Do the symmetric functions have a function-field analogue?

Darij Grinberg

draft, version 1.4, May 11, 2018

Contents

0.1. Introduction (Abstract?)

This is a preliminary report on a question that is almost naive: Is there a ring (or another structure) that has the same relation to the ring Λ of symmetric functions as $\mathbb{F}_q$ has to the "mythical field $\mathbb{F}_1$" ?

This question allows for at least two different interpretations. One of them is just about q-deforming the structure coefficients of the symmetric functions in such a way that (some of) their combinatorial interpretations are reinterpreted (i.e., counting sets becomes counting $\mathbb{F}_q$-vector spaces). This naturally leads to Hall algebras, studied e.g. in [5]. A different option, however, presents itself if we are willing to replace the bases of Λ itself (rather than just its structure coefficients). Namely, recall that all (or most) of the usual bases of Λ are indexed by integer partitions. An integer partition can be regarded as a weakly decreasing sequence of positive integers, or, equivalently, a conjugacy class of a permutation in a symmetric group. A natural "$\mathbb{F}_q$-analogue" of an integer partition, thus, is a conjugacy class of a matrix in $\mathrm{GL}_n\left(\mathbb{F}_q\right)$. Could we find a ring (or anything similar – a commutative $\mathbb{F}_q[T]$-algebra sounds like a reasonable thing to expect) which plays a similar role to Λ and whose bases are indexed by these $\mathbb{F}_q$-analogues?

This report is a bait-and-switch, as I do not have a good answer to this question. Instead I recall the classical interpretation of the ring Λ as the coordinate ring of the affine group of Witt vectors ([10, §9–§10]), and construct an $\mathbb{F}_q$-analogue of the affine group of Witt vectors. This analogue has a coordinate ring, which can reasonably be called an $\mathbb{F}_q$-analogue of Λ. But this answer is lacking something very important: the combinatorial bases. The most interesting structure on the ring Λ of symmetric functions is not so much its Hopf algebra structure, but its various bases, such as the homogeneous symmetric functions $(h_\lambda)_{\lambda\in\mathrm{Par}}$, the elementary symmetric functions $(e_\lambda)_{\lambda\in\mathrm{Par}}$ and the Schur functions $(s_\lambda)_{\lambda\in\mathrm{Par}}$. I am unable to find a counterpart to any of the bases just mentioned in the $\mathbb{F}_q$-analogue of Λ suggested. All I can offer is an analogue of the power-sum functions $(p_\lambda)_{\lambda\in\mathrm{Par}}$ (which do not even form a basis, although with functoriality they are sufficient for many computational purposes) and of a

basis $(w_\lambda)_{\lambda \in \mathrm{Par}}$ defined in [6, Exercise 2.9.3 (c)] (which, while having interesting properties, hardly feels at home in combinatorics). So the $\mathbb{F}_q$-analogue of Λ I find is somewhat of an empty shell. Still, there are some surprises and my hope is not lost that it can be made whole.

James Borger had a significant role in the studies made below. In particular, he suggested to me to look for analogues of Theorem 2.6 and Theorem 2.9 (which I found – Theorem 2.23 and Theorem 2.28), considering them as a litmus test that shows whether a functor really deserves to be called a Witt vector functor.

The $\mathbb{F}_q$-analogue of the Witt vectors uses the *Carlitz polynomials*; a highly readable introduction to these polynomials appears in [3].

This report is built as follows: In Section 1, we introduce notations and present basic definitions. In Section 2, we remind the reader of a construction (actually, one of many constructions) of the Witt vectors, and then introduce the $\mathbb{F}_q$-analogue of this construction. In Section 3, we shall give detailed proofs for some of the claims made before. (This section is still under construction, so only few of the proofs are available.) In Section 4, we speculate on how this analogue could lead to an $\mathbb{F}_q$-analogue of Λ. In Section 5, we prove a formula for the so-called Carlitz logarithm which, while not having any direct relation to the rest of this report, has emerged in my experiments in connection to it.

Being a preliminary report, this one will occasionally make for some rough reading, although I am trying to make the more-or-less finished parts (Section 2) more-or-less readable. The reader is assumed to know about Witt vectors ([18] or [10] or [11, §1]) and a bit about Carlitz polynomials ([3]). Symmetric functions will only be really used in Section 4.

0.2. Remark on Borger's work

In [1, §1–§2], James Borger has generalized the notion of Witt vectors to a rather broad setting, which includes both the classical and the "nested" Witt vectors. His generalization also includes my Carlitz-Witt functor W_N in Theorem 2.4 below, namely when one takes $R = \mathbb{F}_q[T]$ and $E = \{\text{all maximal ideals of } R\}$. We have yet to fill in the details, but in a nutshell, the reason why our constructions are equivalent is that the universal property of our $W_N(B)$ given in Corollary 2.26 below is the same as the one for $W^{\mathrm{fl}}_{R,E}(A)$ in [1, Proposition 1.9 (c)] (up to technicalities). Thus, it appears likely that several of the results below are particular cases of results from [1]. Nevertheless, our approach to the Carlitz-Witt functor is different from Borger's, and somewhat more explicit.

1. Notations

1.1. General number theory

I use the symbol $\mathbb{P}$ for the set of all primes. Further, $\mathbb{N}$ denotes the set $\{0,1,2,...\}$, and $\mathbb{N}_+$ the set $\{1,2,3,...\}$.

A *nest* means a nonempty subset N of $\mathbb{N}_+$ such that for every element $d \in N$, every divisor of d lies in N. What I call "nest" is called a "nonempty truncation set" by some authors (e.g., by James Borger in some of his work), and a "divisor-stable set" by others (e.g., by Joseph Rabinoff in [18]).

For every prime p, the nest $\left\{1, p, p^2, p^3, ...\right\} = \left\{p^i \mid i \in \mathbb{N}\right\}$ is called $p^{\mathbb{N}}$.

For any prime p and any $n \in \mathbb{Z}$, we denote by $v_p(n)$ the largest nonnegative integer m satisfying $p^m \mid n$; this is set to be $+\infty$ if $n = 0$.

For any $n \in \mathbb{N}_+$, we denote by $\operatorname{PF} n$ the set of all prime divisors of n.

We let μ denote the Möbius function and ϕ the Euler totient function (both are defined on $\mathbb{N}_+$).

For every ring R and indeterminate T, we denote by $R[T]_+$ the set of all **monic** polynomials in the indeterminate T over R. (All rings are supposed to have a unity.)

We consider polynomials over fields to be analogous to integers.[1] Under this analogy, monic polynomials correspond to positive integers; divisibility of polynomials corresponds to divisibility of integers; monic irreducible polynomials correspond to primes. Thus, for example, if R is a field and $M \in R[T]_+$ is a monic polynomial, then a sum like $\sum_{D \mid M} a_D$ is to be read as a sum over all **monic** divisors of M, not over all arbitrary divisors of M. Moreover, if R is a field and $M \in R[T]_+$ is a monic polynomial, then $\operatorname{PF} M$ will denote the set of all monic irreducible divisors of M (rather than all irreducible divisors of M). Finally, if π is an irreducible polynomial in $R[T]_+$ and f is any polynomial in $R[T]_+$ (for a field R), then $v_\pi(f)$ means the largest nonnegative integer m satisfying $\pi^m \mid f$; this is set to be $+\infty$ if $f = 0$.

1.2. Algebra

We denote by **CRing** the category of commutative rings, and by $\mathbf{CRing}_R$ the category of commutative R-algebras for a fixed commutative ring R. Also, for any ring R, we denote by ${}_R\mathbf{Mod}$ the category of left R-modules.

We denote by Λ the ring of symmetric functions over $\mathbb{Z}$. (This is also known as **Symm** or *Sym*. See [6, §2] and [19, Chapter 7] for studies of this ring Λ.)

[1] This is a well-known analogy, often taught in number theory classes.

1.3. Carlitz polynomials

In discussing Carlitz polynomials, I use the notations from Keith Conrad's [3] (but I'm using blackboard bold instead of boldface for labelling rings; so what Conrad calls $\mathbf{F}_p$ will be called $\mathbb{F}_p$ here, etc.). In particular, let q be a prime power. For any $M \in \mathbb{F}_q[T]$, the Carlitz polynomial in $\mathbb{F}_q[T][X]$ corresponding to the polynomial M will be denoted by $[M]$. Let us recall how it is defined:

Definition 1.1. For every $n \in \mathbb{N}$, define a polynomial $[T^n] \in \mathbb{F}_q[T][X]$ recursively, by setting $\left[T^0\right] = X$ and $\left[T^n\right] = \left[T^{n-1}\right]^q + T\left[T^{n-1}\right]$ for every $n \geq 1$. For example,

$$\left[T^0\right] = X; \qquad \left[T^1\right] = \left[T^0\right]^q + T\left[T^0\right] = X^q + TX;$$
$$\left[T^2\right] = \left[T^1\right]^q + T\left[T^1\right] = \left(X^q + TX\right)^q + T\left(X^q + TX\right) = X^{q^2} + \left(T^q + T\right)X^q + T^2X.$$

(Here, we have used the fact that taking the q-th power is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_q[T][X]$.)

Now, if $M \in \mathbb{F}_q[T]$, then we define a polynomial $[M] \in \mathbb{F}_q[T][X]$ to be $a_0\left[T^0\right] + a_1\left[T^1\right] + \cdots + a_k\left[T^k\right]$, where the polynomial M is written in the form $M = a_0T^0 + a_1T^1 + \cdots + a_kT^k$. (In other words, we define a polynomial $[M] \in \mathbb{F}_q[T][X]$ in such a way that $[M]$ depends $\mathbb{F}_q$-linearly on M, and that our new definition of $[M]$ does not conflict with our existing definition of $[T^n]$ for $n \in \mathbb{N}$.) We call $[M]$ the *Carlitz polynomial* corresponding to M.

Carlitz polynomials can be used to take the above-mentioned analogy between $\mathbb{Z}$ and $\mathbb{F}_q[T]$ to a new level. Namely, evaluating a Carlitz polynomial $[M]$ at an element a of a commutative $\mathbb{F}_q[T]$-algebra A can be viewed as the analogue of taking the m-th power of an element a of a commutative ring A.

Notice that

$$[\pi](X) \equiv X^{q^{\deg \pi}} \bmod \pi \qquad \text{for any monic irreducible } \pi \in \mathbb{F}_q[T]. \tag{1}$$

(This is proven in [3, Theorem 2.11] in the case when q is a prime. In the general case, the proof is analogous.)

In the Carlitz context there is an obvious analogue of the Möbius function: it is simply the Möbius function of the lattice $\mathbb{F}_q[T]_+$ (whose partial order is the divisibility relation). In other words, it is the function $\mu : \mathbb{F}_q[T]_+ \to \{-1, 0, 1\}$ defined by

$$\mu(M) = \begin{cases} (-1)^{|\operatorname{PF} M|}, & \text{if } M \text{ is squarefree;} \\ 0, & \text{if } M \text{ is not squarefree} \end{cases} \qquad \text{for all } M \in \mathbb{F}_q[T]_+.$$

Yet, in the Carlitz context, there are two reasonable analogues of the Euler totient function. Let us give their definitions (which both are taken from [3]):

1. The first analogue is the function $\varphi_C : \mathbb{F}_q[T]_+ \to \mathbb{F}_q[T]_+$ defined by

$$\varphi_C(M) = M \prod_{\pi \in \operatorname{PF} M} \left(1 - \frac{1}{\pi}\right) = \sum_{D \mid M} \mu(D) \frac{M}{D} \qquad \text{for all } M \in \mathbb{F}_q[T]_+ .$$

Some properties of this φ_C are shown in [3, Theorem 4.5]. In particular, every $M \in \mathbb{F}_q[T]_+$ satisfies $M = \sum_{D \mid M} \varphi_C(D)$.

2. The second analogue is the function $\varphi : \mathbb{F}_q[T]_+ \to \mathbb{N}_+$ defined by

$$\varphi(M) = q^{\deg M} \prod_{\pi \in \operatorname{PF} M} \left(1 - \frac{1}{q^{\deg \pi}}\right) = \sum_{D \mid M} \mu(D) q^{\deg(M/D)} \qquad \text{for all } M \in \mathbb{F}_q[T]_+ .$$

This function appears in [3, Section 6]. It has the property that $\varphi(M) \equiv \mu(M) \bmod p$ for every $M \in \mathbb{F}_q[T]_+$ (where $p = \operatorname{char} \mathbb{F}_q$). Thus, $\varphi(M) = \mu(M)$ in $\mathbb{F}_q$. To us, this makes this function φ less interesting than φ_C.

The existence of two different analogues of the same thing is a phenomenon that we will see a few more times in this theory.

2. The Carlitz-Witt suite

2.1. The classical ghost-Witt equivalence theorem

There are several approaches to the notion of Witt vectors. One of these approaches is based on the following theorem (the "ghost-Witt equivalence theorem", also known in parts as "Dwork's lemma"):

Theorem 2.1. Let N be a nest. Let A be a commutative ring. For every $n \in N$, let $\varphi_n : A \to A$ be an endomorphism of the additive group A.

Further, let us make three more assumptions:

Assumption 1: For every $n \in N$, the map φ_n is an endomorphism of the **ring** A.

Assumption 2: We have $\varphi_p(a) \equiv a^p \bmod pA$ for every $a \in A$ and $p \in \mathbb{P} \cap N$.

Assumption 3: We have $\varphi_1 = \operatorname{id}$, and we have $\varphi_n \circ \varphi_m = \varphi_{nm}$ for every $n \in N$ and every $m \in N$ satisfying $nm \in N$.

Let $(b_n)_{n \in N} \in A^N$ be a family of elements of A. Then, the following assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$, and $\mathcal{J}$ are equivalent:

Assertion $\mathcal{C}$: Every $n \in N$ and every $p \in \operatorname{PF} n$ satisfy

$$\varphi_p\left(b_{n/p}\right) \equiv b_n \bmod p^{v_p(n)} A.$$

Assertion $\mathcal{D}$: There exists a family $(x_n)_{n \in N} \in A^N$ of elements of A such that

$$\left(b_n = \sum_{d \mid n} d x_d^{n/d} \text{ for every } n \in N\right).$$

Assertion $\mathcal{E}$: There exists a family $(y_n)_{n \in N} \in A^N$ of elements of A such that

$$\left(b_n = \sum_{d \mid n} d \varphi_{n/d}\left(y_d\right) \text{ for every } n \in N \right).$$

Assertion $\mathcal{F}$: Every $n \in N$ satisfies

$$\sum_{d \mid n} \mu\left(d\right) \varphi_d\left(b_{n/d}\right) \in nA.$$

Assertion $\mathcal{G}$: Every $n \in N$ satisfies

$$\sum_{d \mid n} \phi\left(d\right) \varphi_d\left(b_{n/d}\right) \in nA.$$

Assertion $\mathcal{H}$: Every $n \in N$ satisfies

$$\sum_{i=1}^{n} \varphi_{n/\gcd(i,n)}\left(b_{\gcd(i,n)}\right) \in nA.$$

Assertion $\mathcal{J}$: There exists a ring homomorphism from the ring Λ to A which sends p_n (the n-th power sum symmetric function) to b_n for every $n \in N$.

Definition 2.2. The families $(b_n)_{n \in N} \in A^N$ which satisfy the equivalent assertions $\mathcal{C}$, $\mathcal{D}$, $\mathcal{E}$, $\mathcal{F}$, $\mathcal{G}$, $\mathcal{H}$, and $\mathcal{J}$ of Theorem 2.1 will be called *ghost-Witt vectors* (over A).

There are many variations on Theorem 2.1. An easy way to get a more intuitive particular case of Theorem 2.1 is to set $\varphi_n = \mathrm{id}_A$ for all $n \in N$, after which Assumptions 1 and 3 become tautologies. However, Assumption 2 is not guaranteed to hold in this setting; but it holds in $\mathbb{Z}$, and more generally in binomial rings, and in some non-torsionfree rings as well. Unfortunately, this case is in some sense too simple: it is too weak to yield the basic properties of Witt vectors (such as the well-definedness of addition, multiplication, Frobenius and Verschiebung). Instead one needs the case when A is a polynomial ring $\mathbb{Z}\left[\Xi\right]$ for some family Ξ of indeterminates, and the maps φ_n are defined by $\varphi_n\left(P\right) = P\left(\Xi^n\right)$ for every $P \in \mathbb{Z}\left[\Xi\right]$ (where $P\left(\Xi^n\right)$ means the result of P upon substituting every variable by its n-th power). The only part of Theorem 2.1 which is needed for this proof is the equivalence $\mathcal{C} \Longleftrightarrow \mathcal{D}$.

The proof of Theorem 2.1 is everywhere and nowhere: it is a straightforward generalization of arguments easily found in literature, but I haven't seen it explicit in this generality anywhere. I've written it up (save for Assertion $\mathcal{J}$) in [7, Theorem 11]. Also, the proof of the whole Theorem 2.1 in the case when $N = \mathbb{N}_+$ appears in [6, Exercise 2.9.6]; it is not hard to derive the general case from it.

Some parts of Theorem 2.1 are valid in somewhat more general situations. The equivalence $\mathcal{C} \iff \mathcal{D}$ needs Assumptions 1 and 2 but not 3 (unsurprisingly), and the equivalence $\mathcal{C} \iff \mathcal{E} \iff \mathcal{F} \iff \mathcal{G} \iff \mathcal{H}$ needs only Assumption 3 (not 1 and 2; actually, A can be any additive group rather than a ring for this equivalence). The equivalence $\mathcal{D} \iff \mathcal{J}$ needs nothing. This is all old news.

2.2. Classical Witt vectors

We recall a way to define the classical notion of Witt vectors. We work with a nest N, so that both p-typical and big Witt vectors are provided for.

Definition 2.3. Let N be a nest. Let A be a commutative ring. The *ghost ring* of A will mean the ring A^N with componentwise ring structure (i. e., a direct product of rings A indexed over N). The *N-ghost map* $w_N : A^N \to A^N$ is the map defined by

$$w_N\left(\left(x_n\right)_{n\in N}\right) = \left(\sum_{d\mid n} d x_d^{n/d}\right)_{n\in N} \qquad \text{for all } \left(x_n\right)_{n\in N} \in A^N.$$

This N-ghost map is (generally) neither additive nor multiplicative.

The following theorem is easily derived from Theorem 2.1 (more precisely, the equivalence $\mathcal{C} \iff \mathcal{D}$) applied to the case $A = \mathbb{Z}\left[\Xi\right]$ and $\varphi_n\left(P\right) = P\left(\Xi^n\right)$:

Theorem 2.4. Let N be a nest. There exists a unique functor $W_N : \mathbf{CRing} \to \mathbf{CRing}$ with the following two properties:

– We have $W_N\left(A\right) = A^N$ **as a set** for every commutative ring A.

– The map $w_N : A^N \to A^N$ **regarded as a map** $W_N\left(A\right) \to A^N$ is a ring homomorphism for every commutative ring A.

This functor W_N is called the *N-Witt vector functor*. For every commutative ring A, we call the commutative ring $W_N\left(A\right)$ the *N-Witt vector ring over A*. Its zero is the family $\left(0\right)_{n\in N}$, and its unity is the family $\left(\delta_{n,1}\right)_{n\in N}$ (where $\delta_{u,v}$ is defined to be $\begin{cases} 1, & \text{if } u = v; \\ 0, & \text{if } u \neq v \end{cases}$ for any two objects u and v).

The map $w_N : W_N\left(A\right) \to A^N$ itself becomes a natural transformation from the functor W_N to the functor $\mathbf{CRing} \to \mathbf{CRing}$, $A \mapsto A^N$. We will call this natural transformation w_N as well.

Theorem 2.4 appears in [18, Theorem 2.6]. Note that a consequence of Theorem 2.4 is that the sum and the product of two ghost-Witt vectors **over any commutative ring** A are again ghost-Witt vectors. This is not an immediate consequence of Theorem 2.1 (because it is not clear how we could construct maps φ_n satisfying Assumptions 1, 2 and 3 over any commutative ring A), but rather requires a detour via $\mathbb{Z}\left[\Xi\right]$.

The following theorem ([18, Remark 2.9, part 3]) allows us to prove functorial identities by working with ghost components:

Theorem 2.5. Let N be a nest. For any commutative $\mathbb{Q}$-algebra A, the map $w_N : W_N(A) \to A^N$ is a ring isomorphism.

The Witt vector rings allow for an "almost-universal property" [18, Theorem 6.1]:

Theorem 2.6. Let N be a nest. Let A be a commutative ring such that no element of N is a zero-divisor in A. For every $n \in N$, let σ_n be a ring endomorphism of A. Assume that $\sigma_n \circ \sigma_m = \sigma_{nm}$ for any $n \in N$ and $m \in N$ satisfying $nm \in N$. Also assume that $\sigma_1 = \mathrm{id}$. Finally, assume that $\sigma_p(a) \equiv a^p \bmod pA$ for every prime $p \in N$ and every $a \in A$. Then, there exists a unique ring homomorphism $\varphi : A \to W_N(A)$ satisfying

$$(w_N \circ \varphi)(a) = (\sigma_n(a))_{n \in N} \qquad \text{for every } a \in A.$$

Now let us describe some known functorial operations on $W_N(A)$. I will follow [18] most of the time.

Theorem 2.7. Let N be a nest.

(a) Let m be a positive integer such that every $n \in N$ satisfies $mn \in N$. Then, there exists a unique natural transformation $\mathbf{f}_m : W_N \to W_N$ of **set-valued** (not ring-valued) functors such that any commutative ring A and any $\mathbf{x} \in W_N(A)$ satisfy

$$w_N(\mathbf{f}_m(\mathbf{x})) = (mn\text{-th coordinate of } w_N(\mathbf{x}))_{n \in N},$$

where $\mathbf{f}_m$ is short for $\mathbf{f}_m(A)$.

(b) This natural transformation $\mathbf{f}_m$ is actually a natural transformation $W_N \to W_N$ of **ring-valued** functors as well. That is, $\mathbf{f}_m : W_N(A) \to W_N(A)$ is a ring homomorphism for every commutative ring A. (Here, again, $\mathbf{f}_m$ stands short for $\mathbf{f}_m(A)$.) We call $\mathbf{f}_m$ the *m-th Frobenius* on W_N.

(c) We have $\mathbf{f}_1 = \mathrm{id}$. Any two positive integers n and m such that $\mathbf{f}_n$ and $\mathbf{f}_m$ are well-defined satisfy $\mathbf{f}_n \circ \mathbf{f}_m = \mathbf{f}_{nm}$.

(d) Let p be a prime such that every $n \in N$ satisfies $pn \in N$. We have $\mathbf{f}_p(\mathbf{x}) \equiv \mathbf{x}^p \bmod p$ (in $W_N(A)$) for every commutative ring A and every $\mathbf{x} \in W_N(A)$.

In one or the other form, Theorem 2.7 appears in most sources on Witt vectors; for example, it can be pieced together from parts of [18, Theorem 5.7, Proposition 5.9 and Proposition 5.12].

Here is the definition of Verschiebung ([18, Theorem 5.5 and Proposition 5.9]):

Theorem 2.8. Let N be a nest.

(a) Let m be a positive integer. Then, there exists a unique natural transformation $\mathbf{V}_m : W_N \to W_N$ of **set-valued** (not ring-valued) functors such that any commutative ring A and any $\mathbf{x} \in W_N(A)$ satisfy

$$w_N(\mathbf{V}_m(\mathbf{x})) = \left(\begin{cases} m \cdot \left(\frac{n}{m}\text{-th coordinate of } w_N(\mathbf{x}) \right), & \text{if } m \mid n; \\ 0, & \text{if } m \nmid n \end{cases} \right)_{n \in N},$$

where $\mathbf{V}_m$ is short for $\mathbf{V}_m(A)$.

(b) This natural transformation $\mathbf{V}_m$ is actually a natural transformation $W_N \to W_N$ of **abelian-group-valued** functors as well. More precisely, $\mathbf{V}_m : W_N(A) \to W_N(A)$ is a homomorphism of additive groups for every commutative ring A. (Here, again, $\mathbf{V}_m$ stands short for $\mathbf{V}_m(A)$.) We call $\mathbf{V}_m$ the *m-th Verschiebung* on W_N.

(c) We have $\mathbf{V}_1 = \mathrm{id}$. Any two positive integers n and m satisfy $\mathbf{V}_n \circ \mathbf{V}_m = \mathbf{V}_{nm}$.

(d) Actually, $\mathbf{V}_m\left((x_n)_{n \in N}\right) = \left(\begin{cases} x_{n/m}, & \text{if } m \mid n; \\ 0, & \text{if } m \nmid n \end{cases} \right)_{n \in N}$ for any positive integer m, any commutative ring A and any $(x_n)_{n \in N} \in W_N(A)$.

There are some equalities involving $\mathbf{V}_m$ and $\mathbf{f}_m$ which should be here, but I don't have the time to write them down. They definitely need to be checked for Carlitz analogues.

Finally, here is one possible definition of the comonadic Artin-Hasse exponential[2] ([18, Corollary 6.3]):

Theorem 2.9. Let N be a nest. Assume that $nm \in N$ for all $n \in N$ and $m \in N$.

(a) There exists a unique natural transformation $\mathrm{AH} : W_N \to W_N \circ W_N$ (of functors $\mathbf{CRing} \to \mathbf{CRing}$) such that every commutative ring A, every $n \in N$ and every $\mathbf{x} \in W_N(A)$ satisfy

$$(n\text{-th coordinate of } w_N(\mathrm{AH}(\mathbf{x}))) = \mathbf{f}_n(\mathbf{x})$$

(where w_N this time stands for the natural transformation w_N evaluated at the ring $W_N(A)$; thus, $w_N(\mathrm{AH}(\mathbf{x}))$ is an element of $(W_N(A))^N$).

(b) Let $n \in N$, and let A be a commutative ring. Let $w_n : W_N(A) \to A$ be the map sending each $\mathbf{x} \in W_N(A)$ to the n-th coordinate of $w_N(\mathbf{x})$. Then, $W_N(w_n) \circ \mathrm{AH} = \mathbf{f}_n$.

[2] This is something Hazewinkel, in [10, §16.45], calls Artin-Hasse exponential. I am not sure if I completely understand its relation to the usual Artin-Hasse exponential...

2.3. The Carlitz ghost-Witt equivalence theorem

Now, let us move to the Carlitz case.

Convention 2.10. From now on until the rest of Section 2, we let q denote an arbitrary prime power ($\neq 1$, that is), and let p be the prime whose power q is.

Definition 2.11. A *q-nest* means a nonempty subset N of $\mathbb{F}_q[T]_+$ such that for every element $P \in N$, every monic divisor of P lies in N.

Notice that any q-nest is a subset of $\mathbb{F}_q[T]_+$. Thus, any element of a q-nest must be a monic polynomial. Also, every q-nest contains 1 [3]. We shall use these facts without mention.

Definition 2.12. Let $P \in \mathbb{F}_q[T]_+$. Then, $\operatorname{PF} P$ denotes the set of all monic irreducible divisors of P in $\mathbb{F}_q[T]_+$.

Theorem 2.13. Let N be a q-nest. Let A be a commutative $\mathbb{F}_q[T]$-algebra. For every $P \in N$, let $\varphi_P : A \to A$ be an endomorphism of the $\mathbb{F}_q[T]$-module A.

Further, let us make three more assumptions:

Assumption 1: For every $P \in N$, the map φ_P is an endomorphism of the $\mathbb{F}_q[T]$**-algebra** A.

Assumption 2: We have $\varphi_\pi(a) \equiv [\pi](a) \bmod \pi A$ for every $a \in A$ and every monic irreducible $\pi \in N$. (This rewrites as follows: We have $\varphi_\pi(a) \equiv a^{q^{\deg \pi}} \bmod \pi A$ for every $a \in A$ and every monic irreducible $\pi \in N$.)

Assumption 3: We have $\varphi_1 = \mathrm{id}$, and we have $\varphi_P \circ \varphi_Q = \varphi_{PQ}$ for every $P \in N$ and every $Q \in N$ satisfying $PQ \in N$.

Let $(b_P)_{P \in N} \in A^N$ be a family of elements of A. Then, the following assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ are equivalent:

Assertion $\mathcal{C}_1$: Every $P \in N$ and every $\pi \in \operatorname{PF} P$ satisfy

$$\varphi_\pi(b_{P/\pi}) \equiv b_P \bmod \pi^{v_\pi(P)} A.$$

Assertion $\mathcal{D}_1$: There exists a family $(x_P)_{P \in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D \mid P} D \left[\frac{P}{D} \right] (x_D) \text{ for every } P \in N \right).$$

Assertion $\mathcal{D}_2$: There exists a family $(\widetilde{x}_P)_{P \in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D \mid P} D \widetilde{x}_D^{q^{\deg(P/D)}} \text{ for every } P \in N \right).$$

[3] *Proof.* Let N be a q-nest. We must prove that N contains 1.

Any q-nest is nonempty (by definition). Thus, N is nonempty (since N is a q-nest). In other words, there exists some $P \in N$. Consider this P. Now, 1 is a monic divisor of $P \in N$, and thus must itself belong to N (since N is a q-nest). In other words, N contains 1. Qed.

Assertion $\mathcal{E}_1$: There exists a family $(y_P)_{P \in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D \mid P} D\varphi_{P/D}\left(y_D\right) \text{ for every } P \in N \right).$$

Assertion $\mathcal{F}_1$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \mu\left(D\right) \varphi_D\left(b_{P/D}\right) \in PA.$$

Assertion $\mathcal{G}_1$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \varphi_C\left(D\right) \varphi_D\left(b_{P/D}\right) \in PA.$$

Assertion $\mathcal{G}_2$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \varphi\left(D\right) \varphi_D\left(b_{P/D}\right) \in PA.$$

For this Theorem 2.13 to be a complete analogue of Theorem 2.1, two assertions are missing: $\mathcal{H}$ and $\mathcal{J}$. Finding an analogue of $\mathcal{J}$ requires finding an analogue of Λ, which is the question that I have started this report with; approaches to it will be discussed in Section 4. Two other assertions ($\mathcal{D}$ and $\mathcal{G}$) have two analogues each. However, Assertion $\mathcal{G}_2$ is clearly equivalent to Assertion $\mathcal{F}_1$ because of $\varphi\left(M\right) \equiv \mu\left(M\right) \bmod p$ for every $M \in \mathbb{F}_q\left[T\right]_+$. I have written out the former assertion merely to produce a clearer view of the analogy.

The proof of Theorem 2.13 is analogous to that of (the respective parts of) Theorem 2.1, and finding it should not be difficult. (One of the easier ways to proceed is showing $\mathcal{D}_1 \Longleftrightarrow \mathcal{C}_1 \Longleftrightarrow \mathcal{D}_2$, $\mathcal{C}_1 \Longrightarrow \mathcal{F}_1 \Longrightarrow \mathcal{E}_1 \Longrightarrow \mathcal{C}_1$, $\mathcal{F}_1 \Longleftrightarrow \mathcal{G}_2$ and $\mathcal{E}_1 \Longleftrightarrow \mathcal{G}_1$. Two different analogues of Hensel's exponent lifting are used in proving $\mathcal{C}_1 \Longleftrightarrow \mathcal{D}_1$ and $\mathcal{C}_1 \Longleftrightarrow \mathcal{D}_2$.)

Definition 2.14. The families $(b_n)_{n \in N} \in A^N$ which satisfy the equivalent assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 2.13 will be called *Carlitz ghost-Witt vectors* (over A).

What is more interesting is the following observation:

Remark 2.15. Assumption 1 in Theorem 2.13 can be replaced by the following weaker one:

Assumption 1': For every $P \in N$, the map φ_P is an endomorphism of the $\mathbb{F}_q\left[T\right]$-module A and commutes with the Frobenius endomorphism $A \to A$, $a \mapsto a^q$.

Moreover, instead of assuming that A be a commutative $\mathbb{F}_q[T]$-algebra, it is enough to assume that A is an $\mathbb{F}_q[T]$-module with an $\mathbb{F}_q$-linear Frobenius map $F : A \to A$ which satisfies

$$F(\lambda a) = \lambda^q F(a) \qquad \text{for every } \lambda \in \mathbb{F}_q[T] \text{ and } a \in A. \tag{2}$$

Of course, in this general setup, one has to **define** a^q to mean $F(a)$ for every $a \in A$. (Once this definition is made, the classical definition of $[P](a)$ for any $P \in \mathbb{F}_q[T]$ and any $a \in A$ should work perfectly.)

More about this in Subsection 2.5.

Here is why this is strange. One could wonder whether similar things hold in the classical case (Theorem 2.1): what if A is not a commutative ring but just an (additive) abelian group with "power operations" satisfying rules like $(a^n)^m = a^{nm}$? After all, the only way multiplication in A appears in Theorem 2.1 is through taking powers. However, the proof of Theorem 2.1 depends on exponent lifting, which uses multiplication and its commutativity in a nontrivial way. In contrast, the two exponent lifting lemmata used in the proof of Theorem 2.13 are both extremely simple and **do not** use multiplication in A. It seems that A being a ring is a red herring in Theorem 2.13.

I am wondering what use this generality can be put to. One possible field of application would be restricted Lie algebras. What is a good example of a restricted Lie algebra with an $\mathbb{F}_q[T]$-module structure?[4]

2.4. Carlitz-Witt vectors

Parroting Definition 2.3, we define:

Definition 2.16. Let N be a q-nest. Let A be a commutative $\mathbb{F}_q[T]$-algebra. The *Carlitz ghost ring* of A will mean the $\mathbb{F}_q[T]$-algebra A^N with componentwise $\mathbb{F}_q[T]$-algebra structure (i. e., a direct product of $\mathbb{F}_q[T]$-algebras A indexed over N). The *Carlitz N-ghost map* $w_N : A^N \to A^N$ is the map defined by

$$w_N\left((x_P)_{P\in N}\right) = \left(\sum_{D|P} D\left[\frac{P}{D}\right](x_D)\right)_{P\in N} \qquad \text{for all } (x_P)_{P\in N} \in A^N.$$

This N-ghost map is $\mathbb{F}_q$-linear but (generally) neither multiplicative nor $\mathbb{F}_q[T]$-linear.

From the equivalence $\mathcal{C}_1 \iff \mathcal{D}_1$ in Theorem 2.13, we can obtain:[5]

[4] Non-rhetorical question. Please let me know! (darijgrinberg[at]gmail.com)

[5] I'm not going to show the proof, as I don't think you will have any trouble reconstructing it. One has to set $A = \mathbb{F}_q[T][\Xi]$, where Ξ is a family of indeterminates, and define morphisms φ_P by $\varphi_P(Q) = Q([P](\Xi))$, where $[P](\Xi)$ means the family obtained by applying $[P]$ to

Theorem 2.17. Let N be a q-nest. There exists a unique functor $W_N : \mathbf{CRing}_{\mathbb{F}_q[T]} \to \mathbf{CRing}_{\mathbb{F}_q[T]}$ with the following two properties:

– We have $W_N(A) = A^N$ **as a set** for every commutative $\mathbb{F}_q[T]$-algebra A.

– The map $w_N : A^N \to A^N$ **regarded as a map** $W_N(A) \to A^N$ is an $\mathbb{F}_q[T]$-algebra homomorphism for every commutative $\mathbb{F}_q[T]$-algebra A.

This functor W_N is called the *Carlitz N-Witt vector functor*. For every $\mathbb{F}_q[T]$-algebra A, we call the $\mathbb{F}_q[T]$-algebra $W_N(A)$ the *Carlitz N-Witt vector ring over A*.

The map $w_N : W_N(A) \to A^N$ itself becomes a natural transformation from the functor W_N to the functor $\mathbf{CRing}_{\mathbb{F}_q[T]} \to \mathbf{CRing}_{\mathbb{F}_q[T]}$, $A \mapsto A^N$. We will call this natural transformation w_N as well.

This theorem, of course, yields that the sum and the product of two Carlitz ghost-Witt vectors **over any commutative $\mathbb{F}_q[T]$-algebra** is a Carlitz ghost-Witt vector, and that any $\mathbb{F}_q[T]$-multiple of a Carlitz ghost-Witt vector is a Carlitz ghost-Witt vector.

But this result is not optimal. In fact, it still holds in the more general setup of Remark 2.15. This can no longer be proven using Theorem 2.17, since the polynomial ring $\mathbb{F}_q[T][\Xi]$ is a free commutative $\mathbb{F}_q[T]$-algebra but not (in a reasonable way) a free object in the category of $\mathbb{F}_q[T]$-modules A with an $\mathbb{F}_q$-linear Frobenius map $F : A \to A$ which satisfies (2). I will lose some more words on this in Subsection 2.5.

Remark 2.18. Let N be a q-nest. The $\mathbb{F}_q$-vector space structure on the $\mathbb{F}_q[T]$-algebra $W_N(A)$ is just componentwise. Thus, w_N is an $\mathbb{F}_q$-vector space homomorphism when considered as a map $A^N \to A^N$. As a consequence, the zero of the $\mathbb{F}_q[T]$-algebra $W_N(A)$ is the family $(0)_{P \in N}$.

The unity of the $\mathbb{F}_q[T]$-algebra $W_N(A)$ is not as simple as it was in Theorem 2.4.

We have only used $\mathcal{C}_1 \iff \mathcal{D}_1$ so far. What about $\mathcal{C}_1 \iff \mathcal{D}_2$?

Definition 2.19. Let N be a q-nest. Let A be a commutative $\mathbb{F}_q[T]$-algebra. The *Carlitz tilde N-ghost map* $\widetilde{w}_N : A^N \to A^N$ is the map defined by

$$\widetilde{w}_N\left((x_P)_{P \in N}\right) = \left(\sum_{D \mid P} D x_D^{q^{\deg(P/D)}}\right)_{P \in N} \qquad \text{for all } (x_P)_{P \in N} \in A^N.$$

This tilde N-ghost map is $\mathbb{F}_q$-linear but (generally) neither multiplicative nor $\mathbb{F}_q[T]$-linear.

each variable in the family Ξ. Alternatively, one could define morphisms φ_P by $\varphi_P(Q) = Q\left(\Xi^{q^{\deg P}}\right)$; these are different morphisms but they also work here.

From the equivalence $\mathcal{C}_1 \iff \mathcal{D}_2$ in Theorem 2.13, we get:

Theorem 2.20. Let N be a q-nest. There exists a unique functor $\widetilde{W}_N : \mathbf{CRing}_{\mathbb{F}_q[T]} \to \mathbf{CRing}_{\mathbb{F}_q[T]}$ with the following two properties:

– We have $\widetilde{W}_N(A) = A^N$ **as a set** for every commutative $\mathbb{F}_q[T]$-algebra A.

– The map $\widetilde{w}_N : A^N \to A^N$ **regarded as a map** $\widetilde{W}_N(A) \to A^N$ is an $\mathbb{F}_q[T]$-algebra homomorphism for every commutative $\mathbb{F}_q[T]$-algebra A.

This functor $\widetilde{W}_N$ is called the *Carlitz tilde N-Witt vector functor*. For every $\mathbb{F}_q[T]$-algebra A, we call the $\mathbb{F}_q[T]$-algebra $\widetilde{W}_N(A)$ the *Carlitz tilde N-Witt vector ring over A*. The zero of this $\mathbb{F}_q[T]$-algebra $\widetilde{W}_N(A)$ is the family $(0)_{P \in N}$, and its unity is the family $(\delta_{P,1})_{P \in N}$ (where $\delta_{u,v}$ is defined to be $\begin{cases} 1, & \text{if } u = v; \\ 0, & \text{if } u \neq v \end{cases}$ for any two objects u and v).

The map $\widetilde{w}_N : \widetilde{W}_N(A) \to A^N$ itself becomes a natural transformation from the functor $\widetilde{W}_N$ to the functor $\mathbf{CRing}_{\mathbb{F}_q[T]} \to \mathbf{CRing}_{\mathbb{F}_q[T]}$, $A \mapsto A^N$. We will call this natural transformation $\widetilde{w}_N$ as well.

But we have not really found two really different functors...

Theorem 2.21. Let N be a q-nest. The functors W_N and $\widetilde{W}_N$ are isomorphic by an isomorphism which forms a commutative triangle with w_N and $\widetilde{w}_N$.

This is again proven using Theorem 2.13 and universal polynomials.

The following theorem allows us to prove functorial identities by working with ghost components:

Theorem 2.22. Let N be a q-nest. For any commutative $\mathbb{F}_q(T)$-algebra A, the maps $w_N : W_N(A) \to A^N$ and $\widetilde{w}_N : \widetilde{W}_N(A) \to A^N$ are $\mathbb{F}_q[T]$-algebra isomorphisms.

We have an "almost-universal property" again, following from exponent lifting and the implication $\mathcal{C}_1 \implies \mathcal{D}_1$ in Theorem 2.13:

Theorem 2.23. Let N be a q-nest. Let A be a commutative $\mathbb{F}_q[T]$-algebra such that no element of N is a zero-divisor in A. For every $P \in N$, let σ_P be an $\mathbb{F}_q[T]$-algebra endomorphism of A. Assume that $\sigma_P \circ \sigma_Q = \sigma_{PQ}$ for any $P \in N$ and $Q \in N$ satisfying $PQ \in N$. Also assume that $\sigma_1 = \mathrm{id}$. Finally, assume that $\sigma_\pi(a) \equiv [\pi](a) \bmod \pi A$ (or, equivalently, $\sigma_\pi(a) \equiv a^{q^{\deg \pi}} \bmod \pi A$) for every monic irreducible $\pi \in N$ and every $a \in A$. Then, there exists a unique $\mathbb{F}_q[T]$-algebra homomorphism $\varphi : A \to W_N(A)$ satisfying

$$(w_N \circ \varphi)(a) = (\sigma_P(a))_{P \in N} \qquad \text{for every } a \in A. \tag{3}$$

A similar result holds for $\widetilde{W}_N$ and $\widetilde{w}_N$.
What about Frobenius operations?

Theorem 2.24. Let N be a q-nest.

(a) Let $M \in \mathbb{F}_q[T]_+$ be such that every $P \in N$ satisfies $MP \in N$. Then, there exists a unique natural transformation $\mathbf{f}_M : W_N \to W_N$ of **set-valued** (not $\mathbb{F}_q[T]$-algebra-valued) functors such that any commutative $\mathbb{F}_q[T]$-algebra A and any $\mathbf{x} \in W_N(A)$ satisfy

$$w_N(\mathbf{f}_M(\mathbf{x})) = (MP\text{-th coordinate of } w_N(\mathbf{x}))_{P \in N},$$

where $\mathbf{f}_M$ is short for $\mathbf{f}_M(A)$.

(b) This natural transformation $\mathbf{f}_M$ is actually a natural transformation $W_N \to W_N$ of $\mathbb{F}_q[T]$**-algebra-valued** functors as well. That is, $\mathbf{f}_M : W_N(A) \to W_N(A)$ is an $\mathbb{F}_q[T]$-algebra homomorphism for every commutative $\mathbb{F}_q[T]$-algebra A. (Here, again, $\mathbf{f}_M$ stands short for $\mathbf{f}_M(A)$.) We call $\mathbf{f}_M$ the *M-th Frobenius* on W_N.

(c) We have $\mathbf{f}_1 = \mathrm{id}$. Any $P \in \mathbb{F}_q[T]_+$ and $Q \in \mathbb{F}_q[T]_+$ such that $\mathbf{f}_P$ and $\mathbf{f}_Q$ are well-defined satisfy $\mathbf{f}_P \circ \mathbf{f}_Q = \mathbf{f}_{PQ}$.

(d) Let $\pi \in \mathbb{F}_q[T]$ be a monic irreducible such that every $P \in N$ satisfies $\pi P \in N$. We have $\mathbf{f}_\pi(\mathbf{x}) \equiv [\pi](\mathbf{x}) \bmod \pi W_N(A)$ (in $W_N(A)$) for every commutative $\mathbb{F}_q[T]$-algebra A and every $\mathbf{x} \in W_N(A)$.

Corollary 2.25. Consider the setting of Theorem 2.23. Then (from Theorem 2.23) we know that there exists a unique $\mathbb{F}_q[T]$-algebra homomorphism $\varphi : A \to W_N(A)$ satisfying (3). Consider this φ. Let $M \in N$ be such that every $P \in N$ satisfies $MP \in N$. Then,

$$\varphi \circ \sigma_M = \mathbf{f}_M \circ \varphi \qquad \text{for every } M \in N.$$

Corollary 2.26. Consider the setting of Theorem 2.23. Assume that N is closed under multiplication (i.e., we have $MP \in N$ for every $M \in N$ and $P \in N$). Furthermore, let B be a commutative $\mathbb{F}_q[T]$-algebra such that no element of N is a zero-divisor in B. Let $\mathrm{proj}_B : W_N(B) \to B$ be the map sending every $u \in W_N(B)$ to the 1-st coordinate of $w_N(u) \in B^N$. This proj_B is an $\mathbb{F}_q[T]$-algebra homomorphism (since w_N is an $\mathbb{F}_q[T]$-algebra homomorphism).

Let $g : A \to B$ be an $\mathbb{F}_q[T]$-algebra homomorphism. Then, there exists a unique $\mathbb{F}_q[T]$-algebra homomorphism $G : A \to W_N(B)$ with the properties that $w_1 \circ G = g$ and that

$$G \circ \sigma_M = \mathbf{f}_M \circ g \qquad \text{for every } M \in N.$$

This G can be constructed as follows: Theorem 2.23 shows that there exists a unique $\mathbb{F}_q[T]$-algebra homomorphism $\varphi : A \to W_N(A)$ satisfying (3). Consider this φ. Since W_N is a functor, the $\mathbb{F}_q[T]$-algebra homomorphism $g : A \to$

B gives rise to an $\mathbb{F}_q[T]$-algebra homomorphism $W_N(g) : W_N(A) \to W_N(B)$. Now, the G is constructed as the composition $W_N(g) \circ \varphi$.

A Verschiebung exists too:

Theorem 2.27. Let N be a q-nest.

(a) Let $M \in \mathbb{F}_q[T]_+$. Then, there exists a unique natural transformation $\mathbf{V}_M : W_N \to W_N$ of **set-valued** (not $\mathbb{F}_q[T]$-algebra-valued) functors such that any commutative $\mathbb{F}_q[T]$-algebra A and any $\mathbf{x} \in W_N(A)$ satisfy

$$w_N(\mathbf{V}_M(\mathbf{x})) = \left(\begin{cases} M \cdot \left(\dfrac{P}{M}\text{-th coordinate of } w_N(\mathbf{x}) \right), & \text{if } M \mid P; \\ 0, & \text{if } M \nmid P \end{cases} \right)_{P \in N},$$

where $\mathbf{V}_M$ is short for $\mathbf{V}_M(A)$.

(b) This natural transformation $\mathbf{V}_M$ is actually a natural transformation $W_N \to W_N$ of **abelian-group-valued** functors as well. More precisely, $\mathbf{V}_M : W_N(A) \to W_N(A)$ is a homomorphism of additive groups for every commutative $\mathbb{F}_q[T]$-algebra A. (Here, again, $\mathbf{V}_M$ stands short for $\mathbf{V}_M(A)$.) We call $\mathbf{V}_M$ the *M-th Verschiebung* on W_N.

(c) We have $\mathbf{V}_1 = \mathrm{id}$. Any two $P \in \mathbb{F}_q[T]_+$ and $Q \in \mathbb{F}_q[T]_+$ satisfy $\mathbf{V}_P \circ \mathbf{V}_Q = \mathbf{V}_{PQ}$.

(d) Actually, $\mathbf{V}_M\left((x_P)_{P \in N}\right) = \left(\begin{cases} x_{P/M}, & \text{if } M \mid P; \\ 0, & \text{if } M \nmid P \end{cases} \right)_{P \in N}$ for any $P \in \mathbb{F}_q[T]_+$, any commutative $\mathbb{F}_q[T]$-algebra A and any $(x_P)_{P \in N} \in W_N(A)$.

And here is a Carlitz analogue of the Artin-Hasse exponential:

Theorem 2.28. Let N be a q-nest. Assume that $PQ \in N$ for all $P \in N$ and $Q \in N$.

(a) There exists a unique natural transformation $\mathrm{AH} : W_N \to W_N \circ W_N$ (of functors $\mathbf{CRing}_{\mathbb{F}_q[T]} \to \mathbf{CRing}_{\mathbb{F}_q[T]}$) such that every commutative $\mathbb{F}_q[T]$-algebra A, every $P \in N$ and every $\mathbf{x} \in W_N(A)$ satisfy

$$(P\text{-th coordinate of } w_N(\mathrm{AH}(\mathbf{x}))) = \mathbf{f}_P(\mathbf{x})$$

(where w_N this time stands for the natural transformation w_N evaluated at the $\mathbb{F}_q[T]$-algebra $W_N(A)$; thus, $w_N(\mathrm{AH}(\mathbf{x}))$ is an element of $(W_N(A))^N$).

(b) Let $P \in N$, and let A be a commutative $\mathbb{F}_q[T]$-algebra. Let $w_P : W_N(A) \to A$ be the map sending each $\mathbf{x} \in W_N(A)$ to the P-th coordinate of $w_N(\mathbf{x})$. Then, $W_N(w_P) \circ \mathrm{AH} = \mathbf{f}_P$.

