ring homomorphisms between its objects.

Let  $\text{USet} : \text{Rng}^{\text{SA}} \rightarrow \text{Set}$  be the functor which maps every special  $\lambda$ -ring to its underlying set. Let  $n \in \mathbb{N}$ . Let  $\text{USet}^{(n)} : \text{Rng}^{\text{SA}} \rightarrow \text{Set}$  be the functor which maps every special  $\lambda$ -ring  $K$  to the set  $K^n$  (the  $n$ -th power of  $K$  with respect to the Cartesian product), and maps every homomorphism  $f : K \rightarrow L$  of special  $\lambda$ -rings to the map  $f^{\times n} : K^n \rightarrow L^n$ . (Thus,  $\text{USet}^{(1)} \cong \text{USet}$ .) An  *$n$ -operation of special  $\lambda$ -rings* will mean a natural transformation from the functor  $\text{USet}^{(n)}$  to  $\text{USet}$ .

In other words, an  $n$ -operation  $m$  of special  $\lambda$ -rings is a family of mappings<sup>45</sup>  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} : K^n \rightarrow K$  for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  such that the

<sup>44</sup>We are following [Knut73, pp. 25–27] here, though our Theorem 8.1 is not exactly what [Knut73] calls “verification principle”.

<sup>45</sup>Here, “mapping” actually means “mapping” and not “group homomorphism” or “ring homomorphism”.

diagram

$$\begin{array}{ccc}
 K^n & \xrightarrow{f^{\times n}} & L^n \\
 \downarrow m_{(K, (\lambda^i)_{i \in \mathbb{N}})} & & \downarrow m_{(L, (\mu^i)_{i \in \mathbb{N}})} \\
 K & \xrightarrow{f} & L
 \end{array} \tag{36}$$

commutes for any two special  $\lambda$ -rings  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and  $(L, (\mu^i)_{i \in \mathbb{N}})$  and any  $\lambda$ -ring homomorphism  $f : (K, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (L, (\mu^i)_{i \in \mathbb{N}})$ . Here,  $f^{\times n}$  means the map from  $K^n$  to  $L^n$  which equals  $f$  on each coordinate.

In practice, what are  $n$ -operations of special  $\lambda$ -rings? The answer is: Pretty much every map  $K^n \rightarrow K$  which is defined for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  just using addition, subtraction, multiplication, 0 and 1 and the maps  $\lambda^i$  is an  $n$ -operation. In particular, every polynomial map (where the polynomial has integer coefficients) is an  $n$ -operation, and so are the maps  $\lambda^i : K \rightarrow K$ . To give a different example, the family of maps  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} : K^3 \rightarrow K$  for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  defined by

$$m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(a_1, a_2, a_3) = \lambda^5(\lambda^2(a_1) - \lambda^4(a_2) \cdot a_3)$$

is a 3-operation of special  $\lambda$ -rings.

## 8.2. A useful triviality

Now, here is the theorem we came for:

**Theorem 8.1 ( $\lambda$ -verification principle).** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring. Let  $n \in \mathbb{N}$ . Let  $m$  and  $m'$  be two  $n$ -operations of special  $\lambda$ -rings.

Assume that  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$ . Then,  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}$ .

The proof of this result turns out to be surprisingly simple. First a trivial lemma:

**Theorem 8.2.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Define a mapping  $\text{coeff}_1 : \Lambda(K) \rightarrow K$  by  $\text{coeff}_1\left(\sum_{j \in \mathbb{N}} a_j T^j\right) = a_1$  for every  $\sum_{j \in \mathbb{N}} a_j T^j \in \Lambda(K)$  (with  $a_j \in K$  for every  $j \in \mathbb{N}$ ). (In other words,  $\text{coeff}_1$  is the mapping that takes a power series and returns its coefficient before  $T^1$ .)

Then,  $\text{coeff}_1 \circ \lambda_T = \text{id}_K$ .

Note that the definition of  $\text{coeff}_1$  in Theorem 8.2 is a particular case of the definition of  $\text{coeff}_i$  in Exercise 6.5.

*Proof of Theorem 8.2.* This is clear, since

$$(\text{coeff}_1 \circ \lambda_T)(x) = \text{coeff}_1(\lambda_T(x)) = \text{coeff}_1\left(\sum_{i \in \mathbb{N}} \lambda^i(x) T^i\right) = \lambda^1(x) = x$$

for every  $x \in K$ . Theorem 8.2 is now proven.  $\square$

*Proof of Theorem 8.1.* Since  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring, the map  $\lambda_T : K \rightarrow \Lambda(K)$  is a  $\lambda$ -ring homomorphism. According to (36), we thus have the two commutative diagrams

$$\begin{array}{ccc} K^n & \xrightarrow{(\lambda_T)^{\times n}} & (\Lambda(K))^n \\ \downarrow m_{(K, (\lambda^i)_{i \in \mathbb{N}})} & & \downarrow m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \\ K & \xrightarrow{\lambda_T} & \Lambda(K) \end{array}$$

and

$$\begin{array}{ccc} K^n & \xrightarrow{(\lambda_T)^{\times n}} & (\Lambda(K))^n \\ \downarrow m'_{(K, (\lambda^i)_{i \in \mathbb{N}})} & & \downarrow m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \\ K & \xrightarrow{\lambda_T} & \Lambda(K) \end{array} .$$

Hence,  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$  yields

$$\lambda_T \circ m_{(K, (\lambda^i)_{i \in \mathbb{N}})} = m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \circ (\lambda_T)^{\times n} = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \circ (\lambda_T)^{\times n} = \lambda_T \circ m'_{(K, (\lambda^i)_{i \in \mathbb{N}})} .$$

Hence,  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}$  because  $\lambda_T$  is injective (due to Theorem 8.2). Theorem 8.1 is thus proven!  $\square$

### 8.3. 1-dimensional elements

Before we move on to concrete properties of special  $\lambda$ -rings, let us merge Theorems 8.1 and 5.5 into one simple principle for proving facts about  $\lambda$ -rings – our Theorem 8.4 below. Before we formulate it, let us define the notion of *1-dimensional* elements of a  $\lambda$ -ring.

**Definition.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring, and let  $x \in K$  be an element of  $K$ . Then,  $x$  is said to be *1-dimensional* if and only if  $\lambda^i(x) = 0$  for every integer  $i > 1$ .

**Theorem 8.3.**

(a) Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $x \in K$  be an element of  $K$ . The element  $x$  is 1-dimensional if and only if  $\lambda_T(x) = 1 + xT$  (where  $\lambda_T : K \rightarrow K[[T]]$  is the map defined in Theorem 2.1).

(b) Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring. Let  $x$  and  $y$  be two 1-dimensional elements of  $K$ . Then,  $xy$  is 1-dimensional as well.

(c) Let  $K$  be a ring. Let  $e \in K$ . Then, the element  $1 + eT$  of the  $\lambda$ -ring  $\Lambda(K)$  is 1-dimensional.

*Proof of Theorem 8.3. (a)* In fact,

$$\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i = \underbrace{\lambda^0(x)}_{=1} + \underbrace{\lambda^1(x)}_{=x} T + \sum_{\substack{i > 1 \\ \text{integer}}} \lambda^i(x) T^i = 1 + xT + \sum_{\substack{i > 1 \\ \text{integer}}} \lambda^i(x) T^i.$$

Hence,  $\lambda_T(x) = 1 + xT$  if and only if  $\lambda^i(x) = 0$  for every integer  $i > 1$  (which means that  $x$  is 1-dimensional). Theorem 8.3 (a) is thus proven.

(b) Since the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special, the map  $\lambda_T$ , seen as a map from  $K$  to  $\Lambda(K)$ , is a ring homomorphism, so that  $\lambda_T(xy) = \lambda_T(x) \widehat{\cdot} \lambda_T(y)$ . But Theorem 8.3 (a) yields  $\lambda_T(x) = 1 + xT = \Pi(K, [x])$ . Similarly,  $\lambda_T(y) = \Pi(K, [y])$ . Thus,

$$\begin{aligned} \lambda_T(xy) &= \lambda_T(x) \widehat{\cdot} \lambda_T(y) = \Pi(K, [x]) \widehat{\cdot} \Pi(K, [y]) = \Pi(K, [xy]) && \text{(after Theorem 5.3 (c))} \\ &= 1 + xyT. \end{aligned}$$

By Theorem 8.3 (a) (applied to  $xy$  instead of  $x$ ), this yields that  $xy$  is 1-dimensional. Thus, Theorem 8.3 (b) is proven.

(c) For every integer  $i > 1$ , the element

$$\begin{aligned} \widehat{\lambda}^i(1 + eT) &= \Pi \left( K, \underbrace{\left[ \prod_{i \in I} e \mid I \in \mathcal{P}_i(\{1\}) \right]}_{\substack{\text{empty multiset,} \\ \text{since } i > 1 \text{ yields } \mathcal{P}_i(\{1\}) = \emptyset}} \right) \\ &\quad \text{(by Theorem 5.3 (d), since } 1 + eT = \Pi(K, [e])\text{)} \\ &= \Pi(K, \text{empty multiset}) = 1 \end{aligned}$$

is the zero of  $\Lambda(K)$ . Thus,  $1 + eT$  is 1-dimensional. Theorem 8.3 (c) is proven.  $\square$

## 8.4. The continuous splitting $\lambda$ -verification principle

Now, we can formulate the desired result:

**Theorem 8.4 (continuous splitting  $\lambda$ -verification principle).** Let  $n \in \mathbb{N}$ . Let  $m$  and  $m'$  be two  $n$ -operations of special  $\lambda$ -rings.

Assume that the following two assumptions hold:

*Continuity assumption:* The maps  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} : (\Lambda(K))^n \rightarrow \Lambda(K)$  and  $m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} : (\Lambda(K))^n \rightarrow \Lambda(K)$  are continuous with respect to the  $(T)$ -topology for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ .

*Split equality assumption:* For every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $(u_1, u_2, \dots, u_n) \in K^n$  such that  $u_i$  is the sum of finitely many 1-dimensional elements of  $K$  for every  $i \in \{1, 2, \dots, n\}$ , we have  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n)$ .

Then,  $m = m'$ .

*Proof of Theorem 8.4.* We have to prove that  $m = m'$ . In other words, we must show that  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}$  for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ . According to Theorem 8.1, this will immediately follow once we have shown that  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$  for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ . So it remains to prove this.

Consider a special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ . We must prove that  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$ .

Consider the  $(T)$ -topology on  $\Lambda(K)$ . The maps  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$  and  $m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$  are continuous, while the subset  $1 + K[T]^+$  of  $1 + K[[T]]^+ = \Lambda(K)$  is dense (by Theorem 5.5 (a)). Hence, in order to prove that  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$ , it will be enough to show that

$$m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) \quad (37)$$

for every  $(u_1, u_2, \dots, u_n) \in (1 + K[T]^+)^n$ .

Fix some  $(u_1, u_2, \dots, u_n) \in (1 + K[T]^+)^n$ . For every  $i \in \{1, 2, \dots, n\}$ , there exists some  $(\widetilde{K}_{u_i}, [(u_i)_1, (u_i)_2, \dots, (u_i)_{n_i}]) \in K^{\text{int}}$  such that  $u_i = \Pi(\widetilde{K}_{u_i}, [(u_i)_1, (u_i)_2, \dots, (u_i)_{n_i}])$ . According to Theorem 5.3 (a) (applied several times)<sup>46</sup>, there exists a finite-free extension ring  $K'$  of  $K$  which contains the  $\widetilde{K}_{u_i}$  for all  $i \in \{1, 2, \dots, n\}$  as subrings. Consider such a  $K'$ . Hence,  $u_i = \Pi(K', [(u_i)_1, (u_i)_2, \dots, (u_i)_{n_i}])$  for every  $i \in \{1, 2, \dots, n\}$ .

We have  $K \subseteq K'$ . Thus,  $\Lambda(K')$  is an extension ring of  $\Lambda(K)$  (since  $\Lambda$  is a functor). In this extension ring  $\Lambda(K')$ , we have

$$u_i = \Pi(K', [(u_i)_1, (u_i)_2, \dots, (u_i)_{n_i}]) = \prod_{j=1}^{n_i} (1 + (u_i)_j T) = \widehat{\sum_{j=1}^{n_i} (1 + (u_i)_j T)} \quad (\text{since addition in } \Lambda(K') \text{ is multiplication in } K'[[T]]) \quad (38)$$

for each  $i \in \{1, 2, \dots, n\}$ . On the other hand, for every  $j \in \{1, 2, \dots, n_i\}$ , the element  $1 + (u_i)_j T$  of  $\Lambda(K')$  is 1-dimensional (by Theorem 8.3 (c), applied to  $e = (u_i)_j$ ). Thus, (38) shows that  $u_i$  is a sum of 1-dimensional elements of  $\Lambda(K')$  for every  $i \in \{1, 2, \dots, n\}$ . Hence, applying the split equality assumption to the special  $\lambda$ -ring  $(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  instead of  $(K, (\lambda^i)_{i \in \mathbb{N}})$ , we see that

$$m_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) = m'_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n). \quad (39)$$

This is an equality in the ring  $\Lambda(K')$ , but since  $\Lambda(K)$  can be canonically seen as a sub- $\lambda$ -ring of  $\Lambda(K')$  (because  $K$  is a subring of  $K'$ ), it easily yields the equality

$$m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n)$$

<sup>46</sup>More precisely, what we are using here is the following lemma:

**Lemma.** Let  $L_1, L_2, \dots, L_n$  be finitely many finite-free extension rings of a ring  $K$ . Then, there exists a finite-free extension ring  $K'$  of  $K$  which contains all of the  $L_1, L_2, \dots, L_n$  as subrings.

*Proof of the lemma.* By induction over  $n$ , it suffices to show that for any two finite-free extension rings  $L$  and  $L'$  of  $K$ , there exists a finite-free extension ring  $K'$  of  $K$  which contains both  $L$  and  $L'$  as subrings. But this was essentially shown in our proof of Theorem 5.3 (a).



in the ring  $\Lambda(K)$ .<sup>47</sup> Thus we have proven (37). This proves Theorem 8.4.  $\square$

Roughly speaking, Theorem 8.4 says that whether some identity holds on every special  $\lambda$ -ring or not can be checked just by looking at the sums of 1-dimensional elements. This is why it is worthwhile to study such sums. Let us record a property of these:

### 8.5. $\lambda^i$ of a sum of 1-dimensional elements

**Theorem 8.5.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $u_1, u_2, \dots, u_m$  be 1-dimensional elements of  $K$ . Let  $i \in \mathbb{N}$ . Then,

$$\lambda^i(u_1 + u_2 + \dots + u_m) = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} u_k.$$

---

<sup>47</sup>*Proof.* Let  $\iota$  denote the canonical inclusion  $\Lambda(K) \rightarrow \Lambda(K')$ . Since  $m$  was defined as a natural transformation, and since the inclusion  $\iota : \Lambda(K) \rightarrow \Lambda(K')$  is a  $\lambda$ -ring homomorphism, we then have  $\iota \circ m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} = m_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \circ \iota^{\times n}$ . Now,

$$\begin{aligned} & m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) \\ &= \iota \left( m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) \right) \quad (\text{since } \iota \text{ is just the inclusion map } \Lambda(K) \rightarrow \Lambda(K')) \\ &= \underbrace{\left( \iota \circ m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \right)}_{= m_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \circ \iota^{\times n}}(u_1, u_2, \dots, u_n) = \left( m_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \circ \iota^{\times n} \right)(u_1, u_2, \dots, u_n) \\ &= m_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} \left( \underbrace{\left( \iota^{\times n}(u_1, u_2, \dots, u_n) \right)}_{\substack{= (\iota(u_1), \iota(u_2), \dots, \iota(u_n)) \\ = (u_1, u_2, \dots, u_n)}} \right) = m_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) \\ & \quad (\text{since } \iota \text{ is just an inclusion map}) \end{aligned}$$

and similarly  $m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) = m'_{(\Lambda(K'), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n)$ . Thus, (39) rewrites as

$$m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n) = m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}(u_1, u_2, \dots, u_n),$$

qed.

*Proof of Theorem 8.5.* We have

$$\begin{aligned}
& \sum_{i \in \mathbb{N}} \lambda^i (u_1 + u_2 + \dots + u_m) T^i = \lambda_T (u_1 + u_2 + \dots + u_m) \\
&= \prod_{j=1}^m \lambda_T (u_j) \quad (\text{by Theorem 2.1 (a), applied several times}) \\
&= \prod_{j=1}^m (1 + u_j T) \\
&\quad (\text{since the element } u_j \text{ is 1-dimensional and thus satisfies } \lambda_T (u_j) = 1 + u_j T) \\
&= \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} u_k \cdot T^i \\
&\quad (\text{by Exercise 4.2 (b), applied to } A = K[T], \alpha_j = u_j \text{ and } t = T).
\end{aligned}$$

Comparing coefficients yields the assertion of Theorem 8.5.  $\square$

## 8.6. Exercises

*Exercise 8.1.* Give a new solution to Exercise 6.9.

*Exercise 8.2.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring. If  $x \in K$  is an invertible 1-dimensional element of  $K$ , then prove that  $x^{-1}$  is 1-dimensional as well.

*Exercise 8.3.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $E$  be a generating set of the  $\mathbb{Z}$ -module  $K$  such that every element  $e \in E$  is 1-dimensional.

Prove that the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special.

## 9. Adams operations

### 9.1. The Hirzebruch-Newton polynomials

We are now ready to define Adams operations of special  $\lambda$ -rings. There are two different ways to do this; we will take one of these as the definition and the other one as a theorem.

Remember how we defined the “universal” polynomials  $P_k$  and  $P_{k,j}$  in Section 4? Prepare for some more:

**Definition.** Let  $j \in \mathbb{N} \setminus \{0\}$ . Our goal is to define a polynomial  $N_j \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  such that

$$\sum_{i=1}^m U_i^j = N_j (X_1, X_2, \dots, X_j) \quad (40)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ , where  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  is the  $i$ -th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$  for every  $i \in \mathbb{N}$ .

In order to do this, we first fix some  $m \in \mathbb{N}$ . The polynomial  $\sum_{i=1}^m U_i^j \in \mathbb{Z}[U_1, U_2, \dots, U_m]$  is symmetric. Thus, Theorem 4.1 (a) yields that there exists one and only one polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  such that  $\sum_{i=1}^m U_i^j = Q(X_1, X_2, \dots, X_m)$ . Since the polynomial  $\sum_{i=1}^m U_i^j$  has total degree  $\leq j$  in the variables  $U_1, U_2, \dots, U_m$ , Theorem 4.1 (b) yields that

$$\sum_{i=1}^m U_i^j = Q_j(X_1, X_2, \dots, X_j),$$

where  $Q_j$  is the image of the polynomial  $Q$  under the canonical homomorphism  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m] \rightarrow \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$ . However, this polynomial  $Q_j$  is not independent of  $m$  yet (as the polynomial  $N_j$  that we intend to construct should be), so we call it  $Q_{j,[m]}$  rather than just  $Q_j$ .

Now we forget that we fixed  $m \in \mathbb{N}$ . We have learnt that

$$\sum_{i=1}^m U_i^j = Q_{j,[m]}(X_1, X_2, \dots, X_j),$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ . Now, define a polynomial  $N_j \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  by  $N_j = Q_{j,[j]}$ .

This polynomial  $N_j$  is called the  *$j$ -th Hirzebruch-Newton polynomial*.<sup>48</sup>

**Theorem 9.1. (a)** The polynomial  $N_j$  just defined satisfies the equation (40) in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ . (Hence, the goal mentioned above in the definition is actually achieved.)

**(b)** For every  $m \in \mathbb{N}$ , we have

$$T \sum_{i=1}^m \frac{U_i}{1 - U_i T} = \sum_{j \in \mathbb{N} \setminus \{0\}} N_j(X_1, X_2, \dots, X_j) T^j \quad (41)$$

in the ring  $(\mathbb{Z}[U_1, U_2, \dots, U_m])[ [T] ]$ .

*Proof of Theorem 9.1. (a)* This proof is going to be very similar to that of Theorem 4.4 (a).

*1st Step:* Fix  $m \in \mathbb{N}$  such that  $m \geq j$ . Then, we claim that  $Q_{j,[m]} = N_j$ .

*Proof.* By the definition of  $Q_{j,[m]}$ , we have

$$\sum_{i=1}^m U_i^j = Q_{j,[m]}(X_1, X_2, \dots, X_j)$$

---

<sup>48</sup>The ‘‘Newton’’ in the name of this polynomial  $N_j$  probably refers to the fact that the explicit form of  $N_j$  can be easily computed (recursively) from the so-called Newton identities (which relate the power sums and the elementary symmetric polynomials). See Theorem 9.6 and Corollary 9.7 for details.

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ . Applying the canonical ring epimorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m] \rightarrow \mathbb{Z}[U_1, U_2, \dots, U_j]$  (which maps every  $U_i$  to  $\begin{cases} U_i, & \text{if } i \leq j; \\ 0, & \text{if } i > j \end{cases}$ ) to this equation (and noticing that this epimorphism maps every  $X_i$  with  $i \geq 1$  to the corresponding  $X_i$  of the image ring), we obtain

$$\sum_{i=1}^j U_i^j = Q_{j,[m]}(X_1, X_2, \dots, X_j)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_j]$ . On the other hand, the definition of  $Q_{j,[j]}$  yields

$$\sum_{i=1}^j U_i^j = Q_{j,[j]}(X_1, X_2, \dots, X_j)$$

in the same ring. These two equations yield  $Q_{j,[m]}(X_1, X_2, \dots, X_j) = Q_{j,[j]}(X_1, X_2, \dots, X_j)$ . Since the elements  $X_1, X_2, \dots, X_j$  of  $\mathbb{Z}[U_1, U_2, \dots, U_j]$  are algebraically independent (by Theorem 4.1 (a)), this yields  $Q_{j,[m]} = Q_{j,[j]}$ . In other words,  $Q_{j,[m]} = N_j$ , and the 1st Step is proven.

*2nd Step:* For every  $m \in \mathbb{N}$ , the equation (40) is satisfied in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ .

*Proof.* Let  $m' \in \mathbb{N}$  be such that  $m' \geq m$  and  $m' \geq j$ . Then, the 1st Step (applied to  $m'$  instead of  $m$ ) yields that  $Q_{j,[m']} = N_j$ .

The definition of  $Q_{j,[m']}$  yields

$$\sum_{i=1}^{m'} U_i^j = Q_{j,[m']}(X_1, X_2, \dots, X_j)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_{m'}]$ . Applying the canonical ring epimorphism  $\mathbb{Z}[U_1, U_2, \dots, U_{m'}] \rightarrow \mathbb{Z}[U_1, U_2, \dots, U_m]$  (which maps every  $U_i$  to  $\begin{cases} U_i, & \text{if } i \leq m; \\ 0, & \text{if } i > m \end{cases}$ ) to this equation (and noticing that this epimorphism maps every  $X_i$  with  $i \geq 1$  to the corresponding  $X_i$  of the image ring), we obtain

$$\sum_{i=1}^m U_i^j = Q_{j,[m']}(X_1, X_2, \dots, X_j)$$

in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ . This means that the equation (40) is satisfied in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  (since  $Q_{j,[m']} = N_j$ ). This completes the 2nd Step and proves Theorem 9.1 (a).

(b) We have

$$\begin{aligned} T \sum_{i=1}^m \frac{U_i}{1 - U_i T} &= \sum_{i=1}^m U_i T \underbrace{(1 - U_i T)^{-1}}_{=\sum_{j \in \mathbb{N}} (U_i T)^j} = \sum_{i=1}^m \sum_{j \in \mathbb{N}} (U_i T)^{j+1} = \sum_{i=1}^m \sum_{j \in \mathbb{N} \setminus \{0\}} (U_i T)^j \\ &= \sum_{j \in \mathbb{N} \setminus \{0\}} \sum_{i=1}^m (U_i T)^j = \sum_{j \in \mathbb{N} \setminus \{0\}} \underbrace{\sum_{i=1}^m U_i^j}_{=N_j(X_1, X_2, \dots, X_j) \text{ by (40)}} T^j = \sum_{j \in \mathbb{N} \setminus \{0\}} N_j(X_1, X_2, \dots, X_j) T^j, \end{aligned}$$

and Theorem 9.1 (b) is proven.  $\square$

*Remark:* There is a subtle point here: We have defined, for every  $j \in \mathbb{N} \setminus \{0\}$ , a polynomial  $N_j \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  which satisfies (40) in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ . We *cannot* define such a polynomial  $N_j$  for  $j = 0$ . In fact, if we would try to do this as we did above, then the proof of Theorem 9.1 would fail (in fact, the canonical ring epimorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m] \rightarrow \mathbb{Z}[U_1, U_2, \dots, U_j]$  would *not* send  $\sum_{i=1}^m U_i^j$  to  $\sum_{i=1}^j U_i^j$  anymore, because  $0^j$  is not 0 for  $j = 0$ ). This is why  $N_j$  is well-defined only for  $j \in \mathbb{N} \setminus \{0\}$  and not for all  $j \in \mathbb{N}$ .

**Example.** We can compute the polynomials  $N_j$  in the same way as we have computed the polynomials  $P_{k,j}$  in Section 4 - by unraveling the definition. Here are the first few  $N_j$ :

$$\begin{aligned} N_1 &= \alpha_1; \\ N_2 &= \alpha_1^2 - 2\alpha_2; \\ N_3 &= \alpha_1^3 - 3\alpha_1\alpha_2 + 3\alpha_3; \\ N_4 &= \alpha_1^4 - 4\alpha_1^2\alpha_2 + 4\alpha_1\alpha_3 + 2\alpha_2^2 - 4\alpha_4. \end{aligned}$$

There are easier ways to compute the  $N_j$ , however. For example, Corollary 9.7 gives a recurrent formula, and Exercise 9.6 (c) gives an explicit determinantal one.

## 9.2. Definition of Adams operations

Now, let us define Adams operations:

**Definition.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. For every  $j \in \mathbb{N} \setminus \{0\}$ , we define a map  $\psi^j : K \rightarrow K$  by

$$\psi^j(x) = N_j(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) \quad \text{for every } x \in K. \quad (42)$$

We call  $\psi^j$  the *j-th Adams operation* (or the *j-th Adams character*) of the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ .

## 9.3. The equality $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$ for special $\lambda$ -rings

Before we prove a batch of properties of these Adams characters, let us show another approach to these Adams characters:

**Theorem 9.2.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring.

Define a map  $\tilde{\psi}_T : K \rightarrow K[[T]]$  by  $\tilde{\psi}_T(x) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j$  for every

$x \in K$ . <sup>49</sup>

Let  $x \in K$ .

---

<sup>49</sup>Note that we call this map  $\tilde{\psi}_T$  to distinguish it from the map  $\psi_T$  in [FulLan85] (which is more or less the same but differs slightly).

(a) We have

$$\psi^j(x) = (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x) \quad \text{for every } j \in \mathbb{N} \setminus \{0\}.$$

(b) We have  $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$ . Here, for every power series  $u \in 1 + K[[T]]^+$ , the *logarithmic derivative*  $\frac{d}{dT} \log u$  of  $u$  is defined by

$\frac{d}{dT} \log u = \frac{\frac{d}{dT} u}{u}$  (this definition works even in the cases where the logarithm doesn't exist, such as rings of positive characteristic), and  $\lambda_{-T}(x)$  denotes  $\text{ev}_{-T}(\lambda_T(x))$ .

Before we start proving this, let me admit that Theorem 9.2 can be generalized: It still holds if  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is an *arbitrary* (not necessarily special!)  $\lambda$ -ring. However, the proof of Theorem 9.2 that we are going to give right now cannot be generalized to this situation; it requires the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  to be special. The generalized version of Theorem 9.2 will be proven later (see the proof of Theorem 9.5 below), yielding another proof of Theorem 9.2. The reader is still advised to read the following proof of Theorem 9.2, even if it is not directly generalizable. In fact, its first two steps will be used at later times (in particular, its 1st step will be used in the proof of the generalized version), whereas its 4th step gives a good example of how Theorem 8.4 can be applied to prove properties of special  $\lambda$ -rings.

*Proof of Theorem 9.2. 1st step:* For any fixed special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and any fixed  $x \in K$ , the assertions (a) and (b) are equivalent.

*Proof.* In  $K[[T]]$ , we have

$$\lambda_{-T}(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) (-T)^i = \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(x) T^i,$$

but also

$$\begin{aligned} (\lambda_{-T}(x))^{-1} &= \lambda_{-T}(-x) && \text{(since } (\lambda_T(x))^{-1} = \lambda_T(-x) \text{ by Theorem 2.1 (b))} \\ &= \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(-x) T^i && \left( \begin{array}{l} \text{due to } \lambda_{-T}(x) = \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(x) T^i, \\ \text{applied to } -x \text{ instead of } x \end{array} \right) \end{aligned}$$

and

$$\begin{aligned} \frac{d}{dT} \lambda_{-T}(x) &= \frac{d}{dT} \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(x) T^i && \left( \text{since } \lambda_{-T}(x) = \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(x) T^i \right) \\ &= \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(x) i T^{i-1} \end{aligned}$$

(by the definition of the derivative of a formal power series).

Thus,

$$\begin{aligned}
& -T \cdot \frac{d}{dT} \log \lambda_{-T}(x) \\
&= -T \cdot \frac{\frac{d}{dT} \lambda_{-T}(x)}{\lambda_{-T}(x)} = -T \cdot \underbrace{\frac{d}{dT} \lambda_{-T}(x)}_{=\sum_{i \in \mathbb{N}} (-1)^i \lambda^i(x) iT^{i-1}} \cdot \underbrace{(\lambda_{-T}(x))^{-1}}_{=\sum_{i \in \mathbb{N}} (-1)^i \lambda^i(-x) T^i} \\
&= -T \cdot \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(x) iT^{i-1} \cdot \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(-x) T^i \\
&= \sum_{i \in \mathbb{N}} (-1)^{i+1} \lambda^i(x) iT^i \cdot \sum_{i \in \mathbb{N}} (-1)^i \lambda^i(-x) T^i \\
&= \sum_{j \in \mathbb{N}} \sum_{i=0}^j (-1)^{i+1} \lambda^i(x) i \cdot (-1)^{j-i} \lambda^{j-i}(-x) T^j = \sum_{j \in \mathbb{N}} (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x) \cdot T^j \\
&= \sum_{j \in \mathbb{N} \setminus \{0\}} (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x) \cdot T^j + \underbrace{(-1)^{0+1} \sum_{i=0}^0 i \lambda^i(x) \lambda^{0-i}(-x) \cdot T^0}_{=0} \\
&= \sum_{j \in \mathbb{N} \setminus \{0\}} (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x) \cdot T^j.
\end{aligned}$$

On the other hand,  $\tilde{\psi}_T(x) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j$ . Hence,  $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$  holds if and only if

$$\psi^j(x) = (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x) \quad \text{for every } j \in \mathbb{N} \setminus \{0\}.$$

This proves that the assertions **(a)** and **(b)** are equivalent, and thus the 1st step is complete.

*2nd step:* We will now show that the assertion **(b)** holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$  such that  $x$  is the sum of finitely many 1-dimensional elements of  $K$ .

*Proof.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring, and let  $x \in K$  be a sum of finitely many 1-dimensional elements of  $K$ . In other words,  $x = u_1 + u_2 + \dots + u_m$  for some 1-dimensional elements  $u_1, u_2, \dots, u_m$  of  $K$ .

Then,

$$\lambda_{-T}(x) = \lambda_{-T}(u_1 + u_2 + \dots + u_m) = \prod_{j=1}^m (1 - u_j T)$$

(since  $\lambda_T(u_1 + u_2 + \dots + u_m) = \prod_{j=1}^m (1 + u_j T)$ , as shown in the proof of Theorem 8.5),

so that, by the Leibniz formula,

$$\begin{aligned} \frac{d}{dT} \lambda_{-T}(x) &= \sum_{k=1}^m \left( \underbrace{\frac{d}{dT} (1 - u_k T)}_{=-u_k} \right) \cdot \underbrace{\prod_{j \in \{1,2,\dots,m\} \setminus \{k\}} (1 - u_j T)}_{=(1-u_k T)^{-1} \cdot \prod_{j \in \{1,2,\dots,m\}} (1 - u_j T)} \\ &= - \sum_{k=1}^m \frac{u_k}{1 - u_k T} \cdot \underbrace{\prod_{j \in \{1,2,\dots,m\}} (1 - u_j T)}_{=\lambda_{-T}(x)} = - \sum_{k=1}^m \frac{u_k}{1 - u_k T} \cdot \lambda_{-T}(x). \end{aligned}$$

Hence,

$$\begin{aligned} -T \cdot \frac{d}{dT} \log \lambda_{-T}(x) &= -T \cdot \frac{\frac{d}{dT} \lambda_{-T}(x)}{\lambda_{-T}(x)} = -T \cdot \frac{- \sum_{k=1}^m \frac{u_k}{1 - u_k T} \cdot \lambda_{-T}(x)}{\lambda_{-T}(x)} \\ &= T \cdot \sum_{k=1}^m \frac{u_k}{1 - u_k T} = T \sum_{i=1}^m \frac{u_i}{1 - u_i T}. \end{aligned} \quad (43)$$

On the other hand, Theorem 8.5 yields

$$\lambda^i(x) = \lambda^i(u_1 + u_2 + \dots + u_m) = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} u_k \quad \text{for every } i \in \mathbb{N}.$$

Consider the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ . For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k$

be the  $i$ -th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$ . There exists a ring homomorphism  $\mathbb{Z}[U_1, U_2, \dots, U_m] \rightarrow K$  which maps  $U_i$  to  $u_i$  for every  $i$ . This homomorphism therefore maps  $X_i$  to  $\sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} u_k = \lambda^i(x)$  for every  $i \in \mathbb{N}$ .

Hence, applying this homomorphism to (41), we obtain

$$T \sum_{i=1}^m \frac{u_i}{1 - u_i T} = \sum_{j \in \mathbb{N} \setminus \{0\}} \underbrace{N_j(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))}_{=\psi^j(x) \text{ by (42)}} T^j = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j = \tilde{\psi}_T(x).$$

Comparing this with (43), we obtain

$$-T \cdot \frac{d}{dT} \log \lambda_{-T}(x) = \tilde{\psi}_T(x).$$

Hence, the assertion **(b)** holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$  such that  $x$  is the sum of finitely many 1-dimensional elements of  $K$ . This completes the 2nd step.

*3rd step:* We will now show that the assertion **(a)** holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$  such that  $x$  is the sum of finitely many 1-dimensional elements of  $K$ .



*Proof.* This follows from the 2nd step, since **(a)** and **(b)** are equivalent (by the 1st step).

*4th step:* We will now show that the assertion **(a)** holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$ .

*Proof.* We want to derive this from the 3rd step by applying Theorem 8.4.

Fix some  $j \in \mathbb{N} \setminus \{0\}$ .

Define a 1-operation  $m$  of special  $\lambda$ -rings by  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} = \psi^j$  for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ . (This is indeed a 1-operation, since (42) shows that  $\psi^j$  is a polynomial in  $\lambda^0, \lambda^1, \lambda^2, \dots, \lambda^j$  with integer coefficients.)

Define a 1-operation  $m'$  of special  $\lambda$ -rings by

$$m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x) \quad \text{for every } x \in K$$

for every  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ . (This is, again, a 1-operation, since it is a polynomial in  $\lambda^0(x), \lambda^1(x), \dots, \lambda^j(x), \lambda^0(-x), \lambda^1(-x), \dots, \lambda^j(-x)$  with integer coefficients.)

These two 1-operations  $m$  and  $m'$  satisfy both conditions of Theorem 8.4: The continuity assumption holds (since the operations  $m$  and  $m'$  are polynomials in  $\lambda^1, \lambda^2, \dots, \lambda^j$  with integer coefficients, so that the maps  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$  and  $m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$

are polynomials in  $\widehat{\lambda}^1, \widehat{\lambda}^2, \dots, \widehat{\lambda}^j$  with integer coefficients, and therefore continuous because of Theorem 5.5 **(d)**), and the split equality assumption holds (since it states that for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$  such that  $x$  is the sum of finitely many 1-dimensional elements of  $K$ , we have  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x)$ ;

but this simply means that  $\psi^j(x) = (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x)$ , which was proven in the 3rd step). Hence, by Theorem 8.4, we have  $m = m'$ . Hence, for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$ , we have

$$\psi^j(x) = m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x).$$

Thus, the assertion **(a)** holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$ . This completes the 4th step.

*5th step:* We will now prove that the assertion **(b)** holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$ .

*Proof.* This follows from the 4th step, since **(a)** and **(b)** are equivalent (by the 1st step).

Thus, the proof of Theorem 9.2 is completed.  $\square$

## 9.4. Adams operations are ring homomorphisms when the $\lambda$ -ring is special

The Adams operations  $\psi^j$  have a lot of interesting properties (that make them easier to deal with than  $\lambda$ -operations!):

**Theorem 9.3.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring.

(a) For every  $a \in K$ , we have  $\psi^1(a) = a$ .

(b) For every  $j \in \mathbb{N} \setminus \{0\}$ , the map  $\psi^j : (K, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism.

(c) For every  $i \in \mathbb{N} \setminus \{0\}$  and  $j \in \mathbb{N} \setminus \{0\}$ , we have  $\psi^i \circ \psi^j = \psi^j \circ \psi^i = \psi^{ij}$ .

Before we come to prove this, let us first show an analogue of Theorem 8.5 for the  $\psi^i$ :

**Theorem 9.4.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $u_1, u_2, \dots, u_m$  be 1-dimensional elements of  $K$ . Let  $j \in \mathbb{N} \setminus \{0\}$ . Then,

$$\psi^j(u_1 + u_2 + \dots + u_m) = u_1^j + u_2^j + \dots + u_m^j.$$

*Proof of Theorem 9.4.* Let  $x = u_1 + u_2 + \dots + u_m$ . Just as in the proof of Theorem 9.2 (in the 2nd step)<sup>50</sup>, we can show that

$$T \sum_{i=1}^m \frac{u_i}{1 - u_i T} = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j.$$

Thus,

$$\begin{aligned} \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j &= T \sum_{i=1}^m \frac{u_i}{1 - u_i T} = \sum_{i=1}^m u_i T (1 - u_i T)^{-1} = \sum_{i=1}^m u_i T \sum_{k \in \mathbb{N}} (u_i T)^k \\ &= \sum_{i=1}^m \sum_{k \in \mathbb{N}} (u_i T)^{k+1} = \sum_{i=1}^m \sum_{j \in \mathbb{N} \setminus \{0\}} (u_i T)^j = \sum_{i=1}^m \sum_{j \in \mathbb{N} \setminus \{0\}} u_i^j T^j \\ &= \sum_{j \in \mathbb{N} \setminus \{0\}} \sum_{i=1}^m u_i^j T^j. \end{aligned}$$

Comparing coefficients yields  $\psi^j(x) = \sum_{i=1}^m u_i^j$  for every  $j \in \mathbb{N} \setminus \{0\}$ , and thus Theorem 9.4 is proven.  $\square$

*Proof of Theorem 9.3.* (a) is trivial (for instance, by Theorem 9.2 (a)).

(b) Fix some  $j \in \mathbb{N} \setminus \{0\}$ . First, let us prove that  $\psi^j : K \rightarrow K$  is a ring homomorphism.

This means proving that

$$\psi^j(0) = 0; \tag{44}$$

$$\psi^j(x + y) = \psi^j(x) + \psi^j(y) \quad \text{for any } x \in K \text{ and } y \in K; \tag{45}$$

$$\psi^j(1) = 1; \tag{46}$$

$$\psi^j(xy) = \psi^j(x) \cdot \psi^j(y) \quad \text{for any } x \in K \text{ and } y \in K. \tag{47}$$

<sup>50</sup>Here, we use the fact that the 2nd step of the proof of Theorem 9.2 works for *any*  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ , not only for special ones.

Out of these four equations, two (namely, (44) and (46)) are trivial (just apply Theorem 9.4, remembering that 1 is a 1-dimensional element), so it remains to prove the other two equations - namely, (45) and (47).

First, let us prove (47):

Define a 2-operation  $m$  of special  $\lambda$ -rings as follows: For every special  $\lambda$ -ring  $K$ , let  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} : K^2 \rightarrow K$  be the map defined by  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y) = \psi^j(xy)$  for every  $x \in K$  and  $y \in K$ . (This is indeed a 2-operation of special  $\lambda$ -rings, since  $\psi^j$  is a polynomial in the  $\lambda^1, \lambda^2, \dots, \lambda^j$  with integer coefficients.)

Define a 2-operation  $m'$  of special  $\lambda$ -rings as follows: For every special  $\lambda$ -ring  $K$ , let  $m'_{(K, (\lambda^i)_{i \in \mathbb{N}})} : K^2 \rightarrow K$  be the map defined by  $m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y) = \psi^j(x) \cdot \psi^j(y)$  for every  $x \in K$  and  $y \in K$ . (Again, this is really a 2-operation of special  $\lambda$ -rings.)

We want to prove that  $m = m'$ . According to Theorem 8.4, this will be done once we have verified the continuity assumption and the split equality assumption. The continuity assumption is obviously satisfied (since for every ring  $K$ , the maps  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} : (\Lambda(K))^2 \rightarrow \Lambda(K)$  and  $m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})} : (\Lambda(K))^2 \rightarrow \Lambda(K)$  are continuous by Theorem 5.5 **(d)**, because they are polynomials in  $\widehat{\lambda}^1, \widehat{\lambda}^2, \dots, \widehat{\lambda}^j$  with integer coefficients). Hence, it remains to verify the split equality assumption. This assumption claims that for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $(x, y) \in K^2$  such that each of  $x$  and  $y$  is the sum of finitely many 1-dimensional elements of  $K$ , we have  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y) = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y)$ .

Since  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y) = \psi^j(xy)$  and  $m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y) = \psi^j(x) \cdot \psi^j(y)$ , this is equivalent to claiming that for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $(x, y) \in K^2$  such that each of  $x$  and  $y$  is the sum of finitely many 1-dimensional elements of  $K$ , we have  $\psi^j(xy) = \psi^j(x) \cdot \psi^j(y)$ .

So let us verify this assumption. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring, and let  $(x, y) \in K^2$  be such that each of  $x$  and  $y$  is the sum of finitely many 1-dimensional elements of  $K$ . Thus, there exist 1-dimensional elements  $u_1, u_2, \dots, u_m$  of  $K$  such that  $x = u_1 + u_2 + \dots + u_m$ , and there exist 1-dimensional elements  $v_1, v_2, \dots, v_n$  of  $K$  such that  $y = v_1 + v_2 + \dots + v_n$ . Consider these 1-dimensional elements. Then,

$$\begin{aligned}
& m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y) \\
&= \psi^j(xy) = \psi^j((u_1 + u_2 + \dots + u_m)(v_1 + v_2 + \dots + v_n)) \\
&= \psi^j\left(\sum_{i=1}^m u_i \sum_{i'=1}^n v_{i'}\right) = \psi^j\left(\sum_{i=1}^m \sum_{i'=1}^n u_i v_{i'}\right) = \sum_{i=1}^m \sum_{i'=1}^n (u_i v_{i'})^j \\
&\quad \left(\text{by Theorem 9.4, applied to the 1-dimensional elements } u_i v_{i'}, \right. \\
&\quad \left. \text{which are 1-dimensional because of Theorem 8.3 (b)}\right) \\
&= \sum_{i=1}^m \sum_{i'=1}^n u_i^j v_{i'}^j = \sum_{i=1}^m u_i^j \sum_{i'=1}^n v_{i'}^j = \underbrace{(u_1^j + u_2^j + \dots + u_m^j)}_{\substack{= \psi^j(u_1 + u_2 + \dots + u_m) \\ \text{by Theorem 9.4}}} \underbrace{(v_1^j + v_2^j + \dots + v_n^j)}_{\substack{= \psi^j(v_1 + v_2 + \dots + v_n) \\ \text{by Theorem 9.4}}} \\
&= \psi^j\left(\underbrace{u_1 + u_2 + \dots + u_m}_{=x}\right) \cdot \psi^j\left(\underbrace{v_1 + v_2 + \dots + v_n}_{=y}\right) = \psi^j(x) \cdot \psi^j(y) = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x, y),
\end{aligned}$$

and the proof of the split equality assumption is complete. Thus, using Theorem 8.4, we obtain that  $\psi^j(xy) = \psi^j(x) \cdot \psi^j(y)$  holds for any  $x \in K$  and any  $y \in K$ .

The main idea of the above proof was that, using Theorem 8.4, we can reduce our goal - which was to show that  $\psi^j(xy) = \psi^j(x) \cdot \psi^j(y)$  for any  $x \in K$  and  $y \in K$  - to a simpler goal - namely, to prove that *under the additional condition* that each of  $x$  and  $y$  is the sum of finitely many 1-dimensional elements of  $K$ , we have  $\psi^j(xy) = \psi^j(x) \cdot \psi^j(y)$ . In other words, when proving the equality  $\psi^j(xy) = \psi^j(x) \cdot \psi^j(y)$ , we could WLOG assume that each of  $x$  and  $y$  is the sum of finitely many 1-dimensional elements of  $K$ . Under this assumption, the equality  $\psi^j(xy) = \psi^j(x) \cdot \psi^j(y)$  was an easy consequence of Theorem 9.4. This way, we have proven (47). Similarly, we can show (45).

Again, for every  $i \in \mathbb{N}$ , we can use the same tactic to show that  $(\psi^j \circ \lambda^i)(x) = (\lambda^i \circ \psi^j)(x)$  for every  $x \in K$  (namely, we use Theorem 8.4 to reduce the proof to the case when  $x$  is the sum of finitely many 1-dimensional elements of  $K$ , and we apply Theorems 9.4, 8.5 and 8.3 (b) to verify it in this case). Hence,  $\psi^j \circ \lambda^i = \lambda^i \circ \psi^j$  for every  $i \in \mathbb{N}$ , and thus  $\psi^j$  is a  $\lambda$ -ring homomorphism. Theorem 9.3 (b) is proven.

(c) Fix  $i \in \mathbb{N} \setminus \{0\}$  and  $j \in \mathbb{N} \setminus \{0\}$ . We have to prove that  $\psi^i \circ \psi^j = \psi^j \circ \psi^i = \psi^{ij}$ . In other words, we have to prove that  $(\psi^i \circ \psi^j)(x) = (\psi^j \circ \psi^i)(x) = \psi^{ij}(x)$  for every  $x \in K$ . This can be done by the same method as in the proof of part (b): First, reduce the proof to the case when  $x$  is the sum of finitely many 1-dimensional elements of  $K$  (by an application of Theorem 8.4); then, verify  $(\psi^i \circ \psi^j)(x) = (\psi^j \circ \psi^i)(x) = \psi^{ij}(x)$  in this case by applying Theorems 9.4 and 8.3 (b). Thus, Theorem 9.3 (c) is proven.  $\square$

## 9.5. The equality $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$ for arbitrary $\lambda$ -rings

Now, as promised, we are going to prove a generalization of Theorem 9.2 to arbitrary  $\lambda$ -rings:

**Theorem 9.5.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring.

Define a map  $\tilde{\psi}_T : K \rightarrow K[[T]]$  by  $\tilde{\psi}_T(x) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j$  for every

$x \in K$ . <sup>51</sup>

Let  $x \in K$ .

(a) We have

$$\psi^j(x) = (-1)^{j+1} \sum_{i=0}^j i \lambda^i(x) \lambda^{j-i}(-x) \quad \text{for every } j \in \mathbb{N} \setminus \{0\}.$$

(b) We have  $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$ . Here, for every power series  $u \in 1 + K[[T]]^+$ , the *logarithmic derivative*  $\frac{d}{dT} \log u$  of  $u$  is defined by

$$\frac{d}{dT} \log u = \frac{\frac{d}{dT} u}{u} \quad (\text{this definition works even in the cases where the logarithm doesn't exist, such as rings of positive characteristic), and } \lambda_{-T}(x) \text{ denotes } \text{ev}_{-T}(\lambda_T(x)).$$

---

<sup>51</sup>Note that we call this map  $\tilde{\psi}_T$  to distinguish it from the map  $\psi_T$  in [FulLan85] (which is more or less the same but differs slightly).

Before we prove this, let us show a lemma about symmetric polynomials first - a kind of continuation of Theorem 9.1:

**Theorem 9.6.** Let  $m \in \mathbb{N}$ . Let us recall that, for every  $j \in \mathbb{N} \setminus \{0\}$ , we denote by  $N_j$  the  $j$ -th Hirzebruch-Newton polynomial (defined at the beginning of Section 9). Let us also recall that for every  $i \in \mathbb{N}$ , we denote by  $X_i$  the  $i$ -th elementary symmetric polynomial in the polynomial ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ .

Then, every  $n \in \mathbb{N}$  satisfies

$$nX_n = \sum_{j=1}^n (-1)^{j-1} X_{n-j} N_j(X_1, X_2, \dots, X_j)$$

in the ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ .

This theorem is more or less a rewriting of the famous *Newton identities*.

*Proof of Theorem 9.6.* In the power series ring  $(\mathbb{Z}[U_1, U_2, \dots, U_m])[[T]]$ , we have

$$\begin{aligned} \prod_{i=1}^m (1 - U_i T) &= \sum_{i \in \mathbb{N}} (-1)^i \underbrace{\sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k T^i}_{=X_i} \\ &\left( \text{by Exercise 4.2 (c), applied to } A = (\mathbb{Z}[U_1, U_2, \dots, U_m])[[T]], \right. \\ &\quad \left. \alpha_i = U_i \text{ and } t = T \right) \\ &= \sum_{i \in \mathbb{N}} (-1)^i X_i T^i. \end{aligned} \tag{48}$$

But the product rule for several factors says that whenever  $\alpha_1, \alpha_2, \dots, \alpha_m$  are power series in  $\mathbb{K}[[T]]$  (where  $\mathbb{K}$  is a commutative ring), we have

$$\frac{d}{dT} \prod_{i=1}^m \alpha_i = \sum_{j=1}^m \left( \frac{d}{dT} \alpha_j \right) \prod_{\substack{i \in \{1, 2, \dots, m\}; \\ i \neq j}} \alpha_i.$$

Applying this to the power series  $\alpha_i = 1 - U_i T$ , we obtain

$$\begin{aligned}
\frac{d}{dT} \prod_{i=1}^m (1 - U_i T) &= \sum_{j=1}^m \underbrace{\left( \frac{d}{dT} (1 - U_j T) \right)}_{= -U_j = -\frac{U_j}{1 - U_j T} (1 - U_j T)} \prod_{\substack{i \in \{1, 2, \dots, m\}; \\ i \neq j}} (1 - U_i T) \\
&= \sum_{j=1}^m \left( -\frac{U_j}{1 - U_j T} (1 - U_j T) \right) \prod_{\substack{i \in \{1, 2, \dots, m\}; \\ i \neq j}} (1 - U_i T) \\
&= - \sum_{j=1}^m \frac{U_j}{1 - U_j T} (1 - U_j T) \underbrace{\prod_{\substack{i \in \{1, 2, \dots, m\}; \\ i \neq j}} (1 - U_i T)}_{= \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T)} \\
&= - \sum_{j=1}^m \frac{U_j}{1 - U_j T} \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T) = - \sum_{i=1}^m \frac{U_i}{1 - U_i T} \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T) \\
&\quad \text{(here, we renamed } j \text{ as } i \text{ in the first sum).}
\end{aligned}$$

Since

$$\begin{aligned}
&\frac{d}{dT} \prod_{i=1}^m (1 - U_i T) \\
&= \frac{d}{dT} \sum_{i \in \mathbb{N}} (-1)^i X_i T^i \quad \text{(by (48))} \\
&= \sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i X_i i T^{i-1} \quad \text{(by the definition of the derivative of a power series),}
\end{aligned}$$

this rewrites as

$$\sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i X_i i T^{i-1} = - \sum_{i=1}^m \frac{U_i}{1 - U_i T} \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T). \quad (49)$$

Now,

$$\begin{aligned}
\sum_{n \in \mathbb{N}} (-1)^n n X_n T^n &= \sum_{n \in \mathbb{N}} (-1)^n X_n n T^n = \sum_{n \in \mathbb{N} \setminus \{0\}} (-1)^n X_n n T^n + \underbrace{(-1)^0 X_0 0 T^0}_{=0} \\
&= \sum_{n \in \mathbb{N} \setminus \{0\}} (-1)^n X_n n T^n \\
&= \sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i X_i i \underbrace{T^i}_{=T^{i-1}} \quad (\text{here, we renamed } n \text{ as } i) \\
&= T \underbrace{\sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i X_i i T^{i-1}}_{= - \sum_{i=1}^m \frac{U_i}{1 - U_i T} \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T)} = -T \sum_{i=1}^m \frac{U_i}{1 - U_i T} \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T) \\
&= - \sum_{i=1}^m \frac{U_i}{1 - U_i T} \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T) \quad (\text{by (49)}) \\
&= - \underbrace{\left( T \sum_{i=1}^m \frac{U_i}{1 - U_i T} \right)}_{= \sum_{j \in \mathbb{N} \setminus \{0\}} N_j(X_1, X_2, \dots, X_j) T^j \quad (\text{by (41)})} \underbrace{\left( \prod_{i \in \{1, 2, \dots, m\}} (1 - U_i T) \right)}_{= \sum_{i \in \mathbb{N}} (-1)^i X_i T^i \quad (\text{by (48)})} \\
&= - \sum_{j \in \mathbb{N} \setminus \{0\}} N_j(X_1, X_2, \dots, X_j) T^j \cdot \sum_{i \in \mathbb{N}} (-1)^i X_i T^i \\
&= \sum_{j \in \mathbb{N} \setminus \{0\}} N_j(X_1, X_2, \dots, X_j) T^j \cdot \sum_{i \in \mathbb{N}} \left( -(-1)^i \right) X_i T^i \\
&= \sum_{n \in \mathbb{N}} \left( \sum_{j=1}^n N_j(X_1, X_2, \dots, X_j) \left( -(-1)^{n-j} \right) X_{n-j} \right) T^n \\
&\quad (\text{by the definition of the product of two formal power series}).
\end{aligned}$$

Comparing the coefficients before  $T^n$  on the two sides of this equation, we obtain

$$(-1)^n n X_n = \sum_{j=1}^n N_j(X_1, X_2, \dots, X_j) \left( -(-1)^{n-j} \right) X_{n-j}$$

for every  $n \in \mathbb{N}$ . Dividing this equation by  $(-1)^n$ , we arrive at

$$\begin{aligned}
n X_n &= \sum_{j=1}^n N_j(X_1, X_2, \dots, X_j) \underbrace{\frac{-(-1)^{n-j}}{(-1)^n}}_{= -(-1)^{(n-j)-n} = -(-1)^{-j}} X_{n-j} \\
&= - \left( \frac{1}{-1} \right)^j = -(-1)^j = (-1)^{j-1} \\
&= \sum_{j=1}^n N_j(X_1, X_2, \dots, X_j) (-1)^{j-1} X_{n-j} = \sum_{j=1}^n (-1)^{j-1} X_{n-j} N_j(X_1, X_2, \dots, X_j).
\end{aligned}$$

This proves Theorem 9.6. □

As a consequence of Theorem 9.6, we get the following fact (which can be used as a recurrence equation to easily compute the Hirzebruch-Newton polynomials  $N_j$ ):

**Corollary 9.7.** Let us recall that, for every  $j \in \mathbb{N} \setminus \{0\}$ , we denote by  $N_j$  the  $j$ -th Hirzebruch-Newton polynomial (defined at the beginning of Section 9). Then, every  $n \in \mathbb{N}$  satisfies

$$n\alpha_n = \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j)$$

in the polynomial ring  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$ . Here,  $\alpha_0$  is to be understood as 1.

*Proof of Corollary 9.7.* We WLOG assume that  $n > 0$  (since for  $n = 0$ , Corollary 9.7 is trivial).

Let  $\mathfrak{Q}_1 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$  be the polynomial defined by  $\mathfrak{Q}_1 = n\alpha_n$ . Let  $\mathfrak{Q}_2 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$  be the polynomial defined by  $\mathfrak{Q}_2 = \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j)$ .

We are going to prove that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ .

Consider the ring  $\mathbb{Z}[U_1, U_2, \dots, U_n]$  (the polynomial ring in  $n$  indeterminates  $U_1, U_2, \dots, U_n$  over the ring  $\mathbb{Z}$ ). For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, n\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the so-called  $i$ -th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_n$ . (In particular,  $X_0 = 1$  and  $X_i = 0$  for every  $i > n$ .) Applying Theorem 4.1 (a) to  $K = \mathbb{Z}$ ,  $m = n$  and  $P = nX_n$ , we conclude that there exists one and only one polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$  such that  $nX_n = Q(X_1, X_2, \dots, X_n)$ . In particular, there exists *at most one* such polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$ . Hence,

$$\left( \begin{array}{l} \text{if } \mathfrak{Q}_1 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n] \text{ and } \mathfrak{Q}_2 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n] \text{ are two polynomials} \\ \text{such that } nX_n = \mathfrak{Q}_1(X_1, X_2, \dots, X_n) \text{ and } nX_n = \mathfrak{Q}_2(X_1, X_2, \dots, X_n), \\ \text{then } \mathfrak{Q}_1 = \mathfrak{Q}_2 \end{array} \right). \quad (50)$$

Clearly,  $\mathfrak{Q}_1(X_1, X_2, \dots, X_n) = nX_n$  (since  $\mathfrak{Q}_1 = n\alpha_n$ ). On the other hand,

$$\begin{aligned} \mathfrak{Q}_2 &= \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j) \\ &= \sum_{j=1}^{n-1} (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j) + (-1)^{n-1} \underbrace{\alpha_{n-n}}_{=\alpha_0=1} N_n(\alpha_1, \alpha_2, \dots, \alpha_n) \\ &= \sum_{j=1}^{n-1} (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j) + (-1)^{n-1} 1 N_n(\alpha_1, \alpha_2, \dots, \alpha_n), \end{aligned}$$



so that

$$\begin{aligned}
& \mathfrak{Q}_2(X_1, X_2, \dots, X_n) \\
&= \sum_{j=1}^{n-1} (-1)^{j-1} X_{n-j} N_j(X_1, X_2, \dots, X_j) + (-1)^{n-1} \underbrace{1}_{=X_0=X_{n-n}} N_n(X_1, X_2, \dots, X_n) \\
&= \sum_{j=1}^{n-1} (-1)^{j-1} X_{n-j} N_j(X_1, X_2, \dots, X_j) + (-1)^{n-1} X_{n-n} N_n(X_1, X_2, \dots, X_n) \\
&= \sum_{j=1}^n (-1)^{j-1} X_{n-j} N_j(X_1, X_2, \dots, X_j) \\
&= nX_n \quad (\text{by Theorem 9.6, applied to } m = n).
\end{aligned}$$

Hence,  $\mathfrak{Q}_1 = \mathfrak{Q}_2$  (due to (50)). Since  $\mathfrak{Q}_1 = n\alpha_n$  and  $\mathfrak{Q}_2 = \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j)$ , this rewrites as  $n\alpha_n = \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j)$ . This proves Corollary 9.7.  $\square$

*Proof of Theorem 9.5. 1st step:* For any fixed  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and any fixed  $x \in K$ , the assertions **(a)** and **(b)** are equivalent.

*Proof.* This proof is exactly the same as the proof of the 1st step of the proof of Theorem 9.2. (In fact, during the 1st step of the proof of Theorem 9.2, we have never used the assumption that the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special.)

*2nd step:* For any  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and any  $x \in K$ , we have

$$n\lambda^n(x) = \sum_{j=1}^n (-1)^{j-1} \lambda^{n-j}(x) \psi^j(x)$$

for every  $n \in \mathbb{N}$ .

*Proof.* Let  $n \in \mathbb{N}$ . Corollary 9.7 yields

$$\begin{aligned}
n\alpha_n &= \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j) \\
&= \sum_{j=1}^{n-1} (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j) + (-1)^{n-1} \underbrace{\alpha_{n-n}}_{=\alpha_0=1} N_n(\alpha_1, \alpha_2, \dots, \alpha_n) \\
&= \sum_{j=1}^{n-1} (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j) + (-1)^{n-1} 1 N_n(\alpha_1, \alpha_2, \dots, \alpha_n).
\end{aligned}$$

This is a polynomial identity in  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$ . Hence, we can apply this identity to

$\alpha_1 = \lambda^1(x)$ ,  $\alpha_2 = \lambda^2(x)$ , ...,  $\alpha_n = \lambda^n(x)$ , and obtain

$$\begin{aligned}
n\lambda^n(x) &= \sum_{j=1}^{n-1} (-1)^{j-1} \lambda^{n-j}(x) N_j(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) \\
&\quad + (-1)^{n-1} \underbrace{1}_{=\lambda^0(x)=\lambda^{n-n}(x)} N_n(\lambda^1(x), \lambda^2(x), \dots, \lambda^n(x)) \\
&= \sum_{j=1}^{n-1} (-1)^{j-1} \lambda^{n-j}(x) N_j(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) \\
&\quad + (-1)^{n-1} \lambda^{n-n}(x) N_n(\lambda^1(x), \lambda^2(x), \dots, \lambda^n(x)) \\
&= \sum_{j=1}^n (-1)^{j-1} \lambda^{n-j}(x) \underbrace{N_j(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))}_{=\psi^j(x)} \\
&= \sum_{j=1}^n (-1)^{j-1} \lambda^{n-j}(x) \psi^j(x).
\end{aligned}$$

This proves the 2nd step.

*3rd step:* For any  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and any  $x \in K$ , we have

$$-T \cdot \frac{d}{dT} \lambda_T(x) = \lambda_T(x) \cdot \tilde{\psi}_{-T}(x),$$

where we denote the power series  $\text{ev}_{-T}(\tilde{\psi}_T(x))$  by  $\tilde{\psi}_{-T}(x)$ .

*Proof.* We have

$$\begin{aligned}
\tilde{\psi}_{-T}(x) &= \text{ev}_{-T}(\tilde{\psi}_T(x)) \\
&= \text{ev}_{-T} \left( \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j \right) \quad \left( \text{since } \tilde{\psi}_T(x) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j \right) \\
&= \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) \underbrace{(-T)^j}_{=(-1)^j T^j} \quad (\text{by the definition of } \text{ev}_{-T}) \\
&= \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) \underbrace{(-1)^j}_{=-(-1)^{j-1}} T^j = - \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) (-1)^{j-1} T^j,
\end{aligned}$$

so that

$$-\tilde{\psi}_{-T}(x) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) (-1)^{j-1} T^j.$$

Multiplying this formula with the equality  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$ , we obtain

$$\begin{aligned}
(-\tilde{\psi}_{-T}(x)) \cdot \lambda_T(x) &= \left( \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) (-1)^{j-1} T^j \right) \cdot \left( \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \right) \\
&= \sum_{n \in \mathbb{N}} \left( \sum_{j=1}^n \psi^j(x) (-1)^{j-1} \lambda^{n-j}(x) \right) T^n \\
&\quad \text{(by the definition of the product of two power series)} \\
&= \sum_{n \in \mathbb{N}} \underbrace{\left( \sum_{j=1}^n (-1)^{j-1} \lambda^{n-j}(x) \psi^j(x) \right)}_{=n\lambda^n(x)} T^n = \sum_{n \in \mathbb{N}} n\lambda^n(x) T^n \\
&\quad \text{(by the 2nd step)} \\
&= \sum_{n \in \mathbb{N} \setminus \{0\}} n\lambda^n(x) T^n + \underbrace{0\lambda^0(x) T^0}_{=0} = \sum_{n \in \mathbb{N} \setminus \{0\}} n\lambda^n(x) \underbrace{T^n}_{=TT^{n-1}} \\
&= T \cdot \sum_{n \in \mathbb{N} \setminus \{0\}} n\lambda^n(x) T^{n-1}.
\end{aligned}$$

Now,  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i = \sum_{n \in \mathbb{N}} \lambda^n(x) T^n$ , so that

$$\begin{aligned}
\frac{d}{dT} \lambda_T(x) &= \frac{d}{dT} \sum_{n \in \mathbb{N}} \lambda^n(x) T^n = \sum_{n \in \mathbb{N} \setminus \{0\}} n\lambda^n(x) T^{n-1} \\
&\quad \text{(by the definition of the derivative of a formal power series),}
\end{aligned}$$

and thus

$$\begin{aligned}
-T \cdot \frac{d}{dT} \lambda_T(x) &= -T \cdot \underbrace{\sum_{n \in \mathbb{N} \setminus \{0\}} n\lambda^n(x) T^{n-1}}_{=(-\tilde{\psi}_{-T}(x)) \cdot \lambda_T(x)} = -(-\tilde{\psi}_{-T}(x)) \cdot \lambda_T(x) \\
&= \lambda_T(x) \cdot \tilde{\psi}_{-T}(x).
\end{aligned}$$

This proves the 3rd step.

*4th step:* For any fixed  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and any fixed  $x \in K$ , the assertion **(b)** holds.

*Proof.* By the 3rd step, we have

$$-T \cdot \frac{d}{dT} \lambda_T(x) = \lambda_T(x) \cdot \tilde{\psi}_{-T}(x).$$

Now, every formal power series  $\alpha \in K[[T]]$  satisfies  $\text{ev}_{-T} \left( \frac{d}{dT} \alpha \right) = -\frac{d}{dT} (\text{ev}_{-T} \alpha)$ .