2.5. $\mathcal{F}$-modules

The classical N-Witt vector functor for $N \subseteq \mathbb{N}_+$ being a nest is a functor **CRing** $\to$ **CRing**, and I don't see how to extend it to any broader category than **CRing**. The proof of its well-definedness, at least, uses the whole ring structure, not just the power maps. The situation with q-nests and their Carlitz N-Witt vector functors is different, as mentioned in Remark 2.15. Let me develop this a bit further, although I don't really understand where this all is headed.

Let $\mathcal{F}$ be the $\mathbb{F}_q$-algebra $\mathbb{F}_q \langle F, T \mid FT = T^q F \rangle$. This $\mathcal{F}$ can be considered as a skew polynomial ring $\mathbb{F}_q[T][F; \mathrm{Frob}]$ over the polynomial ring $\mathbb{F}_q[T]$, where $\mathrm{Frob} : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$ is the Frobenius endomorphism which sends every $a \in \mathbb{F}_q[T]$ to a^q.

Note that $\mathcal{F}$ is neither an $\mathbb{F}_q[T]$-algebra nor an $\mathbb{F}_q[F]$-algebra in the way I understand these words, since the center of $\mathcal{F}$ is $\mathbb{F}_q$. But we have well-defined $\mathbb{F}_q$-algebra homomorphisms $\mathbb{F}_q[T] \to \mathcal{F}$ and $\mathbb{F}_q[F] \to \mathcal{F}$, which make $\mathcal{F}$ into a left $\mathbb{F}_q[T]$-module, a right $\mathbb{F}_q[T]$-module, a left $\mathbb{F}_q[F]$-module, and a right $\mathbb{F}_q[F]$-module. The left $\mathbb{F}_q[T]$-module structure on $\mathcal{F}$ is probably the most useful one.

- As left $\mathbb{F}_q[T]$-module, $\mathcal{F}$ is free with basis $\left(F^i\right)_{i \geq 0}$ and thus torsionfree (this will be useful).
- As right $\mathbb{F}_q[T]$-module, $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{i \geq 0,\ 0 \leq j < q^i}$.
- As right $\mathbb{F}_q[F]$-module, $\mathcal{F}$ is free with basis $\left(T^j\right)_{j \geq 0}$.
- As left $\mathbb{F}_q[F]$-module, $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{i=0 \text{ or } q \nmid j}$. As a consequence, it is torsionfree (but this also follows from the isomorphism $\mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ introduced below).
- As $\mathbb{F}_q[F]$-$\mathbb{F}_q[T]$-bimodule, $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{(i=0 \text{ or } q \nmid j) \text{ and } 0 \leq j < q^i}$ (that is, $\mathcal{F} = \bigoplus_{\substack{(i,j) \in \mathbb{N}^2; \\ (i=0 \text{ or } q \nmid j) \text{ and } 0 \leq j < q^i}} \mathbb{F}_q[F] \cdot \left(T^j F^i\right) \cdot \mathbb{F}_q[T]$, and each $\mathbb{F}_q[F] \cdot \left(T^j F^i\right) \cdot \mathbb{F}_q[T]$ is isomorphic to $\mathbb{F}_q[F] \otimes \mathbb{F}_q[T]$ as an $\mathbb{F}_q[F]$-$\mathbb{F}_q[T]$-bimodule).

These freeness statements actually have little to do with $\mathbb{F}_q$ or the fact that q is a prime power. They are combinatorial consequences of the fact that $\mathcal{F}$ is the monoid algebra (over $\mathbb{F}_q$) of the monoid $\langle F, T \mid FT = T^q F \rangle$, which monoid is cancellative and whose elements can be uniquely written in the form $T^j F^i$ with $(i, j) \in \mathbb{N}^2$. Actually, this monoid is $\mathcal{J}$-trivial. Finite $\mathcal{J}$-trivial monoids have a very nice representation theory [4]; does ours?[6]

Every commutative $\mathbb{F}_q[T]$-algebra is canonically an $\mathcal{F}$-module, by letting T act as left multiplication with T, and letting F act as taking the q-th power in the algebra.

[6] I wouldn't hope for much; the representation theory of $\langle F, T \mid FT = TF \rangle$ is supposedly ugly.

Let us notice that $FP = P^q F$ in $\mathcal{F}$ for every $P \in \mathbb{F}_q[T]$. This is rather important; it yields that $\mathcal{F} \cdot P \cdot \mathcal{F} \subseteq P \cdot \mathcal{F}$ for every $P \in \mathbb{F}_q[T]$.

By the universal property of the polynomial ring, there exists a unique $\mathbb{F}_q$-algebra homomorphism $\operatorname{Carl} : \mathbb{F}_q[T] \to \mathcal{F}$ which sends T to $F + T$. This Carl is a very important homomorphism.

There is another interesting, and important, map around here. Let $\mathbb{F}_q[T][X]_{q-\lin}$ be the $\mathbb{F}_q[T]$-submodule of the polynomial ring $\mathbb{F}_q[T][X]$ consisting of all **q-polynomials**, i. e., polynomials in which only the monomials X^{q^0}, X^{q^1}, X^{q^2}, ... appear (we consider T as a constant here). Then, $\mathbb{F}_q[T][X]_{q-\lin}$ is not an algebra under usual multiplication, but a (noncommutative) algebra under composition (where again X is the variable and T a constant). It turns out that

$$\begin{aligned} &\mathcal{F} \to \mathbb{F}_q[T][X]_{q-\lin}, \\ &F \mapsto X^q, \\ &T \mapsto TX \end{aligned}$$

yields a well-defined $\mathbb{F}_q$-algebra isomorphism $\mathcal{F} \to \mathbb{F}_q[T][X]_{q-\lin}$. This is easy to check. This isomorphism allows transferring some results from $\mathbb{F}_q[T][X]$ to $\mathcal{F}$ (this is, for example, how I show that $\mathcal{F}$ is a torsionfree right $\mathbb{F}_q[T]$-module).

It can be shown that for every monic irreducible $\pi \in \mathbb{F}_q[T]$,

$$\text{there exists a unique } u(\pi) \in \mathcal{F} \text{ such that } \operatorname{Carl}\pi = F^{\deg \pi} + \pi \cdot u(\pi). \tag{4}$$

[7] Indeed, this follows easily from the fact that $[\pi](X) \equiv X^{q^{\deg \pi}} \bmod \pi$ in $\mathbb{F}_q[T][X]$ using the isomorphism $\mathcal{F} \to \mathbb{F}_q[T][X]_{q-\lin}$.

Now, what is a left $\mathcal{F}$-module? One way to see a left $\mathcal{F}$-module is as a left $\mathbb{F}_q[T]$-module A with an $\mathbb{F}_q$-linear map $F : A \to A$ which satisfies $F(Ta) = T^q F(a)$ for every $a \in A$. This is easily seen to be equivalent to a left $\mathbb{F}_q[T]$-module A with an $\mathbb{F}_q$-linear map $F : A \to A$ which satisfies $F(\lambda a) = \lambda^q F(a)$ for every $\lambda \in \mathbb{F}_q[T]$ and $a \in A$. In every left $\mathcal{F}$-module A, we can **define** the operation of "taking the q-th power" by $a^q = F(a)$ for every $a \in A$. Hence, we can define an operation of "taking the q^i-th power" for every $i \geq 0$. This allows us to evaluate any Carlitz polynomial at elements of A; that is, for any $P \in \mathbb{F}_q[T]$ and $a \in A$ we can define $[P](a) \in A$ (in the same way as this is usually defined for A being a commutative algebra). It is easily seen that

$$[P](a) = (\operatorname{Carl}(P))(a) \qquad \text{for any } P \in \mathbb{F}_q[T] \text{ and } a \in A.$$

Now, the situation described in Remark 2.15 is simply understood as having a left $\mathcal{F}$-module A, and for every $P \in N$, an $\mathcal{F}$-module endomorphism φ_P of A.

The category of left $\mathcal{F}$-modules has its free objects, which simply are free left $\mathcal{F}$-modules. If Ξ is a set (to be viewed as a set of "indeterminates"), then

[7] The notation $u(\pi)$ means that u depends on π; it is not meant to imply that $u(\pi)$ is a polynomial in π.

a family of $\mathcal{F}$-module endomorphisms φ_P of the free $\mathcal{F}$-module $\mathcal{F}\Xi$ satisfying Assumptions 1′, 2 and 3 can be easily constructed (namely, φ_P is the unique $\mathcal{F}$-module homomorphism $\mathcal{F}\Xi \to \mathcal{F}\Xi$ satisfying $\varphi_P(\xi) = [P](\xi)$ for every $\xi \in \Xi$), although it took me a while to show that they actually satisfy Assumption 2 (here I used (4)).

If I haven't done any mistakes, all results of Subsection 2.4 carry over to the category of $\mathcal{F}$-modules; of course, W_N and $\widetilde{W}_N$ will then be functors from ${}_{\mathcal{F}}\mathbf{Mod}$ to ${}_{\mathcal{F}}\mathbf{Mod}$. One has to be somewhat careful in the proofs because $\mathcal{F}$ is noncommutative and it needs to be used that every $P \in \mathbb{F}_q[T]$ satisfies $\mathcal{F} \cdot P \cdot \mathcal{F} \subseteq P \cdot \mathcal{F}$.

3. Proofs

In this (so far unfinished) Section, I am going to prove most of the statements made in Section 2. I shall start from scratch and forget about all the notation introduced in Section 2; this notation will be reintroduced when the need for it arises.

In Section 2, I presented the results for the case of commutative $\mathbb{F}_q[T]$-algebras first, and then pointed out how they can be generalized to $\mathcal{F}$-modules. In the present Section 3, however, I will proceed the other way round, starting with the properties of $\mathcal{F}$. The latter properties are unlikely to be new, as they are elementary and concern a well-studied object ($\mathcal{F}$ is one of the most basic examples of an Ore extension); in particular I suspect that some of them appear in [16] and [17] (two references I regrettably have not had the time to read).

3.1. The skew polynomial ring $\mathcal{M}$

Let us first show a general fact:

Proposition 3.1. Let $\mathbb{K}$ be a commutative ring. Let r be a positive integer. Let $\mathcal{M}$ be the $\mathbb{K}$-algebra $\mathbb{K}\langle F, T \mid FT = T^r F\rangle$. There are well-defined $\mathbb{K}$-algebra homomorphisms $\mathbb{K}[T] \to \mathcal{M}$ (sending T to T) and $\mathbb{K}[F] \to \mathcal{M}$ (sending F to F). These homomorphisms make $\mathcal{M}$ into a left $\mathbb{K}[T]$-module, a right $\mathbb{K}[T]$-module, a left $\mathbb{K}[F]$-module, and a right $\mathbb{K}[F]$-module. Any of these two left module structures can be combined with any of these two right module structures to form a bimodule structure on $\mathcal{M}$ (for example, the left $\mathbb{K}[T]$-module structure and the right $\mathbb{K}[F]$-module structure on $\mathcal{M}$ can be combined to form an $\mathbb{K}[T]$-$\mathbb{K}[F]$-bimodule structure on $\mathcal{M}$). (However, in general, $\mathcal{M}$ is neither a $\mathbb{K}[T]$-algebra nor a $\mathbb{K}[F]$-algebra.)

(a) We have $F^a T^b = T^{r^a b} F^a$ in $\mathcal{M}$ for every $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

(b) The $\mathbb{K}$-module $\mathcal{M}$ is free with basis $\left(T^j F^i\right)_{i \geq 0,\ j \geq 0}$.

(c) As left $\mathbb{K}[T]$-module, $\mathcal{M}$ is free with basis $\left(F^i\right)_{i \geq 0}$.

(d) As right $\mathbb{K}[T]$-module, $\mathcal{M}$ is free with basis $\left(T^j F^i\right)_{i \geq 0,\ 0 \leq j < r^i}$.

(e) As right $\mathbb{K}[F]$-module, $\mathcal{M}$ is free with basis $\left(T^j\right)_{j\geq 0}$.

(f) As left $\mathbb{K}[F]$-module, $\mathcal{M}$ is free with basis $\left(T^jF^i\right)_{i=0 \text{ or } r\nmid j}$.

(g) As $\mathbb{K}[F]$-$\mathbb{K}[T]$-bimodule, $\mathcal{M}$ is free with basis $\left(T^jF^i\right)_{(i=0 \text{ or } r\nmid j) \text{ and } 0\leq j<r^i}$ (that is, we have $\mathcal{M} = \bigoplus_{\substack{(i,j)\in\mathbb{N}^2; \\ (i=0 \text{ or } r\nmid j) \text{ and } 0\leq j<r^i}} \mathbb{K}[F]\cdot\left(T^jF^i\right)\cdot\mathbb{K}[T]$, and each $\mathbb{K}[F]\cdot\left(T^jF^i\right)\cdot\mathbb{K}[T]$ is isomorphic to $\mathbb{K}[F]\otimes\mathbb{K}[T]$ as an $\mathbb{K}[F]$-$\mathbb{K}[T]$-bimodule, where the tensor product is taken over $\mathbb{K}$).

We notice that the $\mathbb{K}$-algebra $\mathcal{M}$ in Proposition 3.1 is actually the monoid algebra (over $\mathbb{K}$) of the monoid with generators F, T and relation $FT = T^rF$. From this viewpoint, all of Proposition 3.1 is easily revealed to be a monoid-theoretical statement (with $\mathbb{K}$ being merely a distraction). However, we shall work with $\mathbb{K}$-algebras rather than monoids for the whole proof, if only for the sake of habitualness.

The only parts of Proposition 3.1 that will be used in the following are parts **(a)**, **(b)**, **(c)** and **(e)**. These are also the easiest ones to prove, so we advise the reader to skip most of the following technical proof.

The following lemma will be used in our proof of Proposition 3.1 **(f)**:

Lemma 3.2. Let S be a set. Let $\phi : S \to S$ be an injective map. Let $\ell : S \to \mathbb{N}$ be a map. Assume that

$$\ell(\phi(s)) > \ell(s) \qquad \text{for every } s \in S. \tag{5}$$

Let $B = S \setminus \phi(S)$. Define a map $\rho : B \times \mathbb{N} \to S$ by

$$\rho(s,k) = \phi^k(s) \qquad \text{for every } (s,k) \in B \times \mathbb{N}.$$

Then, ρ is a bijection.

(If we want to interpret Lemma 3.2 constructively, then we should also require that there is an algorithm which, given an $s \in S$, either reveals that $s \notin \phi(S)$ or computes a preimage of s under ϕ.)

Proof of Lemma 3.2. Let us first prove that the map ρ is injective.

Indeed, let (s,k) and (s',k') be two elements of $B \times \mathbb{N}$ such that $\rho(s,k) = \rho(s',k')$. We are going to prove that $(s,k) = (s',k')$.

The definition of ρ yields $\rho(s,k) = \phi^k(s)$. Thus, $\phi^k(s) = \rho(s,k) = \rho(s',k') = \phi^{k'}(s')$ (by the definition of ρ).

The map $\phi^{k'}$ is injective (since ϕ is injective).

We have $s' \in B = S \setminus \phi(S)$. Thus, $s' \notin \phi(S)$.

Now, assume (for the sake of contradiction) that $k > k'$. Hence, $\phi^k(s) = \phi^{k'+(k-k')}(s) = \phi^{k'}\left(\phi^{k-k'}(s)\right)$. But the map $\phi^{k'}$ is injective. Therefore, from

$\phi^{k'}\left(\phi^{k-k'}(s)\right) = \phi^k(s) = \phi^{k'}(s')$, we obtain $\phi^{k-k'}(s) = s'$. Hence, $s' = \phi^{k-k'}(s) \in \phi^{k-k'}(S) \subseteq \phi(S)$ (since $k - k' \geq 1$ (since $k > k'$)). This contradicts $s' \notin \phi(S)$. This contradiction proves that our assumption (that $k > k'$) was false. Hence, we cannot have $k > k'$. In other words, we must have $k \leq k'$. An analogous argument shows that $k' \leq k$. Combining this with $k \leq k'$, we obtain $k = k'$. Thus, $\phi^k(s) = \phi^{k'}(s)$, so that $\phi^{k'}(s) = \phi^k(s) = \phi^{k'}(s')$. This yields $s = s'$ (since the map $\phi^{k'}$ is injective). Combining this with $k = k'$, we obtain $(s,k) = (s',k')$.

Let us now forget that we fixed (s,k) and (s',k'). We thus have shown that if (s,k) and (s',k') are two elements of $B \times \mathbb{N}$ such that $\rho(s,k) = \rho(s',k')$, then $(s,k) = (s',k')$. In other words, the map ρ is injective.

Let us now show that the map ρ is surjective. Indeed, we shall prove that

$$\ell^{-1}(n) \subseteq \rho(B \times \mathbb{N}) \qquad \text{for every } n \in \mathbb{N}. \tag{6}$$

Proof of (6): We shall prove (6) by strong induction over n. Thus, we fix an $N \in \mathbb{N}$, and we assume (as the induction hypothesis) that (6) holds for every $n < N$. Now we must prove that (6) holds for $n = N$. In other words, we must prove that $\ell^{-1}(N) \subseteq \rho(B \times \mathbb{N})$.

Let $x \in \ell^{-1}(N)$. Thus, $x \in S$ and $\ell(x) = N$. We shall prove that $x \in \rho(B \times \mathbb{N})$.

If $x \notin \phi(S)$, then $x \in \rho(B \times \mathbb{N})$ holds[8]. Hence, for the rest of the proof of $x \subseteq \rho(B \times \mathbb{N})$, we can WLOG assume that $x \in \phi(S)$. Assume this. Thus, there exists an $s \in S$ such that $x = \phi(s)$. Consider this s. From $x = \phi(s)$, we obtain $\ell(x) = \ell(\phi(s)) > \ell(s)$ (by (5)). Hence, $\ell(s) < \ell(x) = N$. Therefore, the induction hypothesis shows that (6) holds for $n = \ell(s)$. In other words, $\ell^{-1}(\ell(s)) \subseteq \rho(B \times \mathbb{N})$. But $s \in \ell^{-1}(\ell(s)) \subseteq \rho(B \times \mathbb{N})$. In other words, there exists a $(t,k) \in B \times \mathbb{N}$ such that $s = \rho(t,k)$. Consider this (t,k). We have $s = \rho(t,k) = \phi^k(t)$ (by the definition of ρ), and $x = \phi\left(\underbrace{s}_{=\phi^k(t)}\right) = \phi\left(\phi^k(t)\right) = \phi^{k+1}(t)$. Comparing this with $\rho(t,k+1) = \phi^{k+1}(t)$ (by the definition of ρ), we obtain $x = \rho(t,k+1) \in \rho(B \times \mathbb{N})$. Hence, $x \in \rho(B \times \mathbb{N})$ is proven.

Let us now forget that we fixed x. We thus have shown that $x \in \rho(B \times \mathbb{N})$ for every $x \in \ell^{-1}(N)$. In other words, $\ell^{-1}(N) \subseteq \rho(B \times \mathbb{N})$. In other words, (6) holds for $n = N$. This completes the induction proof of (6).

Now, ℓ is a map $S \to \mathbb{N}$. Hence, $S = \bigcup_{n \in \mathbb{N}} \underbrace{\ell^{-1}(n)}_{\substack{\subseteq \rho(B \times \mathbb{N}) \\ \text{(by (6))}}} \subseteq \bigcup_{n \in \mathbb{N}} \rho(B \times \mathbb{N}) \subseteq \rho(B \times \mathbb{N})$. In other words, the map ρ is surjective. Hence, the map ρ is bijective (since we already know that ρ is injective). This proves Lemma 3.2. □

We record two corollaries of Lemma 3.2:

[8] *Proof.* Assume that $x \notin \phi(S)$. Thus, $x \in S \setminus \phi(S) = B$, so that $(x,0) \in B \times \mathbb{N}$. Clearly, $\rho(x,0) = \phi^0(x) = x$, so that $x = \rho(x,0) \in \rho(B \times \mathbb{N})$, qed.

Corollary 3.3. Define a subset B of $\mathbb{N}^2$ by

$$B = \left\{ (i,j) \in \mathbb{N}^2 \mid i = 0 \text{ or } r \nmid j \right\}. \tag{7}$$

Define a map $\rho : B \times \mathbb{N} \to \mathbb{N}^2$ by

$$\rho\left((i,j),k\right) = \left(i+k, r^k j\right) \qquad \text{for every } ((i,j),k) \in B \times \mathbb{N}. \tag{8}$$

Then, the map ρ is a bijection.

Proof of Corollary 3.3. Let $\phi : \mathbb{N}^2 \to \mathbb{N}^2$ be the map defined by

$$\phi(i,j) = (i+1, rj) \qquad \text{for every } (i,j) \in \mathbb{N}^2.$$

It is clear that this map ϕ is injective (since $r > 0$). Moreover, $B = \mathbb{N}^2 \setminus \phi\left(\mathbb{N}^2\right)$ [9]. Given an $s \in S$, it is easy to algorithmically check whether $s \notin \phi\left(\mathbb{N}^2\right)$ (because of the equivalence $s \notin \phi\left(\mathbb{N}^2\right) \iff s \in \underbrace{\mathbb{N}^2 \setminus \phi\left(\mathbb{N}^2\right)}_{=B} \iff s \in B$), and if $s \in \phi\left(\mathbb{N}^2\right)$, then it is easy to compute a preimage of s under ϕ (indeed, if $s = (i,j) \in \phi\left(\mathbb{N}^2\right)$, then $\phi^{-1}(s) = (i-1, j/r)$).

Every $(i,j) \in \mathbb{N}^2$ and $k \in \mathbb{N}$ satisfy

$$\phi^k(i,j) = \left(i+k, r^k j\right). \tag{9}$$

[9] *Proof.* We have

$$\begin{aligned}
&\mathbb{N}^2 \setminus \phi\left(\mathbb{N}^2\right) \\
&= \left\{ (i,j) \in \mathbb{N}^2 \mid \text{there exists no } (u,v) \in \mathbb{N}^2 \text{ such that } (i,j) = \underbrace{\phi(u,v)}_{\substack{=(u+1,rv) \\ \text{(by the definition of } \phi\text{)}}} \right\} \\
&= \left\{ (i,j) \in \mathbb{N}^2 \mid \underbrace{\text{there exists no } (u,v) \in \mathbb{N}^2 \text{ such that } (i,j) = (u+1, rv)}_{\substack{\iff \left((i-1, j/r) \notin \mathbb{N}^2\right) \\ \iff (i-1 \notin \mathbb{N} \text{ or } j/r \notin \mathbb{N})}} \right\} \\
&= \left\{ (i,j) \in \mathbb{N}^2 \mid \underbrace{i-1 \notin \mathbb{N}}_{\iff (i=0)} \text{ or } \underbrace{j/r \notin \mathbb{N}}_{\iff (r \nmid j)} \right\} \\
&= \left\{ (i,j) \in \mathbb{N}^2 \mid i = 0 \text{ or } r \nmid j \right\} = B,
\end{aligned}$$

qed.

(Indeed, this follows easily by induction on k.) Thus,

$$\rho(s,k) = \phi^k(s) \qquad \text{for every } (s,k) \in B \times \mathbb{N} \tag{10}$$

[10].

Furthermore, define a map $\ell : \mathbb{N}^2 \to \mathbb{N}$ by

$$\ell(i,j) = i \qquad \text{for every } (i,j) \in \mathbb{N}^2.$$

It is easy to see that for every $s \in \mathbb{N}^2$, we have $\ell(\phi(s)) = \ell(s) + 1 > \ell(s)$. Thus, we can apply Lemma 3.2 to $S = \mathbb{N}^2$ (indeed, the equality (10) shows that our map $\rho : B \times \mathbb{N} \to \mathbb{N}^2$ is identical with the map $\rho : B \times \mathbb{N} \to S$ in Lemma 3.2). As a result, we conclude that ρ is a bijection. This proves Corollary 3.3. □

Corollary 3.4. Define a subset C of $\mathbb{N}^2$ by

$$C = \left\{ (i,j) \in \mathbb{N}^2 \mid (i = 0 \text{ or } r \nmid j) \text{ and } 0 \leq j < r^i \right\}. \tag{11}$$

Define a map $\zeta : C \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}^2$ by

$$\zeta((i,j),\ell,k) = \left(i+k, r^k\left(j + r^i\ell\right)\right) \qquad \text{for every } ((i,j),k,\ell) \in C \times \mathbb{N} \times \mathbb{N}. \tag{12}$$

Then, the map ζ is a bijection.

Proof of Corollary 3.4. Define a subset B of $\mathbb{N}^2$ by (7). Clearly, $C \subseteq B$.

Define a map $\tau : C \times \mathbb{N} \to B$ by

$$\tau((i,j),\ell) = \left(i, j + r^i\ell\right) \qquad \text{for every } ((i,j),\ell) \in C \times \mathbb{N}.$$

It is easy to see that this map τ is well-defined (i.e., that $\left(i, j + r^i\ell\right) \in B$ for every $((i,j),\ell) \in C \times \mathbb{N}$).

For every integer u and every positive integer v, we let $u\%v$ denote the remainder of u when divided by v, and we let $u//v$ denote the quotient of u

[10] *Proof of (10):* Let $(s,k) \in B \times \mathbb{N}$. Then, $s \in B \subseteq \mathbb{N}^2$. Hence, s can be written in the form (i,j) for some $i,j \in \mathbb{N}$. Consider these i,j. We have

$$\begin{aligned}
\phi^k\left(\underbrace{s}_{=(i,j)}\right) &= \phi^k(i,j) = \left(i+k, r^k j\right) && \text{(by (9))} \\
&= \rho\left(\underbrace{(i,j)}_{=s}, k\right) && \text{(by (8))} \\
&= \rho(s,k).
\end{aligned}$$

This proves (10).

when divided by v with remainder. Thus, $u//v \in \mathbb{Z}$, $u\%v \in \{0,1,\ldots,v-1\}$ and $u = (u//v)\, v + u\%v$.

Define a map $\gamma : B \to C \times \mathbb{N}$ by

$$\gamma(i,j) = \left(\left(i, j\%r^i\right), j//r^i\right) \qquad \text{for every } (i,j) \in B.$$

Again, it is easy to see that this map γ is well-defined (i.e., that $\left(\left(i, j\%r^i\right), j//r^i\right) \in C \times \mathbb{N}$ for every $(i,j) \in B$).

Furthermore, it is easy to see that the maps τ and γ are mutually inverse[11]. Hence, the map τ is a bijection.

We shall identify the set $C \times \mathbb{N} \times \mathbb{N}$ with $(C \times \mathbb{N}) \times \mathbb{N}$. Then, the map $\tau \times \mathrm{id}_{\mathbb{N}} : (C \times \mathbb{N}) \times \mathbb{N} \to B \times \mathbb{N}$ can be viewed as a map $C \times \mathbb{N} \times \mathbb{N} \to B \times \mathbb{N}$. This map $\tau \times \mathrm{id}_{\mathbb{N}}$ sends every $((i,j),\ell,k) \in C \times \mathbb{N} \times \mathbb{N}$ to $(\tau((i,j),\ell),k)$. Clearly, the map $\tau \times \mathrm{id}_{\mathbb{N}}$ is a bijection (since τ is a bijection).

On the other hand, define a map ρ as in Corollary 3.3. Then, Corollary 3.3

[11] *Proof.* Let us first show that $\tau \circ \gamma = \mathrm{id}$.

Indeed, every $(i,j) \in B$ satisfies

$$(\tau \circ \gamma)(i,j) = \tau\left(\underbrace{\gamma(i,j)}_{=\left(\left(i, j\%r^i\right), j//r^i\right)}\right) = \tau\left(\left(i, j\%r^i\right), j//r^i\right) = \left(i, \underbrace{j\%r^i + r^i\left(j//r^i\right)}_{=j}\right)$$

(by the definition of τ)

$$= (i,j).$$

Thus, $\tau \circ \gamma = \mathrm{id}$.

On the other hand, let us prove that $\gamma \circ \tau = \mathrm{id}$. Indeed, fix $((i,j),\ell) \in C \times \mathbb{N}$. Then, $(i,j) \in C$. Thus, $(i = 0$ or $r \nmid j)$ and $0 \le j < r^i$. Now,

$$(\gamma \circ \tau)((i,j),\ell) = \gamma\left(\underbrace{\tau((i,j),\ell)}_{=\left(i, j+r^i\ell\right)}\right) = \gamma\left(i, j + r^i\ell\right)$$

$$= \left(\left(i, \underbrace{\left(j + r^i\ell\right)\%r^i}_{\substack{=j \\ (\text{since } 0 \le j < r^i)}}\right), \underbrace{\left(j + r^i\ell\right)//r^i}_{\substack{=\ell \\ (\text{since } 0 \le j < r^i)}}\right) = ((i,j),\ell).$$

This proves that $\gamma \circ \tau = \mathrm{id}$. Combining this with $\tau \circ \gamma = \mathrm{id}$, we obtain that the maps τ and γ are mutually inverse, qed.

shows that the map ρ is a bijection. But every $((i,j),\ell,k) \in C \times \mathbb{N} \times \mathbb{N}$ satisfies

$$\begin{aligned}
&(\rho \circ (\tau \times \mathrm{id}_{\mathbb{N}}))((i,j),\ell,k) \\
&= \rho\left(\underbrace{(\tau \times \mathrm{id}_{\mathbb{N}})((i,j),\ell,k)}_{=(\tau((i,j),\ell),k)}\right) = \rho\left(\left(\underbrace{\tau((i,j),\ell)}_{=\left(i,j+r^i\ell\right)},k\right)\right) \\
&= \rho\left(\left(i,j+r^i\ell\right),k\right) = \left(i+k, r^k\left(j+r^i\ell\right)\right) \qquad \text{(by the definition of } \rho\text{)} \\
&= \zeta((i,j),\ell,k) \qquad \text{(by (12))}.
\end{aligned}$$

Hence, $\rho \circ (\tau \times \mathrm{id}_{\mathbb{N}}) = \zeta$. Since the map $\rho \circ (\tau \times \mathrm{id}_{\mathbb{N}})$ is a bijection (because both ρ and $\tau \times \mathrm{id}_{\mathbb{N}}$ are bijections), this shows that the map ζ is a bijection. This proves Corollary 3.4. □

Proof of Proposition 3.1. **(a)** First, we have the equality

$$FT^b = T^{rb}F \tag{13}$$

in $\mathcal{M}$ for every $b \in \mathbb{N}$ (this can be proven by straightforward induction over b). Using this equality, Proposition 3.1 **(a)** can be proven by straightforward induction over a.

(b) Let $\mathcal{N}$ be the free $\mathbb{K}$-module with basis $\left(a_{i,j}\right)_{i\geq 0,\ j\geq 0}$. We let $\mathfrak{f}$ be the $\mathbb{K}$-linear map $\mathcal{N} \to \mathcal{N}$ which sends every $a_{i,j}$ to $a_{i+1,rj}$. We let $\mathfrak{t}$ be the $\mathbb{K}$-linear map $\mathcal{N} \to \mathcal{N}$ which sends every $a_{i,j}$ to $a_{i,j+1}$. Every $i,j,k \in \mathbb{N}$ satisfy

$$\mathfrak{f}^k\left(a_{i,j}\right) = a_{i+k,r^k j} \tag{14}$$

and

$$\mathfrak{t}^k\left(a_{i,j}\right) = a_{i,j+k}. \tag{15}$$

(Both of these equalities are easily proven by induction over k.) Using (15), it is easy to see that $\mathfrak{f} \circ \mathfrak{t} = \mathfrak{t}^r \circ \mathfrak{f}$. Thus, we can define a $\mathbb{K}$-algebra homomorphism $\Phi : \mathcal{M} \to \operatorname{End}\mathcal{N}$ by setting

$$\Phi(F) = \mathfrak{f} \qquad \text{and} \qquad \Phi(T) = \mathfrak{t} \tag{16}$$

(where $\operatorname{End}\mathcal{N}$ denotes the $\mathbb{K}$-algebra of all $\mathbb{K}$-module endomorphisms of $\mathcal{N}$). Consider this Φ. For every $i,j \in \mathbb{N}$, we have

$$\Phi\left(T^jF^i\right) = \Phi(T)^j \circ \Phi(F)^i = \mathfrak{t}^j \circ \mathfrak{f}^i \qquad \text{(by (16))}$$

and thus

$$\begin{aligned}
\underbrace{\left(\Phi\left(T^jF^i\right)\right)}_{=\mathfrak{t}^j\circ\mathfrak{f}^i}(a_{0,0}) &= \left(\mathfrak{t}^j \circ \mathfrak{f}^i\right)(a_{0,0}) = \mathfrak{t}^j\left(\underbrace{\mathfrak{f}^i(a_{0,0})}_{\substack{=a_{i,0} \\ \text{(by (14))}}}\right) \\
&= \mathfrak{t}^j(a_{i,0}) = a_{i,j}
\end{aligned} \tag{17}$$

(by (15)). Hence, the family $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ of elements of $\mathcal{M}$ is $\mathbb{K}$-linearly independent[12].

Let us now show that this family spans $\mathcal{M}$. Indeed, let $\mathcal{M}'$ be the $\mathbb{K}$-submodule of $\mathcal{M}$ spanned by the family $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$. Then, $1 = T^0 F^0 \in \mathcal{M}'$. Moreover, the $\mathbb{K}$-submodule $\mathcal{M}'$ satisfies $T\mathcal{M}' \subseteq \mathcal{M}'$ (since $T \cdot T^j F^i = T^{j+1} F^i$ for every $i, j \in \mathbb{N}$) and $F\mathcal{M}' \subseteq \mathcal{M}'$ (since $F \cdot T^j F^i = \underbrace{FT^j}_{\substack{=T^{rj}F \\ \text{(by (13))}}} F^i = T^{rj} F F^i = T^{rj} F^{i+1}$ for every $i, j \in \mathbb{N}$). Hence, $\mathcal{M}'$ is a left $\mathcal{M}$-submodule of $\mathcal{M}$ (since the $\mathbb{K}$-algebra $\mathcal{M}$ is generated by F and T) [13]. Therefore, $\mathcal{M} \cdot \mathcal{M}' \subseteq \mathcal{M}'$. But $\mathcal{M} = \mathcal{M} \cdot \underbrace{1}_{\in \mathcal{M}'} \subseteq \mathcal{M} \cdot \mathcal{M}' \subseteq \mathcal{M}'$. This shows that the family $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ spans the $\mathbb{K}$-module $\mathcal{M}$ (since the $\mathbb{K}$-linear span of this family is $\mathcal{M}'$). Since we already know that this family is $\mathbb{K}$-linearly independent, we can thus conclude that this family is a basis of the $\mathbb{K}$-module $\mathcal{M}$. This proves Proposition 3.1 **(b)**.

(c) Let $(e_0, e_1, e_2, \ldots)$ be the standard basis of the left $\mathbb{K}[T]$-module $\mathbb{K}[T]^{(\mathbb{N})}$. Define a left $\mathbb{K}[T]$-module homomorphism $\alpha : \mathbb{K}[T]^{(\mathbb{N})} \to \mathcal{M}$ by sending each e_i to F^i. Define a $\mathbb{K}$-module homomorphism $\beta : \mathcal{M} \to \mathbb{K}[T]^{(\mathbb{N})}$ by sending each $T^j F^i$ to $T^j e_i$. (This β is well-defined, since Proposition 3.1 **(b)** shows that $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ is a basis of the $\mathbb{K}$-module $\mathcal{M}$.) It is easy to see that β is a left $\mathbb{K}[T]$-module homomorphism. It is straightforward to see that the homomorphisms α and β are mutually inverse. Thus, α is a left $\mathbb{K}[T]$-module isomorphism. As a consequence, the left $\mathbb{K}[T]$-module $\mathcal{M}$ has a basis $\left(\underbrace{\alpha(e_i)}_{=F^i}\right)_{i\geq 0} = \left(F^i\right)_{i\geq 0}$. This

[12] because any linear dependence relation $\sum_{i\geq 0,\ j\geq 0} \lambda_{i,j} T^j F^i = 0$ would yield

$$\sum_{i\geq 0,\ j\geq 0} \lambda_{i,j} \underbrace{a_{i,j}}_{\substack{=\left(\Phi\left(T^j F^i\right)\right)(a_{0,0}) \\ \text{(by (17))}}} = \sum_{i\geq 0,\ j\geq 0} \lambda_{i,j} \left(\Phi\left(T^j F^i\right)\right)(a_{0,0})$$

$$= \left(\Phi\left(\underbrace{\sum_{i\geq 0,\ j\geq 0} \lambda_{i,j} T^j F^i}_{=0}\right)\right)(a_{0,0}) = 0,$$

which would lead to $\left(\lambda_{i,j}\right)_{i\geq 0,\ j\geq 0} = (0)_{i\geq 0,\ j\geq 0}$ since the family $\left(a_{i,j}\right)_{i\geq 0,\ j\geq 0}$ is linearly independent

[13] This argument in more detail:

The $\mathbb{K}$-algebra $\mathcal{M}$ is generated by F and T. From this, it is easy to derive the following fact: If $\mathcal{V}$ is an $\mathbb{K}$-vector subspace of some left $\mathcal{M}$-module $\mathcal{U}$ satisfying $F\mathcal{V} \subseteq \mathcal{V}$ and $T\mathcal{V} \subseteq \mathcal{V}$, then $\mathcal{V}$ is a left $\mathcal{M}$-submodule of $\mathcal{U}$. Applying this to $\mathcal{U} = \mathcal{M}$ and $\mathcal{V} = \mathcal{M}'$, we conclude that $\mathcal{M}'$ is a left $\mathcal{M}$-submodule of $\mathcal{M}$ (since $F\mathcal{M}' \subseteq \mathcal{M}'$ and $T\mathcal{M}' \subseteq \mathcal{M}'$).

proves Proposition 3.1 **(c)**.

(d) For every integer u and every positive integer v, we let $u\%v$ denote the remainder of u when divided by v, and we let $u//v$ denote the quotient of u when divided by v with remainder. Thus, $u//v \in \mathbb{Z}$, $u\%v \in \{0,1,\ldots,v-1\}$ and $u = (u//v)\,v + u\%v$.

Let $\mathcal{G}$ be the free right $\mathbb{K}[T]$-module with basis $\left(g_{i,j}\right)_{i\geq 0,\ 0\leq j<r^i}$. Define a right $\mathbb{K}[T]$-module homomorphism $\alpha : \mathcal{G} \to \mathcal{M}$ by sending each $g_{i,j}$ to T^jF^i. Define a $\mathbb{K}$-module homomorphism $\beta : \mathcal{M} \to \mathcal{G}$ by sending each T^jF^i to $g_{i,j\%r^i}T^{j//r^i}$. (This β is well-defined, since Proposition 3.1 **(b)** shows that $\left(T^jF^i\right)_{i\geq 0,\ j\geq 0}$ is a basis of the $\mathbb{K}$-module $\mathcal{M}$.) It is easy to see that the homomorphisms α and β are mutually inverse[14]. Thus, α is a right $\mathbb{K}[T]$-module isomorphism. Since the

[14] *Proof.* We need to show that $\alpha\circ\beta = \mathrm{id}$ and $\beta\circ\alpha = \mathrm{id}$.

To prove that $\alpha\circ\beta = \mathrm{id}$, we need to show that $(\alpha\circ\beta)\left(T^jF^i\right) = T^jF^i$ for every $i,j\in\mathbb{N}$. So let us fix $i,j\in\mathbb{N}$. Then,

$$(\alpha\circ\beta)\left(T^jF^i\right) = \alpha\left(\underbrace{\beta\left(T^jF^i\right)}_{=g_{i,j\%r^i}T^{j//r^i}}\right) = \alpha\left(g_{i,j\%r^i}T^{j//r^i}\right) = \underbrace{\alpha\left(g_{i,j\%r^i}\right)}_{\substack{=T^{j\%r^i}F^i \\ \text{(by the definition of } \alpha\text{)}}} T^{j//r^i}$$

(since α is a right $\mathbb{K}[T]$-module homomorphism)

$$= T^{j\%r^i}\underbrace{F^iT^{j//r^i}}_{\substack{=T^{r^i\left(j//r^i\right)}F^i \\ \text{(by Proposition 3.1 (a),} \\ \text{applied to } a=i \text{ and } b=j//r^i\text{)}}} = \underbrace{T^{j\%r^i}T^{r^i\left(j//r^i\right)}}_{\substack{=T^{j\%r^i+r^i\left(j//r^i\right)}=T^j \\ \text{(since } j\%r^i+r^i\left(j//r^i\right)=\left(j//r^i\right)r^i+j\%r^i=j\text{)}}}F^i = T^jF^i,$$

which is what we wanted to prove.

Thus, $\alpha\circ\beta = \mathrm{id}$ is proven. It remains to prove that $\beta\circ\alpha = \mathrm{id}$.

We know that $\mathcal{G}$ is spanned by $\left(g_{i,j}\right)_{i\geq 0,\ 0\leq j<r^i}$ as a right $\mathbb{K}[T]$-module (by the definition of $\mathcal{G}$). Hence, $\mathcal{G}$ is spanned by $\left(g_{i,j}T^k\right)_{i\geq 0,\ 0\leq j<r^i,\ k\geq 0}$ as a $\mathbb{K}$-module. Hence, in order to prove that $\beta\circ\alpha = \mathrm{id}$, it suffices to show that $(\beta\circ\alpha)\left(g_{i,j}T^k\right) = g_{i,j}T^k$ for every $i\geq 0$, $0\leq j<r^i$ and $k\geq 0$.

So let us fix $i\geq 0$, $0\leq j<r^i$ and $k\geq 0$. The definition of α yields $\alpha\left(g_{i,j}\right) = T^jF^i$. But since α is a right $\mathbb{K}[T]$-module homomorphism, we have

$$\alpha\left(g_{i,j}T^k\right) = \underbrace{\alpha\left(g_{i,j}\right)}_{=T^jF^i}T^k = T^j\underbrace{F^iT^k}_{\substack{=T^{r^ik}F^i \\ \text{(by Proposition 3.1 (a),} \\ \text{applied to } a=i \text{ and } b=k\text{)}}} = \underbrace{T^jT^{r^ik}}_{=T^{j+r^ik}}F^i = T^{j+r^ik}F^i.$$

Now,

$$(\beta\circ\alpha)\left(g_{i,j}T^k\right) = \beta\left(\underbrace{\alpha\left(g_{i,j}T^k\right)}_{=T^{j+r^ik}F^i}\right) = \beta\left(T^{j+r^ik}F^i\right) = g_{i,\left(j+r^ik\right)\%r^i}T^{\left(j+r^ik\right)//r^i}. \tag{18}$$

right $\mathbb{K}[T]$-module $\mathcal{G}$ has a basis $\left(g_{i,j}\right)_{i\geq 0,\ 0\leq j<r^i}$, this shows that the right $\mathbb{K}[T]$-module $\mathcal{M}$ has a basis $\left(\underbrace{\alpha\left(g_{i,j}\right)}_{=T^jF^i}\right)_{i\geq 0,\ 0\leq j<r^i} = \left(T^jF^i\right)_{i\geq 0,\ 0\leq j<r^i}$. This proves Proposition 3.1 **(d)**.

(e) Let $(e_0, e_1, e_2, \ldots)$ be the standard basis of the right $\mathbb{K}[F]$-module $\mathbb{K}[F]^{(\mathbb{N})}$. Define a right $\mathbb{K}[F]$-module homomorphism $\alpha : \mathbb{K}[F]^{(\mathbb{N})} \to \mathcal{M}$ by sending each e_j to T^j. Define a $\mathbb{K}$-module homomorphism $\beta : \mathcal{M} \to \mathbb{K}[T]^{(\mathbb{N})}$ by sending each T^jF^i to e_jF^i. (This β is well-defined, since Proposition 3.1 **(b)** shows that $\left(T^jF^i\right)_{i\geq 0,\ j\geq 0}$ is a basis of the $\mathbb{K}$-module $\mathcal{M}$.) It is easy to see that β is a right $\mathbb{K}[F]$-module homomorphism. It is straightforward to see that the homomorphisms α and β are mutually inverse. Thus, α is a right $\mathbb{K}[F]$-module isomorphism. As a consequence, the right $\mathbb{K}[F]$-module $\mathcal{M}$ has a basis $\left(\underbrace{\alpha\left(e_j\right)}_{=T^j}\right)_{j\geq 0} = \left(T^j\right)_{j\geq 0}$. This proves Proposition 3.1 **(e)**.

(f) Define a subset B of $\mathbb{N}^2$ by (7). Define a map $\rho : B \times \mathbb{N} \to \mathbb{N}^2$ by (8). Corollary 3.3 shows that ρ is a bijection. Hence, its inverse $\rho^{-1} : \mathbb{N}^2 \to B \times \mathbb{N}$ is well-defined.

Now, let $\mathcal{H}$ be the free left $\mathbb{K}[F]$-module with basis $\left(h_{(i,j)}\right)_{(i,j)\in B}$. Define a left $\mathbb{K}[F]$-module homomorphism $\alpha : \mathcal{H} \to \mathcal{M}$ by sending each $h_{(i,j)}$ to T^jF^i. Define a $\mathbb{K}$-module homomorphism $\beta : \mathcal{M} \to \mathcal{H}$ by sending each T^jF^i to $F^k h_{(u,v)}$, where $((u,v),k) = \rho^{-1}(i,j)$. (This β is well-defined, since Proposition 3.1 **(b)** shows that $\left(T^jF^i\right)_{i\geq 0,\ j\geq 0}$ is a basis of the $\mathbb{K}$-module $\mathcal{M}$.) It is straightforward to see that the homomorphisms α and β are mutually inverse[15]. Thus, α is a left $\mathbb{K}[F]$-module isomorphism. As a consequence, the left $\mathbb{K}[F]$-module $\mathcal{M}$ has a basis

$$\left(\underbrace{\alpha\left(h_{(i,j)}\right)}_{=T^jF^i}\right)_{(i,j)\in B} = \left(T^jF^i\right)_{(i,j)\in B} = \left(T^jF^i\right)_{i=0 \text{ or } r\nmid j}$$

(since $B = \left\{(i,j) \in \mathbb{N}^2 \mid i = 0 \text{ or } r \nmid j\right\}$). This proves Proposition 3.1 **(f)**.

But $0 \leq j < r^i$. Hence, $\left(j + r^ik\right) \% r^i = j$ and $\left(j + r^ik\right) // r^i = k$. In view of these two equalities, (18) rewrites as $(\beta\circ\alpha)\left(g_{i,j}T^k\right) = g_{i,j}T^k$. This completes our proof of $\beta\circ\alpha = \mathrm{id}$. Thus, we have shown that α and β are mutually inverse.

[15] *Proof.* We need to show that $\alpha\circ\beta = \mathrm{id}$ and $\beta\circ\alpha = \mathrm{id}$.

To prove that $\alpha\circ\beta = \mathrm{id}$, we need to show that $(\alpha\circ\beta)\left(T^jF^i\right) = T^jF^i$ for every $i, j \in \mathbb{N}$. So let us fix $i, j \in \mathbb{N}$. Set $((u,v),k) = \rho^{-1}(i,j)$. Then, $(i,j) = \rho((u,v),k) = \left(u+k, r^kv\right)$ (by the definition of ρ). In other words, $i = u + k$ and $j = r^kv$.

(g) Define C and ζ as in Corollary 3.4. In this proof, the $\otimes$ sign always shall mean tensor products over $\mathbb{K}$.

Corollary 3.4 shows that the map ζ is a bijection. In other words, the map

$$C \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}^2, \qquad ((i,j),\ell,k) \mapsto \left(i+k, r^k\left(j + r^i \ell\right)\right) \tag{19}$$

is a bijection (since this map is the map ζ).

Proposition 3.1 **(b)** shows that $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ is a basis of the $\mathbb{K}$-module $\mathcal{M}$. We can reindex this basis using the bijection (19); thus, we conclude that

---

The definition of β shows that $\beta\left(T^j F^i\right) = F^k h_{(u,v)}$. Now,

$$(\alpha\circ\beta)\left(T^j F^i\right) = \alpha\left(\underbrace{\beta\left(T^j F^i\right)}_{=F^k h_{(u,v)}}\right) = \alpha\left(F^k h_{(u,v)}\right) = F^k \underbrace{\alpha\left(h_{(u,v)}\right)}_{\substack{=T^v F^u \\ \text{(by the definition of } \alpha\text{)}}}$$

$$\begin{aligned} &\left(\text{since } \alpha \text{ is a left } \mathbb{K}[F]\text{-module homomorphism}\right) \\ &= \underbrace{F^k T^v}_{\substack{=T^{r^k v} F^k \\ \text{(by Proposition 3.1 (a),} \\ \text{applied to } a=k \text{ and } b=v\text{)}}} F^u = \underbrace{T^{r^k v}}_{\substack{=T^j \\ \text{(since } r^k v = j\text{)}}} \underbrace{F^k F^u}_{\substack{=F^{u+k}=F^i \\ \text{(since } u+k=i\text{)}}} = T^j F^i, \end{aligned}$$

which is what we wanted to prove.

Thus, $\alpha\circ\beta = \mathrm{id}$ is proven. It thus remains to prove that $\beta\circ\alpha = \mathrm{id}$.