<sup>52</sup> Applied to  $\alpha = \lambda_T(x)$ , this yields  $\text{ev}_{-T} \left( \frac{d}{dT} \lambda_T(x) \right) = -\frac{d}{dT} (\text{ev}_{-T} (\lambda_T(x)))$ . Since

---

<sup>52</sup>*Proof.* Let  $\alpha \in K[[T]]$  be a formal power series. Write  $\alpha$  in the form  $\sum_{i \in \mathbb{N}} \alpha_i T^i$  with  $\alpha_i \in K$  for every

$\text{ev}_{-T}(\lambda_T(x)) = \lambda_{-T}(x)$ , this rewrites as  $\text{ev}_{-T}\left(\frac{d}{dT}\lambda_T(x)\right) = -\frac{d}{dT}\lambda_{-T}(x)$ . On the other hand, every formal power series  $\alpha \in K[[T]]$  satisfies  $\text{ev}_{-T}(\text{ev}_{-T}\alpha) = \alpha$ .<sup>53</sup> Applied to  $\alpha = \tilde{\psi}_T(x)$ , this yields  $\text{ev}_{-T}\left(\text{ev}_{-T}\left(\tilde{\psi}_T(x)\right)\right) = \tilde{\psi}_T(x)$ . Since  $\text{ev}_{-T}\left(\tilde{\psi}_T(x)\right) = \tilde{\psi}_{-T}(x)$ , this becomes  $\text{ev}_{-T}\left(\tilde{\psi}_{-T}(x)\right) = \tilde{\psi}_T(x)$ .

---

$i \in \mathbb{N}$ . Then,  $\text{ev}_{-T}\alpha = \text{ev}_{-T}\left(\sum_{i \in \mathbb{N}} \alpha_i T^i\right) = \sum_{i \in \mathbb{N}} \alpha_i (-1)^i T^i$  (by the definition of  $\text{ev}_{-T}$ ), so that

$$\frac{d}{dT}(\text{ev}_{-T}\alpha) = \frac{d}{dT} \sum_{i \in \mathbb{N}} \alpha_i (-1)^i T^i = \sum_{i \in \mathbb{N} \setminus \{0\}} \alpha_i (-1)^i i T^{i-1}$$

(by the definition of the derivative of a formal power series).

On the other hand,  $\alpha = \sum_{i \in \mathbb{N}} \alpha_i T^i$ , so that

$$\begin{aligned} \frac{d}{dT}\alpha &= \frac{d}{dT} \sum_{i \in \mathbb{N}} \alpha_i T^i = \sum_{i \in \mathbb{N} \setminus \{0\}} \alpha_i i T^{i-1} \\ &\quad \text{(by the definition of the derivative of a formal power series)} \\ &= \sum_{i \in \mathbb{N}} \alpha_{i+1} (i+1) T^i \end{aligned}$$

(here we substituted  $i$  for  $i-1$ ). Thus,

$$\begin{aligned} \text{ev}_{-T}\left(\frac{d}{dT}\alpha\right) &= \text{ev}_{-T}\left(\sum_{i \in \mathbb{N}} \alpha_{i+1} (i+1) T^i\right) = \sum_{i \in \mathbb{N}} \alpha_{i+1} (i+1) (-1)^i T^i \\ &\quad \text{(by the definition of } \text{ev}_{-T}\text{)} \\ &= \sum_{i \in \mathbb{N} \setminus \{0\}} \alpha_i i \underbrace{(-1)^{i-1}}_{=-(-1)^i} T^{i-1} \quad \text{(here, we substituted } i \text{ for } i+1\text{)} \\ &= - \sum_{i \in \mathbb{N} \setminus \{0\}} \alpha_i i \underbrace{(-1)^i}_{=(-1)^i} T^{i-1} = - \underbrace{\sum_{i \in \mathbb{N} \setminus \{0\}} \alpha_i (-1)^i i T^{i-1}}_{=\frac{d}{dT}(\text{ev}_{-T}\alpha)} = -\frac{d}{dT}(\text{ev}_{-T}\alpha), \end{aligned}$$

qed.

<sup>53</sup>*Proof.* Let  $\alpha \in K[[T]]$  be a formal power series. Write  $\alpha$  in the form  $\sum_{i \in \mathbb{N}} \alpha_i T^i$  with  $\alpha_i \in K$  for every

$i \in \mathbb{N}$ . Then,  $\text{ev}_{-T}\alpha = \text{ev}_{-T}\left(\sum_{i \in \mathbb{N}} \alpha_i T^i\right) = \sum_{i \in \mathbb{N}} \alpha_i (-1)^i T^i$  (by the definition of  $\text{ev}_{-T}$ ), so that

$$\begin{aligned} \text{ev}_{-T}(\text{ev}_{-T}\alpha) &= \text{ev}_{-T}\left(\sum_{i \in \mathbb{N}} \alpha_i (-1)^i T^i\right) = \sum_{i \in \mathbb{N}} \alpha_i \underbrace{(-1)^i (-1)^i}_{=1} T^i \quad \text{(by the definition of } \text{ev}_{-T}\text{)} \\ &= \sum_{i \in \mathbb{N}} \alpha_i T^i = \alpha, \end{aligned}$$

qed.

Now,

$$\begin{aligned} \text{ev}_{-T} \left( -T \cdot \frac{d}{dT} \lambda_T(x) \right) &= - \underbrace{\text{ev}_{-T}(T)}_{=-T} \cdot \underbrace{\text{ev}_{-T} \left( \frac{d}{dT} \lambda_T(x) \right)}_{=\frac{d}{dT} \lambda_{-T}(x)} \\ &\quad (\text{since } \text{ev}_{-T} \text{ is a } K\text{-algebra homomorphism}) \\ &= -T \cdot \frac{d}{dT} \lambda_{-T}(x) \end{aligned}$$

and

$$\begin{aligned} \text{ev}_{-T} \left( \lambda_T(x) \cdot \tilde{\psi}_{-T}(x) \right) &= \underbrace{\text{ev}_{-T}(\lambda_T(x))}_{=\lambda_{-T}(x)} \cdot \underbrace{\text{ev}_{-T}(\tilde{\psi}_{-T}(x))}_{=\tilde{\psi}_T(x)} \\ &\quad (\text{since } \text{ev}_{-T} \text{ is a } K\text{-algebra homomorphism}) \\ &= \lambda_{-T}(x) \cdot \tilde{\psi}_T(x). \end{aligned}$$

Hence,

$$-T \cdot \frac{d}{dT} \lambda_{-T}(x) = \text{ev}_{-T} \left( \underbrace{-T \cdot \frac{d}{dT} \lambda_T(x)}_{=\lambda_T(x) \cdot \tilde{\psi}_{-T}(x)} \right) = \text{ev}_{-T} \left( \lambda_T(x) \cdot \tilde{\psi}_{-T}(x) \right) = \lambda_{-T}(x) \cdot \tilde{\psi}_T(x),$$

so that

$$\tilde{\psi}_T(x) = \frac{-T \cdot \frac{d}{dT} \lambda_{-T}(x)}{\lambda_{-T}(x)} = -T \cdot \underbrace{\frac{\frac{d}{dT} \lambda_{-T}(x)}{\lambda_{-T}(x)}}_{=\frac{d}{dT} \log \lambda_{-T}(x)} = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x).$$

Hence, assertion **(b)** holds. This completes the proof of the 4th step.

*5th step:* For any fixed  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and any fixed  $x \in K$ , the assertion **(a)** holds.

*Proof.* This follows from the 4th step, since **(a)** and **(b)** are equivalent (by the 1st step).

Thus, the proof of Theorem 9.5 is complete.  $\square$

Theorem 9.5 is clearly a generalization of Theorem 9.2, and thus our above proof of Theorem 9.5 is, at the same time, a new proof of Theorem 9.2.

## 9.6. Exercises

*Exercise 9.1.* Let  $K$  be a ring. Let  $u \in 1 + K[T]^+$ . For every  $j \in \mathbb{N} \setminus \{0\}$ , let us denote by  $\widehat{\psi}^j$  the  $j$ -th Adams operation of the  $\lambda$ -ring  $(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$ .

Assume that  $u = \Pi \left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right)$  for some  $\left( \tilde{K}_u, [u_1, u_2, \dots, u_m] \right) \in K^{\text{int}}$ . Let  $j \in \mathbb{N} \setminus \{0\}$ . Then,  $\widehat{\psi}^j(u) = \Pi \left( \tilde{K}_u, [u_1^j, u_2^j, \dots, u_m^j] \right)$ .

[This gives a formula for  $\widehat{\psi}^j$  similar to the formula for  $\widehat{\lambda}^j$  given in Theorem 5.3 (d).]

*Exercise 9.2.* Let  $K$  be a ring. For each  $i \in \mathbb{N}$ , define a mapping  $\text{Coeff}_i : K[[T]] \rightarrow K$  as in Exercise 6.8.

Let  $i \in \mathbb{N} \setminus \{0\}$ .

(a) Prove that the map

$$\Lambda(K) \rightarrow K,$$

$$u \mapsto (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log u \right)$$

is a ring homomorphism.

(b) This fact, combined with Theorem 9.2 (b), can be used to give a new proof of a part of Theorem 9.3 (b). Which part, and how?

*Exercise 9.3.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring.

(a) Prove that

$$n\lambda^n(x) = \sum_{i=1}^n (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x) \quad \text{for every } x \in K \text{ and } n \in \mathbb{N}.$$

(b) Let  $x \in K$  and  $n \in \mathbb{N}$ . Let  $A_n = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in K^{n \times n}$  be the matrix defined by

$$a_{i,j} = \begin{cases} \psi^{i-j+1}(x), & \text{if } i \geq j; \\ i, & \text{if } i = j - 1; \\ 0, & \text{if } i < j - 1 \end{cases}.$$

Prove that  $n!\lambda^n(x) = \det A_n$ .

[The matrix  $A_n$  has the following form:

$$A_n = \begin{pmatrix} \psi^1(x) & 1 & 0 & \cdots & 0 & 0 \\ \psi^2(x) & \psi^1(x) & 2 & \cdots & 0 & 0 \\ \psi^3(x) & \psi^2(x) & \psi^1(x) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \psi^{n-1}(x) & \psi^{n-2}(x) & \psi^{n-3}(x) & \cdots & \psi^1(x) & n-1 \\ \psi^n(x) & \psi^{n-1}(x) & \psi^{n-2}(x) & \cdots & \psi^2(x) & \psi^1(x) \end{pmatrix}.$$

]

(c) Let  $x \in K$  and  $n \in \mathbb{N}$ . Let  $B_n = (b_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in K^{n \times n}$  be the matrix defined by

$$b_{i,j} = \begin{cases} i\lambda^i(x), & \text{if } j = 1; \\ \lambda^{i-j+1}(x), & \text{if } i \geq j > 1; \\ 1, & \text{if } i = j - 1; \\ 0, & \text{if } i < j - 1 \end{cases}.$$

Prove that  $\psi^n(x) = \det B_n$ , where we define  $\psi^0(x)$  to mean 1.

[The matrix  $B_n$  has the following form:

$$B_n = \begin{pmatrix} \lambda^1(x) & 1 & 0 & \cdots & 0 & 0 \\ 2\lambda^2(x) & \lambda^1(x) & 1 & \cdots & 0 & 0 \\ 3\lambda^3(x) & \lambda^2(x) & \lambda^1(x) & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)\lambda^{n-1}(x) & \lambda^{n-2}(x) & \lambda^{n-3}(x) & \cdots & \lambda^1(x) & 1 \\ n\lambda^n(x) & \lambda^{n-1}(x) & \lambda^{n-2}(x) & \cdots & \lambda^2(x) & \lambda^1(x) \end{pmatrix}.$$

]

*Exercise 9.4.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a binomial  $\lambda$ -ring. Prove that  $\psi^n = \text{id}$  for every  $n \in \mathbb{N} \setminus \{0\}$ .

[Note that, if we recall the definition of a binomial  $\lambda$ -ring and Exercise 9.3 (c), then we could reformulate this result without reference to  $\lambda$ -rings.]

*Exercise 9.5.* Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a (not necessarily special)  $\lambda$ -ring. Prove that  $\psi^j : K \rightarrow K$  is a homomorphism of additive groups for every  $j \in \mathbb{N} \setminus \{0\}$ .

[This shows that at least part of Theorem 9.3 (b) does not require the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  to be special.]

*Exercise 9.6.* In this exercise, we are going to view  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  as a subring of  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$  for any two  $m \in \mathbb{N}$  and  $n \in \mathbb{N}$  satisfying  $m \leq n$ . Thus, the polynomial  $N_m \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  automatically becomes an element of  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$  whenever  $1 \leq m \leq n$ .

(a) Prove that

$$n\alpha_n = \sum_{i=1}^n (-1)^{i-1} \alpha_{n-i} N_i \text{ in } \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n] \quad \text{for every } n \in \mathbb{N}.$$

Here,  $\alpha_0$  is to be understood as 1.

(b) Let  $n \in \mathbb{N}$ . Let  $A_n = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]^{n \times n}$  be the matrix defined by

$$a_{i,j} = \begin{cases} N_{i-j+1}, & \text{if } i \geq j; \\ i, & \text{if } i = j - 1; \\ 0, & \text{if } i < j - 1 \end{cases}.$$

Prove that  $n!\alpha_n = \det A_n$ .

[The matrix  $A_n$  has the following form:

$$A_n = \begin{pmatrix} N_1 & 1 & 0 & \cdots & 0 & 0 \\ N_2 & N_1 & 2 & \cdots & 0 & 0 \\ N_3 & N_2 & N_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ N_{n-1} & N_{n-2} & N_{n-3} & \cdots & N_1 & n-1 \\ N_n & N_{n-1} & N_{n-2} & \cdots & N_2 & N_1 \end{pmatrix}.$$

]

(c) Let  $n \in \mathbb{N}$ . Let  $B_n = (b_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]^{n \times n}$  be the matrix defined by

$$b_{i,j} = \begin{cases} i\alpha_i, & \text{if } j = 1; \\ \alpha_{i-j+1}, & \text{if } i \geq j > 1; \\ 1, & \text{if } i = j - 1; \\ 0, & \text{if } i < j - 1 \end{cases}.$$

Prove that  $N_n = \det B_n$ , where we define  $N_0$  to mean 1.

[The matrix  $B_n$  has the following form:

$$B_n = \begin{pmatrix} \alpha_1 & 1 & 0 & \cdots & 0 & 0 \\ 2\alpha_2 & \alpha_1 & 1 & \cdots & 0 & 0 \\ 3\alpha_3 & \alpha_2 & \alpha_1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ (n-1)\alpha_{n-1} & \alpha_{n-2} & \alpha_{n-3} & \cdots & \alpha_1 & 1 \\ n\alpha_n & \alpha_{n-1} & \alpha_{n-2} & \cdots & \alpha_2 & \alpha_1 \end{pmatrix}.$$

]

(d) Derive the results of Exercise 9.3 from Exercise 9.6 (a), (b), (c).

*Exercise 9.7.* Let  $p$  be a prime number. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a (not necessarily special)  $\lambda$ -ring. Prove that  $\psi^p(x) \equiv x^p \pmod{pK}$  for every  $x \in K$ .

## 10. Todd homomorphisms of power series

We now devote a section to the notion of Todd homomorphisms. First, two warnings:

- **Warning:** The following may be wrong or differ from the standard notations. I am trying to generalize [FulLan85, I §6] (mostly because it is slightly flawed<sup>54</sup> and the generalization looks more natural to me), but I cannot guarantee that this is the “right” generalization.
- **Another warning:** In the following, we will often formulate results over a ring which we will call  $\mathbf{Z}$ . The letter  $\mathbf{Z}$  will denote any ring (commutative with unity, of course). Please don’t confuse it with the similarly-looking letter  $\mathbb{Z}$ , which always denote the ring of integers. The reason why I chose the letter  $\mathbf{Z}$  for the ring is that in most applications the ring  $\mathbf{Z}$  will indeed be the ring  $\mathbb{Z}$  of integers.

### 10.1. The universal polynomials $\text{Td}_{\varphi,j}$

We begin this section with a construction similar to the construction of the Adams operations in Section 9. The goal of this construction is to find, for every ring  $\mathbf{Z}$  (in most cases, this ring will be the ring  $\mathbb{Z}$  of integers) and every power series  $\varphi \in 1 + \mathbf{Z}[[t]]^+$

<sup>54</sup>[FulLan85, I §6, p. 24] states that  $\text{td}_{\varphi}(e)$  is a universal polynomial in  $\lambda^1(e), \dots, \lambda^r(e)$ , determined by  $\varphi$  alone. I think it isn’t; instead, it is just a power series. On the other hand, my generalization  $\text{td}_{\varphi,T}$  is a universal polynomial.



with constant term equal to 1, a polynomial  $\text{Td}_{\varphi,j} \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  for every  $j \in \mathbb{N}$  such that

$$\prod_{i=1}^m \varphi(U_i T) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j) T^j$$

in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$  for every  $m \in \mathbb{N}$ , where  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\} \\ |S|=i}} \prod_{k \in S} U_k$  as

usual. To achieve this goal, we must again work with symmetric polynomials. First a definition:

**Definition.** Let  $R$  be any ring. Let  $i \in \mathbb{N}$ . Then, we define a map  $\text{Coeff}_i : R[[T]] \rightarrow R$  (where  $R[[T]]$  is, as always, the  $R$ -algebra of all formal power series in the variable  $T$  over the ring  $R$ ) by

$$\left( \begin{array}{l} \text{Coeff}_i(P) = (\text{the coefficient of } P \text{ before } T^i) \\ \text{for every power series } P \in R[[T]] \end{array} \right).$$

In other words, we define a map  $\text{Coeff}_i : R[[T]] \rightarrow R$  by

$$\left( \begin{array}{l} \text{Coeff}_i \left( \sum_{j \in \mathbb{N}} a_j T^j \right) = a_i \\ \text{for every } \sum_{j \in \mathbb{N}} a_j T^j \in R[[T]] \text{ (with } a_j \in R \text{ for every } j \in \mathbb{N}) \end{array} \right).$$

Two remarks about this definition:

- The definition of  $\text{Coeff}_i$  that we just gave is clearly equivalent to the definition of  $\text{Coeff}_i$  given in Exercise 9.2.
- The only difference between the map  $\text{Coeff}_i$  just defined and the map  $\text{coeff}_i$  defined in Exercise 6.5 is that they have different domains (namely, the map  $\text{Coeff}_i$  is defined on all of  $R[[T]]$ , whereas the map  $\text{coeff}_i$  is defined only on  $\Lambda(R)$ ). This looks like a minor difference, but is substantial enough to cause confusion if we neglect it! For example, when we say that  $\text{coeff}_i$  is a homomorphism of additive groups, we mean that it maps sums in  $\Lambda(R)$  to sums in  $R$ ; however, when we say that  $\text{Coeff}_i$  is a homomorphism of additive groups, we mean that it maps sums in  $R[[T]]$  to sums in  $R$ . These are two completely different assertions, even though  $\Lambda(R)$  is a subset of  $R[[T]]$  and the maps  $\text{coeff}_i$  and  $\text{Coeff}_i$  are pointwise equal on this subset! (Actually, it is very easy to see that the assertion that  $\text{coeff}_i$  is a homomorphism of additive groups is completely different from the assertion that  $\text{Coeff}_i$  is a homomorphism of additive groups. The latter assertion holds for all  $i \in \mathbb{N}$ , whereas the former assertion holds only for  $i = 1$  (in general).)
- It is clear that for every ring  $R$  and for every  $i \in \mathbb{N}$ , the map  $\text{Coeff}_i : R[[T]] \rightarrow R$  is an additive group homomorphism. It is also clear that if two power series  $P \in R[[T]]$  and  $Q \in R[[T]]$  satisfy  $(\text{Coeff}_i(P) = \text{Coeff}_i(Q))$  for all  $i \in \mathbb{N}$ , then  $P = Q$ .

Now let us define what we mean by  $1 + \mathbf{Z}[[t]]^+$ :

**Definition.** Let  $\mathbf{Z}$  be a ring. Consider the ring  $\mathbf{Z}[[t]]$  of formal power series in the variable  $t$  over  $\mathbf{Z}$ . Let  $\mathbf{Z}[[t]]^+$  denote the subset

$$\begin{aligned} t\mathbf{Z}[[t]] &= \left\{ \sum_{i \in \mathbb{N}} a_i t^i \in \mathbf{Z}[[t]] \mid a_i \in \mathbf{Z} \text{ for all } i, \text{ and } a_0 = 0 \right\} \\ &= \{p \in \mathbf{Z}[[t]] \mid p \text{ is a power series with constant term } 0\} \end{aligned}$$

of the ring  $\mathbf{Z}[[t]]$ . Note that

$$\begin{aligned} 1 + \mathbf{Z}[[t]]^+ &= \{1 + u \mid u \in \mathbf{Z}[[t]]^+\} \\ &= \{p \in \mathbf{Z}[[t]] \mid p \text{ is a power series with constant term } 1\}. \end{aligned}$$

We notice that this is an exact copy of a definition we made in Section 5 (namely, of the definition of  $K[[T]]^+$ ), with the only difference that the ring that used to be called  $K$  in Section 5 is called  $\mathbf{Z}$  here, and that the variable that used to be  $T$  in Section 5 is  $t$  here.

Now to our universal polynomials:

**Definition.** Let  $\mathbf{Z}$  be a ring. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Our goal is to define a polynomial  $\text{Td}_{\varphi,j} \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  for every  $j \in \mathbb{N}$  such that

$$\prod_{i=1}^m \varphi(U_i T) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j) T^j \quad (51)$$

in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$  for every  $m \in \mathbb{N}$ , where  $X_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; k \in S \\ |S|=i}} \prod U_k$

is the  $i$ -th elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$  for every  $i \in \mathbb{N}$ .

In order to do this, we first fix some  $m \in \mathbb{N}$  and  $j \in \mathbb{N}$ . Consider the polynomial  $\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right) \in \mathbf{Z}[U_1, U_2, \dots, U_m]$  (this is the coefficient of the power series  $\prod_{i=1}^m \varphi(U_i T) \in (\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$  before  $T^j$ ). This polynomial  $\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right)$  is symmetric. Thus, Theorem 4.1 (a) yields that there exists one and only one polynomial  $\text{Todd}_{(\varphi,j)} \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  such that  $\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Todd}_{(\varphi,j)}(X_1, X_2, \dots, X_m)$ . Since  $\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right)$  is a polynomial of total degree  $\leq j$  in the variables  $U_1, U_2, \dots, U_m$ <sup>55</sup>,

<sup>55</sup>*Proof.* There are several ways to prove this; here is the simplest one: We use the notion of an “equigraded” power series over a graded ring; this notion was defined in [Grin-w4a]. Now let  $A$  be the graded ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$ , where the grading is given by the total degree (thus  $U_1, U_2, \dots, U_m$  all lie in the 1-st graded component  $A_1$ ). According to [Grin-w4a, Theorem 1 (a)], the set

$$\{\alpha \in A[[T]] \mid \text{the power series } \alpha \text{ is equigraded}\}$$

Theorem 4.1 (b) yields that

$$\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Todd}_{(\varphi,j),j}(X_1, X_2, \dots, X_j),$$

where  $\text{Todd}_{(\varphi,j),j}$  is the image of the polynomial  $\text{Todd}_{(\varphi,j)}$  under the canonical homomorphism  $\mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_m] \rightarrow \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$ . However, this polynomial  $\text{Todd}_{(\varphi,j),j}$  is not independent of  $m$  yet (as the polynomial  $\text{Td}_{\varphi,j}$  that we intend to construct should be), so we call it  $\text{Todd}_{(\varphi,j),j,[m]}$  rather than just  $\text{Todd}_{(\varphi,j),j}$ .

Now we forget that we fixed  $m \in \mathbb{N}$  (but still fix  $j \in \mathbb{N}$ ). We have learnt that

$$\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j)$$

in the polynomial ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$  for every  $m \in \mathbb{N}$ . Now, define a polynomial  $\text{Td}_{\varphi,j} \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  by  $\text{Td}_{\varphi,j} = \text{Todd}_{(\varphi,j),j,[j]}$ .

This polynomial  $\text{Td}_{\varphi,j}$  is called the  *$j$ -th Todd polynomial of  $\varphi$* .

**Theorem 10.1.** The polynomials  $\text{Td}_{\varphi,j}$  just defined satisfy the equation (51) in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$  for every  $m \in \mathbb{N}$ . (Hence, the goal mentioned above in the definition is actually achieved.)

Before we prove this, we need a lemma; it is not really a fact of independent importance, but if we don't formulate it as a lemma we will have to run through its proof several times:

**Lemma 10.2.** Let  $\mathbf{Z}$  be a ring. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $m \in \mathbb{N}$  and  $n \in \mathbb{N}$  be such that  $m \geq n$ . Then, in the polynomial ring  $\mathbf{Z}[U_1, U_2, \dots, U_n]$ , we have  $\text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j) = \text{Todd}_{(\varphi,j),j,[n]}(X_1, X_2, \dots, X_j)$ .

*Proof of Lemma 10.2.* By the definition of  $\text{Todd}_{(\varphi,j),j,[m]}$ , we have

$$\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j) \quad (52)$$

---

is a sub- $A_0$ -algebra of  $A[[T]]$ . Since the power series  $\varphi(U_1 T), \varphi(U_2 T), \dots, \varphi(U_m T)$  all lie in this set (because they are equigraded - just look at them), it therefore follows that  $\prod_{i=1}^m \varphi(U_i T)$  also lies in this set. In other words, the power series  $\prod_{i=1}^m \varphi(U_i T)$  is equigraded. Hence, the coefficient of the power series  $\prod_{i=1}^m \varphi(U_i T)$  before  $T^j$  lies in the  $j$ -th graded component of  $A$  (by the definition of "equigraded"). In other words, the coefficient of the power series  $\prod_{i=1}^m \varphi(U_i T)$  before  $T^j$  is a homogeneous polynomial of degree  $j$  in the variables  $U_1, U_2, \dots, U_m$ . Since this coefficient is  $\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right)$ , this yields that  $\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right)$  is a homogeneous polynomial of degree  $j$  in the variables  $U_1, U_2, \dots, U_m$ . Hence,  $\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right)$  is a polynomial of total degree  $\leq j$  in the variables  $U_1, U_2, \dots, U_m$ .

in the polynomial ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$ .

Let  $\text{proj}_{m,n}$  be the canonical  $\mathbf{Z}$ -algebra epimorphism  $\mathbf{Z}[U_1, U_2, \dots, U_m] \rightarrow \mathbf{Z}[U_1, U_2, \dots, U_n]$

which maps every  $U_i$  to  $\begin{cases} U_i, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases}$ . This  $\mathbf{Z}$ -algebra homomorphism  $\text{proj}_{m,n}$  induces a  $\mathbf{Z}$ -algebra homomorphism  $\text{proj}_{m,n}[[T]] : (\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]] \rightarrow (\mathbf{Z}[U_1, U_2, \dots, U_n])[[T]]$

which maps every power series  $\sum_{k \in \mathbb{N}} a_k T^k$  (with  $a_k \in \mathbf{Z}[U_1, U_2, \dots, U_m]$  for every  $k \in \mathbb{N}$ ) to  $\sum_{k \in \mathbb{N}} \text{proj}_{m,n}(a_k) T^k$ . For every  $i \in \{1, 2, \dots, m\}$ , this homomorphism  $\text{proj}_{m,n}[[T]]$  satisfies  $(\text{proj}_{m,n}[[T]])(\varphi(U_i T)) = \begin{cases} \varphi(U_i T), & \text{if } i \leq n; \\ 1, & \text{if } i > n \end{cases}$  <sup>56</sup>. Now, since  $\text{proj}_{m,n}[[T]]$  is

<sup>56</sup>*Proof.* Write the power series  $\varphi \in \mathbf{Z}[[t]]$  in the form  $\varphi = \sum_{k \in \mathbb{N}} \varphi_k t^k$  with  $\varphi_k \in \mathbf{Z}$  for every  $k \in \mathbb{N}$ . Notice that  $\varphi_0 = 1$  since  $\varphi$  has constant term 1. Let  $i \in \{1, 2, \dots, m\}$ . Since  $\varphi = \sum_{k \in \mathbb{N}} \varphi_k t^k$ , we have  $\varphi(U_i T) = \sum_{k \in \mathbb{N}} \varphi_k \underbrace{(U_i T)^k}_{=U_i^k T^k} = \sum_{k \in \mathbb{N}} \varphi_k U_i^k T^k$ .

Thus,

$$\begin{aligned} & (\text{proj}_{m,n}[[T]])(\varphi(U_i T)) \\ &= (\text{proj}_{m,n}[[T]]) \left( \sum_{k \in \mathbb{N}} \varphi_k U_i^k T^k \right) = \sum_{k \in \mathbb{N}} \underbrace{\text{proj}_{m,n}(\varphi_k U_i^k)}_{= \varphi_k (\text{proj}_{m,n} U_i)^k} T^k \quad (\text{by the definition of } \text{proj}_{m,n}[[T]]) \\ & \quad (\text{since } \text{proj}_{m,n} \text{ is a } \mathbf{Z}\text{-algebra homomorphism}) \\ &= \sum_{k \in \mathbb{N}} \varphi_k (\text{proj}_{m,n} U_i)^k T^k = \sum_{k \in \mathbb{N}} \varphi_k \left( \begin{cases} U_i, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases} \right)^k T^k \\ & \quad \left( \text{since } \text{proj}_{m,n} U_i = \begin{cases} U_i, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases} \text{ by the definition of } \text{proj}_{m,n} \right) \\ &= \begin{cases} \sum_{k \in \mathbb{N}} \varphi_k U_i^k T^k, & \text{if } i \leq n; \\ \sum_{k \in \mathbb{N}} \varphi_k 0^k T^k, & \text{if } i > n \end{cases} = \begin{cases} \varphi(U_i T), & \text{if } i \leq n; \\ 1, & \text{if } i > n \end{cases} \\ & \quad \left( \begin{array}{l} \text{since } \sum_{k \in \mathbb{N}} \varphi_k U_i^k T^k = \varphi(U_i T) \text{ for } i \leq n, \text{ but on the other hand} \\ \sum_{k \in \mathbb{N}} \varphi_k 0^k T^k = \underbrace{\varphi_0}_{=1} \underbrace{0^0}_{=1} \underbrace{T^0}_{=1} + \sum_{\substack{k \in \mathbb{N}; \\ k \neq 0}} \varphi_k \underbrace{0^k}_{=0} T^k = 1 + \underbrace{\sum_{\substack{k \in \mathbb{N}; \\ k \neq 0}} \varphi_k 0 T^k}_{=0} = 1 \text{ for } i > n \end{array} \right), \end{aligned}$$

qed.

a  $\mathbf{Z}$ -algebra homomorphism, we have

$$\begin{aligned}
(\text{proj}_{m,n} [[T]]) \left( \prod_{i=1}^m \varphi(U_i T) \right) &= \prod_{i=1}^m \underbrace{(\text{proj}_{m,n} [[T]]) (\varphi(U_i T))}_{= \begin{cases} \varphi(U_i T), & \text{if } i \leq n; \\ 1, & \text{if } i > n \end{cases}} = \prod_{i=1}^m \begin{cases} \varphi(U_i T), & \text{if } i \leq n; \\ 1, & \text{if } i > n \end{cases} \\
&= \prod_{i=1}^n \underbrace{\begin{cases} \varphi(U_i T), & \text{if } i \leq n; \\ 1, & \text{if } i > n \end{cases}}_{= \varphi(U_i T) \text{ (since } i \leq n)} \cdot \prod_{i=n+1}^m \underbrace{\begin{cases} \varphi(U_i T), & \text{if } i \leq n; \\ 1, & \text{if } i > n \end{cases}}_{= 1 \text{ (since } i > n)} \\
&= \prod_{i=1}^n \varphi(U_i T) \cdot \underbrace{\prod_{i=n+1}^m 1}_{=1} = \prod_{i=1}^n \varphi(U_i T).
\end{aligned}$$

But the diagram

$$\begin{array}{ccc}
(\mathbf{Z}[U_1, U_2, \dots, U_m]) [[T]] & \xrightarrow{\text{proj}_{m,n} [[T]]} & (\mathbf{Z}[U_1, U_2, \dots, U_m]) [[T]] \\
\text{Coeff}_j \downarrow & & \text{Coeff}_j \downarrow \\
\mathbf{Z}[U_1, U_2, \dots, U_m] & \xrightarrow{\text{proj}_{m,n}} & \mathbf{Z}[U_1, U_2, \dots, U_n]
\end{array}$$

is commutative (this is clear from the definitions of  $\text{Coeff}_j$  and  $\text{proj}_{m,n} [[T]]$ ), so that  $\text{proj}_{m,n} \circ \text{Coeff}_j = \text{Coeff}_j \circ (\text{proj}_{m,n} [[T]])$  and thus

$$\begin{aligned}
(\text{proj}_{m,n} \circ \text{Coeff}_j) \left( \prod_{i=1}^m \varphi(U_i T) \right) &= (\text{Coeff}_j \circ (\text{proj}_{m,n} [[T]])) \left( \prod_{i=1}^m \varphi(U_i T) \right) \\
&= \text{Coeff}_j \left( \underbrace{(\text{proj}_{m,n} [[T]]) \left( \prod_{i=1}^m \varphi(U_i T) \right)}_{= \prod_{i=1}^n \varphi(U_i T)} \right) \\
&= \text{Coeff}_j \left( \prod_{i=1}^n \varphi(U_i T) \right) \\
&= \text{Todd}_{(\varphi, j), j, [n]} (X_1, X_2, \dots, X_j) \\
&\quad \text{(by (52), applied to } n \text{ instead of } m \text{).}
\end{aligned}$$

Comparing this with

$$\begin{aligned}
& (\text{proj}_{m,n} \circ \text{Coeff}_j) \left( \prod_{i=1}^m \varphi(U_i T) \right) \\
&= \text{proj}_{m,n} \left( \underbrace{\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right)}_{\substack{= \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j) \\ \text{(by (52))}}} \right) = \text{proj}_{m,n} \left( \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j) \right) \\
&= \text{Todd}_{(\varphi,j),j,[m]}(\text{proj}_{m,n} X_1, \text{proj}_{m,n} X_2, \dots, \text{proj}_{m,n} X_j) \\
&\quad \left( \begin{array}{l} \text{since } \text{Todd}_{(\varphi,j),j,[m]} \text{ is a polynomial over } \mathbf{Z} \\ \text{and } \text{proj}_{m,n} \text{ is a } \mathbf{Z}\text{-algebra homomorphism,} \\ \text{and since polynomials over } \mathbf{Z} \text{ commute} \\ \text{with } \mathbf{Z}\text{-algebra homomorphisms} \end{array} \right) \\
&= \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j) \\
&\quad \left( \begin{array}{l} \text{since } \text{proj}_{m,n} \text{ is the } \mathbf{Z}\text{-algebra homomorphism which maps} \\ \text{every } U_i \text{ to } \begin{cases} U_i, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases}, \\ \text{and thus we know that it maps every } X_i \text{ with } i \geq 1 \text{ to} \\ \text{the corresponding } X_i \text{ of the image ring, so} \\ \text{that } \text{proj}_{m,n} X_1 = X_1, \text{proj}_{m,n} X_2 = X_2, \dots, \text{proj}_{m,n} X_j = X_j \end{array} \right),
\end{aligned}$$

we obtain

$$\text{Todd}_{(\varphi,j),j,[n]}(X_1, X_2, \dots, X_j) = \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j)$$

in the polynomial ring  $\mathbf{Z}[U_1, U_2, \dots, U_n]$ . This proves Lemma 10.2.  $\square$

*Proof of Theorem 10.1.* This proof is going to be very similar to the proofs of Theorem 4.4 (a) and Theorem 9.1 (a) - except that this time, we already have done most of our work when proving Lemma 10.2.

*1st Step:* Fix  $m \in \mathbb{N}$  and  $j \in \mathbb{N}$  such that  $m \geq j$ . Then, we claim that  $\text{Todd}_{(\varphi,j),j,[m]} = \text{Td}_{\varphi,j}$ .

*Proof.* Lemma 10.2 (applied to  $n = j$ ) yields that  $\text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j) = \text{Todd}_{(\varphi,j),j,[j]}(X_1, X_2, \dots, X_j)$  in the polynomial ring  $\mathbf{Z}[U_1, U_2, \dots, U_j]$ . Since the elements  $X_1, X_2, \dots, X_j$  of  $\mathbf{Z}[U_1, U_2, \dots, U_j]$  are algebraically independent (by Theorem 4.1 (a)), this yields  $\text{Todd}_{(\varphi,j),j,[m]} = \text{Todd}_{(\varphi,j),j,[j]}$ . Thus,  $\text{Todd}_{(\varphi,j),j,[m]} = \text{Todd}_{(\varphi,j),j,[j]} = \text{Td}_{\varphi,j}$ , and the 1st Step is proven.

*2nd Step:* For every  $m \in \mathbb{N}$  and  $j \in \mathbb{N}$ , we have

$$\text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j) = \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j)$$

in the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$ .

*Proof.* Let  $m' \in \mathbb{N}$  be such that  $m' \geq m$  and  $m' \geq j$ . Then, the 1st Step (applied to  $m'$  instead of  $m$ ) yields that  $\text{Todd}_{(\varphi,j),j,[m']} = \text{Td}_{\varphi,j}$ . On the other hand, Lemma 10.2 (applied to  $m'$  and  $m$  instead of  $m$  and  $n$ ) yields that  $\text{Todd}_{(\varphi,j),j,[m']}(X_1, X_2, \dots, X_j) =$

$\text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j)$  in the polynomial ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$ . Since  $\text{Todd}_{(\varphi,j),j,[m']} = \text{Td}_{\varphi,j}$ , this rewrites as  $\text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j) = \text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j)$ . This proves the 2nd Step.

*3rd Step:* For every  $m \in \mathbb{N}$ , the equation (51) is satisfied in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$ .

*Proof.* Every power series  $P \in (\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$  satisfies  $P = \sum_{j \in \mathbb{N}} (\text{Coeff}_j P) T^j$

(by the definition of  $\text{Coeff}_j$ ). Applied to  $P = \prod_{i=1}^m \varphi(U_i T)$ , this yields

$$\begin{aligned} \prod_{i=1}^m \varphi(U_i T) &= \sum_{j \in \mathbb{N}} \underbrace{\text{Coeff}_j \left( \prod_{i=1}^m \varphi(U_i T) \right)}_{=\text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j) \text{ (by (52))}} T^j = \sum_{j \in \mathbb{N}} \underbrace{\text{Todd}_{(\varphi,j),j,[m]}(X_1, X_2, \dots, X_j)}_{=\text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j) \text{ (by the 2nd step)}} T^j \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j) T^j \end{aligned}$$

in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$ . This proves the 3rd Step, and thus Theorem 10.1 is proven.  $\square$

## 10.2. Defining the Todd homomorphism

Now, let us define the Todd homomorphism:

**Definition.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. We define a map  $\text{td}_{\varphi,T} : K \rightarrow K[[T]]$  by

$$\text{td}_{\varphi,T}(x) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \quad \text{for every } x \in K. \quad (53)$$

We call  $\text{td}_{\varphi,T}$  the  $\varphi$ -Todd homomorphism of the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ .

As already mentioned above, this notation  $\text{td}_{\varphi,T}$  and the name “ $\varphi$ -Todd homomorphism” by which I denote it might not be standard terminology.<sup>57</sup>

## 10.3. The case when the power series is $1 + ut$

As complicated as this definition was, we might wonder whether there is a more explicit approach to  $\varphi$ -Todd homomorphisms. It turns out that there is, if  $\varphi$  is a polynomial factoring into linear polynomials of the form  $1 + ut$  with  $u \in \mathbf{Z}$ . Let us begin with computing the  $\varphi$ -Todd homomorphism for  $\varphi$  itself being of this form:

<sup>57</sup>For instance, what [FulLan85] calls “Todd homomorphism” is the map  $\text{td}_{\varphi} := \text{td}_{\varphi,1}$  (where  $\text{td}_{\varphi,1}$  means “take the formal power series  $\text{td}_{\varphi,T}$  and replace every  $T$  by 1”), which is only defined on  $x$  if  $x$  is finite-dimensional, i. e. if  $x$  satisfies  $\lambda^i(x) = 0$  for all sufficiently large  $i$ . But I prefer the power series  $\text{td}_{\varphi,T}(x)$  since it is defined on every  $x$ .

I am not even sure whether there exists standard terminology for Todd homomorphisms - there does not seem to be much literature about them.

**Proposition 10.3.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $u \in \mathbf{Z}$ . For every  $x \in K$ , we have  $\text{td}_{1+ut, T}(x) = \lambda_{uT}(x)$ , where  $\lambda_{uT}(x)$  means  $\text{ev}_{uT}(\lambda_T(x))$ .

To prove this, we need to compute the  $j$ -th Todd polynomials of  $1 + ut$ . This can be done explicitly:

**Proposition 10.4.** Let  $\mathbf{Z}$  be a ring. Let  $u \in \mathbf{Z}$ . Then,  $\text{Td}_{1+ut, j} = u^j \alpha_j$  (in the polynomial ring  $\mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$ ) for every positive  $j \in \mathbb{N}$ .

Note that Proposition 10.4 makes no sense for  $j = 0$ ; this will cause us some minor trouble in the proof of Proposition 10.3.

*Proof of Proposition 10.4.* Let  $m \in \mathbb{N}$ . Consider the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$  (the polynomial ring in  $m$  indeterminates  $U_1, U_2, \dots, U_m$  over the ring  $\mathbf{Z}$ ). For every  $i \in \mathbb{N}$ , let  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  be the so-called  *$i$ -th elementary symmetric polynomial* in the variables  $U_1, U_2, \dots, U_m$ .

We know from Theorem 10.1 that (51) holds in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$  whenever  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  is a power series with constant term equal to 1. Applying this to  $\varphi = 1 + ut$ , we obtain

$$\prod_{i=1}^m (1 + ut)(U_i T) = \sum_{j \in \mathbb{N}} \text{Td}_{1+ut, j}(X_1, X_2, \dots, X_j) T^j,$$

where  $(1 + ut)(U_i T)$  means “the power series  $1 + ut$ , applied to  $U_i T$ ” (and not a product of  $1 + ut$  and  $U_i T$ , whatever such a product could mean). Since

$$\begin{aligned} & \prod_{i=1}^m \underbrace{(1 + ut)(U_i T)}_{=1+uU_i T=1+U_i \cdot uT} \\ &= \prod_{i=1}^m (1 + U_i \cdot uT) = \sum_{i \in \mathbb{N}} \underbrace{\sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k}_{=X_i} \underbrace{(uT)^i}_{=u^i T^i} \\ & \quad \left( \text{by Exercise 4.2 (b), applied to } U_i, (\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]], \text{ and } uT \right. \\ & \quad \left. \text{instead of } \alpha_i, A, \text{ and } t \right) \\ &= \sum_{i \in \mathbb{N}} X_i u^i T^i = \sum_{j \in \mathbb{N}} X_j u^j T^j \quad (\text{here, we renamed the index } i \text{ as } j), \end{aligned}$$

this rewrites as

$$\sum_{j \in \mathbb{N}} X_j u^j T^j = \sum_{j \in \mathbb{N}} \text{Td}_{1+ut, j}(X_1, X_2, \dots, X_j) T^j.$$

By comparing coefficients in this equation, we conclude that

$$X_j u^j = \text{Td}_{1+ut, j}(X_1, X_2, \dots, X_j) \text{ in } \mathbf{Z}[U_1, U_2, \dots, U_m] \quad \text{for all } j \in \mathbb{N}.$$



Now we forget that we fixed  $m$ . Instead, fix some positive  $j \in \mathbb{N}$ , and take  $m = j$ . Then, we have just proved that

$$X_j u^j = \text{Td}_{1+ut,j}(X_1, X_2, \dots, X_j) \text{ in } \mathbf{Z}[U_1, U_2, \dots, U_j].$$

Applying Theorem 4.1 (a) to  $K = \mathbf{Z}$ ,  $m = j$  and  $P = X_j u^j$ , we conclude that there exists one and only one polynomial  $Q \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  such that  $X_j u^j = Q(X_1, X_2, \dots, X_j)$ . In particular, there exists *at most one* such polynomial  $Q \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$ . Hence,

$$\left( \begin{array}{l} \text{if } \Omega_1 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j] \text{ and } \Omega_2 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j] \text{ are two polynomials} \\ \text{such that } X_j u^j = \Omega_1(X_1, X_2, \dots, X_j) \text{ and } X_j u^j = \Omega_2(X_1, X_2, \dots, X_j), \\ \text{then } \Omega_1 = \Omega_2 \end{array} \right). \quad (54)$$

Let  $\Omega_1 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  be the polynomial defined by  $\Omega_1 = u^j \alpha_j$ . Let  $\Omega_2 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  be the polynomial defined by  $\Omega_2 = \text{Td}_{1+ut,j}$ . We are now going to prove that  $\Omega_1 = \Omega_2$ .

Since our two polynomials  $\Omega_1$  and  $\Omega_2$  satisfy

$$\begin{aligned} \Omega_1(X_1, X_2, \dots, X_j) &= u^j X_j && \text{(since } \Omega_1 = u^j \alpha_j \text{)} \\ &= X_j u^j \end{aligned}$$

and

$$\begin{aligned} \Omega_2(X_1, X_2, \dots, X_j) &= \text{Td}_{1+ut,j}(X_1, X_2, \dots, X_j) && \text{(since } \Omega_2 = \text{Td}_{1+ut,j} \text{)} \\ &= X_j u^j, \end{aligned}$$

we can conclude from (54) that  $\Omega_1 = \Omega_2$ . Hence,  $u^j \alpha_j = \Omega_1 = \Omega_2 = \text{Td}_{1+ut,j}$ . This proves Proposition 10.4.  $\square$

#### 10.4. The 0-th and 1-st coefficients of $\text{td}_{\varphi,T}(x)$

We keep back the proof of Proposition 10.3 for a moment - instead, we first show a proposition which gives the first two coefficients of the power series  $\text{td}_{\varphi,T}(x)$  in the general case (with  $\varphi$  arbitrary):

**Proposition 10.5.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1.

(a) Then,  $\text{Coeff}_0(\text{td}_{\varphi,T}(x)) = 1$  for every  $x \in K$ .

(b) Let  $\varphi_1$  be the coefficient of the power series  $\varphi \in \mathbf{Z}[[t]]$  before  $t^1$ . Then,  $\text{Coeff}_1(\text{td}_{\varphi,T}(x)) = \varphi_1 x$  for every  $x \in K$ .

To prove this, we need to compute the 0-th and the 1-st Todd polynomials of  $\varphi$ :

**Proposition 10.6.** Let  $\mathbf{Z}$  be a ring. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1.

(a) Then,  $\text{Td}_{\varphi,0} = 1$ .

(b) Let  $\varphi_1$  be the coefficient of the power series  $\varphi \in \mathbf{Z}[[t]]$  before  $t^1$ . Then,  $\text{Td}_{\varphi,1} = \varphi_1 \alpha_1$ .

*Proof of Proposition 10.6.* Let  $m \in \mathbb{N}$ . Consider the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$  and its elements  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  as in the definition of  $\text{Td}_{\varphi, j}$ .

We know from Theorem 10.1 that (51) holds in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$ . In other words,

$$\prod_{i=1}^m \varphi(U_i T) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(X_1, X_2, \dots, X_j) T^j.$$

Thus,

$$\text{Coeff}_0 \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Coeff}_0 \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(X_1, X_2, \dots, X_j) T^j \right) = \text{Td}_{\varphi, 0}(X_1, X_2, \dots, X_0) \quad (55)$$

<sup>58</sup> (by the definition of  $\text{Coeff}_0$ ) and

$$\text{Coeff}_1 \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Coeff}_1 \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(X_1, X_2, \dots, X_j) T^j \right) = \text{Td}_{\varphi, 1}(X_1, X_2, \dots, X_1) \quad (56)$$

(by the definition of  $\text{Coeff}_1$ ). Both of these equations (55) and (56) hold in the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$ .

(a) Let  $m = 0$ . Then, the polynomial rings  $\mathbf{Z}[U_1, U_2, \dots, U_m] = \mathbf{Z}[U_1, U_2, \dots, U_0]$  and  $\mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_0]$  can be canonically identified with the ring  $\mathbf{Z}$  (because they are polynomial rings in zero variables, and a polynomial ring in zero variables over a ring  $K$  is the same as the ring  $K$  itself). Under this identification, the “value”  $\text{Td}_{\varphi, 0}(X_1, X_2, \dots, X_0)$  corresponds to the polynomial  $\text{Td}_{\varphi, 0}$ , so that we can write  $\text{Td}_{\varphi, 0}(X_1, X_2, \dots, X_0) = \text{Td}_{\varphi, 0}$ .

But the equation (55) holds in the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m] = \mathbf{Z}[U_1, U_2, \dots, U_0] \cong \mathbf{Z}$ . Hence, we have

$$\text{Td}_{\varphi, 0}(X_1, X_2, \dots, X_0) = \text{Coeff}_0 \left( \underbrace{\prod_{i=1}^m \varphi(U_i T)}_{\substack{=(\text{empty product}) \\ (\text{since } m=0)}} \right) = \text{Coeff}_0 \underbrace{(\text{empty product})}_{=1} = 1$$

in the ring  $\mathbf{Z}$ . Hence,  $\text{Td}_{\varphi, 0} = \text{Td}_{\varphi, 0}(X_1, X_2, \dots, X_0) = 1$ . This proves Proposition 10.6 (a).

(b) Let  $m = 1$ . Then,  $\mathbf{Z}[U_1, U_2, \dots, U_m] = \mathbf{Z}[U_1]$ , and in this ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$  we have  $X_1 = U_1$  (because  $X_1$  is the 1-st elementary symmetric polynomial of the one

<sup>58</sup>The notation  $\text{Td}_{\varphi, 0}(X_1, X_2, \dots, X_0)$  is somewhat unusual, but it should not be surprising: The polynomial  $\text{Td}_{\varphi, 0}$  is an element of  $\mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_0]$ , that is, a polynomial in zero variables. (Of course, polynomials in zero variables are just elements of the base ring - in this case, elements of  $\mathbf{Z}$ .)

variable  $U_1$ ). Thus, in this ring, we have

$$\begin{aligned}
\text{Td}_{\varphi,1}(U_1) &= \text{Td}_{\varphi,1}(X_1) = \text{Td}_{\varphi,1}(X_1, X_2, \dots, X_1) \\
&= \text{Coeff}_1 \left( \underbrace{\prod_{i=1}^m \varphi(U_i T)}_{=\varphi(U_1 T) \text{ (since } m=1)} \right) \quad (\text{by (56)}) \\
&= \text{Coeff}_1(\varphi(U_1 T)) = (\text{the coefficient of the power series } \varphi(U_1 T) \text{ before } T^1) \\
&= U_1 \underbrace{(\text{the coefficient of the power series } \varphi \text{ before } t^1)}_{=\varphi_1} = U_1 \varphi_1.
\end{aligned}$$

Now, let  $\kappa$  be the  $\mathbf{Z}$ -algebra homomorphism  $\mathbf{Z}[\alpha_1] \rightarrow \mathbf{Z}[U_1]$  which maps  $\alpha_1$  to  $U_1$ . This homomorphism  $\kappa$  must be an isomorphism (since  $U_1$  is obviously algebraically independent). Since  $\kappa$  is a  $\mathbf{Z}$ -algebra homomorphism and  $\text{Td}_{\varphi,1}$  is a polynomial, we have  $\kappa(\text{Td}_{\varphi,1}(\alpha_1)) = \text{Td}_{\varphi,1}(\kappa(\alpha_1))$  (because  $\mathbf{Z}$ -algebra homomorphisms commute with polynomials). Now,

$$\begin{aligned}
\kappa \left( \underbrace{\text{Td}_{\varphi,1}}_{=\text{Td}_{\varphi,1}(\alpha_1)} \right) &= \kappa(\text{Td}_{\varphi,1}(\alpha_1)) = \text{Td}_{\varphi,1} \left( \underbrace{\kappa(\alpha_1)}_{=U_1} \right) = \text{Td}_{\varphi,1}(U_1) \\
&= \underbrace{U_1}_{=\kappa(\alpha_1)} \varphi_1 = \kappa(\alpha_1) \varphi_1 = \varphi_1 \kappa(\alpha_1) = \kappa(\varphi_1 \alpha_1)
\end{aligned}$$

(since  $\kappa$  is a  $\mathbf{Z}$ -algebra homomorphism). Thus,  $\text{Td}_{\varphi,1} = \varphi_1 \alpha_1$  (since  $\kappa$  is an isomorphism). This proves Proposition 10.6 (b).  $\square$

*Proof of Proposition 10.5.* Let  $x \in K$ .

(a) We have

$$\begin{aligned}
\text{Coeff}_0(\text{td}_{\varphi,T}(x)) &= \text{Coeff}_0 \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \right) \quad (\text{by (53)}) \\
&= \text{Td}_{\varphi,0}(\lambda^1(x), \lambda^2(x), \dots, \lambda^0(x)) \quad (\text{by the definition of } \text{Coeff}_0) \\
&= \text{Td}_{\varphi,0} = 1 \quad (\text{by Proposition 10.6 (a)}).
\end{aligned}$$

(b) We have

$$\begin{aligned}
\text{Coeff}_1(\text{td}_{\varphi,T}(x)) &= \text{Coeff}_1 \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \right) \quad (\text{by (53)}) \\
&= \text{Td}_{\varphi,1}(\lambda^1(x), \lambda^2(x), \dots, \lambda^1(x)) \quad (\text{by the definition of } \text{Coeff}_1) \\
&= \text{Td}_{\varphi,1} \left( \underbrace{\lambda^1(x)}_{=x} \right) = \text{Td}_{\varphi,1}(x) = \varphi_1 x \\
&\quad (\text{since Proposition 10.6 (b) yields } \text{Td}_{\varphi,1} = \varphi_1 \alpha_1).
\end{aligned}$$

Proposition 10.5 is now proven.  $\square$

## 10.5. Proof of Proposition 10.3

*Proof of Proposition 10.3.* Let  $x \in K$ . Applying (53) to  $\varphi = 1 + ut$ , we obtain

$$\begin{aligned}
& \text{td}_{1+ut, T}(x) \\
&= \sum_{j \in \mathbb{N}} \text{Td}_{1+ut, j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \\
&= \underbrace{\text{Td}_{1+ut, 0}(\lambda^1(x), \lambda^2(x), \dots, \lambda^0(x)) T^0}_{\substack{=\text{Td}_{1+ut, 0}=1 \\ \text{(by Proposition 10.6 (a),} \\ \text{applied to } \varphi=1+ut)}} + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \underbrace{\text{Td}_{1+ut, j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j}_{\substack{=u^j \alpha_j \\ \text{(by Proposition 10.4)}}} \\
&= 1T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \underbrace{(u^j \alpha_j)(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j}_{=u^j \lambda^j(x) = \lambda^j(x) u^j} = 1T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \lambda^j(x) u^j T^j.
\end{aligned}$$

Compared with

$$\begin{aligned}
\lambda_{uT}(x) &= \text{ev}_{uT} \left( \underbrace{\lambda_T(x)}_{=\sum_{j \in \mathbb{N}} \lambda^j(x) T^j} \right) = \text{ev}_{uT} \left( \sum_{j \in \mathbb{N}} \lambda^j(x) T^j \right) \\
&= \sum_{j \in \mathbb{N}} \lambda^j(x) u^j T^j \quad (\text{by the definition of } \text{ev}_{uT}) \\
&= \underbrace{\lambda^0(x)}_{=1} \underbrace{u^0}_{=1} T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \lambda^j(x) u^j T^j = 1T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \lambda^j(x) u^j T^j,
\end{aligned}$$

this yields that  $\text{td}_{1+ut, T}(x) = \lambda_{uT}(x)$ . This proves Proposition 10.3.  $\square$

## 10.6. The Todd homomorphism is multiplicative in $\varphi$

Our next proposition is another step to making the  $\varphi$ -Todd homomorphism manageable:

**Proposition 10.7.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  and  $\psi \in 1 + \mathbf{Z}[[t]]^+$  be two power series with constant terms equal to 1. For every  $x \in K$ , we have  $\text{td}_{\varphi\psi, T}(x) = \text{td}_{\varphi, T}(x) \text{td}_{\psi, T}(x)$ .

Again, this boils down to an identity for Todd polynomials:

**Proposition 10.8.** Let  $\mathbf{Z}$  be a ring. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  and  $\psi \in 1 + \mathbf{Z}[[t]]^+$  be two power series with constant terms equal to 1. Then,

$$\text{Td}_{\varphi\psi, j}(\alpha_1, \alpha_2, \dots, \alpha_j) = \sum_{i=0}^j \text{Td}_{\varphi, i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi, j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i})$$

(in the polynomial ring  $\mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$ ) for every  $j \in \mathbb{N}$ .

*Proof of Proposition 10.8. 1st Step:* We have  $\varphi\psi \in 1 + \mathbf{Z}[[t]]^+$ .

*Proof.* The constant term of the product of two power series always equals the product of the constant terms of these power series. Applying this to the power series  $\varphi$  and  $\psi$ , we obtain

$$\begin{aligned} & (\text{constant term of the power series } \varphi\psi) \\ &= \underbrace{(\text{constant term of the power series } \varphi)}_{=1 \text{ (since } \varphi \in 1 + \mathbf{Z}[[t]]^+)} \cdot \underbrace{(\text{constant term of the power series } \psi)}_{=1 \text{ (since } \psi \in 1 + \mathbf{Z}[[t]]^+)} \\ &= 1 \cdot 1 = 1, \end{aligned}$$

so that  $\varphi\psi \in 1 + \mathbf{Z}[[t]]^+$ . The 1st Step is thus proven.

*2nd Step:* We are going to show that for every  $m \in \mathbb{N}$ , we have

$$\text{Td}_{\varphi\psi,j}(X_1, X_2, \dots, X_j) = \sum_{i=0}^j \text{Td}_{\varphi,i}(X_1, X_2, \dots, X_i) \cdot \text{Td}_{\psi,j-i}(X_1, X_2, \dots, X_{j-i})$$

in the polynomial ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$  for every  $j \in \mathbb{N}$  (where, as usual,  $X_i$  denotes the polynomial  $\sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k$  (the  $i$ -th elementary symmetric polynomial in the

variables  $U_1, U_2, \dots, U_m$ ) for every  $i \in \mathbb{N}$ ).

*Proof.* Let  $m \in \mathbb{N}$ . By Theorem 10.1, the equality (51) holds in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$ . In other words,

$$\prod_{i=1}^m \varphi(U_i T) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j) T^j.$$

Applying this equality to  $\psi$  instead of  $\varphi$ , we get

$$\prod_{i=1}^m \psi(U_i T) = \sum_{j \in \mathbb{N}} \text{Td}_{\psi,j}(X_1, X_2, \dots, X_j) T^j.$$

On the other hand, applying it to  $\varphi\psi$  instead of  $\varphi$ , we get

$$\prod_{i=1}^m (\varphi\psi)(U_i T) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi\psi,j}(X_1, X_2, \dots, X_j) T^j.$$

Hence,

$$\begin{aligned}
& \sum_{j \in \mathbb{N}} \text{Td}_{\varphi\psi, j}(X_1, X_2, \dots, X_j) T^j \\
&= \prod_{i=1}^m \underbrace{(\varphi\psi)(U_i T)}_{=\varphi(U_i T)\psi(U_i T)} = \prod_{i=1}^m (\varphi(U_i T) \psi(U_i T)) \\
&= \underbrace{\prod_{i=1}^m \varphi(U_i T)}_{=\sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(X_1, X_2, \dots, X_j) T^j} \cdot \underbrace{\prod_{i=1}^m \psi(U_i T)}_{=\sum_{j \in \mathbb{N}} \text{Td}_{\psi, j}(X_1, X_2, \dots, X_j) T^j} \\
&= \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(X_1, X_2, \dots, X_j) T^j \right) \cdot \left( \sum_{j \in \mathbb{N}} \text{Td}_{\psi, j}(X_1, X_2, \dots, X_j) T^j \right) \\
&= \sum_{j \in \mathbb{N}} \left( \sum_{i=0}^j \text{Td}_{\varphi, i}(X_1, X_2, \dots, X_i) \cdot \text{Td}_{\psi, j-i}(X_1, X_2, \dots, X_{j-i}) \right) T^j \\
&\quad \text{(by the definition of the product of two formal power series)}.
\end{aligned}$$

Comparing coefficients in this equation, we conclude that

$$\text{Td}_{\varphi\psi, j}(X_1, X_2, \dots, X_j) = \sum_{i=0}^j \text{Td}_{\varphi, i}(X_1, X_2, \dots, X_i) \cdot \text{Td}_{\psi, j-i}(X_1, X_2, \dots, X_{j-i})$$

for every  $j \in \mathbb{N}$ . This proves the 2nd Step.

*3rd Step:* Let us now prove Proposition 10.8.

Fix some  $j \in \mathbb{N}$ . Let  $m = j$ . We are going to work in the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m] = \mathbf{Z}[U_1, U_2, \dots, U_j]$ .

Applying Theorem 4.1 (a) to  $K = \mathbf{Z}$ ,  $m = j$  and  $P = \text{Td}_{\varphi\psi, j}(X_1, X_2, \dots, X_j)$ , we conclude that there exists one and only one polynomial  $Q \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  such that  $\text{Td}_{\varphi\psi, j}(X_1, X_2, \dots, X_j) = Q(X_1, X_2, \dots, X_j)$ . In particular, there exists *at most one* such polynomial  $Q \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$ . Hence,

$$\left( \begin{array}{l} \text{if } \mathfrak{Q}_1 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j] \text{ and } \mathfrak{Q}_2 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j] \text{ are two polynomials} \\ \text{such that } \text{Td}_{\varphi\psi, j}(X_1, X_2, \dots, X_j) = \mathfrak{Q}_1(X_1, X_2, \dots, X_j) \text{ and} \\ \text{Td}_{\varphi\psi, j}(X_1, X_2, \dots, X_j) = \mathfrak{Q}_2(X_1, X_2, \dots, X_j), \text{ then } \mathfrak{Q}_1 = \mathfrak{Q}_2 \end{array} \right). \quad (57)$$

Let  $\mathfrak{Q}_1 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  be the polynomial defined by  $\mathfrak{Q}_1 = \text{Td}_{\varphi\psi, j}(\alpha_1, \alpha_2, \dots, \alpha_j)$ .

Let  $\mathfrak{Q}_2 \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  be the polynomial defined by  $\mathfrak{Q}_2 = \sum_{i=0}^j \text{Td}_{\varphi, i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi, j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i})$ . We are now going to prove that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ .

Since our two polynomials  $\mathfrak{Q}_1$  and  $\mathfrak{Q}_2$  satisfy

$$\mathfrak{Q}_1(X_1, X_2, \dots, X_j) = \text{Td}_{\varphi\psi, j}(X_1, X_2, \dots, X_j) \quad (\text{since } \mathfrak{Q}_1 = \text{Td}_{\varphi\psi, j}(\alpha_1, \alpha_2, \dots, \alpha_j))$$

and

$$\begin{aligned}\mathfrak{Q}_2(X_1, X_2, \dots, X_j) &= \sum_{i=0}^j \text{Td}_{\varphi,i}(X_1, X_2, \dots, X_i) \cdot \text{Td}_{\psi,j-i}(X_1, X_2, \dots, X_{j-i}) \\ &\quad \left( \text{since } \mathfrak{Q}_2 = \sum_{i=0}^j \text{Td}_{\varphi,i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi,j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i}) \right) \\ &= \text{Td}_{\varphi\psi,j}(X_1, X_2, \dots, X_j) \quad (\text{by the 2nd Step}),\end{aligned}$$

we can conclude from (57) that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ . Hence,

$$\text{Td}_{\varphi\psi,j}(\alpha_1, \alpha_2, \dots, \alpha_j) = \mathfrak{Q}_1 = \mathfrak{Q}_2 = \sum_{i=0}^j \text{Td}_{\varphi,i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi,j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i}).$$

This proves Proposition 10.8. □

*Proof of Proposition 10.7. 1st Step:* For every  $j \in \mathbb{N}$  and  $x \in K$ , we have

$$\begin{aligned}\text{Td}_{\varphi\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) \\ = \sum_{i=0}^j \text{Td}_{\varphi,i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^i(x)) \cdot \text{Td}_{\psi,j-i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^{j-i}(x)).\end{aligned}$$

*Proof.* Let  $j \in \mathbb{N}$  and  $x \in K$ . Since the polynomials  $\text{Td}_{\varphi\psi,j}(\alpha_1, \alpha_2, \dots, \alpha_j)$  and  $\sum_{i=0}^j \text{Td}_{\varphi,i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi,j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i})$  are equal (by Proposition 10.8), their evaluations at  $(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))$  must also be equal. But since the evaluation of  $\text{Td}_{\varphi\psi,j}(\alpha_1, \alpha_2, \dots, \alpha_j)$  at  $(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))$  is  $\text{Td}_{\varphi\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))$ , whereas the evaluation of  $\sum_{i=0}^j \text{Td}_{\varphi,i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi,j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i})$  at  $(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))$  is  $\sum_{i=0}^j \text{Td}_{\varphi,i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^i(x)) \cdot \text{Td}_{\psi,j-i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^{j-i}(x))$ , this yields that the values  $\text{Td}_{\varphi\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))$  and  $\sum_{i=0}^j \text{Td}_{\varphi,i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^i(x)) \cdot \text{Td}_{\psi,j-i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^{j-i}(x))$  are equal. This proves the 1st step.

*2nd Step:* Now let us prove Proposition 10.7.

Let  $x \in K$ . By (53) (applied to  $\varphi\psi$  instead of  $\varphi$ ), we have

$$\text{td}_{\varphi\psi,T}(x) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j.$$

But

$$\begin{aligned}
& \underbrace{\text{td}_{\varphi,T}(x)}_{\substack{= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \\ \text{(by (53))}}} \quad \underbrace{\text{td}_{\psi,T}(x)}_{\substack{= \sum_{j \in \mathbb{N}} \text{Td}_{\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \\ \text{(by (53), applied to } \psi \text{ instead of } \varphi)}} \\
&= \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \right) \cdot \left( \sum_{j \in \mathbb{N}} \text{Td}_{\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \right) \\
&= \sum_{j \in \mathbb{N}} \underbrace{\left( \sum_{i=0}^j \text{Td}_{\varphi,i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^i(x)) \cdot \text{Td}_{\psi,j-i}(\lambda^1(x), \lambda^2(x), \dots, \lambda^{j-i}(x)) \right)}_{\substack{= \text{Td}_{\varphi\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) \\ \text{(by the 1st Step)}}} T^j \\
&\quad \text{(by the definition of the product of two formal power series)} \\
&= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi\psi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j = \text{td}_{\varphi\psi,T}(x).
\end{aligned}$$

This proves Proposition 10.7. □

An easy consequence of Proposition 10.7:

**Proposition 10.9.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $m \in \mathbb{N}$ . For every  $i \in \{1, 2, \dots, m\}$ , let  $\varphi_i \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. For every  $x \in K$ , we have

$$\text{td}_{\prod_{i=1}^m \varphi_i, T}(x) = \prod_{i=1}^m \text{td}_{\varphi_i, T}(x).$$

*Proof of Proposition 10.9.* This can be proven by induction over  $m$ . The induction base (the case  $m = 0$ ) requires showing that  $\text{td}_{1,T}(x) = 1$ , but this follows from Proposition 10.3<sup>59</sup>. The induction step is a straightforward application of Proposition 10.7. Thus Proposition 10.9 is proven. □

## 10.7. $\text{td}_{\varphi,T}$ takes sums into products

Our next goal is to show the following general property of  $\text{td}_{\varphi,T}$ :

**Theorem 10.10.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $x \in K$  and  $y \in K$ . Then,  $\text{td}_{\varphi,T}(x) \cdot \text{td}_{\varphi,T}(y) = \text{td}_{\varphi,T}(x + y)$ .

<sup>59</sup>In fact, Proposition 10.3 (applied to  $u = 0$ ) yields  $\text{td}_{1+0t,T}(x) = \lambda_{0T}(x)$ . Now  $\lambda_{0T}(x) = \text{ev}_{0T}(\lambda_T(x))$ . Since  $\text{ev}_{0T}$  is the map  $K[[T]] \rightarrow K[[T]]$  which sends every power series to its constant term (viewed as a constant power series), we have  $\text{ev}_{0T}(\lambda_T(x)) = (\text{constant term of the power series } \lambda_T(x)) = 1$ . Thus,  $\text{td}_{1,T}(x) = \text{td}_{1+0t,T}(x) = \lambda_{0T}(x) = \text{ev}_{0T}(\lambda_T(x)) = 1$ .



How can we prove a theorem like this? By using Proposition 10.3, we could prove it in the case of  $\varphi$  being a polynomial of the form  $1 + ut$  with  $u \in \mathbf{Z}$ . Using Proposition 10.9, we could therefore also prove it in the case of  $\varphi$  being a product of finitely many such polynomials. However, the case of  $\varphi$  being a general power series does not directly follow from any of our above-proven propositions. Not even the case of  $\varphi$  being a general polynomial - in fact, a general polynomial does not always factor into polynomials of the form  $1 + ut$  with  $u \in \mathbf{Z}$ .

However, we can prove Theorem 10.10 (and similar results) using the following two tricks: First, we need a kind of continuity (similar to the one we used in Section 5) to reduce the case of  $\varphi$  a power series to the case of  $\varphi$  a polynomial. Second, we need to split every arbitrary polynomial  $\varphi$  with constant term equal to 1 into a product of polynomials of the form  $1 + ut$ ; this will be done by an appropriate extension of the ring  $\mathbf{Z}$  (again, similarly to how we extended  $K$  in Section 5). However, these tricks do not yet give us a proof of Theorem 10.10 unless we change our viewpoint to a more general one: Rather than working in a  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ , we work with power series over an arbitrary ring. Here is what we do, precisely:

## 10.8. The $\mathfrak{Todd}_\varphi$ map

**Definition.** Let  $\mathbf{Z}$  be a ring. Let  $K$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. We define a map  $\mathfrak{Todd}_\varphi : K[[T]] \rightarrow K[[T]]$  by

$$\mathfrak{Todd}_\varphi(p) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \quad \text{for every } p \in K[[T]]. \quad (58)$$

The reason why we can consider this a generalization of the  $\varphi$ -Todd homomorphism is the following:

**Proposition 10.11.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Then, every  $x \in K$  satisfies  $\text{td}_{\varphi,T}(x) = \mathfrak{Todd}_\varphi(\lambda_T(x))$ .

*Proof of Proposition 10.11.* Let  $x \in K$ . Then,  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$ , so that every

$k \in \mathbb{N}$  satisfies  $\text{Coeff}_k(\lambda_T(x)) = \text{Coeff}_k\left(\sum_{i \in \mathbb{N}} \lambda^i(x) T^i\right) = \lambda^k(x)$  (by the definition of  $\text{Coeff}_k$ ). Thus,  $(\text{Coeff}_1(\lambda_T(x)), \text{Coeff}_2(\lambda_T(x)), \dots, \text{Coeff}_j(\lambda_T(x))) = (\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))$  for every  $j \in \mathbb{N}$ . Now, (58) (applied to  $p = \lambda_T(x)$ ) yields

$$\begin{aligned} & \mathfrak{Todd}_\varphi(\lambda_T(x)) \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\text{Coeff}_1(\lambda_T(x)), \text{Coeff}_2(\lambda_T(x)), \dots, \text{Coeff}_j(\lambda_T(x))) T^j \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x)) T^j \\ & \quad (\text{since } (\text{Coeff}_1(\lambda_T(x)), \text{Coeff}_2(\lambda_T(x)), \dots, \text{Coeff}_j(\lambda_T(x))) = (\lambda^1(x), \lambda^2(x), \dots, \lambda^j(x))) \\ &= \text{td}_{\varphi,T}(x). \end{aligned}$$

This proves Proposition 10.11. □

Now let us generalize our above results about  $\text{td}_{\varphi, T}$  to results about  $\mathfrak{Z}\text{odd}_{\varphi}$ . This will be rather easy since our proofs generalize.

Here comes the generalization of Proposition 10.3:

**Proposition 10.12.** Let  $\mathbf{Z}$  be a ring. Let  $K$  be a  $\mathbf{Z}$ -algebra. Let  $u \in \mathbf{Z}$ . Let  $p \in 1 + K[[T]]^+$ . Then,  $\mathfrak{Z}\text{odd}_{1+ut}(p) = \text{ev}_{uT}(p)$ . <sup>60</sup>

*Proof of Proposition 10.12.* The coefficient of the power series  $p$  before  $T^0$  is 1 (since  $p \in 1 + K[[T]]^+$ ). In other words,  $\text{Coeff}_0 p = 1$  (since  $\text{Coeff}_0 p$  is defined as the coefficient of the power series  $p$  before  $T^0$ ).

For every  $j \in \mathbb{N}$ , the coefficient of  $p$  before  $T^j$  is  $\text{Coeff}_j p$ . Hence,  $p = \sum_{j \in \mathbb{N}} (\text{Coeff}_j p) \cdot T^j$ . Thus,

$$\begin{aligned} \text{ev}_{uT} p &= \text{ev}_{uT} \left( \sum_{j \in \mathbb{N}} (\text{Coeff}_j p) \cdot T^j \right) = \sum_{j \in \mathbb{N}} (\text{Coeff}_j p) \cdot u^j T^j && \text{(by the definition of } \text{ev}_{uT} \text{)} \\ &= \sum_{j \in \mathbb{N}} u^j (\text{Coeff}_j p) T^j = \underbrace{u^0}_{=1} \underbrace{(\text{Coeff}_0 p)}_{=1} T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} u^j (\text{Coeff}_j p) T^j \\ &= 1T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} u^j (\text{Coeff}_j p) T^j. \end{aligned}$$

Compared with

$$\begin{aligned} &\mathfrak{Z}\text{odd}_{1+ut}(p) \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{1+ut, j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j && \text{(by (58), applied to } \varphi = 1 + ut \text{)} \\ &= \underbrace{\text{Td}_{1+ut, 0}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_0 p) T^0}_{\substack{= \text{Td}_{1+ut, 0} = 1 \\ \text{(by Proposition 10.6 (a),} \\ \text{applied to } \varphi = 1 + ut \text{)}}} \\ &\quad + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \underbrace{\text{Td}_{1+ut, j}}_{= u^j \alpha_j} (\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \\ &\quad \text{(by Proposition 10.4)} \\ &= 1T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \underbrace{(u^j \alpha_j) (\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j}_{= u^j (\text{Coeff}_j p)} \\ &= 1T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} u^j (\text{Coeff}_j p) T^j, \end{aligned}$$

this yields that  $\text{ev}_{uT} p = \mathfrak{Z}\text{odd}_{1+ut}(p)$ . This proves Proposition 10.12. □

<sup>60</sup>Let us recall that  $\text{ev}_{uT}$  denotes the map  $K[[T]] \rightarrow K[[T]]$  defined by

$$\text{ev}_{uT} \left( \sum_{i \in \mathbb{N}} a_i T^i \right) = \sum_{i \in \mathbb{N}} a_i u^i T^i \quad \text{for every power series } \sum_{i \in \mathbb{N}} a_i T^i \in K[[T]] \text{ (with } a_i \in K \text{ for every } i \text{)}.$$

Next, the generalization of Proposition 10.5:

**Proposition 10.13.** Let  $\mathbf{Z}$  be a ring. Let  $K$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $p \in K[[T]]$ .

(a) Then,  $\text{Coeff}_0(\mathfrak{Iodd}_\varphi(p)) = 1$ .

(b) Let  $\varphi_1$  be the coefficient of the power series  $\varphi \in \mathbf{Z}[[t]]$  before  $t^1$ . Then,  $\text{Coeff}_1(\mathfrak{Iodd}_\varphi(p)) = \varphi_1 \text{Coeff}_1 p$ .

*Proof of Proposition 10.13.* (a) We have

$$\begin{aligned} & \text{Coeff}_0(\mathfrak{Iodd}_\varphi(p)) \\ &= \text{Coeff}_0\left(\sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j\right) \quad (\text{by (58)}) \\ &= \text{Td}_{\varphi,0}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_0 p) \quad (\text{by the definition of } \text{Coeff}_0) \\ &= \text{Td}_{\varphi,0} = 1 \quad (\text{by Proposition 10.6 (a)}). \end{aligned}$$

(b) We have

$$\begin{aligned} & \text{Coeff}_1(\mathfrak{Iodd}_\varphi(p)) \\ &= \text{Coeff}_1\left(\sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j\right) \quad (\text{by (53)}) \\ &= \text{Td}_{\varphi,1}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_1 p) \quad (\text{by the definition of } \text{Coeff}_1) \\ &= \text{Td}_{\varphi,1}(\text{Coeff}_1 p) = \varphi_1 \text{Coeff}_1 p \\ & \quad (\text{since Proposition 10.6 (b) yields } \text{Td}_{\varphi,1} = \varphi_1 \alpha_1). \end{aligned}$$

Proposition 10.13 is now proven. □

Our next generalization is that of Proposition 10.7:

**Proposition 10.14.** Let  $\mathbf{Z}$  be a ring. Let  $K$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  and  $\psi \in 1 + \mathbf{Z}[[t]]^+$  be two power series with constant terms equal to 1. Let  $p \in K[[T]]$ . Then,  $\mathfrak{Iodd}_{\varphi\psi}(p) = \mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\psi(p)$ .

*Proof of Proposition 10.14.* For every  $j \in \mathbb{N}$ , we will abbreviate  $\text{Coeff}_j p$  by  $p_j$ . Then,  $(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) = (p_1, p_2, \dots, p_j)$ .

*1st Step:* For every  $j \in \mathbb{N}$ , we have

$$\text{Td}_{\varphi\psi,j}(p_1, p_2, \dots, p_j) = \sum_{i=0}^j \text{Td}_{\varphi,i}(p_1, p_2, \dots, p_i) \cdot \text{Td}_{\psi,j-i}(p_1, p_2, \dots, p_{j-i}).$$

*Proof.* Let  $j \in \mathbb{N}$ . Since the polynomials  $\text{Td}_{\varphi\psi,j}(\alpha_1, \alpha_2, \dots, \alpha_j)$  and  $\sum_{i=0}^j \text{Td}_{\varphi,i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi,j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i})$  are equal (by Proposition 10.8), their evaluations at  $(p_1, p_2, \dots, p_j)$  must also be equal. But since the evaluation of  $\text{Td}_{\varphi\psi,j}(\alpha_1, \alpha_2, \dots, \alpha_j)$  at  $(p_1, p_2, \dots, p_j)$  is  $\text{Td}_{\varphi\psi,j}(p_1, p_2, \dots, p_j)$ , whereas the evaluation of  $\sum_{i=0}^j \text{Td}_{\varphi,i}(\alpha_1, \alpha_2, \dots, \alpha_i) \cdot \text{Td}_{\psi,j-i}(\alpha_1, \alpha_2, \dots, \alpha_{j-i})$

at  $(p_1, p_2, \dots, p_j)$  is  $\sum_{i=0}^j \text{Td}_{\varphi,i}(p_1, p_2, \dots, p_i) \cdot \text{Td}_{\psi,j-i}(p_1, p_2, \dots, p_{j-i})$ , this yields that the values  $\text{Td}_{\varphi\psi,j}(p_1, p_2, \dots, p_j)$  and  $\sum_{i=0}^j \text{Td}_{\varphi,i}(p_1, p_2, \dots, p_i) \cdot \text{Td}_{\psi,j-i}(p_1, p_2, \dots, p_{j-i})$  are equal.

This proves the 1st step.

*2nd Step:* Now let us prove Proposition 10.14.

By (58) (applied to  $\varphi\psi$  instead of  $\varphi$ ), we have

$$\begin{aligned} \mathfrak{Iodd}_{\varphi\psi}(p) &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi\psi,j} \underbrace{(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)}_{=(p_1, p_2, \dots, p_j)} T^j \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi\psi,j}(p_1, p_2, \dots, p_j) T^j. \end{aligned}$$

But

$$\begin{aligned} &\underbrace{\mathfrak{Iodd}_{\varphi}(p)}_{\substack{= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \\ \text{(by (58))}}} \cdot \underbrace{\mathfrak{Iodd}_{\psi}(p)}_{\substack{= \sum_{j \in \mathbb{N}} \text{Td}_{\psi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \\ \text{(by (58), applied to } \psi \text{ instead of } \varphi)}} \\ &= \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j} \underbrace{(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)}_{=(p_1, p_2, \dots, p_j)} T^j \right) \cdot \left( \sum_{j \in \mathbb{N}} \text{Td}_{\psi,j} \underbrace{(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)}_{=(p_1, p_2, \dots, p_j)} T^j \right) \\ &= \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(p_1, p_2, \dots, p_j) T^j \right) \cdot \left( \sum_{j \in \mathbb{N}} \text{Td}_{\psi,j}(p_1, p_2, \dots, p_j) T^j \right) \\ &= \sum_{j \in \mathbb{N}} \underbrace{\left( \sum_{i=0}^j \text{Td}_{\varphi,i}(p_1, p_2, \dots, p_i) \cdot \text{Td}_{\psi,j-i}(p_1, p_2, \dots, p_{j-i}) \right)}_{\substack{= \text{Td}_{\varphi\psi,j}(p_1, p_2, \dots, p_j) \\ \text{(by the 1st Step)}}} T^j \\ &\quad \text{(by the definition of the product of two formal power series)} \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi\psi,j}(p_1, p_2, \dots, p_j) T^j = \mathfrak{Iodd}_{\varphi\psi}(p). \end{aligned}$$

This proves Proposition 10.14. □

Next, Proposition 10.9 generalizes to the following result:

**Proposition 10.15.** Let  $\mathbf{Z}$  be a ring. Let  $K$  be a  $\mathbf{Z}$ -algebra. Let  $m \in \mathbb{N}$ . For every  $i \in \{1, 2, \dots, m\}$ , let  $\varphi_i \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $p \in K[[T]]$ . Then,

$$\mathfrak{Iodd}_{\prod_{i=1}^m \varphi_i}(p) = \prod_{i=1}^m \mathfrak{Iodd}_{\varphi_i}(p).$$

*Proof of Proposition 10.15.* This can be proven by induction over  $m$ . The induction

base (the case  $m = 0$ ) requires showing that  $\mathfrak{Iodd}_1(p) = 1$ , but this is easy<sup>61</sup>. The induction step is a straightforward application of Proposition 10.14. Thus Proposition 10.15 is proven.  $\square$

We now formulate our generalization of Theorem 10.10 - it is through this generalization that we are going to prove Theorem 10.10:

**Theorem 10.16.** Let  $\mathbf{Z}$  be a ring. Let  $K$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $p \in 1 + K[[T]]^+$  and  $q \in 1 + K[[T]]^+$ . Then,  $\mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q) = \mathfrak{Iodd}_\varphi(pq)$ .

To prove this theorem, we first reduce it to the case when  $K = \mathbf{Z}$ :

**Lemma 10.17.** Let  $K$  be a ring. Let  $\varphi \in 1 + K[[t]]^+$  be a power series with constant term equal to 1. Let  $p \in 1 + K[[T]]^+$  and  $q \in 1 + K[[T]]^+$ . Then,  $\mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q) = \mathfrak{Iodd}_\varphi(pq)$ .

We will now prepare to the proof of this lemma. First, let us introduce the version of continuity that we need.

## 10.9. Preparing for the proof of Lemma 10.17

The following two definitions are copies of two definitions which we made in Section 5, with the only difference that the variable that used to be  $T$  in Section 5 is called  $t$  here.

**Definition.** Let  $K$  be a ring. Let  $K[t]^+$  be the subset of  $K[t]$  defined by

$$\begin{aligned} K[t]^+ &= tK[t] = \left\{ \sum_{i \in \mathbb{N}} a_i t^i \in K[t] \mid a_i \in K \text{ for all } i, \text{ and } a_0 = 0 \right\} \\ &= \{p \in K[t] \mid p \text{ is a polynomial with constant term } 0\}. \end{aligned}$$

Then, the set  $1 + K[t]^+$  is a subset of  $1 + K[[t]]^+$ . The elements of  $1 + K[t]^+$  are polynomials.

---

<sup>61</sup>*Proof.* Applying (58) to  $\varphi = 1$ , we obtain

$$\begin{aligned} \mathfrak{Iodd}_1(p) &= \sum_{j \in \mathbb{N}} \text{Td}_{1,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \\ &= \underbrace{\text{Td}_{1,0}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_0 p) T^0}_{\substack{=\text{Td}_{1,0}=1 \\ \text{(by Proposition 10.6 (a),} \\ \text{applied to } \varphi=1)}} + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \underbrace{\text{Td}_{1,j}}_{\substack{=\text{Td}_{1+0t,j}=0^j \alpha_j \\ \text{(by Proposition 10.4,} \\ \text{applied to } u=0)}} (\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \\ &= \underbrace{1}_{=1} T^0 + \sum_{\substack{j \in \mathbb{N}; \\ j > 0}} \underbrace{0^j}_{=0} \alpha_j (\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \\ &= 1 + \underbrace{\sum_{\substack{j \in \mathbb{N}; \\ j > 0}} 0 \alpha_j (\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j}_{=0} = 1. \end{aligned}$$

**Definition.** Let  $K$  be a ring. As a  $K$ -module,  $K[[t]] = \prod_{k \in \mathbb{N}} Kt^k$ . Now, we define the so-called  $(t)$ -topology on the ring  $K[[t]]$  as the topology generated by

$$\{u + t^N K[[t]] \mid u \in K[[t]] \text{ and } N \in \mathbb{N}\}.$$

In other words, the open sets of this topology should be all translates of the  $K$ -submodules  $t^N K[[t]]$  for  $N \in \mathbb{N}$ , as well as the unions of these translates<sup>62</sup>. (Note that, for each  $N \in \mathbb{N}$ , the set  $t^N K[[t]]$  is actually an ideal of  $K[[t]]$ , and consists of all power series  $f \in K[[t]]$  whose coefficients before  $t^0, t^1, \dots, t^{N-1}$  all vanish. This ideal  $t^N K[[t]]$  can also be described as the  $N$ -th power of the ideal  $tK[[t]]$ ; therefore, the  $(t)$ -topology on  $K[[t]]$  is precisely the so-called  $tK[[t]]$ -adic topology. Also note that every translate of the submodule  $t^N K[[t]]$  for  $N \in \mathbb{N}$  actually has the form  $p + t^N K[[t]]$  for a polynomial  $p \in K[t]$  of degree  $< N$ , and this polynomial is uniquely determined.) It is well-known that the  $(t)$ -topology makes  $K[[t]]$  into a topological ring.

Now, we have:

**Theorem 10.18.** Let  $K$  be a ring. The  $(t)$ -topology on the ring  $K[[t]]$  restricts to a topology on its subset  $1 + K[[t]]^+$ ; we call this topology the  $(t)$ -topology again. Whenever we say “open”, “continuous”, “dense”, etc., we are referring to this topology.

(a) The subset  $1 + K[t]^+$  is dense in  $1 + K[[t]]^+$ .

(b) Let  $f : 1 + K[[t]]^+ \rightarrow K[[T]]$  be a map such that for every  $n \in \mathbb{N}$  there exists some  $N \in \mathbb{N}$  such that the first  $n$  coefficients of the image of a formal power series under  $f$  depend only on the first  $N$  coefficients of the series itself (and not on the remaining ones). Then,  $f$  is continuous. (Here, the topology on  $K[[T]]$  is supposed to be the  $(T)$ -topology defined in Section 5.)

(c) The topological spaces  $K[[t]]$  and  $1 + K[[t]]^+$  are Hausdorff spaces.

*Proof of Theorem 10.18.* The parts (a) and (c) of Theorem 10.18 are obviously obtained from the parts (a) and (e) of Theorem 5.5 by renaming the variable  $T$  as  $t$ . Hence, they follow from Theorem 5.5. Part (b) of Theorem 10.18 is also true (it is an exercise in topology, proven in the same way as Theorem 5.5 (b)). This proves Theorem 10.18.  $\square$

The good thing about the topology on  $1 + K[[t]]^+$  just defined is that it makes the map  $1 + K[[t]]^+ \rightarrow K[[T]]$ ,  $\varphi \mapsto \mathfrak{I}o\delta\delta_\varphi(p)$  continuous for every given  $p \in K[[T]]$ :

**Proposition 10.19.** Let  $K$  be a ring. Let  $p \in K[[T]]$ . Then, the map

$$1 + K[[t]]^+ \rightarrow K[[T]], \quad \varphi \mapsto \mathfrak{I}o\delta\delta_\varphi(p)$$

is continuous. Here, the topology on  $1 + K[[t]]^+$  is supposed to be the  $(t)$ -topology, and the topology on  $K[[T]]$  is supposed to be the  $(T)$ -topology defined in Section 5.

<sup>62</sup>This includes the empty union, which is  $\emptyset$ .

*Proof of Proposition 10.19.* Let  $f$  denote the map

$$1 + K[[t]]^+ \rightarrow K[[T]], \quad \varphi \mapsto \mathfrak{I}od\mathfrak{d}_\varphi(p).$$

Then, in order to verify Proposition 10.19, we must prove that this map  $f$  is continuous.

*1st Step:* Let  $n \in \mathbb{N}$ . Let  $\varphi \in 1 + K[[t]]^+$  and  $\psi \in 1 + K[[t]]^+$  be two power series such that the first  $n$  coefficients<sup>63</sup> of  $\varphi$  are equal to the respective coefficients of  $\psi$ . Then, the first  $n$  coefficients of the power series  $\mathfrak{I}od\mathfrak{d}_\varphi(p)$  are equal to the respective coefficients of the power series  $\mathfrak{I}od\mathfrak{d}_\psi(p)$ .

*Proof.* Let  $m \in \{0, 1, \dots, n-1\}$  be arbitrary.

Since the first  $n$  coefficients of the power series  $\varphi$  are equal to the respective coefficients of the power series  $\psi$ , we have  $\varphi \equiv \psi \pmod{t^n}$  in the ring  $K[[t]]$ . Thus, there exists some formal power series  $\eta \in K[[t]]$  such that  $\varphi - \psi = \eta t^n$ . Consider such an  $\eta$ .

Consider the polynomial ring  $K[U_1, U_2, \dots, U_m]$  and its elements  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$

as in the definition of  $\text{Td}_{\varphi, j}$ .

Every  $i \in \{1, 2, \dots, m\}$  satisfies

$$\begin{aligned} \varphi(U_i T) - \psi(U_i T) &= \underbrace{(\varphi - \psi)}_{=\eta t^n}(U_i T) = (\eta t^n)(U_i T) \\ &\left( \begin{array}{l} \text{where } (\eta t^n)(U_i T) \text{ means the application of the formal} \\ \text{power series } \eta t^n \in K[[t]] \text{ to } U_i T, \text{ and not a product of } \eta t^n \\ \text{with } U_i T \text{ (whatever that could mean)} \end{array} \right) \\ &= \eta(U_i T) \cdot \underbrace{(U_i T)^n}_{=U_i^n T^n} = \eta(U_i T) \cdot U_i^n T^n \end{aligned}$$

and thus  $T^n \mid \varphi(U_i T) - \psi(U_i T)$ , so that  $\varphi(U_i T) \equiv \psi(U_i T) \pmod{T^n}$  in the ring  $(K[U_1, U_2, \dots, U_m])[[T]]$ . Multiplying the congruences  $\varphi(U_i T) \equiv \psi(U_i T) \pmod{T^n}$  for all  $i \in \{1, 2, \dots, m\}$ , we obtain  $\prod_{i=1}^m \varphi(U_i T) \equiv \prod_{i=1}^m \psi(U_i T) \pmod{T^n}$ . In other words, the

first  $n$  coefficients of the power series  $\prod_{i=1}^m \varphi(U_i T)$  are equal to the respective coefficients of the power series  $\prod_{i=1}^m \psi(U_i T)$ . In other words, every  $k \in \{0, 1, \dots, n-1\}$

satisfies  $\text{Coeff}_k \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Coeff}_k \left( \prod_{i=1}^m \psi(U_i T) \right)$ . Applied to  $k = m$ , this yields

$$\text{Coeff}_m \left( \prod_{i=1}^m \varphi(U_i T) \right) = \text{Coeff}_m \left( \prod_{i=1}^m \psi(U_i T) \right).$$

According to Theorem 10.1, the equation (51) holds in the ring  $(K[U_1, U_2, \dots, U_m])[[T]]$ . Thus,

$$\begin{aligned} \text{Coeff}_m \left( \prod_{i=1}^m \varphi(U_i T) \right) &= \text{Coeff}_m \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(X_1, X_2, \dots, X_j) T^j \right) \quad (\text{by (51)}) \\ &= \text{Td}_{\varphi, m}(X_1, X_2, \dots, X_m). \end{aligned}$$

<sup>63</sup>Note that when we say ‘‘the first  $n$  coefficients’’ (of some power series), we mean the coefficients before  $t^0, t^1, \dots, t^{n-1}$ .

The same argument, but applied to  $\psi$  instead of  $\varphi$ , yields

$$\text{Coeff}_m \left( \prod_{i=1}^m \psi(U_i T) \right) = \text{Td}_{\psi, m}(X_1, X_2, \dots, X_m).$$

Thus,

$$\begin{aligned} \text{Td}_{\varphi, m}(X_1, X_2, \dots, X_m) &= \text{Coeff}_m \left( \prod_{i=1}^m \varphi(U_i T) \right) \\ &= \text{Coeff}_m \left( \prod_{i=1}^m \psi(U_i T) \right) = \text{Td}_{\psi, m}(X_1, X_2, \dots, X_m). \end{aligned}$$

We will now use this to prove  $\text{Td}_{\varphi, m} = \text{Td}_{\psi, m}$ .

In fact, applying Theorem 4.1 **(a)** to  $\text{Td}_{\varphi, m}(X_1, X_2, \dots, X_m)$  instead of  $P$ , we conclude that there exists one and only one polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  such that  $\text{Td}_{\varphi, m}(X_1, X_2, \dots, X_m) = Q(X_1, X_2, \dots, X_m)$ . In particular, there exists *at most one* such polynomial  $Q \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$ . Hence,

$$\left( \begin{array}{l} \text{if } \mathfrak{Q}_1 \in K[\alpha_1, \alpha_2, \dots, \alpha_m] \text{ and } \mathfrak{Q}_2 \in K[\alpha_1, \alpha_2, \dots, \alpha_m] \text{ are two polynomials} \\ \text{such that } \text{Td}_{\varphi, m}(X_1, X_2, \dots, X_m) = \mathfrak{Q}_1(X_1, X_2, \dots, X_m) \text{ and} \\ \text{Td}_{\psi, m}(X_1, X_2, \dots, X_m) = \mathfrak{Q}_2(X_1, X_2, \dots, X_m), \text{ then } \mathfrak{Q}_1 = \mathfrak{Q}_2 \end{array} \right). \quad (59)$$

Let  $\mathfrak{Q}_1 \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  be the polynomial defined by  $\mathfrak{Q}_1 = \text{Td}_{\varphi, m}$ . Let  $\mathfrak{Q}_2 \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  be the polynomial defined by  $\mathfrak{Q}_2 = \text{Td}_{\psi, m}$ . We are now going to prove that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ .

Since our two polynomials  $\mathfrak{Q}_1$  and  $\mathfrak{Q}_2$  satisfy

$$\mathfrak{Q}_1(X_1, X_2, \dots, X_m) = \text{Td}_{\varphi, m}(X_1, X_2, \dots, X_m) \quad (\text{since } \mathfrak{Q}_1 = \text{Td}_{\varphi, m})$$

and

$$\begin{aligned} \mathfrak{Q}_2(X_1, X_2, \dots, X_m) &= \text{Td}_{\psi, m}(X_1, X_2, \dots, X_m) \quad (\text{since } \mathfrak{Q}_2 = \text{Td}_{\psi, m}) \\ &= \text{Td}_{\varphi, m}(X_1, X_2, \dots, X_m), \end{aligned}$$

we can conclude from (59) that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ . Hence,  $\text{Td}_{\varphi, m} = \mathfrak{Q}_1 = \mathfrak{Q}_2 = \text{Td}_{\psi, m}$ .

Now,

$$\begin{aligned} \text{Coeff}_m(\mathfrak{Todd}_{\varphi}(p)) &= \text{Coeff}_m \left( \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \right) \quad (\text{by (58)}) \\ &= \text{Td}_{\varphi, m}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_m p). \end{aligned}$$

The same argument, applied to  $\psi$  instead of  $\varphi$ , yields

$$\text{Coeff}_m(\mathfrak{Todd}_{\psi}(p)) = \text{Td}_{\psi, m}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_m p).$$

Thus,

$$\begin{aligned} \text{Coeff}_m(\mathfrak{Todd}_{\varphi}(p)) &= \underbrace{\text{Td}_{\varphi, m}}_{=\text{Td}_{\psi, m}}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_m p) \\ &= \text{Td}_{\psi, m}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_m p) = \text{Coeff}_m(\mathfrak{Todd}_{\psi}(p)). \end{aligned}$$



So we have proven that  $\text{Coeff}_m(\mathfrak{Iodd}_\varphi(p)) = \text{Coeff}_m(\mathfrak{Iodd}_\psi(p))$  for every  $m \in \{0, 1, \dots, n-1\}$ . In other words, for every  $m \in \{0, 1, \dots, n-1\}$ , the  $m$ -th coefficient of the power series  $\mathfrak{Iodd}_\varphi(p)$  equals the respective coefficient of the power series  $\mathfrak{Iodd}_\psi(p)$ . In other words, the first  $n$  coefficients of the power series  $\mathfrak{Iodd}_\varphi(p)$  are equal to the respective coefficients of the power series  $\mathfrak{Iodd}_\psi(p)$ .

This proves the 1st Step.

*2nd Step:* Let  $n \in \mathbb{N}$ . Let  $\varphi \in 1 + K[[t]]^+$  and  $\psi \in 1 + K[[t]]^+$  be two power series such that the first  $n$  coefficients<sup>64</sup> of  $\varphi$  are equal to the respective coefficients of  $\psi$ . Then, the first  $n$  coefficients of the power series  $f(\varphi)$  are equal to the respective coefficients of the power series  $f(\psi)$ .

*Proof.* This is just an equivalent restatement of the 1st Step, since  $f(\varphi) = \mathfrak{Iodd}_\varphi(p)$  (by the definition of  $f$ ) and  $f(\psi) = \mathfrak{Iodd}_\psi(p)$  (by the definition of  $f$ ).

*3rd Step:* We can rewrite the result of the 2nd Step as follows: If, for some  $n \in \mathbb{N}$ , two power series  $\varphi$  and  $\psi$  in  $1 + K[[t]]^+$  have the same first  $n$  coefficients (i. e., the first  $n$  coefficients of  $\varphi$  are equal to the respective coefficients of  $\psi$ ), then the images  $f(\varphi)$  and  $f(\psi)$  of these two power series under  $f$  also have the same first  $n$  coefficients. In other words, for every  $n \in \mathbb{N}$ , the first  $n$  coefficients of the image of a formal power series under  $f$  depend only on the first  $n$  coefficients of the series itself (and not on the remaining ones).

Hence, for every  $n \in \mathbb{N}$ , there exists some  $N \in \mathbb{N}$  such that the first  $n$  coefficients of the image of a formal power series under  $f$  depend only on the first  $N$  coefficients of the series itself (and not on the remaining ones)<sup>65</sup>. According to Theorem 10.18 (b), this yields that  $f$  is continuous.

Since  $f$  was defined as the map

$$1 + K[[t]]^+ \rightarrow K[[T]], \quad \varphi \mapsto \mathfrak{Iodd}_\varphi(p),$$

this shows that the map

$$1 + K[[t]]^+ \rightarrow K[[T]], \quad \varphi \mapsto \mathfrak{Iodd}_\varphi(p)$$

is continuous. Proposition 10.19 is thus proven.  $\square$

So much for the topology on  $1 + K[[t]]^+$ . We now discuss extensions of  $K$  that make polynomials factor.

By renaming the polynomial  $p$  as  $\varphi$  and the variable  $T$  as  $t$  in Theorem 5.2, we obtain the following fact:

**Theorem 10.20.** Let  $K$  be a ring. For every element  $\varphi \in 1 + K[t]^+$ , there exists an integer  $n$  (the degree of the polynomial  $\varphi$ ), a finite-free extension ring  $K_\varphi$  of the ring  $K$  and  $n$  elements  $p_1, p_2, \dots, p_n$  of this extension ring  $K_\varphi$  such that  $\varphi = \prod_{i=1}^n (1 + p_i t)$  in  $K_\varphi[t]$ .

<sup>64</sup>Note that when we say “the first  $n$  coefficients” (of some power series), we mean the coefficients before  $t^0, t^1, \dots, t^{n-1}$ .

<sup>65</sup>Namely, we can take  $N = n$ .

## 10.10. Proof of Lemma 10.17

Now, finally, to the proof of Lemma 10.17:

*Proof of Lemma 10.17.* Fix  $p \in 1+K[[T]]^+$  and  $q \in 1+K[[T]]^+$ , but let  $\varphi \in 1+K[[t]]^+$  vary.

*1st Step:* For every  $\varphi \in 1+K[t]^+$ , we have  $\mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q) = \mathfrak{Iodd}_\varphi(pq)$ .

*Proof.* Assume that  $\varphi \in 1+K[t]^+$ . According to Theorem 10.20, there exists an integer  $n$  (the degree of the polynomial  $\varphi$ ), a finite-free extension ring  $K_\varphi$  of the ring  $K$  and  $n$  elements  $p_1, p_2, \dots, p_n$  of this extension ring  $K_\varphi$  such that  $\varphi = \prod_{i=1}^n (1+p_it)$  in  $K_\varphi[t]$ . Consider this ring  $K_\varphi$  and these  $n$  elements  $p_1, p_2, \dots, p_n$ .

Since  $K$  is a subring of  $K_\varphi$ , we can canonically view the ring  $K[t]$  as a subring of  $K_\varphi[t]$ , and similarly we can view the ring  $K[[t]]$  as a subring of  $K_\varphi[[t]]$ , and we can view the ring  $K[[T]]$  as a subring of  $K_\varphi[[T]]$ .

Here is a trivial observation that we will tacitly use: For every  $r \in K[[T]]$ , the value of the term  $\mathfrak{Iodd}_\varphi(r)$  does not depend on whether we interpret  $\varphi$  as an element of  $1+K[t]^+$  or as an element of  $1+K_\varphi[t]^+$ , and also does not depend on whether we interpret  $r$  as an element of  $K[[T]]$  or as an element of  $K_\varphi[[T]]$ . This is because the definition of  $\mathfrak{Iodd}_\varphi(r)$  was functorial both in  $\mathbf{Z}$  and in  $K$ .

Let  $r \in 1+K[[T]]^+$  be arbitrary. Proposition 10.15 (applied to  $r, K_\varphi, K_\varphi, n$  and  $1+p_it$  instead of  $p, K, \mathbf{Z}, m$  and  $\varphi_i$ ) yields that  $\mathfrak{Iodd}_{\prod_{i=1}^n (1+p_it)}(r) = \prod_{i=1}^n \mathfrak{Iodd}_{1+p_it}(r)$ .

Since  $\prod_{i=1}^n (1+p_it) = \varphi$ , this rewrites as

$$\mathfrak{Iodd}_\varphi(r) = \prod_{i=1}^n \underbrace{\mathfrak{Iodd}_{1+p_it}(r)}_{=\text{ev}_{p_i T}(r)} = \prod_{i=1}^n \text{ev}_{p_i T}(r). \quad (60)$$

(by Proposition 10.12,  
applied to  $K_\varphi, K_\varphi, r$  and  $p_i$   
instead of  $\mathbf{Z}, K, p$  and  $u$ )

Applying (60) to  $r = p$ , we obtain  $\mathfrak{Iodd}_\varphi(p) = \prod_{i=1}^n \text{ev}_{p_i T}(p)$ . Applying (60) to  $r = q$ ,

we obtain  $\mathfrak{Iodd}_\varphi(q) = \prod_{i=1}^n \text{ev}_{p_i T}(q)$ . Applying (60) to  $r = pq$ , we obtain

$$\begin{aligned} \mathfrak{Iodd}_\varphi(pq) &= \prod_{i=1}^n \underbrace{\text{ev}_{p_i T}(pq)}_{=\text{ev}_{p_i T}(p) \cdot \text{ev}_{p_i T}(q)} \\ &\quad \text{(since } \text{ev}_{p_i T} \text{ is a ring homomorphism)} \\ &= \prod_{i=1}^n (\text{ev}_{p_i T}(p) \cdot \text{ev}_{p_i T}(q)) = \underbrace{\prod_{i=1}^n \text{ev}_{p_i T}(p)}_{=\mathfrak{Iodd}_\varphi(p)} \cdot \underbrace{\prod_{i=1}^n \text{ev}_{p_i T}(q)}_{=\mathfrak{Iodd}_\varphi(q)} \\ &= \mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q). \end{aligned}$$

This proves the 1st Step.

*2nd Step:* Let  $\mathfrak{f}_1 : 1+K[[t]]^+ \rightarrow K[[T]]$  be the map which sends every  $\varphi \in 1+K[[t]]^+$  to  $\mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q)$ .

Let  $\mathfrak{f}_2 : 1+K[[t]]^+ \rightarrow K[[T]]$  be the map which sends every  $\varphi \in 1+K[[t]]^+$  to  $\mathfrak{Iodd}_\varphi(pq)$ .

These maps  $\mathfrak{f}_1$  and  $\mathfrak{f}_2$  are equal to each other on a dense subset of  $1 + K[[t]]^+$ .

*Proof.* Every  $\varphi \in 1 + K[t]^+$  satisfies  $\mathfrak{f}_1(\varphi) = \mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q)$  (by the definition of  $\mathfrak{f}_1$ ) and  $\mathfrak{f}_2(\varphi) = \mathfrak{Iodd}_\varphi(pq)$  (by the definition of  $\mathfrak{f}_2$ ). Thus, every  $\varphi \in 1 + K[t]^+$  satisfies

$$\begin{aligned} \mathfrak{f}_1(\varphi) &= \mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q) = \mathfrak{Iodd}_\varphi(pq) && \text{(by the 1st Step)} \\ &= \mathfrak{f}_2(\varphi). \end{aligned}$$

In other words, the maps  $\mathfrak{f}_1$  and  $\mathfrak{f}_2$  are equal to each other on the subset  $1 + K[t]^+$ . Since  $1 + K[t]^+$  is a dense subset of  $1 + K[[t]]^+$  (by Theorem 10.18 (a)), this yields that the maps  $\mathfrak{f}_1$  and  $\mathfrak{f}_2$  are equal to each other on a dense subset of  $1 + K[[t]]^+$ . This proves the 2nd Step.

*3rd Step:* Consider the maps  $\mathfrak{f}_1$  and  $\mathfrak{f}_2$  defined in the 2nd Step.

The map  $1 + K[[t]]^+ \rightarrow K[[T]]$ ,  $\varphi \mapsto \mathfrak{Iodd}_\varphi(p)$  is continuous (by Proposition 10.19), and the map  $1 + K[[t]]^+ \rightarrow K[[T]]$ ,  $\varphi \mapsto \mathfrak{Iodd}_\varphi(q)$  is continuous (by Proposition 10.19, applied to  $q$  instead of  $p$ ). The pointwise product of these two maps is the map  $1 + K[[t]]^+ \rightarrow K[[T]]$ ,  $\varphi \mapsto \mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q)$ ; this is clearly the map  $\mathfrak{f}_1$ . Hence, we see that the map  $\mathfrak{f}_1$  is the pointwise product of two continuous maps. Thus, the map  $\mathfrak{f}_1$  itself is continuous (because the multiplication map  $K[[T]] \times K[[T]] \rightarrow K[[T]]$  is continuous, and therefore the pointwise product of two continuous maps to  $K[[T]]$  must be continuous itself).

On the other hand, the map  $\mathfrak{f}_2$  equals the map  $1 + K[[t]]^+ \rightarrow K[[T]]$ ,  $\varphi \mapsto \mathfrak{Iodd}_\varphi(pq)$ , and this map is continuous (by Proposition 10.19, applied to  $pq$  instead of  $p$ ). We thus see that the map  $\mathfrak{f}_2$  is continuous.

Recall the known fact that if two continuous maps from a topological space  $\mathfrak{P}$  to a Hausdorff topological space  $\mathfrak{Q}$  are equal to each other on a dense subset of  $\mathfrak{P}$ , then they are equal to each other on the whole  $\mathfrak{P}$ . Applying this to the two continuous maps  $\mathfrak{f}_1$  and  $\mathfrak{f}_2$  from the topological space  $1 + K[[t]]^+$  to the Hausdorff topological space  $K[[T]]$ , we conclude that the maps  $\mathfrak{f}_1$  and  $\mathfrak{f}_2$  are equal to each other on the whole  $1 + K[[t]]^+$  (because we know from the 2nd Step that they are equal to each other on a dense subset of  $1 + K[[t]]^+$ ).

In other words, every  $\varphi \in 1 + K[[t]]^+$  satisfies  $\mathfrak{f}_1(\varphi) = \mathfrak{f}_2(\varphi)$ . Since every  $\varphi \in 1 + K[[t]]^+$  satisfies  $\mathfrak{f}_1(\varphi) = \mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q)$  (by the definition of  $\mathfrak{f}_1$ ) and  $\mathfrak{f}_2(\varphi) = \mathfrak{Iodd}_\varphi(pq)$  (by the definition of  $\mathfrak{f}_2$ ), this rewrites as follows: Every  $\varphi \in 1 + K[[t]]^+$  satisfies  $\mathfrak{Iodd}_\varphi(p) \cdot \mathfrak{Iodd}_\varphi(q) = \mathfrak{Iodd}_\varphi(pq)$ . This proves Lemma 10.17.  $\square$

## 10.11. Preparing for the proof of Theorem 10.16: some trivial functoriality facts

We will eventually derive Theorem 10.16 from Lemma 10.17. This requires a very easy proposition and its corollary:

**Proposition 10.21.** Let  $\mathbf{Z}$  and  $\mathbf{Z}'$  be two rings, and let  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$  be a ring homomorphism. Let  $j \in \mathbb{N}$ . Clearly, the ring homomorphism  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$  canonically induces a ring homomorphism  $\rho[\alpha_1, \alpha_2, \dots, \alpha_j] : \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j] \rightarrow \mathbf{Z}'[\alpha_1, \alpha_2, \dots, \alpha_j]$  and a ring homomorphism  $\rho[[t]] : \mathbf{Z}[[t]] \rightarrow \mathbf{Z}'[[t]]$ . It is also clear that the latter homomorphism  $\rho[[t]]$  maps the subset  $1 + \mathbf{Z}[[t]]^+$  to the subset  $1 + \mathbf{Z}'[[t]]^+$ .

Every  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  satisfies  $\text{Td}_{(\rho[[t]])(\varphi),j} = \rho[\alpha_1, \alpha_2, \dots, \alpha_j](\text{Td}_{\varphi,j})$ .

All that this proposition tells us is that the object  $\text{Td}_{\varphi,j}$  is canonical with respect to the ring  $\mathbf{Z}$ . You may consider this obvious (it does, indeed, become obvious if you add to Theorem 4.1 (a) the additional assertion that the polynomial  $Q$ , for fixed  $P$ , is canonical with respect to the ring  $K$ ); if you do so, then you can immediately continue to Corollary 10.22. Here is, however, an alternative proof of Proposition 10.21 which does not resort to this kind of handwaving:

*Proof of Proposition 10.21.* Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$ .

Let  $m = j$ . We are going to work in the ring  $\mathbf{Z}'[U_1, U_2, \dots, U_m] = \mathbf{Z}'[U_1, U_2, \dots, U_j]$ . Note that the ring homomorphism  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$  canonically induces a ring homomorphism  $\rho[U_1, U_2, \dots, U_m] : \mathbf{Z}[U_1, U_2, \dots, U_m] \rightarrow \mathbf{Z}'[U_1, U_2, \dots, U_m]$ . Also note that

$$(\rho[\alpha_1, \alpha_2, \dots, \alpha_j](\text{Td}_{\varphi,j}))(X_1, X_2, \dots, X_j) = \rho[U_1, U_2, \dots, U_m](\text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j)).$$

66

The ring homomorphism  $\rho[U_1, U_2, \dots, U_m] : \mathbf{Z}[U_1, U_2, \dots, U_m] \rightarrow \mathbf{Z}'[U_1, U_2, \dots, U_m]$  canonically induces a ring homomorphism  $\rho[U_1, U_2, \dots, U_m][[T]] : \mathbf{Z}[U_1, U_2, \dots, U_m][[T]] \rightarrow$

<sup>66</sup>*Proof.* Let  $\rho' = \rho[U_1, U_2, \dots, U_m]$ . Then,  $\rho'$  is the ring homomorphism  $\mathbf{Z}[U_1, U_2, \dots, U_m] \rightarrow \mathbf{Z}'[U_1, U_2, \dots, U_m]$  canonically induced by the ring homomorphism  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$ . Hence,  $\rho'$  is a  $\mathbf{Z}$ -algebra homomorphism (where  $\mathbf{Z}'$  becomes a  $\mathbf{Z}$ -algebra by virtue of the ring homomorphism  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$ ) satisfying  $\rho'(U_k) = U_k$  for every  $k \in \{1, 2, \dots, m\}$ . Thus,

$$\begin{aligned} \rho'(X_i) &= \rho' \left( \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; k \in S \\ |S|=i}} \prod U_k \right) && \left( \text{since } X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; k \in S \\ |S|=i}} \prod U_k \right) \\ &= \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; k \in S \\ |S|=i}} \prod_{\substack{\rho'(U_k) \\ = U_k}} \rho'(U_k) && \text{(since } \rho' \text{ is a } \mathbf{Z}\text{-algebra homomorphism)} \\ &= \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; k \in S \\ |S|=i}} \prod U_k = X_i \end{aligned}$$

for every  $i \in \mathbb{N}$ . Thus,  $(\rho'(X_1), \rho'(X_2), \dots, \rho'(X_j)) = (X_1, X_2, \dots, X_j)$ .

Since  $\rho'$  is a  $\mathbf{Z}$ -algebra homomorphism and  $\text{Td}_{\varphi,j}$  is a polynomial over  $\mathbf{Z}$ , we have  $\rho'(\text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j)) = \text{Td}_{\varphi,j}(\rho'(X_1), \rho'(X_2), \dots, \rho'(X_j))$  (because  $\mathbf{Z}$ -algebra homomorphisms commute with polynomials over  $\mathbf{Z}$ ).

On the other hand, whenever  $U \in \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  is a polynomial and  $x_1, x_2, \dots, x_j$  are  $j$  elements of a commutative  $\mathbf{Z}'$ -algebra, we have  $(\rho[\alpha_1, \alpha_2, \dots, \alpha_j](U))(x_1, x_2, \dots, x_j) = U(x_1, x_2, \dots, x_j)$  (because this is more or less how  $U(x_1, x_2, \dots, x_j)$  is defined). Applied to  $U = \text{Td}_{\varphi,j}$  and  $x_k = X_k$ , this yields

$$\begin{aligned} (\rho[\alpha_1, \alpha_2, \dots, \alpha_j](\text{Td}_{\varphi,j}))(X_1, X_2, \dots, X_j) &= \text{Td}_{\varphi,j} \underbrace{(X_1, X_2, \dots, X_j)}_{=(\rho'(X_1), \rho'(X_2), \dots, \rho'(X_j))} \\ &= \text{Td}_{\varphi,j}(\rho'(X_1), \rho'(X_2), \dots, \rho'(X_j)) \\ &= \underbrace{\rho'}_{=\rho[U_1, U_2, \dots, U_m]}(\text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j)) \\ &= \rho[U_1, U_2, \dots, U_m](\text{Td}_{\varphi,j}(X_1, X_2, \dots, X_j)), \end{aligned}$$

qed.

$\mathbf{Z}' [U_1, U_2, \dots, U_m] [[T]]$  which is continuous with respect to the  $(T)$ -topology. By definition of this ring homomorphism, the diagram

$$\begin{array}{ccc} \mathbf{Z} [U_1, U_2, \dots, U_m] [[T]] & \xrightarrow{\text{Coeff}_j} & \mathbf{Z} [U_1, U_2, \dots, U_m] \\ \rho[U_1, U_2, \dots, U_m] [[T]] \downarrow & & \downarrow \rho[U_1, U_2, \dots, U_m] \\ \mathbf{Z}' [U_1, U_2, \dots, U_m] [[T]] & \xrightarrow{\text{Coeff}_j} & \mathbf{Z}' [U_1, U_2, \dots, U_m] \end{array}$$

commutes. Hence,

$$\rho [U_1, U_2, \dots, U_m] \left( \text{Coeff}_j \left( \prod_{i=1}^m \varphi (U_i T) \right) \right) = \text{Coeff}_j \left( \rho [U_1, U_2, \dots, U_m] [[T]] \left( \prod_{i=1}^m \varphi (U_i T) \right) \right).$$

Also,

$$\underbrace{\text{Td}_{\varphi, j}}_{\substack{=\text{Todd}_{(\varphi, j), j, [j]} \\ =\text{Todd}_{(\varphi, j), j, [m]} \\ \text{(since } j=m\text{)}}} (X_1, X_2, \dots, X_j) = \text{Todd}_{(\varphi, j), j, [m]} (X_1, X_2, \dots, X_j) = \text{Coeff}_j \left( \prod_{i=1}^m \varphi (U_i T) \right)$$

(by (52)), so that

$$\begin{aligned} \rho [U_1, U_2, \dots, U_m] (\text{Td}_{\varphi, j} (X_1, X_2, \dots, X_j)) &= \rho [U_1, U_2, \dots, U_m] \left( \text{Coeff}_j \left( \prod_{i=1}^m \varphi (U_i T) \right) \right) \\ &= \text{Coeff}_j \left( \rho [U_1, U_2, \dots, U_m] [[T]] \left( \prod_{i=1}^m \varphi (U_i T) \right) \right). \end{aligned} \tag{61}$$

The map  $\rho [U_1, U_2, \dots, U_m] [[T]]$  is a  $\mathbf{Z}$ -algebra homomorphism continuous with respect to the  $(T)$ -topology. Hence, it commutes with power series over  $\mathbf{Z}$ . Thus, for every  $i \in \{1, 2, \dots, m\}$ , we have

$$\rho [U_1, U_2, \dots, U_m] [[T]] (\varphi (U_i T)) = \varphi (\rho [U_1, U_2, \dots, U_m] [[T]] (U_i T)).$$

Since  $\rho [U_1, U_2, \dots, U_m] [[T]] (U_i T) = U_i T$  (because the map  $\rho [U_1, U_2, \dots, U_m] [[T]]$  is a ring homomorphism which (by its definition) maps  $U_i$  to  $U_i$  and  $T$  to  $T$ ), this simplifies to

$$\rho [U_1, U_2, \dots, U_m] [[T]] (\varphi (U_i T)) = \varphi (U_i T) = ((\rho [[t]]) (\varphi)) (U_i T).$$

Now,

$$\begin{aligned} \rho [U_1, U_2, \dots, U_m] [[T]] \left( \prod_{i=1}^m \varphi (U_i T) \right) &= \prod_{i=1}^m \underbrace{\rho [U_1, U_2, \dots, U_m] [[T]] (\varphi (U_i T))}_{=((\rho [[t]]) (\varphi)) (U_i T)} \\ &\quad \text{(since } \rho [U_1, U_2, \dots, U_m] [[T]] \text{ is a ring homomorphism)} \\ &= \prod_{i=1}^m ((\rho [[t]]) (\varphi)) (U_i T), \end{aligned}$$

so that (61) becomes

$$\rho [U_1, U_2, \dots, U_m] (\text{Td}_{\varphi, j} (X_1, X_2, \dots, X_j)) = \text{Coeff}_j \left( \prod_{i=1}^m ((\rho [[t]]) (\varphi)) (U_i T) \right).$$

Compared with

$$\begin{aligned} \underbrace{\text{Td}_{(\rho[[t]]) (\varphi), j}}_{\substack{= \text{Todd}_{((\rho[[t]]) (\varphi), j), j, [j]} \\ = \text{Todd}_{((\rho[[t]]) (\varphi), j), j, [m]} \\ \text{(since } j=m\text{)}}} (X_1, X_2, \dots, X_j) &= \text{Todd}_{((\rho[[t]]) (\varphi), j), j, [m]} (X_1, X_2, \dots, X_j) \\ &= \text{Coeff}_j \left( \prod_{i=1}^m ((\rho [[t]]) (\varphi)) (U_i T) \right) \\ &\quad \text{(by (52), applied to } (\rho [[t]]) (\varphi) \text{ instead of } \varphi), \end{aligned}$$

this yields

$$\rho [U_1, U_2, \dots, U_m] (\text{Td}_{\varphi, j} (X_1, X_2, \dots, X_j)) = \text{Td}_{(\rho[[t]]) (\varphi), j} (X_1, X_2, \dots, X_j). \quad (62)$$

Applying Theorem 4.1 (a) to  $K = \mathbf{Z}'$ ,  $m = j$  and  $P = \text{Td}_{(\rho[[t]]) (\varphi), j} (X_1, X_2, \dots, X_j)$ , we conclude that there exists one and only one polynomial  $Q \in \mathbf{Z}' [\alpha_1, \alpha_2, \dots, \alpha_j]$  such that  $\text{Td}_{(\rho[[t]]) (\varphi), j} (X_1, X_2, \dots, X_j) = Q (X_1, X_2, \dots, X_j)$ . In particular, there exists *most one* such polynomial  $Q \in \mathbf{Z}' [\alpha_1, \alpha_2, \dots, \alpha_j]$ . Hence,

$$\left( \begin{array}{l} \text{if } \mathfrak{Q}_1 \in \mathbf{Z}' [\alpha_1, \alpha_2, \dots, \alpha_j] \text{ and } \mathfrak{Q}_2 \in \mathbf{Z}' [\alpha_1, \alpha_2, \dots, \alpha_j] \text{ are two polynomials} \\ \text{such that } \text{Td}_{(\rho[[t]]) (\varphi), j} (X_1, X_2, \dots, X_j) = \mathfrak{Q}_1 (X_1, X_2, \dots, X_j) \text{ and} \\ \text{Td}_{(\rho[[t]]) (\varphi), j} (X_1, X_2, \dots, X_j) = \mathfrak{Q}_2 (X_1, X_2, \dots, X_j), \text{ then } \mathfrak{Q}_1 = \mathfrak{Q}_2 \end{array} \right). \quad (63)$$

Let  $\mathfrak{Q}_1 \in \mathbf{Z}' [\alpha_1, \alpha_2, \dots, \alpha_j]$  be the polynomial defined by  $\mathfrak{Q}_1 = \text{Td}_{(\rho[[t]]) (\varphi), j}$ . Let  $\mathfrak{Q}_2 \in \mathbf{Z}' [\alpha_1, \alpha_2, \dots, \alpha_j]$  be the polynomial defined by  $\mathfrak{Q}_2 = \rho [\alpha_1, \alpha_2, \dots, \alpha_j] (\text{Td}_{\varphi, j})$ . We are now going to prove that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ .

Since our two polynomials  $\mathfrak{Q}_1$  and  $\mathfrak{Q}_2$  satisfy

$$\mathfrak{Q}_1 (X_1, X_2, \dots, X_j) = \text{Td}_{(\rho[[t]]) (\varphi), j} (X_1, X_2, \dots, X_j) \quad \text{(since } \mathfrak{Q}_1 = \text{Td}_{(\rho[[t]]) (\varphi), j}\text{)}$$

and

$$\begin{aligned} \mathfrak{Q}_2 (X_1, X_2, \dots, X_j) &= (\rho [\alpha_1, \alpha_2, \dots, \alpha_j] (\text{Td}_{\varphi, j})) (X_1, X_2, \dots, X_j) \\ &\quad \text{(since } \mathfrak{Q}_2 = \rho [\alpha_1, \alpha_2, \dots, \alpha_j] (\text{Td}_{\varphi, j})\text{)} \\ &= \rho [U_1, U_2, \dots, U_m] (\text{Td}_{\varphi, j} (X_1, X_2, \dots, X_j)) \\ &= \text{Td}_{(\rho[[t]]) (\varphi), j} (X_1, X_2, \dots, X_j) \quad \text{(by (62))}, \end{aligned}$$

we can conclude from (63) that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ . Hence,

$$\text{Td}_{(\rho[[t]]) (\varphi), j} = \mathfrak{Q}_1 = \mathfrak{Q}_2 = \rho [\alpha_1, \alpha_2, \dots, \alpha_j] (\text{Td}_{\varphi, j}).$$

This proves Proposition 10.21. □

**Corollary 10.22.** Let  $\mathbf{Z}$  and  $\mathbf{Z}'$  be two rings, and let  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$  be a ring homomorphism. Clearly, the ring homomorphism  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$  canonically induces a ring homomorphism  $\rho[[t]] : \mathbf{Z}[[t]] \rightarrow \mathbf{Z}'[[t]]$ . It is also clear that the latter homomorphism  $\rho[[t]]$  maps the subset  $1 + \mathbf{Z}[[t]]^+$  to the subset  $1 + \mathbf{Z}'[[t]]^+$ .

Let  $K$  be a  $\mathbf{Z}'$ -algebra. Then,  $K$  also becomes a  $\mathbf{Z}$ -algebra by virtue of the ring homomorphism  $\rho$ . Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1.

Let  $p \in K[[T]]$ . Then,  $\mathfrak{Iodd}_\varphi(p) = \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(p)$ .

*Proof of Corollary 10.22.* Clearly, the ring homomorphism  $\rho : \mathbf{Z} \rightarrow \mathbf{Z}'$  canonically induces a ring homomorphism  $\rho[\alpha_1, \alpha_2, \dots, \alpha_j] : \mathbf{Z}[\alpha_1, \alpha_2, \dots, \alpha_j] \rightarrow \mathbf{Z}'[\alpha_1, \alpha_2, \dots, \alpha_j]$ .

Let  $j \in \mathbb{N}$ . Since  $K$  is a  $\mathbf{Z}$ -algebra by virtue of the ring homomorphism  $\rho$ , the value of  $\text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)$  is actually defined as

$$(\rho[\alpha_1, \alpha_2, \dots, \alpha_j](\text{Td}_{\varphi,j}))(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)$$

(since  $\text{Td}_{\varphi,j}$  itself is a polynomial over  $\mathbf{Z}$  rather than over  $\mathbf{Z}'$ ). Thus,

$$\begin{aligned} \text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) &= \underbrace{(\rho[\alpha_1, \alpha_2, \dots, \alpha_j](\text{Td}_{\varphi,j}))}_{\substack{=\text{Td}_{(\rho[[t]])(\varphi),j} \\ \text{(by Proposition 10.21)}}}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) \\ &= \text{Td}_{(\rho[[t]])(\varphi),j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p). \end{aligned}$$

Now, forget that we fixed  $j$ . By (58), we have

$$\begin{aligned} \mathfrak{Iodd}_\varphi(p) &= \sum_{j \in \mathbb{N}} \underbrace{\text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)}_{=\text{Td}_{(\rho[[t]])(\varphi),j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)} T^j \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{(\rho[[t]])(\varphi),j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j. \end{aligned}$$

On the other hand, (58) (applied to  $\mathbf{Z}'$  and  $(\rho[[t]])(\varphi)$  instead of  $\mathbf{Z}$  and  $\varphi$ ) yields

$$\mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(p) = \sum_{j \in \mathbb{N}} \text{Td}_{(\rho[[t]])(\varphi),j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j.$$

Thus,

$$\begin{aligned} \mathfrak{Iodd}_\varphi(p) &= \sum_{j \in \mathbb{N}} \text{Td}_{(\rho[[t]])(\varphi),j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) T^j \\ &= \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(p). \end{aligned}$$

This proves Corollary 10.22. □

## 10.12. Proof of Theorems 10.16 and 10.10

*Proof of Theorem 10.16.* Since  $K$  is a  $\mathbf{Z}$ -algebra, there is a canonical ring homomorphism  $\rho : \mathbf{Z} \rightarrow K$ . This homomorphism induces a canonical ring homomorphism  $\rho[[t]] : \mathbf{Z}[[t]] \rightarrow K[[t]]$ , which maps the subset  $1 + \mathbf{Z}[[t]]^+$  to  $1 + K[[t]]^+$ . Thus,  $(\rho[[t]])(\varphi) \in 1 + K[[t]]^+$  (since  $\varphi \in 1 + \mathbf{Z}[[t]]^+$ ).

Corollary 10.22 yields  $\mathfrak{Iodd}_\varphi(p) = \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(p)$ . Corollary 10.22 (applied to  $q$  instead of  $p$ ) yields  $\mathfrak{Iodd}_\varphi(q) = \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(q)$ . Corollary 10.22 (applied to  $pq$  instead of  $p$ ) yields  $\mathfrak{Iodd}_\varphi(pq) = \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(pq)$ . Lemma 10.17 (applied to  $(\rho[[t]])(\varphi)$  instead of  $\varphi$ ) yields  $\mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(p) \cdot \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(q) = \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(pq)$ . Now,

$$\underbrace{\mathfrak{Iodd}_\varphi(p)}_{=\mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(p)} \cdot \underbrace{\mathfrak{Iodd}_\varphi(q)}_{=\mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(q)} = \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(p) \cdot \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(q) = \mathfrak{Iodd}_{(\rho[[t]])(\varphi)}(pq) = \mathfrak{Iodd}_\varphi(pq).$$

Theorem 10.16 is thus proven.  $\square$

*Proof of Theorem 10.10.* Theorem 2.1 (a) yields  $\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x + y)$  (since  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring). Proposition 10.11 yields  $\text{td}_{\varphi, T}(x) = \mathfrak{Iodd}_\varphi(\lambda_T(x))$ . Proposition 10.11 (applied to  $y$  instead of  $x$ ) yields  $\text{td}_{\varphi, T}(y) = \mathfrak{Iodd}_\varphi(\lambda_T(y))$ . Hence,

$$\underbrace{\text{td}_{\varphi, T}(x)}_{=\mathfrak{Iodd}_\varphi(\lambda_T(x))} \cdot \underbrace{\text{td}_{\varphi, T}(y)}_{=\mathfrak{Iodd}_\varphi(\lambda_T(y))} = \mathfrak{Iodd}_\varphi(\lambda_T(x)) \cdot \mathfrak{Iodd}_\varphi(\lambda_T(y)) = \mathfrak{Iodd}_\varphi(\lambda_T(x) \cdot \lambda_T(y))$$

(by Theorem 10.16, applied to  $p = \lambda_T(x)$  and  $q = \lambda_T(y)$ ).