We know that $\mathcal{H}$ is spanned by $\left(h_{(i,j)}\right)_{(i,j)\in B}$ as a left $\mathbb{K}[F]$-module (by the definition of $\mathcal{H}$). Hence, $\mathcal{H}$ is spanned by $\left(F^k h_{(i,j)}\right)_{((i,j),k)\in B\times\mathbb{N}}$ as a $\mathbb{K}$-module. Hence, in order to prove that $\beta\circ\alpha = \mathrm{id}$, it suffices to show that $(\beta\circ\alpha)\left(F^k h_{(i,j)}\right) = F^k h_{(i,j)}$ for every $((i,j),k) \in B\times\mathbb{N}$.

So let us fix $((i,j),k) \in B\times\mathbb{N}$. The definition of α yields $\alpha\left(h_{(i,j)}\right) = T^j F^i$. But since α is a left $\mathbb{K}[F]$-module homomorphism, we have

$$\alpha\left(F^k h_{(i,j)}\right) = F^k \underbrace{\alpha\left(h_{(i,j)}\right)}_{=T^j F^i} = \underbrace{F^k T^j}_{\substack{=T^{r^k j} F^k \\ \text{(by Proposition 3.1 (a),} \\ \text{applied to } a=k \text{ and } b=j\text{)}}} F^i = T^{r^k j} \underbrace{F^k F^i}_{=F^{k+i}} = T^{r^k j} F^{k+i}.$$

On the other hand, the definition of ρ yields $\rho((i,j),k) = \left(\underbrace{i+k}_{=k+i}, r^k j\right) = \left(k+i, r^k j\right)$, so that $((i,j),k) = \rho^{-1}\left(k+i, r^k j\right)$. Hence, the definition of β yields $\beta\left(T^{r^k j} F^{k+i}\right) = F^k h_{(i,j)}$. Now,

$$(\beta\circ\alpha)\left(F^k h_{(i,j)}\right) = \beta\left(\underbrace{\alpha\left(F^k h_{(i,j)}\right)}_{=T^{r^k j} F^{k+i}}\right) = \beta\left(T^{r^k j} F^{k+i}\right) = F^k h_{(i,j)}.$$

This completes our proof of $\beta\circ\alpha = \mathrm{id}$. Thus, we have shown that α and β are mutually inverse.

$\left(T^{r^k\left(j+r^i\ell\right)}F^{i+k}\right)_{((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}}$ is a basis of the $\mathbb{K}$-module $\mathcal{M}$.

Let $\mathcal{R}$ be the free $\mathbb{K}$-module with basis $\left(r_{(i,j)}\right)_{(i,j)\in C}$. Then, $\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)_{((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}}$ is a basis of the $\mathbb{K}$-module $\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$ (since $\left(F^k\right)_{k\in\mathbb{N}}$ is a basis of $\mathbb{K}[F]$, and since $\left(T^\ell\right)_{\ell\in\mathbb{N}}$ is a basis of $\mathbb{K}[T]$). Hence, we can define a $\mathbb{K}$-linear map $\eta:\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]\to\mathcal{M}$ by

$$\eta\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)=T^{r^k\left(j+r^i\ell\right)}F^{i+k}.$$

Consider this map η. It sends the basis $\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)_{((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}}$ of $\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$ to the basis $\left(T^{r^k\left(j+r^i\ell\right)}F^{i+k}\right)_{((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}}$ of $\mathcal{M}$. Thus, η is an isomorphism of $\mathbb{K}$-modules.

Now, $\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$ becomes a left $\mathbb{K}[F]$-module (by having $\mathbb{K}[F]$ act on the tensorand $\mathbb{K}[F]$) and a right $\mathbb{K}[T]$-module (by having $\mathbb{K}[T]$ act on the tensorand $\mathbb{K}[T]$). The map η is a left $\mathbb{K}[F]$-module homomorphism[16] and a right $\mathbb{K}[T]$-module homomorphism[17]. Thus, η is a $\mathbb{K}[F]$-$\mathbb{K}[T]$-bimodule homomorphism.

[16] *Proof.* It suffices to show that $\eta(fz)=f\eta(z)$ for every $f\in\mathbb{K}[F]$ and $z\in\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$. So let us prove this.

Fix $f\in\mathbb{K}[F]$ and $z\in\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$. We need to show the equality $\eta(fz)=f\eta(z)$. Since this equality is $\mathbb{K}$-linear in each of f and z, we can WLOG assume that f belongs to the basis $\left(F^k\right)_{k\in\mathbb{N}}$ of $\mathbb{K}[F]$, and that z belongs to the basis $\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)_{((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}}$ of $\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$. Assume this. Thus, $f=F^p$ for some $p\in\mathbb{N}$, and $z=r_{(i,j)}\otimes F^k\otimes T^\ell$ for some $((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}$. Consider these p and $((i,j),\ell,k)$.

From $f=F^p$ and $z=r_{(i,j)}\otimes F^k\otimes T^\ell$, we obtain $fz=F^p\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)=r_{(i,j)}\otimes\underbrace{F^pF^k}_{=F^{p+k}}\otimes T^\ell=r_{(i,j)}\otimes F^{p+k}\otimes T^\ell$. Hence,

$$\eta(fz)=\eta\left(r_{(i,j)}\otimes F^{p+k}\otimes T^\ell\right)=T^{r^{p+k}\left(j+r^i\ell\right)}F^{i+p+k}$$

(by the definition of η). On the other hand, from $z=r_{(i,j)}\otimes F^k\otimes T^\ell$, we obtain $\eta(z)=\eta\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)=T^{r^k\left(j+r^i\ell\right)}F^{i+k}$, so that

$$\begin{aligned}\underbrace{f}_{=F^p}\underbrace{\eta(z)}_{=T^{r^k\left(j+r^i\ell\right)}F^{i+k}} &= \underbrace{F^pT^{r^k\left(j+r^i\ell\right)}}_{\substack{=T^{r^pr^k\left(j+r^i\ell\right)}F^p\\ \text{(by Proposition 3.1 (a),}\\ \text{applied to } a=p \text{ and } b=r^k\left(j+r^i\ell\right))}}F^{i+k}=\underbrace{T^{r^pr^k\left(j+r^i\ell\right)}}_{=T^{r^{p+k}\left(j+r^i\ell\right)}}\underbrace{F^pF^{i+k}}_{=F^{p+i+k}=F^{i+p+k}}\\ &=T^{r^{p+k}\left(j+r^i\ell\right)}F^{i+p+k}.\end{aligned}$$

Comparing this with $\eta(fz)=T^{r^{p+k}\left(j+r^i\ell\right)}F^{i+p+k}$, we obtain $\eta(fz)=f\eta(z)$, qed.

[17] *Proof.* It suffices to show that $\eta(zt)=\eta(z)t$ for every $t\in\mathbb{K}[T]$ and $z\in\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$. So let us prove this.

Now, recall that $\left(r_{(i,j)}\right)_{(i,j)\in C}$ is a basis of the free $\mathbb{K}$-module $\mathcal{R}$. Hence, $\mathcal{R} = \bigoplus_{(i,j)\in C} r_{(i,j)}\mathbb{K}$. Since direct sums commute with tensor products, this yields

$$\begin{aligned}\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T] &= \bigoplus_{(i,j)\in C} \underbrace{r_{(i,j)}\mathbb{K}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]}_{=\mathbb{K}[F]\cdot\left(r_{(i,j)}\otimes F^0\otimes T^0\right)\cdot\mathbb{K}[T]} \\ &\qquad \begin{array}{c}\text{(this follows easily from the definition of the}\\ \mathbb{K}[F]\text{-}\mathbb{K}[T]\text{-bimodule structure on } \mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]\text{)}\end{array} \\ &= \bigoplus_{(i,j)\in C} \mathbb{K}[F]\cdot\left(r_{(i,j)}\otimes F^0\otimes T^0\right)\cdot\mathbb{K}[T].\end{aligned}$$

We can apply the map η to this equality. The left hand side becomes $\mathcal{M}$ (since η is an isomorphism of $\mathbb{K}$-modules), and the direct sum on the right hand side

---

Fix $t\in\mathbb{K}[T]$ and $z\in\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$. We need to show the equality $\eta(zt)=\eta(z)\,t$. Since this equality is $\mathbb{K}$-linear in each of t and z, we can WLOG assume that t belongs to the basis $\left(T^\ell\right)_{\ell\in\mathbb{N}}$ of $\mathbb{K}[T]$, and that z belongs to the basis $\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)_{((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}}$ of $\mathcal{R}\otimes\mathbb{K}[F]\otimes\mathbb{K}[T]$. Assume this. Thus, $t=T^p$ for some $p\in\mathbb{N}$, and $z=r_{(i,j)}\otimes F^k\otimes T^\ell$ for some $((i,j),\ell,k)\in C\times\mathbb{N}\times\mathbb{N}$. Consider these p and $((i,j),\ell,k)$.

From $t=T^p$ and $z=r_{(i,j)}\otimes F^k\otimes T^\ell$, we obtain $zt=\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)T^p = r_{(i,j)}\otimes F^k\otimes \underbrace{T^\ell T^p}_{=T^{\ell+p}} = r_{(i,j)}\otimes F^k\otimes T^{\ell+p}$. Hence,

$$\eta(zt)=\eta\left(r_{(i,j)}\otimes F^k\otimes T^{\ell+p}\right)=T^{r^k\left(j+r^i(\ell+p)\right)}F^{i+k}$$

(by the definition of η). On the other hand, from $z=r_{(i,j)}\otimes F^k\otimes T^\ell$, we obtain $\eta(z)=\eta\left(r_{(i,j)}\otimes F^k\otimes T^\ell\right)=T^{r^k\left(j+r^i\ell\right)}F^{i+k}$, so that

$$\begin{aligned}\underbrace{\eta(z)}_{=T^{r^k\left(j+r^i\ell\right)}F^{i+k}}\ \underbrace{t}_{=T^p} &= T^{r^k\left(j+r^i\ell\right)}\ \underbrace{F^{i+k}T^p}_{\substack{=T^{r^{i+k}p}F^{i+k}\\ \text{(by Proposition 3.1 \textbf{(a)},}\\ \text{applied to } a=i+k \text{ and } b=p\text{)}}} = \underbrace{T^{r^k\left(j+r^i\ell\right)}T^{r^{i+k}p}}_{\substack{=T^{r^k\left(j+r^i\ell\right)+r^{i+k}p}\\ =T^{r^k\left(j+r^i(\ell+p)\right)}\\ \text{(since}\\ r^k\left(j+r^i\ell\right)+r^{i+k}p=r^k\left(j+r^i(\ell+p)\right)\text{)}}}F^{i+k}\\ &= T^{r^k\left(j+r^i(\ell+p)\right)}F^{i+k}.\end{aligned}$$

Comparing this with $\eta(zt)=T^{r^k\left(j+r^i(\ell+p)\right)}F^{i+k}$, we obtain $\eta(zt)=\eta(z)\,t$, qed.

remains direct (for the same reason). Hence, we obtain

$$\begin{aligned}
\mathcal{M} &= \bigoplus_{(i,j)\in C} \underbrace{\eta\left(\mathbb{K}\left[F\right]\cdot\left(r_{(i,j)}\otimes F^0\otimes T^0\right)\cdot\mathbb{K}\left[T\right]\right)}_{=\mathbb{K}[F]\cdot\eta\left(r_{(i,j)}\otimes F^0\otimes T^0\right)\cdot\mathbb{K}[T]} \\
&\qquad \text{(since } \eta \text{ is a } \mathbb{K}[F]\text{-}\mathbb{K}[T]\text{-bimodule homomorphism)} \\
&= \bigoplus_{(i,j)\in C} \mathbb{K}\left[F\right]\cdot\underbrace{\eta\left(r_{(i,j)}\otimes F^0\otimes T^0\right)}_{=T^{r^0\left(j+r^i0\right)}F^{i+0}}\cdot\mathbb{K}\left[T\right] \\
&\qquad \text{(by the definition of } \eta) \\
&= \underbrace{\bigoplus_{(i,j)\in C}}_{=\bigoplus_{\substack{(i,j)\in\mathbb{N}^2;\\ (i=0 \text{ or } r\nmid j) \text{ and } 0\leq j<r^i}}} \mathbb{K}\left[F\right]\cdot\underbrace{T^{r^0\left(j+r^i0\right)}}_{=T^j}\underbrace{F^{i+0}}_{=F^i}\cdot\mathbb{K}\left[T\right] \\
&= \bigoplus_{\substack{(i,j)\in\mathbb{N}^2;\\ (i=0 \text{ or } r\nmid j) \text{ and } 0\leq j<r^i}} \mathbb{K}\left[F\right]\cdot\left(T^jF^i\right)\cdot\mathbb{K}\left[T\right].
\end{aligned}$$

It remains to show that each $\mathbb{K}\left[F\right]\cdot\left(T^jF^i\right)\cdot\mathbb{K}\left[T\right]$ is isomorphic to $\mathbb{K}\left[F\right]\otimes\mathbb{K}\left[T\right]$ as an $\mathbb{K}\left[F\right]$-$\mathbb{K}\left[T\right]$-bimodule. This follows from η being an isomorphism (the details are left to the reader). Thus, Proposition 3.1 **(g)** is proven. □

3.2. The skew polynomial ring $\mathcal{F}$

Now, let us return to the setup of polynomials over $\mathbb{F}_q$.

We are still using the notations of Section 1. In particular, q is a (nontrivial) power of a prime p.

For every commutative $\mathbb{F}_q$-algebra A, we let $\mathrm{Frob}_A : A \to A$ be the map which sends every $a \in A$ to a^q. This map Frob_A is called the *Frobenius endomorphism* of A. It is well-known that Frob_A is an $\mathbb{F}_q$-algebra homomorphism[18]. We will often denote the $\mathbb{F}_q$-algebra homomorphism Frob_A by Frob when no confusion can arise from the omission of A. A rather important particular case is the endomorphism $\mathrm{Frob} = \mathrm{Frob}_{\mathbb{F}_q[T]}$ of the commutative $\mathbb{F}_q$-algebra $\mathbb{F}_q\left[T\right]$.

We let $\mathcal{F}$ be the $\mathbb{F}_q$-algebra $\mathbb{F}_q\left\langle F, T \mid FT = T^qF\right\rangle$. We can immediately define the following $\mathbb{F}_q$-algebra homomorphisms (whose well-definedness is easy to check using the universal properties of their domains):

- We define an $\mathbb{F}_q$-algebra homomorphism $\mathrm{Finc}_F : \mathbb{F}_q\left[F\right] \to \mathcal{F}$ by $\mathrm{Finc}_F\left(F\right) = F$. Thus, $\mathrm{Finc}_F\left(p\right) = p\left(F\right)$ for every $p \in \mathbb{F}_q\left[F\right]$ (where $p\left(F\right)$ means the result of substituting F into the polynomial p).

[18]This follows from the fact that $(\lambda a)^q = \underbrace{\lambda^q}_{\substack{=\lambda\\ (\text{since } \lambda\in\mathbb{F}_q)}} a^q = \lambda a^q$ for every $a \in A$ and $\lambda \in \mathbb{F}_q$, and the fact that $(a+b)^q = a^q + b^q$ for every $a, b \in A$.

- We define an $\mathbb{F}_q$-algebra homomorphism $\operatorname{Finc}_T : \mathbb{F}_q[T] \to \mathcal{F}$ by $\operatorname{Finc}_T(T) = T$. Thus, $\operatorname{Finc}_T(p) = p(T)$ for every $p \in \mathbb{F}_q[T]$ (where $p(T)$ means the result of substituting T into the polynomial p).
- We define an $\mathbb{F}_q$-algebra homomorphism $\operatorname{Carl} : \mathbb{F}_q[T] \to \mathcal{F}$ by $\operatorname{Carl}(T) = F + T$. Thus, $\operatorname{Carl}(p) = p(F + T)$ for every $p \in \mathbb{F}_q[T]$ (where $p(F + T)$ means the result of substituting $F + T$ into the polynomial p).

Furthermore, recall that $\mathcal{F}$ is the $\mathbb{F}_q$-algebra $\mathbb{F}_q\langle F, T \mid FT = T^q F\rangle$. Thus, $\mathcal{F}$ has the following universal property: If u and v are two elements of an $\mathbb{F}_q$-algebra $\mathcal{U}$ satisfying $uv = v^q u$, then there exists a unique $\mathbb{F}_q$-algebra homomorphism $\mathcal{F} \to \mathcal{U}$ sending F and T to u and v, respectively. This allows us to define $\mathbb{F}_q$-algebra homomorphisms out of $\mathcal{F}$, such as the following:

- We define an $\mathbb{F}_q$-algebra homomorphism $\operatorname{Fpro}_F : \mathcal{F} \to \mathbb{F}_q[F]$ by $\operatorname{Fpro}_F(F) = F$ and $\operatorname{Fpro}_F(T) = 0$. It is easy to see that $\operatorname{Fpro}_F \circ \operatorname{Finc}_F = \mathrm{id}$. Hence, the $\mathbb{F}_q$-algebra homomorphism Finc_F is injective. Thus, we shall regard Finc_F as an inclusion, so that $\mathbb{F}_q[F] \subseteq \mathcal{F}$. (Notice that this does not make $\mathcal{F}$ into an $\mathbb{F}_q[F]$-algebra, since $\mathbb{F}_q[F]$ is not contained in the center of $\mathcal{F}$.)
- We define an $\mathbb{F}_q$-algebra homomorphism $\operatorname{Fpro}_T : \mathcal{F} \to \mathbb{F}_q[T]$ by $\operatorname{Fpro}_T(F) = 0$ and $\operatorname{Fpro}_T(T) = T$. It is easy to see that $\operatorname{Fpro}_T \circ \operatorname{Finc}_T = \mathrm{id}$. Hence, the $\mathbb{F}_q$-algebra homomorphism Finc_T is injective. Thus, we shall regard Finc_T as an inclusion, so that $\mathbb{F}_q[T] \subseteq \mathcal{F}$. (Notice that this does not make $\mathcal{F}$ into an $\mathbb{F}_q[T]$-algebra, since $\mathbb{F}_q[T]$ is not contained in the center of $\mathcal{F}$.)
- For every $a \in \mathbb{F}_q$ and $b \in \mathbb{F}_q$, we define an $\mathbb{F}_q$-algebra homomorphism $\operatorname{Fscal}_{a,b} : \mathcal{F} \to \mathcal{F}$ by $\operatorname{Fscal}_{a,b}(F) = aF$ and $\operatorname{Fscal}_{a,b}(T) = bT$. (This is well-defined, since $(aF)(bT) = (bT)^q (aF)$.) If a and b are nonzero, then $\operatorname{Fscal}_{a,b}$ is invertible (with inverse $\operatorname{Fscal}_{a^{-1},b^{-1}}$).

Now, we shall derive some structural properties of $\mathcal{F}$ straight from Proposition 3.1:

Proposition 3.5. The homomorphisms Finc_T and Finc_F make $\mathcal{F}$ into a left $\mathbb{F}_q[T]$-module, a right $\mathbb{F}_q[T]$-module, a left $\mathbb{F}_q[F]$-module, and a right $\mathbb{F}_q[F]$-module. Any of these two left module structures can be combined with any of these two right module structures to form a bimodule structure on $\mathcal{F}$ (for example, the left $\mathbb{F}_q[T]$-module structure and the right $\mathbb{F}_q[F]$-module structure on $\mathcal{F}$ can be combined to form an $\mathbb{F}_q[T]$-$\mathbb{F}_q[F]$-bimodule structure on $\mathcal{F}$).

(a) We have $F^a T^b = T^{q^a b} F^a$ in $\mathcal{F}$ for every $a \in \mathbb{N}$ and $b \in \mathbb{N}$.

(b) The $\mathbb{F}_q$-module $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{i \geq 0,\ j \geq 0}$.

(c) As left $\mathbb{F}_q[T]$-module, $\mathcal{F}$ is free with basis $\left(F^i\right)_{i \geq 0}$.

(d) As right $\mathbb{F}_q[T]$-module, $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{i \geq 0,\ 0 \leq j < q^i}$.

(e) As right $\mathbb{F}_q[F]$-module, $\mathcal{F}$ is free with basis $\left(T^j\right)_{j \geq 0}$.

(f) As left $\mathbb{F}_q[F]$-module, $\mathcal{F}$ is free with basis $\left(T^jF^i\right)_{i=0 \text{ or } q\nmid j}$.

(g) As $\mathbb{F}_q[F]$-$\mathbb{F}_q[T]$-bimodule, $\mathcal{F}$ is free with basis $\left(T^jF^i\right)_{(i=0 \text{ or } q\nmid j) \text{ and } 0\leq j<q^i}$ (that is, we have $\mathcal{F} = \bigoplus_{\substack{(i,j)\in\mathbb{N}^2; \\ (i=0 \text{ or } q\nmid j) \text{ and } 0\leq j<q^i}} \mathbb{F}_q[F]\cdot\left(T^jF^i\right)\cdot\mathbb{F}_q[T]$, and each $\mathbb{F}_q[F]\cdot\left(T^jF^i\right)\cdot\mathbb{F}_q[T]$ is isomorphic to $\mathbb{F}_q[F]\otimes\mathbb{F}_q[T]$ as an $\mathbb{F}_q[F]$-$\mathbb{F}_q[T]$-bimodule, where the tensor product is taken over $\mathbb{F}_q$).

Proof of Proposition 3.5. Proposition 3.5 follows immediately from Proposition 3.1 by setting $\mathbb{K} = \mathbb{F}_q$ and $r = q$. □

One simple identity in $\mathcal{F}$ is the following:

Proposition 3.6. Let $P \in \mathbb{F}_q[T]$. Then, $FP = P^qF$ in $\mathcal{F}$.

Proof of Proposition 3.6. We are going to prove that $FP = (\operatorname{Frob} P)\,F$. Since both sides of this equality are $\mathbb{F}_q$-linear in P (because Frob is an $\mathbb{F}_q$-linear map), we can WLOG assume that P belongs to the basis $\left(T^i\right)_{i\geq 0}$ of the $\mathbb{F}_q$-vector space $\mathbb{F}_q[T]$. Assume this. Thus, $P = T^i$ for some $i \in \mathbb{N}$. Consider this i. The definition of Frob yields $\operatorname{Frob} P = \left(\underbrace{P}_{=T^i}\right)^q = \left(T^i\right)^q = T^{qi}$.

Now, $\underbrace{F}_{=F^1}\underbrace{P}_{=T^i} = F^1T^i = T^{q^1i}F^1$ (by Proposition 3.5 **(a)**), so that $FP = \underbrace{T^{q^1i}}_{=T^{qi}=\operatorname{Frob} P}\underbrace{F^1}_{=F} = (\operatorname{Frob} P)\,F$.

Thus, $FP = (\operatorname{Frob} P)\,F$ is proven. Hence, $FP = \underbrace{(\operatorname{Frob} P)}_{=P^q}F = P^qF$. This proves Proposition 3.6. □

Corollary 3.7. Let $P \in \mathbb{F}_q[T]$. Then, $\mathcal{F}\cdot P\cdot\mathcal{F} \subseteq P\cdot\mathcal{F}$.

Proof of Corollary 3.7. We first claim that

$$F^iP \in P\cdot\mathcal{F} \qquad \text{for every } i\in\mathbb{N}. \tag{20}$$

Proof of (20): We shall prove (20) by induction on i.

The *induction base* (i.e., the case $i = 0$) is trivial.

For the *induction step*, we fix an $n \in \mathbb{N}$, and we assume that (20) holds for $i = n$. We then must prove that (20) holds for $i = n+1$.

By assumption, (20) holds for $i = n$. In other words, $F^nP \in P\cdot\mathcal{F}$. Now,

$$\underbrace{F^{n+1}}_{=FF^n}P = F\underbrace{F^nP}_{\in P\cdot\mathcal{F}} \in \underbrace{FP}_{\substack{=P^qF \\ \text{(by Proposition 3.6)}}}\cdot\mathcal{F} = \underbrace{P^q}_{=PP^{q-1}}F\cdot\mathcal{F}$$
$$= P\underbrace{P^{q-1}F\cdot\mathcal{F}}_{\subseteq\mathcal{F}} \subseteq P\cdot\mathcal{F}.$$

In other words, (20) holds for $i = n+1$. This completes the induction step. Thus, (20) is proven.

Recall that $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ is a basis of the $\mathbb{F}_q$-module $\mathcal{F}$ (by Proposition 3.5 **(b)**).

Now, we shall prove that

$$uP \in P \cdot \mathcal{F} \qquad \text{for every } u \in \mathcal{F}. \tag{21}$$

Proof of (21): Let $u \in \mathcal{F}$. We must prove the equality (21). Since this equality is $\mathbb{F}_q$-linear in u, we can WLOG assume that u belongs to the basis $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ of the $\mathbb{F}_q$-module $\mathcal{F}$. Assume this. Thus, $u = T^j F^i$ for some $(i,j) \in \mathbb{N}^2$. Consider this (i,j). Now,

$$\underbrace{u}_{=T^jF^i} P = T^j \underbrace{F^i P}_{\substack{\in P\cdot\mathcal{F} \\ \text{(by (20))}}} \in \underbrace{T^j P}_{\substack{=PT^j \\ \text{(since } P \text{ and } T^j \text{ both} \\ \text{lie in } \mathbb{F}_q[T]\text{)}}} \cdot\mathcal{F} = P \underbrace{T^j \cdot \mathcal{F}}_{\subseteq\mathcal{F}} \subseteq P \cdot \mathcal{F}.$$

This proves (21).

Now, (21) immediately yields $\mathcal{F} \cdot P \subseteq P \cdot \mathcal{F}$. Hence, $\underbrace{\mathcal{F}\cdot P}_{\subseteq P\cdot\mathcal{F}} \cdot \mathcal{F} \subseteq P \cdot \underbrace{\mathcal{F}\cdot\mathcal{F}}_{\subseteq\mathcal{F}} \subseteq P \cdot \mathcal{F}$. This proves Corollary 3.7. □

3.3. q-polynomials

Next, we shall see an alternative description of the $\mathbb{F}_q$-algebra $\mathcal{F}$. We begin with a general definition:

Definition 3.8. Let A be a commutative $\mathbb{F}_q$-algebra. A polynomial in $A[X]$ is said to be a *q-polynomial* if it is an A-linear combination of the monomials $X^{q^0}, X^{q^1}, X^{q^2}, \ldots$. We let $A[X]_{q-\text{lin}}$ be the set of all q-polynomials in $A[X]$. Thus, $A[X]_{q-\text{lin}}$ is an A-submodule of $A[X]$; as an A-submodule, it has basis $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$.

Thus, a polynomial in $A[X]$ belongs to $A[X]_{q-\text{lin}}$ if and only if the only monomials it contains are (some of) the monomials $X^{q^0}, X^{q^1}, X^{q^2}, \ldots$.

The A-submodule $A[X]_{q-\text{lin}}$ of $A[X]$ is not a subring of $A[X]$ (unless $A = 0$). However, it is closed under a different operation: namely, composition of polynomials. Let us see this in more detail:

Definition 3.9. Let A be a commutative ring. Let $f \in A[X]$ and $g \in A[X]$. Then, $f \circ g$ denotes the polynomial $f(g) \in A[X]$. (This is the polynomial obtained from f by substituting g for X.) This defines a binary operation $\circ$ on the set $A[X]$.

Proposition 3.10. Let A be a commutative ring.

(a) The pair $(A[X], \circ)$ is a monoid with neutral element X.

(b) Assume that A is a commutative $\mathbb{F}_q$-algebra. Then, $A[X]_{q-\mathrm{lin}}$ is a submonoid of the monoid $(A[X], \circ)$. Moreover, $\left(A[X]_{q-\mathrm{lin}}, +, \circ\right)$ is a (noncommutative) $\mathbb{F}_q$-algebra with unity X (where the $\mathbb{F}_q$-module structure is the one obtained by restricting the $A[X]$-module structure to $\mathbb{F}_q$).

Proof of Proposition 3.10. **(a)** If B is any commutative A-algebra, and if $b \in B$ is any element, then there exists a unique A-algebra homomorphism $\varphi : A[X] \to B$ satisfying $\varphi(X) = b$. [19] We shall denote this homomorphism φ by ev_b. It has the property that

$$\mathrm{ev}_b(f) = f(b) \qquad \text{for every } f \in A[X]. \tag{22}$$

Now, every $f, g \in A[X]$ satisfy

$$\begin{aligned} \mathrm{ev}_g(f) &= f(g) && \text{(by (22), applied to } B = A[X] \text{ and } b = g) \\ &= f \circ g && \text{(since } f \circ g = f(g)). \end{aligned} \tag{23}$$

Let $f, g, h \in A[X]$. Then, (23) yields $\mathrm{ev}_g(f) = f \circ g$. Furthermore, (23) (applied to $f \circ g$ and h instead of f and g) yields $\mathrm{ev}_h(f \circ g) = (f \circ g) \circ h$. But (23) (applied to g and h instead of f and g) yields $\mathrm{ev}_h(g) = g \circ h$. Finally, (23) (applied to $g \circ h$ instead of g) yields $\mathrm{ev}_{g \circ h}(f) = f \circ (g \circ h)$.

The defining property of $\mathrm{ev}_{g \circ h}$ yields $\mathrm{ev}_{g \circ h}(X) = g \circ h$. But the defining property of ev_g yields $\mathrm{ev}_g(X) = g$. Now,

$$\left(\mathrm{ev}_h \circ \mathrm{ev}_g\right)(X) = \mathrm{ev}_h\left(\underbrace{\mathrm{ev}_g(X)}_{=g}\right) = \mathrm{ev}_h(g) = g \circ h.$$

Comparing this with $\mathrm{ev}_{g \circ h}(X) = g \circ h$, we obtain $\left(\mathrm{ev}_h \circ \mathrm{ev}_g\right)(X) = \mathrm{ev}_{g \circ h}(X)$. The two maps $\mathrm{ev}_h \circ \mathrm{ev}_g$ and $\mathrm{ev}_{g \circ h}$ thus agree on the generator X of the A-algebra $A[X]$. Since these two maps are A-algebra homomorphisms (because ev_h, ev_g and $\mathrm{ev}_{g \circ h}$ are A-algebra homomorphisms), this shows that these two maps are equal. In other words, $\mathrm{ev}_h \circ \mathrm{ev}_g = \mathrm{ev}_{g \circ h}$. Hence, $\underbrace{\left(\mathrm{ev}_h \circ \mathrm{ev}_g\right)}_{=\mathrm{ev}_{g \circ h}}(f) = \mathrm{ev}_{g \circ h}(f) = f \circ (g \circ h)$. Thus,

$$f \circ (g \circ h) = \left(\mathrm{ev}_h \circ \mathrm{ev}_g\right)(f) = \mathrm{ev}_h\left(\underbrace{\mathrm{ev}_g(f)}_{=f \circ g}\right) = \mathrm{ev}_h(f \circ g) = (f \circ g) \circ h.$$

[19] This is simply the universal property of the polynomial ring $A[X]$.

Now, let us forget that we fixed f, g, h. We thus have shown that $f \circ (g \circ h) = (f \circ g) \circ h$ for every $f, g, h \in A[X]$. Thus, $(A[X], \circ)$ is a semigroup. Furthermore, X is a neutral element of this semigroup (since every $f \in A[X]$ satisfies $X \circ f = X(f) = f$ and $f \circ X = f(X) = f$). Therefore, this semigroup $(A[X], \circ)$ is a monoid with neutral element X. This proves Proposition 3.10 **(a)**.

(b) *Step 1:* Let $\operatorname{End}(A[X])$ denote the $\mathbb{F}_q$-algebra of all endomorphisms of the $\mathbb{F}_q$-vector space $A[X]$. It is easy to see that $\operatorname{Frob} = \operatorname{Frob}_{A[X]} \in \operatorname{End}(A[X])$. Hence, $\operatorname{Frob}^n \in \operatorname{End}(A[X])$ for every $n \in \mathbb{N}$. It is straightforward to see (by induction over n) that

$$\operatorname{Frob}^n(f) = f^{q^n} \qquad \text{for every } f \in A[X] \text{ and } n \in \mathbb{N}. \tag{24}$$

It is easy to see that

$$\operatorname{Frob}\left(A[X]_{q-\lin}\right) \subseteq A[X]_{q-\lin} \tag{25}$$

[20]. Using this fact, it is straightforward to see (by induction over n) that

$$\operatorname{Frob}^n\left(A[X]_{q-\lin}\right) \subseteq A[X]_{q-\lin} \qquad \text{for every } n \in \mathbb{N}. \tag{26}$$

Step 2: Now, let us prove that

$$f \circ (\lambda_1 g_1 + \lambda_2 g_2) = \lambda_1 (f \circ g_1) + \lambda_2 (f \circ g_2) \tag{27}$$

for every $f \in A[X]_{q-\lin}$, $g_1 \in A[X]$, $g_2 \in A[X]$, $\lambda_1 \in \mathbb{F}_q$ and $\lambda_2 \in \mathbb{F}_q$.

Proof of (27): Let $f \in A[X]_{q-\lin}$.

---

[20] *Proof of (25):* Let $g \in A[X]_{q-\lin}$. We shall prove that $\operatorname{Frob} g \in A[X]_{q-\lin}$.

Indeed, $g \in A[X]_{q-\lin}$. Thus, g is an A-linear combination of $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$ (since the A-module $A[X]_{q-\lin}$ has basis $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$). In other words, there exists a sequence $(a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}}$ of elements of A such that $g = \sum_{n \in \mathbb{N}} a_n X^{q^n}$, and such that all but finitely many $n \in \mathbb{N}$ satisfy $a_n = 0$. Consider this sequence.

Applying the map Frob to the equality $g = \sum_{n \in \mathbb{N}} a_n X^{q^n}$, we obtain

$$\operatorname{Frob} g = \operatorname{Frob}\left(\sum_{n \in \mathbb{N}} a_n X^{q^n}\right) = \sum_{n \in \mathbb{N}} \underbrace{\operatorname{Frob}\left(a_n X^{q^n}\right)}_{=\left(a_n X^{q^n}\right)^q = a_n^q \left(X^{q^n}\right)^q} \qquad \left(\text{since the map } \operatorname{Frob} \text{ is } \mathbb{F}_q\text{-linear}\right)$$

$$= \sum_{n \in \mathbb{N}} a_n^q \underbrace{\left(X^{q^n}\right)^q}_{= X^{q^n q} = X^{q^{n+1}} \in A[X]_{q-\lin}} \in \sum_{n \in \mathbb{N}} a_n^q A[X]_{q-\lin} \subseteq A[X]_{q-\lin}$$

(since $A[X]_{q-\lin}$ is an A-module).

Now, let us forget that we fixed g. We thus have proven that $\operatorname{Frob} g \in A[X]_{q-\lin}$ for every $g \in A[X]_{q-\lin}$. In other words, $\operatorname{Frob}\left(A[X]_{q-\lin}\right) \subseteq A[X]_{q-\lin}$. This proves (25).

We have $f \in A[X]_{q-\mathrm{lin}}$. Thus, f is an A-linear combination of $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$ (since the A-module $A[X]_{q-\mathrm{lin}}$ has basis $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$). In other words, there exists a sequence $(a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}}$ of elements of A such that $f = \sum_{n \in \mathbb{N}} a_n X^{q^n}$, and such that all but finitely many $n \in \mathbb{N}$ satisfy $a_n = 0$. Consider this sequence.

Let $\widehat{f}$ denote the element $\sum_{n \in \mathbb{N}} a_n \operatorname{Frob}^n$ of $\operatorname{End}(A[X])$. (This is well-defined, since $\operatorname{Frob}^n \in \operatorname{End}(A[X])$ for every $n \in \mathbb{N}$.) Now, every $h \in A[X]$ satisfies

$$f \circ h = \widehat{f}(h) \tag{28}$$

[21].

Now, let $g_1 \in A[X]$, $g_2 \in A[X]$, $\lambda_1 \in \mathbb{F}_q$ and $\lambda_2 \in \mathbb{F}_q$. Applying (28) to $h = \lambda_1 g_1 + \lambda_2 g_2$, we obtain

$$f \circ (\lambda_1 g_1 + \lambda_2 g_2) = \widehat{f}(\lambda_1 g_1 + \lambda_2 g_2) = \lambda_1 \widehat{f}(g_1) + \lambda_2 \widehat{f}(g_2)$$

(since $\widehat{f} \in \operatorname{End}(A[X])$). Comparing this with

$$\lambda_1 \underbrace{(f \circ g_1)}_{\substack{=\widehat{f}(g_1) \\ \text{(by (28))}}} + \lambda_2 \underbrace{(f \circ g_2)}_{\substack{=\widehat{f}(g_2) \\ \text{(by (28))}}} = \lambda_1 \widehat{f}(g_1) + \lambda_2 \widehat{f}(g_2),$$

we obtain $f \circ (\lambda_1 g_1 + \lambda_2 g_2) = \lambda_1 (f \circ g_1) + \lambda_2 (f \circ g_2)$. Thus, (27) is proven.

Step 3: Furthermore, we have

$$(\lambda_1 f_1 + \lambda_2 f_2) \circ g = \lambda_1 (f_1 \circ g) + \lambda_2 (f_2 \circ g) \tag{29}$$

for every $f_1 \in A[X]$, $f_2 \in A[X]$, $g \in A[X]$, $\lambda_1 \in \mathbb{F}_q$ and $\lambda_2 \in \mathbb{F}_q$.

Proof of (29): Let $f_1 \in A[X]$, $f_2 \in A[X]$, $g \in A[X]$, $\lambda_1 \in \mathbb{F}_q$ and $\lambda_2 \in \mathbb{F}_q$. Then,

$$(\lambda_1 f_1 + \lambda_2 f_2) \circ g = (\lambda_1 f_1 + \lambda_2 f_2)(g) = \lambda_1 f_1(g) + \lambda_2 f_2(g).$$

[21] *Proof of (28):* Let $h \in A[X]$. Then,

$$f \circ h = f(h) = \sum_{n \in \mathbb{N}} a_n h^{q^n} \qquad \left(\text{since } f = \sum_{n \in \mathbb{N}} a_n X^{q^n}\right).$$

Comparing this with

$$\widehat{f}(h) = \sum_{n \in \mathbb{N}} a_n \underbrace{\operatorname{Frob}^n(h)}_{\substack{=h^{q^n} \\ \text{(by (24), applied to } h \\ \text{instead of } f)}} \qquad \left(\text{since } \widehat{f} = \sum_{n \in \mathbb{N}} a_n \operatorname{Frob}^n\right)$$
$$= \sum_{n \in \mathbb{N}} a_n h^{q^n},$$

this yields $f \circ h = \widehat{f}(h)$, qed.

Comparing this with $\lambda_1 \underbrace{(f_1 \circ g)}_{=f_1(g)} + \lambda_2 \underbrace{(f_2 \circ g)}_{=f_2(g)} = \lambda_1 f_1(g) + \lambda_2 f_2(g)$, we obtain $(\lambda_1 f_1 + \lambda_2 f_2) \circ g = \lambda_1 (f_1 \circ g) + \lambda_2 (f_2 \circ g)$. This proves (29).

Step 4: Now, let us show that

$$f \circ g \in A[X]_{q-\mathrm{lin}} \qquad \text{for every } f, g \in A[X]_{q-\mathrm{lin}}. \tag{30}$$

Proof of (30): Let $f, g \in A[X]_{q-\mathrm{lin}}$. Define the sequence $(a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}}$ and the element $\widehat{f} \in \mathrm{End}(A[X])$ as in the proof of (27). Then, (28) holds. Applying (28) to $h = g$, we obtain

$$f \circ g = \widehat{f}(g) = \sum_{n \in \mathbb{N}} a_n \mathrm{Frob}^n \left(\underbrace{g}_{\in A[X]_{q-\mathrm{lin}}} \right) \qquad \left(\text{since } \widehat{f} = \sum_{n \in \mathbb{N}} a_n \mathrm{Frob}^n \right)$$

$$\in \sum_{n \in \mathbb{N}} a_n \underbrace{\mathrm{Frob}^n \left(A[X]_{q-\mathrm{lin}} \right)}_{\substack{\subseteq A[X]_{q-\mathrm{lin}} \\ \text{(by (26))}}} \subseteq \sum_{n \in \mathbb{N}} a_n A[X]_{q-\mathrm{lin}} \subseteq A[X]_{q-\mathrm{lin}}$$

(since $A[X]_{q-\mathrm{lin}}$ is an A-module). Thus, we have proven (30).

Step 5: We have $X = X^1 \in A[X]_{q-\mathrm{lin}}$. This, combined with (30), shows that $A[X]_{q-\mathrm{lin}}$ is a submonoid of the monoid $(A[X], \circ)$. Furthermore, the binary operation $\circ$ on $A[X]_{q-\mathrm{lin}}$ is $\mathbb{F}_q$-bilinear (by (27) and (29)) and associative (since $(A[X], \circ)$ is a monoid) and has neutral element X (since $(A[X], \circ)$ is a monoid with neutral element X). Thus, $\left(A[X]_{q-\mathrm{lin}}, +, \circ \right)$ is a (noncommutative) $\mathbb{F}_q$-algebra with unity X. This concludes the proof of Proposition 3.10 **(b)**. □

Definition 3.11. Let A be a commutative ring. Whenever $f \in A[X]$ and $n \in \mathbb{N}$, we shall use the notation $f^{\circ n}$ for the n-th power of f in the monoid $(A[X], \circ)$.

Definition 3.12. Let A be a commutative $\mathbb{F}_q$-algebra. The (noncommutative) $\mathbb{F}_q$-algebra $\left(A[X]_{q-\mathrm{lin}}, +, \circ \right)$ constructed in Proposition 3.10 **(b)** will be called the *Ore polynomial ring over A*, and simply denoted by $A[X]_{q-\mathrm{lin}}$ (since there are no other $\mathbb{F}_q$-algebra structures on $A[X]_{q-\mathrm{lin}}$ that could be confused with this one).

The connection between these Ore polynomial rings and our $\mathcal{F}$ is the following:

Theorem 3.13. Consider the Ore polynomial ring $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ over $\mathbb{F}_q[T]$; recall that this is the $\mathbb{F}_q$-algebra $\left(\mathbb{F}_q[T][X]_{q-\mathrm{lin}}, +, \circ\right)$. (Notice that polynomials in $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ can contain arbitrary powers of T, but the only powers of X they can contain are $X^{q^0}, X^{q^1}, X^{q^2}, \ldots$.) Define an $\mathbb{F}_q$-algebra homomorphism $\mathrm{Fqpol} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ by $\mathrm{Fqpol}(F) = X^q$ and $\mathrm{Fqpol}(T) = TX$.

(a) This homomorphism Fqpol is well-defined.

(b) This homomorphism Fqpol is an $\mathbb{F}_q$-algebra isomorphism.

(c) We have $\mathrm{Fqpol}\left(T^j F^i\right) = T^j X^{q^i}$ for every $i \in \mathbb{N}$ and $j \in \mathbb{N}$.

(d) We have $\mathrm{Fqpol}\, t = t \cdot X$ for every $t \in \mathbb{F}_q[T]$. (Here, we regard $\mathbb{F}_q[T]$ as an $\mathbb{F}_q$-subalgebra of $\mathcal{F}$ as before. The expression "$t \cdot X$" means the product of $t \in \mathbb{F}_q[T] \subseteq \mathbb{F}_q[T][X]$ with X in $\mathbb{F}_q[T][X]$.)

Proof of Theorem 3.13. For every $n \in \mathbb{N}$, we have

$$(TX)^{\circ n} = T^n X \qquad \text{in } \mathbb{F}_q[T][X]_{q-\mathrm{lin}}. \tag{31}$$

(This follows by a straightforward induction on n.) Furthermore, for every $n \in \mathbb{N}$, we have

$$(X^q)^{\circ n} = X^{q^n} \qquad \text{in } \mathbb{F}_q[T][X]_{q-\mathrm{lin}}. \tag{32}$$

(Again, this is easy to prove by induction.)

(a) In $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$, we have $X^q \circ (TX) = (TX)^{\circ q} \circ X^q$ (indeed, this follows by comparing $X^q \circ (TX) = X^q (TX) = (TX)^q = T^q X^q$ and $\underbrace{(TX)^{\circ q}}_{\substack{=T^q X \\ \text{(by (31), applied to } n=q\text{)}}} \circ X^q = (T^q X) \circ X^q = T^q X^q$). Now, recall that if u and v are two elements of an $\mathbb{F}_q$-algebra $\mathcal{U}$ satisfying $uv = v^q u$, then there exists a unique $\mathbb{F}_q$-algebra homomorphism $\mathcal{F} \to \mathcal{U}$ sending F and T to u and v, respectively. Applying this to $\mathcal{U} = \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$, $u = X^q$ and $v = TX$, we thus conclude that there exists a unique $\mathbb{F}_q$-algebra homomorphism $\mathcal{F} \to \mathcal{U}$ sending F and T to X^q and TX, respectively. In other words, the homomorphism Fqpol is well-defined. This proves Theorem 3.13 **(a)**.

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

$$\begin{aligned}
\mathrm{Fqpol}\left(T^j F^i\right) &= \left(\underbrace{\mathrm{Fqpol}\, T}_{=TX}\right)^{\circ j} \circ \left(\underbrace{\mathrm{Fqpol}\, F}_{=X^q}\right)^{\circ i} \\
&\qquad \left(\text{since Fqpol is an } \mathbb{F}_q\text{-algebra homomorphism}\right) \\
&= \underbrace{(TX)^{\circ j}}_{\substack{=T^j X \\ \text{(by (31))}}} \circ \underbrace{(X^q)^{\circ i}}_{\substack{=X^{q^i} \\ \text{(by (32))}}} = \left(T^j X\right) \circ X^{q^i} = T^j X^{q^i}.
\end{aligned}$$

This proves Theorem 3.13 **(c)**.

(b) The $\mathbb{F}_q[T]$-module $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ has basis $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right) = \left(X^{q^i}\right)_{i\geq 0}$. Thus, as an $\mathbb{F}_q$-module, it has basis $\left(T^j X^{q^i}\right)_{i\geq 0,\ j\geq 0}$.

On the other hand, Proposition 3.5 **(b)** says that the $\mathbb{F}_q$-module $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$.

For every $i \in \mathbb{N}$ and $j \in \mathbb{N}$, we have $\mathrm{Fqpol}\left(T^j F^i\right) = T^j X^{q^i}$ (by Theorem 3.13 **(c)**). Hence, the $\mathbb{F}_q$-linear map Fqpol sends the basis $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ of the $\mathbb{F}_q$-module $\mathcal{F}$ to the basis $\left(T^j X^{q^i}\right)_{i\geq 0,\ j\geq 0}$ of the $\mathbb{F}_q$-module $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$. Consequently, Fqpol is an $\mathbb{F}_q$-module isomorphism, thus an $\mathbb{F}_q$-algebra isomorphism. This proves Theorem 3.13 **(b)**.

(d) Let $t \in \mathbb{F}_q[T]$. We must prove the equality $\mathrm{Fqpol}\, t = t \cdot X$. Since this equality is clearly $\mathbb{F}_q$-linear in t, we can WLOG assume that t belongs to the basis $\left(T^j\right)_{j\geq 0}$ of the $\mathbb{F}_q$-module $\mathbb{F}_q[T]$. Assume this. Thus, $t = T^j$ for some $j \in \mathbb{N}$. Consider this j. We have $t = T^j = T^j F^0$ in $\mathcal{F}$. Thus, $\mathrm{Fqpol}\, t = \mathrm{Fqpol}\left(T^j F^0\right) = T^j X^{q^0}$ (by Theorem 3.13 **(c)**, applied to $i = 0$). Hence, $\mathrm{Fqpol}\, t = \underbrace{T^j}_{=t}\ \underbrace{X^{q^0}}_{=X^1=X} = t \cdot X$. Thus, Theorem 3.13 **(d)** is proven. □

Theorem 3.13 **(b)** shows that the $\mathbb{F}_q$-algebra $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ is isomorphic to $\mathcal{F}$; this algebra can thus be regarded as a rather concrete manifestation of $\mathcal{F}$. We shall make more use of this later.

Let us prove one further simple property of $A[X]_{q-\mathrm{lin}}$ (for general A):

Proposition 3.14. Let A be a commutative $\mathbb{F}_q$-algebra. Let $f \in A[X]_{q-\mathrm{lin}}$. Let B be a commutative A-algebra. Then, the map $B \to B,\ b \mapsto f(b)$ is $\mathbb{F}_q$-linear. (It might not be A-linear.)

Proof of Proposition 3.14. Let $\mathrm{End}\, B$ denote the $\mathbb{F}_q$-algebra of all endomorphisms of the $\mathbb{F}_q$-vector space B. It is easy to see that $\mathrm{Frob} = \mathrm{Frob}_B \in \mathrm{End}\, B$. Hence, $\mathrm{Frob}^n \in \mathrm{End}\, B$ for every $n \in \mathbb{N}$. It is straightforward to see (by induction over n) that

$$\mathrm{Frob}^n(b) = b^{q^n} \qquad \text{for every } b \in B \text{ and } n \in \mathbb{N}. \tag{33}$$

We have $f \in A[X]_{q-\mathrm{lin}}$. Thus, f is an A-linear combination of $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$ (since the A-module $A[X]_{q-\mathrm{lin}}$ has basis $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$). In other words, there exists a sequence $(a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}}$ of elements of A such that $f = \sum_{n\in\mathbb{N}} a_n X^{q^n}$, and such that all but finitely many $n \in \mathbb{N}$ satisfy $a_n = 0$. Consider this sequence.