Proposition 10.11 (applied to  $x + y$  instead of  $x$ ) yields

$$\text{td}_{\varphi, T}(x + y) = \mathfrak{Iodd}_\varphi \left( \underbrace{\lambda_T(x + y)}_{=\lambda_T(x) \cdot \lambda_T(y)} \right) = \mathfrak{Iodd}_\varphi(\lambda_T(x) \cdot \lambda_T(y)).$$

Thus,

$$\text{td}_{\varphi, T}(x) \cdot \text{td}_{\varphi, T}(y) = \mathfrak{Iodd}_\varphi(\lambda_T(x) \cdot \lambda_T(y)) = \text{td}_{\varphi, T}(x + y).$$

Theorem 10.10 is thus proven.  $\square$

## 10.13. $\text{td}_{\varphi, T}$ is a homomorphism of additive groups

A slightly improved restatement of Theorem 10.10:

**Corollary 10.23.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Then,  $\text{td}_{\varphi, T}(K) \subseteq \Lambda(K)$ , and  $\text{td}_{\varphi, T} : K \rightarrow \Lambda(K)$  is a homomorphism of additive groups.

*Proof of Corollary 10.23.* Every  $x \in K$  satisfies  $\text{td}_{\varphi, T}(x) \in \Lambda(K)$  (since Proposition 10.5 (a) says that  $\text{Coeff}_0(\text{td}_{\varphi, T}(x)) = 1$ , so that the power series  $\text{td}_{\varphi, T}(x)$  has the constant term 1, and thus  $\text{td}_{\varphi, T}(x) \in 1 + K[[T]]^+ = \Lambda(K)$ ). In other words,  $\text{td}_{\varphi, T}(K) \subseteq \Lambda(K)$ .



Now we are going to prove that  $\text{td}_{\varphi,T} : K \rightarrow \Lambda(K)$  is a homomorphism of additive groups.

Theorem 10.10 (applied to  $x = 0$  and  $y = 0$ ) yields  $\text{td}_{\varphi,T}(0) \cdot \text{td}_{\varphi,T}(0) = \text{td}_{\varphi,T}(0 + 0) = \text{td}_{\varphi,T}(0)$ . Since  $\text{td}_{\varphi,T}(0)$  is an invertible element of  $K[[T]]$  (because  $\text{td}_{\varphi,T}(0)$  is a power series with constant term 1<sup>67</sup>, and every such power series is an invertible element of  $K[[T]]$ ), we can cancel  $\text{td}_{\varphi,T}(0)$  from this equation, and obtain  $\text{td}_{\varphi,T}(0) = 1$ . Since 0 is the neutral element of the additive group  $K$ , while 1 is the neutral element of the additive group  $\Lambda(K)$ , this yields that the map  $\text{td}_{\varphi,T}$  respects the neutral elements of the additive groups  $K$  and  $\Lambda(K)$ .

Any  $x \in K$  and  $y \in K$  satisfy

$$\begin{aligned} \text{td}_{\varphi,T}(x + y) &= \text{td}_{\varphi,T}(x) \cdot \text{td}_{\varphi,T}(y) && \text{(by Theorem 10.10)} \\ &= \text{td}_{\varphi,T}(x) \widehat{+} \text{td}_{\varphi,T}(y) && \left( \begin{array}{l} \text{since multiplication of power series} \\ \text{in } 1 + K[[T]]^+ \text{ is addition in the ring } \Lambda(K) \end{array} \right). \end{aligned}$$

Combined with the fact that the map  $\text{td}_{\varphi,T}$  respects the neutral elements of the additive groups  $K$  and  $\Lambda(K)$ , this yields: The map  $\text{td}_{\varphi,T} : K \rightarrow \Lambda(K)$  is a homomorphism of additive groups. Corollary 10.23 is proven.  $\square$

### 10.14. $\text{td}_{\varphi,T}$ of a 1-dimensional element

Next on our plan is to compute  $\text{td}_{\varphi,T}(x)$  for  $x$  any 1-dimensional element of  $K$ . We recall that we defined the notion of a 1-dimensional element of a  $\lambda$ -ring in Section 8.

Our main claim here is:

**Proposition 10.24.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $u$  be a 1-dimensional element of  $K$ . Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Then,  $\text{td}_{\varphi,T}(u) = \varphi(uT)$ .

For the proof of this, we again have to study the universal polynomials  $\text{Td}_{\varphi,j}$ :

**Proposition 10.25.** Let  $\mathbf{Z}$  be a ring. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $j \in \mathbb{N}$ . Let  $\varphi_j$  denote the coefficient of the power series  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  before  $t^j$ . Then, in the polynomial ring  $\mathbf{Z}[S]$ , we have  $\text{Td}_{\varphi,j}(S, 0, 0, \dots, 0) = \varphi_j S^j$ . (Here, when  $j = 0$ , the term  $\text{Td}_{\varphi,j}(S, 0, 0, \dots, 0)$  is understood to denote  $\text{Td}_{\varphi,j}$ .)

And again, we can generalize Proposition 10.24 (and in fact, we are going to prove Proposition 10.24 via this generalization):

**Proposition 10.26.** Let  $\mathbf{Z}$  be a ring. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $K$  be a  $\mathbf{Z}$ -algebra. Let  $u \in K$ . Then,  $\mathfrak{S} \circ \text{td}_{\varphi}(1 + uT) = \varphi(uT)$ .

*Proof of Proposition 10.25.* Let  $m = 1$ . Consider the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$  and its elements  $X_i = \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k$  as in the definition of  $\text{Td}_{\varphi,j}$ .

<sup>67</sup>since  $\text{td}_{\varphi,T}(0) \in \text{td}_{\varphi,T}(K) \subseteq \Lambda(K) = 1 + K[[T]]^+$

Since  $m = 1$ , we have  $\mathbf{Z}[U_1, U_2, \dots, U_m] = \mathbf{Z}[U_1]$ , and in this ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$  we have  $X_1 = U_1$  (because  $X_1$  is the 1-st elementary symmetric polynomial of the one variable  $U_1$ ).

For every integer  $i > 1$ , we have

$$\begin{aligned} X_i &= \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} U_k = \sum_{\substack{S \subseteq \{1\}; \\ |S|=i}} \prod_{k \in S} U_k & \quad (\text{since } m = 1, \text{ so that } \{1, 2, \dots, m\} = \{1\}) \\ &= (\text{empty sum}) & \quad (\text{since there doesn't exist any } S \subseteq \{1\} \text{ with } |S| = i \text{ (because } i > 1)) \\ &= 0 \end{aligned}$$

in the ring  $\mathbf{Z}[U_1, U_2, \dots, U_m]$ . Thus,  $(X_2, X_3, \dots, X_j) = (0, 0, \dots, 0)$ . Combining this with  $X_1 = U_1$ , we obtain  $(X_1, X_2, \dots, X_j) = (U_1, 0, 0, \dots, 0)$ .

We know from Theorem 10.1 that (51) holds in the ring  $(\mathbf{Z}[U_1, U_2, \dots, U_m])[[T]]$ . In other words,

$$\prod_{i=1}^m \varphi(U_i T) = \sum_{i \in \mathbb{N}} \text{Td}_{\varphi, i}(X_1, X_2, \dots, X_i) T^i$$

(this follows from (51) upon renaming the index  $j$  as  $i$ ). Since  $\prod_{i=1}^m \varphi(U_i T) = \varphi(U_1 T)$  (because  $m = 1$ ), this rewrites as

$$\varphi(U_1 T) = \sum_{i \in \mathbb{N}} \text{Td}_{\varphi, i}(X_1, X_2, \dots, X_i) T^i.$$

Thus,

$$\begin{aligned} \text{Coeff}_j(\varphi(U_1 T)) &= \text{Coeff}_j \left( \sum_{i \in \mathbb{N}} \text{Td}_{\varphi, i}(X_1, X_2, \dots, X_i) T^i \right) = \text{Td}_{\varphi, j}(\underbrace{X_1, X_2, \dots, X_j}_{=(U_1, 0, 0, \dots, 0)}) \\ &= \text{Td}_{\varphi, j}(U_1, 0, 0, \dots, 0). \end{aligned}$$

Compared with

$$\begin{aligned} \text{Coeff}_j(\varphi(U_1 T)) &= (\text{the coefficient of the power series } \varphi(U_1 T) \text{ before } T^j) \\ &= U_1^j \underbrace{(\text{the coefficient of the power series } \varphi \text{ before } t^j)}_{=\varphi_j} = U_1^j \varphi_j = \varphi_j U_1^j, \end{aligned}$$

this yields

$$\text{Td}_{\varphi, j}(U_1, 0, 0, \dots, 0) = \varphi_j U_1^j.$$

Now, let  $\kappa$  be the  $\mathbf{Z}$ -algebra homomorphism  $\mathbf{Z}[S] \rightarrow \mathbf{Z}[U_1]$  which maps  $S$  to  $U_1$ . This homomorphism  $\kappa$  must be an isomorphism (since  $U_1$  is obviously algebraically independent). Since  $\kappa$  is a  $\mathbf{Z}$ -algebra homomorphism and  $\text{Td}_{\varphi, j}$  is a polynomial, we have  $\kappa(\text{Td}_{\varphi, j}(S, 0, 0, \dots, 0)) = \text{Td}_{\varphi, j}(\kappa(S), \kappa(0), \kappa(0), \dots, \kappa(0))$  (because  $\mathbf{Z}$ -algebra homomorphisms commute with polynomials). But  $(\kappa(S), \kappa(0), \kappa(0), \dots, \kappa(0)) = (U_1, 0, 0, \dots, 0)$  (since  $\kappa(S) = U_1$  and  $\kappa(0) = 0$ ). Thus,

$$\begin{aligned} \kappa(\text{Td}_{\varphi, j}(S, 0, 0, \dots, 0)) &= \text{Td}_{\varphi, j}(\underbrace{\kappa(S), \kappa(0), \kappa(0), \dots, \kappa(0)}_{=(U_1, 0, 0, \dots, 0)}) = \text{Td}_{\varphi, j}(U_1, 0, 0, \dots, 0) = \varphi_j U_1^j \\ &= \varphi_j \kappa(S)^j & \quad (\text{since } U_1 = \kappa(S)) \\ &= \kappa(\varphi_j S^j) & \quad (\text{since } \kappa \text{ is a } \mathbf{Z}\text{-algebra homomorphism}). \end{aligned}$$

Thus,  $\text{Td}_{\varphi,j}(S, 0, 0, \dots, 0) = \varphi_j S^j$  (since  $\kappa$  is an isomorphism). This proves Proposition 10.25.  $\square$

*Proof of Proposition 10.26.* For every  $j \in \mathbb{N}$ , let  $\varphi_j$  denote the coefficient of the power series  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  before  $t^j$ . Let  $p = 1 + uT$ . Then,  $\text{Coeff}_1 p = u$  (by the definition of  $\text{Coeff}_1$ ) and  $\text{Coeff}_i p = 0$  for every integer  $i > 1$ .

Let  $j \in \mathbb{N}$  be arbitrary. Proposition 10.25 yields  $\text{Td}_{\varphi,j}(S, 0, 0, \dots, 0) = \varphi_j S^j$  in the polynomial ring  $\mathbf{Z}[S]$ . Applying this polynomial identity to  $S = u$ , we obtain  $\text{Td}_{\varphi,j}(u, 0, 0, \dots, 0) = \varphi_j u^j$ .

On the other hand,  $(\text{Coeff}_2 p, \text{Coeff}_3 p, \dots, \text{Coeff}_j p) = (0, 0, \dots, 0)$  (since  $\text{Coeff}_i p = 0$  for every integer  $i > 1$ ). Combining this with  $\text{Coeff}_1 p = u$ , we obtain

$$(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p) = (u, 0, 0, \dots, 0).$$

Thus,

$$\text{Td}_{\varphi,j}(\underbrace{(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)}_{=(u,0,0,\dots,0)}) = \text{Td}_{\varphi,j}(u, 0, 0, \dots, 0) = \varphi_j u^j.$$

Now forget that we fixed  $j \in \mathbb{N}$ . By (58), we have

$$\mathfrak{Iodd}_{\varphi}(p) = \sum_{j \in \mathbb{N}} \underbrace{\text{Td}_{\varphi,j}(\text{Coeff}_1 p, \text{Coeff}_2 p, \dots, \text{Coeff}_j p)}_{=\varphi_j u^j} T^j = \sum_{j \in \mathbb{N}} \varphi_j \underbrace{u^j T^j}_{=(uT)^j} = \sum_{j \in \mathbb{N}} \varphi_j (uT)^j.$$

On the other hand,  $\varphi = \sum_{j \in \mathbb{N}} \varphi_j t^j$  (since the coefficient of the power series  $\varphi$  before  $t^j$  is  $\varphi_j$  for every  $j \in \mathbb{N}$ ) and thus  $\varphi(uT) = \sum_{j \in \mathbb{N}} \varphi_j (uT)^j$ .

Altogether,  $\mathfrak{Iodd}_{\varphi}(p) = \sum_{j \in \mathbb{N}} \varphi_j (uT)^j = \varphi(uT)$ . Since  $1 + uT = p$ , we have  $\mathfrak{Iodd}_{\varphi}(1 + uT) = \mathfrak{Iodd}_{\varphi}(p) = \varphi(uT)$ . This proves Proposition 10.26.  $\square$

*Proof of Proposition 10.24.* Proposition 10.11 (applied to  $x = u$ ) yields  $\text{td}_{\varphi,T}(u) = \mathfrak{Iodd}_{\varphi}(\lambda_T(u))$ . But Theorem 8.3 (a) (applied to  $x = u$ ) yields that  $\lambda_T(u) = 1 + uT$  (since the element  $u$  is 1-dimensional). Thus,  $\text{td}_{\varphi,T}(u) = \mathfrak{Iodd}_{\varphi}\left(\underbrace{\lambda_T(u)}_{=1+uT}\right) = \mathfrak{Iodd}_{\varphi}(1 + uT) = \varphi(uT)$  (by Proposition 10.26). This proves Proposition 10.24.  $\square$

As a consequence of Proposition 10.24, we can obtain the following formula for  $\text{td}_{\varphi,T}$  on sums of 1-dimensional elements:

**Theorem 10.27.** Let  $\mathbf{Z}$  be a ring. Let  $\varphi \in 1 + \mathbf{Z}[[t]]^+$  be a power series with constant term equal to 1. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $u_1, u_2, \dots, u_m$  be 1-dimensional elements of  $K$ . Then,

$$\text{td}_{\varphi,T}(u_1 + u_2 + \dots + u_m) = \prod_{i=1}^m \varphi(u_i T).$$

*Proof of Theorem 10.27.* By Corollary 10.23, we know that  $\text{td}_{\varphi,T} : K \rightarrow \Lambda(K)$  is a homomorphism of additive groups. Hence,

$$\begin{aligned} \text{td}_{\varphi,T} \left( \sum_{i=1}^m u_i \right) &= \widehat{\sum_{i=1}^m} \text{td}_{\varphi,T}(u_i) = \prod_{i=1}^m \text{td}_{\varphi,T}(u_i) \\ &\left( \begin{array}{l} \text{since the addition in the ring } \Lambda(K) \text{ is the multiplication of power series,} \\ \text{so that } \widehat{\sum_{i=1}^m} = \prod_{i=1}^m \end{array} \right) \\ &= \prod_{i=1}^m \varphi(u_i T) \quad \left( \begin{array}{l} \text{because every } i \in \{1, 2, \dots, m\} \text{ satisfies } \text{td}_{\varphi,T}(u_i) = \varphi(u_i T) \\ \text{(by Proposition 10.24, applied to } u = u_i) \end{array} \right). \end{aligned}$$

Since  $\sum_{i=1}^m u_i = u_1 + u_2 + \dots + u_m$ , this rewrites as  $\text{td}_{\varphi,T}(u_1 + u_2 + \dots + u_m) = \prod_{i=1}^m \varphi(u_i T)$ .

Theorem 10.27 is thus proven.  $\square$

### 10.15. $\text{td}_{\varphi,T}$ for special $\lambda$ -rings

Theorem 10.27 gives us a shortcut to working with  $\text{td}_{\varphi,T}$  in the case when  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a *special*  $\lambda$ -ring: In fact, in this case, we can often prove a property of an arbitrary element of a special  $\lambda$ -ring just by proving it for sums of 1-dimensional elements (because of Theorem 8.4), and Theorem 10.27 gives us an explicit formula for the value of  $\text{td}_{\varphi,T}$  at every sum of 1-dimensional elements. The next theorem (Theorem 10.28) will give an example of this. First, a definition.

**Definition.** Let  $j \in \mathbb{N} \setminus \{0\}$ . Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Define a homomorphism  $\theta_T^j : K \rightarrow \Lambda(K)$  of additive groups by  $\theta_T^j = \text{td}_{\varphi_j, T}$ , where  $\varphi_j \in \mathbb{Z}[t]$  is the polynomial  $1 + t + t^2 + \dots + t^{j-1} = \frac{1 - t^j}{1 - t}$ .

[Again, [FulLan85] considers only  $\theta^j := \theta_1^j$ , which again is defined on  $x$  only if  $x$  is finite-dimensional. These  $\theta^j$  (or  $\theta^j(x)$ ?) are called *Bott's cannibalistic classes*, for whatever reason.]

**Theorem 10.28.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special  $\lambda$ -ring. Let  $x \in K$ . Let  $j \in \mathbb{N} \setminus \{0\}$ . Let  $\text{fr}_j : K[[T]] \rightarrow K[[T]]$  be the map which sends every power series  $\sum_{i \in \mathbb{N}} a_i T^i$  (with  $a_i \in K$  for every  $i \in \mathbb{N}$ ) to the power series  $\sum_{i \in \mathbb{N}} a_i T^{ji}$ . Then,  $\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x))) = \text{td}_{1-t^j, T}(x) = \lambda_{-T}(x) \theta_T^j(x)$  (where  $\psi^j[[T]]$  means the homomorphism  $K[[T]] \rightarrow K[[T]]$  defined by  $(\psi^j[[T]])(\sum_{i \in \mathbb{N}} a_i T^i) = \sum_{i \in \mathbb{N}} \psi^j(a_i) T^i$  for every power series  $\sum_{i \in \mathbb{N}} a_i T^i \in K[[T]]$ ).

*Proof of Theorem 10.28. 1st Step:* The equality  $\text{td}_{1-t^j, T}(x) = \lambda_{-T}(x) \theta_T^j(x)$  holds for every  $x \in K$  (no matter whether the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special or not).

*Proof.* Let  $\varphi_j \in \mathbb{Z}[t]$  be the polynomial  $1 + t + t^2 + \dots + t^{j-1} = \frac{1 - t^j}{1 - t}$ . According to the definition of  $\theta_T^j$ , we have  $\theta_T^j = \text{td}_{\varphi_j, T}$ .

Let  $x \in K$ . Applying Proposition 10.7 to  $\mathbf{Z} = \mathbb{Z}$ ,  $\varphi = 1 - t$  and  $\psi = \varphi_j$ , we obtain  $\text{td}_{\varphi\psi, T}(x) = \text{td}_{\varphi, T}(x) \text{td}_{\psi, T}(x)$ . Since

$$\text{td}_{\varphi\psi, T}(x) = \text{td}_{1-t^j, T}(x) \quad \left( \begin{array}{l} \text{because } \varphi = 1 - t \text{ and } \psi = \varphi_j = \frac{1 - t^j}{1 - t}, \\ \text{so that } \varphi\psi = (1 - t) \cdot \frac{1 - t^j}{1 - t} = 1 - t^j \end{array} \right),$$

$$\begin{aligned} \text{td}_{\varphi, T}(x) &= \text{td}_{1+(-1)t, T}(x) && \text{(since } \varphi = 1 - t = 1 + (-1)t \text{)} \\ &= \lambda_{(-1)T}(x) && \text{(by Proposition 10.3, applied to } \mathbf{Z} = \mathbb{Z} \text{ and } u = -1 \text{)} \\ &= \lambda_{-T}(x) \end{aligned}$$

and

$$\begin{aligned} \text{td}_{\psi, T}(x) &= \underbrace{\text{td}_{\varphi_j, T}(x)}_{=\theta_T^j} && \text{(since } \psi = \varphi_j \text{)} \\ &= \theta_T^j(x), \end{aligned}$$

this rewrites as  $\text{td}_{1-t^j, T}(x) = \lambda_{-T}(x) \theta_T^j(x)$ . This proves the 1st Step.

*2nd Step:* A remark about the map  $\text{fr}_j$ : This map sends every power series  $P \in K[[T]]$  to the power series  $P(T^j)$ . It is easy to see that this map  $\text{fr}_j$  is a  $K$ -algebra homomorphism continuous with respect to the  $(T)$ -topology. It satisfies  $\text{fr}_j(T) = T^j$  (obviously) and can be shown to be the only continuous (with respect to the  $(T)$ -topology)  $K$ -algebra homomorphism  $K[[T]] \rightarrow K[[T]]$  which sends  $T$  to  $T^j$ .

*3rd Step:* The equality  $\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x))) = \text{td}_{1-t^j, T}(x)$  holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$  such that  $x$  is the sum of finitely many 1-dimensional elements of  $K$ .

*Proof.* Let  $\varphi = 1 - t^j$ .

Let  $x \in K$  be such that  $x$  is the sum of finitely many 1-dimensional elements of  $K$ . In other words,  $x = u_1 + u_2 + \dots + u_m$  for some 1-dimensional elements  $u_1, u_2, \dots, u_m$  of  $K$ . Consider these elements  $u_1, u_2, \dots, u_m$ . Then,

$$\begin{aligned} \text{td}_{\varphi, T}(x) &= \text{td}_{\varphi, T}(u_1 + u_2 + \dots + u_m) = \prod_{i=1}^m \underbrace{\varphi(u_i T)}_{\substack{=1-(u_i T)^j \\ \text{(since } \varphi=1-t^j)}} && \text{(by Theorem 10.27)} \\ &= \prod_{i=1}^m \left( 1 - \underbrace{(u_i T)^j}_{=u_i^j T^j} \right) = \prod_{i=1}^m (1 - u_i^j T^j). \end{aligned}$$

On the other hand,  $x = u_1 + u_2 + \dots + u_m = \sum_{i=1}^m u_i$ , so that

$$\begin{aligned} \lambda_T(x) &= \lambda_T\left(\sum_{i=1}^m u_i\right) = \widehat{\sum_{i=1}^m} \lambda_T(u_i) && \text{(since } \lambda_T \text{ is a ring homomorphism)} \\ &= \prod_{i=1}^m \lambda_T(u_i) && \left( \begin{array}{l} \text{since the addition in the ring } \Lambda(K) \text{ is the} \\ \text{multiplication of power series, and thus } \widehat{\sum_{i=1}^m} = \prod_{i=1}^m \end{array} \right) \\ &= \prod_{i=1}^m (1 + u_i T) && \left( \begin{array}{l} \text{because every } i \in \{1, 2, \dots, m\} \text{ satisfies } \lambda_T(u_i) = 1 + u_i T \\ \text{(by Theorem 8.3 (a) (applied to } u_i \text{ instead of } x), \\ \text{since } u_i \text{ is 1-dimensional)} \end{array} \right). \end{aligned}$$

Now,

$$\begin{aligned} \lambda_{-T}(x) &= \text{ev}_{-T} \left( \underbrace{\lambda_T(x)}_{=\prod_{i=1}^m (1+u_i T)} \right) = \text{ev}_{-T} \left( \prod_{i=1}^m (1 + u_i T) \right) \\ &= \prod_{i=1}^m \underbrace{\text{ev}_{-T}(1 + u_i T)}_{=1-u_i T} && \text{(since } \text{ev}_{-T} \text{ is a ring homomorphism)} \\ &\quad \text{(by the definition of } \text{ev}_{-T} \text{)} \\ &= \prod_{i=1}^m (1 - u_i T). \end{aligned}$$

Thus,

$$\begin{aligned} (\psi^j [[T]]) (\lambda_{-T}(x)) &= (\psi^j [[T]]) \left( \prod_{i=1}^m (1 - u_i T) \right) = \prod_{i=1}^m \left( 1 - \underbrace{(\psi^j [[T]]) (u_i T)}_{=\psi^j(u_i) T} \right) \\ &\quad \text{(since } \psi^j [[T]] \text{ is a ring homomorphism)} \\ &= \prod_{i=1}^m (1 - \psi^j(u_i) T), \end{aligned}$$

so that

$$\begin{aligned} \text{fr}_j((\psi^j [[T]]) (\lambda_{-T}(x))) &= \text{fr}_j \left( \prod_{i=1}^m (1 - \psi^j(u_i) T) \right) = \prod_{i=1}^m \left( 1 - \psi^j(u_i) \underbrace{\text{fr}_j(T)}_{=T^j} \right) \\ &\quad \text{(since } \text{fr}_j \text{ is a } K\text{-algebra homomorphism)} \\ &= \prod_{i=1}^m (1 - \psi^j(u_i) T^j). \end{aligned}$$

Now, for every  $i \in \{1, 2, \dots, m\}$ , we can apply Theorem 9.4 to 1 and  $u_i$  instead of  $m$  and  $u_i$ , and obtain  $\psi^j(u_i) = u_i^j$ . Hence,

$$\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x))) = \prod_{i=1}^m \left( 1 - \underbrace{\psi^j(u_i)}_{=u_i^j} T^j \right) = \prod_{i=1}^m (1 - u_i^j T^j) = \text{td}_{\varphi, T}(x) = \text{td}_{1-t^j, T}(x)$$

(since  $\varphi = 1 - t^j$ ). This proves the 3rd Step.

*4th Step:* The equality  $\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x))) = \text{td}_{1-t^j, T}(x)$  holds for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$ .

*Proof.* We want to derive this from the 3rd Step by applying Theorem 8.4.

Fix some  $k \in \mathbb{N}$ .

Define a 1-operation  $m$  of special  $\lambda$ -rings by  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})} = \text{Coeff}_k \circ \text{fr}_j \circ (\psi^j[[T]]) \circ \lambda_{-T}$  for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ . (This is indeed a 1-operation, since (42) shows that  $\psi^j$  is a polynomial in  $\lambda^1, \lambda^2, \dots, \lambda^j$  with integer coefficients.)

Define a 1-operation  $m'$  of special  $\lambda$ -rings by  $m'_{(K, (\lambda^i)_{i \in \mathbb{N}})} = \text{Coeff}_k \circ \text{td}_{1-t^j, T}$  for every  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ . (This is, again, a 1-operation, since (53) shows that  $\text{Coeff}_k \circ \text{td}_{1-t^j, T} = \text{Td}_{1-t^j, k}(\lambda^1, \lambda^2, \dots, \lambda^k)$  is a polynomial in  $\lambda^1, \lambda^2, \dots, \lambda^k$  with integer coefficients.)

These two 1-operations  $m$  and  $m'$  satisfy both conditions of Theorem 8.4: The continuity assumption holds (since the operations  $m$  and  $m'$  are obtained by taking polynomials (with integer coefficients) and compositions of finitely many of the  $\lambda^1, \lambda^2, \lambda^3, \dots$ , so that the maps  $m_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$  and  $m'_{(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})}$  are obtained by taking polynomials (with integer coefficients) and compositions of finitely many of the  $\widehat{\lambda}^1, \widehat{\lambda}^2, \widehat{\lambda}^3, \dots$ , and therefore continuous because of Theorem 5.5 (d)), and the split equality assumption holds (since it states that for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$  such that  $x$  is the sum of finitely many 1-dimensional elements of  $K$ , we have  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x)$ ; but this simply means that  $\text{Coeff}_k(\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x)))) = \text{Coeff}_k(\text{td}_{1-t^j, T}(x))$ , which was proven in the 3rd step). Hence, by Theorem 8.4, we have  $m = m'$ . Hence, for every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$ , we have  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x)$ . Since  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = \text{Coeff}_k(\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x))))$  (by the definition of  $m_{(K, (\lambda^i)_{i \in \mathbb{N}})}$ ) and  $m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}(x) = \text{Coeff}_k(\text{td}_{1-t^j, T}(x))$  (by the definition of  $m'_{(K, (\lambda^i)_{i \in \mathbb{N}})}$ ), this rewrites as follows: For every special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and every  $x \in K$ , we have  $\text{Coeff}_k(\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x)))) = \text{Coeff}_k(\text{td}_{1-t^j, T}(x))$ .

Now fix some special  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  and some  $x \in K$ , and forget that we fixed  $k$ . We have just proven that  $\text{Coeff}_k(\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x)))) = \text{Coeff}_k(\text{td}_{1-t^j, T}(x))$  for every  $k \in \mathbb{N}$ . In other words, we have just proven that each coefficient of the power series  $\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x)))$  equals to the corresponding coefficient of the power series  $\text{td}_{1-t^j, T}(x)$ . Thus,  $\text{fr}_j((\psi^j[[T]])(\lambda_{-T}(x))) = \text{td}_{1-t^j, T}(x)$ . This proves the 4th Step.

*5th Step:* Theorem 10.28 now follows by combining the 1st Step and the 4th Step.  $\square$

## 10.16. A somewhat more general context for Todd homomorphisms

Having proven Theorem 10.28, we are done proving all important properties of the  $\varphi$ -Todd homomorphisms. One thing that I still want to do is to give a (not particularly unexpected, and apparently not particularly useful) generalization of our notion of  $\varphi$ -Todd homomorphisms to the case when the power series  $\varphi$  does not lie in  $1 + \mathbf{Z}[[t]]^+$  but, instead, lies in  $1 + \mathbf{Z}'[[t]]^+$  for  $\mathbf{Z}'$  being a  $\mathbf{Z}$ -algebra. In this case, it turns out, not much will change - but, of course,  $\text{td}_{\varphi,T}$  will no longer be a map  $K \rightarrow K[[T]]$  but instead will be a map  $K \rightarrow (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]$ . Here is the precise definition:

**Definition.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1. We define a map  $\text{td}_{\varphi,T,\mathbf{Z}'} : K \rightarrow (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]$  by

$$\text{td}_{\varphi,T,\mathbf{Z}'}(x) = \sum_{j \in \mathbb{N}} \text{Td}_{\varphi,j}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1) T^j \quad \text{for every } x \in K. \quad (64)$$

Let me explain what I mean by  $\text{Td}_{\varphi,j}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1)$  here: The tensor product  $K \otimes_{\mathbf{Z}} \mathbf{Z}'$  is both a  $K$ -algebra and a  $\mathbf{Z}'$ -algebra (since the tensor product of two commutative  $\mathbf{Z}$ -algebras is an algebra over each of its tensorands). Since it is a  $\mathbf{Z}'$ -algebra, we can apply the polynomial  $\text{Td}_{\varphi,j} \in \mathbf{Z}'[\alpha_1, \alpha_2, \dots, \alpha_j]$  to the elements  $\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1$  of  $K \otimes_{\mathbf{Z}} \mathbf{Z}'$ ; the result of this application is what we denote by  $\text{Td}_{\varphi,j}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1)$ .

We call  $\text{td}_{\varphi,T,\mathbf{Z}'}$  the  $(\varphi, \mathbf{Z}')$ -Todd homomorphism of the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$ .

Note that, in the particular case when  $\mathbf{Z}' = \mathbf{Z}$ , the map  $\text{td}_{\varphi,T,\mathbf{Z}'}$  is identical with the map  $\text{td}_{\varphi,T}$  if we make the canonical identification of  $K$  with  $K \otimes_{\mathbf{Z}} \mathbf{Z}$ .

All results about maps of the form  $\text{td}_{\varphi,T}$  that we have formulated possess analoga pertaining to  $\text{td}_{\varphi,T,\mathbf{Z}'}$ . Proving these analoga is usually as simple as repeating the proofs of the original results and replacing some of the  $\mathbf{Z}$ 's by  $\mathbf{Z}'$ 's, some of the  $K$ 's by  $(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ 's, and some of the  $\lambda^i(x)$ 's by  $\lambda^i(x) \otimes 1$ 's. However, it is yet easier to prove these analoga by deriving them from the corresponding properties of the maps  $\mathfrak{Todd}_{\varphi}$ . What makes this possible is the following generalization of Proposition 10.11:

**Proposition 10.29.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1. Let  $\iota : K \rightarrow K \otimes_{\mathbf{Z}} \mathbf{Z}'$  be the canonical map (mapping every  $\xi \in K$  to  $\xi \otimes 1 \in K \otimes_{\mathbf{Z}} \mathbf{Z}'$ ). Then, every  $x \in K$  satisfies  $\text{td}_{\varphi,T,\mathbf{Z}'}(x) = \mathfrak{Todd}_{\varphi}(\iota[[T]](\lambda_T(x)))$ .

The proof of this is very similar to that of Proposition 10.11, and is part of Exercise 10.2.

Let us formulate the analoga of our above-proven results about  $\text{td}_{\varphi,T}$ . The proofs of all these analoga will be done in Exercise 10.2.

Here is the analogue of Proposition 10.3:



**Proposition 10.30.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $u \in \mathbf{Z}'$ . For every  $x \in K$ , we have  $\text{td}_{1+ut, T, \mathbf{Z}'}(x) = \lambda_{(1 \otimes u)T}(x)$ , where  $\lambda_{(1 \otimes u)T}(x)$  means  $\text{ev}_{(1 \otimes u)T}(\lambda_T(x))$ .

Similarly, here is the analogue of Proposition 10.5:

**Proposition 10.31.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1.

(a) Then,  $\text{Coeff}_0(\text{td}_{\varphi, T, \mathbf{Z}'}(x)) = 1$  for every  $x \in K$ .

(b) Let  $\varphi_1$  be the coefficient of the power series  $\varphi \in \mathbf{Z}'[[t]]$  before  $t^1$ . Then,  $\text{Coeff}_1(\text{td}_{\varphi, T, \mathbf{Z}'}(x)) = \varphi_1(x \otimes 1)$  for every  $x \in K$ .

The analogue of Proposition 10.7:

**Proposition 10.32.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  and  $\psi \in 1 + \mathbf{Z}'[[t]]^+$  be two power series with constant terms equal to 1. For every  $x \in K$ , we have  $\text{td}_{\varphi\psi, T, \mathbf{Z}'}(x) = \text{td}_{\varphi, T, \mathbf{Z}'}(x) \text{td}_{\psi, T, \mathbf{Z}'}(x)$ .

Next, the analogue of Proposition 10.9:

**Proposition 10.33.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $m \in \mathbb{N}$ . For every  $i \in \{1, 2, \dots, m\}$ , let  $\varphi_i \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1. For every  $x \in K$ , we have

$$\text{td}_{\prod_{i=1}^m \varphi_i, T, \mathbf{Z}'}(x) = \prod_{i=1}^m \text{td}_{\varphi_i, T, \mathbf{Z}'}(x).$$

Next, the analogue of Theorem 10.10:

**Theorem 10.34.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1. Let  $x \in K$  and  $y \in K$ . Then,  $\text{td}_{\varphi, T, \mathbf{Z}'}(x) \cdot \text{td}_{\varphi, T, \mathbf{Z}'}(y) = \text{td}_{\varphi, T, \mathbf{Z}'}(x + y)$ .

The analogue of Corollary 10.23 is what one would expect it to be:

**Corollary 10.35.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1. Then,  $\text{td}_{\varphi, T, \mathbf{Z}'}(K) \subseteq \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ , and  $\text{td}_{\varphi, T, \mathbf{Z}'} : K \rightarrow \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$  is a homomorphism of additive groups.

We can also generalize Proposition 10.24:

**Proposition 10.36.** Let  $\mathbf{Z}$  be a ring. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $u$  be a 1-dimensional element of  $K$ . Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1. Then,  $\text{td}_{\varphi, T, \mathbf{Z}'}(u) = \varphi((u \otimes 1)T)$ , where  $u \otimes 1$  denotes the element  $u \otimes 1$  of  $K \otimes_{\mathbf{Z}} \mathbf{Z}'$ .

Finally, the analogue to Theorem 10.27:

**Theorem 10.37.** Let  $\mathbf{Z}$  be a ring. Let  $\mathbf{Z}'$  be a  $\mathbf{Z}$ -algebra. Let  $\varphi \in 1 + \mathbf{Z}'[[t]]^+$  be a power series with constant term equal to 1. Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring such that  $K$  is a  $\mathbf{Z}$ -algebra. Let  $u_1, u_2, \dots, u_m$  be 1-dimensional elements of  $K$ . Then,

$$\text{td}_{\varphi, T, \mathbf{Z}'}(u_1 + u_2 + \dots + u_m) = \prod_{i=1}^m \varphi((u_i \otimes 1)T).$$

## 10.17. Exercises

*Exercise 10.2.* Prove Proposition 10.29, Proposition 10.30, Proposition 10.31, Proposition 10.32, Proposition 10.33, Theorem 10.34, Corollary 10.35, Proposition 10.36 and Theorem 10.37.

[...]

## Appendix X. Positive structure on $\lambda$ -rings

**WARNING:** The following appendix is incomplete.

Almost all  $\lambda$ -rings in Fulton/Lang [Fullan85] and many  $\lambda$ -rings in nature carry an additional structure called a *positive structure*:

**Definition. 1)** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $\varepsilon : K \rightarrow \mathbb{Z}$  be a surjective<sup>68</sup> ring homomorphism. Let  $\mathbf{E}$  be a subset of  $K$  such that  $\mathbf{E}$  is closed under addition and multiplication and contains the subset  $\mathbb{Z}^+$  of  $K$  (that is, the image of  $\mathbb{Z}^+$  under the canonical ring homomorphism  $\mathbb{Z}^+ \rightarrow K$ ). Also assume that  $K = \mathbf{E} - \mathbf{E}$  (that is, every element of  $K$  can be written as difference of two elements of  $\mathbf{E}$ ). Furthermore, assume that every  $e \in \mathbf{E}$  satisfies

$$\varepsilon(e) > 0; \quad \lambda^i(e) = 0 \quad \text{for any } i > \varepsilon(e), \quad \text{and that } \lambda^{\varepsilon(e)}(e) \text{ is a unit in the ring } K.$$

Besides, we assume that for every invertible element  $u \in \mathbf{E}$ , the inverse of  $u$  must lie in  $\mathbf{E}$  as well.

<sup>68</sup>I am quoting this from [Fullan85]. Personally, I have never have met a non-surjective ring homomorphism to  $\mathbb{Z}$  in my life.

Then,  $(\varepsilon, \mathbf{E})$  is called a *positive structure* on the  $\lambda$ -ring. The homomorphism  $\varepsilon : K \rightarrow \mathbb{Z}$  is called an *augmentation* for the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  with its positive structure  $(\varepsilon, \mathbf{E})$ . The elements of the set  $\mathbf{E}$  are called the *positive elements* of the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  with its positive structure  $(\varepsilon, \mathbf{E})$ .<sup>69</sup>

[Some assumptions may still be missing here. For example, we might want to require that  $\lambda^i(\mathbf{E}) \subseteq \mathbf{E}$ .] [#2]

**2)** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring with a positive structure  $(\varepsilon, \mathbf{E})$ . The subset  $\{u \in \mathbf{E} \mid \varepsilon(u) = 1\}$  of  $\mathbf{E}$  is usually denoted as  $\mathbf{L}$ . The elements of  $\mathbf{L}$  are called the *line elements* of the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  with its positive structure  $(\varepsilon, \mathbf{E})$ .

**Theorem X.1.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring with a positive structure  $(\varepsilon, \mathbf{E})$ .

**(a)** Then,  $\mathbf{L} = \{u \in \mathbf{E} \mid \varepsilon(u) = 1\}$  is a subgroup of the (multiplicative) unit group  $K^\times$  of  $K$ .

**(b)** We have  $\mathbf{L} = \{u \in \mathbf{E} \mid \lambda_T(u) = 1 + uT\} = \{u \in \mathbf{E} \mid u \text{ is 1-dimensional}\}$ .

*Proof of Theorem X.1. (b) 1st Step:* We have  $\mathbf{L} \subseteq \{u \in \mathbf{E} \mid u \text{ is 1-dimensional}\}$ .

*Proof.* For every  $u \in \mathbf{L}$ , we have  $\varepsilon(u) = 1$  (by the definition of  $\mathbf{L}$ ) and  $\lambda^i(u) = 0$  for any  $i > \varepsilon(u)$  (by the axioms of a positive structure, since  $u \in \mathbf{L} \subseteq \mathbf{E}$ ). Thus, for every  $u \in \mathbf{L}$ , we have  $\lambda^i(u) = 0$  for any  $i > 1$  (because for any  $i > 1$ , we have  $i > 1 = \varepsilon(u)$  and thus  $\lambda^i(u) = 0$ ). In other words, every  $u \in \mathbf{L}$  is 1-dimensional. Thus,  $\mathbf{L} \subseteq \{u \in \mathbf{E} \mid u \text{ is 1-dimensional}\}$ .

<sup>69</sup>One remark about the assumption that for every invertible element  $u \in \mathbf{E}$ , the inverse of  $u$  must lie in  $\mathbf{E}$  as well:

Fulton and Lang do not make this assumption in [FulLan85], but this is a mistake on their side. In fact, they claim that the set of all  $u \in \mathbf{E}$  such that  $\varepsilon(u) = 1$  is a subgroup of  $K^\times$ . But to make this claim, they need the above-mentioned assumption (or another similar one). In fact, here is an example of a  $\lambda$ -ring  $K$  which satisfies all of their assumptions, but for which the set of all  $u \in \mathbf{E}$  such that  $\varepsilon(u) = 1$  is *not* a subgroup of  $K^\times$ :

Let  $Z$  be the free group on one generator. (This group  $Z$  is, of course, none other than  $\mathbb{Z}$ , written multiplicatively; however we must avoid calling it  $\mathbb{Z}$ , lest it is confused with the *ring*  $\mathbb{Z}$ .) Let  $X$  be the generator of  $Z$ . Applying Exercise 3.4 to  $M = Z$ , we get a  $\lambda$ -ring  $(\mathbb{Z}[Z], (\lambda^i)_{i \in \mathbb{N}})$ . Now define a map  $\varepsilon : \mathbb{Z}[Z] \rightarrow \mathbb{Z}$  by

$$\varepsilon \left( \sum_{m \in Z} \alpha_m m \right) = \sum_{m \in Z} \alpha_m \quad \text{for all } (\alpha_m)_{m \in Z} \in \mathbb{Z}^{(Z)}.$$

Then,  $\varepsilon$  is a surjective ring homomorphism. Define  $\mathbf{E}$  to be the additive and multiplicative closure of the subset

$$\{1, X, X^2, \dots\} \cup \{1 + X^{-1}, 1 + X^{-2}, 1 + X^{-3}, \dots\}$$

of  $\mathbb{Z}[Z]$ . It is easy to see that all of our conditions are satisfied, except for the assumption that for every invertible element  $u \in \mathbf{E}$ , the inverse of  $u$  must lie in  $\mathbf{E}$  as well. Hence, if we would omit this assumption (as Fulton and Lang do in [FulLan85]), the pair  $(\varepsilon, \mathbf{E})$  would be a positive structure on our  $\lambda$ -ring  $(\mathbb{Z}[Z], (\lambda^i)_{i \in \mathbb{N}})$ . However, the set of all  $u \in \mathbf{E}$  such that  $\varepsilon(u) = 1$  is not a subgroup of  $K^\times$  in this case, since this set contains  $X$  but not its inverse  $X^{-1}$  (in fact, it is easy to see that  $X^{-1} \notin \mathbf{E}$ ; otherwise  $X^{-1}$  would be a sum of products of elements of  $\{1, X, X^2, \dots\} \cup \{1 + X^{-1}, 1 + X^{-2}, 1 + X^{-3}, \dots\}$ , and applying  $\varepsilon$  we would conclude that the sum has only 1 summand, which is easy to rule out).

*2nd Step:* We have  $\{u \in \mathbf{E} \mid u \text{ is 1-dimensional}\} \subseteq \{u \in \mathbf{E} \mid \lambda_T(u) = 1 + uT\}$ .

*Proof.* Every 1-dimensional  $u \in \mathbf{E}$  satisfies  $\lambda^i(u) = 0$  for any  $i > 1$  (by the definition of “1-dimensional”). Now, every 1-dimensional  $u \in \mathbf{E}$  satisfies

$$\lambda_T(u) = \sum_{i \in \mathbb{N}} \lambda^i(u) T^i = \underbrace{\lambda^0(u)}_{=1} + \underbrace{\lambda^1(u)}_{=u} T + \sum_{i \geq 2} \underbrace{\lambda^i(u)}_{=0, \text{ since } i > 1} T^i = 1 + uT.$$

Thus, we have shown that every 1-dimensional  $u \in \mathbf{E}$  satisfies  $\lambda_T(u) = 1 + uT$ . In other words,  $\{u \in \mathbf{E} \mid u \text{ is 1-dimensional}\} \subseteq \{u \in \mathbf{E} \mid \lambda_T(u) = 1 + uT\}$ .

*3rd Step:* We have  $\{u \in \mathbf{E} \mid \lambda_T(u) = 1 + uT\} \subseteq \mathbf{L}$ .

*Proof.* Let  $u \in \mathbf{E}$  be an element satisfying  $\lambda_T(u) = 1 + uT$ . Then this  $u$  must satisfy

$$\sum_{i \in \mathbb{N}} \lambda^i(u) T^i = \lambda_T(u) = 1 + uT,$$

and thus (by comparison of coefficients)  $\lambda^i(u) = 0$  for every  $i > 1$ , so that  $\varepsilon(u) \leq 1$  (because  $\lambda^{\varepsilon(u)}(u)$  is a unit in the ring  $K$  (since  $u \in \mathbf{E}$ ), so that  $\lambda^{\varepsilon(u)}(u) \neq 0$  and thus  $\varepsilon(u) \leq 1$ ). Together with  $\varepsilon(u) > 0$ , this yields  $\varepsilon(u) = 1$  and thus  $u \in \mathbf{L}$ .

We have thus proven that every  $u \in \mathbf{E}$  satisfying  $\lambda_T(u) = 1 + uT$  must satisfy  $u \in \mathbf{L}$ . In other words, we have proven that  $\{u \in \mathbf{E} \mid \lambda_T(u) = 1 + uT\} \subseteq \mathbf{L}$ .

*4th Step:* Combining the results of the 1st Step, the 2nd Step and the 3rd Step, we conclude that  $\mathbf{L} = \{u \in \mathbf{E} \mid \lambda_T(u) = 1 + uT\} = \{u \in \mathbf{E} \mid u \text{ is 1-dimensional}\}$ . This proves Theorem X.1 (b).

(a) *1st Step:* Every  $u \in \mathbf{L}$  is invertible in  $K$ , and the inverse of every  $u \in \mathbf{L}$  lies in  $\mathbf{L}$ .

*Proof.* Let  $u \in \mathbf{L}$ . Then,  $\lambda^{\varepsilon(u)}(u)$  is a unit in the ring  $K$  (since  $u \in \mathbf{E}$ ). But  $\varepsilon(u) = 1$  (since  $u \in \mathbf{L}$ ) and thus  $\lambda^{\varepsilon(u)}(u) = \lambda^1(u) = u$ . Thus,  $u$  is a unit in  $K$ ; that is,  $u$  is invertible. Its inverse  $u^{-1}$  must lie in  $\mathbf{E}$  as well (because  $u \in \mathbf{L} \subseteq \mathbf{E}$ , and because of our assumption that for every invertible element  $u \in \mathbf{E}$ , the inverse of  $u$  must lie in  $\mathbf{E}$

as well). Since  $\varepsilon$  is a ring homomorphism, we have  $\varepsilon(u^{-1}) = \left( \underbrace{\varepsilon(u)}_{=1} \right)^{-1} = 1^{-1} = 1$ .

This, together with  $u^{-1} \in \mathbf{E}$ , yields  $u^{-1} \in \mathbf{L}$  (by the definition of  $\mathbf{L}$ ).

We have thus proven that every  $u \in \mathbf{L}$  is invertible in  $K$ , and the inverse of every  $u \in \mathbf{L}$  lies in  $\mathbf{L}$ .

*2nd Step:* The set  $\mathbf{L}$  is closed under multiplication and contains the multiplicative unity of  $K$ .

*Proof.* This is trivial.

*3rd Step:* Theorem X.1 (a) trivially follows from the 1st Step and the 2nd Step.  $\square$

**Theorem X.2.** Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a special(?)  $\lambda$ -ring with a positive structure  $(\varepsilon, \mathbf{E})$ . Let  $e \in \mathbf{E}$ , and let  $r = \varepsilon(e) - 1$ . Define a polynomial  $p_e \in K[T]$  by  $p_e(T) = \sum_{i=0}^{r+1} (-1)^i \lambda^i(e) T^{r+1-i}$ . Set  $K_e = K[T] / (p_e(T)) = K[\ell]$ , where  $\ell$  denotes the equivalence class of  $T$  modulo  $p_e(T)$ . Then,  $K_e$  is a finite-free extension ring of  $K$ . There exists a map  $\tilde{\lambda}^i : K_e \rightarrow K_e$  for every  $i \in \mathbb{N}$  such that  $\left( K_e, \left( \tilde{\lambda}^i \right)_{i \in \mathbb{N}} \right)$  is a  $\lambda$ -ring such that the inclusion  $K \rightarrow K_e$

is a  $\lambda$ -ring homomorphism and such that  $\ell \in K_e$  is a 1-dimensional element. Moreover, there exists a positive structure  $(\varepsilon_e, \mathbf{E}_e)$  on  $K_e$  defined by  $\varepsilon_e(\ell) = 1$  and  $\mathbf{E}_e = \left\{ \sum_{i \in \mathbb{N}, j \in \mathbb{N}} a_{i,j} \ell^i (e - \ell)^j \mid a_{i,j} \in \mathbf{E} \text{ for all } i \in \mathbb{N} \text{ and } j \in \mathbb{N} \right\}$ .

By iterating the construction in Theorem X.2, we can find, for any  $e \in \mathbf{E}$ , an extension ring of  $K$  with a  $\lambda$ -ring structure in which  $e$  is the sum of  $r$  1-dimensional elements. This is called the *splitting principle*, and is what Fulton/Lang [Fullan85] use instead of Theorem 8.4 above when they want to prove an identity just by verifying it for sums of 1-dimensional elements. However, this way they can only show it for positive elements, while Theorem 8.4 yields it for arbitrary elements.

## 11. Hints and solutions to exercises

### 11.1. To Section 1

### 11.2. To Section 2

*Exercise 2.1: Solution:* (a) Theorem 2.1 (c) says that  $f$  is a homomorphism of  $\lambda$ -rings if and only if  $\mu_T \circ f = f [[T]] \circ \lambda_T$ . Thus, it remains to show that  $\mu_T \circ f = f [[T]] \circ \lambda_T$  holds if and only if every  $e \in E$  satisfies  $(\mu_T \circ f)(e) = (f [[T]] \circ \lambda_T)(e)$ . Since  $E$  is a generating set of the  $\mathbb{Z}$ -module  $K$ , this comes down to proving the following three facts:

- We have  $(\mu_T \circ f)(0) = (f [[T]] \circ \lambda_T)(0)$ .
- We have  $(\mu_T \circ f)(-x) = (f [[T]] \circ \lambda_T)(-x)$  for every  $x \in K$  which satisfies  $(\mu_T \circ f)(x) = (f [[T]] \circ \lambda_T)(x)$ .
- We have  $(\mu_T \circ f)(x + y) = (f [[T]] \circ \lambda_T)(x + y)$  for any  $x \in K$  and  $y \in K$  which satisfy  $(\mu_T \circ f)(x) = (f [[T]] \circ \lambda_T)(x)$  and  $(\mu_T \circ f)(y) = (f [[T]] \circ \lambda_T)(y)$ .

We will only prove the last of these three assertions (the other two are similar): If  $(\mu_T \circ f)(x) = (f [[T]] \circ \lambda_T)(x)$  and  $(\mu_T \circ f)(y) = (f [[T]] \circ \lambda_T)(y)$ , then

$$\begin{aligned}
& (\mu_T \circ f)(x + y) \\
&= \mu_T(f(x + y)) = \mu_T(f(x) + f(y)) \quad (\text{since } f \text{ is a ring homomorphism}) \\
&= \mu_T(f(x)) \cdot \mu_T(f(y)) \quad \left( \text{by Theorem 2.1 (a), applied to the } \lambda\text{-ring } \left( L, (\mu^i)_{i \in \mathbb{N}} \right) \right) \\
&= \underbrace{(\mu_T \circ f)(x)}_{=(f [[T]] \circ \lambda_T)(x)} \cdot \underbrace{(\mu_T \circ f)(y)}_{=(f [[T]] \circ \lambda_T)(y)} = (f [[T]] \circ \lambda_T)(x) \cdot (f [[T]] \circ \lambda_T)(y) \\
&= (f [[T]]) \left( \underbrace{\lambda_T(x) \cdot \lambda_T(y)}_{=\lambda_T(x+y) \text{ by Theorem 2.1 (a)}} \right) = (f [[T]] \circ \lambda_T)(x + y),
\end{aligned}$$

qed.

- (b) This follows from (a) in the same way as Theorem 2.1 (c) was proven.

*Exercise 2.2: Solution:* It is an exercise in basic algebra to see that  $L - L$  is a subring of  $K$ . Thus, it only remains to show that  $\lambda^i(L - L) \subseteq L - L$  for every  $i \in \mathbb{N}$ . In other words, we have to prove that  $\lambda^i(\ell - \ell') \in L - L$  for every  $\ell \in L$  and  $\ell' \in L$ .

We are going to prove this by induction, so we assume that  $\lambda^j(\ell - \ell') \in L - L$  for all  $j < i$ . Then,

$$\begin{aligned} \lambda^i(\ell) &= \lambda^i((\ell - \ell') + \ell') = \sum_{j=0}^i \lambda^j(\ell - \ell') \lambda^{i-j}(\ell') && \text{(by the definition of } \lambda\text{-rings)} \\ &= \sum_{j=0}^{i-1} \underbrace{\lambda^j(\ell - \ell')}_{\substack{\in L-L, \text{ since} \\ j < i}} \underbrace{\lambda^{i-j}(\ell')}_{\substack{\in L, \text{ since} \\ \ell' \in L}} + \lambda^i(\ell - \ell') \underbrace{\lambda^0(\ell')}_{=1} \\ &\in \underbrace{(L - L)L}_{\substack{\subseteq LL - LL \subseteq L - L \\ \text{(since } LL \subseteq L)}} + \lambda^i(\ell - \ell') \subseteq (L - L) + \lambda^i(\ell - \ell'). \end{aligned}$$

But  $\lambda^i(\ell)$  itself lies in  $L - L$  (since  $\ell \in L$ , so that  $\lambda^i(\ell) \in L$  and thus  $\lambda^i(\ell) = \underbrace{\lambda^i(\ell)}_{\in L} - \underbrace{0}_{\in L} \in L - L$ ), so this yields  $\lambda^i(\ell - \ell') \in L - L$ , and this completes our induction.

*Exercise 2.3: Solution:*

*Proof of Theorem 2.2. (a)* Let  $x \in K/I$ . Let  $y \in K$  and  $z \in K$  be two elements of  $K$  satisfying  $\bar{y} = x$  and  $\bar{z} = x$ . Then,  $\bar{y} = x = \bar{z}$ , so that  $y \equiv z \pmod{I}$ . In other words,  $y - z \in I$ .

We know (from the definition of  $\lambda$ -ideals) that  $I$  is a  $\lambda$ -ideal of  $K$  if and only if every  $t \in I$  and every positive integer  $i$  satisfy  $\lambda^i(t) \in I$ . Since we know that  $I$  is a  $\lambda$ -ideal, we conclude that every  $t \in I$  and every positive integer  $i$  satisfy  $\lambda^i(t) \in I$ . Applied to  $t = y - z$ , this yields that every positive integer  $i$  satisfies  $\lambda^i(y - z) \in I$ .

Fix  $k \in \mathbb{N}$ . The equality (5), applied to  $y - z$  and  $z$  instead of  $x$  and  $y$ , yields

$$\begin{aligned} \lambda^k((y - z) + z) &= \sum_{i=0}^k \lambda^i(y - z) \lambda^{k-i}(z) = \underbrace{\lambda^0(y - z)}_{\substack{=1 \\ \text{(since } \lambda^0(t)=1 \\ \text{for every } t \in K)}} \underbrace{\lambda^{k-0}(z)}_{=\lambda^k} + \sum_{i=0}^k \underbrace{\lambda^i(y - z)}_{\substack{\in I \\ \text{(since } i \text{ is a positive} \\ \text{integer)}}} \lambda^{k-i}(z) \\ &\in \underbrace{1\lambda^k(z)}_{=\lambda^k(z)} + \underbrace{\sum_{i=0}^k I\lambda^{k-i}(z)}_{\substack{\subseteq I \\ \text{(since } I \text{ is an ideal)}}} \subseteq \lambda^k(z) + I. \end{aligned}$$

Since  $(y - z) + z = y$ , this rewrites as  $\lambda^k(y) \in \lambda^k(z) + I$ . In other words,  $\overline{\lambda^k(y)} = \overline{\lambda^k(z)}$ .

Now, forget that we fixed  $k$ . We thus have proven that  $\overline{\lambda^k(y)} = \overline{\lambda^k(z)}$  for every  $k \in \mathbb{N}$ . Renaming  $k$  as  $i$  in this claim, we conclude that we have  $\overline{\lambda^i(y)} = \overline{\lambda^i(z)}$  for every  $i \in \mathbb{N}$ . Theorem 2.2 (a) is proven.

(b) First of all,

$$\left( \tilde{\lambda}^0(x) = 1 \text{ for every } x \in K/I \right) \tag{65}$$

70. Next,

$$\left( \tilde{\lambda}^1(x) = x \text{ for every } x \in K/I \right) \quad (66)$$

71. Finally,

$$\left( \tilde{\lambda}^k(x+y) = \sum_{i=0}^k \tilde{\lambda}^i(x) \tilde{\lambda}^{k-i}(y) \quad \text{for every } k \in \mathbb{N}, x \in K/I \text{ and } y \in K/I \right) \quad (67)$$

72.

Now, according to the definition of a  $\lambda$ -ring, we know that  $\left( K/I, \left( \tilde{\lambda}^i \right)_{i \in \mathbb{N}} \right)$  is a  $\lambda$ -ring if and only if it satisfies the relations (65), (66) and (67). Since we have shown that

<sup>70</sup>*Proof of (65):* Let  $x \in K/I$ . By the definition of  $\tilde{\lambda}^0$ , the value  $\tilde{\lambda}^0(x)$  is defined as  $\overline{\lambda^0(w)}$ , where  $w$  is an element of  $K$  satisfying  $\bar{w} = x$ . So let  $w$  be an element of  $K$  satisfying  $\bar{w} = x$  (such a  $w$  clearly exists). Then,  $\tilde{\lambda}^0(x) = \overline{\lambda^0(w)}$ . But  $\lambda^0(w) = 1$  (since every  $t \in K$  satisfies  $\lambda^0(t) = 1$ ). Thus,  $\overline{\lambda^0(w)} = \bar{1} = 1$ , so that  $\tilde{\lambda}^0(x) = \overline{\lambda^0(w)} = 1$ . This proves (65).

<sup>71</sup>*Proof of (66):* Let  $x \in K/I$ . By the definition of  $\tilde{\lambda}^1$ , the value  $\tilde{\lambda}^1(x)$  is defined as  $\overline{\lambda^1(w)}$ , where  $w$  is an element of  $K$  satisfying  $\bar{w} = x$ . So let  $w$  be an element of  $K$  satisfying  $\bar{w} = x$  (such a  $w$  clearly exists). Then,  $\tilde{\lambda}^1(x) = \overline{\lambda^1(w)}$ . But  $\lambda^1(w) = w$  (since every  $t \in K$  satisfies  $\lambda^1(t) = t$ ). Thus,  $\overline{\lambda^1(w)} = \bar{w} = x$ , so that  $\tilde{\lambda}^1(x) = \overline{\lambda^1(w)} = x$ . This proves (66).

<sup>72</sup>*Proof of (67):* Let  $x \in K/I$ ,  $y \in K/I$  and  $k \in \mathbb{N}$ .

Pick any  $u \in K$  satisfying  $\bar{u} = x$ . (Such a  $u$  clearly exists.) Pick any  $v \in K$  satisfying  $\bar{v} = y$ . (Such a  $v$  clearly exists.)

Let  $i \in \{0, 1, \dots, k\}$ .

By the definition of  $\tilde{\lambda}^i$ , the value  $\tilde{\lambda}^i(x)$  is defined as  $\overline{\lambda^i(w)}$ , where  $w$  is an element of  $K$  satisfying  $\bar{w} = x$ . Thus,  $\tilde{\lambda}^i(x) = \overline{\lambda^i(w)}$  for every  $w \in K$  satisfying  $\bar{w} = x$ . Applied to  $w = u$ , this yields  $\tilde{\lambda}^i(x) = \overline{\lambda^i(u)}$  (since  $\bar{u} = x$ ).

By the definition of  $\tilde{\lambda}^{k-i}$ , the value  $\tilde{\lambda}^{k-i}(y)$  is defined as  $\overline{\lambda^{k-i}(w)}$ , where  $w$  is an element of  $K$  satisfying  $\bar{w} = y$ . Thus,  $\tilde{\lambda}^{k-i}(y) = \overline{\lambda^{k-i}(w)}$  for every  $w \in K$  satisfying  $\bar{w} = y$ . Applied to  $w = v$ , this yields  $\tilde{\lambda}^{k-i}(y) = \overline{\lambda^{k-i}(v)}$  (since  $\bar{v} = y$ ).

Now forget that we fixed  $i \in \{0, 1, \dots, k\}$ . We thus have shown that every  $i \in \{0, 1, \dots, k\}$  satisfies  $\tilde{\lambda}^i(x) = \overline{\lambda^i(u)}$  and  $\tilde{\lambda}^{k-i}(y) = \overline{\lambda^{k-i}(v)}$ . Thus,

$$\sum_{i=0}^k \underbrace{\tilde{\lambda}^i(x)}_{=\overline{\lambda^i(u)}} \underbrace{\tilde{\lambda}^{k-i}(y)}_{=\overline{\lambda^{k-i}(v)}} = \sum_{i=0}^k \overline{\lambda^i(u) \lambda^{k-i}(v)} = \overline{\sum_{i=0}^k \lambda^i(u) \lambda^{k-i}(v)}.$$

By the definition of  $\tilde{\lambda}^k$ , the value  $\tilde{\lambda}^k(x+y)$  is defined as  $\overline{\lambda^k(w)}$ , where  $w$  is an element of  $K$  satisfying  $\bar{w} = x+y$ . Thus,  $\tilde{\lambda}^k(x+y) = \overline{\lambda^k(w)}$  for every  $w \in K$  satisfying  $\bar{w} = x+y$ . Applied to  $w = u+v$ , this yields  $\tilde{\lambda}^k(x+y) = \overline{\lambda^k(u+v)}$  (since  $\overline{u+v} = \underbrace{\bar{u}}_{=x} + \underbrace{\bar{v}}_{=y} = x+y$ ). Thus,

$$\begin{aligned} \tilde{\lambda}^k(x+y) &= \overline{\lambda^k(u+v)} = \overline{\sum_{i=0}^k \lambda^i(u) \lambda^{k-i}(v)} \\ &\left( \text{since (5) (applied to } u \text{ and } v \text{ instead of } x \text{ and } y \text{) yields} \right. \\ &\quad \left. \lambda^k(u+v) = \sum_{i=0}^k \lambda^i(u) \lambda^{k-i}(v) \right) \\ &= \sum_{i=0}^k \tilde{\lambda}^i(x) \tilde{\lambda}^{k-i}(y). \end{aligned}$$

This proves (67).

it satisfies the relations (65), (66) and (67), we thus conclude that  $\left(K/I, \left(\tilde{\lambda}^i\right)_{i \in \mathbb{N}}\right)$  is a  $\lambda$ -ring. Theorem 2.2 (b) is proven.

(c) Let  $\pi$  be the canonical projection  $K \rightarrow K/I$ .

The definition of a  $\lambda$ -ring homomorphism tells us: The map  $\pi$  is a  $\lambda$ -ring homomorphism if and only if  $\pi$  is a ring homomorphism and satisfies  $\tilde{\lambda}^i \circ \pi = \pi \circ \lambda^i$  for every  $i \in \mathbb{N}$ . But since  $\pi$  is a ring homomorphism (because it is a canonical projection of a ring onto a factor ring) and satisfies  $\tilde{\lambda}^i \circ \pi = \pi \circ \lambda^i$  for every  $i \in \mathbb{N}$ <sup>73</sup>, this yields that  $\pi$  is a  $\lambda$ -ring homomorphism. Since  $\pi$  is the canonical projection  $K \rightarrow K/I$ , we thus have proven that the canonical projection  $K \rightarrow K/I$  is a  $\lambda$ -ring homomorphism. Theorem 2.2 (c) is proven.  $\square$

*Exercise 2.4: Solution:*

*Proof of Theorem 2.3.* Let  $t \in \text{Ker } f$ , and let  $i$  be a positive integer. Since  $t \in \text{Ker } f$ , we have  $f(t) = 0$ , thus  $\mu^i(f(t)) = \mu^i(0) = 0$  (by Theorem 2.1 (d)).

Since  $f$  is a  $\lambda$ -ring homomorphism, we have  $\mu^i \circ f = f \circ \lambda^i$ , so that  $(\mu^i \circ f)(t) = (f \circ \lambda^i)(t) = f(\lambda^i(t))$ . Thus,  $f(\lambda^i(t)) = (\mu^i \circ f)(t) = \mu^i(f(t)) = 0$ , so that  $\lambda^i(t) \in \text{Ker } f$ .