Let $\widehat{f}$ denote the element $\sum_{n\in\mathbb{N}} a_n \mathrm{Frob}^n$ of $\mathrm{End}\, B$. (This is well-defined, since $\mathrm{Frob}^n \in \mathrm{End}\, B$ for every $n \in \mathbb{N}$.) Now, every $b \in B$ satisfies

$$f(b) = \widehat{f}(b) \tag{34}$$

[22]. Hence, the map $B \to B,\ b \mapsto f(b)$ equals the map $B \to B,\ b \mapsto \widehat{f}(b)$. But the latter map is simply the map $\widehat{f} \in \operatorname{End} B$, and thus clearly $\mathbb{F}_q$-linear. Hence, the former map is $\mathbb{F}_q$-linear. Proposition 3.14 is thus proven. □

Proposition 3.14 also has a partial converse:

Proposition 3.15. Let A be a commutative $\mathbb{F}_q$-algebra which is an integral domain. Let $f \in A[X]$ be such that, for every commutative A-algebra B, the map $B \to B,\ b \mapsto f(b)$ is $\mathbb{F}_q$-linear. Then, $f \in A[X]_{q-\mathrm{lin}}$.

The proof of Proposition 3.15 can be found in [3, Corollary A.3]; we shall not give it here, as we shall not use Proposition 3.15. Propositions 3.14 and 3.15 are the reason why the q-polynomials over A (that is, the elements of $A[X]_{q-\mathrm{lin}}$) are often called the "$\mathbb{F}_q$-linear polynomials over A", but we shall not use this terminology (as it is mildly misleading: it sounds too much like degree-1 polynomials).

3.4. q-polynomials from subspaces

We shall now see a classical way to construct q-polynomials.

Definition 3.16. Let A be a commutative $\mathbb{F}_q$-algebra. For every finite subset V of A, let f_V be the polynomial $\prod_{v \in V} (X + v) \in A[X]$.

The following result is a consequence of [15, (7.7)] (and also appears in [3, Theorem A.1 2)] in the particular case when A is an integral domain):

Theorem 3.17. Let A be a commutative $\mathbb{F}_q$-algebra. Let V be a finite $\mathbb{F}_q$-vector subspace of A. Then, f_V is a q-polynomial.

We shall prove Theorem 3.17 following an idea that appears in [15, proof of (7.15)]; but first, let us slightly generalize it:

[22] *Proof of (34):* Let $b \in B$. From $f = \sum_{n \in \mathbb{N}} a_n X^{q^n}$, we obtain $f(b) = \sum_{n \in \mathbb{N}} a_n b^{q^n}$. Comparing this with

$$\widehat{f}(b) = \sum_{n \in \mathbb{N}} a_n \underbrace{\operatorname{Frob}^n(b)}_{\substack{= b^{q^n} \\ \text{(by (33))}}} \qquad \left(\text{since } \widehat{f} = \sum_{n \in \mathbb{N}} a_n \operatorname{Frob}^n \right)$$
$$= \sum_{n \in \mathbb{N}} a_n b^{q^n},$$

this yields $f(b) = \widehat{f}(b)$, qed.

Definition 3.18. Let A be a commutative $\mathbb{F}_q$-algebra. For every finite set V and every map $\varphi : V \to A$, we let $f_{V,\varphi}$ be the polynomial $\prod_{v \in V} (X + \varphi(v)) \in A[X]$.

Theorem 3.19. Let A be a commutative $\mathbb{F}_q$-algebra. Let V be a finite $\mathbb{F}_q$-vector space, and let $\varphi : V \to A$ be an $\mathbb{F}_q$-linear map. Then, $f_{V,\varphi}$ is a q-polynomial.

Theorem 3.19 is not significantly more general than Theorem 3.17 (it is easily derived from the latter), but this little generality helps in proving it. The proof will need the following lemmas:

Lemma 3.20. Let A be a commutative $\mathbb{F}_q$-algebra. Let V and W be two finite $\mathbb{F}_q$-vector spaces. Let $\varphi : V \to A$ and $\psi : W \to A$ be two $\mathbb{F}_q$-linear maps. Assume that $f_{W,\psi}$ is a q-polynomial. Let $h : A \to A$ be an $\mathbb{F}_q$-linear map such that every $a \in A$ satisfies

$$h(a) = f_{W,\psi}(a). \tag{35}$$

Let $\chi : V \oplus W \to A$ be the $\mathbb{F}_q$-linear map which sends every $(v, w) \in V \oplus W$ to $\varphi(v) + \psi(w) \in A$. Then,

$$f_{V \oplus W, \chi} = f_{V, h \circ \varphi} \circ f_{W,\psi} \qquad \text{in } A[X].$$

Proof of Lemma 3.20. The definition of $f_{W,\psi}$ yields

$$f_{W,\psi} = \prod_{v \in W} (X + \psi(v)) = \prod_{w \in W} (X + \psi(w)) \tag{36}$$

(here, we renamed the summation index v as w).

Fix some $v \in V$. If we substitute $X + \varphi(v)$ for X on both sides of (36), then we obtain

$$f_{W,\psi}(X + \varphi(v)) = \prod_{w \in W} (X + \varphi(v) + \psi(w)). \tag{37}$$

We have assumed that $f_{W,\psi}$ is a q-polynomial. In other words, $f_{W,\psi} \in A[X]_{q-\lin}$. Hence, Proposition 3.14 (applied to $B = A[X]$ and $f = f_{W,\psi}$) shows that the map $A[X] \to A[X]$, $b \mapsto f_{W,\psi}(b)$ is $\mathbb{F}_q$-linear. Hence, $f_{W,\psi}(x_1 + x_2) = f_{W,\psi}(x_1) + f_{W,\psi}(x_2)$ for every $x_1, x_2 \in A[X]$. Applying this to $x_1 = X$ and $x_2 = \varphi(v)$, we obtain

$$\begin{aligned} f_{W,\psi}(X + \varphi(v)) &= \underbrace{f_{W,\psi}(X)}_{=f_{W,\psi}} + \underbrace{f_{W,\psi}(\varphi(v))}_{\substack{=h(\varphi(v)) \\ \text{(because (35) (applied to } a=\varphi(v)\text{)} \\ \text{yields } h(\varphi(v))=f_{W,\psi}(\varphi(v)))}} \\ &= f_{W,\psi} + \underbrace{h(\varphi(v))}_{=(h\circ\varphi)(v)} = f_{W,\psi} + (h \circ \varphi)(v). \end{aligned}$$

Comparing this with (37), we obtain

$$\prod_{w\in W}\left(X+\varphi\left(v\right)+\psi\left(w\right)\right)=f_{W,\psi}+\left(h\circ\varphi\right)\left(v\right). \tag{38}$$

Let us now forget that we fixed v. We thus have shown proven the equality (38) for all $v\in V$.

The definition of $f_{V,h\circ\varphi}$ yields

$$f_{V,h\circ\varphi}=\prod_{v\in V}\left(X+\left(h\circ\varphi\right)\left(v\right)\right).$$

Substituting $f_{W,\psi}$ for X on both sides of this equality, we obtain

$$f_{V,h\circ\varphi}\left(f_{W,\psi}\right)=\prod_{v\in V}\left(f_{W,\psi}+\left(h\circ\varphi\right)\left(v\right)\right). \tag{39}$$

The definition of $f_{V\oplus W,\chi}$ yields

$$\begin{aligned}
f_{V\oplus W,\chi} &= \prod_{v\in V\oplus W}\left(X+\chi\left(v\right)\right)=\underbrace{\prod_{(v,w)\in V\oplus W}}_{=\prod_{v\in V}\prod_{w\in W}}\left(X+\underbrace{\chi\left(v,w\right)}_{\substack{=\varphi(v)+\psi(w)\\ \text{(by the definition of }\chi\text{)}}}\right)\\
&\qquad \text{(here, we renamed the index } v \text{ as } (v,w) \text{ in the product)}\\
&= \prod_{v\in V}\underbrace{\prod_{w\in W}\left(X+\varphi\left(v\right)+\psi\left(w\right)\right)}_{\substack{=f_{W,\psi}+(h\circ\varphi)(v)\\ \text{(by (38))}}}=\prod_{v\in V}\left(f_{W,\psi}+\left(h\circ\varphi\right)\left(v\right)\right)\\
&= f_{V,h\circ\varphi}\left(f_{W,\psi}\right) \qquad \text{(by (39))}\\
&= f_{V,h\circ\varphi}\circ f_{W,\psi}.
\end{aligned}$$

This proves Lemma 3.20. □

Lemma 3.21. We have

$$\prod_{\lambda\in\mathbb{F}_q}\left(X-\lambda Y\right)=X^q-XY^{q-1} \tag{40}$$

in the polynomial ring $\mathbb{F}_q\left[X,Y\right]$.

Proof of Lemma 3.21. It is well-known that

$$\prod_{\lambda\in\mathbb{F}_q}\left(X-\lambda\right)=X^q-X \tag{41}$$

in the polynomial ring $\mathbb{F}_q[X]$ [23].

Now, consider the element X/Y in the quotient field $\mathbb{F}_q(X,Y)$ of the ring $\mathbb{F}_q[X,Y]$. Substituting this element X/Y for X in (41), we obtain

$$\prod_{\lambda\in\mathbb{F}_q}(X/Y-\lambda) = (X/Y)^q - X/Y.$$

Multiplying this equality by Y^q, we obtain

$$Y^q \prod_{\lambda\in\mathbb{F}_q}(X/Y-\lambda) = Y^q\left((X/Y)^q - X/Y\right) = X^q - XY^{q-1}.$$

Hence,

$$\begin{aligned} X^q - XY^{q-1} &= Y^q \prod_{\lambda\in\mathbb{F}_q}(X/Y-\lambda) = \prod_{\lambda\in\mathbb{F}_q} \underbrace{\left(Y\left(X/Y-\lambda\right)\right)}_{=X-\lambda Y} \qquad \left(\text{since } \left|\mathbb{F}_q\right| = q\right) \\ &= \prod_{\lambda\in\mathbb{F}_q}(X-\lambda Y). \end{aligned}$$

This proves Lemma 3.21. □

[23] Let us give a *proof of (41)* for the sake of completeness:

The polynomial $\prod_{\lambda\in\mathbb{F}_q}(X-\lambda)$ is a product of $\left|\mathbb{F}_q\right| = q$ monic polynomials of degree 1. Thus, it is a monic polynomial of degree q. Hence, both polynomials $\prod_{\lambda\in\mathbb{F}_q}(X-\lambda)$ and $X^q - X$ are monic polynomials of degree q. Their difference $\prod_{\lambda\in\mathbb{F}_q}(X-\lambda) - (X^q - X)$ therefore is a polynomial of degree $< q$ (since the subtraction causes their leading terms to cancel).

On the other hand, every $\mu \in \mathbb{F}_q$ satisfies

$$\underbrace{\prod_{\lambda\in\mathbb{F}_q}(\mu-\lambda)}_{\substack{=0 \\ \text{(since one of the factors of} \\ \text{this product is } \mu-\mu=0)}} - \left(\underbrace{\mu^q}_{\substack{=\mu \\ \text{(since } \mu\in\mathbb{F}_q\text{)}}} - \mu\right) = 0 - (\mu-\mu) = 0.$$

In other words, every $\mu \in \mathbb{F}_q$ is a root of the polynomial $\prod_{\lambda\in\mathbb{F}_q}(X-\lambda) - (X^q - X)$. Hence, the polynomial $\prod_{\lambda\in\mathbb{F}_q}(X-\lambda) - (X^q - X)$ has at least q roots (since $\mathbb{F}_q$ has at least q elements).

But $\mathbb{F}_q$ is a field. Hence, any polynomial in $\mathbb{F}_q[X]$ whose degree is smaller than its number of roots must be the zero polynomial. The polynomial $\prod_{\lambda\in\mathbb{F}_q}(X-\lambda) - (X^q - X)$ is such a polynomial (since its degree is $< q$, but it has at least q roots), and thus must be the zero polynomial. In other words, $\prod_{\lambda\in\mathbb{F}_q}(X-\lambda) = (X^q - X)$. This proves (41).

Lemma 3.22. Let A be a commutative $\mathbb{F}_q$-algebra. Let V be a one-dimensional $\mathbb{F}_q$-vector space. Let $\varphi : V \to A$ be an $\mathbb{F}_q$-linear map. Let e be a nonzero element of V. Then, $f_{V,\varphi} = X^q - (\varphi(e))^{q-1} X$.

Proof of Lemma 3.22. The element $-e$ of V is nonzero (since e is nonzero).

The $\mathbb{F}_q$-vector space V is one-dimensional, and thus any nonzero element of V forms a basis of V. Thus, $-e$ forms a basis of V (since $-e$ is a nonzero element of V). In other words, the map $\mathbb{F}_q \to V$, $\lambda \mapsto \lambda(-e)$ is a bijection. Now, the definition of $f_{V,\varphi}$ yields

$$f_{V,\varphi} = \prod_{v \in V} (X + \varphi(v)) = \prod_{\lambda \in \mathbb{F}_q} \left(X + \varphi\left(\underbrace{\lambda(-e)}_{=-\lambda e} \right) \right)$$

$$\left(\begin{array}{c} \text{here, we have substituted } \lambda(-e) \text{ for } v \text{ in the product,} \\ \text{since the map } \mathbb{F}_q \to V,\ \lambda \mapsto \lambda(-e) \text{ is a bijection} \end{array} \right)$$

$$= \prod_{\lambda \in \mathbb{F}_q} \left(X + \underbrace{\varphi(-\lambda e)}_{\substack{=-\lambda\varphi(e) \\ \text{(since } \varphi \text{ is } \mathbb{F}_q\text{-linear)}}} \right) = \prod_{\lambda \in \mathbb{F}_q} (X - \lambda\varphi(e))$$

$$= X^q - X(\varphi(e))^{q-1} \qquad \text{(this follows by substituting } \varphi(e) \text{ for } Y \text{ in (40))}$$

$$= X^q - (\varphi(e))^{q-1} X.$$

This proves Lemma 3.22. □

Proof of Theorem 3.19. We shall prove Theorem 3.19 by induction over $\dim V$:

Induction base: Theorem 3.19 holds in the case when $\dim V = 0$ [24]. This completes the induction base.

Induction step: Let $N \in \mathbb{N}$. Assume (as the induction hypothesis) that Theorem 3.19 holds in the case when $\dim V = N$. We need to show that Theorem 3.19 holds in the case when $\dim V = N + 1$.

Consider the setting of Theorem 3.19, and assume that $\dim V = N + 1$. Thus, $\dim V = N + 1 > 0$. Hence, V contains a nonzero element e. Consider this e. Let U be the $\mathbb{F}_q$-vector subspace $\mathbb{F}_q e$ of V; thus, $\dim U = 1$ (since e is nonzero).

[24] *Proof.* Consider the setting of Theorem 3.19, and assume that $\dim V = 0$. From $\dim V = 0$, we obtain $V = 0$. The definition of $f_{V,\varphi}$ yields

$$f_{V,\varphi} = \prod_{v \in V} (X + \varphi(v)) = X + \underbrace{\varphi(0)}_{\substack{=0 \\ \text{(since } \varphi \text{ is } \mathbb{F}_q\text{-linear)}}} \qquad \text{(since } V = 0\text{)}$$

$$= X.$$

Thus, $f_{V,\varphi}$ is a q-polynomial (since X is a q-polynomial). Thus, Theorem 3.19 is proven in the case when $\dim V = 0$.

Pick any complement W to the subspace U of V (such a complement exists by one of the basic theorems of linear algebra). Then, W is an $\mathbb{F}_q$-vector subspace of V satisfying $U \oplus W = V$. We shall identify V with the **external** direct sum of U and W (that is, we shall identify each element v of V with the unique pair $(u, w) \in U \times W$ satisfying $v = u + w$). Thus, the $\mathbb{F}_q$-linear map $\varphi : V \to A$ can be regarded as an $\mathbb{F}_q$-linear map $\varphi : U \oplus W \to A$.

Define two $\mathbb{F}_q$-linear maps $\gamma : U \to A$ and $\psi : W \to A$ by $\gamma = \varphi \mid_U$ and $\psi = \varphi \mid_W$. Then, the $\mathbb{F}_q$-linear map $\varphi : U \oplus W \to A$ sends every $(v, w) \in U \oplus W$ to $\gamma(v) + \psi(w)$ [25].

From $V = U \oplus W$, we obtain $\dim V = \dim U + \dim W$, so that $\dim W = \underbrace{\dim V}_{=N+1} - \underbrace{\dim U}_{=1} = N + 1 - 1 = N$. Thus, (according to the induction hypothesis) Theorem 3.19 can be applied to W and ψ instead of V and φ. As a consequence, we obtain that $f_{W,\psi}$ is a q-polynomial. In other words, $f_{W,\psi} \in A[X]_{q-\mathrm{lin}}$. Thus, Proposition 3.14 (applied to $f = f_{W,\psi}$ and $B = A$) shows that the map $A \to A$, $b \mapsto f_{W,\psi}(b)$ is $\mathbb{F}_q$-linear. Let us denote this map by h. Thus, h is the map $A \to A$, $b \mapsto f_{W,\psi}(b)$, and is $\mathbb{F}_q$-linear. Every $a \in A$ satisfies $h(a) = f_{W,\psi}(a)$ (by the definition of h).

Now, Lemma 3.20 (applied to U, γ and φ instead of V, φ and χ) shows that $f_{U \oplus W,\varphi} = f_{U,h\circ\gamma} \circ f_{W,\psi}$ in $A[X]$.

But the $\mathbb{F}_q$-vector space U is one-dimensional (since $\dim U = 1$) and contains the nonzero vector e (since $U = \mathbb{F}_q e \supseteq e$). Thus, Lemma 3.22 (applied to U and $h \circ \gamma$ instead of V and φ) shows that $f_{U,h\circ\gamma} = X^q - ((h \circ \gamma)(e))^{q-1} X$. This is clearly a q-polynomial (since $((h \circ \gamma)(e))^{q-1}$ is just a coefficient in A). In other words, $f_{U,h\circ\gamma} \in A[X]_{q-\mathrm{lin}}$.

Proposition 3.10 **(b)** shows that $A[X]_{q-\mathrm{lin}}$ is a submonoid of the monoid $(A[X], \circ)$. Hence, $A[X]_{q-\mathrm{lin}}$ is closed under the binary operation $\circ$. Therefore, $f_{U,h\circ\gamma} \circ f_{W,\psi} \in A[X]_{q-\mathrm{lin}}$ (since $f_{U,h\circ\gamma} \in A[X]_{q-\mathrm{lin}}$ and $f_{W,\psi} \in A[X]_{q-\mathrm{lin}}$). But $V = U \oplus W$, so that $f_{V,\varphi} = f_{U\oplus W,\varphi} = f_{U,h\circ\gamma} \circ f_{W,\psi} \in A[X]_{q-\mathrm{lin}}$. In other words, $f_{V,\varphi}$ is a q-polynomial. Thus, Theorem 3.19 is proven in the case when $\dim V = N + 1$. This completes the induction step.

The proof of Theorem 3.19 is thus complete. □

As a consequence of Theorem 3.19, we can remove one unneeded assumption from Lemma 3.20:

[25] *Proof.* Let $(v, w) \in U \oplus W$. We must show that $\varphi(v, w) = \gamma(v) + \psi(w)$.

We have $v \in U$, and thus $\gamma(v) = \varphi(v)$ (since $\gamma = \varphi \mid_U$). We have $w \in W$, and thus $\psi(w) = \varphi(w)$ (since $\psi = \varphi \mid_W$). The map φ is $\mathbb{F}_q$-linear, and thus $\varphi(v + w) = \underbrace{\varphi(v)}_{=\gamma(v)} + \underbrace{\varphi(w)}_{=\psi(w)} = \gamma(v) + \psi(w)$. But recall that we are identifying $(v, w) \in U \oplus W$ with $v + w \in V$. Thus, $\varphi(v, w) = \varphi(v + w) = \gamma(v) + \psi(w)$, qed.

Corollary 3.23. Let A be a commutative $\mathbb{F}_q$-algebra. Let V and W be two $\mathbb{F}_q$-vector spaces. Let $\varphi : V \to A$ and $\psi : W \to A$ be two $\mathbb{F}_q$-linear maps. Let $h : A \to A$ be an $\mathbb{F}_q$-linear map such that every $a \in A$ satisfies $h(a) = f_{W,\psi}(a)$. Let $\chi : V \oplus W \to A$ be the $\mathbb{F}_q$-linear map which sends every $(v, w) \in V \oplus W$ to $\varphi(v) + \psi(w) \in A$. Then,

$$f_{V \oplus W, \chi} = f_{V, h \circ \varphi} \circ f_{W,\psi} \qquad \text{in } A[X].$$

Proof of Corollary 3.23. Theorem 3.19 (applied to W and ψ instead of V and φ) shows that $f_{W,\psi}$ is a q-polynomial. Thus, Lemma 3.20 shows that $f_{V \oplus W, \chi} = f_{V, h \circ \varphi} \circ f_{W,\psi}$ in $A[X]$. This proves Corollary 3.23. □

Let us finally derive Theorem 3.17 from Theorem 3.19:

Proof of Theorem 3.17. Let ι be the canonical inclusion map $V \to A$. Thus, ι is an $\mathbb{F}_q$-linear map. Hence, Theorem 3.19 (applied to $\varphi = \iota$) shows that $f_{V,\iota}$ is a q-polynomial. But the definition of $f_{V,\iota}$ shows that

$$f_{V,\iota} = \prod_{v \in V} \left(X + \underbrace{\iota(v)}_{\substack{=v \\ \text{(since } \iota \text{ is an} \\ \text{inclusion map)}}} \right) = \prod_{v \in V} (X + v) = f_V$$

(since this is how f_V is defined). Thus, f_V is a q-polynomial (since $f_{V,\iota}$ is a q-polynomial). This proves Theorem 3.17. □

3.5. Further consequences of the Fqpol isomorphism

Let us return to $\mathcal{F}$. We shall now exploit the isomorphism Fqpol to obtain properties of $\mathcal{F}$.

First, let us recall that if A is any commutative $\mathbb{F}_q$-algebra, then $A[X]_{q-\mathrm{lin}}$ is an A-submodule of $A[X]$. Applying this to $A = \mathbb{F}_q[T]$, we see that

$$\mathbb{F}_q[T][X]_{q-\mathrm{lin}} \text{ is an } \mathbb{F}_q[T]\text{-submodule of } \mathbb{F}_q[T][X]. \tag{42}$$

We shall write this $\mathbb{F}_q[T]$-module structure on the left (i.e., we use it to make $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ into a left $\mathbb{F}_q[T]$-module). This left $\mathbb{F}_q[T]$-module structure is given by plain multiplication inside $\mathbb{F}_q[T][X]$. It has the following property:

Proposition 3.24. The map $\mathrm{Fqpol} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ is an isomorphism of left $\mathbb{F}_q[T]$-modules.

Proof of Proposition 3.24. Proposition 3.5 **(b)** says that the $\mathbb{F}_q$-module $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$.

Theorem 3.13 **(b)** shows that Fqpol is an $\mathbb{F}_q$-algebra isomorphism. Thus, it remains to prove that Fqpol is a homomorphism of left $\mathbb{F}_q[T]$-modules. In other words, it remains to prove that $\operatorname{Fqpol}(fu) = f \operatorname{Fqpol}(u)$ for every $f \in \mathbb{F}_q[T]$ and $u \in \mathcal{F}$.

So let $f \in \mathbb{F}_q[T]$ and $u \in \mathcal{F}$. We need to prove the equality $\operatorname{Fqpol}(fu) = f \operatorname{Fqpol}(u)$. This equality is $\mathbb{F}_q$-linear in u. Hence, we can WLOG assume that u belongs to the basis $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ of the $\mathbb{F}_q$-module $\mathcal{F}$. Assume this. Thus, $u = T^j F^i$ for some $i \in \mathbb{N}$ and $j \in \mathbb{N}$. Consider these i and j.

We still need to prove the equality $\operatorname{Fqpol}(fu) = f \operatorname{Fqpol}(u)$. This equality is $\mathbb{F}_q$-linear in f. Hence, we can WLOG assume that f belongs to the basis $\left(T^k\right)_{k\geq 0}$ of the $\mathbb{F}_q$-module $\mathbb{F}_q[T]$. Assume this. Thus, $f = T^k$ for some $k \in \mathbb{N}$. Consider this k.

Multiplying the equalities $f = T^k$ and $u = T^j F^i$, we obtain $fu = \underbrace{T^k T^j}_{=T^{k+j}} F^i = T^{k+j} F^i$. Hence, $\operatorname{Fqpol}(fu) = \operatorname{Fqpol}\left(T^{k+j} F^i\right) = T^{k+j} X^{q^i}$ (by Theorem 3.13 **(c)**, applied to $k+j$ instead of j). On the other hand, $u = T^j F^i$, so that $\operatorname{Fqpol}(u) = \operatorname{Fqpol}\left(T^j F^i\right) = T^j X^{q^i}$ (by Theorem 3.13 **(c)**). Multiplying the equalities $f = T^k$ and $\operatorname{Fqpol}(u) = T^j X^{q^i}$, we obtain $f \operatorname{Fqpol}(u) = \underbrace{T^k T^j}_{=T^{k+j}} X^{q^i} = T^{k+j} X^{q^i}$. Comparing this with $\operatorname{Fqpol}(fu) = T^{k+j} X^{q^i}$, we obtain $\operatorname{Fqpol}(fu) = f \operatorname{Fqpol}(u)$. As explained, this completes the proof of Proposition 3.24. □

Notice that we can use Proposition 3.24 to recover Proposition 3.5 **(c)**:

Second proof of Proposition 3.5 (c). Proposition 3.24 yields that $\mathcal{F} \cong \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ as left $\mathbb{F}_q[T]$-modules, via the isomorphism Fqpol. Since the left $\mathbb{F}_q[T]$-module $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ has basis $\left(X^{q^0}, X^{q^1}, X^{q^2}, \ldots\right)$, we can therefore conclude that the left $\mathbb{F}_q[T]$-module $\mathcal{F}$ has basis $\left(\operatorname{Fqpol}^{-1}\left(X^{q^0}\right), \operatorname{Fqpol}^{-1}\left(X^{q^1}\right), \operatorname{Fqpol}^{-1}\left(X^{q^2}\right), \ldots\right)$. Since $\operatorname{Fqpol}^{-1}\left(X^{q^i}\right) = F^i$ for every $i \in \mathbb{N}$ [26], this rewrites as follows: The left $\mathbb{F}_q[T]$-module $\mathcal{F}$ has basis $\left(F^i\right)_{i\geq 0}$. This proves Proposition 3.5 **(c)** again. □

Let us make some more remarks (in less detail, since these will not be used in the following):

Proposition 3.24 can be rewritten as follows: If we transport the left $\mathbb{F}_q[T]$-module structure on $\mathcal{F}$ to $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ via the isomorphism $\operatorname{Fqpol} : \mathcal{F} \to$

[26] *Proof.* Let $i \in \mathbb{N}$. Theorem 3.13 **(c)** (applied to $j = 0$) yields $\operatorname{Fqpol}\left(T^0 F^i\right) = \underbrace{T^0}_{=1} X^{q^i} = X^{q^i}$. Thus, $\operatorname{Fqpol}^{-1}\left(X^{q^i}\right) = \underbrace{T^0}_{=1} F^i = F^i$, qed.

$\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$, then we obtain the left $\mathbb{F}_q[T]$-module structure on $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ constructed in (42). Of course, we can also use the isomorphism Fqpol to transport all the other module structures from $\mathcal{F}$ to $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ along Fqpol. In more detail:

From Proposition 3.5, we know that $\mathcal{F}$ is a left $\mathbb{F}_q[T]$-module, a right $\mathbb{F}_q[T]$-module, a left $\mathbb{F}_q[F]$-module, and a right $\mathbb{F}_q[F]$-module. Thus, we have altogether four module structures on $\mathcal{F}$. Using the isomorphism $\mathrm{Fqpol} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$, we can transport them to $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$; therefore, $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ becomes a left $\mathbb{F}_q[T]$-module, a right $\mathbb{F}_q[T]$-module, a left $\mathbb{F}_q[F]$-module, and a right $\mathbb{F}_q[F]$-module. As we have already said, the first of these four module structures is precisely the left $\mathbb{F}_q[T]$-module structure on $\mathcal{F}$ constructed in (42). The other three structures are new. Explicitly, two of them are characterized as follows:

- If $t \in \mathbb{F}_q[T]$, then the action of t on the right $\mathbb{F}_q[T]$-module $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ sends every $m \in \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ to $m \circ \underbrace{\mathrm{Fqpol}\, t}_{\substack{=t\cdot X \\ \text{(by Theorem 3.13 \textbf{(d)})}}} = m \circ (t \cdot X) = m(t \cdot X)$ (that is, the result of substituting $t \cdot X$ for X in m).
- If $f \in \mathbb{F}_q[F]$, then the action of f on the left $\mathbb{F}_q[F]$-module $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ sends every $m \in \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ to $\mathrm{Fqpol}\, f \circ m = f\left(\mathrm{Frob}_{\mathbb{F}_q[T][X]}\right) \circ m$.

3.6. Frobenius $\mathbb{F}_q[T]$-modules

In the following, "$\mathcal{F}$-module" will always mean "left $\mathcal{F}$-module", unless stated otherwise. The following fact is a simple consequence of the definition of $\mathcal{F}$ (specifically, of the fact that $\mathcal{F}$ is generated by F and T as an $\mathbb{F}_q$-algebra):

Lemma 3.25. Let M and N be two $\mathcal{F}$-modules. Let $f : M \to N$ be an $\mathbb{F}_q$-linear map. Assume that

$$f(Tu) = Tf(u) \qquad \text{for every } u \in M.$$

Assume also that

$$f(Fu) = Ff(u) \qquad \text{for every } u \in M.$$

Then, f is an $\mathcal{F}$-module homomorphism.

This lemma shall be used tacitly further below; it is the most reasonable way to prove that a certain map between two $\mathcal{F}$-modules M and N is an $\mathcal{F}$-module homomorphism, particularly in the case when the $\mathcal{F}$-module structure on at least one of M and N is defined not explicitly but by providing the actions of F and T.

Part of the interest in the $\mathbb{F}_q$-algebra $\mathcal{F}$ is due to its category of modules: it can be described as the category of "Frobenius $\mathbb{F}_q[T]$-modules", by which we mean $\mathbb{F}_q[T]$-modules equipped with a "Frobenius map" satisfying a certain rule. Let us define this in more detail:

Definition 3.26. (a) A *Frobenius $\mathbb{F}_q[T]$-module* means a pair $(M, \mathfrak{f})$, where M is an $\mathbb{F}_q[T]$-module, and where $\mathfrak{f} : M \to M$ is an $\mathbb{F}_q$-linear map satisfying

$$\mathfrak{f}(Tm) = T^q \mathfrak{f}(m) \qquad \text{for every } m \in M. \tag{43}$$

This map $\mathfrak{f}$ is called the *Frobenius map* of the Frobenius $\mathbb{F}_q[T]$-module $(M, \mathfrak{f})$. By abuse of notation, we shall often speak of the "Frobenius $\mathbb{F}_q[T]$-module M" instead of the "Frobenius $\mathbb{F}_q[T]$-module $(M, \mathfrak{f})$", leaving the Frobenius map $\mathfrak{f}$ implicit; in this situation, the Frobenius map $\mathfrak{f}$ will be denoted by $\mathfrak{f}_M$.

(b) Let M and N be two Frobenius $\mathbb{F}_q[T]$-modules. Then, a map $h : M \to N$ is said to be a *homomorphism of Frobenius $\mathbb{F}_q[T]$-modules* if and only if it is $\mathbb{F}_q[T]$-linear and "respects the Frobenius maps" (i.e., satisfies $\mathfrak{f}_N \circ h = h \circ \mathfrak{f}_M$).

(c) We let $\mathrm{FrobMod}_{\mathbb{F}_q[T]}$ denote the category whose objects are the Frobenius $\mathbb{F}_q[T]$-modules, and whose morphisms are the homomorphisms of Frobenius $\mathbb{F}_q[T]$-modules.

It turns out that this category $\mathrm{FrobMod}_{\mathbb{F}_q[T]}$ is isomorphic to the category of $\mathcal{F}$-modules:

Proposition 3.27. Let $\mathrm{Mod}_{\mathcal{F}}$ be the category of all (left) $\mathcal{F}$-modules.

Recall that we are regarding the $\mathbb{F}_q$-algebra homomorphism $\mathrm{Finc}_T : \mathbb{F}_q[T] \to \mathcal{F}$ as an inclusion. Thus, $\mathbb{F}_q[T]$ is an $\mathbb{F}_q$-subalgebra of $\mathcal{F}$.

(a) Let M be a Frobenius $\mathbb{F}_q[T]$-module. Then, there exists a unique $\mathcal{F}$-module structure on M which extends the $\mathbb{F}_q[T]$-module structure on M and satisfies

$$F \cdot m = \mathfrak{f}_M(m) \qquad \text{for every } m \in M.$$

(b) Let N be an $\mathcal{F}$-module. Then, N becomes an $\mathbb{F}_q[T]$-module (since $\mathbb{F}_q[T] \subseteq \mathcal{F}$). Let $\mathfrak{f}$ be the action of $F \in \mathcal{F}$ on N (that is, the $\mathbb{F}_q$-linear map $N \to N$, $n \mapsto F \cdot n$). Then, $(N, \mathfrak{f})$ is a Frobenius $\mathbb{F}_q[T]$-module.

(c) Proposition 3.27 **(a)** defines a functor from $\mathrm{FrobMod}_{\mathbb{F}_q[T]}$ to $\mathrm{Mod}_{\mathcal{F}}$ (because, to any Frobenius $\mathbb{F}_q[T]$-module M, it assigns an $\mathcal{F}$-module structure on M, and this assignment can easily be extended to morphisms). Proposition 3.27 **(b)** defines a functor from $\mathrm{Mod}_{\mathcal{F}}$ to $\mathrm{FrobMod}_{\mathbb{F}_q[T]}$ (because, to any $\mathcal{F}$-module N, it assigns a Frobenius $\mathbb{F}_q[T]$-module $(N, \mathfrak{f})$, and this assignment can easily be extended to morphisms). These two functors are mutually inverse. Thus, the categories $\mathrm{FrobMod}_{\mathbb{F}_q[T]}$ and $\mathrm{Mod}_{\mathcal{F}}$ are isomorphic.

Proof of Proposition 3.27. **(a)** We let $\mathrm{End}\, M$ denote the $\mathbb{F}_q$-algebra of all $\mathbb{F}_q$-module endomorphisms of M.

It is clear that there exists **at most one** $\mathcal{F}$-module structure on M which extends the $\mathbb{F}_q[T]$-module structure on M and satisfies

$$F \cdot m = \mathfrak{f}_M(m) \qquad \text{for every } m \in M \tag{44}$$

[27]. It thus remains to prove that there exists **at least one** such structure. So let us construct such a structure.

As usual, we abbreviate $\mathfrak{f}_M$ as $\mathfrak{f}$.

Let $\mathfrak{t}$ be the $\mathbb{F}_q$-linear map $M \to M,\ m \mapsto T \cdot m$. Then, for every $n \in \mathbb{N}$ and $m \in M$, we have

$$\mathfrak{t}^n(m) = T^n \cdot m. \tag{45}$$

(This is easy to prove by induction over n.)

For every $m \in M$, we have

$$\begin{aligned}(\mathfrak{f} \circ \mathfrak{t})(m) &= \mathfrak{f}\left(\underbrace{\mathfrak{t}(m)}_{\substack{=T\cdot m \\ \text{(by the definition of } \mathfrak{t})}}\right) = \mathfrak{f}(T \cdot m) = \mathfrak{f}(Tm) = T^q \mathfrak{f}(m) \qquad \text{(by (43))} \\ &= \mathfrak{t}^q(\mathfrak{f}(m)) \\ &\qquad \left(\begin{array}{c}\text{because (45) (applied to } q \text{ and } \mathfrak{f}(m) \text{ instead of } n \text{ and } m)\\ \text{shows that } \mathfrak{t}^q(\mathfrak{f}(m)) = T^q \cdot \mathfrak{f}(m) = T^q \mathfrak{f}(m)\end{array}\right) \\ &= (\mathfrak{t}^q \circ \mathfrak{f})(m).\end{aligned}$$

Hence, $\mathfrak{f} \circ \mathfrak{t} = \mathfrak{t}^q \circ \mathfrak{f}$.

Now, recall the universal property of $\mathcal{F}$: If u and v are two elements of an $\mathbb{F}_q$-algebra $\mathcal{U}$ satisfying $uv = v^q u$, then there exists a unique $\mathbb{F}_q$-algebra homomorphism $\mathcal{F} \to \mathcal{U}$ sending F and T to u and v, respectively. Applying this to $\mathcal{U} = \operatorname{End} M$, $u = \mathfrak{f}$ and $v = \mathfrak{t}$, we conclude that there exists a unique $\mathbb{F}_q$-algebra homomorphism $\mathcal{F} \to \operatorname{End} M$ sending F and T to $\mathfrak{f}$ and $\mathfrak{t}$, respectively. Let Φ be this homomorphism. The definition of Φ shows that $\Phi(F) = \mathfrak{f}$ and $\Phi(T) = \mathfrak{t}$.

We have

$$(\Phi(f))(m) = f \cdot m \qquad \text{for every } f \in \mathbb{F}_q[T] \text{ and } m \in M \tag{46}$$

[28]. Thus, the $\mathcal{F}$-module structure on M obtained from the map $\Phi : \mathcal{F} \to \operatorname{End} M$ extends the $\mathbb{F}_q[T]$-module structure on M.

[27] Indeed, the requirement that this structure extends the $\mathbb{F}_q[T]$-module structure on M uniquely determines how T acts on M. Meanwhile, the requirement (44) uniquely determines how F acts on M. Thus, the actions of both T and F on M are uniquely determined. But therefore, the action of any element of $\mathcal{F}$ on M is uniquely determined as well (since the $\mathbb{F}_q$-algebra $\mathcal{F}$ is generated by T and F); in other words, the $\mathcal{F}$-module structure on M is uniquely determined, qed.

[28] *Proof of (45):* Let $f \in \mathbb{F}_q[T]$ and $m \in M$. We have to prove the equality $(\Phi(f))(m) = f \cdot m$. This equality is $\mathbb{F}_q$-linear in f; we can therefore WLOG assume that f belongs to the basis $(T^n)_{n \geq 0}$ of the $\mathbb{F}_q$-module $\mathbb{F}_q[T]$. Assume this. Hence, $f = T^n$ for some $n \in \mathbb{N}$. Consider this n. From

Furthermore, $\underbrace{(\Phi(F))}_{=\mathfrak{f}=\mathfrak{f}_M}(m) = \mathfrak{f}_M(m)$ for every $m \in M$. Thus, the $\mathcal{F}$-module structure on M obtained from the map $\Phi : \mathcal{F} \to \operatorname{End} M$ satisfies (44).

Hence, there exists at least one $\mathcal{F}$-module structure on M which extends the $\mathbb{F}_q[T]$-module structure on M and satisfies (44) (namely, the $\mathcal{F}$-module structure on M obtained from the map $\Phi : \mathcal{F} \to \operatorname{End} M$). This completes the proof of Proposition 3.27 **(a)**.

(b) We need to show that $(N, \mathfrak{f})$ is a Frobenius $\mathbb{F}_q[T]$-module. In other words, we need to show that N is an $\mathbb{F}_q[T]$-module, that $\mathfrak{f} : N \to N$ is an $\mathbb{F}_q$-linear map, and that this map $\mathfrak{f}$ satisfies

$$\mathfrak{f}(Tm) = T^q \mathfrak{f}(m) \qquad \text{for every } m \in N. \tag{47}$$

The first two of these statements are obvious. It thus remains to prove the third statement, i.e., to prove that the map $\mathfrak{f}$ satisfies (47).

So let $m \in N$. The definition of $\mathfrak{f}$ yields $\mathfrak{f}(m) = Fm$ and $\mathfrak{f}(Tm) = F \cdot Tm = \underbrace{FT}_{=T^q F} m = T^q \underbrace{Fm}_{=\mathfrak{f}(m)} = T^q \mathfrak{f}(m)$. Thus, (47) is proven. As we have already explained, this completes the proof of Proposition 3.27 **(b)**.

(c) It is clear that if we apply the functor $\mathrm{FrobMod}_{\mathbb{F}_q[T]} \to \mathrm{Mod}_{\mathcal{F}}$ first and then the functor $\mathrm{Mod}_{\mathcal{F}} \to \mathrm{FrobMod}_{\mathbb{F}_q[T]}$, then we get back to where we started. It is somewhat less obvious, but still easy, to prove that if we apply the functor $\mathrm{Mod}_{\mathcal{F}} \to \mathrm{FrobMod}_{\mathbb{F}_q[T]}$ first and then the functor $\mathrm{FrobMod}_{\mathbb{F}_q[T]} \to \mathrm{Mod}_{\mathcal{F}}$, then we get back to where we started[29]. Thus, the functors $\mathrm{FrobMod}_{\mathbb{F}_q[T]} \to \mathrm{Mod}_{\mathcal{F}}$ and $\mathrm{Mod}_{\mathcal{F}} \to \mathrm{FrobMod}_{\mathbb{F}_q[T]}$ are mutually inverse. This proves Proposition 3.27 **(c)**. □

An ample supply of Frobenius $\mathbb{F}_q[T]$-modules (and thus, $\mathcal{F}$-module) is given by commutative $\mathbb{F}_q[T]$-algebras and their Frobenius homomorphisms:

Proposition 3.28. (a) If A is a commutative $\mathbb{F}_q[T]$-algebra, then (A, Frob_A) is a Frobenius $\mathbb{F}_q[T]$-module.

(b) If A and B are two commutative $\mathbb{F}_q[T]$-algebras, and if $f : A \to B$ is an $\mathbb{F}_q[T]$-algebra homomorphism, then f is also a homomorphism of Frobenius $\mathbb{F}_q[T]$-modules from (A, Frob_A) to (B, Frob_B).

$f = T^n$, we obtain $\Phi(f) = \Phi(T^n) = (\Phi(T))^n$ (since Φ is an $\mathbb{F}_q$-algebra homomorphism). Since $\Phi(T) = \mathfrak{t}$, this rewrites as $\Phi(f) = \mathfrak{t}^n$. Therefore, $\underbrace{(\Phi(f))}_{=\mathfrak{t}^n}(m) = \mathfrak{t}^n(m) = T^n \cdot m$ (by (45)). Hence, $(\Phi(f))(m) = \underbrace{T^n}_{=f} \cdot m = f \cdot m$. This proves (45).

[29] In order to prove this, it suffices to observe that an $\mathcal{F}$-module structure on a given $\mathbb{F}_q$-vector space is uniquely determined by the actions of F and T (because the $\mathbb{F}_q$-algebra $\mathcal{F}$ is generated by F and T).

(c) Proposition 3.28 **(a)** assigns a Frobenius $\mathbb{F}_q[T]$-module (A, Frob_A) to each commutative $\mathbb{F}_q[T]$-algebra A. This defines a functor from the category of commutative $\mathbb{F}_q[T]$-algebras to the category $\mathrm{FrobMod}_{\mathbb{F}_q[T]}$ of Frobenius $\mathbb{F}_q[T]$-modules (the action of this functor on morphisms just leaves morphisms unchanged), and thus to the category $\mathrm{Mod}_{\mathcal{F}}$ of $\mathcal{F}$-modules (because Proposition 3.27 **(c)** shows that $\mathrm{FrobMod}_{\mathbb{F}_q[T]} \cong \mathrm{Mod}_{\mathcal{F}}$). Explicitly, this shows that every commutative $\mathbb{F}_q[T]$-algebra A canonically becomes an $\mathcal{F}$-module, and this $\mathcal{F}$-module structure extends the $\mathbb{F}_q[T]$-module structure on A and has the property that

$$F \cdot m = \mathrm{Frob}_A(m) \qquad \text{for every } m \in A.$$

Proof of Proposition 3.28. **(a)** Let A be a commutative $\mathbb{F}_q[T]$-algebra. As we know, $\mathrm{Frob}_A : A \to A$ is an $\mathbb{F}_q$-algebra homomorphism, and thus an $\mathbb{F}_q$-linear map. Furthermore, it satisfies

$$\mathrm{Frob}_A(Tm) = T^q \mathrm{Frob}_A(m)$$

for every $m \in A$ [30]. Hence, (A, Frob_A) is a Frobenius $\mathbb{F}_q[T]$-module (by the definition of a "Frobenius $\mathbb{F}_q[T]$-module"). This proves Proposition 3.28 **(a)**.

(b) The proof of Proposition 3.28 **(b)** is straightforward.

(c) Proposition 3.28 **(c)** follows from what we have proven above. (Specifically, the statement that the $\mathcal{F}$-module structure on A extends the $\mathbb{F}_q[T]$-module structure on A and has the property that

$$F \cdot m = \mathrm{Frob}_A(m) \qquad \text{for every } m \in A$$

is a consequence of Proposition 3.27 **(a)**.) □

Restricted Lie algebras (see, e.g., [14]) can be used as another source of Frobenius $\mathbb{F}_q[T]$-modules, provided they can be equipped with an appropriate $\mathbb{F}_q[T]$-module structure. We are not currently aware of specific examples of interest, however.

Convention 3.29. Let A be a commutative $\mathbb{F}_q[T]$-algebra. Then, (A, Frob_A) is a Frobenius $\mathbb{F}_q[T]$-module (by Proposition 3.28 **(a)**), and thus Proposition 3.27 **(a)** (applied to $M = A$) defines an $\mathcal{F}$-module structure on A. In the following, we shall always regard a commutative $\mathbb{F}_q[T]$-algebra A as equipped with this $\mathcal{F}$-module structure by default. This structure extends the $\mathbb{F}_q[T]$-module structure on A, and satisfies

$$F \cdot m = \mathrm{Frob}_A(m) = m^q \qquad \text{(by the definition of } \mathrm{Frob}_A\text{)} \tag{48}$$

for every $m \in A$.

[30] *Proof.* Let $m \in A$. Then, the definition of Frob_A shows that $\mathrm{Frob}_A(m) = m^q$ and $\mathrm{Frob}_A(Tm) = (Tm)^q = T^q \underbrace{m^q}_{=\mathrm{Frob}_A(m)} = T^q \mathrm{Frob}_A(m)$, qed.

Proposition 3.30. Let A be a commutative $\mathbb{F}_q[T]$-algebra. Then, A is an $\mathcal{F}$-module (according to Convention 3.29). This $\mathcal{F}$-module structure has the following property: For every $k \in \mathbb{N}$ and $m \in A$, we have

$$F^k \cdot m = m^{q^k}. \tag{49}$$

Proof of Proposition 3.30. Only (49) needs to be proven.

From (48), we know that

$$F \cdot m = m^q \qquad \text{for every } m \in A. \tag{50}$$

Thus,

$$F^k \cdot m = m^{q^k} \qquad \text{for every } m \in A \text{ and } k \in \mathbb{N}. \tag{51}$$

(Indeed, (51) can be proven by a straightforward induction over k; the induction step will rely on (50). The details of this proof are left to the reader.)

So we know that (51) holds. In other words, (49) holds. This proves Proposition 3.30. □

Proposition 3.31. The commutative $\mathbb{F}_q[T]$-algebra $\mathbb{F}_q[T][X]$ becomes an $\mathcal{F}$-module (by Convention 3.29, applied to $A = \mathbb{F}_q[T][X]$). Let $\overline{\mathrm{Fqpol}}$ denote the map $\mathrm{Fqpol} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$, considered as a map $\mathcal{F} \to \mathbb{F}_q[T][X]$ (this is well-defined because $\mathbb{F}_q[T][X]_{q-\mathrm{lin}} \subseteq \mathbb{F}_q[T][X]$). Then, this map $\overline{\mathrm{Fqpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]$ is an $\mathcal{F}$-module homomorphism.

Proof of Proposition 3.31. Proposition 3.24 shows that the map $\mathrm{Fqpol} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ is an isomorphism of left $\mathbb{F}_q[T]$-modules. Thus, the map $\overline{\mathrm{Fqpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]$ (which differs from $\mathrm{Fqpol} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ only in its target) is also a homomorphism of left $\mathbb{F}_q[T]$-modules. In other words, $\overline{\mathrm{Fqpol}}(fu) = f\overline{\mathrm{Fqpol}}(u)$ for every $f \in \mathbb{F}_q[T]$ and $u \in \mathcal{F}$. Applying this to $f = T$, we obtain

$$\overline{\mathrm{Fqpol}}(Tu) = T\overline{\mathrm{Fqpol}}(u) \qquad \text{for every } u \in \mathcal{F}. \tag{52}$$

On the other hand, let $u \in \mathcal{F}$. Then,

$$\begin{aligned}
&\overline{\mathrm{Fqpol}}(Fu) \\
&= \mathrm{Fqpol}(Fu) \qquad \Big(\text{by the definition of } \overline{\mathrm{Fqpol}}\Big) \\
&= \underbrace{(\mathrm{Fqpol}(F))}_{=X^q} \circ (\mathrm{Fqpol}(u)) \\
&\qquad \Big(\text{since } \mathrm{Fqpol} \text{ is an } \mathbb{F}_q\text{-algebra homomorphism } \mathcal{F} \to \Big(\mathbb{F}_q[T][X]_{q-\mathrm{lin}}, +, \circ\Big)\Big) \\
&= X^q \circ (\mathrm{Fqpol}(u)) = (\mathrm{Fqpol}(u))^q.
\end{aligned}$$

Comparing this with

$$F\overline{\mathrm{Fqpol}}\left(u\right) = F \cdot \overline{\mathrm{Fqpol}}\left(u\right) = \left(\underbrace{\overline{\mathrm{Fqpol}}\left(u\right)}_{\substack{=\mathrm{Fqpol}(u) \\ \text{(by the definition of } \overline{\mathrm{Fqpol}}\text{)}}} \right)^q$$

$$\left(\text{by (48), applied to } A = \mathbb{F}_q\left[T\right]\left[X\right] \text{ and } m = \overline{\mathrm{Fqpol}}\left(u\right)\right)$$

$$= \left(\mathrm{Fqpol}\left(u\right)\right)^q,$$

we obtain $\overline{\mathrm{Fqpol}}\left(Fu\right) = F\overline{\mathrm{Fqpol}}\left(u\right)$. Let us now forget that we fixed u. We thus have shown that

$$\overline{\mathrm{Fqpol}}\left(Fu\right) = F\overline{\mathrm{Fqpol}}\left(u\right) \qquad \text{for every } u \in \mathcal{F}. \tag{53}$$

Now, Lemma 3.25 (applied to $M = \mathcal{F}$, $N = \mathbb{F}_q\left[T\right]\left[X\right]$ and $f = \overline{\mathrm{Fqpol}}$) shows that $\overline{\mathrm{Fqpol}}$ is an $\mathcal{F}$-module homomorphism (because of (52) and (53)). This proves Proposition 3.31. □

3.7. The Carlitz action

Now, let us recall the Carlitz polynomials $\left[M\right]$ defined in Definition 1.1. We can connect these polynomials to $\mathcal{F}$ in the following way[31]:

Proposition 3.32. Let A be a commutative $\mathbb{F}_q\left[T\right]$-algebra. Thus, A becomes an $\mathcal{F}$-module (by Convention 3.29).

For every $M \in \mathbb{F}_q\left[T\right]$ and $a \in A$, we have $\left[M\right]\left(a\right) = \left(\mathrm{Carl}\, M\right) \cdot a$. (Here, the $\left[M\right]\left(a\right)$ on the left hand side means the result of substituting a for X in the polynomial $\left[M\right] \in \mathbb{F}_q\left[T\right]\left[X\right]$, whereas the $\left(\mathrm{Carl}\, M\right) \cdot a$ on the right hand side denotes the action of $\mathrm{Carl}\, M \in \mathcal{F}$ on $a \in A$.)

Proof of Proposition 3.32. We first claim that

$$\left[T^n\right]\left(a\right) = \left(F + T\right)^n a \qquad \text{for every } n \in \mathbb{N} \text{ and } a \in A. \tag{54}$$

Proof of (54): We shall prove (54) by induction over n:

Induction base: We have $\left[T^0\right] = X$, thus $\left[T^0\right]\left(a\right) = X\left(a\right) = a$. Comparing this with $\underbrace{\left(F + T\right)^0}_{=1} a = a$, we obtain $\left[T^0\right]\left(a\right) = \left(F + T\right)^0 a$. In other words, (54) holds for $n = 0$. This completes the induction base.

Induction step: Fix a positive integer N. Assume that (54) holds for $n = N - 1$. We now need to show that (54) holds for $n = N$.

[31] Recall that Carl is the $\mathbb{F}_q$-algebra homomorphism $\mathbb{F}_q\left[T\right] \to \mathcal{F}$ sending T to $F + T$.

We have assumed that (54) holds for $n = N - 1$. In other words, we have

$$\left[T^{N-1}\right](a) = (F+T)^{N-1} a \qquad \text{for every } a \in A. \tag{55}$$

Now, fix $a \in A$. Applying (48) to $m = \left[T^{N-1}\right](a)$, we obtain

$$F \cdot \left[T^{N-1}\right](a) = \left(\left[T^{N-1}\right](a)\right)^q. \tag{56}$$

The recursive definition of $\left[T^N\right]$ yields $\left[T^N\right] = \left[T^{N-1}\right]^q + T\left[T^{N-1}\right]$. Hence,

$$\begin{aligned}
\left[T^N\right](a) &= \left(\left[T^{N-1}\right]^q + T\left[T^{N-1}\right]\right)(a) = \underbrace{\left(\left[T^{N-1}\right](a)\right)^q}_{=F\cdot\left[T^{N-1}\right](a)} + T\left[T^{N-1}\right](a) \\
&= F \cdot \left[T^{N-1}\right](a) + T \cdot \left[T^{N-1}\right](a) = (F+T) \underbrace{\left[T^{N-1}\right](a)}_{\substack{=(F+T)^{N-1}a \\ \text{(by (55))}}} \\
&= \underbrace{(F+T)(F+T)^{N-1}}_{=(F+T)^N} a = (F+T)^N a.
\end{aligned}$$

Now, let us forget that we fixed a. We thus have shown that $\left[T^N\right](a) = (F+T)^N a$ for every $a \in A$. In other words, (54) holds for $n = N$. This completes the induction step, and thus (54) is proven.

Now, let $M \in \mathbb{F}_q[T]$ and $a \in A$. Write the polynomial M in the form $M = a_0 T^0 + a_1 T^1 + \cdots + a_k T^k$ for some $k \in \mathbb{N}$ and $a_0, a_1, \ldots, a_k \in \mathbb{F}_q$. Thus,

$$M = a_0 T^0 + a_1 T^1 + \cdots + a_k T^k = \sum_{n=0}^{k} a_n T^n.$$

The definition of $[M]$ now yields

$$[M] = a_0 \left[T^0\right] + a_1 \left[T^1\right] + \cdots + a_k \left[T^k\right] = \sum_{n=0}^{k} a_n \left[T^n\right].$$

Recall that Carl is the $\mathbb{F}_q$-algebra homomorphism $\mathbb{F}_q[T] \to \mathcal{F}$ sending T to $F + T$. Thus, $\operatorname{Carl} T = F + T$. The map Carl commutes with applications of polynomials in $\mathbb{F}_q[T]$ (since it is an $\mathbb{F}_q$-algebra homomorphism). Thus,

$$\operatorname{Carl}(M(T)) = M\left(\underbrace{\operatorname{Carl} T}_{=F+T}\right) = M(F+T) = \sum_{n=0}^{k} a_n (F+T)^n$$

(since $M = \sum_{n=0}^{k} a_n T^n$). Since $M(T) = M$, this rewrites as

$$\operatorname{Carl} M = \sum_{n=0}^{k} a_n (F+T)^n .$$

Hence,

$$\begin{aligned}(\operatorname{Carl} M) \cdot a &= \left(\sum_{n=0}^{k} a_n (F+T)^n \right) \cdot a = \sum_{n=0}^{k} a_n \underbrace{(F+T)^n a}_{\substack{=[T^n](a) \\ \text{(by (54))}}} \\ &= \sum_{n=0}^{k} a_n [T^n](a) = \underbrace{\left(\sum_{n=0}^{k} a_n [T^n] \right)}_{=[M]} (a) = [M](a) .\end{aligned}$$

This proves Proposition 3.32. □

Corollary 3.33. Let $M \in \mathbb{F}_q[T]$. Then, the homomorphism $\operatorname{Fqpol} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\lin}$ satisfies $[M] = \operatorname{Fqpol}(\operatorname{Carl} M)$.

Corollary 3.33 yields, in particular, that every $M \in \mathbb{F}_q[T]$ satisfies $[M] = \operatorname{Fqpol}(\operatorname{Carl} M) \in \operatorname{Fqpol} \mathcal{F} \subseteq \mathbb{F}_q[T][X]_{q-\lin}$.

Proof of Corollary 3.33. Let $M \in \mathbb{F}_q[T]$.

Consider the map $\overline{\operatorname{Fqpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]$ defined in Proposition 3.31. This map $\overline{\operatorname{Fqpol}}$ is an $\mathcal{F}$-module homomorphism (according to Proposition 3.31).

The definition of $\overline{\operatorname{Fqpol}}$ shows that $\overline{\operatorname{Fqpol}}(1) = \operatorname{Fqpol}(1) = X$ (since Fqpol is an $\mathbb{F}_q$-algebra homomorphism $\mathcal{F} \to \left(\mathbb{F}_q[T][X]_{q-\lin}, +, \circ\right)$, and since the unity of the $\mathbb{F}_q$-algebra $\left(\mathbb{F}_q[T][X]_{q-\lin}, +, \circ\right)$ is X).

But the definition of $\overline{\operatorname{Fqpol}}$ shows that $\overline{\operatorname{Fqpol}}(\operatorname{Carl} M) = \operatorname{Fqpol}(\operatorname{Carl} M)$, so that

$$\begin{aligned}\operatorname{Fqpol}(\operatorname{Carl} M) &= \overline{\operatorname{Fqpol}} \left(\underbrace{\operatorname{Carl} M}_{=(\operatorname{Carl} M)\cdot 1} \right) = \overline{\operatorname{Fqpol}}((\operatorname{Carl} M) \cdot 1) \\ &= (\operatorname{Carl} M) \cdot \underbrace{\overline{\operatorname{Fqpol}}(1)}_{=X} \\ &\qquad \left(\text{since } \overline{\operatorname{Fqpol}} \text{ is an } \mathcal{F}\text{-module homomorphism} \right) \\ &= (\operatorname{Carl} M) \cdot X. \end{aligned} \tag{57}$$

On the other hand, Proposition 3.32 (applied to $A = \mathbb{F}_q[T][X]$ and $a = X$) yields $[M](X) = (\operatorname{Carl} M) \cdot X$. Comparing this with (57), we obtain $\operatorname{Fqpol}(\operatorname{Carl} M) = [M](X) = [M]$. This proves Corollary 3.33. □

3.8. "Fermat's Little Theorem" for the Carlitz action

Let us first state a simple fact:

Lemma 3.34. Let A be an $\mathbb{F}_q[T]$-algebra which is torsionfree as an $\mathbb{F}_q[T]$-module. Let f be a nonzero element of $\mathbb{F}_q[T]$. Let $\mathbf{u} \in A[X]$ be such that $f\mathbf{u} \in A[X]_{q-\mathrm{lin}}$. Then, $\mathbf{u} \in A[X]_{q-\mathrm{lin}}$.

Proof of Lemma 3.34. We have $f\mathbf{u} \in A[X]_{q-\mathrm{lin}}$. In other words, the polynomial $f\mathbf{u} \in A[X]$ is a q-polynomial, that is, an A-linear combination of the monomials $X^{q^0}, X^{q^1}, X^{q^2}, \ldots$. In other words, for every $k \in \mathbb{N} \setminus \{q^0, q^1, q^2, \ldots\}$, we have

$$\left(\text{the } X^k\text{-coefficient of } f\mathbf{u}\right) = 0. \tag{58}$$

Now, for every $k \in \mathbb{N} \setminus \{q^0, q^1, q^2, \ldots\}$, we have

$$f \cdot \left(\text{the } X^k\text{-coefficient of } \mathbf{u}\right) = \left(\text{the } X^k\text{-coefficient of } f\mathbf{u}\right) = 0$$

(by (58)), and thus $\left(\text{the } X^k\text{-coefficient of } \mathbf{u}\right) = 0$ (because $f \neq 0$, and because A is torsionfree as an $\mathbb{F}_q[T]$-module). In other words, the polynomial $\mathbf{u}$ is an A-linear combination of the monomials $X^{q^0}, X^{q^1}, X^{q^2}, \ldots$. In other words, $\mathbf{u}$ is a q-polynomial; that is, $\mathbf{u} \in A[X]_{q-\mathrm{lin}}$. This proves Lemma 3.34. □

We now shall prove a crucial fact:

Proposition 3.35. Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Then, there exists a unique $u(\pi) \in \mathcal{F}$ such that $\operatorname{Carl}\pi = F^{\deg\pi} + \pi \cdot u(\pi)$. (The notation $u(\pi)$ means that u depends on π; it is not meant to imply that $u(\pi)$ is a polynomial in π.)

The first proof of this proposition will reveal it to be a translation of part of [3, Theorem 2.11]:

First proof of Proposition 3.35. The left $\mathbb{F}_q[T]$-module $\mathcal{F}$ is free (by Proposition 3.5 **(c)**), and thus torsionfree.

From [3, Theorem 2.11], we know that $\overline{[\pi]}(X) = X^{q^{\deg\pi}}$, where $\overline{[\pi]}(X)$ denotes the projection of $[\pi](X) = [\pi] \in \mathbb{F}_q[T][X]$ onto $\left(\mathbb{F}_q[T]/\pi\right)[X]$. In other words, $[\pi](X) \equiv X^{q^{\deg\pi}} \bmod K$, where K is the kernel of the projection $\mathbb{F}_q[T][X] \to \left(\mathbb{F}_q[T]/\pi\right)[X]$. Since this kernel K is simply $\pi\mathbb{F}_q[T][X]$, this rewrites as follows: $[\pi](X) \equiv X^{q^{\deg\pi}} \bmod \pi\mathbb{F}_q[T][X]$.

Thus, $[\pi] = [\pi](X) \equiv X^{q^{\deg\pi}} \bmod \pi\mathbb{F}_q[T][X]$. In other words, $\pi \mid [\pi] - X^{q^{\deg\pi}}$ in the ring $\mathbb{F}_q[T][X]$. Hence, $\dfrac{1}{\pi}\left([\pi] - X^{q^{\deg\pi}}\right)$ is a well-defined polynomial in

the ring $\mathbb{F}_q[T][X]$ (since this ring is an integral domain). Let us denote this polynomial by $\mathbf{u}$.

We have

$$[\pi] = \operatorname{Fqpol}\left(\underbrace{\operatorname{Carl}\pi}_{\in\mathcal{F}}\right) \qquad \text{(by Corollary 3.33, applied to } M=\pi\text{)}$$
$$\in \operatorname{Carl}\mathcal{F} \subseteq \mathbb{F}_q[T][X]_{q-\mathrm{lin}}.$$

But $\mathbf{u} = \dfrac{1}{\pi}\left([\pi] - X^{q^{\deg\pi}}\right)$, so that $\pi\mathbf{u} = [\pi] - X^{q^{\deg\pi}} \in \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ (since both $[\pi]$ and $X^{q^{\deg\pi}}$ belong to $\mathbb{F}_q[T][X]_{q-\mathrm{lin}}$). Therefore, $\mathbf{u} \in \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ (by Lemma 3.34, applied to $A=\mathbb{F}_q[T]$ and $f=\pi$).

Theorem 3.13 **(c)** (applied to $j=0$ and $i=\deg\pi$) yields $\operatorname{Fqpol}\left(T^0F^{\deg\pi}\right) = \underbrace{T^0}_{=1}X^{q^{\deg\pi}} = X^{q^{\deg\pi}}$, so that $X^{q^{\deg\pi}} = \operatorname{Fqpol}\left(\underbrace{T^0}_{=1}F^{\deg\pi}\right) = \operatorname{Fqpol}\left(F^{\deg\pi}\right)$.

Theorem 3.13 **(b)** shows that the map $\operatorname{Fqpol}: \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\mathrm{lin}}$ is an $\mathbb{F}_q$-algebra isomorphism. Thus, its inverse map $\operatorname{Fqpol}^{-1}$ is well-defined. Set $\widetilde{\mathbf{u}} = \operatorname{Fqpol}^{-1}(\mathbf{u})$. Thus, $\widetilde{\mathbf{u}} \in \mathcal{F}$ and $\operatorname{Fqpol}(\widetilde{\mathbf{u}}) = \mathbf{u}$.

But Fqpol is an isomorphism of left $\mathbb{F}_q[T]$-modules (according to Proposition 3.24). Hence,

$$\operatorname{Fqpol}(\pi\widetilde{\mathbf{u}}) = \pi\underbrace{\operatorname{Fqpol}(\widetilde{\mathbf{u}})}_{=\mathbf{u}} = \pi\mathbf{u} = \underbrace{[\pi]}_{\substack{=\operatorname{Fqpol}(\operatorname{Carl}\pi)\\ \text{(by Corollary 3.33,}\\ \text{applied to } M=\pi\text{)}}} - \underbrace{X^{q^{\deg\pi}}}_{=\operatorname{Fqpol}\left(F^{\deg\pi}\right)}$$
$$= \operatorname{Fqpol}(\operatorname{Carl}\pi) - \operatorname{Fqpol}\left(F^{\deg\pi}\right) = \operatorname{Fqpol}\left(\operatorname{Carl}\pi - F^{\deg\pi}\right)$$

(since the map Fqpol is $\mathbb{F}_q$-linear). Since Fqpol is injective (because Fqpol is an isomorphism), this yields $\pi\widetilde{\mathbf{u}} = \operatorname{Carl}\pi - F^{\deg\pi}$.

Hence, there exists at least one $u(\pi) \in \mathcal{F}$ such that $\pi\cdot u(\pi) = \operatorname{Carl}\pi - F^{\deg\pi}$ (namely, $u(\pi) = \widetilde{\mathbf{u}}$). Moreover, such a $u(\pi)$ is clearly unique (because any element $u(\pi) \in \mathcal{F}$ is uniquely determined by $\pi\cdot u(\pi)$ (since $\pi \neq 0$, and since the left $\mathbb{F}_q[T]$-module $\mathcal{F}$ is torsionfree)). Thus, there exists a **unique** $u(\pi) \in \mathcal{F}$ such that $\pi\cdot u(\pi) = \operatorname{Carl}\pi - F^{\deg\pi}$. In other words, there exists a **unique** $u(\pi) \in \mathcal{F}$ such that $\operatorname{Carl}\pi = F^{\deg\pi} + \pi\cdot u(\pi)$. This proves Proposition 3.35. □

3.9. A second proof of Proposition 3.35

Let us next give another proof of Proposition 3.35, which does not rely on Carlitz polynomials. This proof is not directly relevant for the rest of this report, but illustrates some techniques of working with $\mathcal{F}$.

We first state a classical fact:

Proposition 3.36. Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Let $d = \deg \pi$.

Let $\mathbb{F}_\pi$ denote the field $\mathbb{F}_q[T]/\pi\mathbb{F}_q[T]$. This is a field extension of $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_\pi$ be the residue class of $T \in \mathbb{F}_q[T]$ modulo the ideal $\pi\mathbb{F}_q[T]$. Thus, $\mathbb{F}_\pi = \mathbb{F}[\alpha]$ and $\pi(\alpha) = 0$.

(a) The $\mathbb{F}_q$-vector space $\mathbb{F}_\pi$ has basis $\left(\alpha^0, \alpha^1, \ldots, \alpha^{d-1}\right)$.

(b) The elements $\alpha^{q^0}, \alpha^{q^1}, \ldots, \alpha^{q^{d-1}}$ are pairwise distinct and are precisely the roots of π.

(c) We have

$$\pi = \prod_{k=0}^{d-1} \left(T - \alpha^{q^k}\right) \qquad \text{in } \mathbb{F}_\pi[T]. \tag{59}$$

Proof of Proposition 3.36. **(a)** This is well-known (and holds for any commutative ring instead of $\mathbb{F}_q$).

(c) Recall that Frob_A is an $\mathbb{F}_q$-algebra endomorphism of A whenever A is a commutative $\mathbb{F}_q$-algebra. Applying this to $A = \mathbb{F}_\pi$, we conclude that $\mathrm{Frob}_{\mathbb{F}_\pi}$ is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_\pi$. Denote this $\mathbb{F}_q$-algebra endomorphism by f. Thus, $f = \mathrm{Frob}_{\mathbb{F}_\pi}$.

We have $f = \mathrm{Frob}_{\mathbb{F}_\pi}$, and thus

$$f(a) = \mathrm{Frob}_{\mathbb{F}_\pi}(a) = a^q \qquad \text{(by the definition of } \mathrm{Frob}_{\mathbb{F}_\pi}\text{)} \tag{60}$$

for every $a \in \mathbb{F}_\pi$. Now,

$$f^k(a) = a^{q^k} \qquad \text{for every } k \in \mathbb{N} \text{ and } a \in \mathbb{F}_\pi. \tag{61}$$

(Indeed, this can be proven by a straightforward induction on k, using (60).)

But $\mathbb{F}_\pi = \mathbb{F}_q[T]/\pi\mathbb{F}_q[T]$ is an $\mathbb{F}_q$-vector space of dimension $\deg \pi = d$. Hence, $|\mathbb{F}_\pi| = \left|\mathbb{F}_q\right|^d = q^d$ (since $\left|\mathbb{F}_q\right| = q$). But it is well-known that if L is a finite field, then every $a \in L$ satisfies $a^{|L|} = a$. Applying this to $L = \mathbb{F}_\pi$, we conclude that every $a \in \mathbb{F}_\pi$ satisfies $a^{|\mathbb{F}_\pi|} = a$. Hence,

$$f^d = \mathrm{id} \tag{62}$$

[32]. Thus, $\mathrm{id} = f^d = f^{d-1} \circ f$. Hence, the map f is left-invertible, and thus injective.

[32] *Proof of (62):* We have just shown that every $a \in \mathbb{F}_\pi$ satisfies $a^{|\mathbb{F}_\pi|} = a$. Now, every $a \in \mathbb{F}_\pi$ satisfies

$$\begin{aligned} f^d(a) &= a^{q^d} && \text{(by (61), applied to } k = d\text{)} \\ &= a^{|\mathbb{F}_\pi|} && \left(\text{since } q^d = |\mathbb{F}_\pi|\right) \\ &= a = \mathrm{id}(a). \end{aligned}$$

In other words, $f^d = \mathrm{id}$. Qed.

Every nonzero polynomial $g \in \mathbb{F}_q[T]$ has at most $\deg g$ roots (since $\mathbb{F}_q$ is a field). Applying this to $g = \pi$, we conclude that the polynomial π has at most $\deg \pi = d$ roots.

Now, we notice that

$$\pi\left(\alpha^{q^k}\right) = 0 \text{ for each } k \in \{0, 1, \ldots, d-1\} \tag{63}$$

[33]. Also,

$$\alpha^{q^k} \neq \alpha \qquad \text{for each } k \in \{1, 2, \ldots, d-1\} \tag{64}$$

[34]. Hence,

$$\text{the elements } \alpha^{q^0}, \alpha^{q^1}, \ldots, \alpha^{q^{d-1}} \text{ are pairwise distinct} \tag{65}$$

[33] *Proof of (63):* Let $k \in \{0, 1, \ldots, d-1\}$. Then, (61) (applied to $a = \alpha$) yields $f^k(\alpha) = \alpha^{q^k}$.

Recall that f is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_\pi$. Thus, f^k is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_\pi$ as well. Hence, f^k commutes with polynomials in $\mathbb{F}_q[T]$. In other words, $f^k(g(\beta)) = g\left(f^k(\beta)\right)$ for every $g \in \mathbb{F}_q[T]$ and every $\beta \in \mathbb{F}_\pi$. Applying this to $g = \pi$ and $\beta = \alpha$, we obtain $f^k(\pi(\alpha)) = \pi\left(\underbrace{f^k(\alpha)}_{=\alpha^{q^k}}\right) = \pi\left(\alpha^{q^k}\right)$. Hence, $\pi\left(\alpha^{q^k}\right) = f^k\left(\underbrace{\pi(\alpha)}_{=0}\right) = f^k(0) = 0$ (since f^k is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_\pi$). This proves (63).

[34] *Proof of (64):* Let $k \in \{1, 2, \ldots, d-1\}$. We shall show that $\alpha^{q^k} \neq \alpha$.

Indeed, assume the contrary. Thus, $\alpha^{q^k} = \alpha$. But (61) (applied to $a = \alpha$) yields $f^k(\alpha) = \alpha^{q^k} = \alpha$.

Let $x \in \mathbb{F}_\pi$. We are going to show that $x^{q^k} - x = 0$.

Indeed, $x \in \mathbb{F}_\pi = \mathbb{F}_q[\alpha]$. Hence, $x = h(\alpha)$ for some polynomial $h \in \mathbb{F}_q[T]$. Consider this h.

Recall that f is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_\pi$. Thus, f^k is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_\pi$ as well. Hence, f^k commutes with polynomials in $\mathbb{F}_q[T]$. In other words, $f^k(g(\beta)) = g\left(f^k(\beta)\right)$ for every $g \in \mathbb{F}_q[T]$ and every $\beta \in \mathbb{F}_\pi$. Applying this to $g = h$ and $\beta = \alpha$, we obtain $f^k(h(\alpha)) = h\left(\underbrace{f^k(\alpha)}_{=\alpha}\right) = h(\alpha)$. Since $x = h(\alpha)$, this rewrites as $f^k(x) = x$. But (61) (applied to $a = x$) yields $f^k(x) = x^{q^k}$. Hence, $x^{q^k} = f^k(x) = x$, so that $x^{q^k} - x = 0$.

Now, forget that we fixed x. We thus have proven that every $x \in \mathbb{F}_\pi$ satisfies $x^{q^k} - x = 0$. In other words, every $x \in \mathbb{F}_\pi$ is a root of the polynomial $T^{q^k} - T \in \mathbb{F}_q[T]$. Hence, the polynomial $T^{q^k} - T$ has at least $|\mathbb{F}_\pi|$ roots. Since $|\mathbb{F}_\pi| = q^d > q^k$ (since $d > k$ (because $k \in \{1, 2, \ldots, d-1\}$)), this shows that the polynomial $T^{q^k} - T$ has $> q^k$ roots.

But $k > 0$, so that the polynomial $T^{q^k} - T$ is a nonzero polynomial of degree $\deg\left(T^{q^k} - T\right) = q^k$. It is well-known that each nonzero polynomial $w \in \mathbb{F}_q[T]$ has at most $\deg w$ roots (since $\mathbb{F}_q$ is a field). Applying this to $w = T^{q^k} - T$, we conclude that the polynomial $T^{q^k} - T$ has at most $\deg\left(T^{q^k} - T\right) = q^k$ roots. This contradicts the fact that the polynomial $T^{q^k} - T$ has $> q^k$ roots. This contradiction shows that our assumption was false. Hence, $\alpha^{q^k} \neq \alpha$ is proven, qed.

[35].

Let γ be the polynomial

$$\pi - \prod_{k=0}^{d-1} \left(T - \alpha^{q^k} \right) \in \mathbb{F}_\pi [T] .$$

The polynomial π is monic and has degree $\deg \pi = d$. The polynomial $\prod_{k=0}^{d-1} \left(T - \alpha^{q^k} \right)$ is also obviously a monic polynomial of degree d (since it is a product of d monic polynomials of degree 1). Thus, γ is a difference of two monic polynomials of degree d (since $\gamma = \pi - \prod_{k=0}^{d-1} \left(T - \alpha^{q^k} \right)$). Consequently, γ is a polynomial of degree $< d$ (because the difference of two monic polynomials of degree d must always be a polynomial of degree $< d$). In other words, $\deg \gamma < d$.

Assume (for the sake of contradiction) that $\gamma \neq 0$.

Every nonzero polynomial $g \in \mathbb{F}_\pi [T]$ has at most $\deg g$ roots (since $\mathbb{F}_\pi$ is a field). Applying this to $g = \gamma$, we conclude that γ has at most $\deg \gamma$ roots (since $\gamma \neq 0$). Thus, γ has $< d$ roots (since $\deg \gamma < d$).

But for every $\ell \in \{0, 1, \ldots, d-1\}$, the element α^{q^ℓ} of $\mathbb{F}_\pi$ is a root of γ [36]. In other words, $\alpha^{q^0}, \alpha^{q^1}, \ldots, \alpha^{q^{d-1}}$ are d roots of γ. These d roots are pairwise distinct (by (65)). Thus, the polynomial γ has at least d roots. This contradicts the fact

[35] *Proof of (65):* Assume the contrary. Thus, two of the elements $\alpha^{q^0}, \alpha^{q^1}, \ldots, \alpha^{q^{d-1}}$ are equal. In other words, there exist two elements i and j of $\{0, 1, \ldots, d-1\}$ satisfying $i < j$ and $\alpha^{q^i} = \alpha^{q^j}$. Consider these i and j.

We have $j - i \in \{1, 2, \ldots, d-1\}$ (since i and j belong to $\{0, 1, \ldots, d-1\}$ and satisfy $i < j$). Hence, (64) (applied to $k = j - i$) yields $\alpha^{q^{j-i}} \neq \alpha$. But (61) (applied to $a = \alpha$ and $k = j - i$) yields $f^{j-i}(\alpha) = \alpha^{q^{j-i}} \neq \alpha$.

Applying (61) to $a = \alpha$ and $k = i$, we obtain $f^i(\alpha) = \alpha^{q^i}$. Applying (61) to $a = \alpha$ and $k = j$, we obtain $f^j(\alpha) = \alpha^{q^j}$. Thus, $\alpha^{q^j} = \underbrace{f^j}_{\substack{= f^i \circ f^{j-i} \\ \text{(since } i<j\text{)}}} (\alpha) = \left(f^i \circ f^{j-i} \right)(\alpha) = f^i \left(f^{j-i}(\alpha) \right)$.

Now, $f^i(\alpha) = \alpha^{q^i} = \alpha^{q^j} = f^i \left(f^{j-i}(\alpha) \right)$. Since the map f^i is injective (because f is injective), this entails $\alpha = f^{j-i}(\alpha) \neq \alpha$. This is clearly absurd. This contradiction proves that our assumption was false. Hence, (65) is proven.

[36] *Proof.* Let $\ell \in \{0, 1, \ldots, d-1\}$. From $\gamma = \pi - \prod_{k=0}^{d-1} \left(T - \alpha^{q^k} \right)$, we obtain

$$\gamma \left(\alpha^{q^\ell} \right) = \underbrace{\pi \left(\alpha^{q^\ell} \right)}_{\substack{=0 \\ \text{(by (63),} \\ \text{applied to } k=\ell\text{)}}} - \underbrace{\prod_{k=0}^{d-1} \left(\alpha^{q^\ell} - \alpha^{q^k} \right)}_{\substack{=0 \\ \text{(because one of the factors in this product is } \alpha^{q^\ell} - \alpha^{q^\ell} \\ \text{(namely, the factor for } k=\ell\text{), and this factor is clearly } 0\text{)}}} = 0 - 0 = 0.$$

In other words, the element α^{q^ℓ} of $\mathbb{F}_\pi$ is a root of γ. Qed.

that γ has $< d$ roots. This contradiction proves that our assumption (that $\gamma \neq 0$) was false. Hence, we have $\gamma = 0$. Thus, $0 = \gamma = \pi - \prod_{k=0}^{d-1} \left(T - \alpha^{q^k}\right)$, so that $\pi = \prod_{k=0}^{d-1} \left(T - \alpha^{q^k}\right)$. This proves Proposition 3.36 **(c)**.

(b) The elements $\alpha^{q^0}, \alpha^{q^1}, \ldots, \alpha^{q^{d-1}}$ are pairwise distinct (by (65)) and are precisely the roots of π (because of (59)). This proves Proposition 3.36 **(b)**. □

Here are some more useful lemmas:

Lemma 3.37. Let $\mathbb{K}$ be a commutative ring. Let $d \in \mathbb{N}$. Let $\pi \in \mathbb{K}[T]$ be a polynomial of degree $\leq d$. For each $i \in \mathbb{N}$, let π_i be the coefficient of T^i in π. For each $k \in \{0, 1, \ldots, d\}$, define a polynomial $p_k \in \mathbb{K}[T]$ by $p_k = \sum_{i=k+1}^{d} \pi_i T^{i-1-k}$. Then:

(a) We have $p_{d-1} = \pi_d$ (a constant polynomial) and $p_d = 0$.

(b) We have $\pi(X) - \pi(Y) = (X - Y) \sum_{i=0}^{d-1} p_i(X) Y^i$ in the ring $\mathbb{K}[X, Y]$.

Proof of Lemma 3.37. The definition of p_{d-1} yields

$$p_{d-1} = \sum_{i=(d-1)+1}^{d} \pi_i T^{i-1-(d-1)} = \sum_{i=d}^{d} \pi_i T^{i-1-(d-1)} = \pi_d \underbrace{T^{d-1-(d-1)}}_{=T^0=1} = \pi_d.$$

The definition of p_d yields

$$p_d = \sum_{i=d+1}^{d} \pi_i T^{i-1-d} = (\text{empty sum}) = 0.$$

This proves Lemma 3.37 **(a)**.

For every $i \in \{0, 1, \ldots, d\}$, we have

$$X^i - Y^i = (X - Y) \underbrace{\sum_{k=0}^{i-1} X^k Y^{i-1-k}}_{\substack{= \sum_{\ell=0}^{i-1} X^{i-1-\ell} Y^\ell \\ \text{(here, we have substituted } \ell \\ \text{for } i-1-k \text{ in the sum)}}} \qquad \text{(by a known formula)}$$

$$= (X - Y) \sum_{\ell=0}^{i-1} X^{i-1-\ell} Y^\ell. \tag{66}$$

We have $\pi = \sum_{i=0}^{d} \pi_i T^i$ (since π is a polynomial of degree $\leq d$, and since the π_i are its coefficients). Thus, $\pi(X) = \sum_{i=0}^{d} \pi_i X^i$ and $\pi(Y) = \sum_{i=0}^{d} \pi_i Y^i$. Hence,

$$\begin{aligned}
\pi(X) - \pi(Y) &= \sum_{i=0}^{d} \pi_i X^i - \sum_{i=0}^{d} \pi_i Y^i \\
&= \sum_{i=0}^{d} \pi_i \underbrace{\left(X^i - Y^i\right)}_{\substack{=(X-Y)\sum_{\ell=0}^{i-1} X^{i-1-\ell}Y^\ell \\ \text{(by (66))}}} = \sum_{i=0}^{d} \pi_i \cdot (X-Y) \sum_{\ell=0}^{i-1} X^{i-1-\ell}Y^\ell \\
&= (X-Y) \sum_{i=0}^{d} \pi_i \sum_{\ell=0}^{i-1} X^{i-1-\ell}Y^\ell.
\end{aligned}$$

Since

$$\begin{aligned}
\sum_{i=0}^{d} \pi_i \sum_{\ell=0}^{i-1} X^{i-1-\ell}Y^\ell &= \underbrace{\sum_{i=0}^{d}\sum_{\ell=0}^{i-1}}_{=\sum_{\ell=0}^{d}\sum_{i=\ell+1}^{d}} \pi_i X^{i-1-\ell}Y^\ell = \sum_{\ell=0}^{d} \underbrace{\sum_{i=\ell+1}^{d} \pi_i X^{i-1-\ell}}_{\substack{=p_\ell(X) \\ \text{(since } p_\ell = \sum_{i=\ell+1}^{d} \pi_i T^{i-1-\ell} \\ \text{(by the definition of } p_\ell\text{) and thus} \\ p_\ell(X) = \sum_{i=\ell+1}^{d} \pi_i X^{i-1-\ell}\text{)}}} Y^\ell \\
&= \sum_{\ell=0}^{d} p_\ell(X) Y^\ell = \sum_{\ell=0}^{d-1} p_\ell(X) Y^\ell + \underbrace{p_d(X)}_{\substack{=0 \\ \text{(since } p_d = 0\text{)}}} Y^d \\
&= \sum_{\ell=0}^{d-1} p_\ell(X) Y^\ell = \sum_{i=0}^{d-1} p_i(X) Y^i \\
&\qquad \left(\text{here, we have renamed the summation index } \ell \text{ as } i\right),
\end{aligned}$$

this rewrites as $\pi(X) - \pi(Y) = (X-Y) \sum_{i=0}^{d-1} p_i(X) Y^i$. This proves Lemma 3.37 **(b)**. □

Lemma 3.38. Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Let $d = \deg \pi$.

Let $\mathbb{F}_\pi$ denote the field $\mathbb{F}_q[T]/\pi\mathbb{F}_q[T]$. This is a field extension of $\mathbb{F}_q$. Let $\alpha \in \mathbb{F}_\pi$ be the residue class of $T \in \mathbb{F}_q[T]$ modulo the ideal $\pi\mathbb{F}_q[T]$. Thus, $\mathbb{F}_\pi = \mathbb{F}[\alpha]$ and $\pi(\alpha) = 0$. Let $\mathcal{F}_\pi$ denote the $\mathbb{F}_\pi$-algebra $\mathbb{F}_\pi \otimes \mathcal{F}$ (where $\mathbb{F}_\pi$ acts on the first tensorand).

Let $h \in \mathcal{F}$ be such that $1 \otimes h \in (1 \otimes T - \alpha)\mathcal{F}_\pi$. (Notice that the α here really means the element $\alpha 1_{\mathcal{F}_\pi} = \alpha \otimes 1$ of $\mathcal{F}_\pi$.) Then, $h \in \pi\mathcal{F}$.

Remark 3.39. Lemma 3.38 can be viewed as a noncommutative version of the following known fact: If $h \in \mathbb{F}_q[T]$ is such that $h \in (T-\alpha)\,\mathbb{F}_\pi[T]$, then $h \in \pi\mathbb{F}_q[T]$. (That is, a polynomial in $\mathbb{F}_q[T]$ that vanishes at α must be a multiple of π.)

Proof of Lemma 3.38. For each $i \in \mathbb{N}$, let π_i be the coefficient of T^i in π. For each $k \in \{0,1,\ldots,d\}$, define a polynomial $p_k \in \mathbb{F}_q[T]$ by $p_k = \sum_{i=k+1}^{d} \pi_i T^{i-1-k}$. Then, Lemma 3.37 **(a)** (applied to $\mathbb{K} = \mathbb{F}_q$) yields that $p_{d-1} = \pi_d$ (a constant polynomial) and $p_d = 0$. But $\pi_d = 1$ (since π is a monic polynomial of degree d). Thus, $p_{d-1} = \pi_d = 1$.

Furthermore, Lemma 3.37 **(b)** (applied to $\mathbb{K} = \mathbb{F}_q$) yields

$$\pi(X) - \pi(Y) = (X-Y)\sum_{i=0}^{d-1} p_i(X)\,Y^i = \left(\sum_{i=0}^{d-1} p_i(X)\,Y^i\right)(X-Y)$$

in the ring $\mathbb{K}[X,Y]$. Since the two elements $1\otimes T$ and α of $\mathcal{F}_\pi$ commute with each other, we can substitute $1\otimes T$ and α for X and Y in this identity. We thus obtain

$$\begin{aligned}
\pi(1\otimes T) - \pi(\alpha) &= \left(\sum_{i=0}^{d-1} \underbrace{p_i(1\otimes T)}_{\substack{=1\otimes p_i(T)=1\otimes p_i \\ \text{(since } p_i(T)=p_i\text{)}}} \underbrace{\alpha^i}_{\substack{=\alpha^i\otimes 1 \\ \text{(since } \alpha^i\in\mathbb{F}_\pi\text{)}}}\right)(1\otimes T-\alpha) \\
&= \left(\sum_{i=0}^{d-1} \underbrace{(1\otimes p_i)\left(\alpha^i\otimes 1\right)}_{=\alpha^i\otimes p_i}\right)(1\otimes T-\alpha) \\
&= \left(\sum_{i=0}^{d-1} \alpha^i\otimes p_i\right)(1\otimes T-\alpha)
\end{aligned}$$

in the ring $\mathcal{F}_\pi = \mathbb{F}_\pi\otimes\mathcal{F}$. Since $\pi(1\otimes T) - \underbrace{\pi(\alpha)}_{=0} = \pi(1\otimes T) = 1\otimes\underbrace{\pi(T)}_{=\pi} = 1\otimes\pi$, this rewrites as

$$1\otimes\pi = \left(\sum_{i=0}^{d-1}\alpha^i\otimes p_i\right)(1\otimes T-\alpha). \tag{67}$$

Now,

$$\begin{aligned}
&\sum_{i=0}^{d-1} \underbrace{\alpha^i \otimes p_i h}_{=\left(\alpha^i \otimes p_i\right)(1\otimes h)} \\
&= \sum_{i=0}^{d-1} \left(\alpha^i \otimes p_i\right)(1\otimes h) = \left(\sum_{i=0}^{d-1} \alpha^i \otimes p_i\right) \underbrace{(1\otimes h)}_{\in (1\otimes T-\alpha)\mathcal{F}_\pi} \\
&\in \underbrace{\left(\sum_{i=0}^{d-1} \alpha^i \otimes p_i\right)(1\otimes T-\alpha)\,\mathcal{F}_\pi}_{\substack{=1\otimes\pi \\ \text{(by (67))}}} = (1\otimes\pi)\,\mathcal{F}_\pi. \qquad (68)
\end{aligned}$$

But Proposition 3.36 **(a)** shows that the $\mathbb{F}_q$-vector space $\mathbb{F}_\pi$ has basis $\left(\alpha^0, \alpha^1, \ldots, \alpha^{d-1}\right)$. Hence, we can define an $\mathbb{F}_q$-linear map $\lambda : \mathbb{F}_\pi \to \mathbb{F}_q$ by

$$\left(\lambda\left(\alpha^i\right) = \delta_{i,d-1} \qquad \text{for each } i \in \{0,1,\ldots,d-1\}\right). \qquad (69)$$

Consider this λ. The $\mathbb{F}_q$-linear map $\lambda : \mathbb{F}_\pi \to \mathbb{F}_q$ induces an $\mathbb{F}_q$-linear map $\lambda \otimes \mathrm{id}_\mathcal{F} : \mathbb{F}_\pi \otimes \mathcal{F} \to \mathbb{F}_q \otimes \mathcal{F}$. In view of $\mathbb{F}_\pi \otimes \mathcal{F} = \mathcal{F}_\pi$ and $\mathbb{F}_q \otimes \mathcal{F} = \mathcal{F}$, this latter map is thus an $\mathbb{F}_q$-linear map $\lambda \otimes \mathrm{id}_\mathcal{F} : \mathcal{F}_\pi \to \mathcal{F}$. This map satisfies

$$(\lambda \otimes \mathrm{id}_\mathcal{F})\left((1\otimes\pi)\,\mathcal{F}_\pi\right) \subseteq \pi\mathcal{F} \qquad (70)$$

[37]. Now, applying the map $\lambda \otimes \mathrm{id}_\mathcal{F}$ to both sides of the equality (68), we obtain

$$(\lambda \otimes \mathrm{id}_\mathcal{F})\left(\sum_{i=0}^{d-1} \alpha^i \otimes p_i h\right) \in (\lambda \otimes \mathrm{id}_\mathcal{F})\left((1\otimes\pi)\,\mathcal{F}_\pi\right) \subseteq \pi\mathcal{F}$$

[37] *Proof of (70):* We have

$$\begin{aligned}
&(\lambda \otimes \mathrm{id}_\mathcal{F})\left((1\otimes\pi)\ \underbrace{\mathcal{F}_\pi}_{=\mathbb{F}_\pi\otimes\mathcal{F}}\right) \\
&= (\lambda \otimes \mathrm{id}_\mathcal{F})\ \underbrace{\left((1\otimes\pi)\left(\mathbb{F}_\pi \otimes \mathcal{F}\right)\right)}_{\substack{=\mathbb{F}_\pi\otimes\pi\mathcal{F} \\ \text{(seen as a subspace of } \mathbb{F}_\pi\otimes\mathcal{F})}} = (\lambda \otimes \mathrm{id}_\mathcal{F})\left(\mathbb{F}_\pi \otimes \pi\mathcal{F}\right) \\
&= \underbrace{\lambda\left(\mathbb{F}_\pi\right)}_{\subseteq\mathbb{F}_q} \otimes \underbrace{\mathrm{id}_\mathcal{F}\left(\pi\mathcal{F}\right)}_{=\pi\mathcal{F}} \qquad \left(\text{seen as a subspace of } \mathbb{F}_q \otimes \mathcal{F}\right) \\
&\subseteq \mathbb{F}_q \otimes \pi\mathcal{F} = \pi\mathcal{F} \qquad \left(\text{using our identification of } \mathbb{F}_q \otimes \mathcal{F} \text{ with } \mathcal{F}\right),
\end{aligned}$$

qed.

(by (70)). Since

$$
\begin{aligned}
&(\lambda \otimes \mathrm{id}_{\mathcal{F}}) \left(\sum_{i=0}^{d-1} \alpha^i \otimes p_i h \right) \\
&= \sum_{i=0}^{d-1} \underbrace{\lambda\left(\alpha^i\right)}_{\substack{=\delta_{i,d-1} \\ \text{(by (69))}}} \otimes \underbrace{\mathrm{id}_{\mathcal{F}}\left(p_i h\right)}_{=p_i h} = \sum_{i=0}^{d-1} \delta_{i,d-1} \otimes p_i h \\
&= \sum_{i=0}^{d-1} \delta_{i,d-1} p_i h \qquad \left(\text{using our identification of } \mathbb{F}_q \otimes \mathcal{F} \text{ with } \mathcal{F}\right) \\
&= \sum_{i=0}^{d-2} \underbrace{\delta_{i,d-1}}_{\substack{=0 \\ (\text{since } i \neq d-1 \\ (\text{since } i \leq d-2))}} p_i h + \underbrace{\delta_{d-1,d-1}}_{=1} \underbrace{p_{d-1}}_{=1} h = \underbrace{\sum_{i=0}^{d-2} 0 p_i h}_{=0} + h = h,
\end{aligned}
$$

this rewrites as $h \in \pi\mathcal{F}$. This proves Lemma 3.38. □

Lemma 3.40. Let R be a ring (not necessarily commutative). If $b_0, b_1, \ldots, b_{d-1}$ are some elements of R (for some $d \in \mathbb{N}$), then the product $\prod_{k=0}^{d-1} b_k$ shall be defined as $b_0 b_1 \cdots b_{d-1}$. (Thus, we have defined this product even if the elements $b_0, b_1, \ldots, b_{d-1}$ do not commute.)

Let $r \in \mathbb{N}$. Let f, t and a be three elements of R satisfying $ft = t^r f$, $fa = af$ and $ta = at$. Let $d \in \mathbb{N}$. Then, every $d \in \mathbb{N}$ satisfies

$$
\prod_{k=0}^{d-1} \left(f + t - a^{r^k} \right) \equiv f^d \bmod (t-a) R. \tag{71}
$$

(Note that $(t-a)R$ is only a right ideal of R, not necessarily an ideal of R.)

Proof of Lemma 3.40. We have

$$
f^i t = t^{r^i} f^i \qquad \text{for every } i \in \mathbb{N}. \tag{72}
$$

(This can be proven by a straightforward induction on i, using the relation $ft = t^r f$.) Also, the relation $fa = af$ shows that the $\mathbb{Z}$-subalgebra of R generated by a and f is commutative. Thus, every $i \in \mathbb{N}$ and $j \in \mathbb{N}$ satisfy

$$
f^i a^j = a^j f^i \tag{73}
$$

(since both f^i and a^j belong to this commutative $\mathbb{Z}$-subalgebra).

Moreover, every $i \in \mathbb{N}$ satisfies

$$
t^i - a^i \equiv 0 \bmod (t-a) R \tag{74}
$$

[38].

We shall prove (71) by induction over d:

Induction base: For $d = 0$, the congruence (71) is obviously true (because both sides of this congruence equal 1). This completes the induction base.

Induction step: Let $D \in \mathbb{N}$. Assume that (71) holds for $d = D$. We must prove that (71) holds for $d = D + 1$.

We have assumed that (71) holds for $d = D$. In other words,

$$\prod_{k=0}^{D-1} \left(f + t - a^{r^k} \right) \equiv f^D \bmod (t-a) R. \tag{75}$$

Now,

$$\begin{aligned}
\prod_{k=0}^{D} \left(f + t - a^{r^k} \right) &= \underbrace{\left(\prod_{k=0}^{D-1} \left(f + t - a^{r^k} \right) \right)}_{\substack{\equiv f^D \bmod (t-a) R \\ \text{(by (75))}}} \left(f + t - a^{r^D} \right) \\
&\equiv f^D \left(f + t - a^{r^D} \right) = \underbrace{f^D f}_{= f^{D+1}} + \underbrace{f^D t}_{\substack{= t^{r^D} f^D \\ \text{(by (72), applied to } i=D\text{)}}} - \underbrace{f^D a^{r^D}}_{\substack{= a^{r^D} f^D \\ \text{(by (73), applied to } i=D \text{ and } j=r^D\text{)}}} \\
&= f^{D+1} + \underbrace{t^{r^D} f^D - a^{r^D} f^D}_{= \left(t^{r^D} - a^{r^D} \right) f^D} = f^{D+1} + \underbrace{\left(t^{r^D} - a^{r^D} \right)}_{\substack{\equiv 0 \bmod (t-a) R \\ \text{(by (74), applied to } i=r^D\text{)}}} f^D \\
&\equiv f^{D+1} \bmod (t-a) R.
\end{aligned}$$

In other words, (71) holds for $d = D + 1$. This completes the induction step. Hence, (71) is proven by induction. In other words, Lemma 3.40 is proven. □

Now we can prove Proposition 3.35 again:

Second proof of Proposition 3.35. The left $\mathbb{F}_q[T]$-module $\mathcal{F}$ is free (by Proposition 3.5 **(c)**), and thus torsionfree.