Now forget that we fixed  $t$  and  $i$ . We have thus proven that every  $t \in \text{Ker } f$  and every positive integer  $i$  satisfy  $\lambda^i(t) \in \text{Ker } f$ .

But the definition of a  $\lambda$ -ideal tells us that  $\text{Ker } f$  is a  $\lambda$ -ideal if and only if every  $t \in \text{Ker } f$  and every positive integer  $i$  satisfy  $\lambda^i(t) \in \text{Ker } f$ . Since we know that every  $t \in \text{Ker } f$  and every positive integer  $i$  satisfy  $\lambda^i(t) \in \text{Ker } f$ , we thus conclude that  $\text{Ker } f$  is a  $\lambda$ -ideal. Theorem 2.3 is proven.  $\square$

### 11.3. To Section 3

*Exercise 3.1: Solution:*

*First solution:* The localization  $\{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  is the subring  $\left\{ \frac{u}{p^i} \mid u \in \mathbb{Z}, i \in \mathbb{N} \right\}$  of  $\mathbb{Q}$ . Let  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$ . We then must show that  $\binom{x}{n} \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  for every  $n \in \mathbb{N}$ .

Since  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z} = \left\{ \frac{u}{p^i} \mid u \in \mathbb{Z}, i \in \mathbb{N} \right\}$ , we can write  $x$  in the form  $\frac{u}{p^i}$

<sup>73</sup>*Proof.* Let  $i \in \mathbb{N}$ . Let  $z \in K$ . Then,  $\pi(z) = \bar{z}$  (because  $\pi$  is the canonical projection  $K \rightarrow K/I$ ) and  $\pi(\lambda^i(z)) = \overline{\lambda^i(z)}$  (for the same reason).

By the definition of  $\tilde{\lambda}^i$ , the value  $\tilde{\lambda}^i(\bar{z})$  is defined as  $\overline{\lambda^i(w)}$ , where  $w$  is an element of  $K$  satisfying  $\bar{w} = \bar{z}$ . Thus,  $\tilde{\lambda}^i(\bar{z}) = \overline{\lambda^i(w)}$  for every  $w \in K$  satisfying  $\bar{w} = \bar{z}$ . Applied to  $w = z$ , this yields  $\tilde{\lambda}^i(\bar{z}) = \overline{\lambda^i(z)}$  (since  $\bar{z} = \bar{z}$ ).

Now,  $(\tilde{\lambda}^i \circ \pi)(z) = \tilde{\lambda}^i\left(\underbrace{\pi(z)}_{=\bar{z}}\right) = \tilde{\lambda}^i(\bar{z}) = \overline{\lambda^i(z)} = \pi(\lambda^i(z)) = (\pi \circ \lambda^i)(z)$ .

Now forget that we fixed  $z$ . We thus have proven that  $(\tilde{\lambda}^i \circ \pi)(z) = (\pi \circ \lambda^i)(z)$  for every  $z \in K$ . In other words,  $\tilde{\lambda}^i \circ \pi = \pi \circ \lambda^i$ , qed.



for some  $u \in \mathbb{Z}$  and  $i \in \mathbb{N}$ . Thus,

$$\begin{aligned} \binom{x}{n} &= \frac{x(x-1)\dots(x-n+1)}{n!} = \frac{\prod_{k=0}^{n-1} (x-k)}{n!} = \frac{\prod_{k=0}^{n-1} \left(\frac{u}{p^i} - k\right)}{n!} && \left(\text{since } x = \frac{u}{p^i}\right) \\ &= \frac{\prod_{k=0}^{n-1} \frac{u - kp^i}{p^i}}{n!} = \frac{\prod_{k=0}^{n-1} (u - kp^i)}{n! \cdot (p^i)^n}. \end{aligned}$$

Now, let  $p^v$  be the highest power of  $p$  that divides  $n!$ . Then,  $\frac{n!}{p^v}$  is a positive integer not divisible by  $p$ . Denoting  $\frac{n!}{p^v}$  by  $r$ , we thus have shown that  $r$  is a positive integer not divisible by  $p$ . Thus,  $p$  is coprime to  $r$  (since  $p$  is prime), so that  $p^{\varphi(r)} \equiv 1 \pmod{r}$  (by Euler's theorem), where  $\varphi$  is Euler's totient function.

Notice that  $r = \frac{n!}{p^v}$  yields  $n! = p^v r$ , so that  $n! \equiv 0 \pmod{r}$ . On the other hand,

$$p^{(\varphi(r)-1)in} \cdot \prod_{k=0}^{n-1} (u - kp^i) = \prod_{k=0}^{n-1} (p^{(\varphi(r)-1)i} (u - kp^i)) = \prod_{k=0}^{n-1} (p^{(\varphi(r)-1)i} u - p^{(\varphi(r)-1)i} kp^i).$$

Since  $p^{(\varphi(r)-1)i} kp^i = p^{(\varphi(r)-1)i+i} k = p^{\varphi(r)i} k = \underbrace{\left(p^{\varphi(r)}\right)}_{\equiv 1 \pmod{r}} k \equiv 1^r k = k \pmod{r}$ , this becomes

$$\begin{aligned} p^{(\varphi(r)-1)in} \cdot \prod_{k=0}^{n-1} (u - kp^i) &\equiv \prod_{k=0}^{n-1} (p^{(\varphi(r)-1)i} u - k) = \underbrace{n!}_{\equiv 0 \pmod{r}} \binom{p^{(\varphi(r)-1)i} u}{n} \\ &\left( \text{since } \frac{\prod_{k=0}^{n-1} (p^{(\varphi(r)-1)i} u - k)}{n!} = \binom{p^{(\varphi(r)-1)i} u}{n} \right) \\ &\equiv 0 \pmod{r}. \end{aligned}$$

Thus,  $\frac{p^{(\varphi(r)-1)in} \cdot \prod_{k=0}^{n-1} (u - kp^i)}{r}$  is an integer. Now,

$$\begin{aligned} \binom{x}{n} &= \frac{\prod_{k=0}^{n-1} (u - kp^i)}{n! \cdot (p^i)^n} = \frac{r}{p^{(\varphi(r)-1)in} \cdot (p^i)^n n!} \cdot \frac{p^{(\varphi(r)-1)in} \cdot \prod_{k=0}^{n-1} (u - kp^i)}{r} \\ &= \frac{r}{\underbrace{p^{(\varphi(r)-1)in} \cdot (p^i)^n p^v r}_{=p^{-v-in-(\varphi(r)-1)in}}} \cdot \underbrace{\frac{p^{(\varphi(r)-1)in} \cdot \prod_{k=0}^{n-1} (u - kp^i)}{r}}_{\text{an integer}} && \left(\text{since } n! = p^v r\right) \end{aligned}$$

is a product of a negative power of  $p$  with an integer, and therefore lies in  $\{1, p, p^2, \dots\}^{-1} \mathbb{Z}$ .

So we have shown that  $\binom{x}{n} \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  for every  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  and every  $n \in \mathbb{N}$ . This proves that  $\{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  is a binomial ring, qed.

*Second solution (sketched):* Let  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$ . Just as in the First solution, we can write  $x$  in the form  $\frac{u}{p^i}$  for some  $u \in \mathbb{Z}$  and  $i \in \mathbb{N}$ , and we see that  $\binom{x}{n} =$

$$\frac{\prod_{k=0}^{n-1} (u - kp^i)}{n! \cdot (p^i)^n}.$$

A careful analysis now shows that every prime  $q$  that is distinct from

$p$  appears in the prime factor decomposition of  $\prod_{k=0}^{n-1} (u - kp^i)$  at least as often as it

appears in that of  $n! \cdot (p^i)^n$ . As a consequence, the ratio  $\frac{\prod_{k=0}^{n-1} (u - kp^i)}{n! \cdot (p^i)^n}$ , once brought

to simplest form, can have no primes distinct from  $p$  in its denominator. Thus, this ratio (which, as we know, is  $\binom{x}{n}$ ) lies in  $\{1, p, p^2, \dots\}^{-1} \mathbb{Z}$ . So we have shown that

$\binom{x}{n} \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  for every  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  and every  $n \in \mathbb{N}$ . This proves that  $\{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  is a binomial ring, qed.

*Third solution:* [Grin-detn, Exercise 3.26] shows that if  $a$  and  $b$  are two integers such that  $b \neq 0$ , and if  $n \in \mathbb{N}$ , then

$$\text{there exists some } N \in \mathbb{N} \text{ such that } b^N \binom{a/b}{n} \in \mathbb{Z}. \quad (68)$$

Let  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$ . We then must show that  $\binom{x}{n} \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  for every  $n \in \mathbb{N}$ .

Fix  $n \in \mathbb{N}$ . We have  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z} = \left\{ \frac{u}{p^i} \mid u \in \mathbb{Z}, i \in \mathbb{N} \right\}$ . Thus,  $x = \frac{u}{p^i}$  for some  $u \in \mathbb{Z}$  and  $i \in \mathbb{N}$ . But (68) (applied to  $a = u$  and  $b = p^i$ ) shows that there exists some  $N \in \mathbb{N}$  such that  $(p^i)^N \binom{u/p^i}{n} \in \mathbb{Z}$ . Consider this  $N$ . We have  $x = \frac{u}{p^i} = \frac{u}{p^i} \cdot (p^i)^N \cdot (p^i)^{-N} = \frac{u}{p^i} \cdot (p^i)^N \cdot \frac{1}{(p^i)^N}$ , so that

$$\begin{aligned} \binom{x}{n} &= \binom{u/p^i}{n} \in \frac{1}{(p^i)^N} \mathbb{Z} && \left( \text{since } (p^i)^N \binom{u/p^i}{n} \in \mathbb{Z} \right) \\ &\subseteq \{1, p, p^2, \dots\}^{-1} \mathbb{Z}. \end{aligned}$$

So we have shown that  $\binom{x}{n} \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  for every  $x \in \{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  and every  $n \in \mathbb{N}$ . This proves that  $\{1, p, p^2, \dots\}^{-1} \mathbb{Z}$  is a binomial ring, qed.

*Exercise 3.2: Hints to solution:* Let  $\mathbb{N}_K^+$  be the subset  $\{1, 2, 3, \dots\}$  of  $K$ . Obviously, this subset is multiplicatively closed and contains no zero-divisors. Hence, the

localization  $(\mathbb{N}_K^+)^{-1}K$  can be considered as an extension ring of  $K$ . We now can define  $\binom{x}{i} \in (\mathbb{N}_K^+)^{-1}K$  for every  $x \in (\mathbb{N}_K^+)^{-1}K$  and  $i \in \mathbb{N}$ . It remains to show that

$\binom{x}{i} \in K$  for every  $x \in K$  and  $i \in \mathbb{N}$ , given that  $\binom{x}{i} \in K$  for every  $x \in E$  and  $i \in \mathbb{N}$ .

This will follow once we show the following three claims:

*Claim 1:* Let  $i \in \mathbb{N}$ . Then, the polynomial  $\binom{X+Y}{i} \in \mathbb{Q}[X, Y]$  is a polynomial in  $\binom{X}{0}, \binom{X}{1}, \dots, \binom{X}{i}, \binom{Y}{0}, \binom{Y}{1}, \dots, \binom{Y}{i}$  with integer coefficients.

*Claim 2:* Let  $i \in \mathbb{N}$ . Then, the polynomial  $\binom{-X}{i} \in \mathbb{Q}[X]$  is a polynomial in  $\binom{X}{0}, \binom{X}{1}, \dots, \binom{X}{i}$  with integer coefficients.

*Claim 3:* Let  $i \in \mathbb{N}$ . Then, the polynomial  $\binom{XY}{i} \in \mathbb{Q}[X, Y]$  is a polynomial in  $\binom{X}{0}, \binom{X}{1}, \dots, \binom{X}{i}, \binom{Y}{0}, \binom{Y}{1}, \dots, \binom{Y}{i}$  with integer coefficients.

*Proof of Claim 1:* In our proof of Theorem 3.1, we have proven the identity (7) for every  $k \in \mathbb{N}$ ,  $x \in \mathbb{Z}$  and  $y \in \mathbb{Z}$ . Renaming  $i$  as  $j$  in this identity, we can rewrite it as

$$\binom{x+y}{k} = \sum_{j=0}^k \binom{x}{j} \binom{y}{k-j}.$$

Applying this to  $k = i$ , we obtain

$$\binom{x+y}{i} = \sum_{j=0}^i \binom{x}{j} \binom{y}{i-j}. \quad (69)$$

Now, in the polynomial ring  $\mathbb{Q}[X, Y]$ , we have the following equality:

$$\binom{X+Y}{i} = \sum_{j=0}^i \binom{X}{j} \binom{Y}{i-j}. \quad (70)$$

(*Proof of (70):* Both sides of the equality (70) are polynomials in  $X$  and  $Y$  with rational coefficients. Hence, in order to prove this equality, we only need to check that it holds whenever it is evaluated at  $X = x$  and  $Y = y$  for two nonnegative integers  $x$  and  $y$ . But the latter follows from (69). Thus, (70) is proven.)

The equality (70) immediately proves Claim 2.

*Proof of Claim 2:* We have the identity  $\binom{-X}{i} = (-1)^i \binom{X+i-1}{i}$  (this is the so-called *upper negation identity*). Thus,

$$\begin{aligned} \binom{-X}{i} &= (-1)^i \underbrace{\binom{X+i-1}{i}}_{=\sum_{j=0}^i \binom{X}{j} \binom{i-1}{i-j}} = (-1)^i \sum_{j=0}^i \binom{X}{j} \binom{i-1}{i-j}. \\ &\quad \text{(by (70), with } i-1 \text{ substituted for } Y) \end{aligned}$$

This proves Claim 2.

Claim 3 is noticeably harder than each of Claims 1 and Claim 2. One way to prove Claim 3 is to use the proof of Theorem 7.1 below. For a completely elementary (combinatorial) proof of Claim 3 (leading to a different polynomial!!), see [Grin-detrn, Exercise 3.8]. Let me finally sketch a third proof of Claim 3:

*Proof of Claim 3:* Recall the fact ([Harts77, Proposition I.7.3]) that the subset

$$\{p \in \mathbb{Q}[X] \mid p(n) \in \mathbb{Z} \text{ for every } n \in \mathbb{Z}\}$$

of the polynomial ring  $\mathbb{Q}[X]$  is the  $\mathbb{Z}$ -linear span of the polynomials  $\binom{X}{0}$ ,  $\binom{X}{1}$ ,  $\binom{X}{2}$ , .... This generalizes to two variables: The subset

$$\{p \in \mathbb{Q}[X, Y] \mid p(n, m) \in \mathbb{Z} \text{ for every } n \in \mathbb{Z} \text{ and every } m \in \mathbb{Z}\}$$

of the polynomial ring  $\mathbb{Q}[X, Y]$  is the  $\mathbb{Z}$ -linear span of the polynomials  $\binom{X}{i} \binom{Y}{j}$  for  $i \in \mathbb{N}$  and  $j \in \mathbb{N}$ . Of course, the polynomial  $\binom{XY}{i}$  belongs to this subset, so we conclude that it belongs to this  $\mathbb{Z}$ -linear span. This proves Claim 3 again.

Now, all three Claims 1, 2 and 3 are proven. Using these claims, we can see (by induction) that the values

$$\binom{x}{i} \quad \text{for } x \in K \text{ and } i \in \mathbb{N}$$

can be written as polynomials (with integer coefficients) in the values

$$\binom{x}{i} \quad \text{for } x \in E \text{ and } i \in \mathbb{N}.$$

Since we have assumed that the latter values belong to  $K$ , we can therefore conclude that the former values also belong to  $K$ . This solves the exercise.

*Exercise 3.3: Hints to solution:* (a) Use Theorem 2.1 (a) and  $(1 + pT)^x (1 + pT)^y = (1 + pT)^{x+y}$ .

(b) Use the binomial formula.

*Detailed solution:* (a) Define a map  $\lambda_T : K \rightarrow K[[T]]$  by

$$\left( \lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \quad \text{for every } x \in K \right).$$

Then,

$$\lambda_T(x) = (1 + pT)^x \quad \text{for every } x \in K \quad (71)$$

<sup>74</sup>. Thus, we can easily see that every  $x \in K$  satisfies  $\lambda_T(x) \equiv 1 + xT \pmod{T^2 K[[T]]}$

<sup>74</sup>*Proof of (71):* Fix  $x \in K$ . Then,  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$ . Hence, for every  $i \in \mathbb{N}$ , we have

$$\begin{aligned} & \text{(the coefficient of } T^i \text{ in the power series } \lambda_T(x)) \\ &= \lambda^i(x) = \text{(the coefficient of the power series } (1 + pT)^x \text{ before } T^i) \\ & \quad \text{(by the definition of } \lambda^i(x)) \\ &= \text{(the coefficient of } T^i \text{ in the power series } (1 + pT)^x). \end{aligned}$$

In other words,  $\lambda_T(x) = (1 + pT)^x$ . This proves (71).

<sup>75</sup>. Hence, we have  $\lambda^0(x) = 1$  and  $\lambda^1(x) = x$  for every  $x \in K$  <sup>76</sup>.

On the other hand, the equality (7) holds for every  $k \in \mathbb{N}$ ,  $x \in K$  and  $y \in K$  <sup>77</sup>. In other words, every  $k \in \mathbb{N}$ ,  $x \in K$  and  $y \in K$  satisfy

$$\binom{x+y}{k} = \sum_{i=0}^k \binom{x}{i} \binom{y}{k-i}. \quad (72)$$

---

<sup>75</sup>*Proof.* Fix  $x \in K$ . Recall that the power series  $p$  has coefficient 1 before  $T^0$ . Thus,  $p \equiv 1 \pmod{TK[[T]]}$ , so that  $p-1 \in TK[[T]]$ . Hence,  $pT - T = T \underbrace{(p-1)}_{\in TK[[T]]} \in TTK[[T]] = T^2K[[T]]$ . In

other words,  $pT \equiv T \pmod{T^2K[[T]]}$ .

Now, (71) yields

$$\begin{aligned} \lambda_T(x) &= (1+pT)^x = \sum_{k \in \mathbb{N}} \binom{x}{k} (pT)^k \\ &= \underbrace{\binom{x}{0}}_{=1} \underbrace{(pT)^0}_{=1} + \underbrace{\binom{x}{1}}_{=x} \underbrace{(pT)^1}_{=pT} + \sum_{\substack{k \in \mathbb{N}; \\ k \geq 2}} \binom{x}{k} \underbrace{(pT)^k}_{=p^k T^k = p^k T^{k-2} T^2} \\ &= 1 + x \underbrace{pT}_{\equiv T \pmod{T^2K[[T]]}} + \sum_{\substack{k \in \mathbb{N}; \\ k \geq 2}} \binom{x}{k} p^k T^{k-2} \underbrace{T^2}_{\equiv 0 \pmod{T^2K[[T]]}} \\ &\equiv 1 + xT + \underbrace{\sum_{\substack{k \in \mathbb{N}; \\ k \geq 2}} \binom{x}{k} p^k T^{k-2} 0}_{=0} = 1 + xT \pmod{T^2K[[T]]}, \end{aligned}$$

qed.

<sup>76</sup>*Proof.* Let  $x \in K$ . Then,  $\lambda_T(x) \equiv 1 + xT \pmod{T^2K[[T]]}$ . In other words,

$$(\text{the coefficient of } T^0 \text{ in the power series } \lambda_T(x)) = 1$$

and

$$(\text{the coefficient of } T^1 \text{ in the power series } \lambda_T(x)) = x.$$

But from  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$ , we obtain

$$\lambda^0(x) = (\text{the coefficient of } T^0 \text{ in the power series } \lambda_T(x)) = 1$$

and

$$\lambda^1(x) = (\text{the coefficient of } T^1 \text{ in the power series } \lambda_T(x)) = x.$$

Qed.

<sup>77</sup>This was proven during our proof of Theorem 3.2.

Now, every  $x \in K$  and  $y \in K$  satisfy

$$\begin{aligned}
& \underbrace{(1+T)^x}_{=\sum_{k \in \mathbb{N}} \binom{x}{k} T^k} \quad \underbrace{(1+T)^y}_{=\sum_{k \in \mathbb{N}} \binom{y}{k} T^k} \\
& \text{(by the definition of } (1+T)^x \text{) (by the definition of } (1+T)^y \text{)} \\
& = \left( \sum_{k \in \mathbb{N}} \binom{x}{k} T^k \right) \left( \sum_{k \in \mathbb{N}} \binom{y}{k} T^k \right) \\
& = \sum_{k \in \mathbb{N}} \underbrace{\left( \sum_{i=0}^k \binom{x}{i} \binom{y}{k-i} \right)}_{=\binom{x+y}{k}} T^k \\
& \text{(by the definition of the product of two power series)} \\
& = \sum_{k \in \mathbb{N}} \binom{x+y}{k} T^k = (1+T)^{x+y}
\end{aligned}$$

(since  $(1+T)^{x+y}$  is defined as  $\sum_{k \in \mathbb{N}} \binom{x+y}{k} T^k$ ). We can substitute  $pT$  for  $T$  in this equality; thus, we obtain

$$(1+pT)^x (1+pT)^y = (1+pT)^{x+y}$$

for every  $x \in K$  and  $y \in K$ . Now, if  $x$  and  $y$  are elements of  $K$ , then

$$\begin{aligned}
\underbrace{\lambda_T(x)}_{=\binom{x}{k} T^k} \cdot \underbrace{\lambda_T(y)}_{=\binom{y}{k} T^k} &= (1+pT)^x (1+pT)^y = (1+pT)^{x+y}. \\
\text{(by (71))} \quad \text{(by (71), applied to } y \text{ instead of } x \text{)}
\end{aligned}$$

Comparing this with

$$\lambda_T(x+y) = (1+pT)^{x+y} \quad \text{(by (71), applied to } x+y \text{ instead of } x \text{),}$$

we obtain

$$\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x+y) \quad \text{for every } x \in K \text{ and } y \in K. \quad (73)$$

But Theorem 2.1 (a) shows that (73) holds if and only if  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. Thus,  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring (since (73) holds). This solves Exercise 3.3 (a).

(b) Assume that  $p = 1$ . Define a map  $\lambda_T : K \rightarrow K[[T]]$  as in our solution to Exercise 3.3 (a). Then,

$$\lambda_T(x) = (1+pT)^x \quad \text{for every } x \in K.$$

(This is the identity (71), and has already been proven above.) Now,

$$\lambda^i(x) = \binom{x}{i} \quad \text{for every } x \in K \text{ and } i \in \mathbb{N} \quad (74)$$

<sup>78</sup>. Thus, the maps  $\lambda^i$  defined in Exercise 3.3 (a) are identical with the maps  $\lambda^i$  defined in Theorem 3.2. Hence, the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  defined in Exercise 3.3 (a) is identical with the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  defined in Theorem 3.2. This solves Exercise 3.3 (b).

*Exercise 3.4: Hints to solution:* It is clear from the very definition of  $\lambda^i$  that Theorem 2.1 (a) is to be applied here.

*Exercise 3.5: Hints to solution:* Same idea as for Exercise 3.4.

## 11.4. To Section 4

*Exercise 4.2: Detailed solution:* There are several ways to solve Exercise 4.2 (many people would call it trivial). Here is not the simplest one, but the easiest-to-formalize one:

(a) Let us prove that every  $n \in \{0, 1, \dots, m\}$  satisfies

$$\prod_{i=1}^n (1 + \alpha_i) = \sum_{S \subseteq \{1, 2, \dots, n\}} \prod_{k \in S} \alpha_k. \quad (75)$$

*Proof of (75).* We will prove (75) by induction over  $n$ :

*Induction base:* If  $n = 0$ , then  $\prod_{i=1}^n (1 + \alpha_i) = (\text{empty product}) = 1$  and

$$\begin{aligned} \sum_{S \subseteq \{1, 2, \dots, n\}} \prod_{k \in S} \alpha_k &= \sum_{S \subseteq \{1, 2, \dots, 0\}} \prod_{k \in S} \alpha_k = \prod_{k \in \emptyset} \alpha_k \\ &\quad (\text{since the only subset } S \text{ of } \{1, 2, \dots, 0\} \text{ is } \emptyset) \\ &= (\text{empty product}) = 1. \end{aligned}$$

Thus,  $\prod_{i=1}^n (1 + \alpha_i) = \sum_{S \subseteq \{1, 2, \dots, n\}} \prod_{k \in S} \alpha_k$  holds for  $n = 0$ . In other words, we have proven

(75) for  $n = 0$ . This completes the induction base.

*Induction step:* Let  $N \in \{0, 1, \dots, m-1\}$ . Assume that (75) holds for  $n = N$ . Now let us prove (75) for  $n = N + 1$ .

Since (75) holds for  $n = N$ , we have

$$\prod_{i=1}^N (1 + \alpha_i) = \sum_{S \subseteq \{1, 2, \dots, N\}} \prod_{k \in S} \alpha_k.$$

---

<sup>78</sup>*Proof of (74):* Let  $x \in K$ . Comparing the identity  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$  with  $\lambda_T(x) = \left(1 + \underbrace{p}_{=1} T\right)^x = (1+T)^x$ , we obtain  $\sum_{i \in \mathbb{N}} \lambda^i(x) T^i = (1+pT)^x$ . Hence, for every  $i \in \mathbb{N}$ , we have

$$\begin{aligned} \lambda^i(x) &= (\text{the coefficient of the power series } (1+T)^x \text{ before } T^i) \\ &= \binom{x}{i} \quad \left( \text{since } (1+T)^x = \sum_{k \in \mathbb{N}} \binom{x}{k} T^k \right). \end{aligned}$$

This proves (74).

Now, let  $P$  be the set of all subsets of  $\{1, 2, \dots, N\}$ . Then,  $P$  is the set of all subsets  $S$  of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \notin S$  (because subsets  $S$  of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \notin S$  are the same thing as subsets of  $\{1, 2, \dots, N\}$ ). Therefore, summing over all  $S \in P$  is the same as summing over all subsets  $S$  of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \notin S$ . Hence, 
$$\sum_{S \in P} \prod_{k \in S} \alpha_k = \sum_{\substack{S \subseteq \{1, 2, \dots, N+1\}; \\ N+1 \notin S}} \prod_{k \in S} \alpha_k.$$

On the other hand, summing over all  $S \in P$  is the same as summing over all subsets  $S$  of  $\{1, 2, \dots, N\}$  (since  $P$  is the set of all subsets of  $\{1, 2, \dots, N\}$ ). Thus, 
$$\sum_{S \in P} \prod_{k \in S} \alpha_k = \sum_{S \subseteq \{1, 2, \dots, N\}} \prod_{k \in S} \alpha_k.$$

Notice that every  $S \in P$  is a subset of  $\{1, 2, \dots, N\}$  (since  $P$  is the set of all subsets of  $\{1, 2, \dots, N\}$ ) and thus satisfies  $N + 1 \notin S$ .

Now, let  $Q$  be the set of all subsets  $T$  of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \in T$ . Then, summing over all  $T \in Q$  is the same as summing over all subsets  $T$  of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \in T$ . Thus, 
$$\sum_{T \in Q} \prod_{k \in T} \alpha_k = \sum_{\substack{T \subseteq \{1, 2, \dots, N+1\}; \\ N+1 \in T}} \prod_{k \in T} \alpha_k.$$
 Renaming the index  $T$

as  $S$  in both sides of this equation, we obtain 
$$\sum_{S \in Q} \prod_{k \in S} \alpha_k = \sum_{\substack{S \subseteq \{1, 2, \dots, N+1\}; \\ N+1 \in S}} \prod_{k \in S} \alpha_k.$$

From the definitions of  $P$  and  $Q$ , it easily follows that every  $S \in P$  satisfies  $S \cup \{N + 1\} \in Q$ <sup>79</sup>. Hence, we can define a map  $\iota : P \rightarrow Q$  by

$$(\iota(S) = S \cup \{N + 1\} \quad \text{for any } S \in P).$$

This map  $\iota$  is injective (because if two sets  $S \in P$  and  $S' \in P$  satisfy  $\iota(S) = \iota(S')$ , then  $S = S'$ <sup>80</sup>) and surjective (because every  $T \in Q$  satisfies  $T = \iota(S)$  for some  $S \in P$ <sup>81</sup>). Thus,  $\iota$  is a bijective map. Hence, we can substitute  $S$  for  $\iota(S)$  in the

<sup>79</sup>*Proof.* Let  $S \in P$ . Then,  $S$  is a subset of  $\{1, 2, \dots, N\}$  (since  $P$  is the set of all subsets of  $\{1, 2, \dots, N\}$ ).

Thus,  $S \cup \{N + 1\}$  is a subset of  $\{1, 2, \dots, N + 1\}$ . Clearly,  $N + 1 \in S \cup \{N + 1\}$ . Thus,  $S \cup \{N + 1\}$  is a subset of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \in S \cup \{N + 1\}$ . In other words,  $S \cup \{N + 1\} \in Q$  (since  $Q$  is the set of all subsets  $T$  of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \in T$ ), qed.

<sup>80</sup>*Proof.* Let  $S \in P$  and  $S' \in P$  be two sets satisfying  $\iota(S) = \iota(S')$ .

The set  $S$  is a subset of  $\{1, 2, \dots, N\}$  (since  $S \in P$  and since  $P$  is the set of all subsets of  $\{1, 2, \dots, N\}$ ). Hence,  $N + 1 \notin S$ . But  $\iota(S) = S \cup \{N + 1\}$ , so that

$$\iota(S) \setminus \{N + 1\} = (S \cup \{N + 1\}) \setminus \{N + 1\} = \underbrace{(S \setminus \{N + 1\})}_{=S \text{ (since } N+1 \notin S)} \cup \underbrace{(\{N + 1\} \setminus \{N + 1\})}_{=\emptyset} = S \cup \emptyset = S.$$

Similarly,  $\iota(S') \setminus \{N + 1\} = S'$ . Hence,  $S = \underbrace{\iota(S) \setminus \{N + 1\}}_{=\iota(S')}$   $= \iota(S') \setminus \{N + 1\} = S'$ , qed.

<sup>81</sup>*Proof.* Let  $T \in Q$ . We want to find an  $S \in P$  such that  $T = \iota(S)$ .

We have  $T \in Q$ . In other words,  $T$  is a subset of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \in T$  (since  $Q$  is the set of all subsets  $T$  of  $\{1, 2, \dots, N + 1\}$  satisfying  $N + 1 \in T$ ).

Let  $S = T \setminus \{N + 1\}$ . Since  $T$  is a subset of  $\{1, 2, \dots, N + 1\}$ , it is clear that  $T \setminus \{N + 1\}$  is a subset of  $\{1, 2, \dots, N + 1\} \setminus \{N + 1\} = \{1, 2, \dots, N\}$ , so that  $T \setminus \{N + 1\} \in P$  (since  $P$  is the set of all subsets of  $\{1, 2, \dots, N\}$ ). Hence,  $S = T \setminus \{N + 1\} \in P$ .

Since  $N + 1 \in T$ , we have  $\{N + 1\} \subseteq T$  and thus  $(T \setminus \{N + 1\}) \cup \{N + 1\} = T$ . Now,  $\iota(S) = S \cup \{N + 1\} = (T \setminus \{N + 1\}) \cup \{N + 1\} = T$ . Hence, we have found an  $S \in P$  such that  $T = \iota(S)$ . Qed.



sum  $\sum_{S \in P} \prod_{k \in \iota(S)} \alpha_k$ , so that  $\sum_{S \in P} \prod_{k \in \iota(S)} \alpha_k = \sum_{S \in Q} \prod_{k \in S} \alpha_k$ . Since every  $S \in P$  satisfies

$$\begin{aligned} \prod_{k \in \iota(S)} \alpha_k &= \prod_{k \in S \cup \{N+1\}} \alpha_k && \text{(since } \iota(S) = S \cup \{N+1\} \text{)} \\ &= \alpha_{N+1} \prod_{k \in S} \alpha_k && \text{(since } S \in P, \text{ so that } N+1 \notin S \text{),} \end{aligned}$$

this rewrites as  $\sum_{S \in P} \left( \alpha_{N+1} \prod_{k \in S} \alpha_k \right) = \sum_{S \in Q} \prod_{k \in S} \alpha_k$ .

Now,

$$\begin{aligned} \sum_{S \subseteq \{1,2,\dots,N+1\}} \prod_{k \in S} \alpha_k &= \underbrace{\sum_{\substack{S \subseteq \{1,2,\dots,N+1\}; \\ N+1 \notin S}} \prod_{k \in S} \alpha_k}_{= \sum_{S \in P} \prod_{k \in S} \alpha_k} + \underbrace{\sum_{\substack{S \subseteq \{1,2,\dots,N+1\}; \\ N+1 \in S}} \prod_{k \in S} \alpha_k}_{= \sum_{S \in Q} \prod_{k \in S} \alpha_k = \sum_{S \in P} \left( \alpha_{N+1} \prod_{k \in S} \alpha_k \right)} \\ &= \sum_{S \in P} \prod_{k \in S} \alpha_k + \sum_{S \in P} \left( \alpha_{N+1} \prod_{k \in S} \alpha_k \right) = \sum_{S \in P} \underbrace{\left( \prod_{k \in S} \alpha_k + \alpha_{N+1} \prod_{k \in S} \alpha_k \right)}_{=(1+\alpha_{N+1}) \prod_{k \in S} \alpha_k} \\ &= \sum_{S \in P} (1 + \alpha_{N+1}) \prod_{k \in S} \alpha_k = (1 + \alpha_{N+1}) \underbrace{\sum_{S \in P} \prod_{k \in S} \alpha_k}_{= \sum_{S \subseteq \{1,2,\dots,N\}} \prod_{k \in S} \alpha_k = \prod_{i=1}^N (1 + \alpha_i)} \\ &= (1 + \alpha_{N+1}) \prod_{i=1}^N (1 + \alpha_i) = \prod_{i=1}^{N+1} (1 + \alpha_i). \end{aligned}$$

We have thus shown that  $\prod_{i=1}^{N+1} (1 + \alpha_i) = \sum_{S \subseteq \{1,2,\dots,N+1\}} \prod_{k \in S} \alpha_k$ . In other words, (75) holds for  $n = N + 1$ . This completes the induction step.

We have thus shown that (75) holds for every  $n \in \{0, 1, \dots, m\}$ . Thus, we can now apply (75) to  $n = m$ , and obtain  $\prod_{i=1}^m (1 + \alpha_i) = \sum_{S \subseteq \{1,2,\dots,m\}} \prod_{k \in S} \alpha_k$ . This solves Exercise

4.2 (a).

(b) Applying Exercise 4.2 (a) to  $\alpha_k t$  instead of  $\alpha_k$ , we obtain

$$\begin{aligned} \prod_{i=1}^m (1 + \alpha_i t) &= \sum_{S \subseteq \{1,2,\dots,m\}} \prod_{k \in S} (\alpha_k t) \\ &= \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k = \left( \prod_{k \in S} \alpha_k \right) t^{|S|} \\ &= \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \left( \prod_{k \in S} \alpha_k \right) \underbrace{t^{|S|}}_{=t^i \text{ (since } |S|=i)} = \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k t^i. \end{aligned}$$

This solves Exercise 4.2 (b).

(c) Applying Exercise 4.2 (b) to  $-\alpha_k$  instead of  $\alpha_k$ , we obtain

$$\begin{aligned} \prod_{i=1}^m (1 + (-\alpha_i)t) &= \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k \underbrace{(-t)^i}_{=(-1)^i t^i} = \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k (-1)^i t^i \\ &= \sum_{i \in \mathbb{N}} (-1)^i \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k t^i. \end{aligned}$$

This simplifies to

$$\prod_{i=1}^m (1 - \alpha_i t) = \sum_{i \in \mathbb{N}} (-1)^i \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k t^i.$$

This proves Exercise 4.2 (c).

(d) Since  $Q$  is a finite set, and we only use the elements of  $Q$  as labels, we can WLOG assume that  $Q = \{1, 2, \dots, m\}$  for some  $m \in \mathbb{N}$  (because otherwise, we can just relabel the elements of  $Q$  as  $1, 2, \dots, m$  for some  $m \in \mathbb{N}$ ). Then,

$$\begin{aligned} \prod_{q \in Q} (1 + \alpha_q t) &= \prod_{i \in Q} (1 + \alpha_i t) && \text{(here we substituted } i \text{ for } q) \\ &= \prod_{i=1}^m (1 + \alpha_i t) && \text{(since } Q = \{1, 2, \dots, m\}) \\ &= \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq \{1, 2, \dots, m\}; \\ |S|=i}} \prod_{k \in S} \alpha_k t^i && \text{(by Exercise 4.2 (b))} \\ &= \sum_{i \in \mathbb{N}} \sum_{\substack{S \subseteq Q; \\ |S|=i}} \prod_{k \in S} \alpha_k t^i && \text{(since } \{1, 2, \dots, m\} = Q) \\ &= \sum_{k \in \mathbb{N}} \sum_{\substack{S \subseteq Q; \\ |S|=k}} \prod_{q \in S} \alpha_q t^k && \text{(here we renamed } i \text{ and } k \text{ as } k \text{ and } q). \end{aligned}$$

This solves Exercise 4.2 (d).

*Exercise 4.3: Detailed solution:* Let  $P \in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  be a polynomial satisfying  $P(p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n) = 0$  (where  $K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  denotes the polynomial ring in the  $m + n$  indeterminates  $\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n$  over  $K$ ). We want to prove that  $P = 0$  (as a polynomial).

Since  $P$  is a polynomial in  $K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$ , we can write it in the form

$$P = \sum_{((i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)) \in \mathbb{N}^m \times \mathbb{N}^n} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot \alpha_1^{i_1} \alpha_2^{i_2} \dots \alpha_m^{i_m} \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n}, \quad (76)$$

where  $\lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)}$  is the coefficient of the polynomial  $P$  before the monomial  $\alpha_1^{i_1} \alpha_2^{i_2} \dots \alpha_m^{i_m} \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n}$  for every  $((i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)) \in \mathbb{N}^m \times \mathbb{N}^n$ . So let us

write it in this way. Then,

$$\begin{aligned}
0 &= P(p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n) \\
&= \sum_{((i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)) \in \mathbb{N}^m \times \mathbb{N}^n} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot p_1^{i_1} p_2^{i_2} \dots p_m^{i_m} \cdot q_1^{j_1} q_2^{j_2} \dots q_n^{j_n} \\
&\quad \text{(because of (76))} \\
&= \sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot p_1^{i_1} p_2^{i_2} \dots p_m^{i_m} \cdot q_1^{j_1} q_2^{j_2} \dots q_n^{j_n}. \quad (77)
\end{aligned}$$

Define a polynomial  $\tilde{P} \in T[\beta_1, \beta_2, \dots, \beta_n]$  by

$$\tilde{P} = \sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot p_1^{i_1} p_2^{i_2} \dots p_m^{i_m} \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n}. \quad (78)$$

Then,

$$\begin{aligned}
&\tilde{P}(q_1, q_2, \dots, q_n) \\
&= \sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot p_1^{i_1} p_2^{i_2} \dots p_m^{i_m} \cdot q_1^{j_1} q_2^{j_2} \dots q_n^{j_n} \\
&= 0 \quad \text{(by (77))}.
\end{aligned}$$

Hence,  $\tilde{P} = 0$  as polynomials (since  $q_1, q_2, \dots, q_n$  are algebraically independent over  $T$ ). Comparing this with (78), we obtain

$$0 = \sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot p_1^{i_1} p_2^{i_2} \dots p_m^{i_m} \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n}. \quad (79)$$

For every  $(j_1, j_2, \dots, j_n) \in \mathbb{N}^n$ , define a polynomial  $P_{(j_1, j_2, \dots, j_n)} \in K[\alpha_1, \alpha_2, \dots, \alpha_m]$  by  $P_{(j_1, j_2, \dots, j_n)} = \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot \alpha_1^{i_1} \alpha_2^{i_2} \dots \alpha_m^{i_m}$ . Then,

$$P_{(j_1, j_2, \dots, j_n)}(p_1, p_2, \dots, p_m) = \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot p_1^{i_1} p_2^{i_2} \dots p_m^{i_m}$$

for every  $(j_1, j_2, \dots, j_n) \in \mathbb{N}^n$ . Thus, in the ring  $T[\beta_1, \beta_2, \dots, \beta_n]$ , we have

$$\begin{aligned}
&\sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} P_{(j_1, j_2, \dots, j_n)}(p_1, p_2, \dots, p_m) \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n} \\
&= \sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} \sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot p_1^{i_1} p_2^{i_2} \dots p_m^{i_m} \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n} = 0
\end{aligned}$$

(by (79)). Since the elements  $\beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n}$  (with  $(j_1, j_2, \dots, j_n) \in \mathbb{N}^n$ ) of the  $T$ -module  $T[\beta_1, \beta_2, \dots, \beta_n]$  are  $T$ -linearly independent (because these elements are the monomials), this yields that  $P_{(j_1, j_2, \dots, j_n)}(p_1, p_2, \dots, p_m) = 0$  for every  $(j_1, j_2, \dots, j_n) \in \mathbb{N}^n$ . Hence,  $P_{(j_1, j_2, \dots, j_n)} = 0$  for every  $(j_1, j_2, \dots, j_n) \in \mathbb{N}^n$  (since  $p_1, p_2, \dots, p_m$  are algebraically

independent over  $K$ ). Now,

$$\begin{aligned}
P &= \sum_{((i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)) \in \mathbb{N}^m \times \mathbb{N}^n} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot \alpha_1^{i_1} \alpha_2^{i_2} \dots \alpha_m^{i_m} \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n} \\
&= \sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} \underbrace{\sum_{(i_1, i_2, \dots, i_m) \in \mathbb{N}^m} \lambda_{(i_1, i_2, \dots, i_m), (j_1, j_2, \dots, j_n)} \cdot \alpha_1^{i_1} \alpha_2^{i_2} \dots \alpha_m^{i_m} \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n}}_{=P_{(j_1, j_2, \dots, j_n)}=0} \\
&= \sum_{(j_1, j_2, \dots, j_n) \in \mathbb{N}^n} 0 \cdot \beta_1^{j_1} \beta_2^{j_2} \dots \beta_n^{j_n} = 0.
\end{aligned}$$

We have thus proven that every polynomial  $P \in K[\alpha_1, \alpha_2, \dots, \alpha_m, \beta_1, \beta_2, \dots, \beta_n]$  satisfying  $P(p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n) = 0$  must satisfy  $P = 0$ . In other words, the  $m + n$  elements  $p_1, p_2, \dots, p_m, q_1, q_2, \dots, q_n$  are algebraically independent over  $K$ . Exercise 4.3 is solved.

*Exercise 4.4: Detailed solution:* Fix some  $j \in \mathbb{N}$ .

*1st Step:* Let  $m \in \mathbb{N}$ . We are going to prove that

$$P_{2,j}(X_1, X_2, \dots, X_{2j}) = \sum_{i=0}^{j-1} (-1)^{i+j-1} X_i X_{2j-i}$$

in the ring  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ .

*Proof.* It is a known (and very easy) fact that whenever  $A$  is a ring,  $F$  is a finite set and  $a_I$  is an element of  $A$  for every  $I \in F$ , then

$$\left( \sum_{I \in F} a_I \right)^2 = \sum_{I \in F} a_I^2 + 2 \sum_{S \in \mathcal{P}_2(F)} \prod_{I \in S} a_I. \quad (80)$$

<sup>82</sup> Applied to  $A = \mathbb{Z}[U_1, U_2, \dots, U_m]$ ,  $F = \mathcal{P}_j(\{1, 2, \dots, m\})$  and  $a_I = \prod_{i \in I} U_i$ , this yields

$$\left( \sum_{I \in \mathcal{P}_j(\{1, 2, \dots, m\})} \prod_{i \in I} U_i \right)^2 = \sum_{I \in \mathcal{P}_j(\{1, 2, \dots, m\})} \left( \prod_{i \in I} U_i \right)^2 + 2 \sum_{S \in \mathcal{P}_2(\mathcal{P}_j(\{1, 2, \dots, m\}))} \prod_{I \in S} \prod_{i \in I} U_i.$$

<sup>82</sup> *Proof of (80).* Let  $A$  be a ring, let  $F$  be a finite set, and let  $a_I$  be an element of  $A$  for every  $I \in F$ . We must prove (80).

The set  $F$  is used only for indexing in (80). Hence, we can WLOG assume that  $F = \{1, 2, \dots, n\}$  for some  $n \in \mathbb{N}$ . Assume this, and consider this  $n$ .

Since  $F = \{1, 2, \dots, n\}$ , we have  $\sum_{I \in F} a_I = \sum_{I \in \{1, 2, \dots, n\}} a_I = a_1 + a_2 + \dots + a_n$  and  $\sum_{I \in F} a_I^2 =$

$$\sum_{I \in \{1, 2, \dots, n\}} a_I^2 = a_1^2 + a_2^2 + \dots + a_n^2.$$

On the other hand, let  $L$  be the set of all pairs  $(i, j) \in F \times F$  satisfying  $i < j$ . Then,  $\sum_{(i, j) \in L} a_i a_j =$

$$\sum_{\substack{(i, j) \in F \times F; \\ i < j}} a_i a_j. \text{ From the definition of } L, \text{ it is clear that every } (i, j) \in L \text{ satisfies } i < j.$$

Let  $\mathfrak{S}$  denote the map

$$L \rightarrow \mathcal{P}_2(F), \quad (i, j) \mapsto \{i, j\}.$$

This map is a bijection. (In fact, the elements of  $L$  are pairs  $(i, j) \in F \times F$  satisfying  $i < j$ ; such pairs are clearly in bijection with the 2-element subsets of  $F$ , and this bijection is given by the map  $\mathfrak{S}$ .)

Since

$$\sum_{S \in \mathcal{P}_2(\mathcal{P}_j(\{1,2,\dots,m\}))} \prod_{I \in S} \prod_{i \in I} U_i = \sum_{\substack{S \subseteq \mathcal{P}_j(\{1,2,\dots,m\}); \\ |S|=2}} \prod_{I \in S} \prod_{i \in I} U_i = P_{2,j}(X_1, X_2, \dots, X_{2j})$$

(by (22), applied to  $k = 2$ ),

this becomes

$$\begin{aligned} \left( \sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i \right)^2 &= \sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \underbrace{\left( \prod_{i \in I} U_i \right)^2}_{= \prod_{i \in I} U_i^2} + 2 \underbrace{\sum_{S \in \mathcal{P}_2(\mathcal{P}_j(\{1,2,\dots,m\}))} \prod_{I \in S} \prod_{i \in I} U_i}_{= P_{2,j}(X_1, X_2, \dots, X_{2j})} \\ &= \sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i^2 + 2P_{2,j}(X_1, X_2, \dots, X_{2j}). \end{aligned}$$

Since

$$\begin{aligned} \sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i &= \sum_{\substack{I \subseteq \{1,2,\dots,m\}; \\ |I|=j}} \prod_{i \in I} U_i = \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=j}} \prod_{k \in S} U_k \\ &\quad \text{(here, we renamed the indices } I \text{ and } i \text{ as } S \text{ and } k) \\ &= X_j \left( \text{since } X_j \text{ was defined as } \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=j}} \prod_{k \in S} U_k \right), \end{aligned}$$

this rewrites as

$$X_j^2 = \sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i^2 + 2P_{2,j}(X_1, X_2, \dots, X_{2j}). \quad (81)$$

---

For every  $(i, j) \in L$ , we have

$$\begin{aligned} \prod_{I \in \mathfrak{S}(i,j)} a_I &= \prod_{I \in \{i,j\}} a_I \quad (\text{since } \mathfrak{S}(i,j) = \{i,j\} \text{ by the definition of } \mathfrak{S}) \\ &= a_i a_j \quad (\text{since } (i,j) \in L, \text{ so that } i < j). \end{aligned}$$

Now,

$$\sum_{\substack{(i,j) \in F \times F; \\ i < j}} a_i a_j = \sum_{(i,j) \in L} \underbrace{a_i a_j}_{\prod_{I \in \mathfrak{S}(i,j)} a_I} = \sum_{(i,j) \in L} \prod_{I \in \mathfrak{S}(i,j)} a_I = \sum_{S \in \mathcal{P}_2(F)} \prod_{I \in S} a_I$$

(here we substituted  $S$  for  $\mathfrak{S}(i,j)$  in the sum, since  $\mathfrak{S}$  is a bijection). But  $\sum_{I \in F} a_I = a_1 + a_2 + \dots + a_n$ , so that

$$\begin{aligned} \left( \sum_{I \in F} a_I \right)^2 &= (a_1 + a_2 + \dots + a_n)^2 = \underbrace{(a_1^2 + a_2^2 + \dots + a_n^2)}_{= \sum_{I \in F} a_I^2} + 2 \underbrace{\sum_{\substack{(i,j) \in F \times F; \\ i < j}} a_i a_j}_{= \sum_{S \in \mathcal{P}_2(F)} \prod_{I \in S} a_I} = \sum_{I \in F} a_I^2 + 2 \sum_{S \in \mathcal{P}_2(F)} \prod_{I \in S} a_I. \end{aligned}$$

This proves (80).

We will now show that

$$\sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i^2 = \sum_{i=0}^{2j} (-1)^{i+j} X_i X_{2j-i} \quad (82)$$

(an identity interesting for its own).

In fact, consider the polynomial  $\prod_{i=1}^m (1 - U_i^2 T^2) \in (\mathbb{Z}[U_1, U_2, \dots, U_m])[T]$ . Exercise 4.2 (c) (applied to  $A = (\mathbb{Z}[U_1, U_2, \dots, U_m])[T]$ ,  $t = T^2$  and  $\alpha_i = U_i^2$ ) yields

$$\prod_{i=1}^m (1 - U_i^2 T^2) = \sum_{i \in \mathbb{N}} (-1)^i \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k^2 \underbrace{(T^2)^i}_{=T^{2i}} = \sum_{i \in \mathbb{N}} \left( (-1)^i \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k^2 \right) T^{2i}.$$

Thus,

$$\begin{aligned} & \left( \text{the coefficient of the polynomial } \prod_{i=1}^m (1 - U_i^2 T^2) \text{ before } T^{2j} \right) \\ &= \left( \text{the coefficient of the polynomial } \sum_{i \in \mathbb{N}} \left( (-1)^i \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k^2 \right) T^{2i} \text{ before } T^{2j} \right) \\ &= (-1)^j \sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=j}} \prod_{k \in S} U_k^2 = (-1)^j \sum_{S \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{k \in S} U_k^2 = (-1)^j \sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i^2 \\ &= \sum_{S \in \mathcal{P}_j(\{1,2,\dots,m\})} \end{aligned} \quad (83)$$

(here, we renamed the indices  $S$  and  $k$  as  $I$  and  $i$ ).

But Exercise 4.2 (c) (applied to  $A = (\mathbb{Z}[U_1, U_2, \dots, U_m])[T]$ ,  $t = T$  and  $\alpha_i = U_i$ ) yields

$$\prod_{i=1}^m (1 - U_i T) = \sum_{i \in \mathbb{N}} (-1)^i \underbrace{\sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k T^i}_{=X_i} = \sum_{i \in \mathbb{N}} (-1)^i X_i T^i.$$

Also, Exercise 4.2 (b) (applied to  $A = (\mathbb{Z}[U_1, U_2, \dots, U_m])[T]$ ,  $t = T$  and  $\alpha_i = U_i$ ) yields

$$\prod_{i=1}^m (1 + U_i T) = \sum_{i \in \mathbb{N}} \underbrace{\sum_{\substack{S \subseteq \{1,2,\dots,m\}; \\ |S|=i}} \prod_{k \in S} U_k T^i}_{=X_i} = \sum_{i \in \mathbb{N}} X_i T^i.$$

Now,

$$\begin{aligned}
\prod_{i=1}^m \underbrace{(1 - U_i^2 T^2)}_{=(1-U_i T)(1+U_i T)} &= \prod_{i=1}^m ((1 - U_i T)(1 + U_i T)) = \underbrace{\left( \prod_{i=1}^m (1 - U_i T) \right)}_{=\sum_{i \in \mathbb{N}} (-1)^i X_i T^i} \underbrace{\left( \prod_{i=1}^m (1 + U_i T) \right)}_{=\sum_{i \in \mathbb{N}} X_i T^i} \\
&= \left( \sum_{i \in \mathbb{N}} (-1)^i X_i T^i \right) \cdot \left( \sum_{i \in \mathbb{N}} X_i T^i \right) = \sum_{i \in \mathbb{N}} \left( \sum_{k=0}^i (-1)^k X_k X_{i-k} \right) T^i \\
&\quad \text{(by the definition of the product of two polynomials).}
\end{aligned}$$

Hence,

$$\begin{aligned}
&\left( \text{the coefficient of the polynomial } \prod_{i=1}^m (1 - U_i^2 T^2) \text{ before } T^{2j} \right) \\
&= \left( \text{the coefficient of the polynomial } \sum_{i \in \mathbb{N}} \left( \sum_{k=0}^i (-1)^k X_k X_{i-k} \right) T^i \text{ before } T^{2j} \right) \\
&= \sum_{k=0}^{2j} (-1)^k X_k X_{2j-k} = \sum_{i=0}^{2j} (-1)^i X_i X_{2j-i}
\end{aligned}$$

(here we renamed the index  $k$  as  $i$ ). Compared to (83), this yields

$$(-1)^j \sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i^2 = \sum_{i=0}^{2j} (-1)^i X_i X_{2j-i}.$$

Divided by  $(-1)^j$ , this yields

$$\sum_{I \in \mathcal{P}_j(\{1,2,\dots,m\})} \prod_{i \in I} U_i^2 = \sum_{i=0}^{2j} \underbrace{\frac{(-1)^i}{(-1)^j}}_{=(-1)^{i+j}} X_i X_{2j-i} = \sum_{i=0}^{2j} (-1)^{i+j} X_i X_{2j-i}.$$

Thus we have proven (82).

Substituting (82) into (81), we obtain

$$X_j^2 = \sum_{i=0}^{2j} (-1)^{i+j} X_i X_{2j-i} + 2P_{2,j}(X_1, X_2, \dots, X_{2j}).$$

Since

$$\begin{aligned}
\sum_{i=0}^{2j} (-1)^{i+j} X_i X_{2j-i} &= \sum_{i=0}^j (-1)^{i+j} X_i X_{2j-i} + \sum_{i=j+1}^{2j} (-1)^{i+j} X_i X_{2j-i} \\
&= \underbrace{\sum_{i=0}^j (-1)^{i+j} X_i X_{2j-i}}_{=(-1)^{j+j} X_j X_{2j-j} + \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i}} + \sum_{i=0}^{j-1} \underbrace{(-1)^{(2j-i)+j}}_{=(-1)^{2(j-i)+i+j}=(-1)^{i+j}} X_{2j-i} \underbrace{X_{2j-(2j-i)}}_{=X_i} \\
&\quad \text{(here, we substituted } 2j - i \text{ for } i \text{ in the second sum)} \\
&= \underbrace{(-1)^{j+j} X_j X_{2j-j}}_{=(-1)^{2j}=1=X_j X_j=X_j^2} + \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i} + \sum_{i=0}^{j-1} (-1)^{i+j} \underbrace{X_{2j-i} X_i}_{=X_i X_{2j-i}} \\
&= X_j^2 + \underbrace{\sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i} + \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i}}_{=2 \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i}} \\
&= X_j^2 + 2 \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i},
\end{aligned}$$

this becomes

$$X_j^2 = X_j^2 + 2 \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i} + 2P_{2,j}(X_1, X_2, \dots, X_{2j}).$$

Subtracting  $X_j^2$  from this and dividing by 2 (we are allowed to divide by 2 since 2 is not a zero-divisor in  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ ), we obtain

$$0 = \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i} + P_{2,j}(X_1, X_2, \dots, X_{2j}),$$

so that

$$\begin{aligned}
P_{2,j}(X_1, X_2, \dots, X_{2j}) &= - \sum_{i=0}^{j-1} (-1)^{i+j} X_i X_{2j-i} = \sum_{i=0}^{j-1} \underbrace{(-(-1)^{i+j})}_{=(-1)^{i+j-1}} X_i X_{2j-i} \\
&= \sum_{i=0}^{j-1} (-1)^{i+j-1} X_i X_{2j-i}.
\end{aligned}$$

This proves the 1st Step.

*2nd Step:* Let us now prove  $P_{2,j} = \sum_{i=0}^{j-1} (-1)^{i+j-1} \alpha_i \alpha_{2j-i}$  now.

*Proof.* Let  $m = 2j$ . Applying Theorem 4.1 (a) to  $K = \mathbb{Z}$  and  $P = P_{2,j}(X_1, X_2, \dots, X_{2j})$ , we conclude that there exists one and only one polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  such



that  $P_{2,j}(X_1, X_2, \dots, X_{2j}) = Q(X_1, X_2, \dots, X_m)$ . In particular, there exists *at most one* such polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$ . Hence,

$$\left( \begin{array}{l} \text{if } \mathfrak{Q}_1 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m] \text{ and } \mathfrak{Q}_2 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m] \text{ are two polynomials} \\ \text{such that } P_{2,j}(X_1, X_2, \dots, X_{2j}) = \mathfrak{Q}_1(X_1, X_2, \dots, X_m) \text{ and} \\ P_{2,j}(X_1, X_2, \dots, X_{2j}) = \mathfrak{Q}_2(X_1, X_2, \dots, X_m), \text{ then } \mathfrak{Q}_1 = \mathfrak{Q}_2 \end{array} \right). \quad (84)$$

Define a polynomial  $\mathfrak{Q}_1 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  by  $\mathfrak{Q}_1 = P_{2,j}$ , and define a polynomial  $\mathfrak{Q}_2 \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  by  $\mathfrak{Q}_2 = \sum_{i=0}^{j-1} (-1)^{i+j-1} \alpha_i \alpha_{2j-i}$ . We are going to prove that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ .

Since our two polynomials  $\mathfrak{Q}_1$  and  $\mathfrak{Q}_2$  satisfy

$$\mathfrak{Q}_1(X_1, X_2, \dots, X_m) = P_{2,j}(X_1, X_2, \dots, X_{2j}) \quad (\text{since } \mathfrak{Q}_1 = P_{2,j} \text{ and } m = 2j)$$

and

$$\begin{aligned} \mathfrak{Q}_2(X_1, X_2, \dots, X_m) &= \left( \sum_{i=0}^{j-1} (-1)^{i+j-1} \alpha_i \alpha_{2j-i} \right) (X_1, X_2, \dots, X_{2j}) \\ &\quad \left( \text{since } \mathfrak{Q}_2 = \sum_{i=0}^{j-1} (-1)^{i+j-1} \alpha_i \alpha_{2j-i} \text{ and } m = 2j \right) \\ &= \sum_{i=0}^{j-1} (-1)^{i+j-1} X_i X_{2j-i} \\ &= P_{2,j}(X_1, X_2, \dots, X_{2j}) \quad (\text{by the 1st Step}), \end{aligned}$$

we can conclude from (84) that  $\mathfrak{Q}_1 = \mathfrak{Q}_2$ . Hence,  $P_{2,j} = \mathfrak{Q}_1 = \mathfrak{Q}_2 = \sum_{i=0}^{j-1} (-1)^{i+j-1} \alpha_i \alpha_{2j-i}$ .

This solves Exercise 4.4.

## 11.5. To Section 5

*Exercise 5.1: Hints to solution:* This can be proven by induction over  $n$ : The ring  $K[T]/(P)$  is a finite-free extension of  $K$  containing a root of the polynomial  $P$  (namely, the equivalence class  $\bar{T}$  of  $T \in K[T]$  modulo  $(P)$ ). Now, the polynomial  $\frac{P(S)}{S - \bar{T}} \in (K[T]/(P))[S]$  is monic and has degree  $n - 1$ , so by induction there exists a finite-free extension ring  $K_P$  of the ring  $K[T]/(P)$  and  $n - 1$  elements  $p_2, \dots, p_n$  of this extension ring  $K_P$  such that  $\frac{P(S)}{S - \bar{T}} = \prod_{i=2}^n (T - p_i)$  in  $K_P[S]$ . Thus,

$P(S) = (S - \bar{T}) \prod_{i=2}^n (T - p_i)$  in  $K_P[S]$ . If we denote  $\bar{T}$  by  $p_1$ , this takes the form

$P(S) = \prod_{i=1}^n (T - p_i)$ , which shows that we have just completed the induction step.

Notice the similarity between this solution and the proof of the existence of splitting fields in Galois theory.

*Detailed solution:* We first show a lemma:

**Lemma 5.1.S.1.** Let  $K$  be a ring, and  $P \in K[T]$  be a monic polynomial. Then, there exists a finite-free extension ring  $K'$  of the ring  $K$  and an element  $p \in K'$  such that  $P(p) = 0$  in  $K'$ .

*Proof of Lemma 5.1.S.1.* Let  $n = \deg P$ . Let  $K'$  be the quotient ring  $K[T]/(P)$ . For every  $Q \in K[T]$ , let us denote by  $\overline{Q}$  the projection of  $Q$  onto  $K[T]/(P)$  (that is, the residue class of  $Q$  modulo  $(P)$ ).

Since the polynomial  $P$  is monic of degree  $n$ , we can easily see that  $(\overline{T^0}, \overline{T^1}, \dots, \overline{T^{n-1}})$  is a basis of the  $K$ -module  $K'$ . This is because the sequence  $(\overline{T^0}, \overline{T^1}, \dots, \overline{T^{n-1}})$  is linearly independent<sup>83</sup> and generates the  $K$ -module  $K'$ <sup>84</sup>. Thus, the  $K$ -module  $K'$  is finite-free. Also, since  $(\overline{T^0}, \overline{T^1}, \dots, \overline{T^{n-1}})$  is a basis of the  $K$ -module  $K'$ , its

<sup>83</sup>*Proof.* In fact, assume that we have a sequence  $(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in K^n$  such that  $\alpha_0 \overline{T^0} + \alpha_1 \overline{T^1} + \dots + \alpha_{n-1} \overline{T^{n-1}} = 0$ .

Then,  $0 = \alpha_0 \overline{T^0} + \alpha_1 \overline{T^1} + \dots + \alpha_{n-1} \overline{T^{n-1}} = \overline{\alpha_0 T^0 + \alpha_1 T^1 + \dots + \alpha_{n-1} T^{n-1}}$ , so that  $0 \equiv \alpha_0 T^0 + \alpha_1 T^1 + \dots + \alpha_{n-1} T^{n-1} \pmod{(P)}$ . In other words,  $\alpha_0 T^0 + \alpha_1 T^1 + \dots + \alpha_{n-1} T^{n-1} \in (P)$ . In other words,  $P \mid \alpha_0 T^0 + \alpha_1 T^1 + \dots + \alpha_{n-1} T^{n-1}$ . But  $P$  is a monic polynomial of degree  $n$ , and thus every polynomial divisible by  $P$  has either degree  $\geq n$  or is the zero polynomial. Hence, the polynomial  $\alpha_0 T^0 + \alpha_1 T^1 + \dots + \alpha_{n-1} T^{n-1}$  must have either degree  $\geq n$  or be the zero polynomial (since  $P \mid \alpha_0 T^0 + \alpha_1 T^1 + \dots + \alpha_{n-1} T^{n-1}$ ). Since this polynomial does not have degree  $\geq n$ , it must thus be the zero polynomial. This means that all its coefficients are zero. That is,  $\alpha_i = 0$  for every  $i \in \{0, 1, \dots, n-1\}$ .

We have thus proven that whenever a sequence  $(\alpha_0, \alpha_1, \dots, \alpha_{n-1}) \in K^n$  satisfies  $\alpha_0 \overline{T^0} + \alpha_1 \overline{T^1} + \dots + \alpha_{n-1} \overline{T^{n-1}} = 0$ , it must satisfy  $\alpha_i = 0$  for every  $i \in \{0, 1, \dots, n-1\}$ . In other words, the sequence  $(\overline{T^0}, \overline{T^1}, \dots, \overline{T^{n-1}})$  is linearly independent.

<sup>84</sup>*Proof.* Let  $K'_1$  be the  $K$ -submodule of  $K'$  generated by  $(\overline{T^0}, \overline{T^1}, \dots, \overline{T^{n-1}})$ . Then, we will prove that  $K'_1 = K'$ .

From the definition of  $K'_1$ , it follows that  $\overline{T^j} \in K'_1$  for every  $j \in \{0, 1, \dots, n-1\}$ .

Write the polynomial  $P$  in the form  $P = \sum_{i=0}^n \beta_i T^i$  for some  $(\beta_0, \beta_1, \dots, \beta_n) \in K^{n+1}$  (this is possible since  $\deg P = n$ ). Since  $P$  is monic of degree  $n$ , we must then have  $\beta_n = 1$ .

Let us prove that every  $j \in \mathbb{N}$  satisfies  $\overline{T^j} \in K'_1$ .

In fact, we will prove this by strong induction over  $j$ :

*Induction step:* Let  $j \in \mathbb{N}$  be arbitrary. Assume that  $\overline{T^\ell} \in K'_1$  is already proven for every  $\ell \in \mathbb{N}$  satisfying  $\ell < j$ . We must now prove that  $\overline{T^j} \in K'_1$ .