---

[38] *Proof of (74):* Let $i \in \mathbb{N}$. Then, a known formula shows that $X^i - Y^i = (X - Y) \sum_{k=0}^{i-1} X^k Y^{i-1-k}$ in the polynomial ring $\mathbb{Z}[X, Y]$. Since the elements t and a of R commute (because $ta = at$), we can substitute t and a for X and Y in this formula. We thus obtain

$$t^i - a^i = (t-a) \underbrace{\sum_{k=0}^{i-1} t^k a^{i-1-k}}_{\in R} \in (t-a) R.$$

In other words, $t^i - a^i \equiv 0 \bmod (t-a) R$. This proves (74).

Define d, $\mathbb{F}_\pi$, α and $\mathcal{F}_\pi$ as in Lemma 3.38. Define $h \in \mathcal{F}$ by $h = \operatorname{Carl}\pi - F^{\deg\pi}$. We shall show that $h \in \pi\mathcal{F}$.

Recall that Carl is the $\mathbb{F}_q$-algebra homomorphism $\mathbb{F}_q[T] \to \mathcal{F}$ sending T to $F+T$. This homomorphism sends every polynomial $g \in \mathbb{F}_q[T]$ to $g(F+T)$ (where $g(F+T)$ denotes the result of substituting $F+T$ for T in g, not the product of g with $F+T$). In other words, $\operatorname{Carl} g = g(F+T)$ for every $g \in \mathbb{F}_q[T]$. Applying this to $g = \pi$, we obtain $\operatorname{Carl}\pi = \pi(F+T)$.

Now, we can substitute $1\otimes F + 1\otimes T \in \mathcal{F}_\pi$ for T in the equality (59) (since $1\otimes F + 1\otimes T$ is an element of the $\mathbb{F}_\pi$-algebra $\mathcal{F}_\pi$). As a result, we obtain

$$\pi(1\otimes F + 1\otimes T) = \prod_{k=0}^{d-1}\left(1\otimes F + 1\otimes T - \alpha^{q^k}\right). \tag{76}$$

But the elements $1\otimes F$, $1\otimes T$ and α of $\mathcal{F}_\pi$ satisfy

$$\begin{aligned}
(1\otimes F)(1\otimes T) &= 1\otimes \underbrace{FT}_{=T^qF} = 1\otimes T^qF = (1\otimes T)^q(1\otimes F), \\
(1\otimes F)\alpha &= \alpha(1\otimes F) \qquad (\text{since } \alpha \text{ really means } \alpha\otimes 1 \in \mathcal{F}_\pi), \\
(1\otimes T)\alpha &= \alpha(1\otimes T) \qquad (\text{since } \alpha \text{ really means } \alpha\otimes 1 \in \mathcal{F}_\pi).
\end{aligned}$$

Hence, Lemma 3.40 (applied to $R = \mathcal{F}_\pi$, $r = q$, $f = 1\otimes F$, $t = 1\otimes T$ and $a = \alpha$) yields

$$\prod_{k=0}^{d-1}\left(1\otimes F + 1\otimes T - \alpha^{q^k}\right) \equiv (1\otimes F)^d = 1\otimes F^d \bmod (1\otimes T - \alpha)\mathcal{F}_\pi.$$

Hence, (76) becomes

$$\begin{aligned}
\pi(1\otimes F + 1\otimes T) &= \prod_{k=0}^{d-1}\left(1\otimes F + 1\otimes T - \alpha^{q^k}\right) \\
&\equiv 1\otimes F^d \bmod (1\otimes T - \alpha)\mathcal{F}_\pi.
\end{aligned}$$

Since

$$\pi\left(\underbrace{1\otimes F + 1\otimes T}_{=1\otimes(F+T)}\right) = \pi(1\otimes(F+T)) = 1\otimes\pi(F+T),$$

this rewrites as

$$1\otimes\pi(F+T) \equiv 1\otimes F^d \bmod (1\otimes T - \alpha)\mathcal{F}_\pi. \tag{77}$$

Now, $h = \underbrace{\operatorname{Carl}\pi}_{=\pi(F+T)} - \underbrace{F^{\deg\pi}}_{\substack{=F^d \\ (\text{since } \deg\pi = d)}} = \pi(F+T) - F^d$, so that

$$1\otimes h = 1\otimes\left(\pi(F+T) - F^d\right) = 1\otimes\pi(F+T) - 1\otimes F^d \in (1\otimes T - \alpha)\mathcal{F}_\pi$$

(by (77)). Hence, Lemma 3.38 shows that $h \in \pi\mathcal{F}$. Hence, there exists at least one $u(\pi) \in \mathcal{F}$ such that $\pi \cdot u(\pi) = h$. Moreover, such a $u(\pi)$ is clearly unique (because any element $u(\pi) \in \mathcal{F}$ is uniquely determined by $\pi \cdot u(\pi)$ (since $\pi \neq 0$, and since the left $\mathbb{F}_q[T]$-module $\mathcal{F}$ is torsionfree)). Thus, there exists a **unique** $u(\pi) \in \mathcal{F}$ such that $\pi \cdot u(\pi) = h$. In other words, there exists a **unique** $u(\pi) \in \mathcal{F}$ such that $\operatorname{Carl}\pi = F^{\deg\pi} + \pi \cdot u(\pi)$ (because we have the logical equivalence

$$\left(\pi \cdot u(\pi) = \underbrace{h}_{=\operatorname{Carl}\pi - F^{\deg\pi}}\right) \iff \left(\pi \cdot u(\pi) = \operatorname{Carl}\pi - F^{\deg\pi}\right)$$
$$\iff \left(\operatorname{Carl}\pi = F^{\deg\pi} + \pi \cdot u(\pi)\right)$$

). This proves Proposition 3.35 again. □

Remark 3.41. Now that we have a proof of Proposition 3.35 that is independent of [3, Theorem 2.11], we can turn the cart around and give a new proof of [3, Theorem 2.11, last equality] (though this proof, of course, will be rather roundabout):

Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Our goal is to show that $\overline{[\pi]}(X) = X^{q^{\deg\pi}}$, where $\overline{[\pi]}(X)$ denotes the projection of $[\pi](X) = [\pi] \in \mathbb{F}_q[T][X]$ onto $\left(\mathbb{F}_q[T]/\pi\right)[X]$.

We have $X^{q^{\deg\pi}} = \operatorname{Fqpol}\left(F^{\deg\pi}\right)$. (This can be proven as in our first proof of Proposition 3.35.) Also, Fqpol is an isomorphism of left $\mathbb{F}_q[T]$-modules (according to Proposition 3.24).

Proposition 3.35 shows that there exists a unique $u(\pi) \in \mathcal{F}$ such that $\operatorname{Carl}\pi = F^{\deg\pi} + \pi \cdot u(\pi)$. Consider this $u(\pi)$. Corollary 3.33 (applied to $M = \pi$) yields

$$\begin{aligned}
[\pi] &= \operatorname{Fqpol}\left(\underbrace{\operatorname{Carl}\pi}_{=F^{\deg\pi}+\pi\cdot u(\pi)}\right) = \operatorname{Fqpol}\left(F^{\deg\pi} + \pi \cdot u(\pi)\right) \\
&= \underbrace{\left(\operatorname{Fqpol}\left(F^{\deg\pi}\right)\right)}_{=X^{q^{\deg\pi}}} + \pi \underbrace{\operatorname{Fqpol}\left(u(\pi)\right)}_{\in\mathbb{F}_q[T][X]} \\
&\qquad \left(\text{since Fqpol is a homomorphism of left } \mathbb{F}_q[T]\text{-modules}\right) \\
&\in X^{q^{\deg\pi}} + \pi\mathbb{F}_q[T][X].
\end{aligned}$$

In other words, $[\pi] \equiv X^{q^{\deg\pi}} \bmod \pi\mathbb{F}_q[T][X]$. Projecting both sides of this congruence down to $\mathbb{F}_q[T][X] / \left(\pi\mathbb{F}_q[T][X]\right) = \left(\mathbb{F}_q[T]/\pi\right)[X]$, we obtain $\overline{[\pi]} = X^{q^{\deg\pi}}$. In other words, $\overline{[\pi]}(X) = X^{q^{\deg\pi}}$, qed.

3.10. Corollary: Carlitz action vs. Frobenius power

Corollary 3.42. Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Let A be an $\mathcal{F}$-module. Then, $(\operatorname{Carl}\pi)\, a \equiv F^{\deg\pi} a \bmod \pi A$ for every $a \in A$.

Proof of Corollary 3.42. Let $a \in A$. Proposition 3.35 shows that there exists a unique $u(\pi) \in \mathcal{F}$ such that $\operatorname{Carl}\pi = F^{\deg\pi} + \pi \cdot u(\pi)$. Consider this $u(\pi)$.

Now,

$$\underbrace{(\operatorname{Carl}\pi)}_{=F^{\deg\pi}+\pi\cdot u(\pi)}\ a = \left(F^{\deg\pi} + \pi \cdot u(\pi)\right) a = F^{\deg\pi} a + \underbrace{\pi \cdot u(\pi)\, a}_{\equiv 0 \bmod \pi A} \equiv F^{\deg\pi} a \bmod \pi A.$$

This proves Corollary 3.42. □

3.11. Exponent lifting for $\mathcal{F}$-modules

Next, we shall show a series of simple propositions which will culminate (if this can be called a culmination) in a Carlitz analogue of the classical "lifting the exponent" theorem (see, e.g., [6, version with solutions (ancillary file), (12.68.8)] for it).

Proposition 3.43. (a) The $\mathbb{F}_q$-vector subspace $\mathcal{F}F$ of $\mathcal{F}$ is a two-sided ideal of $\mathcal{F}$.

(b) Let $P \in \mathbb{F}_q[T]$. Then, $\operatorname{Carl} P \equiv P \bmod \mathcal{F}F$.

Proof of Proposition 3.43. **(a)** First, we claim that

$$Fu \in \mathcal{F}F \qquad \text{for every } u \in \mathcal{F}. \tag{78}$$

Proof of (78): Proposition 3.5 **(b)** shows that the $\mathbb{F}_q$-module $\mathcal{F}$ is free with basis $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$.

Let $u \in \mathcal{F}$. We must prove the relation (78). Since this relation is $\mathbb{F}_q$-linear in u (because $\mathcal{F}F$ is an $\mathbb{F}_q$-vector subspace of $\mathcal{F}$), we can WLOG assume that u belongs to the basis $\left(T^j F^i\right)_{i\geq 0,\ j\geq 0}$ of the $\mathbb{F}_q$-module $\mathcal{F}$. Assume this. Thus, $u = T^j F^i$ for some $i \in \mathbb{N}$ and $j \in \mathbb{N}$. Consider these i and j. Now,

$$F \underbrace{u}_{=T^jF^i} = \underbrace{FT^j}_{\substack{=\left(T^j\right)^q F \\ \text{(by Proposition 3.6,} \\ \text{applied to } P=T^j\text{)}}} F^i = \left(T^j\right)^q \underbrace{FF^i}_{=F^{i+1}=F^iF} = \underbrace{\left(T^j\right)^q F^i}_{\in\mathcal{F}} F \in \mathcal{F}F.$$

This proves (78).

Now,

$$F\mathcal{F} = \{Fu \mid u \in \mathcal{F}\} \subseteq \mathcal{F}F \qquad \text{(by (78))}.$$

But it is clear that $\mathcal{F}F$ is a left ideal of $\mathcal{F}$. Since we furthermore have $\mathcal{F}\underbrace{F\cdot\mathcal{F}}_{=F\mathcal{F}\subseteq\mathcal{F}F}\subseteq\underbrace{\mathcal{F}\mathcal{F}}_{\subseteq\mathcal{F}}F\subseteq\mathcal{F}F$, we thus conclude that $\mathcal{F}F$ is a two-sided ideal of $\mathcal{F}$. This proves Proposition 3.43 **(a)**.

(b) Proposition 3.43 **(a)** shows that $\mathcal{F}F$ is a two-sided ideal of $\mathcal{F}$. Hence, $\mathcal{F}/(\mathcal{F}F)$ is a quotient ring of $\mathcal{F}$, hence a quotient $\mathbb{F}_q$-algebra of $\mathcal{F}$. Let π denote the canonical projection map $\mathcal{F}\to\mathcal{F}/(\mathcal{F}F)$. Then, π is an $\mathbb{F}_q$-algebra homomorphism (since $\mathcal{F}/(\mathcal{F}F)$ is a quotient $\mathbb{F}_q$-algebra of $\mathcal{F}$).

But $\operatorname{Carl}(T)=F+T\equiv T \bmod \mathcal{F}F$ (since $F=\underbrace{1}_{\in\mathcal{F}}F\in\mathcal{F}F$). In other words, $\pi(\operatorname{Carl}(T))=\pi(T)$ (since π is the canonical projection map $\mathcal{F}\to\mathcal{F}/(\mathcal{F}F)$). Thus,

$$\begin{aligned}(\pi\circ\operatorname{Carl})(T)&=\pi(\operatorname{Carl}(T))=\pi\left(\underbrace{T}_{=\operatorname{Finc}_T(T)}\right)=\pi(\operatorname{Finc}_T(T))\\&=(\pi\circ\operatorname{Finc}_T)(T).\end{aligned}\tag{79}$$

But the three maps π, Carl and Finc_T are $\mathbb{F}_q$-algebra homomorphisms; hence, $\pi\circ\operatorname{Carl}$ and $\pi\circ\operatorname{Finc}_T$ are $\mathbb{F}_q$-algebra homomorphisms as well. The two $\mathbb{F}_q$-algebra homomorphisms $\pi\circ\operatorname{Carl}:\mathbb{F}_q[T]\to\mathcal{F}/(\mathcal{F}F)$ and $\pi\circ\operatorname{Finc}_T:\mathbb{F}_q[T]\to\mathcal{F}/(\mathcal{F}F)$ are equal to each other on the generator T of the $\mathbb{F}_q$-algebra $\mathbb{F}_q[T]$ (because of (79)). Therefore, these two homomorphisms must be identical. In other words, $\pi\circ\operatorname{Carl}=\pi\circ\operatorname{Finc}_T$.

Now,

$$\pi(\operatorname{Carl}P)=\underbrace{(\pi\circ\operatorname{Carl})}_{=\pi\circ\operatorname{Finc}_T}(P)=(\pi\circ\operatorname{Finc}_T)(P)=\pi\left(\underbrace{\operatorname{Finc}_T(P)}_{\substack{=P\\(\text{since we are regarding the}\\\text{map }\operatorname{Finc}_T\text{ as an inclusion})}}\right)=\pi(P).$$

In other words, $\operatorname{Carl}P\equiv P \bmod \mathcal{F}F$ (since π is the canonical projection map $\mathcal{F}\to\mathcal{F}/(\mathcal{F}F)$). This proves Proposition 3.43 **(b)**. □

Proposition 3.44. Let A be an $\mathcal{F}$-module. Let $P\in\mathbb{F}_q[T]$.
(a) We have $FPA\subseteq P^qA$.
(b) The $\mathbb{F}_q$-vector subspace PA of A is a left $\mathcal{F}$-submodule of A.
(c) Let k be a positive integer. Then, $FP^kA\subseteq P^{k+1}A$.
(d) Let k be a positive integer. Then, $(\operatorname{Carl}P)\,P^kA\subseteq P^{k+1}A$.

Proof of Proposition 3.44. **(a)** Proposition 3.6 yields $FP=P^qF$ in $\mathcal{F}$. Hence, $\underbrace{FP}_{=P^qF}A=P^q\underbrace{FA}_{\subseteq A}\subseteq P^qA$. Thus, Proposition 3.44 **(a)** is proven.

(b) Proposition 3.44 **(a)** yields $FPA \subseteq \underbrace{P^q}_{\substack{=PP^{q-1} \\ \text{(since } q \geq 1\text{)}}} A = P\underbrace{P^{q-1}A}_{\subseteq A} \subseteq PA$. Also, $\underbrace{TP}_{=PT} A = P\underbrace{TA}_{\subseteq A} \subseteq PA$.

Now, recall that the $\mathbb{F}_q$-algebra $\mathcal{F}$ is generated by F and T. From this, it is easy to derive the following fact: If $\mathcal{V}$ is an $\mathbb{F}_q$-vector subspace of some left $\mathcal{F}$-module $\mathcal{U}$ satisfying $F\mathcal{V} \subseteq \mathcal{V}$ and $T\mathcal{V} \subseteq \mathcal{V}$, then $\mathcal{V}$ is a left $\mathcal{F}$-submodule of $\mathcal{U}$. Applying this to $\mathcal{U} = A$ and $\mathcal{V} = PA$, we conclude that PA is a left $\mathcal{F}$-submodule of A (since $FPA \subseteq PA$ and $TPA \subseteq PA$). Proposition 3.44 **(b)** is thus shown.

(c) Proposition 3.44 **(a)** (applied to P^k instead of P) yields

$$FP^kA \subseteq \underbrace{\left(P^k\right)^q}_{\substack{=\left(P^k\right)^2\left(P^k\right)^{q-2} \\ \text{(since } q \geq 2\text{)}}} A = \left(P^k\right)^2 \underbrace{\left(P^k\right)^{q-2} A}_{\subseteq A} \subseteq \left(P^k\right)^2 A = P^k \underbrace{P^k}_{\substack{=PP^{k-1} \\ \text{(since } k \text{ is a positive integer)}}} A$$
$$= \underbrace{P^kP}_{=P^{k+1}} \underbrace{P^{k-1}A}_{\subseteq A} \subseteq P^{k+1}A.$$

This establishes Proposition 3.44 **(c)**.

(d) Proposition 3.43 **(b)** yields $\operatorname{Carl} P \equiv P \bmod \mathcal{F}F$. In other words, $\operatorname{Carl} P - P \in \mathcal{F}F$. In other words, there exists some $u \in \mathcal{F}$ such that $\operatorname{Carl} P - P = uF$. Consider this u.

Proposition 3.44 **(b)** (applied to P^{k+1} instead of P) shows that the $\mathbb{F}_q$-vector subspace $P^{k+1}A$ of A is a left $\mathcal{F}$-submodule of A. Hence, $uP^{k+1}A \subseteq P^{k+1}A$ (since $u \in \mathcal{F}$).

But $\operatorname{Carl} P - P = uF$ shows that $\operatorname{Carl} P = P + uF$. Hence,

$$\underbrace{(\operatorname{Carl} P)}_{=P+uF} P^kA = (P+uF)\,P^kA \subseteq \underbrace{PP^k}_{=P^{k+1}} A + u \underbrace{FP^kA}_{\substack{\subseteq P^{k+1}A \\ \text{(by Proposition 3.44 (c))}}} \subseteq P^{k+1}A + \underbrace{uP^{k+1}A}_{\subseteq P^{k+1}A}$$
$$\subseteq P^{k+1}A + P^{k+1}A \subseteq P^{k+1}A.$$

This proves Proposition 3.44 **(d)**. □

Proposition 3.45. Let A be an $\mathcal{F}$-module. Let $P \in \mathbb{F}_q[T]$. Let k be a positive integer.

Let a and b be two elements of A such that $a \equiv b \bmod P^kA$.

(a) We have $F^{\deg P}a \equiv F^{\deg P}b \bmod P^{k+1}A$.

(b) We have $(\operatorname{Carl} P)\,a \equiv (\operatorname{Carl} P)\,b \bmod P^{k+1}A$.

Proof of Proposition 3.45. From $a \equiv b \bmod P^kA$, we obtain $a - b \in P^kA$.

(a) If $P = 0$, then the claim of Proposition 3.45 **(a)** is true[39]. Hence, we WLOG

[39] *Proof.* Assume that $P = 0$. Thus, $P^k = 0^k = 0$ (since k is positive), so that $P^kA = 0A = 0$. Hence, $a \equiv b \bmod P^kA$ rewrites as $a \equiv b \bmod 0$. In other words, $a = b$. Hence, $F^{\deg P}a = F^{\deg P}b$, so that $F^{\deg P}a \equiv F^{\deg P}b \bmod P^{k+1}A$. In other words, the claim of Proposition 3.45 **(a)** is true; qed.

assume that $P \neq 0$.

If $\deg P = 0$, then the claim of Proposition 3.45 **(a)** is true[40]. Hence, we WLOG assume that $\deg P \neq 0$. Thus, $\deg P \geq 1$.

Let $d = \deg P$. Then, $d \geq 1$, so that $F^d = FF^{d-1}$.

But Proposition 3.44 **(b)** (applied to P^k instead of P) shows that the $\mathbb{F}_q$-vector subspace $P^k A$ of A is a left $\mathcal{F}$-submodule of A. Hence, $\mathcal{F} \cdot P^k A \subseteq P^k A$.

Now, $\deg P = d$, so that

$$F^{\deg P} a - F^{\deg P} b = F^d a - F^d b = \underbrace{F^d}_{=FF^{d-1}} \underbrace{(a-b)}_{\in P^k A} \in F \underbrace{F^{d-1}}_{\in \mathcal{F}} P^k A \subseteq F \underbrace{\mathcal{F} \cdot P^k A}_{\subseteq P^k A}$$
$$\subseteq FP^k A \subseteq P^{k+1} A \qquad \text{(by Proposition 3.44 \textbf{(c)})}.$$

In other words, $F^{\deg P} a \equiv F^{\deg P} b \bmod P^{k+1} A$. This proves Proposition 3.45 **(a)**.

(b) We have

$$(\operatorname{Carl} P)\, a - (\operatorname{Carl} P)\, b = (\operatorname{Carl} P) \underbrace{(a-b)}_{\in P^k A} \in (\operatorname{Carl} P)\, P^k A \subseteq P^{k+1} A$$

(by Proposition 3.44 **(d)**). In other words, $(\operatorname{Carl} P)\, a \equiv (\operatorname{Carl} P)\, b \bmod P^{k+1} A$. This proves Proposition 3.45 **(b)**. □

Corollary 3.46. Let A be an $\mathcal{F}$-module. Let $P \in \mathbb{F}_q[T]$. Let k be a positive integer.

Let a and b be two elements of A such that $a \equiv b \bmod P^k A$.

(a) We have $F^{\deg\left(P^\ell\right)} a \equiv F^{\deg\left(P^\ell\right)} b \bmod P^{k+\ell} A$ for every $\ell \in \mathbb{N}$.

(b) We have $\left(\operatorname{Carl}\left(P^\ell\right)\right) a \equiv \left(\operatorname{Carl}\left(P^\ell\right)\right) b \bmod P^{k+\ell} A$ for every $\ell \in \mathbb{N}$.

Proof of Corollary 3.46. **(a)** We can prove Corollary 3.46 **(a)** by induction over ℓ:

Induction base: We have $\deg \underbrace{\left(P^0\right)}_{=1} = \deg 1 = 0$ and thus $F^{\deg\left(P^0\right)} = F^0 = 1$. Hence, $F^{\deg\left(P^0\right)} a = 1a = a$ and similarly $F^{\deg\left(P^0\right)} b = b$. But $a \equiv b \bmod P^k A$. Since $k + 0 = k$, this rewrites as $a \equiv b \bmod P^{k+0} A$. Now, $F^{\deg\left(P^0\right)} a = a \equiv b = F^{\deg\left(P^0\right)} b \bmod P^{k+0} A$. In other words, Corollary 3.46 **(a)** holds for $\ell = 0$. This completes the induction base.

Induction step: Let $L \in \mathbb{N}$. Assume that Corollary 3.46 **(a)** holds for $\ell = L$. We must now prove that Corollary 3.46 **(a)** holds for $\ell = L + 1$.

We have assumed that Corollary 3.46 **(a)** holds for $\ell = L$. In other words, we have $F^{\deg\left(P^L\right)} a \equiv F^{\deg\left(P^L\right)} b \bmod P^{k+L} A$.

[40] *Proof.* Assume that $\deg P = 0$. Thus, the polynomial P is constant. Since $P \neq 0$, this shows that the polynomial P is invertible in $\mathbb{F}_q[T]$. Hence, P is invertible in $\mathcal{F}$. Therefore, P^{k+1} is also invertible in $\mathcal{F}$. Hence, $P^{k+1} A = A$. But $F^{\deg P} a \equiv F^{\deg P} b \bmod A$ is obviously true. Since $P^{k+1} A = A$, this rewrites as $F^{\deg P} a \equiv F^{\deg P} b \bmod P^{k+1} A$. In other words, the claim of Proposition 3.45 **(a)** is true; qed.

But k is a positive integer, and hence $k+L$ is a positive integer. Hence, Proposition 3.45 **(a)** (applied to $k+L$, $F^{\deg\left(P^L\right)}a$ and $F^{\deg\left(P^L\right)}b$ instead of k, a and b) yields

$$F^{\deg P}F^{\deg\left(P^L\right)}a \equiv F^{\deg P}F^{\deg\left(P^L\right)}b \bmod P^{k+L+1}A. \tag{80}$$

Now, $\deg\left(\underbrace{P^{L+1}}_{=PP^L}\right) = \deg\left(PP^L\right) = \deg P + \deg\left(P^L\right)$. Hence, $F^{\deg\left(P^{L+1}\right)} = F^{\deg P+\deg\left(P^L\right)} = F^{\deg P}F^{\deg\left(P^L\right)}$. Therefore, (80) rewrites as follows:

$$F^{\deg\left(P^{L+1}\right)}a \equiv F^{\deg\left(P^{L+1}\right)}b \bmod P^{k+L+1}A.$$

In other words, Corollary 3.46 **(a)** holds for $\ell = L+1$. This completes the induction step. The induction proof of Corollary 3.46 **(a)** is thus finished.

(b) We can prove Corollary 3.46 **(b)** by induction over ℓ:

Induction base: We have $\operatorname{Carl}\underbrace{\left(P^0\right)}_{=1} = \operatorname{Carl}1 = 1$ (since Carl is an $\mathbb{F}_q$-algebra homomorphism). Hence, $\left(\operatorname{Carl}\left(P^0\right)\right)a = 1a = a$ and similarly $\left(\operatorname{Carl}\left(P^0\right)\right)b = b$. But $a \equiv b \bmod P^kA$. Since $k+0=k$, this rewrites as $a \equiv b \bmod P^{k+0}A$. Now, $\left(\operatorname{Carl}\left(P^0\right)\right)a = a \equiv b = \left(\operatorname{Carl}\left(P^0\right)\right)b \bmod P^{k+0}A$. In other words, Corollary 3.46 **(b)** holds for $\ell = 0$. This completes the induction base.

Induction step: Let $L \in \mathbb{N}$. Assume that Corollary 3.46 **(b)** holds for $\ell = L$. We must now prove that Corollary 3.46 **(b)** holds for $\ell = L+1$.

We have assumed that Corollary 3.46 **(b)** holds for $\ell = L$. In other words, we have $\left(\operatorname{Carl}\left(P^L\right)\right)a \equiv \left(\operatorname{Carl}\left(P^L\right)\right)b \bmod P^{k+L}A$.

But k is a positive integer, and hence $k+L$ is a positive integer. Hence, Proposition 3.45 **(b)** (applied to $k+L$, $\left(\operatorname{Carl}\left(P^L\right)\right)a$ and $\left(\operatorname{Carl}\left(P^L\right)\right)b$ instead of k, a and b) yields

$$\left(\operatorname{Carl}P\right)\left(\operatorname{Carl}\left(P^L\right)\right)a \equiv \left(\operatorname{Carl}P\right)\left(\operatorname{Carl}\left(P^L\right)\right)b \bmod P^{k+L+1}A. \tag{81}$$

Now, $\operatorname{Carl}\left(\underbrace{P^{L+1}}_{=PP^L}\right) = \operatorname{Carl}\left(PP^L\right) = \left(\operatorname{Carl}P\right)\left(\operatorname{Carl}\left(P^L\right)\right)$ (since Carl is an $\mathbb{F}_q$-algebra homomorphism). Thus, (81) rewrites as follows:

$$\left(\operatorname{Carl}\left(P^{L+1}\right)\right)a \equiv \left(\operatorname{Carl}\left(P^{L+1}\right)\right)b \bmod P^{k+L+1}A.$$

In other words, Corollary 3.46 **(b)** holds for $\ell = L+1$. This completes the induction step. The induction proof of Corollary 3.46 **(b)** is thus finished. □

In order to state the last corollary in this section, we need a definition:

Definition 3.47. Let $\mathbb{K}$ be a field. Let π be a monic irreducible polynomial in $\mathbb{K}[T]$. Let f be any polynomial in $\mathbb{K}[T]$. Then, $v_\pi(f)$ means the largest nonnegative integer m satisfying $\pi^m \mid f$; this is set to be $+\infty$ if $f = 0$. Thus, $v_\pi(f) \in \mathbb{N} \cup \{+\infty\}$ for each f.

We set $P^{+\infty} = 0$ for each $P \in \mathbb{K}[T]$. Thus, $\pi^{v_\pi(f)} \mid f$ holds for each $f \in \mathbb{K}[T]$ (including the case when $f = 0$).

Corollary 3.48. Let A be an $\mathcal{F}$-module. Let $N \in \mathbb{F}_q[T]$. Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$.

Let a and b be two elements of A such that $a \equiv b \bmod \pi A$.

(a) We have $F^{\deg N} a \equiv F^{\deg N} b \bmod \pi^{v_\pi(N)+1} A$. (Here, $F^{\deg N}$ is understood to mean 0 when $N = 0$.)

(b) We have $(\operatorname{Carl} N)\, a \equiv (\operatorname{Carl} N)\, b \bmod \pi^{v_\pi(N)+1} A$.

Proof of Corollary 3.48. We have $a \equiv b \bmod \pi A$. In other words, $a \equiv b \bmod \pi^1 A$ (since $\pi = \pi^1$).

If $N = 0$, then Corollary 3.48 is easily seen to hold (since $F^{\deg N} = 0$ and $\operatorname{Carl} \underbrace{N}_{=0} = \operatorname{Carl} 0 = 0$ in this case). Hence, we WLOG assume that $N \neq 0$. Thus, $v_\pi(N) \in \mathbb{N}$. Set $\ell = v_\pi(N)$. Then, $\pi^\ell \mid N$. In other words, there exists some polynomial $M \in \mathbb{F}_q[T]$ such that $N = M\pi^\ell$. Consider this M.

Proposition 3.44 **(b)** (applied to $P = \pi^{1+\ell}$) shows that the $\mathbb{F}_q$-vector subspace $\pi^{1+\ell} A$ of A is a left $\mathcal{F}$-submodule of A. Hence, $\mathcal{F} \cdot \pi^{1+\ell} A \subseteq \pi^{1+\ell} A$.

(a) From $N = M\pi^\ell$, we obtain $\deg N = \deg\left(M\pi^\ell\right) = \deg M + \deg\left(\pi^\ell\right)$, so that $F^{\deg N} = F^{\deg M + \deg\left(\pi^\ell\right)} = F^{\deg M} F^{\deg\left(\pi^\ell\right)}$.

Corollary 3.46 **(a)** (applied to $P = \pi$ and $k = 1$) yields $F^{\deg\left(\pi^\ell\right)} a \equiv F^{\deg\left(\pi^\ell\right)} b \bmod \pi^{1+\ell} A$ (since $a \equiv b \bmod \pi^1 A$). In other words, $F^{\deg\left(\pi^\ell\right)} a - F^{\deg\left(\pi^\ell\right)} b \in \pi^{1+\ell} A$. But

$$\begin{aligned} & F^{\deg N} a - F^{\deg N} b \\ &= \underbrace{F^{\deg N}}_{= F^{\deg M} F^{\deg\left(\pi^\ell\right)}} (a-b) = \underbrace{F^{\deg M}}_{\in \mathcal{F}} \underbrace{F^{\deg\left(\pi^\ell\right)}(a-b)}_{= F^{\deg\left(\pi^\ell\right)} a - F^{\deg\left(\pi^\ell\right)} b \in \pi^{1+\ell} A} \\ &\in \mathcal{F} \cdot \pi^{1+\ell} A \subseteq \pi^{1+\ell} A. \end{aligned}$$

In other words, $F^{\deg N} a \equiv F^{\deg N} b \bmod \pi^{1+\ell} A$. Since $1 + \underbrace{\ell}_{= v_\pi(N)} = 1 + v_\pi(N) = v_\pi(N) + 1$, this rewrites as $F^{\deg N} a \equiv F^{\deg N} b \bmod \pi^{v_\pi(N)+1} A$. This proves Corollary 3.48 **(a)**.

(b) From $N = M\pi^\ell$, we obtain $\operatorname{Carl} N = \operatorname{Carl}\left(M\pi^\ell\right) = (\operatorname{Carl} M)\left(\operatorname{Carl}\left(\pi^\ell\right)\right)$ (since Carl is an $\mathbb{F}_q$-algebra homomorphism).

Corollary 3.46 **(b)** (applied to $P = \pi$ and $k = 1$) yields $\left(\operatorname{Carl}\left(\pi^\ell\right)\right) a \equiv \left(\operatorname{Carl}\left(\pi^\ell\right)\right) b \bmod \pi^{1+\ell} A$ (since $a \equiv b \bmod \pi^1 A$). In other words, $\left(\operatorname{Carl}\left(\pi^\ell\right)\right) a -$

$\left(\operatorname{Carl}\left(\pi^{\ell}\right)\right) b \in \pi^{1+\ell} A$. But

$$\begin{aligned}
&(\operatorname{Carl} N)\, a - (\operatorname{Carl} N)\, b \\
&= \underbrace{(\operatorname{Carl} N)}_{=(\operatorname{Carl} M)\left(\operatorname{Carl}\left(\pi^{\ell}\right)\right)} (a-b) = \underbrace{(\operatorname{Carl} M)}_{\in \mathcal{F}} \underbrace{\left(\operatorname{Carl}\left(\pi^{\ell}\right)\right)(a-b)}_{=\left(\operatorname{Carl}\left(\pi^{\ell}\right)\right)a - \left(\operatorname{Carl}\left(\pi^{\ell}\right)\right)b \in \pi^{1+\ell}A} \\
&\in \mathcal{F} \cdot \pi^{1+\ell} A \subseteq \pi^{1+\ell} A.
\end{aligned}$$

In other words, $(\operatorname{Carl} N)\, a \equiv (\operatorname{Carl} N)\, b \bmod \pi^{1+\ell} A$. Since $1 + \underbrace{\ell}_{=v_\pi(N)} = 1 + v_\pi(N) = v_\pi(N) + 1$, this rewrites as $(\operatorname{Carl} N)\, a \equiv (\operatorname{Carl} N)\, b \bmod \pi^{v_\pi(N)+1} A$. This proves Corollary 3.48 **(b)**. □

Each of the two parts of Corollary 3.48 can be viewed as an analogue of the classical "exponent lifting lemma" [6, version with solutions (ancillary file), (12.68.8)].

3.12. The Chinese Remainder Theorem

Next, we recall one of the many versions of the Chinese Remainder Theorem:

Theorem 3.49. Let A be a commutative ring. Let M be an A-module. Let $N \in \mathbb{N}$. Let $I_1, I_2, \ldots, I_N$ be N ideals of A. Assume that $I_i + I_j = A$ for any two elements i and j of $\{1, 2, \ldots, N\}$ satisfying $i < j$.

(a) We have $I_1 I_2 \cdots I_N \cdot M = I_1 M \cap I_2 M \cap \cdots \cap I_N M$.

(b) The canonical A-module homomorphism

$$\begin{aligned}
M / \left(I_1 I_2 \cdots I_N \cdot M\right) &\to \prod_{k=1}^{N} \left(M / I_k M\right), \\
m + I_1 I_2 \cdots I_N \cdot M &\mapsto \left(m + I_1 M, m + I_2 M, \ldots, m + I_N M\right)
\end{aligned}$$

is well-defined and an A-module isomorphism.

Theorem 3.49 is precisely [8, Theorem 1 **(a)** and **(b)**]; thus, we are not giving a proof of it here.

For us, the following restatement of Theorem 3.49 will be more useful:

Theorem 3.50. Let A be a commutative ring. Let M be an A-module. Let $\mathbf{S}$ be a finite set. For every $s \in \mathbf{S}$, let I_s be an ideal of A. Assume that the ideals I_s of A are *comaximal*; this means that every two distinct elements s and t of $\mathbf{S}$ satisfy $I_s + I_t = A$. Then:

(a) We have

$$\left(\prod_{s \in \mathbf{S}} I_s\right) \cdot M = \bigcap_{s \in \mathbf{S}} \left(I_s M\right).$$

(b) The canonical A-module homomorphism

$$M/\left(\left(\prod_{s\in\mathbf{S}} I_s\right)\cdot M\right) \to \prod_{s\in\mathbf{S}} \left(M/I_s M\right),$$
$$m+\left(\prod_{s\in\mathbf{S}} I_s\right)\cdot M \mapsto \left(m+I_s M\right)_{s\in\mathbf{S}}$$

is well-defined and an A-module isomorphism.

Proof of Theorem 3.50. We can freely relabel the elements of $\mathbf{S}$. Thus, we can WLOG assume that $\mathbf{S} = \{1,2,\ldots,N\}$ for some $N \in \mathbb{N}$. Assume this, and consider this N. Then, the claim of Theorem 3.50 becomes identical with the claim of Theorem 3.49. But since we already know that Theorem 3.49 holds, we thus conclude that Theorem 3.50 holds as well. □

We shall only use part **(a)** of Theorem 3.50.

As a consequence of Theorem 3.50 **(a)**, we have the following:

Corollary 3.51. Let A be an $\mathbb{F}_q[T]$-module. Let P be a monic polynomial in $\mathbb{F}_q[T]$. Then,

$$\bigcap_{\pi\in \mathrm{PF}\, P} \pi^{v_\pi(P)} A = PA.$$

Before we can prove Corollary 3.51, we need a simple lemma:

Lemma 3.52. Let $\mathbb{F}$ be a field. Let s and t be two distinct monic irreducible polynomials in $\mathbb{F}[T]$. Let $n \in \mathbb{N}$ and $m \in \mathbb{N}$. Let R be the ring $\mathbb{F}[T]$. Then, $s^n R + t^m R = R$.

Proof of Lemma 3.52. The polynomials s and t are two distinct monic irreducible polynomials in $\mathbb{F}[T]$. Hence, s and t are coprime. Consequently, s^n and t^m are coprime as well (since $\mathbb{F}[T]$ is a principal ideal domain). By Bezout's theorem, we thus conclude that there exist polynomials a and b in $\mathbb{F}[T]$ satisfying $as^n + bt^m = 1$. Consider these a and b.

The unity 1 of the ring $R = \mathbb{F}[T]$ satisfies

$$1 = as^n + bt^m = s^n \underbrace{a}_{\in \mathbb{F}[T]=R} + t^m \underbrace{b}_{\in \mathbb{F}[T]=R} \in s^n R + t^m R.$$

But $s^n R + t^m R$ is an ideal of R (since $s^n R$ and $t^m R$ are ideals of R). This ideal $s^n R + t^m R$ contains 1 (since $1 \in s^n R + t^m R$), and thus must equal the whole ring R (because if an ideal of some ring contains 1, then this ideal must equal the whole ring). In other words, $s^n R + t^m R = R$. This proves Lemma 3.52. □

Proof of Corollary 3.51. For each $s \in \operatorname{PF} P$, define an ideal I_s of $\mathbb{F}_q[T]$ by $I_s = s^{v_s(P)}\mathbb{F}_q[T]$. Notice that $\mathbb{F}_q[T]$ is a principal ideal domain.

For each $s \in \operatorname{PF} P$, we have

$$I_s A = s^{v_s(P)} A \tag{82}$$

[41].

On the other hand, P is a monic polynomial in $\mathbb{F}_q[T]$. Hence, the prime factorization of P in the principal ideal domain $\mathbb{F}_q[T]$ is $P = \prod_{s \in \operatorname{PF} P} s^{v_s(P)}$ (indeed, for each $s \in \operatorname{PF} P$, the multiplicity of s in the prime factorization of P is $v_s(P)$). Now,

$$\begin{aligned}\prod_{s\in\operatorname{PF} P} \underbrace{I_s}_{\substack{=s^{v_s(P)}\mathbb{F}_q[T] \\ \text{(by the} \\ \text{definition of } I_s)}} &= \prod_{s\in\operatorname{PF} P} \left(s^{v_s(P)}\mathbb{F}_q[T]\right) = \underbrace{\left(\prod_{s\in\operatorname{PF} P} s^{v_s(P)}\right)}_{=P}\mathbb{F}_q[T] \\ &= P\cdot\mathbb{F}_q[T]. \end{aligned} \tag{83}$$

If s and t are two distinct elements of $\operatorname{PF} P$, then $I_s + I_t = \mathbb{F}_q[T]$ [42]. Hence, Theorem 3.50 **(a)** (applied to $\mathbb{F}_q[T]$, A and $\operatorname{PF} P$ instead of A, M and $\mathbf{S}$) shows that

$$\left(\prod_{s\in\operatorname{PF} P} I_s\right)\cdot A = \bigcap_{s\in\operatorname{PF} P} \underbrace{(I_s A)}_{\substack{=s^{v_s(P)}A \\ \text{(by (82))}}} = \bigcap_{s\in\operatorname{PF} P} s^{v_s(P)}A = \bigcap_{\pi\in\operatorname{PF} P} \pi^{v_\pi(P)}A$$

(here, we have renamed the index s as π in the intersection). Thus,

$$\bigcap_{\pi\in\operatorname{PF} P} \pi^{v_\pi(P)}A = \underbrace{\left(\prod_{s\in\operatorname{PF} P} I_s\right)}_{\substack{=P\cdot\mathbb{F}_q[T] \\ \text{(by (83))}}}\cdot A = P\cdot\underbrace{\mathbb{F}_q[T]\cdot A}_{=A} = PA.$$

[41] *Proof of (82):* Let $s \in \operatorname{PF} P$. Then, the definition of I_s yields $I_s = s^{v_s(P)}\mathbb{F}_q[T]$. Now,

$$\underbrace{I_s}_{=s^{v_s(P)}\mathbb{F}_q[T]} A = s^{v_s(P)}\underbrace{\mathbb{F}_q[T]\cdot A}_{=A} = s^{v_s(P)}A.$$

This proves (82).

[42] *Proof.* Let s and t be two distinct elements of $\operatorname{PF} P$. Thus, s and t are two distinct monic irreducible polynomials in $\mathbb{F}_q[T]$. Hence, Lemma 3.52 (applied to $\mathbb{F} = \mathbb{F}_q$, $n = v_s(P)$, $m = v_t(P)$ and $R = \mathbb{F}_q[T]$) yields $s^{v_s(P)}\mathbb{F}_q[T] + t^{v_t(P)}\mathbb{F}_q[T] = \mathbb{F}_q[T]$.

The definition of I_s yields $I_s = s^{v_s(P)}\mathbb{F}_q[T]$. The definition of I_t shows that $I_t = t^{v_t(P)}\mathbb{F}_q[T]$. Hence,

$$\underbrace{I_s}_{=s^{v_s(P)}\mathbb{F}_q[T]} + \underbrace{I_t}_{=t^{v_t(P)}\mathbb{F}_q[T]} = s^{v_s(P)}\mathbb{F}_q[T] + t^{v_t(P)}\mathbb{F}_q[T] = \mathbb{F}_q[T].$$

Qed.

This proves Corollary 3.51. □

Let me also state the "ring version" of the Chinese Remainder theorem:

Theorem 3.53. Let A be a commutative ring. Let $\mathbf{S}$ be a finite set. For every $s \in \mathbf{S}$, let I_s be an ideal of A. Assume that the ideals I_s of A are *comaximal*; this means that every two distinct elements s and t of $\mathbf{S}$ satisfy $I_s + I_t = A$. Then:

(a) We have

$$\prod_{s \in \mathbf{S}} I_s = \bigcap_{s \in \mathbf{S}} I_s.$$

(b) The canonical A-algebra homomorphism

$$A / \left(\prod_{s \in \mathbf{S}} I_s \right) \to \prod_{s \in \mathbf{S}} \left(A / I_s \right), \qquad a + \prod_{s \in \mathbf{S}} I_s \mapsto \left(a + I_s \right)_{s \in \mathbf{S}}$$

is well-defined and an A-algebra isomorphism.

Theorem 3.53 can easily be derived by applying Theorem 3.50 to $M = A$. (The extra claim that the homomorphism in Theorem 3.53 **(b)** is an A-algebra homomorphism is straightforward to check.) But Theorem 3.53 is also a classical fact that appears in many textbooks on algebra (it is probably easier to find than Theorem 3.50).

Let me continue with another simple lemma about divisibility of polynomials:

Lemma 3.54. Let P be a polynomial in $\mathbb{F}_q[T]$. Let π be a monic irreducible divisor of P. Let D be a divisor of P satisfying $D \nmid P/\pi$. Then, $\pi^{v_\pi(P)} \mid D$.

Proof of Lemma 3.54. From $D \nmid P/\pi$, we obtain $P/\pi \neq 0$, hence $P \neq 0$.

We have $D \nmid P/\pi$. In other words, $\dfrac{P/\pi}{D} \notin \mathbb{F}_q[T]$. This rewrites as $\dfrac{P/D}{\pi} \notin \mathbb{F}_q[T]$ (since $\dfrac{P/\pi}{D} = \dfrac{P/D}{\pi}$). Equivalently, $\pi \nmid P/D$ (since $P/D \in \mathbb{F}_q[T]$ (because D is a divisor of P)). In other words, $v_\pi(P/D) = 0$. Hence, $0 = v_\pi(P/D) = v_\pi(P) - v_\pi(D)$, so that $v_\pi(P) = v_\pi(D)$.

But $\pi^{v_\pi(D)} \mid D$ (obviously). Since $v_\pi(P) = v_\pi(D)$, we now have $\pi^{v_\pi(P)} = \pi^{v_\pi(D)} \mid D$. This proves Lemma 3.54. □

Here is a well-known fact about quotients of polynomial rings over fields:

Proposition 3.55. Let $\mathbb{F}$ be a field. Let $s \in \mathbb{F}[T]$ be a monic irreducible polynomial. Let n be a positive integer. Let B be the ring $\mathbb{F}[T]/s^n\mathbb{F}[T]$. Then:

(a) We have $B^\times = B \setminus sB$. (Here, $B^\times$ denotes the group of units of the ring B.)

(b) We have $sB \cong \mathbb{F}[T]/s^{n-1}\mathbb{F}[T]$ as $\mathbb{F}$-vector spaces.

Proof of Proposition 3.55. For every $a \in \mathbb{F}[T]$, we let $\overline{a}$ denote the canonical projection of a on $\mathbb{F}[T]/s^n\mathbb{F}[T] = B$.

(a) We shall prove the inclusions $B^\times \subseteq B \setminus sB$ and $B \setminus sB \subseteq B^\times$ separately:

Proof of $B^\times \subseteq B \setminus sB$: Let $b \in B^\times$.

We have $b \in B^\times$. In other words, the element b of B is invertible. In other words, there exists some $d \in B$ such that $bd = 1$. Consider this d.

We have $d \in B$. Thus, $d = \overline{c}$ for some $c \in \mathbb{F}[T]$. Consider this c.

Now, assume (for the sake of contradiction) that $b \in sB$. In other words, $b = sf$ for some $f \in B$. Consider this f.

We have $f \in B$. Thus, $f = \overline{e}$ for some $e \in \mathbb{F}[T]$. Consider this e. Multiplying the equalities $f = \overline{e}$ and $d = \overline{c}$, we obtain $fd = \overline{e} \cdot \overline{c} = \overline{ec} = \overline{ce}$.

Now, $bd = 1$, so that $1 = \underbrace{b}_{=sf} d = s\underbrace{fd}_{=\overline{ce}} = s\overline{ce} = \overline{sce}$. In other words, $1 \equiv sce \bmod s^n\mathbb{F}[T]$. In other words, $s^n \mid 1 - sce$. But since n is positive, we have $s \mid s^n \mid 1 - sce$. Thus, the polynomial $1 - sce$ is divisible by s. Also, the polynomial sce is divisible by s (clearly). Hence, the sum of these two polynomials $1 - sce$ and sce must also divisible by s. In other words, $(1 - sce) + sce$ is divisible by s. In other words, 1 is divisible by s (since $(1 - sce) + sce = 1$). This is clearly absurd (since s is irreducible). Thus, we have found a contradiction. This shows that our assumption (that $b \in sB$) was false.

Hence, $b \notin sB$. Combining this with $b \in B$, we obtain $b \in B \setminus sB$.

Now, forget that we fixed b. We thus have proven that $b \in B \setminus sB$ for each $b \in B^\times$. In other words, $B^\times \subseteq B \setminus sB$.

Proof of $B \setminus sB \subseteq B^\times$: Let $b \in B \setminus sB$. Then, $b \in B \setminus sB \subseteq B$. Hence, $b = \overline{a}$ for some $a \in \mathbb{F}[T]$. Consider this a.

We have $s \nmid a$ [43]. Hence, the polynomials a and s are coprime (since s is irreducible, and since $\mathbb{F}[T]$ is a principal ideal domain). Therefore, the polynomials a and s^n are coprime (since $\mathbb{F}[T]$ is a principal ideal domain). By Bezout's theorem, we thus conclude that there exist polynomials α and β in $\mathbb{F}[T]$ satisfying $\alpha a + \beta s^n = 1$. Consider these α and β.

The unity 1 of the ring $\mathbb{F}[T]$ satisfies $1 = \alpha a + \underbrace{\beta s^n}_{\substack{\equiv 0 \bmod s^n\mathbb{F}[T] \\ (\text{since } s^n \mid \beta s^n)}} \equiv \alpha a \bmod s^n\mathbb{F}[T]$.

In other words, $\overline{1} = \overline{\alpha a}$. Comparing this with $\overline{\alpha}\underbrace{b}_{=\overline{a}} = \overline{\alpha} \cdot \overline{a} = \overline{\alpha a}$, we obtain $\overline{\alpha} b = \overline{1} = 1$. Hence, the element b of B is invertible. In other words, $b \in B^\times$.

Now, forget that we fixed b. We thus have proven that $b \in B^\times$ for each $b \in B \setminus sB$. In other words, $B \setminus sB \subseteq B^\times$.

[43] *Proof.* Assume the contrary. Thus, $s \mid a$. In other words, $a = cs$ for some $c \in \mathbb{F}[T]$. Consider this c. From $a = cs = sc$, we obtain $\overline{a} = \overline{cs} = \overline{sc} = s\underbrace{\overline{c}}_{\in B} \in sB$. But $\overline{a} = b \in B \setminus sB$ and thus $\overline{a} \notin sB$. This contradicts $\overline{a} \in sB$. This contradiction shows that our assumption was wrong; qed.

Combining the two relations $B^\times \subseteq B \setminus sB$ and $B \setminus sB \subseteq B^\times$, we obtain $B^\times = B \setminus sB$. Thus, Proposition 3.55 **(a)** is proven.

(b) Let ρ be the map $\mathbb{F}[T] \to sB,\ f \mapsto s\overline{f}$. It is straightforward to see that this map ρ is well-defined and $\mathbb{F}$-linear. Moreover, $\operatorname{Ker}\rho \subseteq s^{n-1}\mathbb{F}[T]$ [44] and $s^{n-1}\mathbb{F}[T] \subseteq \operatorname{Ker}\rho$ [45]. Combining these two inclusions, we obtain $\operatorname{Ker}\rho = s^{n-1}\mathbb{F}[T]$. Moreover, the map ρ is surjective[46]. Hence, $\rho(\mathbb{F}[T]) = sB$.

Now, the first isomorphism theorem (applied to the $\mathbb{F}$-linear map $\rho : \mathbb{F}[T] \to sB$) yields $\rho(\mathbb{F}[T]) \cong \mathbb{F}[T] / \underbrace{\operatorname{Ker}\rho}_{=s^{n-1}\mathbb{F}[T]} = \mathbb{F}[T]/s^{n-1}\mathbb{F}[T]$ as $\mathbb{F}$-vector spaces. In light of $\rho(\mathbb{F}[T]) = sB$, this rewrites as $sB \cong \mathbb{F}[T]/s^{n-1}\mathbb{F}[T]$. Thus, Proposition 3.55 **(b)** is proven. □

3.13. Ghost-Witt integrality: a general equivalence

Recall the notion of a "q-nest" defined in Definition 2.11. Recall also Definition 2.12. Furthermore, recall the following convention:

---

[44] *Proof.* Let $a \in \operatorname{Ker}\rho$. Thus, $a \in \mathbb{F}[T]$ and $\rho(a) = 0$. Now, the definition of ρ yields $\rho(a) = s\overline{a} = \overline{sa}$. Hence, $\overline{sa} = \rho(a) = 0$. In other words, $sa \in s^n\mathbb{F}[T]$. In other words, $s^n \mid sa$ in $\mathbb{F}[T]$. In other words, there exists some $g \in \mathbb{F}[T]$ satisfying $sa = s^n g$. Consider this g.

The polynomial s is irreducible and thus nonzero. Hence, we can cancel s from the equation $sa = \underbrace{s^n}_{=ss^{n-1}} g = ss^{n-1}g$ (since $\mathbb{F}[T]$ is an integral domain). We thus obtain $a = s^{n-1}\underbrace{g}_{\in\mathbb{F}[T]} \in s^{n-1}\mathbb{F}[T]$.

Now, forget that we fixed a. We thus have shown that $a \in s^{n-1}\mathbb{F}[T]$ for each $a \in \operatorname{Ker}\rho$. In other words, $\operatorname{Ker}\rho \subseteq s^{n-1}\mathbb{F}[T]$. Qed.

[45] *Proof.* Let $f \in s^{n-1}\mathbb{F}[T]$. Thus, there exists some $g \in \mathbb{F}[T]$ satisfying $f = s^{n-1}g$. Consider this g. Now, the definition of ρ yields

$$\begin{aligned} \rho(f) &= s\overline{f} = s\overline{s^{n-1}g} && \left(\text{since } f = s^{n-1}g\right) \\ &= \overline{ss^{n-1}g} = 0 && \left(\text{since } \underbrace{ss^{n-1}}_{=s^n} g = s^n \underbrace{g}_{\in\mathbb{F}[T]} \in s^n\mathbb{F}[T]\right). \end{aligned}$$

In other words, $f \in \operatorname{Ker}\rho$.

Now, forget that we fixed f. We thus have proven that $f \in \operatorname{Ker}\rho$ for each $f \in s^{n-1}\mathbb{F}[T]$. In other words, $s^{n-1}\mathbb{F}[T] \subseteq \operatorname{Ker}\rho$. Qed.

[46] *Proof.* Let $a \in sB$. Thus, there exists some $b \in B$ such that $a = sb$. Consider this b. Now, we have $b \in B$. Hence, $b = \overline{f}$ for some $f \in \mathbb{F}[T]$. Consider this f. The definition of ρ yields $\rho(f) = s\overline{f} = sb$ (since $\overline{f} = b$). Compared with $a = sb$, this yields $a = \rho\left(\underbrace{f}_{\in\mathbb{F}[T]}\right) \in \rho(\mathbb{F}[T])$.

Now, forget that we fixed a. We thus have proven that $a \in \rho(\mathbb{F}[T])$ for each $a \in sB$. In other words, $sB \subseteq \rho(\mathbb{F}[T])$. In other words, the map ρ is surjective. Qed.

Definition 3.56. Let P be a monic polynomial in $\mathbb{F}_q[T]$. Then, the summation sign $\sum_{D|P}$ means a sum over all **monic** polynomials D dividing P.

We shall now prove a very general fact that encompasses some of the claims of Theorem 2.13:

Theorem 3.57. Let N be a q-nest. Let A be an $\mathcal{F}$-module. For every $P \in N$, let φ_P and ψ_P be two endomorphisms of the $\mathbb{F}_q$-vector space A. Let us make the following five assumptions:

Assumption 1: For every $P \in N$, the map φ_P is an endomorphism of the $\mathcal{F}$-module A.

Assumption 2: We have $\varphi_\pi(a) \equiv (\operatorname{Carl}\pi)\, a \bmod \pi A$ for every $a \in A$ and every monic irreducible $\pi \in N$.

Assumption 3: We have $\varphi_1 = \mathrm{id}$. Furthermore, $\varphi_P \circ \varphi_Q = \varphi_{PQ}$ for every $P \in N$ and every $Q \in N$ satisfying $PQ \in N$.

Assumption 4: We have $\psi_P(a) \equiv \varphi_\pi(\psi_{P/\pi}(a)) \bmod \pi^{v_\pi(P)} A$ for every $a \in A$, every $P \in N$ and every $\pi \in \operatorname{PF} P$.

Assumption 5: We have $\psi_1 = \mathrm{id}$.

Let $(b_P)_{P\in N} \in A^N$ be a family of elements of A. Then, the following assertions $\mathcal{C}_1$ and $\mathcal{E}_\psi$ are equivalent:

Assertion $\mathcal{C}_1$: Every $P \in N$ and every $\pi \in \operatorname{PF} P$ satisfy

$$\varphi_\pi(b_{P/\pi}) \equiv b_P \bmod \pi^{v_\pi(P)} A.$$

Assertion $\mathcal{E}_\psi$: There exists a family $(z_P)_{P\in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D|P} D\psi_{P/D}(z_D) \text{ for every } P \in N \right).$$

Before we prove this theorem, let us make a few comments.

Remark 3.58. Let N be a q-nest. Let A be an $\mathcal{F}$-module. For every $P \in N$, let φ_P be an endomorphism of the $\mathbb{F}_q$-vector space A. Then, Assumption 2 in Theorem 3.57 is equivalent to the following statement: We have $\varphi_\pi(a) \equiv F^{\deg\pi} a \bmod \pi A$ for every $a \in A$ and every monic irreducible $\pi \in N$.

Proof of Remark 3.58. It is clearly enough to show that $(\operatorname{Carl}\pi)\, a \equiv F^{\deg\pi} a \bmod \pi A$ for every $a \in A$ and every monic irreducible $\pi \in N$. But this follows from Corollary 3.42. Thus, Remark 3.58 is proven. □

Next, let us show examples of endomorphisms ψ_P satisfying the Assumption 4 of Theorem 3.57:

Proposition 3.59. Let N be a q-nest. Let A be an $\mathcal{F}$-module. For every $P \in N$, let φ_P be an endomorphism of the $\mathbb{F}_q$-vector space A. Assume that the Assumptions 1 and 2 of Theorem 3.57 are satisfied.

For every $P \in N$, define an endomorphism ψ_P of the $\mathbb{F}_q$-vector space A by

$$\left(\psi_P(a) = (\operatorname{Carl} P)\, a \qquad \text{for every } a \in A\right).$$

Then, Assumptions 4 and 5 of Theorem 3.57 are satisfied.

Proposition 3.60. Let N be a q-nest. Let A be an $\mathcal{F}$-module. For every $P \in N$, let φ_P be an endomorphism of the $\mathbb{F}_q$-vector space A. Assume that the Assumption 1 and 2 of Theorem 3.57 are satisfied.

For every $P \in N$, define an endomorphism ψ_P of the $\mathbb{F}_q$-vector space A by

$$\left(\psi_P(a) = F^{\deg P} a \qquad \text{for every } a \in A\right).$$

Then, Assumptions 4 and 5 of Theorem 3.57 are satisfied.

Proposition 3.61. Let N be a q-nest. Let A be an $\mathcal{F}$-module. For every $P \in N$, let φ_P be an endomorphism of the $\mathbb{F}_q$-vector space A. Assume that the Assumption 3 of Theorem 3.57 is satisfied.

For every $P \in N$, define an endomorphism ψ_P of the $\mathbb{F}_q$-vector space A by

$$\psi_P = \varphi_P.$$

Then, Assumptions 4 and 5 of Theorem 3.57 are satisfied.

Proof of Proposition 3.59. Assumption 5 of Theorem 3.57 is satisfied[47]. Hence, it remains to show that Assumption 4 of Theorem 3.57 is satisfied. In other words, we must prove that we have $\psi_P(a) \equiv \varphi_\pi(\psi_{P/\pi}(a)) \bmod \pi^{v_\pi(P)} A$ for every $a \in A$, every $P \in N$ and every $\pi \in \operatorname{PF} P$.

So let us fix $a \in A$, $P \in N$ and $\pi \in \operatorname{PF} P$. Clearly, $\pi \mid P$ (since $\pi \in \operatorname{PF} P$), and π is a monic irreducible polynomial in $\mathbb{F}_q[T]$ (since $\pi \in \operatorname{PF} P$). From these two facts, we obtain $\pi \in N$ (since N is a q-nest). Thus, Assumption 2 of Theorem 3.57 yields $\varphi_\pi(a) \equiv (\operatorname{Carl} \pi)(a) \bmod \pi A$.

Also, $P/\pi \in \mathbb{F}_q[T]$ (since $\pi \mid P$). Hence, $\psi_{P/\pi}(a) = (\operatorname{Carl}(P/\pi))(a)$ (by the definition of $\psi_{P/\pi}$).

[47] *Proof.* We have $\operatorname{Carl} 1 = 1$ (since Carl is an $\mathbb{F}_q$-algebra homomorphism). Now, every $a \in A$ satisfies

$$\begin{aligned}\psi_1(a) &= \underbrace{(\operatorname{Carl} 1)}_{=1} a \qquad \text{(by the definition of } \psi_1\text{)} \\ &= 1a = a = \operatorname{id}(a).\end{aligned}$$

In other words, $\psi_1 = 1$. In other words, Assumption 5 of Theorem 3.57 is satisfied, qed.

Corollary 3.48 **(b)** (applied to P/π, $\varphi_\pi(a)$ and $(\operatorname{Carl}\pi)\,a$ instead of N, a and b) shows that

$$(\operatorname{Carl}(P/\pi))(\varphi_\pi(a)) \equiv (\operatorname{Carl}(P/\pi))((\operatorname{Carl}\pi)\,a) \bmod \pi^{v_\pi(P/\pi)+1}A.$$

In view of

$$v_\pi(P/\pi) + \underbrace{1}_{=v_\pi(\pi)} = v_\pi(P/\pi) + v_\pi(\pi) = v_\pi\left(\underbrace{(P/\pi)\,\pi}_{=P}\right) = v_\pi(P),$$

this rewrites as

$$(\operatorname{Carl}(P/\pi))(\varphi_\pi(a)) \equiv (\operatorname{Carl}(P/\pi))((\operatorname{Carl}\pi)\,a) \bmod \pi^{v_\pi(P)}A. \tag{84}$$

But φ_π is an endomorphism of the $\mathcal{F}$-module A (by Assumption 1 of Theorem 3.57, applied to π instead of P). Hence,

$$(\operatorname{Carl}(P/\pi))(\varphi_\pi(a)) = \varphi_\pi\left(\underbrace{(\operatorname{Carl}(P/\pi))(a)}_{=\psi_{P/\pi}(a)}\right) = \varphi_\pi(\psi_{P/\pi}(a)).$$

Thus,

$$\begin{aligned}
\varphi_\pi(\psi_{P/\pi}(a)) &= (\operatorname{Carl}(P/\pi))(\varphi_\pi(a)) \equiv (\operatorname{Carl}(P/\pi))((\operatorname{Carl}\pi)\,a) \qquad \text{(by (84))} \\
&= \underbrace{(\operatorname{Carl}(P/\pi)\cdot\operatorname{Carl}\pi)}_{\substack{=\operatorname{Carl}((P/\pi)\pi) \\ \text{(since Carl is an } \mathbb{F}_q\text{-algebra} \\ \text{homomorphism)}}} a \\
&= \left(\operatorname{Carl}\underbrace{((P/\pi)\,\pi)}_{=P}\right) a = (\operatorname{Carl}P)\,a \\
&= \psi_P(a) \bmod \pi^{v_\pi(P)}A
\end{aligned}$$

(since $\psi_P(a) = (\operatorname{Carl}P)\,a$ (by the definition of ψ_P)). In other words, $\psi_P(a) \equiv \varphi_\pi(\psi_{P/\pi}(a)) \bmod \pi^{v_\pi(P)}A$. Thus, Assumption 4 of Theorem 3.57 is satisfied. This proves Proposition 3.59. □

Proof of Proposition 3.60. Assumption 5 of Theorem 3.57 is satisfied[48]. Hence, it remains to show that Assumption 4 of Theorem 3.57 is satisfied. In other

[48] *Proof.* Every $a \in A$ satisfies

$$\begin{aligned}
\psi_1(a) &= F^{\deg 1}a \qquad \text{(by the definition of } \psi_1\text{)} \\
&= 1a \qquad \left(\text{since } \deg 1 = 0 \text{ and thus } F^{\deg 1} = F^0 = 1\right) \\
&= a = \operatorname{id}(a).
\end{aligned}$$

In other words, $\psi_1 = 1$. In other words, Assumption 5 of Theorem 3.57 is satisfied, qed.

words, we must prove that we have $\psi_P(a) \equiv \varphi_\pi(\psi_{P/\pi}(a)) \bmod \pi^{v_\pi(P)}A$ for every $a \in A$, every $P \in N$ and every $\pi \in \operatorname{PF} P$.

So let us fix $a \in A$, $P \in N$ and $\pi \in \operatorname{PF} P$. Clearly, $\pi \mid P$ (since $\pi \in \operatorname{PF} P$), and π is a monic irreducible polynomial in $\mathbb{F}_q[T]$ (since $\pi \in \operatorname{PF} P$). From these two facts, we obtain $\pi \in N$ (since N is a q-nest). Thus, Assumption 2 of Theorem 3.57 yields $\varphi_\pi(a) \equiv (\operatorname{Carl}\pi)(a) \bmod \pi A$. Thus,

$$\varphi_\pi(a) \equiv (\operatorname{Carl}\pi)(a) \equiv F^{\deg\pi} a \bmod \pi A \tag{85}$$

(by Corollary 3.42).

Also, $P/\pi \in \mathbb{F}_q[T]$ (since $\pi \mid P$). Hence, $\psi_{P/\pi}(a) = F^{\deg(P/\pi)}(a)$ (by the definition of $\psi_{P/\pi}$).

Corollary 3.48 **(a)** (applied to P/π, $\varphi_\pi(a)$ and $F^{\deg\pi}a$ instead of N, a and b) shows that

$$F^{\deg(P/\pi)}(\varphi_\pi(a)) \equiv F^{\deg(P/\pi)}\left(F^{\deg\pi}a\right) \bmod \pi^{v_\pi(P/\pi)+1}A.$$

In view of

$$v_\pi(P/\pi) + \underbrace{1}_{=v_\pi(\pi)} = v_\pi(P/\pi) + v_\pi(\pi) = v_\pi\left(\underbrace{(P/\pi)\,\pi}_{=P}\right) = v_\pi(P),$$

this rewrites as

$$F^{\deg(P/\pi)}(\varphi_\pi(a)) \equiv F^{\deg(P/\pi)}\left(F^{\deg\pi}a\right) \bmod \pi^{v_\pi(P)}A. \tag{86}$$

But φ_π is an endomorphism of the $\mathcal{F}$-module A (by Assumption 1 of Theorem 3.57, applied to π instead of P). Hence,

$$F^{\deg(P/\pi)}(\varphi_\pi(a)) = \varphi_\pi\left(\underbrace{F^{\deg(P/\pi)}(a)}_{=\psi_{P/\pi}(a)}\right) = \varphi_\pi(\psi_{P/\pi}(a)).$$

Thus,

$$\begin{aligned}
\varphi_\pi(\psi_{P/\pi}(a)) &= F^{\deg(P/\pi)}(\varphi_\pi(a)) \equiv F^{\deg(P/\pi)}\left(F^{\deg\pi}a\right) && \text{(by (86))} \\
&= \underbrace{\left(F^{\deg(P/\pi)}F^{\deg\pi}\right)}_{\substack{=F^{\deg(P/\pi)+\deg\pi}=F^{\deg P} \\ (\text{since } \deg(P/\pi)+\deg\pi=\deg P \\ (\text{since } \deg(P/\pi)=\deg P-\deg\pi))}} a = F^{\deg P}a \\
&= \psi_P(a) \bmod \pi^{v_\pi(P)}A
\end{aligned}$$

(since $\psi_P(a) = F^{\deg P}a$ (by the definition of ψ_P)). In other words, $\psi_P(a) \equiv \varphi_\pi(\psi_{P/\pi}(a)) \bmod \pi^{v_\pi(P)}A$. Thus, Assumption 4 of Theorem 3.57 is satisfied. This proves Proposition 3.60. □

Proof of Proposition 3.61. Assumption 5 of Theorem 3.57 is satisfied[49]. Hence, it remains to show that Assumption 4 of Theorem 3.57 is satisfied. In other words, we must prove that we have $\psi_P(a) \equiv \varphi_\pi(\psi_{P/\pi}(a)) \bmod \pi^{v_\pi(P)}A$ for every $a \in A$, every $P \in N$ and every $\pi \in \operatorname{PF} P$.

So let us fix $a \in A$, $P \in N$ and $\pi \in \operatorname{PF} P$. Clearly, $\pi \mid P$ (since $\pi \in \operatorname{PF} P$), and π is a monic irreducible polynomial in $\mathbb{F}_q[T]$ (since $\pi \in \operatorname{PF} P$). From these two facts, we obtain $\pi \in N$ (since N is a q-nest). Also, P/π is a monic polynomial in $\mathbb{F}_q[T]$ (since P and π are monic and since $\pi \mid P$), and divides P. Therefore, $P/\pi \in N$ (since $P \in N$). Now, the second sentence of Assumption 3 of Theorem 3.57 (applied to π and P/π instead of P and Q) shows that $\varphi_\pi \circ \varphi_{P/\pi} = \varphi_{\pi\cdot(P/\pi)}$ (since $\pi \cdot (P/\pi) = P \in N$). Since $\pi \cdot (P/\pi) = P$, this rewrites as $\varphi_\pi \circ \varphi_{P/\pi} = \varphi_P$. But the definition of ψ_P yields $\psi_P = \varphi_P$. Hence, $\psi_P = \varphi_P = \varphi_\pi \circ \varphi_{P/\pi}$, so that

$$\underbrace{\psi_P}_{=\varphi_\pi\circ\varphi_{P/\pi}}(a) = (\varphi_\pi \circ \varphi_{P/\pi})(a) = \varphi_\pi(\varphi_{P/\pi}(a)). \tag{87}$$

On the other hand, the definition of $\psi_{P/\pi}$ yields $\psi_{P/\pi} = \varphi_{P/\pi}$. Thus, (87) rewrites as $\psi_P(a) = \varphi_\pi(\psi_{P/\pi}(a))$. Therefore, $\psi_P(a) \equiv \varphi_\pi(\psi_{P/\pi}(a)) \bmod \pi^{v_\pi(P)}A$. Thus, Assumption 4 of Theorem 3.57 is satisfied. This proves Proposition 3.61. □

Let us now turn to the proof of Theorem 3.57[50]:

Proof of Theorem 3.57. We shall prove the two implications $\mathcal{C}_1 \Longrightarrow \mathcal{E}_\psi$ and $\mathcal{E}_\psi \Longrightarrow \mathcal{C}_1$ separately:

Proof of the implication $\mathcal{E}_\psi \Longrightarrow \mathcal{C}_1$: Assume that Assertion $\mathcal{E}_\psi$ holds. That is, there exists a family $(z_P)_{P\in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D\mid P} D\psi_{P/D}(z_D) \text{ for every } P \in N \right). \tag{88}$$

Consider this family $(z_P)_{P\in N}$.

We need to prove that Assertion $\mathcal{C}_1$ holds, i.e., that every $P \in N$ and every $\pi \in \operatorname{PF} P$ satisfy

$$\varphi_\pi(b_{P/\pi}) \equiv b_P \bmod \pi^{v_\pi(P)}A. \tag{89}$$

So let us fix a $P \in N$ and a $\pi \in \operatorname{PF} P$. We need to prove (89).

The polynomial P is monic (since $P \in N$). We have $\pi \in \operatorname{PF} P$. Thus, π is a monic irreducible divisor of P. Hence, P/π is a monic polynomial in $\mathbb{F}_q[T]$ (since P and π are monic). Since N is a q-nest, we obtain $P/\pi \in N$ (since $P \in N$, and since P/π is a monic divisor of N). Since N is a q-nest, we also obtain $\pi \in N$ (since $P \in N$, and since π is a monic divisor of N).

[49] *Proof.* Assumption 3 of Theorem 3.57 shows that $\varphi_1 = 1$. Now, the definition of ψ_1 yields $\psi_1 = \varphi_1 = 1$. In other words, Assumption 5 of Theorem 3.57 is satisfied, qed.

[50] Our proof imitates [6, solution to Exercise 2.9.6].

Assumption 1 (applied to π instead of P) shows that φ_π is an endomorphism of the $\mathcal{F}$-module A.

Applying (88) to P/π instead of P, we obtain $b_{P/\pi} = \sum_{D|P/\pi} D\psi_{(P/\pi)/D}(z_D)$. Applying the map φ_π to both sides of this equality, we obtain

$$\varphi_\pi(b_{P/\pi}) = \varphi_\pi\left(\sum_{D|P/\pi} D\psi_{(P/\pi)/D}(z_D)\right) = \sum_{D|P/\pi} D\varphi_\pi\left(\psi_{(P/\pi)/D}(z_D)\right) \quad (90)$$

(since φ_π is an endomorphism of the $\mathcal{F}$-module A). On the other hand, every monic divisor D of P/π satisfies

$$D\psi_{P/D}(z_D) \equiv D\varphi_\pi\left(\psi_{(P/\pi)/D}(z_D)\right) \bmod \pi^{v_\pi(P)}A \quad (91)$$

[51]. Now,

$$\begin{aligned}
&\sum_{D|P} D\psi_{P/D}\left(z_D\right) \\
&= \underbrace{\sum_{\substack{D|P; \\ D|P/\pi}} D\psi_{P/D}\left(z_D\right)}_{=\sum_{D|P/\pi} D\psi_{P/D}\left(z_D\right)} + \sum_{\substack{D|P; \\ D\nmid P/\pi}} \underbrace{D\psi_{P/D}\left(z_D\right)}_{\substack{\equiv 0 \bmod \pi^{v_\pi(P)}A \\ \text{(since Lemma 3.54 shows that} \\ \pi^{v_\pi(P)} \mid D)}} \\
&\equiv \sum_{D|P/\pi} D\psi_{P/D}\left(z_D\right) + \underbrace{\sum_{\substack{D|P; \\ D\nmid P/\pi}} 0}_{=0} = \sum_{D|P/\pi} \underbrace{D\psi_{P/D}\left(z_D\right)}_{\substack{\equiv D\varphi_\pi\left(\psi_{(P/\pi)/D}\left(z_D\right)\right) \bmod \pi^{v_\pi(P)}A \\ \text{(by (91))}}} \qquad (92) \\
&\equiv \sum_{D|P/\pi} D\varphi_\pi\left(\psi_{(P/\pi)/D}\left(z_D\right)\right) \qquad (93) \\
&= \varphi_\pi\left(b_{P/\pi}\right) \bmod \pi^{v_\pi(P)}A \qquad (94)
\end{aligned}$$

[51] *Proof of (91):* Let D be a monic divisor of P/π. Thus, $D \mid P/\pi$, so that $D \mid P/\pi \mid P$ and therefore $P/D \in \mathbb{F}_q[T]$.

Also, $\dfrac{P/D}{\pi} = \dfrac{P/\pi}{D} \in \mathbb{F}_q[T]$ (since $D \mid P/\pi$). In other words, $\pi \mid P/D$ (since $P/D \in \mathbb{F}_q[T]$). Hence, $\pi \in \operatorname{PF}(P/D)$ (since π is monic irreducible). Also, P/D is a monic divisor of P (since P and D are monic, and since $D \mid P$); thus, $P/D \in N$ (since $P \in N$ and since N is a q-nest). Hence, Assumption 4 (applied to z_D and P/D instead of a and P) yields

$$\psi_{P/D}\left(z_D\right) \equiv \varphi_\pi\left(\psi_{(P/D)/\pi}\left(z_D\right)\right) \bmod \pi^{v_\pi(P/D)}A.$$

In other words, $\psi_{P/D}\left(z_D\right) - \varphi_\pi\left(\psi_{(P/D)/\pi}\left(z_D\right)\right) \in \pi^{v_\pi(P/D)}A$. Since $(P/D)/\pi = (P/\pi)/D$, this rewrites as $\psi_{P/D}\left(z_D\right) - \varphi_\pi\left(\psi_{(P/\pi)/D}\left(z_D\right)\right) \in \pi^{v_\pi(P/D)}A$.

Now,

$$\begin{aligned}
&D\psi_{P/D}\left(z_D\right) - D\varphi_\pi\left(\psi_{(P/\pi)/D}\left(z_D\right)\right) \\
&= D\underbrace{\left(\psi_{P/D}\left(z_D\right) - \varphi_\pi\left(\psi_{(P/\pi)/D}\left(z_D\right)\right)\right)}_{\in \pi^{v_\pi(P/D)}A} \\
&\in D\pi^{v_\pi(P/D)}A = \pi^{v_\pi(P/D)} \underbrace{DA}_{\substack{\subseteq \pi^{v_\pi(D)}A \\ \text{(since } \pi^{v_\pi(D)} \mid D\text{)}}} \subseteq \underbrace{\pi^{v_\pi(P/D)}\pi^{v_\pi(D)}}_{=\pi^{v_\pi(P/D)+v_\pi(D)}}A \\
&= \pi^{v_\pi(P/D)+v_\pi(D)}A = \pi^{v_\pi(P)}A
\end{aligned}$$

(since $v_\pi(P/D) + v_\pi(D) = v_\pi\left(\underbrace{(P/D)\,D}_{=P}\right) = v_\pi(P)$). In other words, $D\psi_{P/D}\left(z_D\right) \equiv D\varphi_\pi\left(\psi_{(P/\pi)/D}\left(z_D\right)\right) \bmod \pi^{v_\pi(P)}A$. This proves (91).

(by (90)). But (88) yields

$$b_P = \sum_{D|P} D\psi_{P/D}\left(z_D\right) \equiv \varphi_\pi\left(b_{P/\pi}\right) \bmod \pi^{v_\pi(P)} A$$

(by (94)). Thus, (89) is proven. In other words, Assertion $\mathcal{C}_1$ holds. This completes the proof of the implication $\mathcal{E}_\psi \Longrightarrow \mathcal{C}_1$.

Proof of the implication $\mathcal{C}_1 \Longrightarrow \mathcal{E}_\psi$: Assume that Assertion $\mathcal{C}_1$ holds. In other words, every $P \in N$ and every $\pi \in \operatorname{PF} P$ satisfy

$$\varphi_\pi\left(b_{P/\pi}\right) \equiv b_P \bmod \pi^{v_\pi(P)} A. \tag{95}$$

We now need to prove that Assertion $\mathcal{E}_\psi$ holds as well. In other words, we need to show that there exists a family $(z_P)_{P\in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D|P} D\psi_{P/D}\left(z_D\right) \text{ for every } P \in N \right).$$

In other words (renaming P as Q), we need to show that there exists a family $\left(z_Q\right)_{Q\in N} \in A^N$ of elements of A such that

$$\left(b_Q = \sum_{D|Q} D\psi_{Q/D}\left(z_D\right) \text{ for every } Q \in N \right).$$

We construct this family $\left(z_Q\right)_{Q\in N}$ recursively, by induction over $\deg Q$. So we fix some $P \in N$, and assume that an element z_Q of A is already constructed for every $Q \in N$ satisfying $\deg Q < \deg P$; we furthermore assume that these z_Q satisfy

$$b_Q = \sum_{D|Q} D\psi_{Q/D}\left(z_D\right) \tag{96}$$

for every $Q \in N$ satisfying $\deg Q < \deg P$. We now need to construct a $z_P \in A$ such that (96) is satisfied for $Q = P$. In other words, we need to construct a $z_P \in A$ satisfying $b_P = \sum_{D|P} D\psi_{P/D}\left(z_D\right)$.

Let us first choose z_P **arbitrarily** (with the intention to tweak it later). Let $\pi \in \operatorname{PF} P$ be arbitrary. Thus, π is a monic irreducible divisor of P. Then, the polynomial P/π is monic (since P and π are monic), and is a divisor of P; hence, $P/\pi \in N$ (since $P \in N$, and since N is a q-nest). Moreover, it satisfies $\deg\left(P/\pi\right) = \deg P - \underbrace{\deg \pi}_{>0} < \deg P$. Hence, (96) (applied to $Q = P/\pi$) shows that

$$b_{P/\pi} = \sum_{D|P/\pi} D\psi_{(P/\pi)/D}\left(z_D\right).$$

Thus, (94) holds (indeed, this can be proven precisely as in our proof of the implication $\mathcal{E}_\psi \Longrightarrow \mathcal{C}_1$ above). Hence,

$$\sum_{D|P} D\psi_{P/D}\left(z_D\right) \equiv \varphi_\pi\left(b_{P/\pi}\right) \equiv b_P \bmod \pi^{v_\pi(P)} A$$

(by (95)). In other words, $b_P \equiv \sum_{D|P} D\psi_{P/D}\left(z_D\right) \bmod \pi^{v_\pi(P)} A$. In other words, $b_P - \sum_{D|P} D\psi_{P/D}\left(z_D\right) \in \pi^{v_\pi(P)} A$.

Now, let us forget that we fixed π. We thus have shown (for our arbitrarily chosen z_P) that

$$b_P - \sum_{D|P} D\psi_{P/D}\left(z_D\right) \in \pi^{v_\pi(P)} A \qquad \text{for each } \pi \in \operatorname{PF} P.$$

As a consequence,

$$b_P - \sum_{D|P} D\psi_{P/D}\left(z_D\right) \in \bigcap_{\pi \in \operatorname{PF} P} \pi^{v_\pi(P)} A = PA$$

(by Corollary 3.51). In other words, there exists a $\gamma \in A$ such that

$$b_P - \sum_{D|P} D\psi_{P/D}\left(z_D\right) = P\gamma.$$

Consider this γ.

We have assumed that Assumption 5 of Theorem 3.57 is satisfied. In other words, $\psi_1 = \mathrm{id}$. Hence,

$$\begin{aligned} & P\psi_{P/P}\left(z_P + \gamma\right) - P\psi_{P/P}\left(z_P\right) \\ & = P\,\mathrm{id}\left(z_P + \gamma\right) - P\,\mathrm{id}\left(z_P\right) \qquad \left(\text{since } \psi_{P/P} = \psi_1 = \mathrm{id}\right) \\ & = P \cdot \left(z_P + \gamma\right) - P \cdot z_P = P\gamma \\ & = b_P - \sum_{D|P} D\psi_{P/D}\left(z_D\right). \end{aligned}$$

In other words,

$$\begin{aligned} & \sum_{D|P} D\psi_{P/D}\left(z_D\right) + \left(P\psi_{P/P}\left(z_P + \gamma\right) - P\psi_{P/P}\left(z_P\right)\right) \\ & = b_P. \end{aligned} \tag{97}$$

Now, if we replace z_P by $z_P + \gamma$, then the sum $\sum_{D|P} D\psi_{P/D}\left(z_D\right)$ increases by $P\psi_{P/P}\left(z_P + \gamma\right) - P\psi_{P/P}\left(z_P\right)$ (because the only addend of the sum that changes is the addend for $D = P$), and thus the new value of this sum is b_P (by (97)).

Hence, by replacing z_P by $z_P + \gamma$, we achieve that $b_P = \sum_{D|P} D\psi_{P/D}(z_D)$ holds. Thus, we have found the z_P we were searching for, and the recursive construction of the family $(z_Q)_{Q \in N}$ has proceeded by one more step. The proof of the implication $\mathcal{C}_1 \Longrightarrow \mathcal{E}_\psi$ is thus complete.

We have now proven both implications $\mathcal{C}_1 \Longrightarrow \mathcal{E}_\psi$ and $\mathcal{E}_\psi \Longrightarrow \mathcal{C}_1$. Combining them, we obtain the equivalence $\mathcal{C}_1 \Longleftrightarrow \mathcal{E}_\psi$. Thus, Theorem 3.57 is proven. □

3.14. $\mathbb{F}_q[T]_+$-analogues of the Möbius and Euler totient functions

Next, we shall discuss the functions μ, φ and φ_C introduced in Section 1. Let me first repeat their definitions:

Definition 3.62. Define a function $\mu : \mathbb{F}_q[T]_+ \to \{-1, 0, 1\}$ by

$$\mu(M) = \begin{cases} (-1)^{|\operatorname{PF} M|}, & \text{if } M \text{ is squarefree;} \\ 0, & \text{if } M \text{ is not squarefree} \end{cases} \qquad \text{for all } M \in \mathbb{F}_q[T]_+ .$$

(Recall that a monic polynomial $M \in \mathbb{F}_q[T]_+$ is said to be *squarefree* if it satisfies the following three equivalent conditions:

- No nonconstant polynomial $P \in \mathbb{F}_q[T]$ satisfies $P^2 \mid M$.
- Every monic irreducible polynomial $\pi \in \mathbb{F}_q[T]$ satisfies $v_\pi(M) \leq 1$.
- The polynomial M is a product of pairwise distinct monic irreducible polynomials.

) The function μ is called the *Möbius function on* $\mathbb{F}_q[T]_+$.

Definition 3.63. Define a function $\varphi_C : \mathbb{F}_q[T]_+ \to \mathbb{F}_q[T]$ by

$$\varphi_C(M) = \sum_{D|M} \mu(D) \frac{M}{D} \qquad \text{for all } M \in \mathbb{F}_q[T]_+ .$$

Definition 3.64. Define a function $\varphi : \mathbb{F}_q[T]_+ \to \mathbb{Z}$ by

$$\varphi(M) = \sum_{D|M} \mu(D) q^{\deg(M/D)} \qquad \text{for all } M \in \mathbb{F}_q[T]_+ .$$

The function μ is an analogue of the number-theoretical Möbius function, whereas the functions φ_C and φ are two distinct analogues of the Euler totient

function. These functions have a number of properties (some well-known) that often imitate analogous properties of the number-theoretical Möbius function and the Euler totient function. See [3, Theorem 4.5] for some properties of φ_C, and see [3, Section 6] for the function φ. We shall prove a number of their properties, many of which will be used below. We begin by citing a well-known combinatorial fact:

Lemma 3.65. Let Z be a finite set.

(a) We have

$$\sum_{I \subseteq Z} (-1)^{|I|} = [Z = \varnothing] .$$

(b) Let R be a commutative ring. Let r_i be an element of R for each $i \in Z$. Then,

$$\sum_{I \subseteq Z} \prod_{i \in I} r_i = \prod_{i \in Z} (1 + r_i) .$$

Proof of Lemma 3.65. Lemma 3.65 **(b)** can be proven by induction over $|Z|$ (or, less rigorously, just by expanding the product $\prod_{i \in Z} (1 + r_i)$). Lemma 3.65 **(a)** can be proven in many ways (e.g., it can be obtained by setting $R = \mathbb{Z}$ and $r_i = -1$ in Lemma 3.65 **(b)**). □

Proposition 3.66. Let $M \in \mathbb{F}_q[T]_+$. Then, $\sum_{D|M} \mu(D) = [M = 1]$. Here, we are using the *Iverson bracket notation*: If $\mathcal{A}$ is any logical statement, then $[\mathcal{A}]$ stands for the integer $\begin{cases} 1, & \text{if } \mathcal{A} \text{ is true;} \\ 0, & \text{if } \mathcal{A} \text{ is false} \end{cases}$.

Proof of Proposition 3.66. (This proof is a carbon copy of [6, proof of (12.68.3)], with minor changes.)

Let $M = P_1^{a_1} P_2^{a_2} \cdots P_k^{a_k}$ be the factorization of M into monic irreducible polynomials, with all of $a_1, a_2, \ldots, a_k$ being positive integers (and with $P_1, P_2, \ldots, P_k$ being distinct).[52] Then, the **squarefree** monic divisors D of M all have the form $\prod_{i \in I} P_i$ for some subset I of $\{1, 2, \ldots, k\}$. More precisely, there exists a bijection

$$\{I \subseteq \{1, 2, \ldots, k\}\} \to (\text{the set of all squarefree monic divisors of } M), \quad I \mapsto \prod_{i \in I} P_i. \tag{98}$$

Moreover, every subset I of $\{1, 2, \ldots, k\}$ satisfies $\operatorname{PF}\left(\prod_{i \in I} P_i\right) = \{P_i \mid i \in I\}$ and thus

$$\left|\operatorname{PF}\left(\prod_{i \in I} P_i\right)\right| = |\{P_i \mid i \in I\}| = |I| \tag{99}$$

[52] This is well-defined, since M is monic and since $\mathbb{F}_q[T]$ is a principal ideal domain. Of course, k can be 0 (when $M = 1$).

(since $P_1, P_2, \ldots, P_k$ are distinct) and therefore

$$\mu\left(\prod_{i\in I} P_i\right) = (-1)^{\left|\mathrm{PF}\left(\prod_{i\in I} P_i\right)\right|} \qquad \left(\text{since } \prod_{i\in I} P_i \text{ is squarefree}\right)$$
$$= (-1)^{|I|} \qquad (\text{by (99)}). \tag{100}$$

Now,

$$\sum_{D|M} \mu(D) = \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D) + \sum_{\substack{D|M; \\ D \text{ is not squarefree}}} \underbrace{\mu(D)}_{\substack{=0 \\ \text{(by the definition of } \mu\text{, since } D \text{ is not squarefree)}}}$$
$$= \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D) + \underbrace{\sum_{\substack{D|M; \\ D \text{ is not squarefree}}} 0}_{=0} = \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D)$$
$$= \sum_{I\subseteq\{1,2,\ldots,k\}} \underbrace{\mu\left(\prod_{i\in I} P_i\right)}_{\substack{=(-1)^{|I|} \\ \text{(by (100))}}} \qquad \left(\begin{array}{c}\text{here, we have substituted } \prod_{i\in I} P_i \text{ for } D \\ \text{due to the bijection (98)}\end{array}\right)$$
$$= \sum_{I\subseteq\{1,2,\ldots,k\}} (-1)^{|I|} = \left[\underbrace{\{1,2,\ldots,k\} = \varnothing}_{\text{This is equivalent to } k=0}\right]$$
$$\text{(by Lemma 3.65 \textbf{(a)}, applied to } Z = \{1,2,\ldots,k\})$$
$$= [k = 0] = [M \text{ is constant}]$$
$$\left(\begin{array}{c}\text{since } k \text{ is the number of monic irreducible divisors of } M, \\ \text{and thus we have } k = 0 \text{ if and only if } M \text{ is constant}\end{array}\right)$$
$$= [M = 1] \qquad (\text{since } M \text{ is monic}).$$

This proves Proposition 3.66. □

Let us explicitly state a simple consequence of Proposition 3.66 for the sake of convenience:

Corollary 3.67. Let $M \in \mathbb{F}_q[T]_+$. Let E be a monic divisor of M. Then,

$$\sum_{\substack{B|M; \\ BE|M}} \mu(B) = [E = M].$$

Proof of Corollary 3.67. We have $\dfrac{M}{E} \in \mathbb{F}_q[T]$ (since E is a divisor of M). Moreover, the polynomial $\dfrac{M}{E}$ is monic (since M and E are monic). Hence, $\dfrac{M}{E} \in \mathbb{F}_q[T]_+$. Proposition 3.66 (applied to $\dfrac{M}{E}$ instead of M) thus shows that $\sum\limits_{D \mid \frac{M}{E}} \mu(D) = \left[\underbrace{\frac{M}{E} = 1}_{\text{This is equivalent to } E=M} \right] = [E = M]$.

But $E \mid M$. Hence, the monic divisors B of M satisfying $BE \mid M$ are exactly the monic divisors B of $\dfrac{M}{E}$. Therefore, $\sum\limits_{\substack{B \mid M; \\ BE \mid M}} = \sum\limits_{B \mid \frac{M}{E}}$. Thus,

$$\begin{aligned}
\underbrace{\sum_{\substack{B \mid M; \\ BE \mid M}} \mu(B)}_{= \sum\limits_{B \mid \frac{M}{E}}} &= \sum_{B \mid \frac{M}{E}} \mu(B) = \sum_{D \mid \frac{M}{E}} \mu(D) \\
&\qquad \left(\text{here, we renamed the summation index } B \text{ as } D\right) \\
&= [E = M].
\end{aligned}$$

Corollary 3.67 is therefore proven. □

Next come some simple properties of φ_C:

Proposition 3.68. Let $M \in \mathbb{F}_q[T]_+$.
(a) We have $\varphi_C(M) \in \mathbb{F}_q[T]_+$.
(b) We have $\varphi_C(M) = M \prod\limits_{\pi \in \mathrm{PF}\, M} \left(1 - \dfrac{1}{\pi}\right)$.
(c) We have $\varphi_C(M) = \sum\limits_{D \mid M} D\mu\left(\dfrac{M}{D}\right)$.

Proof of Proposition 3.68. **(a)** Let $d = \deg M$. Then, the polynomial M is monic of degree d.

Now, let V_d be the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q[T]$ consisting of all polynomials of degree $\leq d-1$. (This subspace is spanned by $T^0, T^1, \ldots, T^{d-1}$.) Then, the monic polynomials in $\mathbb{F}_q[T]$ of degree d are precisely the polynomials in $\mathbb{F}_q[T]$ that are congruent to T^d modulo V_d. Thus, the polynomial M is congruent to T^d modulo V_d (since M is monic of degree d). In other words, $M \equiv T^d \bmod V_d$.

If D is a monic divisor of M satisfying $D \neq 1$, then

$$\mu(D)\frac{M}{D} \equiv 0 \bmod V_d \tag{101}$$

[53]. Now, the definition of φ_C yields

$$\begin{aligned}
\varphi_C(M) &= \sum_{D|M} \mu(D)\frac{M}{D} \\
&= \underbrace{\mu(1)}_{=1}\underbrace{\frac{M}{1}}_{=M\equiv T^d \bmod V_d} + \sum_{\substack{D|M;\\ D\neq 1}} \underbrace{\mu(D)\frac{M}{D}}_{\substack{\equiv 0 \bmod V_d \\ \text{(by (101))}}} \\
&\qquad \text{(here, we have split off the addend for } D=1 \text{ from the sum)} \\
&\equiv T^d + \underbrace{\sum_{\substack{D|M;\\ D\neq 1}} 0}_{=0} = T^d \bmod V_d.
\end{aligned}$$

In other words, the polynomial $\varphi_C(M)$ is congruent to T^d modulo V_d. In other words, the polynomial $\varphi_C(M)$ is monic of degree d (since the monic polynomials in $\mathbb{F}_q[T]$ of degree d are precisely the polynomials in $\mathbb{F}_q[T]$ that are congruent to T^d modulo V_d). Hence, $\varphi_C(M) \in \mathbb{F}_q[T]_+$. This proves Proposition 3.68 **(a)**.

(b) Let $M = P_1^{a_1}P_2^{a_2}\cdots P_k^{a_k}$ be the factorization of M into monic irreducible polynomials, with all of $a_1, a_2, \ldots, a_k$ being positive integers (and with $P_1, P_2, \ldots, P_k$ being distinct).[54] Then, the **squarefree** monic divisors D of M all have the form $\prod_{i\in I} P_i$ for some subset I of $\{1,2,\ldots,k\}$. More precisely, there exists a bijection

$$\begin{aligned}
\{I \subseteq \{1,2,\ldots,k\}\} &\to (\text{the set of all squarefree monic divisors of } M), \\
I &\mapsto \prod_{i\in I} P_i.
\end{aligned} \tag{102}$$

[53] *Proof of (101):* Let D be a monic divisor of M satisfying $D \neq 1$.

We have $\frac{M}{D} \in \mathbb{F}_q[T]$ (since D is a divisor of M). If we had $\deg D = 0$, then we would have $D = 1$ (because D is monic), which would contradict $D \neq 1$. Thus, we cannot have $\deg D = 0$. Hence, we must have $\deg D \geq 1$ (since $D \in \mathbb{F}_q[T]$). Thus, the polynomial $\frac{M}{D} \in \mathbb{F}_q[T]$ satisfies $\deg\frac{M}{D} = \underbrace{\deg M}_{=d} - \underbrace{\deg D}_{\geq 1} \leq d-1$. Hence, $\frac{M}{D}$ is a polynomial of degree $\leq d-1$. In other words, $\frac{M}{D} \in V_d$ (since V_d is the $\mathbb{F}_q$-vector subspace of $\mathbb{F}_q[T]$ consisting of all polynomials of degree $\leq d-1$). In other words, $\frac{M}{D} \equiv 0 \bmod V_d$. Hence, $\mu(D)\frac{M}{D} \equiv 0 \bmod V_d$ as well (since $\mu(D) \in \{-1,0,1\} \subseteq \mathbb{Z}$). This proves (101).

[54] This is well-defined, since M is monic and since $\mathbb{F}_q[T]$ is a principal ideal domain. Of course, k can be 0 (when $M = 1$).

Moreover, every subset I of $\{1,2,\ldots,k\}$ satisfies (100). (This is proven as in our proof of Proposition 3.66.)

The definition of $P_1, P_2, \ldots, P_k$ shows that $(P_1, P_2, \ldots, P_k)$ is a list of all prime factors of M, with no repetitions. Thus, the map $\{1,2,\ldots,k\} \to \operatorname{PF} M$, $i \mapsto P_i$ is a bijection.