If  $j \in \{0, 1, \dots, n-1\}$ , then we are immediately done with proving  $\overline{T^j} \in K'_1$  (since we already know that  $\overline{T^j} \in K'_1$  for every  $j \in \{0, 1, \dots, n-1\}$ ). Thus, we assume that  $j \in \{0, 1, \dots, n-1\}$  is not the case. Hence,  $j \geq n$ , so that  $j - n \geq 0$ . Now,  $P = \sum_{i=0}^n \beta_i T^i$ , so that

$$P \cdot T^{j-n} = \sum_{i=0}^n \beta_i T^i \cdot T^{j-n} = \sum_{i=0}^n \beta_i T^{i+j-n} = \sum_{i=0}^{n-1} \beta_i T^{i+j-n} + \underbrace{\beta_n}_{=1} \underbrace{T^{n+j-n}}_{=T^j} = \sum_{i=0}^{n-1} \beta_i T^{i+j-n} + T^j.$$

Hence,  $T^j = P \cdot T^{j-n} - \sum_{i=0}^{n-1} \beta_i T^{i+j-n} \equiv - \sum_{i=0}^{n-1} \beta_i T^{i+j-n} \pmod{(P)}$ , so that

$$\overline{T^j} = - \sum_{i=0}^{n-1} \beta_i \overline{T^{i+j-n}} = - \sum_{i=0}^{n-1} \beta_i \overline{T^{i+j-n}}.$$

Every  $i \in \{0, 1, \dots, n-1\}$  satisfies  $\overline{T^{i+j-n}} \in K'_1$  (since  $\overline{T^\ell} \in K'_1$  is already proven for every  $\ell \in \mathbb{N}$

subsequence  $(\overline{T^0}) = (\overline{1})$  is linearly independent. Hence, the canonical map  $K \rightarrow K'$  is injective (because it maps the basis (1) of the  $K$ -module  $K$  to the linearly independent sequence  $(\overline{1})$  of the  $K$ -module  $K'$ ). Hence, we can view  $K'$  as an extension ring of  $K$ .

Let  $p = \overline{T}$ . Then,  $P(p) = P(\overline{T}) = \overline{P(T)} = \overline{P} = 0$  (since  $P \equiv 0 \pmod{(P)}$ ). This proves Lemma 5.1.S.1.  $\square$

Another lemma:

**Lemma 5.1.S.2.** Let  $\mathbf{Z}$  be a ring and  $P \in \mathbf{Z}[T]$  be a polynomial. Let  $p$  be an element of  $\mathbf{Z}$  such that  $P(p) = 0$ .

(a) Then, there exists a polynomial  $Q \in \mathbf{Z}[T]$  of degree  $\leq \deg P - 1$  such that  $P = Q \cdot (T - p)$ .

(b) If the polynomial  $P$  is monic, then this polynomial  $Q$  is a monic polynomial of degree  $N - 1$ , where  $N = \deg P$ .

*Proof of Lemma 5.1.S.2.* (a) Lemma 5.1.S.2 (a) is a known fact from basic algebra. We are not going to prove it.

(b) Assume that the polynomial  $P$  is monic. Consider the polynomial  $Q$  from Lemma 5.1.S.2 (a).

Let  $N = \deg P$ . Since  $Q$  has degree  $\leq \deg P - 1$ , we have  $\deg Q \leq \underbrace{\deg P - 1}_{=N} = N - 1$ . We can thus write the polynomial  $Q$  in the form  $Q = \sum_{i=0}^{N-1} q_i T^i$  for some  $(q_0, q_1, \dots, q_{N-1}) \in \mathbf{Z}^N$ . Writing it this way, we have

$$\begin{aligned} Q \cdot (T - p) &= \sum_{i=0}^{N-1} q_i T^i \cdot (T - p) = \sum_{i=0}^{N-1} q_i \underbrace{T^i T}_{=T^{i+1}} - \sum_{i=0}^{N-1} q_i \underbrace{T^i p}_{=pT^i} = \sum_{i=0}^{N-1} q_i T^{i+1} - \sum_{i=0}^{N-1} q_i p T^i \\ &= \sum_{i=1}^N q_{i-1} T^i - \sum_{i=0}^{N-1} q_i p T^i \quad (\text{here, we substituted } i \text{ for } i + 1 \text{ in the first sum}). \end{aligned}$$

---

satisfying  $\ell < j$ , and since every  $i \in \{0, 1, \dots, n-1\}$  satisfies  $\underbrace{i}_{< n} + j - n < j$ . Thus,

$$\overline{T^j} = - \sum_{i=0}^{n-1} \beta_i \underbrace{\overline{T^{i+j-n}}}_{\in K'_1} \in K'_1 \quad (\text{since } K'_1 \text{ is a } K\text{-module}).$$

This proves that  $\overline{T^j} \in K'_1$ . The induction step is thus complete.

We have thus proven by strong induction that every  $j \in \mathbb{N}$  satisfies  $\overline{T^j} \in K'_1$ .

The  $K$ -module  $K[T]$  is generated by the elements  $T^j$  with  $j \in \mathbb{N}$ . Hence, the  $K$ -module  $K' = K[T]/(P)$  (being a quotient module of  $K[T]$ ) is generated by the elements  $\overline{T^j}$  with  $j \in \mathbb{N}$ . Since all of these generators lie in  $K'_1$  (because every  $j \in \mathbb{N}$  satisfies  $\overline{T^j} \in K'_1$ ), we can conclude that  $K' \subseteq K'_1$ . Combined with  $K'_1 \subseteq K'$  (this is trivial), this yields  $K' = K'_1$ . Since  $K'_1$  is the  $K$ -submodule of  $K'$  generated by  $(\overline{T^0}, \overline{T^1}, \dots, \overline{T^{n-1}})$ , this yields that the  $K$ -module  $K'$  is generated by  $(\overline{T^0}, \overline{T^1}, \dots, \overline{T^{n-1}})$ .

Thus,

$$P = Q \cdot (T - p) = \sum_{i=1}^N q_{i-1}T^i - \sum_{i=0}^{N-1} q_i p T^i.$$

Hence,

$$\begin{aligned} & \text{(the coefficient of the polynomial } P \text{ before } T^N) \\ &= \left( \text{the coefficient of the polynomial } \sum_{i=1}^N q_{i-1}T^i - \sum_{i=0}^{N-1} q_i p T^i \text{ before } T^N \right) \\ &= \left( \underbrace{\text{the coefficient of the polynomial } \sum_{i=1}^N q_{i-1}T^i \text{ before } T^N}_{=q_{N-1}} \right) \\ &\quad - \left( \underbrace{\text{the coefficient of the polynomial } \sum_{i=0}^{N-1} q_i p T^i \text{ before } T^N}_{=0} \right) \\ &= q_{N-1} - 0 = q_{N-1}. \end{aligned}$$

Since (the coefficient of the polynomial  $P$  before  $T^N$ ) = 1 (because  $P$  is a monic polynomial with  $\deg P = N$ ), this rewrites as  $1 = q_{N-1}$ . Since  $\deg q \leq N - 1$ , this yields that  $q$  is a monic polynomial of degree  $N - 1$ . This proves Lemma 5.1.S.2.  $\square$

Now, let us solve Exercise 5.1:

We will prove the assertion of Exercise 5.1 by induction over  $n$ .

*Induction base:* For  $n = 0$ , the assertion of Exercise 5.1 is trivially true (take  $K_P = K$ ). This completes the induction base.

*Induction step:* Let  $N \in \mathbb{N}$  be positive. Assume that the assertion of Exercise 5.1 is true for  $n = N - 1$ . Let us now prove the assertion of Exercise 5.1 for  $n = N$ .

First we recall that we assumed that the assertion of Exercise 5.1 is true for  $n = N - 1$ . Hence,

$$\left( \begin{array}{l} \text{If } K' \text{ is a ring, and if } Q \in K'[T] \text{ is a monic polynomial such that} \\ \text{deg } Q = N - 1, \text{ then there exists a finite-free extension ring } K'_Q \text{ of} \\ \text{the ring } K' \text{ and } N - 1 \text{ elements } p_1, p_2, \dots, p_{N-1} \text{ of this extension} \\ \text{ring } K'_Q \text{ such that } Q = \prod_{i=1}^{N-1} (T - p_i) \text{ in } K'_Q[T] \end{array} \right) \quad (85)$$

(this follows from Exercise 5.1, applied to  $K'$ ,  $Q$  and  $N - 1$  instead of  $K$ ,  $P$  and  $n$  <sup>85</sup>).

Let  $K$  be a ring, and let  $P \in K[T]$  be a monic polynomial such that  $\deg P = N$ . According to Lemma 5.1.S.1, there exists a finite-free extension ring  $K'$  of the ring  $K$  and an element  $p \in K'$  such that  $P(p) = 0$  in  $K'$ . Consider these  $K'$  and  $p$ .

<sup>85</sup>In fact, we are allowed to apply Exercise 5.1 to  $K'$ ,  $Q$  and  $N - 1$  instead of  $K$ ,  $P$  and  $n$ , because we assumed that the assertion of Exercise 5.1 is true for  $n = N - 1$ .

By Lemma 5.1.S.2 **(a)** (applied to  $\mathbf{Z} = K'$ ), there exists a polynomial  $Q \in K'[T]$  of degree  $\leq \deg P - 1$  such that  $P = Q \cdot (T - p)$  (since  $P(p) = 0$ )<sup>86</sup>. Consider this  $Q$ . By Lemma 5.1.S.2 **(b)** (applied to  $\mathbf{Z} = K'$ ), this polynomial  $Q$  is a monic polynomial of degree  $N - 1$ . That is,  $Q$  is monic and  $\deg Q = N - 1$ . According to (85), there therefore exists a finite-free extension ring  $K'_Q$  of the ring  $K'$  and  $N - 1$  elements  $p_1, p_2, \dots, p_{N-1}$  of this extension ring  $K'_Q$  such that  $Q = \prod_{i=1}^{N-1} (T - p_i)$  in  $K'_Q[T]$ . Consider this  $K'_Q$  and these  $p_1, p_2, \dots, p_{N-1}$ .

Since  $K'_Q$  is a finite-free  $K'$ -module, and since  $K'$  is a finite-free  $K$ -module, it is clear that  $K'_Q$  is a finite-free  $K$ -module<sup>87</sup>. Also, since  $K'_Q$  is an extension ring of  $K'$ , and since  $K'$  is an extension ring of  $K$ , it is clear that  $K'_Q$  is an extension ring of  $K$ . Thus,  $K'_Q$  is a finite-free extension ring of  $K$ .

Define  $K_P = K'_Q$  and  $p_N = p$ . Then,  $p_1, p_2, \dots, p_{N-1}, p_N$  are  $N$  elements of the ring  $K'_Q = K_P$ . In  $K_P[T] = K'_Q[T]$ , we have

$$P = \underbrace{Q}_{= \prod_{i=1}^{N-1} (T - p_i)} \cdot \left( T - \underbrace{p}_{= p_N} \right) = \prod_{i=1}^{N-1} (T - p_i) \cdot (T - p_N) = \prod_{i=1}^N (T - p_i).$$

The ring  $K_P$  is a finite-free extension ring of  $K$  (since  $K_P = K'_Q$ , and since we know that  $K'_Q$  is a finite-free extension ring of  $K$ ).

So we have proven that if  $K$  is a ring, and if  $P \in K[T]$  is a monic polynomial such that  $\deg P = N$ , then there exists a finite-free extension ring  $K_P$  of the ring  $K$  and  $N$  elements  $p_1, p_2, \dots, p_N$  of this extension ring  $K_P$  such that  $P = \prod_{i=1}^N (T - p_i)$  in  $K_P[T]$ . In other words, we have proven the assertion of Exercise 5.1 for  $n = N$ . Thus, the induction step is complete, and Exercise 5.1 is solved.

*Exercise 5.2: Hints to solution:* **(a)** The idea is to evaluate the identity  $\sum_{i=0}^n a_{n-i} T^i = \prod_{i=1}^n (p_i + T)$  at  $T = \frac{1}{S}$ , where  $S$  is a new variable. The only nontrivial part of the solution is to make formal sense of this idea (this is what Lemma 5.2.S.1 in the solution below is for). **(b)** is similar.

*Detailed solution:* First we need the following lemma:

<sup>86</sup>Note that  $K'[T]$  denotes the polynomial ring in one indeterminate  $T$  over  $K'$ . This  $T$  here is *not* the  $T$  that was used to construct  $K'$  in the proof of Lemma 5.1.S.1. In order to avoid confusing these two  $T$ 's, you are advised to forget the proof of Lemma 5.1.S.1 (you won't need it any more).

<sup>87</sup>Here we are using the following general fact from algebra: If  $K$  is a ring, if  $A$  is a  $K$ -algebra which is a finite-free  $K$ -module, and if  $B$  is a finite-free  $A$ -module, then  $B$  is a finite-free  $K$ -module.

*Proof of this fact.* Since  $A$  is a finite-free  $K$ -module, we have  $A \cong K^n$  as  $K$ -modules for some  $n \in \mathbb{N}$ . Consider this  $n$ . Since  $B$  is a finite-free  $A$ -module, we have  $B \cong A^m$  as  $A$ -modules for some  $m \in \mathbb{N}$ . Consider this  $m$ . Since  $B \cong A^m$  as  $A$ -modules, we also have

$$\begin{aligned} B &\cong A^m \cong (K^n)^m && \text{(since } A \cong K^n \text{)} \\ &\cong K^{nm} \end{aligned}$$

as  $K$ -modules. Thus,  $B$  is a finite-free  $K$ -module, qed.

**Lemma 5.2.S.1.** Let  $L$  be a ring. Consider the polynomial ring  $L[T]$  as a subring of the polynomial ring  $L[T, S]$ . Let  $P \in L[T]$  be a polynomial such that  $TS - 1 \mid P$  in  $L[T, S]$ . Then,  $P = 0$ .

This is a known and very basic lemma and can be proven, for instance, using the fact that the inclusion  $L[T] \rightarrow L[T, S]$  induces an injective map  $L[T] \rightarrow L[T, S]/(TS - 1)$ . But let us give a slightly different proof of this lemma, in the hope that a clever reader will find a better use for the trick it involves:

*Proof of Lemma 5.2.S.1.* Since  $TS - 1 \mid P$  in  $L[T, S]$ , there exists a polynomial  $Q \in L[T, S]$  such that  $P = (TS - 1) \cdot Q$ . Consider this  $Q$ .

Let  $m$  be the degree of the polynomial  $P \in L[T]$ .

By the universal property of the polynomial ring  $L[T, S]$ , there exists a unique  $L$ -algebra homomorphism  $L[T, S] \rightarrow L[T]$  which maps  $T$  and  $S$  to  $T$  and  $T^m$ , respectively. Denote this homomorphism by  $\varphi$ . Then,  $\varphi$  maps  $T$  and  $S$  to  $T$  and  $T^m$ , respectively, so that  $\varphi(T) = T$  and  $\varphi(S) = T^m$ . Since  $\varphi$  is an  $L$ -algebra homomorphism, we have

$$\varphi((TS - 1) \cdot Q) = \left( \underbrace{\varphi(T)}_{=T} \underbrace{\varphi(S)}_{=T^m} - 1 \right) \cdot \varphi(Q) = (TT^m - 1) \cdot \varphi(Q) = (T^{m+1} - 1) \cdot \varphi(Q).$$

On the other hand,  $\varphi(P) = P$ <sup>88</sup>. Now,

$$P = \varphi \left( \underbrace{P}_{=(TS-1) \cdot Q} \right) = \varphi((TS - 1) \cdot Q) = (T^{m+1} - 1) \cdot \varphi(Q).$$

Hence, the polynomial  $P$  is a multiple of  $T^{m+1} - 1$  in  $L[T]$ . Since  $T^{m+1} - 1$  is a monic polynomial of degree  $m + 1$ , this yields that  $P$  is a multiple of a monic polynomial of degree  $m + 1$ . But it is known that a multiple of a monic polynomial of degree  $m + 1$  must either have degree  $\geq m + 1$  or be the zero polynomial. Hence, the fact that  $P$  is a multiple of a monic polynomial of degree  $m + 1$  yields that  $P$  has either degree  $\geq m + 1$  or is the zero polynomial. Since we know that  $P$  does not have degree  $\geq m + 1$  (because  $\deg P = m < m + 1$ ), this tells us that  $P$  is the zero polynomial. In other words,  $P = 0$ . Lemma 5.2.S.1 is proven.  $\square$

Now let us solve Exercise 5.2. Consider the polynomial ring  $L[T]$  as a subring of the polynomial ring  $L[T, S]$ .

---

<sup>88</sup>*Proof.* Since  $P \in L[T]$  and  $\deg P = m$ , we can write  $P$  in the form  $P = \sum_{i=0}^m \beta_i T^i$  for some  $(\beta_0, \beta_1, \dots, \beta_m) \in L^{m+1}$ . Thus,

$$\begin{aligned} \varphi(P) &= \varphi \left( \sum_{i=0}^m \beta_i T^i \right) = \sum_{i=0}^m \beta_i \left( \underbrace{\varphi(T)}_{=T} \right)^i && \text{(since } \varphi \text{ is an } L\text{-algebra homomorphism)} \\ &= \sum_{i=0}^m \beta_i T^i = P. \end{aligned}$$

(a) Assume that  $\sum_{i=0}^n a_{n-i}T^i = \prod_{i=1}^n (p_i + T)$ . This is a polynomial identity, so we can evaluate it at  $T = S$  and obtain  $\sum_{i=0}^n a_{n-i}S^i = \prod_{i=1}^n (p_i + S)$ . Thus,

$$\begin{aligned} T^n \sum_{i=0}^n a_{n-i}S^i &= \underbrace{T^n}_{=\prod_{i=1}^n T} \prod_{i=1}^n (p_i + S) = \prod_{i=1}^n T \prod_{i=1}^n (p_i + S) = \prod_{i=1}^n \underbrace{(T(p_i + S))}_{=p_iT+TS} \\ &= \prod_{i=1}^n \left( p_iT + \underbrace{TS}_{\equiv 1 \pmod{TS-1}} \right) \equiv \prod_{i=1}^n (p_iT + 1) = \prod_{i=1}^n (1 + p_iT) \pmod{TS - 1}. \end{aligned}$$

Combined with

$$\begin{aligned} T^n \sum_{i=0}^n a_{n-i}S^i &= \sum_{i=0}^n a_{n-i} \underbrace{T^n}_{=T^{n-i}T^i} S^i = \sum_{i=0}^n a_{n-i}T^{n-i} \underbrace{T^i S^i}_{=(TS)^i \equiv 1^i \pmod{TS-1}} \\ &\equiv \sum_{i=0}^n a_{n-i}T^{n-i}1^i = \sum_{i=0}^n a_{n-i}T^{n-i} \\ &= \sum_{i=0}^n a_i T^i \pmod{TS - 1} \quad (\text{here we renamed } n - i \text{ as } i), \end{aligned}$$

this yields  $\sum_{i=0}^n a_i T^i \equiv \prod_{i=1}^n (1 + p_i T) \pmod{TS - 1}$ . In other words,  $TS - 1 \mid \sum_{i=0}^n a_i T^i - \prod_{i=1}^n (1 + p_i T)$ . Thus, Lemma 5.2.S.1 (applied to  $P = \sum_{i=0}^n a_i T^i - \prod_{i=1}^n (1 + p_i T)$ ) yields that  $\sum_{i=0}^n a_i T^i - \prod_{i=1}^n (1 + p_i T) = 0$ . In other words,  $\sum_{i=0}^n a_i T^i = \prod_{i=1}^n (1 + p_i T)$ . This proves Exercise 5.2 (a).

(b) Assume that  $\sum_{i=0}^n a_i T^i = \prod_{i=1}^n (1 + p_i T)$ . This is a polynomial identity, so we can evaluate it at  $T = S$  and obtain  $\sum_{i=0}^n a_i S^i = \prod_{i=1}^n (1 + p_i S)$ . Thus,

$$\begin{aligned} T^n \sum_{i=0}^n a_i S^i &= \underbrace{T^n}_{=\prod_{i=1}^n T} \prod_{i=1}^n (1 + p_i S) = \prod_{i=1}^n T \prod_{i=1}^n (1 + p_i S) = \prod_{i=1}^n \underbrace{(T(1 + p_i S))}_{=T+p_iTS} \\ &= \prod_{i=1}^n \left( T + p_i \underbrace{TS}_{\equiv 1 \pmod{TS-1}} \right) \equiv \prod_{i=1}^n \underbrace{(T + p_i)}_{=p_i+T} = \prod_{i=1}^n (p_i + T) \pmod{TS - 1}. \end{aligned}$$

Combined with

$$\begin{aligned} T^n \sum_{i=0}^n a_i S^i &= \sum_{i=0}^n a_i \underbrace{T^n}_{=T^{n-i}T^i} S^i = \sum_{i=0}^n a_i T^{n-i} \underbrace{T^i S^i}_{=(TS)^i \equiv 1^i \pmod{TS-1}} \equiv \sum_{i=0}^n a_i T^{n-i} 1^i = \sum_{i=0}^n a_i T^{n-i} \\ &= \sum_{i=0}^n a_{n-i} T^i \pmod{TS - 1} \quad (\text{here we renamed } n - i \text{ as } i), \end{aligned}$$

this yields  $\sum_{i=0}^n a_{n-i}T^i \equiv \prod_{i=1}^n (p_i + T) \pmod{(TS - 1)}$ . In other words,  $TS - 1 \mid \sum_{i=0}^n a_{n-i}T^i - \prod_{i=1}^n (p_i + T)$ . Thus, Lemma 5.2.S.1 (applied to  $P = \sum_{i=0}^n a_{n-i}T^i - \prod_{i=1}^n (p_i + T)$ ) yields that  $\sum_{i=0}^n a_{n-i}T^i - \prod_{i=1}^n (p_i + T) = 0$ . In other words,  $\sum_{i=0}^n a_{n-i}T^i = \prod_{i=1}^n (p_i + T)$ . This proves Exercise 5.2 (b).

*Exercise 5.3: Hints to solution:* Exercise 5.3 follows from Exercise 5.1, applied to  $\frac{P}{T - p}$  instead of  $P$ .

*Detailed solution:* By Lemma 5.1.S.2 (a) (applied to  $\mathbf{Z} = K$ ), there exists a polynomial  $Q \in K[T]$  of degree  $\leq \deg P - 1$  such that  $P = Q \cdot (T - p)$ . Consider this  $Q$ . By Lemma 5.1.S.2 (b) (applied to  $\mathbf{Z} = K$ ), this polynomial  $Q$  is a monic polynomial of degree  $N - 1$ , where  $N = \deg P$ . Since  $N = \deg P = n$ , this rewrites as follows: The polynomial  $Q$  is a monic polynomial of degree  $n - 1$ .

Thus, Exercise 5.1 (applied to  $Q$  and  $n - 1$  instead of  $P$  and  $n$ ) yields that there exists a finite-free extension ring  $K_Q$  of the ring  $K$  and  $n - 1$  elements  $p_1, p_2, \dots, p_{n-1}$  of this extension ring  $K_Q$  such that  $Q = \prod_{i=1}^{n-1} (T - p_i)$  in  $K_Q[T]$ . Consider this ring  $K_Q$  and these  $n - 1$  elements  $p_1, p_2, \dots, p_{n-1}$ .

Define a further element  $p_n$  of  $K_Q$  by  $p_n = p$ . Then,  $p_1, p_2, \dots, p_n$  are  $n$  elements of  $K_Q$  satisfying

$$P = \underbrace{Q}_{= \prod_{i=1}^{n-1} (T - p_i)} \cdot \left( T - \underbrace{p}_{= p_n} \right) = \prod_{i=1}^{n-1} (T - p_i) \cdot (T - p_n) = \prod_{i=1}^n (T - p_i)$$

in  $K_Q[T]$ .

Let  $K'_P = K_Q$ . Then,  $K'_P$  is a finite-free extension ring of the ring  $K$  (since  $K_Q$  is a finite-free extension ring of the ring  $K$ ), and the  $n$  elements  $p_1, p_2, \dots, p_n$  of  $K_Q$  satisfy  $P = \prod_{i=1}^n (T - p_i)$  in  $K'_P[T]$  and  $p = p_n$ . Thus, Exercise 5.3 is solved.

*Exercise 5.4: Hints to solution:* First here is a rewriting of Exercise 5.2 (b):

**Lemma 5.4.S.1.** Let  $L$  be a ring. Let  $\ell \in \mathbb{N}$ . Let  $a_0, a_1, \dots, a_\ell$  be elements of  $L$ . Let  $S$  be a finite set with  $|S| = \ell$ . For every  $s \in S$ , let  $p_s$  be an element of  $L$ . If  $\sum_{i=0}^{\ell} a_i T^i = \prod_{s \in S} (1 + p_s T)$  in the polynomial ring  $L[T]$ , then

$$\sum_{i=0}^{\ell} a_{\ell-i} T^i = \prod_{s \in S} (p_s + T).$$

*Proof of Lemma 5.4.S.1.* Assume that  $\sum_{i=0}^{\ell} a_i T^i = \prod_{s \in S} (1 + p_s T)$ .

Since the finite set  $S$  is used only for labelling the elements  $p_s$ , we can WLOG assume that  $S = \{1, 2, \dots, \ell\}$  (since  $|S| = \ell$ ). Assume this. Then,

$$\prod_{s \in S} (1 + p_s T) = \prod_{s \in \{1, 2, \dots, \ell\}} (1 + p_s T) = \prod_{s=1}^{\ell} (1 + p_s T) = \prod_{i=1}^{\ell} (1 + p_i T)$$



(here we renamed the index  $s$  as  $i$ ) and

$$\prod_{s \in S} (p_s + T) = \prod_{s \in \{1, 2, \dots, \ell\}} (p_s + T) = \prod_{s=1}^{\ell} (p_s + T) = \prod_{i=1}^{\ell} (p_i + T)$$

(here we renamed the index  $s$  as  $i$ ).

Now,  $\sum_{i=0}^{\ell} a_i T^i = \prod_{s \in S} (1 + p_s T) = \prod_{i=1}^{\ell} (1 + p_i T)$ . Hence, Exercise 5.2 (b) (applied to  $n = \ell$ ) yields  $\sum_{i=0}^{\ell} a_{\ell-i} T^i = \prod_{i=1}^{\ell} (p_i + T) = \prod_{s \in S} (p_s + T)$ . This proves Lemma 5.4.S.1.  $\square$

The next lemma is more or less the statement of our exercise (except for that it has  $-\alpha\beta$  instead of  $\alpha\beta$ , but this doesn't make that much of a difference):

**Lemma 5.4.S.2.** Let  $K$  be a ring, and  $L$  an extension ring of  $K$ . Let  $n \in \mathbb{N}$  and  $m \in \mathbb{N}$ . Let  $\alpha$  and  $\beta$  be two elements of  $L$  such that  $\alpha$  is  $n$ -integral over  $K$  and  $\beta$  is  $m$ -integral over  $K$ . Then,  $-\alpha\beta$  is  $nm$ -integral over  $K$ .

*Proof of Lemma 5.4.S.2.* Since  $\alpha$  is  $n$ -integral over  $K$ , there exists a monic polynomial  $P \in K[T]$  such that  $\deg P = n$  and  $P(\alpha) = 0$  (by the definition of “ $n$ -integral”).

Since  $\beta$  is  $m$ -integral over  $K$ , there exists a monic polynomial  $Q \in K[T]$  such that  $\deg Q = m$  and  $Q(\beta) = 0$  (by the definition of “ $m$ -integral”).

Since  $\deg P = n$ , we can write the polynomial  $P \in K[T]$  in the form  $P = \sum_{i=0}^n c_i T^i$  for some  $(c_0, c_1, \dots, c_n) \in K^{n+1}$ . Consider this  $(c_0, c_1, \dots, c_n)$ . Then,  $c_n = (\text{the coefficient of } P \text{ before } T^n) = 1$  (since  $P$  is a monic polynomial with  $\deg P = n$ ).

Since  $\deg Q = m$ , we can write the polynomial  $Q \in K[T]$  in the form  $Q = \sum_{i=0}^m d_i T^i$  for some  $(d_0, d_1, \dots, d_m) \in K^{m+1}$ . Consider this  $(d_0, d_1, \dots, d_m)$ . Then,  $d_m = (\text{the coefficient of } Q \text{ before } T^m) = 1$  (since  $Q$  is a monic polynomial with  $\deg Q = m$ ).

For every  $i \in \mathbb{N}$ , define an element  $a_i \in K$  by  $a_i = \begin{cases} c_{n-i}, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases}$ . For every  $i \in \mathbb{N}$ , define an element  $b_i \in K$  by  $b_i = \begin{cases} d_{m-i}, & \text{if } i \leq m; \\ 0, & \text{if } i > m \end{cases}$ .

Let  $R \in K[T]$  be the polynomial defined by

$$R = \sum_{i=0}^{mn} P_{mn-i}(a_1, a_2, \dots, a_{mn-i}, b_1, b_2, \dots, b_{mn-i}) T^i.$$

Now we claim that  $R$  is a monic polynomial, that  $\deg R = mn$  and that  $R(-\alpha\beta) = 0$ .

*Proof.* Exercise 5.3 (applied to  $\alpha$  and  $L$  instead of  $p$  and  $K$ ) yields that there exists a finite-free extension ring  $L'_p$  of  $L$  and  $n$  elements  $p_1, p_2, \dots, p_n$  of this extension ring  $L'_p$  such that  $P = \prod_{i=1}^n (T - p_i)$  in  $L'_p[T]$  and such that  $\alpha = p_n$ . Consider this extension ring  $L'_p$  and these elements  $p_1, p_2, \dots, p_n$ . Denote this extension ring  $L'_p$  by  $M$ . All we need to know about  $M$  is that  $M$  is an extension ring of  $L$  containing  $p_1, p_2, \dots, p_n$ .

Exercise 5.3 (applied to  $Q, m, \beta$  and  $M$  instead of  $P, n, p$  and  $K$ ) yields that there exists a finite-free extension ring  $M'_Q$  of  $M$  and  $m$  elements  $q_1, q_2, \dots, q_m$  of this extension ring  $M'_Q$  such that  $Q = \prod_{i=1}^m (T - q_i)$  in  $M'_Q[T]$  and such that  $\beta = q_m$ . Consider this extension ring  $M'_Q$  and these elements  $q_1, q_2, \dots, q_m$ . Denote this extension ring  $M'_Q$  by  $N$ . All we need to know about  $N$  is that  $N$  is an extension ring of  $L$  (since  $N$  is an extension ring of  $M$ , which, in turn, is an extension ring of  $L$ ) containing  $p_1, p_2, \dots, p_n$  (because it contains  $L$  and because  $L$  contains  $p_1, p_2, \dots, p_n$ ) and containing  $q_1, q_2, \dots, q_m$ .

Let  $\tilde{P} \in K[T]$  be the polynomial  $\sum_{i=0}^n c_{n-i}T^i$ . This polynomial  $\tilde{P}$  has constant term  $c_{n-0} = c_n = 1$ , hence lies in  $1 + K[T]^+$ .

Let  $\tilde{Q} \in K[T]$  be the polynomial  $\sum_{i=0}^m d_{m-i}T^i$ . This polynomial  $\tilde{Q}$  has constant term  $d_{m-0} = d_m = 1$ , hence lies in  $1 + K[T]^+$ .

We have  $\sum_{i=0}^n \underbrace{c_{n-(n-i)}}_{=c_i} T^i = \sum_{i=0}^n c_i T^i = P = \prod_{i=1}^n \underbrace{(T - p_i)}_{=-p_i+T} = \prod_{i=1}^n (-p_i + T)$ . Therefore,

Exercise 5.2 (a) (applied to  $N, c_{n-i}$  and  $-p_i$  instead of  $L, a_i$  and  $p_i$ ) yields that

$$\sum_{i=0}^n c_{n-i}T^i = \prod_{i=1}^n (1 + (-p_i)T).$$

Thus,

$$\tilde{P} = \sum_{i=0}^n c_{n-i}T^i = \prod_{i=1}^n (1 + (-p_i)T) = \Pi(N, [-p_1, -p_2, \dots, -p_n]).$$

We have  $\sum_{i=0}^m \underbrace{d_{m-(m-i)}}_{=d_i} T^i = \sum_{i=0}^m d_i T^i = Q = \prod_{i=1}^m \underbrace{(T - q_i)}_{=-q_i+T} = \prod_{i=1}^m (-q_i + T)$ . Therefore,

Exercise 5.2 (a) (applied to  $N, m, d_{m-i}$  and  $-q_i$  instead of  $L, n, a_i$  and  $p_i$ ) yields that

$$\sum_{i=0}^m d_{m-i}T^i = \prod_{i=1}^m (1 + (-q_i)T).$$

Thus,

$$\tilde{Q} = \sum_{i=0}^m d_{m-i}T^i = \prod_{i=1}^m (1 + (-q_i)T) = \Pi(N, [-q_1, -q_2, \dots, -q_m]).$$

Since  $\tilde{Q} = \Pi(N, [-q_1, -q_2, \dots, -q_m])$  and  $\tilde{P} = \Pi(N, [-p_1, -p_2, \dots, -p_n])$ , we can apply Theorem 5.3 (c) to  $u = \tilde{Q}, v = \tilde{P}, \tilde{K}_u = N, \tilde{K}_v = N, \tilde{K}_{u,v} = N, u_i = -q_i$  and  $v_j = -p_j$ . As a result we obtain

$$\begin{aligned} \tilde{Q}\tilde{P} &= \Pi \left( N, \left[ \underbrace{(-q_i)(-p_j)}_{=p_jq_i} \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\} \right] \right) \\ &= \Pi(N, [p_jq_i \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}]) = \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + p_jq_iT). \end{aligned}$$

Thus,  $\tilde{Q} \hat{\cdot} \tilde{P}$  is a polynomial of degree

$$\begin{aligned}
\deg(\tilde{Q} \hat{\cdot} \tilde{P}) &= \deg\left(\prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + p_j q_i T)\right) \\
&= \deg\left(\text{since } \tilde{Q} \hat{\cdot} \tilde{P} = \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + p_j q_i T)\right) \\
&\leq \sum_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} \underbrace{\deg(1 + p_j q_i T)}_{\leq 1} \\
&\quad \left(\text{since the degree of a product of some polynomials}\right. \\
&\quad \left.\text{is } \leq \text{ to the sum of the degrees of these polynomials}\right) \\
&\leq \sum_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} 1 = |\{1, 2, \dots, m\} \times \{1, 2, \dots, n\}| = mn.
\end{aligned}$$

But

$$\begin{aligned}
\sum_{i \in \mathbb{N}} a_i T^i &= \sum_{i \in \mathbb{N}} \begin{cases} c_{n-i}, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases} T^i \quad \left(\text{since } a_i = \begin{cases} c_{n-i}, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases}\right) \\
&= \sum_{i=0}^n \underbrace{\begin{cases} c_{n-i}, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases}}_{=c_{n-i} \text{ (since } i \leq n)} T^i + \sum_{i=n+1}^{\infty} \underbrace{\begin{cases} c_{n-i}, & \text{if } i \leq n; \\ 0, & \text{if } i > n \end{cases}}_{=0} T^i \\
&= \sum_{i=0}^n c_{n-i} T^i + \underbrace{\sum_{i=n+1}^{\infty} 0 T^i}_{=0} = \sum_{i=0}^n c_{n-i} T^i = \tilde{P}
\end{aligned}$$

and similarly  $\sum_{i \in \mathbb{N}} b_i T^i = \tilde{Q}$ . Now,

$$\begin{aligned}
\tilde{Q} \hat{\cdot} \tilde{P} &= \tilde{P} \hat{\cdot} \tilde{Q} = \left(\sum_{i \in \mathbb{N}} a_i T^i\right) \hat{\cdot} \left(\sum_{i \in \mathbb{N}} b_i T^i\right) \quad \left(\text{since } \tilde{P} = \sum_{i \in \mathbb{N}} a_i T^i \text{ and } \tilde{Q} = \sum_{i \in \mathbb{N}} b_i T^i\right) \\
&= \sum_{k \in \mathbb{N}} P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k) T^k
\end{aligned}$$

(by the definition of  $\hat{\cdot}$  at the beginning of Section 5).

Hence, for every  $k \in \mathbb{N}$ , we have

$$\left(\text{the coefficient of the polynomial } \tilde{Q} \hat{\cdot} \tilde{P} \text{ before } T^k\right) = P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k).$$

But since  $\tilde{Q}\tilde{P}$  is a polynomial of degree  $\leq mn$ , we have

$$\begin{aligned}\tilde{Q}\tilde{P} &= \sum_{k=0}^{mn} \underbrace{\left( \text{the coefficient of the polynomial } \tilde{Q}\tilde{P} \text{ before } T^k \right)}_{=P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k)} T^k \\ &= \sum_{k=0}^{mn} P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k) T^k \\ &= \sum_{i=0}^{mn} P_i(a_1, a_2, \dots, a_i, b_1, b_2, \dots, b_i) T^i \quad (\text{here, we renamed } k \text{ as } i).\end{aligned}$$

Thus,

$$\sum_{i=0}^{mn} P_i(a_1, a_2, \dots, a_i, b_1, b_2, \dots, b_i) T^i = \tilde{Q}\tilde{P} = \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + p_j q_i T).$$

Define  $r_{(i,j)}$  to mean  $p_j q_i$  for every  $(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}$ . Then,

$$\begin{aligned}& \sum_{i=0}^{mn} P_i(a_1, a_2, \dots, a_i, b_1, b_2, \dots, b_i) T^i \\ &= \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} \left( 1 + \underbrace{p_j q_i}_{=r_{(i,j)}} T \right) = \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + r_{(i,j)} T) \\ &= \prod_{s \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + r_s T)\end{aligned}$$

(here, we renamed the index  $(i,j)$  as  $s$ ). Thus, Lemma 5.4.S.1 (applied to  $N$ ,  $mn$ ,  $P_i(a_1, a_2, \dots, a_i, b_1, b_2, \dots, b_i)$ ,  $\{1,2,\dots,m\} \times \{1,2,\dots,n\}$  and  $r_s$  instead of  $L$ ,  $\ell$ ,  $a_i$ ,  $S$  and  $p_s$ ) yields that

$$\sum_{i=0}^{mn} P_{mn-i}(a_1, a_2, \dots, a_{mn-i}, b_1, b_2, \dots, b_{mn-i}) T^i = \prod_{s \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (r_s + T).$$

Since  $\sum_{i=0}^{mn} P_{mn-i}(a_1, a_2, \dots, a_{mn-i}, b_1, b_2, \dots, b_{mn-i}) T^i = R$ , this rewrites as

$$\begin{aligned}R &= \prod_{s \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (r_s + T) = \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} \left( \underbrace{r_{(i,j)}}_{=p_j q_i} + T \right) \\ &\quad (\text{here, we renamed the index } s \text{ as } (i,j)) \\ &= \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (p_j q_i + T).\end{aligned}$$

Therefore,

$$R(-\alpha\beta) = \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (p_j q_i + (-\alpha\beta)). \quad (86)$$

One of the factors of the product on the right hand side of (86) (namely, the one for  $(i, j) = (m, n)$ ) is

$$\underbrace{p_n}_{=\alpha} \underbrace{q_m}_{=\beta} + (-\alpha\beta) = \alpha\beta + (-\alpha\beta) = 0.$$

Hence, the product on the right hand side of (86) is 0. Thus, (86) simplifies to  $R(-\alpha\beta) = 0$ .

Since  $R$  was defined by

$$R = \sum_{i=0}^{mn} P_{mn-i}(a_1, a_2, \dots, a_{mn-i}, b_1, b_2, \dots, b_{mn-i}) T^i,$$

it is clear that the polynomial  $R$  has degree  $\leq mn$ , and that the coefficient of  $R$  before  $T^{mn}$  is

$$P_{mn-mn}(a_1, a_2, \dots, a_{mn-mn}, b_1, b_2, \dots, b_{mn-mn}) = P_0(a_1, a_2, \dots, a_0, b_1, b_2, \dots, b_0) = P_0 = 1$$

(here we are using the fact that  $P_0 = 1$ ; this is very easy to see from the definition of  $P_0$ ). Thus,  $R$  is a monic polynomial of degree  $mn$ . Hence  $\deg R = mn = nm$ .

So we have found a monic polynomial  $R \in K[T]$  such that  $\deg R = nm$  and  $R(-\alpha\beta) = 0$ . By the definition of “ $nm$ -integral”, this yields that  $-\alpha\beta$  is  $nm$ -integral over  $K$ . This proves Lemma 5.4.S.2.  $\square$

Now let us finally solve the problem. Let  $\alpha$  and  $\beta$  be two elements of  $L$  such that  $\alpha$  is  $n$ -integral over  $K$  and  $\beta$  is  $m$ -integral over  $K$ . Then, Lemma 5.4.S.2 yields that  $-\alpha\beta$  is  $nm$ -integral over  $K$ . Hence, Lemma 5.4.S.2 (applied to  $nm, 1, -\alpha\beta$  and  $-1$  instead of  $n, m, \alpha$  and  $\beta$ ) yields that  $(-\alpha\beta)(-1)$  is  $(nm) \cdot 1$ -integral over  $K$  (since  $-1$  is 1-integral over  $K$ ). In other words,  $\alpha\beta$  is  $nm$ -integral over  $K$ . This solves Exercise 5.4.

*Exercise 5.5: Detailed solution:* (a) Let  $\pi$  be the canonical projection  $K \rightarrow K/I$ . Then,  $\pi$  is a ring homomorphism, and thus induces a canonical ring homomorphism  $\pi[[T]] : K[[T]] \rightarrow (K/I)[[T]]$  (which sends every  $\sum_{i \in \mathbb{N}} a_i T^i \in K[[T]]$  to  $\sum_{i \in \mathbb{N}} \pi(a_i) T^i \in (K/I)[[T]]$ ). The morphism  $\Lambda(\pi)$  is merely the restriction of this homomorphism  $\pi[[T]]$  to the subset  $\Lambda(K)$  of  $K[[T]]$  (due to the definition of  $\Lambda(\pi)$ ).

Notice that  $1 + I[[T]]^+ \subseteq 1 + K[[T]]^+ = \Lambda(K)$ .

*1st step:* We have  $1 + I[[T]]^+ \subseteq \text{Ker}(\Lambda(\pi))$ .

*Proof:* Let  $q \in 1 + I[[T]]^+$ . Then,  $q - 1 \in I[[T]]^+ = TI[[T]] \subseteq I[[T]]$ . Thus, we can write  $q - 1$  in the form  $q - 1 = \sum_{i \geq 0} r_i T^i$  for some sequence  $(r_0, r_1, r_2, \dots)$  of elements of  $I$ . Consider this  $(r_0, r_1, r_2, \dots)$ . Clearly,  $r_i \in I$  for every  $i \geq 0$ . Thus,  $\pi(r_i) = 0$  for every  $i \geq 0$  (because  $\pi$  is the canonical projection  $K \rightarrow K/I$ ). Now, by the definition of  $\pi[[T]]$ , we have

$$(\pi[[T]]) \left( \sum_{i \geq 0} r_i T^i \right) = \sum_{i \geq 0} \underbrace{\pi(r_i)}_{=0} T^i = \sum_{i \geq 0} 0 T^i = 0.$$

Since  $\sum_{i \geq 0} r_i T^i = q - 1$ , this rewrites as  $(\pi[[T]])(q - 1) = 0$ . Since

$$(\pi[[T]])(q - 1) = (\pi[[T]])(q) - 1 \quad (\text{since } \pi[[T]] \text{ is a ring homomorphism}),$$

this rewrites as  $(\pi [[T]])(q) - 1 = 0$ . That is,  $(\pi [[T]])(q) = 1$ . Since  $\Lambda(\pi)$  is the restriction of  $\pi [[T]]$  to the subset  $\Lambda(K)$  of  $K [[T]]$ , and since  $q \in \Lambda(K)$ , we have  $(\Lambda(\pi))(q) = (\pi [[T]])(q) = 1$ , so that  $q \in \text{Ker}(\Lambda(\pi))$  (because the power series  $1 \in \Lambda(K/I)$  is the zero of the ring  $\Lambda(K/I)$ ).

Now forget that we fixed  $q$ . We thus have proven that every  $q \in 1 + I [[T]]^+$  satisfies  $q \in \text{Ker}(\Lambda(\pi))$ . In other words,  $1 + I [[T]]^+ \subseteq \text{Ker}(\Lambda(\pi))$ . This completes the proof of the 1st step.

*2nd step:* We have  $\text{Ker}(\Lambda(\pi)) \subseteq 1 + I [[T]]^+$ .

*Proof:* Let  $q \in \text{Ker}(\Lambda(\pi))$ . Then,  $q \in \Lambda(K)$  and  $(\Lambda(\pi))(q) = 1$  (because  $1 \in \Lambda(K/I)$  is the zero of the ring  $\Lambda(K/I)$ ).

Since  $q \in \Lambda(K) \subseteq K [[T]]$ , we can write  $q$  in the form  $q = \sum_{i \geq 0} q_i T^i$  for some sequence  $(q_0, q_1, q_2, \dots)$  of elements of  $K$ . Consider this  $(q_0, q_1, q_2, \dots)$ . Then,  $q_0$  is the constant term of the power series  $q$ .

Since  $q \in \Lambda(K) = 1 + K [[T]]^+ = \{p \in K [[T]] \mid p \text{ is a power series with constant term } 1\}$ , we know that  $q$  is a power series with constant term 1. In other words, the constant term of the power series  $q$  is 1. Since  $q_0$  is the constant term of the power series  $q$ , this yields that  $q_0 = 1$ .

Since  $\Lambda(\pi)$  is the restriction of  $\pi [[T]]$  to the subset  $\Lambda(K)$  of  $K [[T]]$ , we have

$$\begin{aligned} (\Lambda(\pi))(q) &= (\pi [[T]])(q) = (\pi [[T]]) \left( \sum_{i \geq 0} q_i T^i \right) && \left( \text{since } q = \sum_{i \geq 0} q_i T^i \right) \\ &= \sum_{i \geq 0} \pi(q_i) T^i && \text{(by the definition of } \pi [[T]] \text{)}. \end{aligned}$$

Since  $(\Lambda(\pi))(q) = 1$ , this rewrites as  $1 = \sum_{i \geq 0} \pi(q_i) T^i$ .

Now, let  $j$  be a positive integer. Then, the coefficient of  $T^j$  on the left hand side of the equality  $1 = \sum_{i \geq 0} \pi(q_i) T^i$  is 0, while the coefficient of  $T^j$  on the right hand side of this equality is  $\pi(q_j)$ . Since the coefficients of  $T^j$  on the two sides of an equality must always be equal, this yields that  $0 = \pi(q_j)$ . But  $\pi$  is the canonical projection  $K \rightarrow K/I$ . Hence, since we have  $\pi(q_j) = 0$ , we conclude that  $q_j \in I$ .

Now forget that we fixed  $j$ . We thus have shown that  $q_j \in I$  for every positive integer  $j$ . Thus,  $\sum_{j > 0} q_j T^j \in I [[T]]$ . Since  $\sum_{j > 0} q_j T^j$  is a power series with constant term 0, we thus have

$$\sum_{j > 0} q_j T^j \in \{p \in I [[T]] \mid p \text{ is a power series with constant term } 0\} = TI [[T]] = I [[T]]^+.$$

Now,

$$q = \sum_{i \geq 0} q_i T^i = \sum_{j \geq 0} q_j T^j = \underbrace{q_0}_{=1} \underbrace{T^0}_{=1} + \underbrace{\sum_{j > 0} q_j T^j}_{\in I [[T]]^+} \in 1 + I [[T]]^+.$$

Now forget that we fixed  $q$ . We thus have proven that every  $q \in \text{Ker}(\Lambda(\pi))$  satisfies  $q \in 1 + I [[T]]^+$ . In other words,  $\text{Ker}(\Lambda(\pi)) \subseteq 1 + I [[T]]^+$ . This completes the proof of the 2nd step.

*3rd step:* We have proven that  $1 + I[[T]]^+ \subseteq \text{Ker}(\Lambda(\pi))$  and  $\text{Ker}(\Lambda(\pi)) \subseteq 1 + I[[T]]^+$ . Combining these two relations, we obtain  $1 + I[[T]]^+ = \text{Ker}(\Lambda(\pi))$ . This solves Exercise 5.5 (a).

(b) We know that  $\Lambda(\pi)$  is a  $\lambda$ -ring homomorphism (since  $\pi$  is a ring homomorphism). Thus,  $\text{Ker}(\Lambda(\pi))$  is a  $\lambda$ -ideal of  $\Lambda(K)$  (by Theorem 2.3, applied to  $\Lambda(K)$ ,  $\Lambda(K/I)$  and  $\Lambda(\pi)$  instead of  $(K, (\lambda^i)_{i \in \mathbb{N}})$ ,  $(L, (\mu^i)_{i \in \mathbb{N}})$  and  $f$ ). Since  $\text{Ker}(\Lambda(\pi)) = 1 + I[[T]]^+$  (by Exercise 5.5 (a)), this yields that  $1 + I[[T]]^+$  is a  $\lambda$ -ideal of  $\Lambda(K)$ . This solves Exercise 5.5 (b).

## 11.6. To Section 6

*Exercise 6.1: Hints to solution:* Recall that  $\widehat{\phantom{x}}$  denotes the subtraction of the ring  $\Lambda(K)$  (that is, the binary operation on  $\Lambda(K)$  that undoes the addition  $\widehat{+}$ ). Then,  $p \widehat{-} q = \frac{p}{q}$  for any  $p \in \Lambda(K)$  and  $q \in \Lambda(K)$  (by the definition of the ring structure on  $\Lambda(K)$ ).

For every two subsets  $U$  and  $U'$  of  $\Lambda(K)$ , let  $U \widehat{-} U'$  denote the subset  $\{u \widehat{-} u' \mid u \in U, u' \in U'\}$  of  $\Lambda(K)$ . Now,

$$\begin{aligned}
& \underbrace{(1 + K[T]^+)^{-1} K[T]}_{=1+K[[T]]^+} \cap \underbrace{\Lambda(K)}_{=1+K[[T]]^+} \\
&= \left\{ \frac{p}{q} \mid p \in K[T], q \in 1 + K[T]^+ \right\} \\
&= \left\{ \frac{p}{q} \mid p \in K[T], q \in 1 + K[T]^+ \right\} \cap (1 + K[[T]]^+) \\
&= \left\{ \frac{p}{q} \mid p \in K[T], q \in 1 + K[T]^+, \frac{p}{q} \in 1 + K[[T]]^+ \right\} \\
&= \left\{ \underbrace{\frac{p}{q}}_{=p \widehat{-} q} \mid p \in 1 + K[T]^+, q \in 1 + K[T]^+ \right\} \\
&\quad \left( \begin{array}{l} \text{because two polynomials } p \in K[T] \text{ and } q \in 1 + K[T]^+ \\ \text{satisfy } \frac{p}{q} \in 1 + K[[T]]^+ \text{ if and only if } p \in 1 + K[T]^+ \end{array} \right) \\
&= \{p \widehat{-} q \mid p \in 1 + K[T]^+, q \in 1 + K[T]^+\} \\
&= (1 + K[T]^+) \widehat{-} (1 + K[T]^+).
\end{aligned}$$

The subset  $1 + K[T]^+$  of  $\Lambda(K)$  is closed under the addition  $\widehat{+}$ , the multiplication  $\widehat{\cdot}$  and the maps  $\widehat{\lambda}^i$  (according to Theorem 5.3, since  $1 + K[T]^+ = \Pi(K^{\text{int}})$ ) and contains the zero 1 and the unity  $1 + T$ . Thus, by Exercise 2.2 (applied to  $\Lambda(K)$  and  $1 + K[T]^+$  instead of  $K$  and  $L$ ), we see that  $(1 + K[T]^+) \widehat{-} (1 + K[T]^+)$  is a sub- $\lambda$ -ring of  $\Lambda(K)$ . In other words,  $(1 + K[T]^+)^{-1} K[T] \cap \Lambda(K)$  is a sub- $\lambda$ -ring of  $\Lambda(K)$  (since  $(1 + K[T]^+)^{-1} K[T] \cap \Lambda(K) = (1 + K[T]^+) \widehat{-} (1 + K[T]^+)$ ). This sub- $\lambda$ -ring is clearly special (since  $\Lambda(K)$  is special). This solves Exercise 6.1.

*Exercise 6.2: Solution:* (a) Consider the map  $\lambda_T$  defined in Theorem 2.1. Fix some  $x \in K$ . Define a map  $\Upsilon : \mathbb{Z} \rightarrow K[[T]]$  by

$$\Upsilon(n) = \lambda_T(nx) \quad \text{for every } n \in \mathbb{Z}.$$

This map  $\Upsilon$  is a group homomorphism from the group  $(\mathbb{Z}, +)$  to the group  $(K[[T]]^\times, \cdot)$  (because every two elements  $n$  and  $m$  of  $\mathbb{Z}$  satisfy

$$\begin{aligned} \Upsilon(n) \cdot \Upsilon(m) &= \lambda_T(nx) \cdot \lambda_T(mx) = \lambda_T(nx + mx) \\ &\left( \begin{array}{c} \text{according to the formula } \lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x + y) \\ \text{given in Theorem 2.1 (b)} \end{array} \right) \\ &= \lambda_T((n + m)x) = \Upsilon(n + m), \end{aligned}$$

and we have  $\Upsilon(0) = \lambda_T(0x) = \lambda_T(0) = 1$  by Theorem 2.1 (b). Thus,  $\Upsilon(n \cdot 1) = (\Upsilon(1))^n$  for every  $n \in \mathbb{Z}$ . Since  $\Upsilon(n \cdot 1) = \Upsilon(n) = \lambda_T(nx)$  and  $\Upsilon(1) = \lambda_T(1x) = \lambda_T(x)$ , this rewrites as  $\lambda_T(nx) = (\lambda_T(x))^n$ . Applying this to  $x = 1_K$ , we obtain

$$\begin{aligned} \lambda_T(n \cdot 1) &= (\lambda_T(1))^n = (1 + T)^n \\ &\quad (\text{since } \lambda_T(1) = 1 + T, \text{ because the } \lambda\text{-ring } K \text{ is special}) \\ &= \sum_{i \in \mathbb{N}} \binom{n}{i} T^i \quad (\text{by the binomial formula}). \end{aligned}$$

Comparing this with  $\lambda_T(n \cdot 1) = \sum_{i \in \mathbb{N}} \lambda^i(n \cdot 1) T^i$ , we conclude that  $\sum_{i \in \mathbb{N}} \lambda^i(n \cdot 1) T^i = \sum_{i \in \mathbb{N}} \binom{n}{i} T^i$ . Comparing coefficients, we obtain  $\lambda^i(n \cdot 1) = \binom{n}{i} \cdot 1$  for every  $i \in \mathbb{N}$ .

(b) Assume, for the sake of contradiction, that  $m = 0$  in  $K$  for some positive integer  $m$ . Then, Theorem 2.1 (a) yields

$$\begin{aligned} \lambda_T(m) &= \lambda_T(\underbrace{1 + 1 + \dots + 1}_{m \text{ times}}) = \underbrace{\lambda_T(1) \cdot \lambda_T(1) \cdot \dots \cdot \lambda_T(1)}_{m \text{ times}} = (\lambda_T(1))^m \\ &= (\lambda_T(1))^m = (1 + T)^m = 1 + \sum_{i=1}^{m-1} \binom{m}{i} T^i + T^m \quad (\text{by the binomial formula}) \end{aligned}$$

in  $K[[T]]$ . On the other hand,  $\lambda_T(m) = \lambda_T(0) = 1$ . Contradiction (unless  $K$  is the trivial ring).

*Exercise 6.3: Hints to solution:* Use Exercise 6.4 or the very definition of special  $\lambda$ -rings together with Exercise 2.1. Do not forget to check that the map  $\lambda_T$  is well-defined.

*Exercise 6.4: Hints to solution:* Repeat the proof of Theorem 6.1, replacing every appearance of “ $x \in K$ ” by “ $x \in E$ ” and every appearance of “ $y \in K$ ” by “ $y \in E$ ”. You need the fact that  $\lambda_T$  is a  $\lambda$ -ring homomorphism if and only if it satisfies the three conditions

$$\begin{aligned} \lambda_T(xy) &= \lambda_T(x) \widehat{\cdot} \lambda_T(y) && \text{for every } x \in E \text{ and } y \in E, \\ \lambda_T(1) &= 1 + T, && \text{and} \\ \lambda_T(\lambda^j(x)) &= \widehat{\lambda}^j(\lambda_T(x)) && \text{for every } j \in \mathbb{N} \text{ and } x \in E. \end{aligned}$$

This is because the first two of these conditions, together with the preassumptions that  $E$  is a generating set of  $K$  as a  $\mathbb{Z}$ -module and that  $\lambda_T$  is an additive group



homomorphism, are equivalent to claiming that  $\lambda_T$  is a ring homomorphism; and the third condition then makes  $\lambda_T$  a  $\lambda$ -ring homomorphism (according to Exercise 2.1 (b)).

*Exercise 6.5: Hints to solution:* First, the mapping  $\text{coeff}_i : \Lambda(K) \rightarrow K$  is continuous (with respect to the  $(T)$ -topology on  $\Lambda(K)$  and *any arbitrary topology* on  $K$ ), and the operation  $\widehat{\lambda}^i$  is continuous as well (by Theorem 5.5 (d)); besides, the subset  $1 + K [T]^+$  of  $1 + K [[T]]^+ = \Lambda(K)$  is dense (by Theorem 5.5 (a)). Hence, in order to prove that  $\text{coeff}_i(u) = \text{coeff}_1(\widehat{\lambda}^i(u))$  for every  $u \in \Lambda(K)$ , it is enough to verify that  $\text{coeff}_i(u) = \text{coeff}_1(\widehat{\lambda}^i(u))$  for every  $u \in 1 + K [T]^+$ .<sup>89</sup> So let us assume that  $u \in 1 + K [T]^+$ . Then, there exist some  $(\widetilde{K}_u, [u_1, u_2, \dots, u_m]) \in K^{\text{int}}$  such that  $u = \Pi(\widetilde{K}_u, [u_1, u_2, \dots, u_m])$ . Consider this  $(\widetilde{K}_u, [u_1, u_2, \dots, u_m])$ . Then,

$$\begin{aligned} u = \Pi(\widetilde{K}, [u_1, u_2, \dots, u_m]) &= \prod_{i=1}^m (1 + u_i T) = \sum_{i \in \mathbb{N}} \left( \sum_{\substack{K \subseteq \{1, 2, \dots, m\} \\ |K|=i}} \prod_{k \in K} u_k \right) \cdot T^i \\ &\quad \left( \text{by Exercise 4.2 (b), applied to } A = \widetilde{K} [[T]], \alpha_i = u_i \text{ and } t = T \right) \\ &= \sum_{i \in \mathbb{N}} \left( \sum_{K \in \mathcal{P}_i(\{1, 2, \dots, m\})} \prod_{k \in K} u_k \right) \cdot T^i \end{aligned}$$

and therefore  $\text{coeff}_i u = \sum_{K \in \mathcal{P}_i(\{1, 2, \dots, m\})} \prod_{k \in K} u_k$ . On the other hand, Theorem 5.3 (d) yields

$$\begin{aligned} \widehat{\lambda}^i(u) &= \Pi \left( \widetilde{K}_u, \left[ \prod_{k \in K} u_k \mid K \in \mathcal{P}_i(\{1, 2, \dots, m\}) \right] \right) \\ &= \prod_{K \in \mathcal{P}_i(\{1, 2, \dots, m\})} \left( 1 + \prod_{k \in K} u_k T \right) = 1 + \sum_{K \in \mathcal{P}_i(\{1, 2, \dots, m\})} \prod_{k \in K} u_k \cdot T + (\text{higher powers of } T), \end{aligned}$$

so that

$$\text{coeff}_1(\widehat{\lambda}^i(u)) = \sum_{K \in \mathcal{P}_i(\{1, 2, \dots, m\})} \prod_{k \in K} u_k.$$

Comparing with  $\text{coeff}_i u = \sum_{K \in \mathcal{P}_i(\{1, 2, \dots, m\})} \prod_{k \in K} u_k$ , we get  $\text{coeff}_i(u) = \text{coeff}_1(\widehat{\lambda}^i(u))$ , qed.

*Exercise 6.6: Hints to solution:* Consider the maps  $\widehat{\lambda}^i : \Lambda(K) \rightarrow \Lambda(K)$  that we have defined in Section 5. Theorem 5.1 (b) yields that  $(\Lambda(K), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. Since  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring, the map  $\lambda_T : K \rightarrow \Lambda(K)$  defined in Theorem 5.6 is a  $\lambda$ -ring homomorphism. Also, we know that the ring homomorphism  $\varphi : K \rightarrow A$

<sup>89</sup>At this point, we are slightly cheating: This argument works only if the topological space  $K$  is Hausdorff. Thus we are not completely free in choosing the topology on  $K$ . However, there are still enough Hausdorff topologies on  $K$  (for example, the discrete topology) to choose from - the argument works if we take any of them.

induces a  $\lambda$ -ring homomorphism  $\Lambda(\varphi) : \Lambda(K) \rightarrow \Lambda(A)$ . Now, consider the composed  $\lambda$ -ring homomorphism  $\Lambda(\varphi) \circ \lambda_T : K \rightarrow \Lambda(A)$ .

*1st Step:* We claim that  $\text{coeff}_1^A \circ \Lambda(\varphi) \circ \lambda_T = \varphi$ .

*Proof.* Define a mapping  $\text{coeff}_i : \Lambda(K) \rightarrow K$  for every  $i \in \mathbb{N}$  as in Exercise 6.5. Then,  $\text{coeff}_1^A \circ \Lambda(\varphi) = \varphi \circ \text{coeff}_1$  (by the definition of  $\Lambda(\varphi)$ ) and  $\text{coeff}_1 \circ \lambda_T = \text{id}_K$  (by Theorem 8.2). Thus,  $\underbrace{\text{coeff}_1^A \circ \Lambda(\varphi)}_{=\varphi \circ \text{coeff}_1} \circ \lambda_T = \varphi \circ \underbrace{\text{coeff}_1 \circ \lambda_T}_{=\text{id}_K} = \varphi$ , and the 1st Step is proven.

*2nd Step:* We claim that if  $\tilde{\varphi} : K \rightarrow \Lambda(A)$  is a  $\lambda$ -ring homomorphism such that  $\text{coeff}_1^A \circ \tilde{\varphi} = \varphi$ , then  $\tilde{\varphi} = \Lambda(\varphi) \circ \lambda_T$ .

*Proof.* For every  $i \in \mathbb{N}$ , define a mapping  $\text{coeff}_i^A : \Lambda(A) \rightarrow A$  by  $\text{coeff}_i^A \left( \sum_{j \in \mathbb{N}} a_j T^j \right) = a_i$  for every  $\sum_{j \in \mathbb{N}} a_j T^j \in \Lambda(A)$  (with  $a_j \in A$  for every  $j \in \mathbb{N}$ ). (In other words,  $\text{coeff}_i^A$  is the mapping that takes a power series and returns its coefficient before  $T^i$ .) Then, Exercise 6.5 (applied to the ring  $A$  instead of  $K$ ) yields  $\text{coeff}_i^A = \text{coeff}_1^A \circ \widehat{\lambda}_A^i$ . Hence,

$$\text{coeff}_i^A \circ \tilde{\varphi} = \text{coeff}_1^A \circ \underbrace{\widehat{\lambda}_A^i \circ \tilde{\varphi}}_{\substack{=\tilde{\varphi} \circ \lambda^i, \\ \text{since } \tilde{\varphi} \text{ is a} \\ \lambda\text{-ring} \\ \text{homomorphism}}} = \underbrace{\text{coeff}_1^A \circ \tilde{\varphi}}_{=\varphi} \circ \lambda^i = \varphi \circ \lambda^i.$$

But on the other hand,

$$\underbrace{\text{coeff}_i^A \circ \Lambda(\varphi) \circ \lambda_T}_{=\varphi \circ \text{coeff}_i \text{ by the} \\ \text{definition of } \Lambda(\varphi)} = \varphi \circ \underbrace{\text{coeff}_i \circ \lambda_T}_{=\lambda^i, \text{ by the} \\ \text{definition of } \lambda_T} = \varphi \circ \lambda^i.$$

Therefore,  $\text{coeff}_i^A \circ \tilde{\varphi} = \text{coeff}_i^A \circ \Lambda(\varphi) \circ \lambda_T$  for every  $i \in \mathbb{N}$ . Thus,  $(\text{coeff}_i^A \circ \tilde{\varphi})(u) = (\text{coeff}_i^A \circ \Lambda(\varphi) \circ \lambda_T)(u)$  for every  $i \in \mathbb{N}$  for every  $u \in K$ . In other words, for every  $u \in K$  and for every  $i \in \mathbb{N}$ , the power series  $\tilde{\varphi}(u) \in \Lambda(A)$  and  $(\Lambda(\varphi) \circ \lambda_T)(u)$  have the same coefficient before  $T^i$ . Since this holds for all  $i \in \mathbb{N}$  at the same time, this simply means that for every  $u \in K$ , the power series  $\tilde{\varphi}(u) \in \Lambda(A)$  and  $(\Lambda(\varphi) \circ \lambda_T)(u)$  are equal. In other words,  $\tilde{\varphi} = \Lambda(\varphi) \circ \lambda_T$ , and thus the 2nd Step is proven.

Together, the 1st and the 2nd Steps yield the assertion of Exercise 6.6 (in fact, the 1st Step yields the existence of a  $\lambda$ -ring homomorphism  $\tilde{\varphi} : K \rightarrow \Lambda(A)$  such that  $\text{coeff}_1^A \circ \tilde{\varphi} = \varphi$ , namely the homomorphism  $\Lambda(\varphi) \circ \lambda_T$ , and the 2nd Step proves that this is the only such homomorphism).

*Exercise 6.7: Solution:* Let  $t \in I$ . Since  $S$  generates the ideal  $I$ , there exists some  $r \in \mathbb{N}$ , some elements  $s_1, s_2, \dots, s_r$  of  $S$ , and some elements  $a_1, a_2, \dots, a_r$  of  $K$  such that  $t = \sum_{j=1}^r a_j s_j$ . Consider this  $r$ , these  $s_1, s_2, \dots, s_r$  and these  $a_1, a_2, \dots, a_r$ .

Consider the map  $\lambda_T : K \rightarrow \Lambda(K)$  defined in Theorem 5.6. Since  $K$  is a special  $\lambda$ -ring, this map  $\lambda_T$  is a  $\lambda$ -ring homomorphism. In particular,  $\lambda_T$  is a ring homomorphism.

Consider the set  $1 + I[[T]]^+$  defined in Exercise 5.5. By Exercise 5.5 (b), this set  $1 + I[[T]]^+$  is a  $\lambda$ -ideal of  $\Lambda(K)$ , thus also an ideal of  $\Lambda(K)$ .

Now, for every  $j \in \{1, 2, \dots, r\}$ , we have  $\lambda_T(s_j) \in 1 + I[[T]]^+$ .<sup>90</sup> But since  $t = \sum_{j=1}^r a_j s_j$ , we have

$$\begin{aligned} \lambda_T(t) &= \lambda_T\left(\sum_{j=1}^r a_j s_j\right) = \widehat{\sum_{j=1}^r} \lambda_T(a_j) \widehat{\lambda_T(s_j)} \\ &\quad \underbrace{\lambda_T(s_j)}_{\in 1 + I[[T]]^+} \\ &\quad \text{(since } \lambda_T : K \rightarrow \Lambda(K) \text{ is a ring homomorphism)} \\ &\in \widehat{\sum_{j=1}^r} \lambda_T(a_j) \widehat{(1 + I[[T]]^+)} \subseteq 1 + I[[T]]^+ \end{aligned}$$

(since  $1 + I[[T]]^+$  is an ideal of  $\Lambda(K)$ ). In other words,  $\lambda_T(t) - 1 \in I[[T]]^+ \subseteq I[[T]]$ . Thus,  $\lambda_T(t) - 1$  is a power series with all its coefficients lying in  $I$ .

By the definition of  $\lambda_T$ , we have  $\lambda_T(t) = \sum_{i \in \mathbb{N}} \lambda^i(t) T^i$ . Thus, (the coefficient before  $T^i$  in  $\lambda_T(t) = \lambda^i(t)$  for every  $i \in \mathbb{N}$ .)

Now, let  $i$  be a positive integer. Then, (the coefficient before  $T^i$  in  $\lambda_T(t) - 1) \in I$  (because  $\lambda_T(t) - 1$  is a power series with all its coefficients lying in  $I$ ). In view of

$$\begin{aligned} &\text{(the coefficient before } T^i \text{ in } \lambda_T(t) - 1) \\ &= \underbrace{\text{(the coefficient before } T^i \text{ in } \lambda_T(t))}_{=\lambda^i(t)} - \underbrace{\text{(the coefficient before } T^i \text{ in } 1)}_{=0 \text{ (since } i \text{ is positive)}} = \lambda^i(t), \end{aligned}$$

this rewrites as  $\lambda^i(t) \in I$ .

Now, forget that we fixed  $t$  and  $i$ . We thus have proven that every  $t \in I$  and every positive integer  $i$  satisfy  $\lambda^i(t) \in I$ . But due to the definition of a  $\lambda$ -ideal, this means precisely that  $I$  is a  $\lambda$ -ideal of  $K$ .

Thus, we have proven that  $I$  is a  $\lambda$ -ideal of  $K$ . Exercise 6.7 is solved.

*Exercise 6.8: Detailed solution:* (a) For every  $i \in \mathbb{N}$ , the map  $\text{Coeff}_i : K[[T]] \rightarrow K$  is a  $K$ -linear map (for obvious reasons). In particular,  $\text{Coeff}_0$  is a  $K$ -linear map. Now let us show that  $\text{Coeff}_0$  is a  $K$ -algebra homomorphism.

<sup>90</sup>*Proof.* Let  $j \in \{1, 2, \dots, r\}$ . By the definition of  $\lambda_T$ , we have

$$\lambda_T(s_j) = \sum_{i \in \mathbb{N}} \lambda^i(s_j) T^i = \underbrace{\lambda^0(s_j)}_{\substack{=1 \\ \text{(since } \lambda^0(x)=1 \\ \text{for every } x \in K)}} \underbrace{T^0}_{=1} + \sum_{i>0} \lambda^i(s_j) T^i = 1 + \sum_{i>0} \lambda^i(s_j) T^i.$$

Now, we have assumed that every  $s \in S$  and every positive integer  $i$  satisfy  $\lambda^i(s) \in I$ . Applied to  $s = s_j$ , this yields that every positive integer  $i$  satisfies  $\lambda^i(s_j) \in I$ . Thus,  $\sum_{i>0} \lambda^i(s_j) T^i \in I[[T]]$ .

Since  $\sum_{i>0} \lambda^i(s_j) T^i$  is a power series with constant term 0, we thus have

$$\sum_{i>0} \lambda^i(s_j) T^i \in \{p \in I[[T]] \mid p \text{ is a power series with constant term } 0\} = TI[[T]] = I[[T]]^+.$$

Now,  $\lambda_T(s_j) = 1 + \underbrace{\sum_{i>0} \lambda^i(s_j) T^i}_{\in I[[T]]^+} \in 1 + I[[T]]^+$ , qed.

The unity of the ring  $K[[T]]$  is 1. Hence,  $\text{Coeff}_0$  sends the unity of the ring  $K[[T]]$  to  $\text{Coeff}_0(1) = 1$ , which is the unity of  $K$ .

Let  $\varphi \in K[[T]]$  and  $\psi \in K[[T]]$  be two power series. Then, by the definition of the product of two power series, we have

$$\text{Coeff}_n(\varphi\psi) = \sum_{k=0}^n \text{Coeff}_k \varphi \cdot \text{Coeff}_{n-k} \psi \quad \text{for every } n \in \mathbb{N}. \quad (87)$$

Applied to  $n = 0$ , this yields

$$\text{Coeff}_0(\varphi\psi) = \sum_{k=0}^0 \text{Coeff}_k \varphi \cdot \text{Coeff}_{0-k} \psi = \text{Coeff}_0 \varphi \cdot \text{Coeff}_0 \psi.$$

This yields that  $\text{Coeff}_0$  is a  $K$ -algebra homomorphism from  $K[[T]]$  to  $K$  (because we also know that  $\text{Coeff}_0$  is a  $K$ -linear map and sends the unity of the ring  $K[[T]]$  to the unity of  $K$ ). Hence,  $\text{Coeff}_0\left(\prod_{i=1}^m \Phi_i\right) = \prod_{i=1}^m \text{Coeff}_0(\Phi_i)$ . This solves Exercise 6.8 (a).

(b) Exercise 6.8 (a) yields  $\text{Coeff}_0\left(\prod_{i=1}^m \Phi_i\right) = \prod_{i=1}^m \underbrace{\text{Coeff}_0(\Phi_i)}_{=1} = \prod_{i=1}^m 1 = 1$ .

Now let us prove that every  $\mu \in \{0, 1, \dots, m\}$  satisfies

$$\text{Coeff}_1\left(\prod_{i=1}^{\mu} \Phi_i\right) = \sum_{i=1}^{\mu} \text{Coeff}_1(\Phi_i). \quad (88)$$

*Proof of (88).* We will prove (88) by induction over  $\mu$ :

*Induction base:* If  $\mu = 0$ , then  $\prod_{i=1}^{\mu} \Phi_i = (\text{empty product}) = 1$  and thus  $\text{Coeff}_1\left(\prod_{i=1}^{\mu} \Phi_i\right) = \text{Coeff}_1 1 = 0$ , which rewrites as  $\text{Coeff}_1\left(\prod_{i=1}^{\mu} \Phi_i\right) = \sum_{i=1}^{\mu} \text{Coeff}_1(\Phi_i)$  (because for  $\mu = 0$  we also have  $\sum_{i=1}^{\mu} \text{Coeff}_1(\Phi_i) = (\text{empty sum}) = 0$ ). Thus, (88) holds for  $\mu = 0$ . The induction base is thus complete.

*Induction step:* Let  $M \in \{0, 1, \dots, m-1\}$  be such that (88) holds for  $\mu = M$ . We must prove that (88) holds for  $\mu = M+1$  as well.

Since (88) holds for  $\mu = M$ , we have  $\text{Coeff}_1\left(\prod_{i=1}^M \Phi_i\right) = \sum_{i=1}^M \text{Coeff}_1(\Phi_i)$ . Let  $\varphi = \prod_{i=1}^M \Phi_i$  and  $\psi = \Phi_{M+1}$ . Then,  $\varphi\psi = \left(\prod_{i=1}^M \Phi_i\right) \Phi_{M+1} = \prod_{i=1}^{M+1} \Phi_i$ . Since  $\varphi = \prod_{i=1}^M \Phi_i$ , we have

$$\begin{aligned} \text{Coeff}_0 \varphi &= \text{Coeff}_0\left(\prod_{i=1}^M \Phi_i\right) \\ &= \prod_{i=1}^M \underbrace{\text{Coeff}_0(\Phi_i)}_{=1} \quad (\text{since } \text{Coeff}_0 \text{ is a } K\text{-algebra homomorphism}) \\ &= \prod_{i=1}^M 1 = 1 \end{aligned}$$

and

$$\text{Coeff}_1 \varphi = \text{Coeff}_1 \left( \prod_{i=1}^M \Phi_i \right) = \sum_{i=1}^M \text{Coeff}_1 (\Phi_i).$$

Since  $\psi = \Phi_{M+1}$ , we have  $\text{Coeff}_0 \psi = \text{Coeff}_0 (\Phi_{M+1}) = 1$  (because  $\text{Coeff}_0 (\Phi_i) = 1$  for every  $i \in \{1, 2, \dots, m\}$ ). On the other hand, (87) (applied to  $n = 1$ ) yields

$$\begin{aligned} \text{Coeff}_1 (\varphi\psi) &= \sum_{k=0}^1 \text{Coeff}_k \varphi \cdot \text{Coeff}_{1-k} \psi = \underbrace{\text{Coeff}_0 \varphi}_{=1} \cdot \text{Coeff}_1 \underbrace{\psi}_{=\Phi_{M+1}} + \underbrace{\text{Coeff}_1 \varphi}_{=\sum_{i=1}^M \text{Coeff}_1 (\Phi_i)} \cdot \underbrace{\text{Coeff}_0 \psi}_{=1} \\ &= 1 \cdot \text{Coeff}_1 (\Phi_{M+1}) + \sum_{i=1}^M \text{Coeff}_1 (\Phi_i) \cdot 1 \\ &= \text{Coeff}_1 (\Phi_{M+1}) + \sum_{i=1}^M \text{Coeff}_1 (\Phi_i) = \sum_{i=1}^{M+1} \text{Coeff}_1 (\Phi_i). \end{aligned}$$

Since  $\varphi\psi = \prod_{i=1}^{M+1} \Phi_i$ , this rewrites as  $\text{Coeff}_1 \left( \prod_{i=1}^{M+1} \Phi_i \right) = \sum_{i=1}^{M+1} \text{Coeff}_1 (\Phi_i)$ . In other words, (88) holds for  $\mu = M + 1$ . This completes the induction step.

We have thus proven (88) by induction. Applying (88) to  $\mu = m$ , we get  $\text{Coeff}_1 \left( \prod_{i=1}^m \Phi_i \right) = \sum_{i=1}^m \text{Coeff}_1 (\Phi_i)$ . This concludes the solution of Exercise 6.8 (b).

*Exercise 6.9: Hints to solution:* Use the fact that  $u \hat{+} v = uv$ , the definition of  $\hat{+}$  and the fact that  $P_1 = \alpha_1 \cdot \beta_1$ .

*Detailed solution:* We need to prove that  $\text{coeff}_1 : \Lambda(K) \rightarrow K$  is a ring homomorphism. In order to prove this, we must verify that

$$\text{coeff}_1 (1) = 0; \tag{89}$$

$$\text{coeff}_1 (u \hat{+} v) = \text{coeff}_1 u + \text{coeff}_1 v \quad \text{for every } u \in \Lambda(K) \text{ and } v \in \Lambda(K); \tag{90}$$

$$\text{coeff}_1 (1 + T) = 1; \tag{91}$$

$$\text{coeff}_1 (u \hat{\cdot} v) = \text{coeff}_1 u \cdot \text{coeff}_1 v \quad \text{for every } u \in \Lambda(K) \text{ and } v \in \Lambda(K). \tag{92}$$

The equations (89) and (91) are immediately obvious. It thus remains to prove (90) and (92).

*Proof of (90):* For every  $i \in \mathbb{N}$ , we define a mapping  $\text{Coeff}_i : K[[T]] \rightarrow K$  as in Exercise 6.8. Then, clearly,

$$\text{coeff}_i P = \text{Coeff}_i P \quad \text{for every } P \in \Lambda(K) \text{ and } i \in \mathbb{N}. \tag{93}$$

Let  $u \in \Lambda(K)$  and  $v \in \Lambda(K)$ . The definition of the addition  $\hat{+}$  yields  $u \hat{+} v = uv$ . Now,  $u \in \Lambda(K)$ , so that  $u$  is a power series with constant term 1. Hence,  $\text{Coeff}_0 u = 1$ . Similarly,  $\text{Coeff}_0 v = 1$ . But the definition of the product of two power series yields

$$\text{Coeff}_n (uv) = \sum_{k=0}^n \text{Coeff}_k u \cdot \text{Coeff}_{n-k} v \quad \text{for every } n \in \mathbb{N}.$$

Applying this to  $n = 1$ , we obtain

$$\begin{aligned}
\text{Coeff}_1(uv) &= \sum_{k=0}^1 \text{Coeff}_k u \cdot \text{Coeff}_{1-k} v \\
&= \underbrace{\text{Coeff}_0 u}_{=1} \cdot \text{Coeff}_1 v + \text{Coeff}_1 u \cdot \underbrace{\text{Coeff}_0 v}_{=1} \\
&= \text{Coeff}_1 v + \text{Coeff}_1 u = \underbrace{\text{Coeff}_1 u}_{\substack{=\text{coeff}_1 u \\ \text{(by (93), applied} \\ \text{to } P=u \text{ and } i=1)}} + \underbrace{\text{Coeff}_1 v}_{\substack{=\text{coeff}_1 v \\ \text{(by (93), applied} \\ \text{to } P=v \text{ and } i=1)}} \\
&= \text{coeff}_1 u + \text{coeff}_1 v.
\end{aligned}$$

Now, (93) (applied to  $P = uv$  and  $i = 1$ ) yields  $\text{coeff}_1(uv) = \text{Coeff}_1(uv) = \text{coeff}_1 u + \text{coeff}_1 v$ . Since  $u \hat{+} v = uv$ , this rewrites as  $\text{coeff}_1(u \hat{+} v) = \text{coeff}_1 u + \text{coeff}_1 v$ . This proves (90).

*Proof of (92):* Theorem 4.3 (b) (applied to  $n = 1$  and  $m = 1$ ) shows that

$$\prod_{(i,j) \in \{1\} \times \{1\}} (1 + U_i V_j T) = \sum_{k \in \mathbb{N}} P_k(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) T^k$$

in the polynomial ring  $(\mathbb{Z}[U_1, V_1])[T]$ . Hence,

$$\sum_{k \in \mathbb{N}} P_k(X_1, X_2, \dots, X_k, Y_1, Y_2, \dots, Y_k) T^k = \prod_{(i,j) \in \{1\} \times \{1\}} (1 + U_i V_j T) = 1 + U_1 V_1 T.$$

Comparing coefficients before  $T^1$  on both sides of this equality, we obtain  $P_1(X_1, Y_1) = U_1 V_1$ . But we are working in  $\mathbb{Z}[U_1, V_1]$ ; hence,  $X_1 = U_1$  and  $Y_1 = V_1$ . Thus,

$$P_1\left(\underbrace{X_1}_{=U_1}, \underbrace{Y_1}_{=V_1}\right) = P_1(U_1, V_1), \text{ so that } P_1(U_1, V_1) = P_1(X_1, Y_1) = U_1 V_1. \text{ Since } U_1$$

and  $V_1$  are algebraically independent, this yields  $P_1 = \alpha_1 \beta_1$ .

Now, write the formal power series  $u \in \Lambda(K) \subseteq K[[T]]$  in the form  $u = \sum_{i \in \mathbb{N}} a_i T^i$  (with  $a_i \in K$ ). Hence,  $\text{coeff}_1 u = a_1$ .

Also, write the formal power series  $v \in \Lambda(K) \subseteq K[[T]]$  in the form  $v = \sum_{i \in \mathbb{N}} b_i T^i$  (with  $b_i \in K$ ). Thus,  $\text{coeff}_1 v = b_1$ .

From  $u = \sum_{i \in \mathbb{N}} a_i T^i$  and  $v = \sum_{i \in \mathbb{N}} b_i T^i$ , we obtain

$$\begin{aligned}
u \hat{\cdot} v &= \left( \sum_{i \in \mathbb{N}} a_i T^i \right) \hat{\cdot} \left( \sum_{i \in \mathbb{N}} b_i T^i \right) = \sum_{k \in \mathbb{N}} P_k(a_1, a_2, \dots, a_k, b_1, b_2, \dots, b_k) T^k \\
&\quad \text{(by the definition of the operation } \hat{\cdot} \text{)}.
\end{aligned}$$

Hence,  $\text{coeff}_1(u \hat{\cdot} v) = P_1(a_1, b_1) = a_1 b_1$  (since  $P_1 = \alpha_1 \beta_1$ ). In view of  $\text{coeff}_1 u = a_1$  and  $\text{coeff}_1 v = b_1$ , this rewrites as  $\text{coeff}_1(u \hat{\cdot} v) = \text{coeff}_1 u \cdot \text{coeff}_1 v$ . This proves (92).

Now, all of the equalities (89), (90), (91) and (92) are proven. This completes the solution of Exercise 6.9.

*Exercise 6.10: Solution:* (a) Define a map  $\eta : A \times B \rightarrow C$  by

$$(\eta(a, b) = \alpha(a) \beta(b) \quad \text{for every } (a, b) \in A \times B).$$

This map  $\eta$  is  $\mathbb{Z}$ -bilinear (since the maps  $\alpha$  and  $\beta$  are  $\mathbb{Z}$ -linear). Thus, the universal property of the tensor product  $A \otimes B$  shows that there exists a unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow C$  satisfying

$$(\phi(a \otimes b) = \eta(a, b) \quad \text{for every } (a, b) \in A \times B).$$

Since  $\eta(a, b) = \alpha(a) \otimes \beta(b)$  for every  $(a, b) \in A \times B$ , this statement rewrites as follows: There exists a unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow C$  satisfying

$$(\phi(a \otimes b) = \alpha(a) \beta(b) \quad \text{for every } (a, b) \in A \times B).$$

This solves Exercise 6.10 (a).

(b) We have

$$\phi(a \otimes b) = \alpha(a) \beta(b) \quad \text{for every } (a, b) \in A \times B \quad (94)$$

(according to the definition of  $\phi$ ). Applying this to  $(a, b) = (1, 1)$ , we obtain

$$\phi(1 \otimes 1) = \underbrace{\alpha(1)}_{=1} \underbrace{\beta(1)}_{=1} = 1.$$

(since  $\alpha$  is a ring homomorphism) (since  $\beta$  is a ring homomorphism)

In other words, the map  $\phi$  sends the unity  $1 \otimes 1$  of  $A \otimes B$  to the unity 1 of  $C$ .

Next, we claim that

$$\phi(x) \phi(y) = \phi(xy) \quad (95)$$

for every  $x \in A \otimes B$  and  $y \in A \otimes B$ .

*Proof of (95):* Let  $x \in A \otimes B$  and  $y \in A \otimes B$ . We need to prove the equality (95). Since this equality is  $\mathbb{Z}$ -linear in each of  $x$  and  $y$ , we can WLOG assume that  $x$  and  $y$  are pure tensors (since the  $\mathbb{Z}$ -module  $A \otimes B$  is spanned by pure tensors). Assume this. Thus,  $x = a \otimes b$  and  $y = a' \otimes b'$  for some  $(a, b) \in A \times B$  and  $(a', b') \in A \times B$ . Consider these  $(a, b)$  and  $(a', b')$ .

Multiplying the equalities  $x = a \otimes b$  and  $y = a' \otimes b'$ , we obtain  $xy = (a \otimes b)(a' \otimes b') = aa' \otimes bb'$ . Applying the map  $\phi$  to both sides of this equality, we find

$$\begin{aligned} \phi(xy) &= \phi(aa' \otimes bb') \\ &= \underbrace{\alpha(aa')}_{=\alpha(a)\alpha(a')} \underbrace{\beta(bb')}_{=\beta(b)\beta(b')} \quad \left( \begin{array}{l} \text{by (94), applied to } (aa', bb') \\ \text{instead of } (a, b) \end{array} \right) \\ &\quad \text{(since } \alpha \text{ is a ring homomorphism) (since } \beta \text{ is a ring homomorphism)} \\ &= \alpha(a) \alpha(a') \beta(b) \beta(b') = \alpha(a) \beta(b) \alpha(a') \beta(b'). \end{aligned}$$

Comparing this with

$$\phi \left( \underbrace{x}_{=a \otimes b} \right) \phi \left( \underbrace{y}_{=a' \otimes b'} \right) = \underbrace{\phi(a \otimes b)}_{=\alpha(a)\beta(b)} \underbrace{\phi(a' \otimes b')}_{=\alpha(a')\beta(b')} = \alpha(a) \beta(b) \alpha(a') \beta(b'),$$

(by (94)) (by (94), applied to  $(a', b')$  instead of  $(a, b)$ )

we obtain  $\phi(x) \phi(y) = \phi(xy)$ . Thus, (95) is proven.

Now, we know that the map  $\phi$  is  $\mathbb{Z}$ -linear, sends the unity  $1 \otimes 1$  of  $A \otimes B$  to the unity 1 of  $C$ , and satisfies (95) for every  $x \in A \otimes B$  and  $y \in A \otimes B$ . In other words,  $\phi$  is a  $\mathbb{Z}$ -algebra homomorphism. In other words,  $\phi$  is a ring homomorphism.

Every  $a \in A$  satisfies

$$\begin{aligned} (\phi \circ \iota_1)(a) &= \phi \left( \underbrace{\iota_1(a)}_{=a \otimes 1} \right) = \phi(a \otimes 1) = \alpha(a) \underbrace{\beta(1)}_{=1} \\ &\quad \text{(by the definition of } \iota_1 \text{)} \quad \text{(since } \beta \text{ is a ring homomorphism)} \\ &\quad \text{(by (94), applied to } (a, 1) \text{ instead of } (a, b) \text{)} \\ &= \alpha(a). \end{aligned}$$

In other words,  $\phi \circ \iota_1 = \alpha$ . Similarly,  $\phi \circ \iota_2 = \beta$ . This completes the solution of Exercise 6.10 (b).

*Exercise 6.11: Solution:* The definition of  $\tau_T$  shows that  $\tau_T : A \otimes B \rightarrow \Lambda(A \otimes B)$  is a  $\mathbb{Z}$ -module homomorphism satisfying

$$\left( \begin{array}{l} \tau_T(a \otimes b) = (\Lambda(\iota_1) \circ \lambda_T)(a) \widehat{\cdot} (\Lambda(\iota_2) \circ \mu_T)(b) \\ \text{for every } (a, b) \in A \times B \end{array} \right). \quad (96)$$

For every  $i \in \mathbb{N}$  and every ring  $K$ , we define a mapping  $\text{coeff}_i : K[[T]] \rightarrow K$  as in Exercise 6.5. For every two rings  $K$  and  $L$ , every ring homomorphism  $f : K \rightarrow L$  and every  $i \in \mathbb{N}$ , we have

$$\text{coeff}_i \circ \Lambda(f) = f \circ \text{coeff}_i \quad (97)$$

<sup>91</sup>. (This follows from the definition of  $\Lambda(f)$ .)

For every ring two rings  $K$  and  $L$ , every ring homomorphism  $f : K \rightarrow L$  and every  $P \in \Lambda(K)$ , we have

$$(\Lambda(f))(P) = (f[[T]])(P). \quad (98)$$

(This follows from the fact that the definitions of the maps  $\Lambda(f)$  and  $f[[T]]$  are identical, except for the different domains.)

For every  $c \in A \otimes B$  and  $i \in \mathbb{N}$ , we have defined  $\tau^i(c)$  as the coefficient of the power series  $\tau_T(c) \in \Lambda(A \otimes B) \subseteq (A \otimes B)[[T]]$  before  $T^i$ . In other words, for every  $c \in A \otimes B$  and  $i \in \mathbb{N}$ , we have

$$\tau^i(c) = \text{coeff}_i(\tau_T(c)). \quad (99)$$

Thus,

$$\tau^i = \text{coeff}_i \circ \tau_T \quad \text{for each } i \in \mathbb{N} \quad (100)$$

---

<sup>91</sup>In other words, the diagram

$$\begin{array}{ccc} \Lambda(K) & \xrightarrow{\Lambda(f)} & \Lambda(L) \\ \text{coeff}_i \downarrow & & \downarrow \text{coeff}_i \\ K & \xrightarrow{f} & L \end{array}$$

is commutative.



92.

For every  $x \in A \otimes B$ , we have

$$\tau_T(x) = \sum_{i \in \mathbb{N}} \tau^i(x) T^i \quad (101)$$

93.

(a) We have

$$\tau^0(x) = 1 \quad \text{for every } x \in A \otimes B \quad (102)$$

94. Also,

$$\tau^1(x) = x \quad \text{for every } x \in A \otimes B \quad (103)$$

95. Thus, Theorem 2.1 (a) (applied to  $A \otimes B$ ,  $(\tau^i)_{i \in \mathbb{N}}$  and  $\tau_T$  instead of  $K$ ,  $(\lambda^i)_{i \in \mathbb{N}}$  and  $\lambda_T$ ) shows that we have

$$\tau_T(x) \cdot \tau_T(y) = \tau_T(x + y) \quad \text{for every } x \in A \otimes B \text{ and } y \in A \otimes B \quad (104)$$

if and only if  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring. Thus,  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring (because

---

<sup>92</sup>*Proof of (100):* Let  $i \in \mathbb{N}$ . Then, every  $c \in A \otimes B$  satisfies

$$\begin{aligned} \tau^i(c) &= \text{coeff}_i(\tau_T(c)) && \text{(by (99))} \\ &= (\text{coeff}_i \circ \tau_T)(c). \end{aligned}$$

In other words,  $\tau^i = \text{coeff}_i \circ \tau_T$ . This proves (100).

<sup>93</sup>*Proof of (101):* Let  $x \in A \otimes B$ . Recall that for every  $c \in A \otimes B$  and  $i \in \mathbb{N}$ , the coefficient of the power series  $\tau_T(c) \in \Lambda(A \otimes B) \subseteq (A \otimes B)[[T]]$  before  $T^i$  is  $\tau^i(c)$ . Applying this to  $c = x$ , we conclude that for every  $i \in \mathbb{N}$ , the coefficient of the power series  $\tau_T(x) \in \Lambda(A \otimes B) \subseteq (A \otimes B)[[T]]$  before  $T^i$  is  $\tau^i(x)$ . Hence,  $\tau_T(x) = \sum_{i \in \mathbb{N}} \tau^i(x) T^i$ . This proves (101).

<sup>94</sup>*Proof of (102):* Let  $x \in A \otimes B$ . Then,  $\tau_T(x) \in \Lambda(A \otimes B)$  (since  $\tau_T$  is a map  $A \otimes B \rightarrow \Lambda(A \otimes B)$ ). Hence,  $\tau_T(x)$  is a power series in  $(A \otimes B)[[T]]$  with constant term 1 (since  $\Lambda(A \otimes B)$  is the set of all such power series). Hence, the constant term of  $\tau_T(x)$  is 1. In other words,  $\text{coeff}_0(\tau_T(x)) = 1$ . But (99) (applied to  $c = x$  and  $i = 0$ ) yields  $\tau^0(x) = \text{coeff}_0(\tau_T(x)) = 1$ . This proves (102).

<sup>95</sup>*Proof of (103):* We have  $\tau^1 = \text{coeff}_1 \circ \tau_T$  (by (100), applied to  $i = 1$ ).

Exercise 6.5 (applied to  $K = A \otimes B$ ) shows that  $\text{coeff}_1 : \Lambda(A \otimes B) \rightarrow A \otimes B$  is a ring homomorphism. Hence,  $\text{coeff}_1 : \Lambda(A \otimes B) \rightarrow A \otimes B$  is a  $\mathbb{Z}$ -module homomorphism. Thus,  $\text{coeff}_1 \circ \tau_T : A \otimes B \rightarrow A \otimes B$  is a  $\mathbb{Z}$ -module homomorphism (since both  $\text{coeff}_1$  and  $\tau_T$  are  $\mathbb{Z}$ -module homomorphisms). In other words,  $\tau^1 : A \otimes B \rightarrow A \otimes B$  is a  $\mathbb{Z}$ -module homomorphism (since  $\tau^1 = \text{coeff}_1 \circ \tau_T$ ).

(104) holds<sup>96</sup>). This solves Exercise 6.11 (a).

(b) Let  $(C, (\nu^i)_{i \in \mathbb{N}})$  be a **special**  $\lambda$ -ring. Let  $\alpha : (A, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (C, (\nu^i)_{i \in \mathbb{N}})$  and  $\beta : (B, (\mu^i)_{i \in \mathbb{N}}) \rightarrow (C, (\nu^i)_{i \in \mathbb{N}})$  be two  $\lambda$ -ring homomorphisms. Consider the unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow C$  constructed in Exercise 6.10 (a). The definition of  $\phi$  shows that

$$(\phi(a \otimes b) = \alpha(a) \beta(b) \quad \text{for every } (a, b) \in A \times B). \quad (105)$$

Moreover, Exercise 6.10 (b) shows that this  $\phi$  is a ring homomorphism and satisfies

Every  $(a, b) \in A \times B$  satisfies

$$\begin{aligned} \tau^1(a \otimes b) &= \text{coeff}_1 \left( \begin{array}{c} \tau_T(a \otimes b) \\ =(\Lambda(\iota_1) \circ \lambda_T)(a) \widehat{+} (\Lambda(\iota_2) \circ \mu_T)(b) \\ \text{(by (96))} \end{array} \right) \quad \left( \begin{array}{l} \text{by (99), applied to } c = a \otimes b \\ \text{and } i = 1 \end{array} \right) \\ &= \text{coeff}_1((\Lambda(\iota_1) \circ \lambda_T)(a) \widehat{+} (\Lambda(\iota_2) \circ \mu_T)(b)) \\ &= \underbrace{\text{coeff}_1((\Lambda(\iota_1) \circ \lambda_T)(a))}_{= (\text{coeff}_1 \circ \Lambda(\iota_1))(\lambda_T(a))} \cdot \underbrace{\text{coeff}_1((\Lambda(\iota_2) \circ \mu_T)(b))}_{= (\text{coeff}_1 \circ \Lambda(\iota_2))(\mu_T(b))} \\ &\quad \text{(since } \text{coeff}_1 : \Lambda(A \otimes B) \rightarrow A \otimes B \text{ is a ring homomorphism)} \\ &= \underbrace{(\text{coeff}_1 \circ \Lambda(\iota_1))}_{= \iota_1 \circ \text{coeff}_1}(\lambda_T(a)) \cdot \underbrace{(\text{coeff}_1 \circ \Lambda(\iota_2))}_{= \iota_2 \circ \text{coeff}_1}(\mu_T(b)) \\ &\quad \text{(by (97), applied to } K=A, L=A \otimes B, f=\iota_1 \text{ and } i=1) \quad \text{(by (97), applied to } K=B, L=A \otimes B, f=\iota_2 \text{ and } i=1) \\ &= \underbrace{(\iota_1 \circ \text{coeff}_1)}_{= \iota_1(\text{coeff}_1(\lambda_T(a)))}(\lambda_T(a)) \cdot \underbrace{(\iota_2 \circ \text{coeff}_1)}_{= \iota_2(\text{coeff}_1(\mu_T(b)))}(\mu_T(b)) \\ &= \iota_1 \left( \begin{array}{c} \text{coeff}_1(\lambda_T(a)) \\ = \lambda^1(a) \\ \text{(since } \lambda_T(a) = \sum_{i \in \mathbb{N}} \lambda^i(a) T^i \\ \text{(by the definition of } \lambda_T)) \end{array} \right) \cdot \iota_2 \left( \begin{array}{c} \text{coeff}_1(\mu_T(b)) \\ = \mu^1(b) \\ \text{(since } \mu_T(b) = \sum_{i \in \mathbb{N}} \mu^i(b) T^i \\ \text{(by the definition of } \mu_T)) \end{array} \right) \\ &= \iota_1 \left( \begin{array}{c} \lambda^1(a) \\ = a \\ \text{(since } (A, (\lambda^i)_{i \in \mathbb{N}}) \\ \text{is a } \lambda\text{-ring)} \end{array} \right) \cdot \iota_2 \left( \begin{array}{c} \mu^1(b) \\ = b \\ \text{(since } (B, (\mu^i)_{i \in \mathbb{N}}) \\ \text{is a } \lambda\text{-ring)} \end{array} \right) = \underbrace{\iota_1(a)}_{= a \otimes 1} \cdot \underbrace{\iota_2(b)}_{= 1 \otimes b} \\ &\quad \text{(by the definition of } \iota_1) \quad \text{(by the definition of } \iota_2) \\ &= (a \otimes 1) \cdot (1 \otimes b) = a \otimes b = \text{id}(a \otimes b). \end{aligned}$$

In other words, the two maps  $\tau^1 : A \otimes B \rightarrow A \otimes B$  and  $\text{id} : A \otimes B \rightarrow A \otimes B$  are equal to each other on each pure tensor. Since these two maps are  $\mathbb{Z}$ -module homomorphisms, this entails that these two maps must be identical (because the pure tensors span the  $\mathbb{Z}$ -module  $A \otimes B$ ). In other words,  $\tau^1 = \text{id}$ . In other words,  $\tau^1(x) = x$  for every  $x \in A \otimes B$ . This proves (103).

<sup>96</sup>*Proof of (104):* Let  $x \in A \otimes B$  and  $y \in A \otimes B$ . Recall that the addition  $\widehat{+}$  of the ring  $\Lambda(A \otimes B)$  is defined by the rule that  $u \widehat{+} v = uv$  for all  $u \in \Lambda(A \otimes B)$  and  $v \in \Lambda(A \otimes B)$ . Applying this rule to  $u = \tau_T(x)$  and  $v = \tau_T(y)$ , we obtain  $\tau_T(x) \widehat{+} \tau_T(y) = \tau_T(x) \cdot \tau_T(y)$ . Thus,

$$\tau_T(x) \cdot \tau_T(y) = \tau_T(x) \widehat{+} \tau_T(y) = \tau_T(x + y)$$

(since the map  $\tau_T$  is a  $\mathbb{Z}$ -module homomorphism). This proves (104).

$\phi \circ \iota_1 = \alpha$  and  $\phi \circ \iota_2 = \beta$ . Since  $\phi : A \otimes B \rightarrow C$  is a ring homomorphism, we see that  $\Lambda(\phi) : \Lambda(A \otimes B) \rightarrow \Lambda(C)$  is a  $\lambda$ -ring homomorphism and therefore a ring homomorphism.

Since  $\Lambda$  is a functor, we have  $\Lambda(\phi) \circ \Lambda(\iota_1) = \Lambda\left(\underbrace{\phi \circ \iota_1}_{=\alpha}\right) = \Lambda(\alpha)$  and  $\Lambda(\phi) \circ \Lambda(\iota_2) = \Lambda\left(\underbrace{\phi \circ \iota_2}_{=\beta}\right) = \Lambda(\beta)$ .

Define a map  $\nu_T : C \rightarrow \Lambda(C)$  by

$$\nu_T(x) = \sum_{i \in \mathbb{N}} \nu^i(x) T^i \quad \text{for every } x \in C.$$

Notice that  $(C, (\nu^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring if and only if the map  $\nu_T : (C, (\nu^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(C), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (by the definition of a ‘‘special  $\lambda$ -ring’’).

Thus, the map  $\nu_T : (C, (\nu^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(C), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (since  $(C, (\nu^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring). In particular,  $\nu_T$  is a ring homomorphism, and thus is a  $\mathbb{Z}$ -module homomorphism. Thus, all four maps  $\tau_T, \phi, \nu_T$  and  $\Lambda(\phi)$  are  $\mathbb{Z}$ -module homomorphisms. Hence, the compositions  $\Lambda(\phi) \circ \tau_T$  and  $\nu_T \circ \phi$  are  $\mathbb{Z}$ -module homomorphisms as well.

Theorem 2.1 (c) (applied to  $(A, (\lambda^i)_{i \in \mathbb{N}})$ ,  $\lambda_T$ ,  $(C, (\nu^i)_{i \in \mathbb{N}})$ ,  $\nu_T$  and  $\alpha$  instead of  $(K, (\lambda^i)_{i \in \mathbb{N}})$ ,  $\lambda_T$ ,  $(L, (\mu^i)_{i \in \mathbb{N}})$ ,  $\mu_T$  and  $f$ ) shows that  $\alpha$  is a  $\lambda$ -ring homomorphism if and only if  $\nu_T \circ \alpha = \alpha[[T]] \circ \lambda_T$ . Since  $\alpha$  is a  $\lambda$ -ring homomorphism, we therefore conclude that

$$\nu_T \circ \alpha = \alpha[[T]] \circ \lambda_T. \quad (106)$$

Similarly, using the fact that  $\beta$  is a  $\lambda$ -ring homomorphism, we can prove that

$$\nu_T \circ \beta = \beta[[T]] \circ \mu_T. \quad (107)$$

Now, we shall prove that the diagram

$$\begin{array}{ccc} A \otimes B & \xrightarrow{\phi} & C \\ \tau_T \downarrow & & \downarrow \nu_T \\ \Lambda(A \otimes B) & \xrightarrow{\Lambda(\phi)} & \Lambda(C) \end{array} \quad (108)$$

is commutative.

Indeed, every  $(a, b) \in A \times B$  satisfies

$$\begin{aligned}
& (\Lambda(\phi) \circ \tau_T)(a \otimes b) \\
&= (\Lambda(\phi)) \left( \underbrace{\tau_T(a \otimes b)}_{\substack{=(\Lambda(\iota_1) \circ \lambda_T)(a) \widehat{\cdot} (\Lambda(\iota_2) \circ \mu_T)(b) \\ \text{(by (96))}}} \right) \\
&= (\Lambda(\phi)) \left( (\Lambda(\iota_1) \circ \lambda_T)(a) \widehat{\cdot} (\Lambda(\iota_2) \circ \mu_T)(b) \right) \\
&= \underbrace{(\Lambda(\phi)) \left( (\Lambda(\iota_1) \circ \lambda_T)(a) \right)}_{\substack{=(\Lambda(\phi) \circ \Lambda(\iota_1) \circ \lambda_T)(a) \\ \text{(since } \Lambda(\phi) \text{ is a ring homomorphism)}}} \widehat{\cdot} \underbrace{(\Lambda(\phi)) \left( (\Lambda(\iota_2) \circ \mu_T)(b) \right)}_{=(\Lambda(\phi) \circ \Lambda(\iota_2) \circ \mu_T)(b)} \\
&= \left( \underbrace{\Lambda(\phi) \circ \Lambda(\iota_1) \circ \lambda_T}_{=\Lambda(\alpha)}(a) \right) \widehat{\cdot} \left( \underbrace{\Lambda(\phi) \circ \Lambda(\iota_2) \circ \mu_T}_{=\Lambda(\beta)}(b) \right) \\
&= \underbrace{(\Lambda(\alpha) \circ \lambda_T)(a)}_{\substack{=(\Lambda(\alpha))(\lambda_T(a)) \\ =(\alpha[[T]])(\lambda_T(a)) \\ \text{(by (98), applied to} \\ K=A, L=C, f=\alpha \text{ and } P=\lambda_T(a))}} \widehat{\cdot} \underbrace{(\Lambda(\beta) \circ \mu_T)(b)}_{\substack{=(\Lambda(\beta))(\mu_T(b)) \\ =(\beta[[T]])(\mu_T(b)) \\ \text{(by (98), applied to} \\ K=B, L=C, f=\beta \text{ and } P=\mu_T(b))}} \\
&= \underbrace{(\alpha[[T]])(\lambda_T(a))}_{=(\alpha[[T]] \circ \lambda_T)(a)} \widehat{\cdot} \underbrace{(\beta[[T]])(\mu_T(b))}_{=(\beta[[T]] \circ \mu_T)(b)} = \underbrace{(\alpha[[T]] \circ \lambda_T)(a)}_{\substack{=\nu_T \circ \alpha \\ \text{(by (106))}}} \widehat{\cdot} \underbrace{(\beta[[T]] \circ \mu_T)(b)}_{\substack{=\nu_T \circ \beta \\ \text{(by (107))}}} \\
&= \underbrace{(\nu_T \circ \alpha)(a)}_{=\nu_T(\alpha(a))} \widehat{\cdot} \underbrace{(\nu_T \circ \beta)(b)}_{=\nu_T(\beta(b))} = \nu_T(\alpha(a)) \widehat{\cdot} \nu_T(\beta(b)) \\
&= \nu_T \left( \underbrace{\alpha(a) \beta(b)}_{\substack{=\phi(a \otimes b) \\ \text{(by (105))}}} \right) \quad \text{(since } \nu_T : C \rightarrow \Lambda(C) \text{ is a ring homomorphism)} \\
&= \nu_T(\phi(a \otimes b)) = (\nu_T \circ \phi)(a \otimes b).
\end{aligned}$$

In other words, the two maps  $\Lambda(\phi) \circ \tau_T$  and  $\nu_T \circ \phi$  are equal to each other on each pure tensor in  $A \otimes B$ . Since these two maps are  $\mathbb{Z}$ -module homomorphisms, this entails that these two maps must be identical (since the  $\mathbb{Z}$ -module  $A \otimes B$  is spanned by the pure tensors). In other words,  $\Lambda(\phi) \circ \tau_T = \nu_T \circ \phi$ . This proves that the diagram (108) is commutative.

From this, it is easy to see that

$$\nu_T \circ \phi = \phi[[T]] \circ \tau_T$$

Now, Theorem 2.1 (c) (applied to  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$ ,  $\tau_T$ ,  $(C, (\nu^i)_{i \in \mathbb{N}})$ ,  $\nu_T$  and  $\phi$  instead of  $(K, (\lambda^i)_{i \in \mathbb{N}})$ ,  $\lambda_T$ ,  $(L, (\mu^i)_{i \in \mathbb{N}})$ ,  $\mu_T$  and  $f$ ) shows that  $\phi$  is a  $\lambda$ -ring homomorphism if and only if  $\nu_T \circ \phi = \phi [[T]] \circ \tau_T$ . Therefore,  $\phi$  is a  $\lambda$ -ring homomorphism (since we have  $\nu_T \circ \phi = \phi [[T]] \circ \tau_T$ ). This solves Exercise 6.11 (b).

(c) Assume that the  $\lambda$ -rings  $(A, (\lambda^i)_{i \in \mathbb{N}})$  and  $(B, (\mu^i)_{i \in \mathbb{N}})$  are special. Notice that  $(A, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring if and only if the map  $\lambda_T : (A, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (by the definition of a “special  $\lambda$ -ring”). Thus, the map  $\lambda_T : (A, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (since  $(A, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring). In particular,  $\lambda_T$  is a ring homomorphism. Hence,  $\lambda_T$  sends the unity 1 of the ring  $A$  to the unity  $1 + T$  of the ring  $\Lambda(A)$ . In other words,  $\lambda_T(1) = 1 + T$ . Similarly,  $\mu_T(1) = 1 + T$  (because the  $\lambda$ -ring  $(B, (\mu^i)_{i \in \mathbb{N}})$  is special).

But  $\iota_2$  is a ring homomorphism, and thus  $\Lambda(\iota_2)$  is a  $\lambda$ -ring homomorphism. Hence,  $\Lambda(\iota_2)$  is a ring homomorphism. Thus,  $\Lambda(\iota_2)$  sends the unity  $1 + T$  of the ring  $\Lambda(B)$  to the unity  $1 + T$  of the ring  $\Lambda(A \otimes B)$ . In other words,  $(\Lambda(\iota_2))(1 + T) = 1 + T$ . Now,

$$(\Lambda(\iota_2) \circ \mu_T)(1) = (\Lambda(\iota_2)) \left( \underbrace{\mu_T(1)}_{=1+T} \right) = (\Lambda(\iota_2))(1 + T) = 1 + T. \quad (109)$$

Now, we claim that

$$\tau_T \circ \iota_1 = \iota_1 [[T]] \circ \lambda_T \quad (110)$$

*Proof of (110):* Let  $a \in A$ . Then,  $\lambda_T(a) \in \Lambda(A)$ . Hence, (98) (applied to  $K = A$ ,  $L = A \otimes B$ ,  $f = \iota_1$  and  $P = \lambda_T(a)$ ) yields

$$(\Lambda(\iota_1))(\lambda_T(a)) = (\iota_1 [[T]]) (\lambda_T(a)) = (\iota_1 [[T]] \circ \lambda_T)(a).$$

But the definition of  $\iota_1$  yields  $\iota_1(a) = a \otimes 1$ . Now,

$$\begin{aligned} (\tau_T \circ \iota_1)(a) &= \tau_T \left( \underbrace{\iota_1(a)}_{=a \otimes 1} \right) = \tau_T(a \otimes 1) = \underbrace{(\Lambda(\iota_1) \circ \lambda_T)(a)}_{\substack{= (\Lambda(\iota_1))(\lambda_T(a)) \\ = (\iota_1 [[T]] \circ \lambda_T)(a)}} \widehat{\underbrace{(\Lambda(\iota_2) \circ \mu_T)(1)}_{\substack{=1+T \\ \text{(by (109))}}}} \\ &\quad \text{(by (96), applied to } (a, 1) \text{ instead of } (a, b)) \\ &= (\iota_1 [[T]] \circ \lambda_T)(a) \widehat{(1 + T)} = (\iota_1 [[T]] \circ \lambda_T)(a) \\ &\quad \text{(since } 1 + T \text{ is the unity of the ring } \Lambda(A \otimes B)). \end{aligned}$$

---

<sup>97</sup>*Proof.* Every  $x \in A \otimes B$  satisfies

$$\begin{aligned} &\underbrace{(\nu_T \circ \phi)}_{\substack{= \Lambda(\phi) \circ \tau_T \\ \text{(since the diagram} \\ \text{(108) is commutative)}}} (x) \\ &= (\Lambda(\phi) \circ \tau_T)(x) = (\Lambda(\phi))(\tau_T(x)) = (\phi [[T]]) (\tau_T(x)) \\ &\quad \text{(by (98), applied to } K = A \otimes B, L = C, f = \phi \text{ and } P = \tau_T(x)) \\ &= (\phi [[T]] \circ \tau_T)(x). \end{aligned}$$

Hence,  $\nu_T \circ \phi = \phi [[T]] \circ \tau_T$ , qed.

Now, forget that we fixed  $a$ . We thus have shown that  $(\tau_T \circ \iota_1)(a) = (\iota_1 [[T]] \circ \lambda_T)(a)$  for every  $a \in A$ . In other words,  $\tau_T \circ \iota_1 = \iota_1 [[T]] \circ \lambda_T$ . This proves (110).

Now, Theorem 2.1 (c) (applied to  $(A, (\lambda^i)_{i \in \mathbb{N}})$ ,  $\lambda_T$ ,  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$ ,  $\tau_T$  and  $\iota_1$  instead of  $(K, (\lambda^i)_{i \in \mathbb{N}})$ ,  $\lambda_T$ ,  $(L, (\mu^i)_{i \in \mathbb{N}})$ ,  $\mu_T$  and  $f$ ) shows that  $\iota_1$  is a  $\lambda$ -ring homomorphism if and only if  $\tau_T \circ \iota_1 = \iota_1 [[T]] \circ \lambda_T$ . Therefore,  $\iota_1$  is a  $\lambda$ -ring homomorphism (since we have  $\tau_T \circ \iota_1 = \iota_1 [[T]] \circ \lambda_T$ ). Similarly,  $\iota_2$  is a  $\lambda$ -ring homomorphism. This solves Exercise 6.11 (c).

(d) Assume that the  $\lambda$ -rings  $(A, (\lambda^i)_{i \in \mathbb{N}})$  and  $(B, (\mu^i)_{i \in \mathbb{N}})$  are special. Notice that  $(A, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring if and only if the map  $\lambda_T : (A, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (by the definition of a “special  $\lambda$ -ring”). Thus, the map  $\lambda_T : (A, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (since  $(A, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring). Similarly, the map  $\mu_T : (B, (\mu^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(B), (\widehat{\mu}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism.

The map  $\iota_1 : A \rightarrow A \otimes B$  is a ring homomorphism; thus, the map  $\Lambda(\iota_1) : (\Lambda(A), (\widehat{\lambda}^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism. Hence,  $\Lambda(\iota_1) \circ \lambda_T : (A, (\lambda^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (being the composition of the two  $\lambda$ -ring homomorphisms  $\lambda_T$  and  $\Lambda(\iota_1)$ ). Similarly,  $\Lambda(\iota_2) \circ \mu_T : (B, (\mu^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism. Also,  $(\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring (by Theorem 6.2, applied to  $K = A \otimes B$ ). Therefore, Exercise 6.11 (b) (applied to  $(\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$ ,  $\Lambda(\iota_1) \circ \lambda_T$ ,  $\Lambda(\iota_2) \circ \mu_T$  and  $\tau_T$  instead of  $(C, (\nu^i)_{i \in \mathbb{N}})$ ,  $\alpha$ ,  $\beta$  and  $\phi$ ) shows that the unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow \Lambda(A \otimes B)$  constructed in Exercise 6.10 (a) (applied to  $C = \Lambda(A \otimes B)$ ,  $\alpha = \Lambda(\iota_1) \circ \lambda_T$  and  $\beta = \Lambda(\iota_2) \circ \mu_T$ ) is a  $\lambda$ -ring homomorphism  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$ . Since this unique  $\mathbb{Z}$ -module homomorphism  $\phi : A \otimes B \rightarrow \Lambda(A \otimes B)$  is our map  $\tau_T$  (because this is how we defined  $\tau_T$ ), we can rewrite this as follows: The map  $\tau_T$  is a  $\lambda$ -ring homomorphism  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$ .

But the  $\lambda$ -ring  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$  is special if and only if the map  $\tau_T : (A \otimes B, (\tau^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism (by the definition of a “special  $\lambda$ -ring”). Thus, the  $\lambda$ -ring  $(A \otimes B, (\tau^i)_{i \in \mathbb{N}})$  is special (since the map  $\tau_T : (A \otimes B, (\tau^i)_{i \in \mathbb{N}}) \rightarrow (\Lambda(A \otimes B), (\widehat{\lambda}^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring homomorphism). This solves Exercise 6.11 (d).

## 11.7. To Section 7

*Exercise 7.1: Hints to solution:* See the more general Exercise 7.2.

*Exercise 7.2: Hints to solution:* Repeat the argument used in the proof of Theorem 7.3.

## 11.8. To Section 8

*Exercise 8.1: Solution:* We need to prove that  $\text{coeff}_1 : \Lambda(K) \rightarrow K$  is a ring homomorphism. In order to prove this, we must verify that

$$\text{coeff}_1(1) = 0; \quad (111)$$

$$\text{coeff}_1(u\hat{+}v) = \text{coeff}_1 u + \text{coeff}_1 v \quad \text{for every } u \in \Lambda(K) \text{ and } v \in \Lambda(K); \quad (112)$$

$$\text{coeff}_1(1+T) = 1; \quad (113)$$

$$\text{coeff}_1(u\hat{\cdot}v) = \text{coeff}_1 u \cdot \text{coeff}_1 v \quad \text{for every } u \in \Lambda(K) \text{ and } v \in \Lambda(K). \quad (114)$$

The equations (111) and (113) are immediately obvious. In order to verify the equations (112) and (114), we notice that  $\text{coeff}_1 : \Lambda(K) \rightarrow K$  is a continuous mapping (with respect to the  $(T)$ -topology on  $\Lambda(K)$  and *any arbitrary topology* on  $K$ ) and the operations  $\hat{+}$  and  $\hat{\cdot}$  are continuous as well (by Theorem 5.5 (d)), and the subset  $1 + K[T]^+$  of  $1 + K[[T]]^+ = \Lambda(K)$  is dense (by Theorem 5.5 (a)), so it suffices to verify the equations (112) and (114) for  $u \in 1 + K[T]^+$  and  $v \in 1 + K[T]^+$  only.<sup>98</sup> So let  $u \in 1 + K[T]^+$  and  $v \in 1 + K[T]^+$ .

Then, there exist some  $(\tilde{K}_u, [u_1, u_2, \dots, u_m]) \in K^{\text{int}}$  such that  $u = \Pi(\tilde{K}_u, [u_1, u_2, \dots, u_m])$ , and some  $(\tilde{K}_v, [v_1, v_2, \dots, v_n]) \in K^{\text{int}}$  such that  $v = \Pi(\tilde{K}_v, [v_1, v_2, \dots, v_n])$ . Obviously,

$$u = \Pi(\tilde{K}, [u_1, u_2, \dots, u_m]) = \prod_{i=1}^m (1 + u_i T) = 1 + \sum_{i=1}^m u_i \cdot T + (\text{higher powers of } T)$$

yields  $\text{coeff}_1 u = \sum_{i=1}^m u_i$ . Similarly,  $\text{coeff}_1 v = \sum_{j=1}^n v_j$ .

By Theorem 5.3 (a), there exists a finite-free extension ring  $\tilde{K}_{u,v}$  of  $K$  which contains both  $\tilde{K}_u$  and  $\tilde{K}_v$  as subrings. Theorem 5.3 (c) yields

$$\begin{aligned} u\hat{\cdot}v &= \Pi(\tilde{K}_{u,v}, [u_i v_j \mid (i, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}]) = \prod_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} (1 + u_i v_j T) \\ &= 1 + \sum_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} u_i v_j \cdot T + (\text{higher powers of } T), \end{aligned}$$

and thus

$$\text{coeff}_1(u\hat{\cdot}v) = \sum_{(i,j) \in \{1,2,\dots,m\} \times \{1,2,\dots,n\}} u_i v_j = \sum_{i=1}^m \sum_{j=1}^n u_i v_j = \underbrace{\sum_{i=1}^m u_i}_{=\text{coeff}_1 u} \underbrace{\sum_{j=1}^n v_j}_{=\text{coeff}_1 v} = \text{coeff}_1 u \cdot \text{coeff}_1 v,$$

so that (114) is proven.

<sup>98</sup>At this point, we are slightly cheating: This argument works only if the topological space  $K$  is Hausdorff. Thus we are not completely free in choosing the topology on  $K$ . However, there are still enough Hausdorff topologies on  $K$  (for example, the discrete topology) to choose from - the argument works if we take any of them.

Besides,

$$\begin{aligned} u \widehat{+} v &= uv = \Pi \left( \widetilde{K}_u, [u_1, u_2, \dots, u_m] \right) \cdot \Pi \left( \widetilde{K}_v, [v_1, v_2, \dots, v_n] \right) \\ &= \prod_{i=1}^m (1 + u_i T) \cdot \prod_{j=1}^n (1 + v_j T) = 1 + \left( \sum_{i=1}^m u_i + \sum_{j=1}^n v_j \right) \cdot T + (\text{higher powers of } T), \end{aligned}$$

and consequently

$$\text{coeff}_1(u \widehat{+} v) = \underbrace{\sum_{i=1}^m u_i}_{=\text{coeff}_1 u} + \underbrace{\sum_{j=1}^n v_j}_{=\text{coeff}_1 v} = \text{coeff}_1 u + \text{coeff}_1 v,$$

and (112) is proven. Thus,  $\text{coeff}_1 : \Lambda(K) \rightarrow K$  is a ring homomorphism, and Exercise 6.9 is solved again. Thus, Exercise 8.1 is solved.

*Exercise 8.2: Hints to solution:* Let  $y = x^{-1}$ . We proceed as in the proof of Theorem 8.3 (b), except that we don't know that  $\lambda_T(y) = \Pi(K, [y])$  and thus cannot conclude anything from this. Instead,  $xy = xx^{-1} = 1$  yields

$$\begin{aligned} \lambda_T(xy) &= \lambda_T(1) = 1 + T && \left( \begin{array}{l} \text{since } \lambda_T : K \rightarrow \Lambda(K) \text{ is a ring homomorphism,} \\ \text{and } 1 + T \text{ is the multiplicative unity of } \Lambda(K) \end{array} \right) \\ &= 1 + xyT = \Pi(K, [xy]) = \Pi(K, [x]) \widehat{\cdot} \Pi(K, [y]) && \text{(by Theorem 5.3 (c))} \\ &= \lambda_T(x) \widehat{\cdot} (1 + yT). \end{aligned}$$

Together with  $\lambda_T(xy) = \lambda_T(x) \widehat{\cdot} \lambda_T(y)$ , this yields  $\lambda_T(x) \widehat{\cdot} \lambda_T(y) = \lambda_T(x) \widehat{\cdot} (1 + yT)$ , so that  $\lambda_T(y) = 1 + yT$  (since  $\lambda_T(x) \in \Lambda(K)$  is invertible, because  $x \in K$  is invertible and  $\lambda_T : K \rightarrow \Lambda(K)$  is a ring homomorphism), and Theorem 8.3 (a) yields that  $y$  is 1-dimensional, qed.

*Exercise 8.3: Hints to solution:* We notice first that every  $x \in E$  is 1-dimensional (by the assumption on  $E$ ). Thus, for every  $x \in E$ , we have  $\lambda_T(x) = 1 + xT$  (by Theorem 8.3 (a)). Thus, for every  $x \in E$ , the element  $\lambda_T(x)$  of  $\Lambda(K)$  is 1-dimensional (since Theorem 8.3 (c) shows that the element  $1 + xT$  of  $\Lambda(K)$  is 1-dimensional). In other words, for every  $x \in E$ , we have  $\widehat{\lambda}^j(\lambda_T(x)) = 1$  for every integer  $j > 1$  (since 1 is the zero of the ring  $\Lambda(K)$ ). Hence, for every  $x \in E$ , we have

$$\widehat{\lambda}^j(\lambda_T(x)) = \begin{cases} 1 + T, & \text{if } j = 0; \\ \lambda_T(x), & \text{if } j = 1; \\ 1, & \text{if } j > 1 \end{cases} \quad \text{for every } j \in \mathbb{N}. \quad (115)$$

On the other hand, every  $x \in E$  is 1-dimensional. In other words, every  $x \in E$  satisfies  $\lambda^j(x) = 0$  for every integer  $j > 1$ . Hence, every  $x \in E$  satisfies

$$\lambda^j(x) = \begin{cases} 1, & \text{if } j = 0; \\ x, & \text{if } j = 1; \\ 0, & \text{if } j > 1 \end{cases} \quad \text{for every } j \in \mathbb{N}. \quad (116)$$

We want to show that the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special. According to Exercise 6.4, we only have to prove that (30) and (31) hold. This is equivalent to showing that

$$\begin{aligned} \lambda_T(xy) &= \lambda_T(x) \widehat{\cdot} \lambda_T(y) && \text{for every } x \in E \text{ and } y \in E, && \text{and} \\ \lambda_T(\lambda^j(x)) &= \widehat{\lambda}^j(\lambda_T(x)) && \text{for every } j \in \mathbb{N} \text{ and } x \in E \end{aligned}$$



(because of the definitions of  $\widehat{\cdot}$  and  $\widehat{\lambda}^j$  and since two formal power series are equal if and only if their respective coefficients are equal). But this is true, since

$$\begin{aligned}\lambda_T(xy) &= 1 + xyT && \text{(since } xy \text{ is 1-dimensional (by Theorem 8.3 (b)))} \\ &= \Pi(K, [xy]) = \Pi(K, [x]) \widehat{\cdot} \Pi(K, [y]) && \text{(by Theorem 5.3 (c))} \\ &= (1 + xT) \cdot (1 + yT) = \lambda_T(x) \widehat{\cdot} \lambda_T(y) && \text{(since } x \text{ and } y \text{ are 1-dimensional)}\end{aligned}$$

for every  $x \in E$  and  $y \in E$ , and since

$$\begin{aligned}\lambda_T(\lambda^j(x)) &= \lambda_T\left(\begin{cases} 1, & \text{if } j = 0; \\ x, & \text{if } j = 1; \\ 0, & \text{if } j > 1 \end{cases}\right) && \text{(by (116))} \\ &= \begin{cases} \lambda_T(1), & \text{if } j = 0; \\ \lambda_T(x), & \text{if } j = 1; \\ \lambda_T(0), & \text{if } j > 1 \end{cases} = \begin{cases} 1 + T, & \text{if } j = 0; \\ \lambda_T(x), & \text{if } j = 1; \\ 1, & \text{if } j > 1 \end{cases} && \left(\begin{array}{l} \text{since } \lambda_T(1) = 1 + T \\ \text{and } \lambda_T(0) = 1 \end{array}\right) \\ &= \widehat{\lambda}^j(\lambda_T(x)) && \text{(by (115))}\end{aligned}$$

for every  $j \in \mathbb{N}$  and  $x \in E$ .

## 11.9. To Section 9

*Exercise 9.1: Hints to solution:* As before, we use the  $\widehat{\sum}$  sign for summation inside the ring  $\Lambda(K)$ . We remember that the addition inside the ring  $\Lambda(K)$  was defined by  $u \widehat{+} v = uv$  for any  $u \in \Lambda(K)$  and  $v \in \Lambda(K)$  (in other words, addition in  $\Lambda(K)$  is the multiplication inherited from  $K[[T]]$ ), so that  $\widehat{\sum} = \prod$ . Now,

$$u = \Pi\left(\widetilde{K}_u, [u_1, u_2, \dots, u_m]\right) = \prod_{i=1}^m (1 + u_i T) = \widehat{\sum}_{i=1}^m (1 + u_i T).$$

But since  $1 + u_i T$  is a 1-dimensional element of  $\Lambda(\widetilde{K}_u)$  for every  $i \in \{1, 2, \dots, m\}$  (by Theorem 8.3 (c)), Theorem 9.4 (applied to  $1 + u_i T$  and  $\Lambda(\widetilde{K}_u)$  instead of  $u_i$  and  $K$ ) yields

$$\widehat{\psi}^j \left( \widehat{\sum}_{i=1}^m (1 + u_i T) \right) = \widehat{\sum}_{i=1}^m (1 + u_i T)^{\widehat{j}},$$

where  $(1 + u_i T)^{\widehat{j}}$  means the  $j$ -th power of  $1 + u_i T$  in the ring  $\Lambda(\widetilde{K}_u)$  (in other words,

$$(1 + u_i T)^{\widehat{j}} = \underbrace{(1 + u_i T) \widehat{\cdot} (1 + u_i T) \widehat{\cdot} \dots \widehat{\cdot} (1 + u_i T)}_{j \text{ times}}, \text{ as opposed to}$$

$$(1 + u_i T)^j = \underbrace{(1 + u_i T) \cdot (1 + u_i T) \cdot \dots \cdot (1 + u_i T)}_{j \text{ times}} \text{ which is the } j\text{-th power of } 1 + u_i T \text{ in}$$

the ring  $\widetilde{K}_u[[T]]$ .

Hence,

$$\begin{aligned}\widehat{\psi}^j(u) &= \widehat{\psi}^j\left(\widehat{\sum_{i=1}^m (1+u_i T)}\right) = \widehat{\sum_{i=1}^m (1+u_i T)}^{\widehat{j}} = \widehat{\sum_{i=1}^m \underbrace{\left(\Pi\left(\widetilde{K}_u, [u_i]\right)\right)}_{=\Pi\left(\widetilde{K}_u, [u_i^j]\right) \text{ by Corollary 5.4 (b)}}^{\widehat{j}} = \widehat{\sum_{i=1}^m \Pi\left(\widetilde{K}_u, [u_i^j]\right)} \\ &= \Pi\left(\widetilde{K}_u, [u_1^j, u_2^j, \dots, u_m^j]\right) \quad (\text{by Corollary 5.4 (a)}).\end{aligned}$$

*Exercise 9.2: Hints to solution:* **(a)** It is easy to see that the map sends the zero 1 of  $\Lambda(K)$  to the zero 0 of  $K$  and the multiplicative unity  $1+T$  of  $\Lambda(K)$  to the multiplicative unity 1 of  $K$ . So it only remains to prove that any two power series  $u \in \Lambda(K)$  and  $v \in \Lambda(K)$  satisfy

$$(-1)^i \text{Coeff}_i\left(-T \frac{d}{dT} \log(u \widehat{+} v)\right) = (-1)^i \text{Coeff}_i\left(-T \frac{d}{dT} \log u\right) + (-1)^i \text{Coeff}_i\left(-T \frac{d}{dT} \log v\right) \quad (117)$$

and

$$(-1)^i \text{Coeff}_i\left(-T \frac{d}{dT} \log(u \widehat{v})\right) = (-1)^i \text{Coeff}_i\left(-T \frac{d}{dT} \log u\right) \cdot (-1)^i \text{Coeff}_i\left(-T \frac{d}{dT} \log v\right). \quad (118)$$

This needs to be verified for  $u \in 1 + K[T]^+$  and  $v \in 1 + K[T]^+$  only (since the operations  $\widehat{+}$  and  $\widehat{\cdot}$  and the mapping

$$\begin{aligned}\Lambda(K) &\rightarrow K, \\ u &\mapsto (-1)^i \text{Coeff}_i\left(-T \frac{d}{dT} \log u\right)\end{aligned}$$

are continuous (where the topology on  $K$  can be chosen arbitrarily), and  $1 + K[T]^+$  is a dense subset of  $1 + K[[T]]^+ = \Lambda(K)$ <sup>99</sup>. So let us assume that  $u \in 1 + K[T]^+$  and  $v \in 1 + K[T]^+$ . Then, there exists some  $\left(\widetilde{K}_u, [u_1, u_2, \dots, u_m]\right) \in K^{\text{int}}$  such that  $u = \Pi\left(\widetilde{K}_u, [u_1, u_2, \dots, u_m]\right)$  and some  $\left(\widetilde{K}_v, [v_1, v_2, \dots, v_n]\right) \in K^{\text{int}}$  such that  $v = \Pi\left(\widetilde{K}_v, [v_1, v_2, \dots, v_n]\right)$ . Then, Theorem 5.3 **(c)** yields that

$$u \widehat{v} = \Pi\left(\widetilde{K}_{u,v}, [u_\ell v_j \mid (\ell, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}]\right)$$

(here, we renamed the index  $i$  as  $\ell$  in Theorem 5.3 **(c)**, because we are already using the label  $i$  for a fixed element of  $\mathbb{N} \setminus \{0\}$ ).

Now,

$$u = \Pi\left(\widetilde{K}_u, [u_1, u_2, \dots, u_m]\right) = \prod_{k=1}^m (1 + u_k T)$$

<sup>99</sup>At this point, we are slightly cheating: This argument works only if the topological space  $K$  is Hausdorff. Thus we are not completely free in choosing the topology on  $K$ . However, there are still enough Hausdorff topologies on  $K$  (for example, the discrete topology) to choose from, and the argument works if we take any of them.

entails

$$\begin{aligned}
\frac{d}{dT}u &= \frac{d}{dT} \prod_{k=1}^m (1 + u_k T) \\
&= \sum_{\tau=1}^m \underbrace{\prod_{k \in \{1,2,\dots,m\} \setminus \{\tau\}} (1 + u_k T)}_{= \frac{\prod_{k=1}^m (1 + u_k T)}{1 + u_\tau T}} \cdot \underbrace{\frac{d}{dT} (1 + u_\tau T)}_{= u_\tau} \quad (\text{by the Leibniz rule}) \\
&= \sum_{\tau=1}^m \left( \underbrace{\prod_{k=1}^m (1 + u_k T)}_{=u} \right) \cdot \frac{u_\tau}{1 + u_\tau T} = u \sum_{\tau=1}^m \frac{u_\tau}{1 + u_\tau T}
\end{aligned}$$

and thus

$$\begin{aligned}
&-T \frac{d}{dT} \log u \\
&= -T \frac{\frac{d}{dT}u}{u} = -T \frac{u \sum_{\tau=1}^m \frac{u_\tau}{1 + u_\tau T}}{u} = -T \sum_{\tau=1}^m \frac{u_\tau}{1 + u_\tau T} = \sum_{\tau=1}^m (-u_\tau T) (1 + u_\tau T)^{-1} \\
&= \sum_{\tau=1}^m (-u_\tau T) \sum_{\rho \in \mathbb{N}} (-1)^\rho (u_\tau T)^\rho = \sum_{\tau=1}^m \sum_{\rho \in \mathbb{N}} (-1)^{\rho+1} (u_\tau T)^{\rho+1} = \sum_{\tau=1}^m \sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i (u_\tau T)^i \\
&= \sum_{\tau=1}^m \sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i u_\tau^i T^i = \sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i \sum_{\tau=1}^m u_\tau^i T^i,
\end{aligned}$$

so that  $\text{Coeff}_i \left( -T \frac{d}{dT} \log u \right) = (-1)^i \sum_{\tau=1}^m u_\tau^i$  (because  $i \in \mathbb{N} \setminus \{0\}$ ). In other words,

$(-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log u \right) = \sum_{\tau=1}^m u_\tau^i$ . Similarly,  $v = \Pi \left( \tilde{K}_v, [v_1, v_2, \dots, v_n] \right)$  yields

$(-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log v \right) = \sum_{\sigma=1}^n v_\sigma^i$ , and  $u \hat{v} = \Pi \left( \tilde{K}_{u,v}, [u_\ell v_j \mid (\ell, j) \in \{1, 2, \dots, m\} \times \{1, 2, \dots, n\}] \right)$

yields  $(-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log (u \hat{v}) \right) = \sum_{\tau=1}^m \sum_{\sigma=1}^n (u_\tau v_\sigma)^i$ . Thus,

$$\begin{aligned}
(-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log (u \hat{v}) \right) &= \sum_{\tau=1}^m \sum_{\sigma=1}^n (u_\tau v_\sigma)^i = \sum_{\tau=1}^m \sum_{\sigma=1}^n u_\tau^i v_\sigma^i \\
&= \underbrace{\sum_{\tau=1}^m u_\tau^i}_{= (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log u \right)} \cdot \underbrace{\sum_{\sigma=1}^n v_\sigma^i}_{= (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log v \right)} \\
&= (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log u \right) \cdot (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log v \right),
\end{aligned}$$

and (118) is thus proven. Similarly we can show (117). This completes the proof.

**(b)** Using Exercise 9.2 **(a)**, we can easily prove the following fact:

*Assertion  $\mathcal{F}$ :* If  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a special  $\lambda$ -ring, then, for any  $i \in \mathbb{N} \setminus \{0\}$ , the  $i$ -th Adams operation  $\psi^i : K \rightarrow K$  is a ring homomorphism.

This assertion is a part of Theorem 9.3 **(b)**.

In order to prove Assertion  $\mathcal{F}$  using Exercise 9.2 **(a)**, we proceed as follows:

Every  $x \in K$  satisfies

$$\sum_{i \in \mathbb{N} \setminus \{0\}} \psi^i(x) T^i = \tilde{\psi}_T(x) = -T \frac{d}{dT} \log \lambda_{-T}(x) \quad (\text{by Theorem 9.2 (b)}),$$

what (upon the substitution of  $-T$  for  $T$ ) becomes

$$\sum_{i \in \mathbb{N} \setminus \{0\}} \psi^i(x) (-T)^i = -(-T) \frac{d}{d(-T)} \log \lambda_{-(-T)}(x) = -T \frac{d}{dT} \log \lambda_T(x),$$

what rewrites as  $\sum_{i \in \mathbb{N} \setminus \{0\}} (-1)^i \psi^i(x) T^i = -T \frac{d}{dT} \log \lambda_T(x)$ . Hence, for every  $x \in K$

and  $i \in \mathbb{N} \setminus \{0\}$ , we have  $(-1)^i \psi^i(x) = \text{Coeff}_i \left( -T \frac{d}{dT} \log \lambda_T(x) \right)$  and therefore  $\psi^i(x) = (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log \lambda_T(x) \right)$ .

Now fix  $i \in \mathbb{N} \setminus \{0\}$ . We have shown that every  $x \in K$  satisfies

$$\psi^i(x) = (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log \lambda_T(x) \right).$$

In other words, the map  $\psi^i$  is the composition of the map  $\lambda_T : K \rightarrow \Lambda(K)$  (which is a ring homomorphism, since the  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is special) with the map

$$\begin{aligned} \Lambda(K) &\rightarrow K, \\ u &\mapsto (-1)^i \text{Coeff}_i \left( -T \frac{d}{dT} \log u \right) \end{aligned}$$

(which is a ring homomorphism according to Exercise 9.2 **(a)**). Thus,  $\psi^i$  is a ring homomorphism (since the composition of two ring homomorphisms is a ring homomorphism). This proves Assertion  $\mathcal{F}$ .

*Exercise 9.3: Hints to solution:* **(a)** We have solved Exercise 9.3 **(a)** in the 2nd step of the proof of Theorem 9.5 (with the only difference that the index of summation that was called  $i$  in Exercise 9.3 **(a)** was denoted by  $j$  in the 2nd step of the proof of Theorem 9.5).

**(b)** We will prove the equation  $n! \lambda^n(x) = \det A_n$  by induction over  $n$ .

The base case,  $n = 0$ , is trivial (for  $0! = 1$ ,  $\lambda^0(x) = 1$ , and the determinant of a  $0 \times 0$  matrix is 1 by definition). If you do not believe in  $0 \times 0$  matrices, the  $n = 1$  case is trivial as well (since  $\lambda^1(x) = x$  and  $\psi^1(x) = x$  by Theorem 9.3 **(a)**<sup>100</sup>) and can equally serve as a base case. The interesting part is the induction step.

<sup>100</sup>Here we are using the fact that Theorem 9.3 **(a)** holds for every  $\lambda$ -ring  $(K, (\lambda^i)_{i \in \mathbb{N}})$  (not only for special ones). This is very easy to see (but not really necessary because, as I said, we can just as well take  $n = 0$  for the base case).

For this step, we develop the determinant of the matrix  $A_n$  along the  $n$ -th row. We obtain

$$\det A_n = \sum_{k=1}^n (-1)^{n-k} \psi^{n-k+1}(x) \cdot \det \left( A_n \begin{bmatrix} \sim k \\ \sim n \end{bmatrix} \right), \quad (119)$$

where  $A_n \begin{bmatrix} \sim k \\ \sim n \end{bmatrix}$  is the matrix obtained from  $A_n$  by removing the  $n$ -th row and the  $k$ -th column.

Now, the matrix  $A_n \begin{bmatrix} \sim k \\ \sim n \end{bmatrix}$  turns out to be a block-triangular matrix<sup>101</sup> (composed of four blocks), with the left upper block (of size  $(k-1) \times (k-1)$ ) being equal to  $A_{k-1}$  and the right lower block (of size  $(n-k) \times (n-k)$ ) being a lower triangular matrix with the numbers  $k, k+1, \dots, n-1$  on its diagonal. Hence,  $\det \left( A_n \begin{bmatrix} \sim k \\ \sim n \end{bmatrix} \right) = \det A_{k-1} \cdot (k(k+1) \dots (n-1))$  (since the determinant of any block-triangular matrix is known to equal the product of the determinants of its diagonal blocks<sup>102</sup>). Since we are proceeding by induction over  $n$ , we can take  $\det A_{k-1} = (k-1)! \lambda^{k-1}(x)$  for granted (since  $k-1 < n$ ), and thus obtain

$$\begin{aligned} \det \left( A_n \begin{bmatrix} \sim k \\ \sim n \end{bmatrix} \right) &= \det A_{k-1} \cdot (k(k+1) \dots (n-1)) = (k-1)! \lambda^{k-1}(x) \cdot (k(k+1) \dots (n-1)) \\ &= \underbrace{(k-1)! \cdot (k(k+1) \dots (n-1))}_{=(n-1)!} \cdot \lambda^{k-1}(x) = (n-1)! \cdot \lambda^{k-1}(x). \end{aligned}$$

Thus, (119) becomes

$$\begin{aligned} \det A_n &= \sum_{k=1}^n (-1)^{n-k} \psi^{n-k+1}(x) \cdot (n-1)! \cdot \lambda^{k-1}(x) \\ &= (n-1)! \cdot \sum_{k=1}^n (-1)^{n-k} \psi^{n-k+1}(x) \lambda^{k-1}(x) \\ &= (n-1)! \cdot \underbrace{\sum_{i=1}^n (-1)^{i-1} \psi^i(x) \lambda^{n-i}(x)}_{=n\lambda^n(x) \text{ by (a)}} \\ &\quad \text{(here we substituted } i \text{ for } n-k+1 \text{ in the sum)} \\ &= \underbrace{(n-1)! \cdot n \lambda^n(x)}_{=n!} = n! \lambda^n(x), \end{aligned}$$

completing the induction step, qed.

(c) The proof (by induction over  $n$ ) is similar to that of part (b), but this time the

<sup>101</sup>Here, when I say “block-triangular matrix”, I always mean a block-triangular matrix whose diagonal blocks are square matrices.

<sup>102</sup>See [Grin-detn, Exercise 6.30] for a proof of this statement (at least in the case of a block-triangular matrix with four blocks, and with the upper-right block being the zero matrix; but this is precisely the case which we are using).

induction step leads us through

$$\begin{aligned}
\det B_n &= \sum_{k=1}^n (-1)^{n-k} \begin{cases} \lambda^{n-k+1}(x), & \text{if } k > 1; \\ n\lambda^n(x), & \text{if } k = 1 \end{cases} \cdot \psi^{k-1}(x) \\
&= \sum_{i=0}^{n-1} (-1)^{n-i-1} \begin{cases} \lambda^{n-i}(x), & \text{if } i > 0; \\ n\lambda^n(x), & \text{if } i = 0 \end{cases} \cdot \psi^i(x) \\
&\quad \text{(here we substituted } i \text{ for } k - 1 \text{ in the sum)} \\
&= \underbrace{(-1)^{n-1} n\lambda^n(x)}_{=-(-1)^n} \underbrace{\psi^0(x)}_{\substack{\text{we defined this} \\ \text{to mean } 1}} + \sum_{i=1}^{n-1} \underbrace{(-1)^{n-i-1}}_{=-(-1)^n(-1)^{i-1}} \lambda^{n-i}(x) \psi^i(x) \\
&= -(-1)^n n\lambda^n(x) + \sum_{i=1}^{n-1} (-1)^n (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x) \\
&= (-1)^n \left( -n\lambda^n(x) + \sum_{i=1}^{n-1} (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x) \right) \\
&= (-1)^n \underbrace{\left( -\sum_{i=1}^n (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x) + \sum_{i=1}^{n-1} (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x) \right)}_{=-(-1)^{n-1} \lambda^{n-n}(x) \psi^n(x)} \\
&\quad \text{(by part (a))} \\
&= (-1)^n \left( -(-1)^{n-1} \lambda^{n-n}(x) \psi^n(x) \right) = \underbrace{\lambda^{n-n}(x)}_{=\lambda^0(x)=1} \psi^n(x) = \psi^n(x),
\end{aligned}$$

what completes the proof.

*Exercise 9.4: Hints to solution:* There are several ways to prove this. Here is one:

We are going to prove that  $\psi^n = \text{id}$  for all  $n \in \mathbb{N} \setminus \{0\}$ . We will do this by strong induction over  $n$ . Since a strong induction does not need an induction base, let us start with the induction step:

Let  $n \in \mathbb{N} \setminus \{0\}$ . Assume (as the induction hypothesis) that we have already proven  $\psi^i = \text{id}$  for all  $i \in \mathbb{N} \setminus \{0\}$  satisfying  $i < n$ . We now must prove that  $\psi^n = \text{id}$ .

Let  $x \in K$ . Exercise 9.3 (a) yields

$$n\lambda^n(x) = \sum_{i=1}^n (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x).$$

Since  $\lambda^n(x) = \binom{x}{n}$  (since  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a binomial  $\lambda$ -ring) and  $\lambda^{n-i}(x) = \binom{x}{n-i}$

for every  $i \in \{1, 2, \dots, n\}$  (for the very same reason), this rewrites as

$$\begin{aligned}
 n \binom{x}{n} &= \sum_{i=1}^n (-1)^{i-1} \binom{x}{n-i} \psi^i(x) \\
 &= \sum_{i=1}^{n-1} (-1)^{i-1} \binom{x}{n-i} \underbrace{\psi^i(x)}_{\substack{= \text{id} \\ (\text{since } i < n)}} + (-1)^{n-1} \underbrace{\binom{n}{n-n}}_{= \binom{n}{0} = 1} \psi^n(x) \\
 &= \sum_{i=1}^{n-1} (-1)^{i-1} \binom{x}{n-i} \underbrace{\text{id}(x)}_{=x} + (-1)^{n-1} \psi^n(x) \\
 &= \sum_{i=1}^{n-1} (-1)^{i-1} \binom{x}{n-i} x + (-1)^{n-1} \psi^n(x).
 \end{aligned}$$

Since<sup>103</sup>

$$\begin{aligned}
& \sum_{i=1}^{n-1} (-1)^{i-1} \binom{x}{n-i} \\
&= \sum_{i=1}^{n-1} (-1)^{i-1} \left( \binom{x-1}{n-i} + \binom{x-1}{n-i-1} \right) \\
& \quad \left( \begin{array}{l} \text{because } \binom{x}{n-i} = \binom{x-1}{n-i} + \binom{x-1}{n-i-1} \\ \text{by the recurrence equation of the binomial coefficients} \end{array} \right) \\
&= \sum_{i=1}^{n-1} (-1)^{i-1} \binom{x-1}{n-i} + \sum_{i=1}^{n-1} (-1)^{i-1} \binom{x-1}{n-i-1} \\
&= \sum_{i=1}^{n-1} (-1)^{i-1} \binom{x-1}{n-i} + \sum_{i=2}^n \underbrace{(-1)^{(i-1)-1}}_{=-(-1)^{i-1}} \underbrace{\binom{x-1}{n-(i-1)-1}}_{=\binom{x-1}{n-i}} \\
& \quad \text{(here, we substituted } i-1 \text{ for } i \text{ in the second sum)} \\
&= \underbrace{\sum_{i=1}^{n-1} (-1)^{i-1} \binom{x-1}{n-i}}_{=(-1)^{1-1} \binom{x-1}{n-1} + \sum_{i=2}^{n-1} (-1)^{i-1} \binom{x-1}{n-i}} + \underbrace{\sum_{i=2}^n (-(-1)^{i-1}) \binom{x-1}{n-i}}_{=\sum_{i=2}^{n-1} (-(-1)^{i-1}) \binom{x-1}{n-i} + (-(-1)^{n-1}) \binom{x-1}{n-n}} \\
&= \underbrace{(-1)^{1-1} \binom{x-1}{n-1}}_{=1} + \underbrace{\sum_{i=2}^{n-1} (-1)^{i-1} \binom{x-1}{n-i} + \sum_{i=2}^{n-1} (-(-1)^{i-1}) \binom{x-1}{n-i}}_{=\sum_{i=2}^{n-1} (-1)^{i-1} \binom{x-1}{n-i} - \sum_{i=2}^{n-1} (-1)^{i-1} \binom{x-1}{n-i} = 0} \\
& \quad + (-(-1)^{n-1}) \underbrace{\binom{x-1}{n-n}}_{=\binom{x-1}{0}=1} \\
&= 1 \binom{x-1}{n-1} + 0 + (-(-1)^{n-1}) 1 = \binom{x-1}{n-1} - (-1)^{n-1},
\end{aligned}$$

this becomes

$$\begin{aligned}
n \binom{x}{n} &= \left( \binom{x-1}{n-1} - (-1)^{n-1} \right) x + (-1)^{n-1} \psi^n(x) \\
&= \binom{x-1}{n-1} x - (-1)^{n-1} x + (-1)^{n-1} \psi^n(x).
\end{aligned}$$

<sup>103</sup>The following computation only makes sense in the case when  $n \geq 2$ . However, in the remaining case, the result of the computation can be checked independently.



Since

$$\begin{aligned}
\binom{x-1}{n-1} x &= \frac{(x-1) \cdot (x-2) \cdot \dots \cdot ((x-1) - (n-1) + 1)}{(n-1)!} x \\
&= \frac{(x-1) \cdot (x-2) \cdot \dots \cdot (x-n+1)}{(n-1)!} x = \frac{x \cdot ((x-1) \cdot (x-2) \cdot \dots \cdot (x-n+1))}{(n-1)!} \\
&= \frac{x \cdot (x-1) \cdot \dots \cdot (x-n+1)}{(n-1)!} = \frac{x \cdot (x-1) \cdot \dots \cdot (x-n+1)}{n! / n} \\
&\quad (\text{since } (n-1)! = n! / n) \\
&= n \underbrace{\frac{x \cdot (x-1) \cdot \dots \cdot (x-n+1)}{n!}}_{= \binom{x}{n}} = n \binom{x}{n},
\end{aligned}$$

this transforms into

$$n \binom{x}{n} = n \binom{x}{n} - (-1)^{n-1} x + (-1)^{n-1} \psi^n(x).$$

This simplifies to  $(-1)^{n-1} x = (-1)^{n-1} \psi^n(x)$ . In other words,  $\psi^n(x) = x$ . Since this holds for every  $x \in K$ , this shows that  $\psi^n = \text{id}$ . This completes the induction step. Thus,  $\psi^n = \text{id}$  for every  $n \in \mathbb{N} \setminus \{0\}$ , and Exercise 9.4 is solved.

*Exercise 9.5: Solution: 1st step:* Any two power series  $u \in 1 + K[[T]]^+$  and  $v \in 1 + K[[T]]^+$  satisfy

$$-T \frac{d}{dT} \log(uv) = \left( -T \frac{d}{dT} \log u \right) + \left( -T \frac{d}{dT} \log v \right). \quad (120)$$

*First proof of (120).* Let  $u \in 1 + K[[T]]^+$  and  $v \in 1 + K[[T]]^+$ . Let us work with the notations of Exercise 9.2. For every  $i \in \mathbb{N} \setminus \{0\}$ , we have

$$\begin{aligned}
\text{Coeff}_i \left( -T \frac{d}{dT} \log(uv) \right) &= \text{Coeff}_i \left( -T \frac{d}{dT} \log(u \hat{+} v) \right) \quad (\text{since } uv = u \hat{+} v) \\
&= \text{Coeff}_i \left( -T \frac{d}{dT} \log u \right) + \text{Coeff}_i \left( -T \frac{d}{dT} \log v \right) \\
&\quad (\text{by (117), divided by } (-1)^i) \\
&= \text{Coeff}_i \left( \left( -T \frac{d}{dT} \log u \right) + \left( -T \frac{d}{dT} \log v \right) \right).
\end{aligned}$$

In other words, the coefficients of the power series  $-T \frac{d}{dT} \log(uv)$  before  $T^1, T^2, T^3, \dots$  are equal to the respective coefficients of the power series  $\left( -T \frac{d}{dT} \log u \right) + \left( -T \frac{d}{dT} \log v \right)$ . Since the same holds for the coefficients before  $T^0$  (in fact, both power

series  $-T \frac{d}{dT} \log(uv)$  and  $\left(-T \frac{d}{dT} \log u\right) + \left(-T \frac{d}{dT} \log v\right)$  are divisible by  $T$  and thus have the coefficient 0 before  $T^0$ , this yields that the power series  $-T \frac{d}{dT} \log(uv)$  and  $\left(-T \frac{d}{dT} \log u\right) + \left(-T \frac{d}{dT} \log v\right)$  are identic. Thus, (120) is proven.

*Second proof of (120).* Let  $u \in 1 + K[[T]]^+$  and  $v \in 1 + K[[T]]^+$ . We have

$$\begin{aligned}
-T \frac{d}{dT} \log(uv) &= -T \frac{\frac{d}{dT}(uv)}{uv} = -T \frac{\left(\frac{d}{dT}u\right)v + u\left(\frac{d}{dT}v\right)}{uv} \\
&= \frac{\frac{d}{dT}(uv)}{uv} = \frac{\frac{d}{dT}u}{u} + \frac{\frac{d}{dT}v}{v} \\
&\quad \left(\text{since } \frac{d}{dT}(uv) = \left(\frac{d}{dT}u\right)v + u\left(\frac{d}{dT}v\right) \text{ by the Leibniz identity}\right) \\
&= -T \left( \frac{\frac{d}{dT}u}{u} + \frac{\frac{d}{dT}v}{v} \right) = -T \left( \frac{d}{dT} \log u + \frac{d}{dT} \log v \right) \\
&\quad \left( \frac{\frac{d}{dT}u}{u} = \frac{d}{dT} \log u, \frac{\frac{d}{dT}v}{v} = \frac{d}{dT} \log v \right) \\
&= \left(-T \frac{d}{dT} \log u\right) + \left(-T \frac{d}{dT} \log v\right).
\end{aligned}$$

This proves (120).

*2nd step:* For every  $x \in K$  and  $y \in K$ , we have  $\tilde{\psi}_T(x+y) = \tilde{\psi}_T(x) + \tilde{\psi}_T(y)$ , where the map  $\tilde{\psi}_T$  is defined as in Theorem 9.5.

*Proof.* Let  $x \in K$  and  $y \in K$ . By Theorem 9.5 (b), we have  $\tilde{\psi}_T(x) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x)$ . By Theorem 9.5 (b) (applied to  $y$  instead of  $x$ ), we have  $\tilde{\psi}_T(y) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(y)$ . By Theorem 9.5 (b) (applied to  $x+y$  instead of  $x$ ), we have  $\tilde{\psi}_T(x+y) = -T \cdot \frac{d}{dT} \log \lambda_{-T}(x+y)$ .

By Theorem 2.1 (b), we have  $\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x+y)$ . Now,

$$\begin{aligned}
&\underbrace{\lambda_{-T}(x)}_{=ev_{-T}(\lambda_T(x))} \cdot \underbrace{\lambda_{-T}(y)}_{=ev_{-T}(\lambda_T(y))} \\
&= ev_{-T}(\lambda_T(x)) \cdot ev_{-T}(\lambda_T(y)) \\
&= ev_{-T} \left( \underbrace{\lambda_T(x) \cdot \lambda_T(y)}_{=\lambda_T(x+y)} \right) \quad (\text{since } ev_{-T} \text{ is a ring homomorphism}) \\
&= ev_{-T}(\lambda_T(x+y)) = \lambda_{-T}(x+y) \quad (\text{since } \lambda_{-T}(x+y) \text{ is defined as } ev_{-T}(\lambda_T(x+y))).
\end{aligned}$$

Now,

$$\begin{aligned}
\tilde{\psi}_T(x+y) &= -T \cdot \frac{d}{dT} \log \underbrace{\lambda_{-T}(x+y)}_{=\lambda_{-T}(x) \cdot \lambda_{-T}(y)} = -T \frac{d}{dT} \log (\lambda_{-T}(x) \cdot \lambda_{-T}(y)) \\
&= \underbrace{\left( -T \frac{d}{dT} \log \lambda_{-T}(x) \right)}_{=\tilde{\psi}_T(x)} + \underbrace{\left( -T \frac{d}{dT} \log \lambda_{-T}(y) \right)}_{=\tilde{\psi}_T(y)} \\
&\quad \text{(by (120), applied to } u = \lambda_{-T}(x) \text{ and } v = \lambda_{-T}(y)\text{)} \\
&= \tilde{\psi}_T(x) + \tilde{\psi}_T(y).
\end{aligned}$$

This proves the 2nd step.

*3rd step:* For every  $x \in K$  and  $y \in K$ , we have  $\psi^j(x+y) = \psi^j(x) + \psi^j(y)$  for every  $j \in \mathbb{N} \setminus \{0\}$ .

*Proof.* Let  $x \in K$  and  $y \in K$ . By the definition of  $\tilde{\psi}_T$ , we have  $\tilde{\psi}_T(x) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j$ ,  $\tilde{\psi}_T(y) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(y) T^j$  and  $\tilde{\psi}_T(x+y) = \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x+y) T^j$ . Now,

$$\begin{aligned}
\sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x+y) T^j &= \tilde{\psi}_T(x+y) = \underbrace{\tilde{\psi}_T(x)}_{=\sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j} + \underbrace{\tilde{\psi}_T(y)}_{=\sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(y) T^j} \quad \text{(by the 2nd step)} \\
&= \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(x) T^j + \sum_{j \in \mathbb{N} \setminus \{0\}} \psi^j(y) T^j = \sum_{j \in \mathbb{N} \setminus \{0\}} (\psi^j(x) + \psi^j(y)) T^j.
\end{aligned}$$

Comparing coefficients before  $T^j$  in this identity of power series, we conclude that  $\psi^j(x+y) = \psi^j(x) + \psi^j(y)$  for every  $j \in \mathbb{N} \setminus \{0\}$ . This proves the 3rd step.

*4th step:* For every  $j \in \mathbb{N} \setminus \{0\}$ , we have  $\psi^j(0) = 0$ .

*Proof.* Let  $j \in \mathbb{N} \setminus \{0\}$ . The 3rd step yields that  $\psi^j(x+y) = \psi^j(x) + \psi^j(y)$  for every  $x \in K$  and  $y \in K$ . Applying this to  $x = 0$  and  $y = 0$ , we obtain  $\psi^j(0+0) = \psi^j(0) + \psi^j(0)$ . In other words,  $\psi^j(0) = \psi^j(0) + \psi^j(0)$ . This simplifies to  $\psi^j(0) = 0$ . Thus, the 4th step is proven.

*5th step:* The map  $\psi^j : K \rightarrow K$  is a homomorphism of additive groups for every  $j \in \mathbb{N} \setminus \{0\}$ .

*Proof.* This follows from the 3rd and 4th steps. This completes the 5th step and thus solves the problem.

*Exercise 9.6: Hints to solution:* (a) Corollary 9.7 yields

$$n\alpha_n = \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j(\alpha_1, \alpha_2, \dots, \alpha_j).$$

Since we identify the polynomial  $N_j(\alpha_1, \alpha_2, \dots, \alpha_j)$  with the polynomial  $N_j$  (because we view the polynomial ring  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_j]$  as a subring of  $\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$ ), this becomes

$$n\alpha_n = \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} \underbrace{N_j(\alpha_1, \alpha_2, \dots, \alpha_j)}_{=N_j} = \sum_{j=1}^n (-1)^{j-1} \alpha_{n-j} N_j = \sum_{i=1}^n (-1)^{i-1} \alpha_{n-i} N_i$$

(here, we renamed the index  $j$  as  $i$ ). This solves Exercise 9.6 (a).

(b), (c) To obtain a solution to Exercises 9.6 (b) and (c), we only have to make the following changes to the solution to Exercises 9.3 (b) and (c):

- Replace every occurrence of  $\lambda^\ell(x)$  (where  $\ell$  is any nonnegative integer) by  $\alpha_\ell$ .
- Replace every occurrence of  $\psi^\ell(x)$  (where  $\ell$  is any nonnegative integer) by  $N_\ell$ .
- Replace the equalities  $\lambda^1(x) = x$  and  $\psi^1(x) = x$  by  $\alpha_1 = \alpha_1$  and  $N_1 = \alpha_1$  (this is very easy to prove).
- Replace every reference to Exercise 9.3 (a) by a reference to Exercise 9.6 (a).

This solves Exercises 9.6 (b) and (c).

(d) Let  $(K, (\lambda^i)_{i \in \mathbb{N}})$  be a  $\lambda$ -ring. Let  $x \in K$ . Let  $n \in \mathbb{N}$ . By the universal property of a polynomial ring, there exists a  $\mathbb{Z}$ -algebra homomorphism  $\varrho : \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n] \rightarrow K$  which maps  $\alpha_i$  to  $\lambda^i(x)$  for every  $i \in \{1, 2, \dots, n\}$ . Consider this homomorphism  $\varrho$ . By its construction, this homomorphism  $\varrho$  maps every polynomial  $P \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$  to its value  $P(\lambda^1(x), \lambda^2(x), \dots, \lambda^n(x))$ .

Every  $i \in \{0, 1, \dots, n\}$  satisfies

$$\varrho(\alpha_i) = \lambda^i(x) \quad \text{and} \quad \varrho(N_i) = \psi^i(x). \quad (121)$$

104

Now, let us derive Exercise 9.3 (a) from Exercise 9.6 (a): According to Exercise 9.6 (a), the equality

$$n\alpha_n = \sum_{i=1}^n (-1)^{i-1} \alpha_{n-i} N_i$$

holds. Applying  $\varrho$  to both sides of the equation, we get  $\varrho(n\alpha_n) = \varrho\left(\sum_{i=1}^n (-1)^{i-1} \alpha_{n-i} N_i\right)$ .

Since

$$\begin{aligned} \varrho(n\alpha_n) &= n \underbrace{\varrho(\alpha_n)}_{\substack{= \lambda^n(x) \\ \text{(by (121))}}} && \text{(since } \varrho \text{ is a } \mathbb{Z}\text{-algebra homomorphism)} \\ &= n\lambda^n(x) \end{aligned}$$

---

<sup>104</sup> *Proof of (121).* We distinguish between two cases:

*Case 1:* We have  $i = 0$ .

*Case 2:* We have  $i > 0$ .

First consider Case 1: In this case,  $\alpha_i = \alpha_0 = 1$ ,  $\lambda^i(x) = \lambda^0(x) = 1$ ,  $\psi^i(x) = \psi^0(x) = 1$  and

$N_i = N_0 = 1$ . Also,  $\varrho(1) = 1$  (since  $\varrho$  is a  $\mathbb{Z}$ -algebra homomorphism). Thus,  $\varrho\left(\underbrace{\alpha_i}_{=1}\right) = \varrho(1) =$

$1 = \lambda^i(x)$  and  $\varrho\left(\underbrace{N_i}_{=1}\right) = \varrho(1) = 1 = \psi^i(x)$ .

We have thus proven (121) in Case 1.

Now let us consider Case 2: In this case,  $i > 0$  and  $i \in \{0, 1, \dots, n\}$ , so that  $i \in \{1, 2, \dots, n\}$ . Hence, by the definition of  $\varrho$ , we know that  $\varrho$  maps  $\alpha_i$  to  $\lambda^i(x)$ . In other words,  $\varrho(\alpha_i) = \lambda^i(x)$ . Besides, we know that  $\varrho$  maps every polynomial  $P \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_n]$  to its value  $P(\lambda^1(x), \lambda^2(x), \dots, \lambda^n(x))$ . Hence,  $\varrho$  maps  $N_i$  to  $N_i(\lambda^1(x), \lambda^2(x), \dots, \lambda^n(x)) = \psi^i(x)$ . In other words,  $\varrho(N_i) = \psi^i(x)$ .

We have thus proven (121) in Case 2.

So we have proven (121) in both possible cases, qed.

and

$$\begin{aligned} \varrho \left( \sum_{i=1}^n (-1)^{i-1} \alpha_{n-i} N_i \right) &= \sum_{i=1}^n (-1)^{i-1} \underbrace{\varrho(\alpha_{n-i})}_{=\lambda^{n-i}(x)} \underbrace{\varrho(N_i)}_{=\psi^i(x)} \\ &\quad \text{(since } \varrho \text{ is a } \mathbb{Z}\text{-algebra homomorphism)} \\ &= \sum_{i=1}^n (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x), \end{aligned}$$

this becomes

$$n\lambda^n(x) = \sum_{i=1}^n (-1)^{i-1} \lambda^{n-i}(x) \psi^i(x).$$

Thus we have proved Exercise 9.3 (a) by means of Exercise 9.6 (a). Similarly, we can derive Exercise 9.3 (b) and (c) from Exercise 9.6 (b) and (c) (again, by applying  $\varrho$ ).

*Exercise 9.7: Detailed solution:* First, we will prove that  $\alpha_1^p - N_p \in p\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_p]$  (where  $N_p$  is the  $p$ -th Hirzebruch polynomial as defined in the beginning of Section 9). Due to our implicit construction of  $N_p$ , this is not easy to prove directly. Instead, we will prove this by defining a “universal” polynomial similar to our Hirzebruch polynomials, and then prove that this polynomial actually is  $\frac{\alpha_1^p - N_p}{p}$ .

*1st step:* Let  $m \in \mathbb{N}$ . The polynomial  $\frac{1}{p}((U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p)) \in \mathbb{Q}[U_1, U_2, \dots, U_m]$  actually lies in  $\mathbb{Z}[U_1, U_2, \dots, U_m]$ .

*Proof.* We need the following fact as a lemma:

$$\left( \begin{array}{l} \text{If } m \in \mathbb{N}, \text{ if } A \text{ is a commutative ring with unity such that } p \cdot 1_A = 0, \text{ and} \\ \text{if } x_1, x_2, \dots, x_m \text{ are } m \text{ elements of } A, \text{ then } (x_1 + x_2 + \dots + x_m)^p = x_1^p + x_2^p + \dots + x_m^p \end{array} \right). \quad (122)$$

105

Now, let  $A$  be the ring  $(\mathbb{Z}[U_1, U_2, \dots, U_m]) / (p\mathbb{Z}[U_1, U_2, \dots, U_m])$ . For every  $u \in \mathbb{Z}[U_1, U_2, \dots, U_m]$ , let  $\bar{u}$  denote the residue class of  $u$  modulo the ideal  $p\mathbb{Z}[U_1, U_2, \dots, U_m]$ ; this  $\bar{u}$  lies in  $(\mathbb{Z}[U_1, U_2, \dots, U_m]) / (p\mathbb{Z}[U_1, U_2, \dots, U_m]) = A$ . Since  $p \cdot 1_{\mathbb{Z}[U_1, U_2, \dots, U_m]} \in p\mathbb{Z}[U_1, U_2, \dots, U_m]$ , we have  $p \cdot 1_{\mathbb{Z}[U_1, U_2, \dots, U_m]} = 0$ . Since  $p \cdot 1_{\mathbb{Z}[U_1, U_2, \dots, U_m]} = p \cdot 1_A$ , this rewrites as  $p \cdot 1_A = 0$ . Thus, (122) (applied to  $x_i = \bar{U}_i$ ) yields  $(\bar{U}_1 + \bar{U}_2 + \dots + \bar{U}_m)^p = \bar{U}_1^p + \bar{U}_2^p + \dots + \bar{U}_m^p$ . Since  $(\bar{U}_1 + \bar{U}_2 + \dots + \bar{U}_m)^p = \overline{(U_1 + U_2 + \dots + U_m)^p}$  and  $\bar{U}_1^p + \bar{U}_2^p + \dots + \bar{U}_m^p = \overline{U_1^p + U_2^p + \dots + U_m^p}$ .

<sup>105</sup>*Proof of (122):* Let  $m \in \mathbb{N}$ . Let  $A$  be a commutative ring with unity such that  $p \cdot 1_A = 0$ . Let  $x_1, x_2, \dots, x_m$  be  $m$  elements of  $A$ .

Let  $\Phi : A \rightarrow A$  be the map defined by  $(\Phi(y) = y^p$  for every  $y \in A)$ . Then,  $\Phi$  is known to be a ring homomorphism (since  $p \cdot 1_A = 0$ ). Thus,

$$\Phi(x_1 + x_2 + \dots + x_m) = \Phi(x_1) + \Phi(x_2) + \dots + \Phi(x_m) = \sum_{i=1}^m \underbrace{\Phi(x_i)}_{=x_i^p} = \sum_{i=1}^m x_i^p = x_1^p + x_2^p + \dots + x_m^p. \quad \text{(by the definition of } \Phi)$$

Compared with  $\Phi(x_1 + x_2 + \dots + x_m) = (x_1 + x_2 + \dots + x_m)^p$  (by the definition of  $\Phi$ ), this yields  $(x_1 + x_2 + \dots + x_m)^p = x_1^p + x_2^p + \dots + x_m^p$ . This proves (122).

$\overline{U_2^p + \dots + U_m^p} = \overline{U_1^p + U_2^p + \dots + U_m^p}$ , this rewrites as  $\overline{(U_1 + U_2 + \dots + U_m)^p} = \overline{U_1^p + U_2^p + \dots + U_m^p}$ . In other words,

$$(U_1 + U_2 + \dots + U_m)^p \equiv U_1^p + U_2^p + \dots + U_m^p \pmod{p\mathbb{Z}[U_1, U_2, \dots, U_m]}.$$

In other words,  $(U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p) \in p\mathbb{Z}[U_1, U_2, \dots, U_m]$ . Thus,  $\frac{1}{p}((U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p)) \in \mathbb{Z}[U_1, U_2, \dots, U_m]$ . This proves the 1st step.

*2nd step:* Until now,  $m$  could be any nonnegative integer. From now on, set  $m = p$ .

The polynomial  $\frac{1}{p}((U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p))$  lies in  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  (due to the 1st step) and is symmetric (since it is a  $\mathbb{Q}$ -linear combination of the polynomials  $(U_1 + U_2 + \dots + U_m)^p$  and  $U_1^p + U_2^p + \dots + U_m^p$ , both of which are symmetric). Thus, Theorem 4.1 (a) (applied to  $K = \mathbb{Z}$  and  $P = \frac{1}{p}((U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p))$ ) yields that there exists one and only one polynomial  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m]$  such that

$$\frac{1}{p}((U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p)) = Q(X_1, X_2, \dots, X_m). \quad (123)$$

Consider this  $Q$ . Note that  $Q \in \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_m] = \mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_p]$  (since  $m = p$ ).

For every  $i \in \mathbb{N}$ , let  $X_i$  be defined as in Theorem 4.1. For every  $j \in \mathbb{N} \setminus \{0\}$ , define  $N_j$  as in the beginning of Section 9. Applying (40) to  $j = p$ , we obtain

$$\sum_{i=1}^m U_i^p = N_p \underbrace{(X_1, X_2, \dots, X_p)}_{\substack{=(X_1, X_2, \dots, X_m) \\ (\text{since } p=m)}} = N_p(X_1, X_2, \dots, X_m).$$

On the other hand,  $X_1 = U_1 + U_2 + \dots + U_m$  (because  $X_1$  is the 1-st elementary symmetric polynomial in the variables  $U_1, U_2, \dots, U_m$ ), so that  $X_1^p = (U_1 + U_2 + \dots + U_m)^p$ . Now,

$$\begin{aligned} (\alpha_1^p - N_p)(X_1, X_2, \dots, X_m) &= \underbrace{X_1^p}_{=(U_1 + U_2 + \dots + U_m)^p} - \underbrace{N_p(X_1, X_2, \dots, X_m)}_{=\sum_{i=1}^m U_i^p = U_1^p + U_2^p + \dots + U_m^p} \\ &= (U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p) \\ &= p \cdot \underbrace{\frac{1}{p}((U_1 + U_2 + \dots + U_m)^p - (U_1^p + U_2^p + \dots + U_m^p))}_{\substack{=Q(X_1, X_2, \dots, X_m) \\ (\text{by (123)}}}} \\ &= pQ(X_1, X_2, \dots, X_m) = (pQ)(X_1, X_2, \dots, X_m). \end{aligned}$$

Since the elements  $X_1, X_2, \dots, X_m$  of  $\mathbb{Z}[U_1, U_2, \dots, U_m]$  are algebraically independent (by Theorem 4.1 (a)), this yields  $\alpha_1^p - N_p = pQ$ . This shows that  $\alpha_1^p - N_p \in p\mathbb{Z}[\alpha_1, \alpha_2, \dots, \alpha_p]$ .

*3rd step:* Let  $x \in K$ . Applying (42) to  $j = p$ , we obtain

$$\psi^p(x) = N_p(\lambda^1(x), \lambda^2(x), \dots, \lambda^p(x)).$$

Now, we recall that  $\alpha_1^p - N_p = pQ$ , so that

$$\begin{aligned} (\alpha_1^p - N_p) (\lambda^1(x), \lambda^2(x), \dots, \lambda^p(x)) &= (pQ) (\lambda^1(x), \lambda^2(x), \dots, \lambda^p(x)) \\ &= p \underbrace{Q (\lambda^1(x), \lambda^2(x), \dots, \lambda^p(x))}_{\in K} \in pK. \end{aligned}$$

Since

$$\begin{aligned} (\alpha_1^p - N_p) (\lambda^1(x), \lambda^2(x), \dots, \lambda^p(x)) &= \underbrace{\alpha_1^p (\lambda^1(x), \lambda^2(x), \dots, \lambda^p(x))}_{=(\lambda^1(x))^p} - \underbrace{N_p (\lambda^1(x), \lambda^2(x), \dots, \lambda^p(x))}_{=\psi^p(x)} \\ &= \left( \underbrace{\lambda^1(x)}_{\substack{=x \\ \text{(by the definition} \\ \text{of a } \lambda\text{-ring)}}} \right)^p - \psi^p(x) = x^p - \psi^p(x), \end{aligned}$$

this rewrites as  $x^p - \psi^p(x) \in pK$ . In other words,  $\psi^p(x) \equiv x^p \pmod{pK}$ . Exercise 9.7 is solved.

## 11.10. To Section 10

*Exercise 10.2: Solution:*

*Proof of Proposition 10.29.* Let  $x \in K$ . Then,  $\lambda_T(x) = \sum_{i \in \mathbb{N}} \lambda^i(x) T^i$ , so that

$$\iota[[T]](\lambda_T(x)) = \iota[[T]] \left( \sum_{i \in \mathbb{N}} \lambda^i(x) T^i \right) = \sum_{i \in \mathbb{N}} \underbrace{\iota(\lambda^i(x))}_{=\lambda^i(x) \otimes 1} T^i = \sum_{i \in \mathbb{N}} (\lambda^i(x) \otimes 1) T^i. \quad \text{(by the definition of } \iota \text{)}$$

Hence, every  $k \in \mathbb{N}$  satisfies  $\text{Coeff}_k(\iota[[T]](\lambda_T(x))) = \text{Coeff}_k \left( \sum_{i \in \mathbb{N}} (\lambda^i(x) \otimes 1) T^i \right) = \lambda^k(x) \otimes 1$  (by the definition of  $\text{Coeff}_k$ ). Thus,

$$\begin{aligned} &(\text{Coeff}_1(\iota[[T]](\lambda_T(x))), \text{Coeff}_2(\iota[[T]](\lambda_T(x))), \dots, \text{Coeff}_j(\iota[[T]](\lambda_T(x)))) \\ &= (\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1) \end{aligned} \quad (124)$$

for every  $j \in \mathbb{N}$ . Now, (58) (applied to  $p = \iota[[T]](\lambda_T(x))$ ) yields

$$\begin{aligned} &\mathfrak{Odd}_\varphi(\iota[[T]](\lambda_T(x))) \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(\text{Coeff}_1(\iota[[T]](\lambda_T(x))), \text{Coeff}_2(\iota[[T]](\lambda_T(x))), \dots, \text{Coeff}_j(\iota[[T]](\lambda_T(x)))) T^j \\ &= \sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1) T^j \quad \text{(by (124))} \\ &= \text{td}_{\varphi, T, \mathbf{Z}'}(x). \end{aligned}$$

This proves Proposition 10.29. □

*Proof of Proposition 10.30.* Let  $\iota : K \rightarrow K \otimes_{\mathbf{Z}} \mathbf{Z}'$  be the canonical map (mapping every  $\xi \in K$  to  $\xi \otimes 1 \in K \otimes_{\mathbf{Z}} \mathbf{Z}'$ ). Proposition 10.29 (applied to  $\varphi = 1 + ut$ ) yields

$$\begin{aligned} \mathrm{td}_{1+ut, T, \mathbf{Z}'}(x) &= \mathfrak{I} \circ \mathrm{odd}_{1+ut}(\iota[[T]](\lambda_T(x))) = \underbrace{\mathrm{ev}_{uT}}_{\substack{= \mathrm{ev}_{(1 \otimes u)T} \\ \text{(since } uT = (1 \otimes u)T \\ \text{in } (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]])}}(\iota[[T]](\lambda_T(x))) \\ &\quad \left( \begin{array}{c} \text{by Proposition 10.12, applied to } \mathbf{Z}', K \otimes_{\mathbf{Z}} \mathbf{Z}' \text{ and } \iota[[T]](\lambda_T(x)) \\ \text{instead of } \mathbf{Z}, K \text{ and } p \end{array} \right) \\ &= \mathrm{ev}_{(1 \otimes u)T}(\iota[[T]](\lambda_T(x))) = (\mathrm{ev}_{(1 \otimes u)T} \circ \iota[[T]]) (\lambda_T(x)). \end{aligned}$$

But the diagram

$$\begin{array}{ccc} K[[T]] & \xrightarrow{\iota[[T]]} & (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]] \\ & \searrow \mathrm{ev}_{(1 \otimes u)T} & \downarrow \mathrm{ev}_{(1 \otimes u)T} \\ & & (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]] \end{array}$$

commutes (since the definition of the map  $\mathrm{ev}_{\mu T} : K[[T]] \rightarrow L[[T]]$  for any ring  $K$ , any  $K$ -algebra  $L$  and any element  $\mu$  of  $L$  was canonical with respect to  $K$ ). Thus,  $\mathrm{ev}_{(1 \otimes u)T} \circ \iota[[T]] = \mathrm{ev}_{(1 \otimes u)T}$ . Now,

$$\mathrm{td}_{1+ut, T, \mathbf{Z}'}(x) = \underbrace{(\mathrm{ev}_{(1 \otimes u)T} \circ \iota[[T]])}_{= \mathrm{ev}_{(1 \otimes u)T}}(\lambda_T(x)) = \mathrm{ev}_{(1 \otimes u)T}(\lambda_T(x)).$$

This proves Proposition 10.30.  $\square$

Alternatively, we could have proven Proposition 10.30 by repeating the proof of Proposition 10.3 with some minor changes.

We could derive Proposition 10.31 from Proposition 10.13 (just as we derived Proposition 10.30 from Proposition 10.12) using Proposition 10.29, but let us instead prove it directly:

*Proof of Proposition 10.31.* Let  $x \in K$ .

(a) We have

$$\begin{aligned} &\mathrm{Coeff}_0(\mathrm{td}_{\varphi, T, \mathbf{Z}'}(x)) \\ &= \mathrm{Coeff}_0\left(\sum_{j \in \mathbb{N}} \mathrm{Td}_{\varphi, j}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1) T^j\right) \quad (\text{by (64)}) \\ &= \mathrm{Td}_{\varphi, 0}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^0(x) \otimes 1) \quad (\text{by the definition of } \mathrm{Coeff}_0) \\ &= \mathrm{Td}_{\varphi, 0} = 1 \quad (\text{by Proposition 10.6 (a), applied to } \mathbf{Z}' \text{ instead of } \mathbf{Z}). \end{aligned}$$



(b) We have

$$\begin{aligned}
& \text{Coeff}_1(\text{td}_{\varphi, T, \mathbf{Z}'}(x)) \\
&= \text{Coeff}_1\left(\sum_{j \in \mathbb{N}} \text{Td}_{\varphi, j}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^j(x) \otimes 1) T^j\right) \quad (\text{by (64)}) \\
&= \text{Td}_{\varphi, 1}(\lambda^1(x) \otimes 1, \lambda^2(x) \otimes 1, \dots, \lambda^1(x) \otimes 1) \quad (\text{by the definition of } \text{Coeff}_1) \\
&= \text{Td}_{\varphi, 1}\left(\underbrace{\lambda^1(x) \otimes 1}_{=x}\right) = \text{Td}_{\varphi, 1}(x \otimes 1) = \varphi_1(x \otimes 1) \\
&\quad (\text{since Proposition 10.6 (b) (applied to } \mathbf{Z}' \text{ instead of } \mathbf{Z}) \text{ yields } \text{Td}_{\varphi, 1} = \varphi_1 \alpha_1).
\end{aligned}$$

Proposition 10.31 is now proven.  $\square$

*Proof of Proposition 10.32.* To obtain a proof of Proposition 10.32, read the proof of Proposition 10.7, doing the following replacements:

- Replace every  $\lambda^k(x)$  by  $\lambda^k(x) \otimes 1$  for  $k$  any nonnegative integer (that is, replace  $\lambda^1(x)$  by  $\lambda^1(x) \otimes 1$ , replace  $\lambda^2(x)$  by  $\lambda^2(x) \otimes 1$ , etc.).
- Replace every  $\text{td}_{\varphi, T}$  by  $\text{td}_{\varphi, T, \mathbf{Z}'}$ .
- Replace every  $\text{td}_{\psi, T}$  by  $\text{td}_{\psi, T, \mathbf{Z}'}$ .
- Replace every  $\text{td}_{\varphi\psi, T}$  by  $\text{td}_{\varphi\psi, T, \mathbf{Z}'}$ .
- Replace all references to Proposition 10.7 by references to Proposition 10.32.
- Replace all references to (53) by references to (64).

$\square$

*Proof of Proposition 10.33.* This can be proven by induction over  $m$ . The induction base (the case  $m = 0$ ) requires showing that  $\text{td}_{1, T, \mathbf{Z}'}(x) = 1$ , but this follows from Proposition 10.30<sup>106</sup>. The induction step is a straightforward application of Proposition 10.32. Thus Proposition 10.33 is proven.  $\square$

*Proof of Theorem 10.34.* Theorem 2.1 (a) yields  $\lambda_T(x) \cdot \lambda_T(y) = \lambda_T(x + y)$  (since  $(K, (\lambda^i)_{i \in \mathbb{N}})$  is a  $\lambda$ -ring).

Let  $\iota : K \rightarrow K \otimes_{\mathbf{Z}} \mathbf{Z}'$  be the canonical map (mapping every  $\xi \in K$  to  $\xi \otimes 1 \in K \otimes_{\mathbf{Z}} \mathbf{Z}'$ ). Then, Proposition 10.29 yields  $\text{td}_{\varphi, T, \mathbf{Z}'}(x) = \mathfrak{I} \circ \mathfrak{O} \circ \mathfrak{D}_{\varphi}(\iota[[T]](\lambda_T(x)))$ . Proposition 10.29

<sup>106</sup>In fact, Proposition 10.30 (applied to  $u = 0$ ) yields  $\text{td}_{1+0t, T, \mathbf{Z}'}(x) = \lambda_{(1 \otimes 0)T}(x)$ . Now  $\lambda_{(1 \otimes 0)T}(x) = \text{ev}_{(1 \otimes 0)T}(\lambda_T(x))$ . Since  $\text{ev}_{(1 \otimes 0)T} = \text{ev}_{0T}$  is the map  $K[[T]] \rightarrow (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]$  which sends every power series to its constant term tensored with 1 (viewed as a constant power series over  $K \otimes_{\mathbf{Z}} \mathbf{Z}'$ ), we have  $\text{ev}_{(1 \otimes 0)T}(\lambda_T(x)) = \underbrace{(\text{constant term of the power series } \lambda_T(x))}_{=1} \otimes 1 = 1 \otimes 1 = 1$ . Thus,

$$\text{td}_{1, T, \mathbf{Z}'}(x) = \text{td}_{1+0t, T, \mathbf{Z}'}(x) = \lambda_{(1 \otimes 0)T}(x) = \text{ev}_{(1 \otimes 0)T}(\lambda_T(x)) = 1.$$

(applied to  $y$  instead of  $x$ ) yields  $\text{td}_{\varphi,T,\mathbf{Z}'}(y) = \mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(y)))$ . Hence,

$$\begin{aligned} & \underbrace{\text{td}_{\varphi,T,\mathbf{Z}'}(x)}_{=\mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(x)))} \cdot \underbrace{\text{td}_{\varphi,T,\mathbf{Z}'}(y)}_{=\mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(y)))} \\ &= \mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(x))) \cdot \mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(y))) = \mathfrak{Iodd}_{\varphi} \left( \underbrace{\iota[[T]](\lambda_T(x)) \cdot \iota[[T]](\lambda_T(y))}_{\substack{=\iota[[T]](\lambda_T(x) \cdot \lambda_T(y)) \\ \text{(since } \iota[[T]] \text{ is a ring homomorphism)}}} \right) \\ & \quad \text{(by Theorem 10.16, applied to } p = \iota[[T]](\lambda_T(x)) \text{ and } q = \iota[[T]](\lambda_T(y))\text{)} \\ &= \mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(x) \cdot \lambda_T(y))). \end{aligned}$$

Proposition 10.29 (applied to  $x + y$  instead of  $x$ ) yields

$$\text{td}_{\varphi,T,\mathbf{Z}'}(x + y) = \mathfrak{Iodd}_{\varphi} \left( \iota[[T]] \left( \underbrace{\lambda_T(x + y)}_{=\lambda_T(x) \cdot \lambda_T(y)} \right) \right) = \mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(x) \cdot \lambda_T(y))).$$

Thus,

$$\text{td}_{\varphi,T,\mathbf{Z}'}(x) \cdot \text{td}_{\varphi,T,\mathbf{Z}'}(y) = \mathfrak{Iodd}_{\varphi}(\iota[[T]](\lambda_T(x) \cdot \lambda_T(y))) = \text{td}_{\varphi,T,\mathbf{Z}'}(x + y).$$

Theorem 10.34 is thus proven.  $\square$

*Proof of Corollary 10.35.* Every  $x \in K$  satisfies  $\text{td}_{\varphi,T,\mathbf{Z}'}(x) \in \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$  (since Proposition 10.31 (a) says that  $\text{Coeff}_0(\text{td}_{\varphi,T,\mathbf{Z}'}(x)) = 1$ , so that the power series  $\text{td}_{\varphi,T,\mathbf{Z}'}(x)$  has the constant term 1, and thus  $\text{td}_{\varphi,T,\mathbf{Z}'}(x) \in 1 + (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]^+ = \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ ). In other words,  $\text{td}_{\varphi,T,\mathbf{Z}'}(K) \subseteq \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ .

Now we are going to prove that  $\text{td}_{\varphi,T,\mathbf{Z}'} : K \rightarrow \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$  is a homomorphism of additive groups.

Theorem 10.34 (applied to  $x = 0$  and  $y = 0$ ) yields  $\text{td}_{\varphi,T,\mathbf{Z}'}(0) \cdot \text{td}_{\varphi,T,\mathbf{Z}'}(0) = \text{td}_{\varphi,T,\mathbf{Z}'}(0 + 0) = \text{td}_{\varphi,T,\mathbf{Z}'}(0)$ . Since  $\text{td}_{\varphi,T,\mathbf{Z}'}(0)$  is an invertible element of  $(K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]$  (because  $\text{td}_{\varphi,T,\mathbf{Z}'}(0)$  is a power series with constant term 1<sup>107</sup>, and every such power series is an invertible element of  $(K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]$ ), we can cancel  $\text{td}_{\varphi,T,\mathbf{Z}'}(0)$  from this equation, and obtain  $\text{td}_{\varphi,T,\mathbf{Z}'}(0) = 1$ . Since 0 is the neutral element of the additive group  $K$ , while 1 is the neutral element of the additive group  $\Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ , this yields that the map  $\text{td}_{\varphi,T,\mathbf{Z}'}$  respects the neutral elements of the additive groups  $K$  and  $\Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ .

Any  $x \in K$  and  $y \in K$  satisfy

$$\begin{aligned} \text{td}_{\varphi,T,\mathbf{Z}'}(x + y) &= \text{td}_{\varphi,T,\mathbf{Z}'}(x) \cdot \text{td}_{\varphi,T,\mathbf{Z}'}(y) && \text{(by Theorem 10.34)} \\ &= \text{td}_{\varphi,T,\mathbf{Z}'}(x) \hat{+} \text{td}_{\varphi,T,\mathbf{Z}'}(y) \end{aligned}$$

(since multiplication of power series in  $1 + (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]^+$  is addition in the ring  $\Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ ). Combined with the fact that the map  $\text{td}_{\varphi,T,\mathbf{Z}'}$  respects the neutral elements of the additive groups  $K$  and  $\Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$ , this yields: The map  $\text{td}_{\varphi,T,\mathbf{Z}'} : K \rightarrow \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}')$  is a homomorphism of additive groups. Corollary 10.35 is proven.  $\square$

<sup>107</sup>since  $\text{td}_{\varphi,T,\mathbf{Z}'}(0) \in \text{td}_{\varphi,T,\mathbf{Z}'}(K) \subseteq \Lambda(K \otimes_{\mathbf{Z}} \mathbf{Z}') = 1 + (K \otimes_{\mathbf{Z}} \mathbf{Z}')[[T]]^+$

*Proof of Proposition 10.36.* Let  $\iota : K \rightarrow K \otimes_{\mathbf{Z}} \mathbf{Z}'$  be the canonical map (mapping every  $\xi \in K$  to  $\xi \otimes 1 \in K \otimes_{\mathbf{Z}} \mathbf{Z}'$ ). Then,  $\iota [[T]] (1 + uT) = 1 + (u \otimes 1) T$ .

Proposition 10.29 (applied to  $x = u$ ) yields  $\text{td}_{\varphi, T, \mathbf{Z}'}(u) = \mathfrak{Iodd}_{\varphi}(\iota [[T]] (\lambda_T(u)))$ . But Theorem 8.3 (a) (applied to  $x = u$ ) yields that  $\lambda_T(u) = 1 + uT$  (since the element  $u$  is 1-dimensional). Thus,

$$\begin{aligned} \text{td}_{\varphi, T, \mathbf{Z}'}(u) &= \mathfrak{Iodd}_{\varphi} \left( \iota [[T]] \left( \underbrace{\lambda_T(u)}_{=1+uT} \right) \right) = \mathfrak{Iodd}_{\varphi} \left( \iota [[T]] \left( \underbrace{(1 + uT)}_{=1+(u \otimes 1)T} \right) \right) = \mathfrak{Iodd}_{\varphi}(1 + (u \otimes 1) T) \\ &= \varphi((u \otimes 1) T) \quad \left( \begin{array}{c} \text{by Proposition 10.26, applied to} \\ \mathbf{Z}', K \otimes_{\mathbf{Z}} \mathbf{Z}' \text{ and } u \otimes 1 \text{ instead of } \mathbf{Z}, K \text{ and } u \end{array} \right). \end{aligned}$$

This proves Proposition 10.36. □

*Proof of Theorem 10.37.* Theorem 10.37 can be proven with the help of Proposition 10.36 in the same way as we proved Theorem 10.27 with the help of Proposition 10.24. We leave the details to the reader. □

## References

- [AtiMac69] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley 1969.
- [BluCos16] Ben Blum-Smith, Samuel Coskey, *The Fundamental Theorem on Symmetric Polynomials: History's First Whiff of Galois Theory*, 8 April 2016, arXiv:1301.7116v4.  
<http://arxiv.org/abs/1301.7116v4>
- [CoLiOS15] David A. Cox, John Little, Donal O'Shea, *Ideals, Varieties, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, Undergraduate Texts in Mathematics, 4th Edition, Springer 2015.
- [DraGij09] Jan Draisma and Dion Gijswijt, *Invariant Theory with Applications*, 8 October 2009.  
<http://www.win.tue.nl/~jdraisma/teaching/invtheory0910/lecturenotes12.pdf>
- [Dumas08] François Dumas, *An introduction to noncommutative polynomial invariants*, lecture notes (Cimpa-Unesco-Argentina "Homological methods and representations of non-commutative algebras", Mar del Plata, Argentina March 6 - 17, 2006).  
<http://math.univ-bpclermont.fr/~fdumas/fichiers/CIMPA.pdf>
- [FulLan85] William Fulton, Serge Lang, *Riemann-Roch algebra*, Grundlehren der mathematischen Wissenschaften #277, Springer, New York 1985.
- [Grin-w4a] Darij Grinberg, *Witt#4a: Equigraded power series*.  
<http://www.cip.ifi.lmu.de/~grinberg/algebra/witt4a.pdf>

- [Grin-detn] Darij Grinberg, *Notes on the combinatorial fundamentals of algebra*, version of 10 January 2019.  
<https://github.com/darijgr/detnotes/releases/tag/2019-01-10>  
 (This is the URL of the frozen version of 10 January 2019, guaranteed to have its numbering match the references above. For a version which is getting updated, see <http://www.cip.ifi.lmu.de/~grinberg/primes2015/sols.pdf> .)
- [Harts77] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics #52, Springer 1977.
- [Hazewi08a] Michiel Hazewinkel, *Niceness theorems*, arXiv:0810.5691v1 [math.HO], 2008.  
<http://arxiv.org/abs/0810.5691v1>
- [Hazewi08b] Michiel Hazewinkel, *Witt vectors. Part 1*, arXiv:0804.3888v1 [math.RA], 2008.  
<http://arxiv.org/abs/0804.3888v1>
- [Hopkin06] John R. Hopkinson, *Universal Polynomials in Lambda rings and the K-theory of the infinite loop space tmf*, PhD thesis at MIT, June 2006.  
<http://dspace.mit.edu/handle/1721.1/34544>
- [Knut73] Donald Knutson,  *$\lambda$ -Rings and the Representation Theory of the Symmetric Group*, Lecture Notes in Mathematics #308, Springer, New York 1973.
- [Laksov09] Dan Laksov, *Splitting algebras, factorization algebras, and residues*, 28 January 2009.  
<https://people.kth.se/~laksov/art/splittingmonthly.pdf>
- [LLPT95] D. Laksov, A. Lascoux, P. Pragacz, and A. Thorup, *The LLPT Notes*, edited by A. Thorup, 1995,  
<http://www.math.ku.dk/~thorup/notes/sympol.pdf> .
- [MiRiRu88] Ray Mines, Fred Richman, Wim Ruitenburg, *A Course in Constructive Algebra*, Universitext, Springer 1988.
- [Neusel07] Mara D. Neusel, *Invariant Theory*, Student Mathematical Library #36, AMS 2007.
- [Newman12] Stephen C. Newman, *A classical introduction to Galois theory*, Wiley 2012.
- [Seiler88] Wolfgang K. Seiler,  *$\lambda$ -rings and Adams operations in algebraic K-Theory*, in: M. Rapoport, N. Schappacher, P. Schneider (eds.), *Beilinson's Conjectures on Special Values of L-functions*, Academic Press 1988, pp. 93–102.
- [Smith95] Larry Smith, *Polynomial Invariants of Finite Groups*, A K Peters 1995.
- [Yau10] Donald Yau, *Lambda-rings*, World Scientific 2010.  
<http://www.worldscientific.com/worldscibooks/10.1142/7664>  
 (includes downloadable Chapter 1).