The definition of φ_C yields

$$\varphi_C(M) = \sum_{D|M} \mu(D) \frac{M}{D} = \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D) \frac{M}{D} + \sum_{\substack{D|M; \\ D \text{ is not squarefree}}} \underbrace{\mu(D)}_{\substack{=0 \\ \text{(by the definition of } \mu\text{, since } D \\ \text{is not squarefree)}}} \frac{M}{D}$$

$$= \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D) \frac{M}{D} + \underbrace{\sum_{\substack{D|M; \\ D \text{ is not squarefree}}} 0 \frac{M}{D}}_{=0} = \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D) \frac{M}{D}$$

$$= \sum_{I \subseteq \{1,2,\ldots,k\}} \underbrace{\mu\left(\prod_{i \in I} P_i\right)}_{\substack{=(-1)^{|I|} \\ \text{(by (100))}}} \frac{M}{\prod_{i \in I} P_i}$$

$$\left(\begin{array}{c} \text{here, we have substituted } \prod_{i \in I} P_i \text{ for } D \\ \text{due to the bijection (98)} \end{array} \right)$$

$$= \sum_{I \subseteq \{1,2,\ldots,k\}} \underbrace{(-1)^{|I|}}_{=\prod_{i \in I}(-1)} \frac{M}{\prod_{i \in I} P_i} = \sum_{I \subseteq \{1,2,\ldots,k\}} \left(\prod_{i \in I} (-1)\right) \frac{M}{\prod_{i \in I} P_i}$$

$$= M \sum_{I \subseteq \{1,2,\ldots,k\}} \underbrace{\frac{\prod_{i \in I}(-1)}{\prod_{i \in I} P_i}}_{=\prod_{i \in I} \frac{-1}{P_i}} = M \underbrace{\sum_{I \subseteq \{1,2,\ldots,k\}} \prod_{i \in I} \frac{-1}{P_i}}_{\substack{= \prod_{i \in \{1,2,\ldots,k\}} \left(1 + \frac{-1}{P_i}\right) \\ \text{(by Lemma 3.65 \textbf{(b)}, applied to } R = \mathbb{F}_q[T], \\ Z = \{1,2,\ldots,k\} \text{ and } r_i = \frac{-1}{P_i}\text{)}}}$$

$$= M \prod_{i \in \{1,2,\ldots,k\}} \left(1 + \frac{-1}{P_i}\right) = M \prod_{\pi \in \operatorname{PF} M} \underbrace{\left(1 + \frac{-1}{\pi}\right)}_{=1-\frac{1}{\pi}}$$

$$\left(\begin{array}{c} \text{here, we have substituted } \pi \text{ for } P_i \text{ in the product,} \\ \text{since the map } \{1,2,\ldots,k\} \to \operatorname{PF} M,\ i \mapsto P_i \text{ is a bijection} \end{array} \right)$$

$$= M \prod_{\pi \in \operatorname{PF} M} \left(1 - \frac{1}{\pi}\right).$$

This proves Proposition 3.68 **(b)**.

(c) Let $\mathfrak{A}$ be the set of all monic divisors of M. Thus, $\sum_{D \in \mathfrak{A}} = \sum_{D|M}$.

But M itself is monic. Hence, the map $\mathfrak{A} \to \mathfrak{A},\ D \mapsto \dfrac{M}{D}$ is well-defined and a bijection. Thus, we can substitute $\dfrac{M}{D}$ for D in the sum $\sum\limits_{D \in \mathfrak{A}} \mu(D) \dfrac{M}{D}$. As a result, we obtain

$$\sum_{D \in \mathfrak{A}} \mu(D) \frac{M}{D} = \underbrace{\sum_{D \in \mathfrak{A}}}_{= \sum\limits_{D \mid M}} \mu\left(\frac{M}{D}\right) \underbrace{\frac{M}{\left(\frac{M}{D}\right)}}_{=D} = \sum_{D \mid M} \mu\left(\frac{M}{D}\right) D = \sum_{D \mid M} D\mu\left(\frac{M}{D}\right).$$

Comparing this with

$$\underbrace{\sum_{D \in \mathfrak{A}}}_{= \sum\limits_{D \mid M}} \mu(D) \frac{M}{D} = \sum_{D \mid M} \mu(D) \frac{M}{D} = \varphi_C(M) \qquad \left(\begin{array}{c} \text{since } \varphi_C(M) \text{ is defined} \\ \text{to be } \sum\limits_{D \mid M} \mu(D) \dfrac{M}{D} \end{array} \right),$$

we obtain $\varphi_C(M) = \sum\limits_{D \mid M} D\mu\left(\dfrac{M}{D}\right)$. This proves Proposition 3.68 **(c)**. □

Proposition 3.69. Let $M \in \mathbb{F}_q[T]_+$. Then, $M = \sum\limits_{D \mid M} \varphi_C(D)$.

Proposition 3.69 is [3, Theorem 4.5 (2)], but let me nevertheless give an independent proof of it:

Proof of Proposition 3.69. We shall use the notation of Proposition 3.66.

Every $E \in \mathbb{F}_q[T]_+$ satisfies

$$\begin{aligned} \varphi_C(E) &= \sum_{D \mid E} \mu(D) \frac{E}{D} \qquad \text{(by the definition of } \varphi_C\text{)} \\ &= \sum_{B \mid E} \mu(B) \frac{E}{B} \end{aligned} \tag{103}$$

(here, we have renamed the summation index D as B).

For any monic divisor B of M, we have

$$\sum_{\substack{D \mid M; \\ B \mid D}} \frac{D}{B} = \sum_{E \mid \frac{M}{B}} E \tag{104}$$

[55].

[55] *Proof of (104):* Let B be a monic divisor of M. Then, the map

$$\begin{aligned} \{D \text{ is a monic divisor of } M \text{ such that } B \mid D\} &\to \left\{E \text{ is a monic divisor of } \frac{M}{B}\right\}, \\ D &\mapsto \frac{D}{B} \end{aligned}$$

Now,

$$\sum_{D|M} \underbrace{\varphi_C(D)}_{=\sum_{B|D}\mu(B)\frac{D}{B}} \quad \text{(by (103), applied to } E{=}D\text{)}$$

$$= \sum_{D|M} \underbrace{\sum_{B|D}}_{=\sum\limits_{\substack{B|M;\\ B|D}} \text{(since } D|M\text{)}} \mu(B)\frac{D}{B} = \underbrace{\sum_{D|M}\sum_{\substack{B|M;\\ B|D}}}_{=\sum_{B|M}\sum_{\substack{D|M;\\ B|D}}} \mu(B)\frac{D}{B} = \sum_{B|M}\sum_{\substack{D|M;\\ B|D}} \mu(B)\frac{D}{B}$$

$$= \sum_{B|M}\mu(B)\underbrace{\sum_{\substack{D|M;\\ B|D}}\frac{D}{B}}_{=\sum\limits_{E|\frac{M}{B}} E \text{ (by (104))}} = \sum_{B|M}\mu(B)\underbrace{\sum_{E|\frac{M}{B}} E}_{=\sum\limits_{\substack{E|M;\\ BE|M}}}$$

(since the monic divisors E of $\frac{M}{B}$ are precisely the monic divisors E of M satisfying $BE|M$)

$$= \sum_{B|M}\mu(B)\sum_{\substack{E|M;\\ BE|M}} E = \underbrace{\sum_{B|M}\sum_{\substack{E|M;\\ BE|M}}}_{=\sum\limits_{E|M}\sum\limits_{\substack{B|M;\\ BE|M}}} \mu(B)E = \sum_{E|M}\underbrace{\sum_{\substack{B|M;\\ BE|M}}\mu(B)}_{=[E=M] \text{ (by Corollary 3.67)}} E$$

$$= \sum_{E|M}[E=M]E = \underbrace{[M=M]}_{=1}M + \sum_{\substack{E|M;\\ E\neq M}} \underbrace{[E=M]}_{=0 \text{ (since } E\neq M\text{)}} E$$

(here, we have split off the addend for $E = M$ from the sum)

$$= M + \underbrace{\sum_{\substack{E|M;\\ E\neq M}} 0E}_{=0} = M.$$

This proves Proposition 3.69. □

Next, let us study the function φ:

(where the symbol "|" means "divides", not "such that") is well-defined and a bijection. Hence, we can substitute E for $\frac{D}{B}$ in the sum $\sum\limits_{\substack{D|M;\\ B|D}}\frac{D}{B}$. We thus obtain $\sum\limits_{\substack{D|M;\\ B|D}}\frac{D}{B} = \sum\limits_{E|\frac{M}{B}} E$. This proves (104).

Proposition 3.70. Let $M \in \mathbb{F}_q[T]_+$.

(a) We have $\varphi(M) \in \mathbb{N}_+$.

(b) We have $\varphi(M) = q^{\deg M} \prod_{\pi \in \operatorname{PF} M} \left(1 - \frac{1}{q^{\deg \pi}}\right)$.

(c) We have $\varphi(M) \equiv \mu(M) \bmod p$.

(d) We have $\varphi(M) = \mu(M)$ in $\mathbb{F}_q$.

(e) Let A be the ring $\mathbb{F}_q[T]$. For any ring B, we let $B^\times$ denote the group of units of B. Then, $\varphi(M) = \left|(A/MA)^\times\right|$.

Proposition 3.70 **(e)** is used as a definition of $\varphi(M)$ in [3, §6].

Proof of Proposition 3.70. **(b)** Let $M = P_1^{a_1} P_2^{a_2} \cdots P_k^{a_k}$ be the factorization of M into monic irreducible polynomials, with all of $a_1, a_2, \ldots, a_k$ being positive integers (and with $P_1, P_2, \ldots, P_k$ being distinct).[56] Then, the **squarefree** monic divisors D of M all have the form $\prod_{i \in I} P_i$ for some subset I of $\{1, 2, \ldots, k\}$. More precisely, there exists a bijection

$$\begin{aligned} \{I \subseteq \{1,2,\ldots,k\}\} &\to (\text{the set of all squarefree monic divisors of } M), \\ I &\mapsto \prod_{i \in I} P_i. \end{aligned} \tag{105}$$

Moreover, every subset I of $\{1, 2, \ldots, k\}$ satisfies (100). (This is proven as in our proof of Proposition 3.66.)

Furthermore, every subset I of $\{1, 2, \ldots, k\}$ satisfies

$$\begin{aligned} q^{\deg\left(M/\prod_{i\in I} P_i\right)} &= q^{\deg M - \sum_{i\in I} \deg(P_i)} \qquad \left(\text{since } \deg\left(M/\prod_{i\in I} P_i\right) = \deg M - \sum_{i\in I} \deg(P_i)\right) \\ &= \frac{q^{\deg M}}{\prod_{i\in I} q^{\deg(P_i)}}. \end{aligned} \tag{106}$$

The definition of $P_1, P_2, \ldots, P_k$ shows that $(P_1, P_2, \ldots, P_k)$ is a list of all prime factors of M, with no repetitions. Thus, the map $\{1, 2, \ldots, k\} \to \operatorname{PF} M$, $i \mapsto P_i$ is a bijection.

[56] This is well-defined, since M is monic and since $\mathbb{F}_q[T]$ is a principal ideal domain. Of course, k can be 0 (when $M = 1$).

The definition of φ yields

$$\begin{aligned}
\varphi(M) &= \sum_{D|M} \mu(D)\, q^{\deg(M/D)} \\
&= \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D)\, q^{\deg(M/D)} + \sum_{\substack{D|M; \\ D \text{ is not squarefree}}} \underbrace{\mu(D)}_{\substack{=0 \\ \text{(by the definition of } \mu\text{, since } D \\ \text{is not squarefree)}}} q^{\deg(M/D)} \\
&= \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D)\, q^{\deg(M/D)} + \underbrace{\sum_{\substack{D|M; \\ D \text{ is not squarefree}}} 0 q^{\deg(M/D)}}_{=0} \\
&= \sum_{\substack{D|M; \\ D \text{ is squarefree}}} \mu(D)\, q^{\deg(M/D)} = \sum_{I \subseteq \{1,2,\ldots,k\}} \underbrace{\mu\left(\prod_{i\in I} P_i\right)}_{\substack{=(-1)^{|I|} \\ \text{(by (100))}}} \underbrace{q^{\deg\left(M/\prod_{i\in I} P_i\right)}}_{\substack{=\frac{q^{\deg M}}{\prod_{i\in I} q^{\deg(P_i)}} \\ \text{(by (106))}}} \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } \prod_{i\in I} P_i \text{ for } D \\ \text{due to the bijection (98)} \end{array} \right) \\
&= \sum_{I \subseteq \{1,2,\ldots,k\}} \underbrace{(-1)^{|I|}}_{=\prod_{i\in I}(-1)} \frac{q^{\deg M}}{\prod_{i\in I} q^{\deg(P_i)}} = \sum_{I \subseteq \{1,2,\ldots,k\}} \left(\prod_{i\in I}(-1)\right) \frac{q^{\deg M}}{\prod_{i\in I} q^{\deg(P_i)}} \\
&= q^{\deg M} \sum_{I \subseteq \{1,2,\ldots,k\}} \underbrace{\frac{\prod_{i\in I}(-1)}{\prod_{i\in I} q^{\deg(P_i)}}}_{=\prod_{i\in I}\frac{-1}{q^{\deg(P_i)}}} = q^{\deg M} \underbrace{\sum_{I \subseteq \{1,2,\ldots,k\}} \prod_{i\in I} \frac{-1}{q^{\deg(P_i)}}}_{=\prod_{i\in\{1,2,\ldots,k\}}\left(1+\frac{-1}{q^{\deg(P_i)}}\right)} \\
&\qquad \text{(by Lemma 3.65 \textbf{(b)}, applied to } R=\mathbb{Q}, \\
&\qquad Z=\{1,2,\ldots,k\} \text{ and } r_i=\frac{-1}{q^{\deg(P_i)}}) \\
&= q^{\deg M} \prod_{i\in\{1,2,\ldots,k\}} \left(1+\frac{-1}{q^{\deg(P_i)}}\right) = q^{\deg M} \prod_{\pi\in \mathrm{PF}\, M} \underbrace{\left(1+\frac{-1}{q^{\deg \pi}}\right)}_{=1-\frac{1}{q^{\deg\pi}}} \\
&\qquad \left(\begin{array}{c} \text{here, we have substituted } \pi \text{ for } P_i \text{ in the product,} \\ \text{since the map } \{1,2,\ldots,k\} \to \mathrm{PF}\, M,\ i \mapsto P_i \text{ is a bijection} \end{array} \right) \\
&= q^{\deg M} \prod_{\pi\in \mathrm{PF}\, M} \left(1-\frac{1}{q^{\deg\pi}}\right).
\end{aligned}$$

This proves Proposition 3.70 **(b)**.

(a) The definition of φ yields $\varphi(M) = \sum_{D|M} \mu(D)\, q^{\deg(M/D)} \in \mathbb{Z}$ (since $\mu(D)$ and $q^{\deg(M/D)}$ are integers for all $D \mid M$). But every $\pi \in \operatorname{PF} M$ satisfies $\deg \pi > 0$ (since π is irreducible) and thus $q^{\deg \pi} > 1$ (since $q > 1$) and therefore

$$1 > \frac{1}{q^{\deg \pi}}. \tag{107}$$

Proposition 3.70 **(b)** yields

$$\varphi(M) = \underbrace{q^{\deg M}}_{>0} \prod_{\pi \in \operatorname{PF} M} \underbrace{\left(1 - \frac{1}{q^{\deg \pi}}\right)}_{\substack{>0 \\ \text{(by (107))}}} > 0.$$

Combining this with $\varphi(M) \in \mathbb{Z}$, we find that $\varphi(M) \in \mathbb{N}_+$. This proves Proposition 3.70 **(a)**.

(c) If D is a monic divisor of M satisfying $D \neq M$, then

$$\mu(D)\, q^{\deg(M/D)} \equiv 0 \bmod p \tag{108}$$

[57]. Now, the definition of φ yields

$$\varphi(M) = \sum_{D|M} \mu(D)\, q^{\deg(M/D)} = \mu(M) \underbrace{q^{\deg(M/M)}}_{\substack{=q^0 \\ \text{(since } \deg(M/M)=\deg 1=0\text{)}}} + \sum_{\substack{D|M; \\ D\neq M}} \underbrace{\mu(D)\, q^{\deg(M/D)}}_{\substack{\equiv 0 \bmod p \\ \text{(by (108))}}}$$

(here, we have split off the addend for $D = M$ from the sum)

$$\equiv \mu(M) \underbrace{q^0}_{=1} + \underbrace{\sum_{\substack{D|M; \\ D\neq M}} 0}_{=0} = \mu(M) \bmod p.$$

This proves Proposition 3.70 **(c)**.

(d) Proposition 3.70 **(c)** shows that $\varphi(M) \equiv \mu(M) \bmod p$. Hence, $\varphi(M) = \mu(M)$ holds in any field of characteristic p. In particular, $\varphi(M) = \mu(M)$ holds in $\mathbb{F}_q$ (since $\mathbb{F}_q$ is a field of characteristic p).

(e) Let us first observe two general facts:

[57] *Proof of (108):* Let D be a monic divisor of M satisfying $D \neq M$. From $M \neq D$, we obtain $M/D \neq 1$.

We have $M/D \in \mathbb{F}_q[T]$ (since D is a divisor of M). Also, the polynomial M/D is monic (since M and D are monic). If we had $\deg(M/D) = 0$, then we would have $M/D = 1$ (because M/D is monic), which would contradict $M/D \neq 1$. Thus, we cannot have $\deg(M/D) = 0$. Hence, we must have $\deg(M/D) \geq 1$ (since $M/D \in \mathbb{F}_q[T]$). Hence, $q^{\deg(M/D)}$ is divisible by q, and thus also divisible by p (since $p \mid q$). In other words, $q^{\deg(M/D)} \equiv 0 \bmod p$. Hence, $\mu(D) \underbrace{q^{\deg(M/D)}}_{\equiv 0 \bmod p} \equiv 0 \bmod p$ (since $\mu(D) \in \{-1, 0, 1\} \subseteq \mathbb{Z}$). This proves (108).

- If $s \in \mathbb{F}_q[T]$ is a nonzero polynomial, then

$$|A/sA| = q^{\deg s} \tag{109}$$

[58].

- If $s \in \mathbb{F}_q[T]$ is a monic irreducible polynomial, and if n is a positive integer, then

$$\left|(A/s^nA)^\times\right| = q^{n\deg s} - q^{(n-1)\deg s} \tag{110}$$

[59].

The polynomial M is monic. Hence, the factorization of M into monic irreducible polynomials is $M = \prod\limits_{s\in \mathrm{PF}\, M} s^{v_s(M)}$. Notice that $v_s(M)$ is a positive integer for each $s \in \mathrm{PF}\, M$.

From $M = \prod\limits_{s\in \mathrm{PF}\, M} s^{v_s(M)}$, we conclude that

$$\deg M = \deg \prod_{s\in \mathrm{PF}\, M} s^{v_s(M)} = \sum_{s\in \mathrm{PF}\, M} \deg\left(s^{v_s(M)}\right),$$

and thus

$$q^{\deg M} = q^{\sum\limits_{s\in \mathrm{PF}\, M} \deg\left(s^{v_s(M)}\right)} = \prod_{s\in \mathrm{PF}\, M} q^{\deg\left(s^{v_s(M)}\right)}. \tag{111}$$

[58] *Proof of (109):* Let $s \in \mathbb{F}_q[T]$ be a nonzero polynomial. Then, it is well-known that A/sA is an $\deg s$-dimensional $\mathbb{F}_q$-vector space (since $A = \mathbb{F}_q[T]$). Hence, $|A/sA| = \left|\mathbb{F}_q\right|^{\deg s}$. Since $\left|\mathbb{F}_q\right| = q$, this rewrites as $|A/sA| = q^{\deg s}$. This proves (109).

[59] *Proof of (110):* Let $s \in \mathbb{F}_q[T]$ be a monic irreducible polynomial, and let n be a positive integer.

Applying (109) to s^{n-1} instead of s, we obtain $\left|A/s^{n-1}A\right| = q^{\deg\left(s^{n-1}\right)} = q^{(n-1)\deg s}$ (since $\deg\left(s^{n-1}\right) = (n-1)\deg s$).

Applying (109) to s^n instead of s, we obtain $|A/s^nA| = q^{\deg(s^n)} = q^{n\deg s}$ (since $\deg(s^n) = n\deg s$).

Let B be the ring A/s^nA. Then, $B = \underbrace{A}_{=\mathbb{F}_q[T]}/s^n\underbrace{A}_{=\mathbb{F}_q[T]} = \mathbb{F}_q[T]/s^n\mathbb{F}_q[T]$. Hence, Proposition 3.55 **(b)** (applied to $\mathbb{F} = \mathbb{F}_q$) shows that $sB \cong \mathbb{F}_q[T]/s^{n-1}\mathbb{F}_q[T]$ as $\mathbb{F}_q$-vector spaces. Thus, $sB \cong \underbrace{\mathbb{F}_q[T]}_{=A}/s^{n-1}\underbrace{\mathbb{F}_q[T]}_{=A} = A/s^{n-1}A$ as $\mathbb{F}_q$-vector spaces. Hence, $|sB| = \left|A/s^{n-1}A\right| = q^{(n-1)\deg s}$. Also, from $B = A/s^nA$, we obtain $|B| = |A/s^nA| = q^{n\deg s}$.

But Proposition 3.55 **(a)** (applied to $\mathbb{F} = \mathbb{F}_q$) yields $B^\times = B \setminus sB$. Hence,

$$\begin{aligned}\left|B^\times\right| = |B\setminus sB| &= \underbrace{|B|}_{=q^{n\deg s}} - \underbrace{|sB|}_{=q^{(n-1)\deg s}} \qquad \text{(since } sB\subseteq B\text{)}\\ &= q^{n\deg s} - q^{(n-1)\deg s}.\end{aligned}$$

Since $B = A/s^nA$, this rewrites as $\left|(A/s^nA)^\times\right| = q^{n\deg s} - q^{(n-1)\deg s}$. Hence, (110) is proven.

For each $s \in \operatorname{PF} M$, define an ideal I_s of A by $I_s = s^{v_s(M)} A$. Notice that A is a principal ideal domain (since $A = \mathbb{F}_q[T]$). We have

$$\left|\left(A/I_s\right)^{\times}\right| = q^{\deg\left(s^{v_s(M)}\right)} \left(1 - \frac{1}{q^{\deg s}}\right) \tag{112}$$

for each $s \in \operatorname{PF} M$ [60].

Every two distinct elements s and t of $\operatorname{PF} M$ satisfy $I_s + I_t = A$ [61]. Hence, Theorem 3.53 **(b)** (applied to $\mathbf{S} = \operatorname{PF} M$) shows that the canonical A-algebra homomorphism

$$A/\left(\prod_{s \in \operatorname{PF} M} I_s\right) \to \prod_{s \in \operatorname{PF} M} \left(A/I_s\right), \qquad a + \prod_{s \in \operatorname{PF} M} I_s \mapsto \left(a + I_s\right)_{s \in \operatorname{PF} M}$$

is well-defined and an A-algebra isomorphism. Hence, $A/\left(\prod_{s \in \operatorname{PF} M} I_s\right) \cong \prod_{s \in \operatorname{PF} M} \left(A/I_s\right)$ as A-algebras.

But

$$\prod_{s \in \operatorname{PF} M} \underbrace{I_s}_{=s^{v_s(M)}A} = \prod_{s \in \operatorname{PF} M} \left(s^{v_s(M)} A\right) = \underbrace{\left(\prod_{s \in \operatorname{PF} M} s^{v_s(M)}\right)}_{=M} A = MA.$$

---

[60] *Proof of (112):* Let $s \in \operatorname{PF} M$. Thus, s is a monic irreducible polynomial dividing M.

Let $n = v_s(M)$. Then, $n = v_s(M)$ is a positive integer (since s divides M). Hence, (110) yields

$$\left|\left(A/s^n A\right)^{\times}\right| = q^{n \deg s} - \underbrace{q^{(n-1)\deg s}}_{\substack{=q^{n\deg s - \deg s} \\ (\text{since } (n-1)\deg s = n\deg s - \deg s)}} = q^{n\deg s} - \underbrace{q^{n\deg s - \deg s}}_{=\frac{q^{n\deg s}}{q^{\deg s}}}$$

$$= q^{n\deg s} - \frac{q^{n\deg s}}{q^{\deg s}} = \underbrace{q^{n\deg s}}_{\substack{=q^{\deg(s^n)} \\ (\text{since } n\deg s = \deg(s^n))}} \left(1 - \frac{1}{q^{\deg s}}\right) = q^{\deg(s^n)} \left(1 - \frac{1}{q^{\deg s}}\right)$$

$$= q^{\deg\left(s^{v_s(M)}\right)} \left(1 - \frac{1}{q^{\deg s}}\right) \qquad (\text{since } n = v_s(M)).$$

Also, $I_s = s^{v_s(M)} A = s^n A$ (since $v_s(M) = n$). Hence, $\left|\left(A/I_s\right)^{\times}\right| = \left|\left(A/s^n A\right)^{\times}\right| = q^{\deg\left(s^{v_s(M)}\right)} \left(1 - \frac{1}{q^{\deg s}}\right)$. This proves (112).

[61] *Proof.* Let s and t be two distinct elements of $\operatorname{PF} M$. Thus, s and t are two distinct monic irreducible polynomials in $\mathbb{F}_q[T]$. Hence, Lemma 3.52 (applied to $\mathbb{F} = \mathbb{F}_q$, $n = v_s(M)$, $m = v_t(M)$ and $R = A$) yields $s^{v_s(M)} A + t^{v_t(M)} A = A$.

On the other hand, $I_s = s^{v_s(M)} A$ (by the definition of I_s) and $I_t = t^{v_t(M)} A$ (by the definition of I_t). Adding these two equalities, we obtain $I_s + I_t = s^{v_s(M)} A + t^{v_t(M)} A = A$. Qed.

Thus, $A/\underbrace{\left(\prod\limits_{s\in \operatorname{PF} M} I_s\right)}_{=MA} = A/MA$. Hence, $A/MA = A/\left(\prod\limits_{s\in \operatorname{PF} M} I_s\right) \cong \prod\limits_{s\in \operatorname{PF} M} (A/I_s)$ as A-algebras. Therefore,

$$(A/MA)^\times \cong \left(\prod_{s\in \operatorname{PF} M} (A/I_s)\right)^\times \cong \prod_{s\in \operatorname{PF} M} (A/I_s)^\times$$

as groups. Hence,

$$\begin{aligned}
\left|(A/MA)^\times\right| &= \left|\prod_{s\in \operatorname{PF} M} (A/I_s)^\times\right| = \prod_{s\in \operatorname{PF} M} \underbrace{\left|(A/I_s)^\times\right|}_{\substack{=q^{\deg\left(s^{v_s(M)}\right)}\left(1-\frac{1}{q^{\deg s}}\right) \\ \text{(by (112))}}} \\
&= \prod_{s\in \operatorname{PF} M} \left(q^{\deg\left(s^{v_s(M)}\right)}\left(1-\frac{1}{q^{\deg s}}\right)\right) \\
&= \underbrace{\left(\prod_{s\in \operatorname{PF} M} q^{\deg\left(s^{v_s(M)}\right)}\right)}_{\substack{=q^{\deg M} \\ \text{(by (111))}}} \underbrace{\prod_{s\in \operatorname{PF} M}\left(1-\frac{1}{q^{\deg s}}\right)}_{\substack{=\prod\limits_{\pi\in \operatorname{PF} M}\left(1-\frac{1}{q^{\deg \pi}}\right) \\ \text{(here, we have renamed the} \\ \text{index } s \text{ as } \pi \text{ in the product)}}} \\
&= q^{\deg M} \prod_{\pi\in \operatorname{PF} M}\left(1-\frac{1}{q^{\deg \pi}}\right) = \varphi(M)
\end{aligned}$$

(by Proposition 3.70 **(b)**). This proves Proposition 3.70 **(e)**. □

Finally, here is an identity that connects the functions μ and φ_C (an analogue of [6, (12.68.6)]):

Proposition 3.71. Let $M \in \mathbb{F}_q[T]_+$. Then,

$$\sum_{D|M} D\mu(D)\,\varphi_C\left(\frac{M}{D}\right) = \mu(M) \qquad \text{in } \mathbb{F}_q[T].$$

Proof of Proposition 3.71. We shall use the notation of Proposition 3.66.

Every $E \in \mathbb{F}_q[T]_+$ satisfies (103). (This can be proven as in our proof of Proposition 3.69 above.) Now, every monic divisor D of M satisfies

$$\varphi_C\left(\frac{M}{D}\right) = \sum_{\substack{B|M; \\ BD|M}} \mu(B)\,\frac{M}{BD} \tag{113}$$

[62]. Also, every monic divisor B of M satisfies

$$\sum_{\substack{D|M; \\ BD|M}} \mu(D) = [B = M] \tag{114}$$

[63].

[62] *Proof of (113):* Let D be a monic divisor of M. Thus, $M/D \in \mathbb{F}_q[T]$. Also, the polynomial M/D is monic (since M and D are monic). Hence, $M/D \in \mathbb{F}_q[T]_+$. Thus, (103) (applied to $E = M/D$) yields

$$\varphi_C(M/D) = \underbrace{\sum_{B|M/D}}_{\substack{= \sum_{\substack{B|M; \\ BD|M}} \\ \text{(since the monic divisors } B \text{ of } M/D \\ \text{are exactly the monic divisors } B \text{ of } M \\ \text{that satisfy } BD|M)}} \mu(B) \underbrace{\frac{M/D}{B}}_{=\frac{M}{BD}} = \sum_{\substack{B|M; \\ BD|M}} \mu(B) \frac{M}{BD}.$$

Thus, $\varphi_C\left(\frac{M}{D}\right) = \varphi_C(M/D) = \sum_{\substack{B|M; \\ BD|M}} \mu(B) \frac{M}{BD}$. This proves (113).

[63] *Proof of (114):* We can rename the variables E and B as B and D in Corollary 3.67. As a result, we conclude that $\sum_{\substack{D|M; \\ DB|M}} \mu(D) = [B = M]$. Hence, $[B = M] = \sum_{\substack{D|M; \\ DB|M}} \mu(D) = \sum_{\substack{D|M; \\ BD|M}} \mu(D)$. This proves (114).

Now,

$$\sum_{D\mid M} D\mu(D) \quad \underbrace{\varphi_C\left(\frac{M}{D}\right)}_{=\sum\limits_{\substack{B\mid M;\\ BD\mid M}} \mu(B)\frac{M}{BD} \text{ (by (113))}}$$

$$= \sum_{D\mid M} D\mu(D) \sum_{\substack{B\mid M;\\ BD\mid M}} \mu(B)\frac{M}{BD} = \underbrace{\sum_{D\mid M} \sum_{\substack{B\mid M;\\ BD\mid M}}}_{=\sum\limits_{B\mid M}\sum\limits_{\substack{D\mid M;\\ BD\mid M}}} \underbrace{D\mu(D)\mu(B)\frac{M}{BD}}_{=\frac{M}{B}\mu(B)\mu(D)}$$

$$= \sum_{B\mid M} \sum_{\substack{D\mid M;\\ BD\mid M}} \frac{M}{B}\mu(B)\mu(D) = \sum_{B\mid M} \frac{M}{B}\mu(B) \underbrace{\sum_{\substack{D\mid M;\\ BD\mid M}} \mu(D)}_{=[B=M] \text{ (by (114))}}$$

$$= \sum_{B\mid M} \frac{M}{B}\mu(B)[B=M] = \underbrace{\frac{M}{M}}_{=1}\mu(M)\underbrace{[M=M]}_{=1} + \sum_{\substack{B\mid M;\\ B\neq M}} \frac{M}{B}\mu(B)\underbrace{[B=M]}_{=0 \text{ (since } B\neq M)}$$

(here, we have split off the addend for $B = M$ from the sum)

$$= \mu(M) + \underbrace{\sum_{\substack{B\mid M;\\ B\neq M}} \frac{M}{B}\mu(B)\,0}_{=0} = \mu(M)$$

in $\mathbb{F}_q[T]$. This proves Proposition 3.71. □

3.15. The Carlitz ghost-Witt equivalence

We are now ready to prove a generalization of Theorem 2.13:

Theorem 3.72. Let N be a q-nest. Let A be an $\mathcal{F}$-module. For every $P \in N$, let φ_P be an endomorphism of the $\mathbb{F}_q$-vector space A. (The notation φ_P for these endomorphisms should not be confused with the notation φ_C defined in Definition 3.63; we shall ensure this by never using the notation C for a polynomial in this context.) Let us make the following three assumptions:

Assumption 1: For every $P \in N$, the map φ_P is an endomorphism of the $\mathcal{F}$-module A.

Assumption 2: We have $\varphi_\pi(a) \equiv (\operatorname{Carl}\pi)\,a \bmod \pi A$ for every $a \in A$ and every monic irreducible $\pi \in N$.

Assumption 3: We have $\varphi_1 = \mathrm{id}$. Furthermore, $\varphi_P \circ \varphi_Q = \varphi_{PQ}$ for every $P \in N$ and every $Q \in N$ satisfying $PQ \in N$.

Let $(b_P)_{P \in N} \in A^N$ be a family of elements of A. Then, the following assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ are equivalent:

Assertion $\mathcal{C}_1$: Every $P \in N$ and every $\pi \in \mathrm{PF}\, P$ satisfy

$$\varphi_\pi\left(b_{P/\pi}\right) \equiv b_P \bmod \pi^{v_\pi(P)} A.$$

Assertion $\mathcal{D}_1$: There exists a family $(x_P)_{P \in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D \mid P} D \cdot \left(\mathrm{Carl}\, \frac{P}{D} \right) x_D \text{ for every } P \in N \right).$$

Assertion $\mathcal{D}_2$: There exists a family $(\widetilde{x}_P)_{P \in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D \mid P} D F^{\deg(P/D)} \widetilde{x}_D \text{ for every } P \in N \right).$$

Assertion $\mathcal{E}_1$: There exists a family $(y_P)_{P \in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D \mid P} D \varphi_{P/D}\left(y_D\right) \text{ for every } P \in N \right).$$

Assertion $\mathcal{F}_1$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \mu(D)\, \varphi_D\left(b_{P/D}\right) \in PA.$$

Assertion $\mathcal{G}_1$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \varphi_C(D)\, \varphi_D\left(b_{P/D}\right) \in PA.$$

Assertion $\mathcal{G}_2$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \varphi(D)\, \varphi_D\left(b_{P/D}\right) \in PA.$$

Theorem 3.72 is a generalization of Theorem 2.13 – namely, it is precisely the generalization outlined in Remark 2.15. In order to see this, the reader should recall Proposition 3.27, which says that (roughly speaking) $\mathcal{F}$-modules are the same as Frobenius $\mathbb{F}_q[T]$-modules (which are precisely $\mathbb{F}_q[T]$-modules A with

an $\mathbb{F}_q$-linear Frobenius map $F : A \to A$ which satisfies (2)[64]).

Before we prove Theorem 3.72, let us show two more general facts:

Lemma 3.73. Let N be a q-nest. Let A be an $\mathbb{F}_q[T]$-module. For every $P \in N$ and every monic divisor D of P, let $g_{P,D}$ be an element of A. Let α, β and γ are three maps from N to $\mathbb{F}_q[T]$.

Assume that

$$\beta(P) = \sum_{D|P} D\gamma(D)\,\alpha\left(\frac{P}{D}\right) \qquad \text{for every } P \in N. \tag{115}$$

Furthermore, assume that every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P;\\ DE|P}} \alpha(D)\, g_{P,DE} \in PA. \tag{116}$$

Then, every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P;\\ DE|P}} \beta(D)\, g_{P,DE} \in PA. \tag{117}$$

Proof of Lemma 3.73. Let $P \in N$. Let E be a monic divisor of P. Then, every monic divisor F of P satisfies

$$F \sum_{\substack{M|P;\\ MF|P}} \alpha(M)\, g_{P,MF} \in PA \tag{118}$$

[65]. Furthermore, every monic divisor D of P satisfies

$$\sum_{\substack{M|P;\\ ME|P;\\ D|M}} \alpha\left(\frac{M}{D}\right) g_{P,ME} = \sum_{\substack{M|P;\\ MDE|P}} \alpha(M)\, g_{P,MDE} \tag{119}$$

[64]This is slightly nontrivial, because the equalities (2) and (43) are not obviously equivalent. Nevertheless, the equivalence of the equalities (2) and (43) is easy to show.

[65]*Proof of (118):* Let F be a monic divisor of P. Then,

$$F \sum_{\substack{M|P;\\ MF|P}} \alpha(M)\, g_{P,MF} = F \sum_{\substack{D|P;\\ DF|P}} \alpha(D)\, g_{P,DF} \qquad \text{(here, we have renamed the summation index } M \text{ as } D\text{)}$$
$$\in PA$$

(by (116) (applied to $E = F$)). This proves (118).

[66]. Finally, every monic divisor D of P satisfies

$$DE \sum_{\substack{M|P; \\ MDE|P}} \alpha(M)\, g_{P,MDE} \in PA \tag{122}$$

[66] *Proof of (119):* Let D be a monic divisor of P.

Let $\mathfrak{A}$ be the set of all monic divisors M of P satisfying $ME \mid P$ and $D \mid M$. Thus, $\sum_{M\in\mathfrak{A}} = \sum_{\substack{M|P; \\ ME|P; \\ D|M}}$.

Let $\mathfrak{B}$ be the set of all monic divisors M of P satisfying $MDE \mid P$. Thus, $\sum_{M\in\mathfrak{B}} = \sum_{\substack{M|P; \\ MDE|P}}$.

We have

$$M/D \in \mathfrak{B} \qquad \text{for each } M \in \mathfrak{A}. \tag{120}$$

[*Proof of (120):* Let $M \in \mathfrak{A}$. In other words, M is a monic divisor of P satisfying $ME \mid P$ and $D \mid M$ (by the definition of $\mathfrak{A}$). Now, $D \mid M$, so that $M/D \in \mathbb{F}_q[T]_+$. The polynomial M/D is monic (since M and D are monic), and is a divisor of P (since $M/D \mid M \mid P$). It furthermore satisfies $(M/D)\, DE = ME \mid P$. Thus, M/D is a monic divisor of P satisfying $(M/D)\, DE \mid P$. In other words, $M/D \in \mathfrak{B}$ (by the definition of $\mathfrak{B}$). This proves (120).]

Furthermore, we have

$$MD \in \mathfrak{A} \qquad \text{for each } M \in \mathfrak{B}. \tag{121}$$

[*Proof of (121):* Let $M \in \mathfrak{B}$. In other words, M is a monic divisor of P satisfying $MDE \mid P$ (by the definition of $\mathfrak{B}$). Now, the polynomial MD is monic (since M and D are monic), and is a divisor of P (since $MD \mid MDE \mid P$). Furthermore, it satisfies $(MD)\, E = MDE \mid P$ and $D \mid MD$. Thus, MD is a monic divisor of P satisfying $(MD)\, E \mid P$ and $D \mid MD$. In other words, $MD \in \mathfrak{A}$ (by the definition of $\mathfrak{A}$). This proves (121).]

Now, the map

$$\mathfrak{A} \to \mathfrak{B}, \qquad M \mapsto M/D$$

is well-defined (according to (120)). Furthermore, the map

$$\mathfrak{B} \to \mathfrak{A}, \qquad M \mapsto MD$$

is well-defined (according to (121)). These two maps are mutually inverse (because one of them divides input by D, whereas the other multiplies its input by D). Hence, they are both invertible. In particular, the map

$$\mathfrak{A} \to \mathfrak{B}, \qquad M \mapsto M/D$$

is invertible, i.e., is a bijection. Thus, we can substitute M/D for M in the sum $\sum_{M\in\mathfrak{B}} \alpha(M)\, g_{P,MDE}$. We thus obtain

$$\sum_{M\in\mathfrak{B}} \alpha(M)\, g_{P,MDE} = \underbrace{\sum_{M\in\mathfrak{A}}}_{= \sum_{\substack{M|P; \\ ME|P; \\ D|M}}} \alpha\left(\underbrace{M/D}_{=\frac{M}{D}}\right) \underbrace{g_{P,(M/D)DE}}_{=g_{P,ME}} = \sum_{\substack{M|P; \\ ME|P; \\ D|M}} \alpha\left(\frac{M}{D}\right) g_{P,ME}.$$

[67].

Thus,

$$\sum_{\substack{M\mid P;\\ ME\mid P;\\ D\mid M}} \alpha\left(\frac{M}{D}\right) g_{P,ME} = \underbrace{\sum_{M\in\mathfrak{B}}}_{=\sum_{\substack{M\mid P;\\ MDE\mid P}}} \alpha(M)\, g_{P,MDE} = \sum_{\substack{M\mid P;\\ MDE\mid P}} \alpha(M)\, g_{P,MDE}.$$

This proves (119).

[67] *Proof of (122):* Let D be a monic divisor of P. We must prove (122).

We are in one of the following two cases:

Case 1: We have $DE \mid P$.

Case 2: We have $DE \nmid P$.

Let us consider Case 1 first. In this case, we have $DE \mid P$. Also, the polynomial DE is monic (since D and E are monic). Hence, DE is a monic divisor of P. Thus, (118) (applied to $F = DE$) yields $DE \sum_{\substack{M\mid P;\\ MDE\mid P}} \alpha(M)\, g_{P,MDE} \in PA$. Thus, (122) is proven in Case 1.

Let us now consider Case 2. In this case, we have $DE \nmid P$. Thus, there exists no $M \mid P$ satisfying $MDE \mid P$ (because if such an M would exist, then it would satisfy $DE \mid MDE \mid P$, which would contradict $DE \nmid P$). Hence, the sum $\sum_{\substack{M\mid P;\\ MDE\mid P}} \alpha(M)\, g_{P,MDE}$ is empty, and thus equals 0. In other words, $\sum_{\substack{M\mid P;\\ MDE\mid P}} \alpha(M)\, g_{P,MDE} = 0$. Now, $DE \underbrace{\sum_{\substack{M\mid P;\\ MDE\mid P}} \alpha(M)\, g_{P,MDE}}_{=0} = 0 \in PA$.

Thus, (122) is proven in Case 2.

We have now proven (122) in both Cases 1 and 2. Thus, (122) always holds.

Now,

$$\sum_{\substack{D|P;\\ DE|P}} \beta(D)\, g_{P,DE}$$

$$= \sum_{\substack{M|P;\\ ME|P}} \underbrace{\beta(M)}_{= \sum_{D|M} D\gamma(D)\alpha\left(\frac{M}{D}\right)} g_{P,ME} \qquad \text{(here, we have renamed the summation index } D \text{ as } M\text{)}$$

(by (115) (applied to M instead of P))

$$= \sum_{\substack{M|P;\\ ME|P}} \underbrace{\sum_{D|M}}_{= \sum_{\substack{D|P;\\ D|M}}} D\gamma(D)\,\alpha\left(\frac{M}{D}\right) g_{P,ME}$$

(since every monic divisor D of M is also a monic divisor of P (since $M|P$))

$$= \underbrace{\sum_{\substack{M|P;\\ ME|P}} \sum_{\substack{D|P;\\ D|M}}}_{= \sum_{D|P} \sum_{\substack{M|P;\\ ME|P;\\ D|M}}} D\gamma(D)\,\alpha\left(\frac{M}{D}\right) g_{P,ME} = \sum_{D|P} \sum_{\substack{M|P;\\ ME|P;\\ D|M}} D\gamma(D)\,\alpha\left(\frac{M}{D}\right) g_{P,ME}$$

$$= \sum_{D|P} D\gamma(D) \underbrace{\sum_{\substack{M|P;\\ ME|P;\\ D|M}} \alpha\left(\frac{M}{D}\right) g_{P,ME}}_{= \sum_{\substack{M|P;\\ MDE|P}} \alpha(M) g_{P,MDE}} = \sum_{D|P} D\gamma(D) \sum_{\substack{M|P;\\ MDE|P}} \alpha(M)\, g_{P,MDE}.$$

(by (119))

Multiplying both sides of this equality by E, we find

$$E \sum_{\substack{D|P;\\ DE|P}} \beta(D)\, g_{P,DE}$$

$$= E \sum_{D|P} D\gamma(D) \sum_{\substack{M|P;\\ MDE|P}} \alpha(M)\, g_{P,MDE} = \sum_{D|P} DE\gamma(D) \sum_{\substack{M|P;\\ MDE|P}} \alpha(M)\, g_{P,MDE}$$

$$= \sum_{D|P} \gamma(D)\, DE \underbrace{\sum_{\substack{M|P;\\ MDE|P}} \alpha(M)\, g_{P,MDE}}_{\in PA} \in \sum_{D|P} \gamma(D)\, PA \subseteq PA.$$

(by (122))

This proves Lemma 3.73. □

Lemma 3.74. Let N be a q-nest. Let A be an $\mathbb{F}_q[T]$-module. For every $P \in N$ and every monic divisor D of P, let $g_{P,D}$ be an element of A. Then, the following two assertions are equivalent:

Assertion $\mathcal{L}$: Every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \mu(D)\, g_{P,DE} \in PA.$$

Assertion $\mathcal{M}$: Every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \varphi_C(D)\, g_{P,DE} \in PA.$$

Proof of Lemma 3.74. We shall consider $\varphi_C : \mathbb{F}_q[T]_+ \to \mathbb{F}_q[T]$ as a map $N \to \mathbb{F}_q[T]$ (by restricting it to the subset N of $\mathbb{F}_q[T]_+$). We shall also consider $\mu : \mathbb{F}_q[T]_+ \to \{-1,0,1\}$ as a map $N \to \mathbb{F}_q[T]$ (by restricting it to the subset N of $\mathbb{F}_q[T]_+$, and by composing it with the canonical map $\{-1,0,1\} \to \mathbb{Z} \to \mathbb{F}_q[T]$).

We shall prove the implications $\mathcal{L} \Longrightarrow \mathcal{M}$ and $\mathcal{M} \Longrightarrow \mathcal{L}$ separately:

Proof of the implication $\mathcal{L} \Longrightarrow \mathcal{M}$: Assume that Assertion $\mathcal{L}$ holds. We must show that Assertion $\mathcal{M}$ holds.

Define a map $\gamma : N \to \mathbb{F}_q[T]$ by ($\gamma(P) = 1$ for every $P \in N$).

For every $P \in N$, we have

$$\varphi_C(P) = \sum_{D|P} \underbrace{D}_{=D1} \mu\left(\frac{P}{D}\right) \qquad \text{(by Proposition 3.68 \textbf{(c)}, applied to } M = P\text{)}$$

$$= \sum_{D|P} D \underbrace{1}_{\substack{=\gamma(D) \\ \text{(since } \gamma(D)=1 \\ \text{(by the definition of } \gamma\text{))}}} \mu\left(\frac{P}{D}\right) = \sum_{D|P} D\gamma(D)\, \mu\left(\frac{P}{D}\right).$$

Furthermore, every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \mu(D)\, g_{P,DE} \in PA$$

(because Assertion $\mathcal{L}$ holds). Thus, Lemma 3.73 (applied to $\alpha = \mu$ and $\beta = \varphi_C$) shows that every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \varphi_C(D)\, g_{P,DE} \in PA.$$

In other words, Assertion $\mathcal{M}$ holds. Thus, we have proven the implication $\mathcal{L} \Longrightarrow \mathcal{M}$.

Proof of the implication $\mathcal{M} \Longrightarrow \mathcal{L}$: Assume that Assertion $\mathcal{M}$ holds. We must show that Assertion $\mathcal{L}$ holds.

For every $P \in N$, we have

$$\sum_{D|P} D\mu(D)\, \varphi_C\left(\frac{P}{D}\right) = \mu(P)$$

(by Proposition 3.71, applied to $M = P$) and thus

$$\mu(P) = \sum_{D|P} D\mu(D)\, \varphi_C\left(\frac{P}{D}\right).$$

Furthermore, every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \varphi_C(D)\, g_{P,DE} \in PA$$

(because Assertion $\mathcal{M}$ holds). Thus, Lemma 3.73 (applied to $\alpha = \varphi_C$, $\beta = \mu$ and $\gamma = \mu$) shows that every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \mu(D)\, g_{P,DE} \in PA.$$

In other words, Assertion $\mathcal{L}$ holds. Thus, we have proven the implication $\mathcal{M} \Longrightarrow \mathcal{L}$.

We have now proven the two implications $\mathcal{L} \Longrightarrow \mathcal{M}$ and $\mathcal{M} \Longrightarrow \mathcal{L}$. Combining them, we obtain the equivalence $\mathcal{L} \Longleftrightarrow \mathcal{M}$. Thus, Lemma 3.74 is proven. □

Proof of Theorem 3.72. Let us observe a few simple facts:

- If D and E are two monic polynomials in $\mathbb{F}_q[T]$ satisfying $DE \in N$, then

$$\varphi_D \circ \varphi_E = \varphi_{DE} \tag{123}$$

[68].

- Every $P \in N$ and every monic divisor D of P satisfy

$$\varphi_D \circ \varphi_{P/D} = \varphi_P \tag{124}$$

[69].

[68] *Proof of (123):* Let D and E be two monic polynomials in $\mathbb{F}_q[T]$ satisfying $DE \in N$.

The polynomial D is a monic divisor of DE (since D is monic and $D \mid DE$). Since $DE \in N$, this entails $D \in N$ (because N is a q-nest). Similarly, $E \in N$.

But Assumption 3 shows that $\varphi_P \circ \varphi_Q = \varphi_{PQ}$ for every $P \in N$ and every $Q \in N$ satisfying $PQ \in N$. Applying this to $P = D$ and $Q = E$, we obtain $\varphi_D \circ \varphi_E = \varphi_{DE}$. This proves (123).

[69] *Proof of (124):* Let $P \in N$, and let D be a monic divisor of P. Then, $P/D \in \mathbb{F}_q[T]$ (since D is a divisor of P). The polynomial P/D is monic (since P and D are monic). Also, $D \cdot (P/D) = P \in N$. Hence, (123) (applied to $E = P/D$) yields $\varphi_D \circ \varphi_{P/D} = \varphi_{D\cdot(P/D)} = \varphi_P$. This proves (124).

- Assumption 3 furthermore shows that $\varphi_1 = \mathrm{id}$.

Assumption 1 shows that, for every $P \in N$, the map φ_P is an endomorphism of the $\mathcal{F}$-module A. In other words, for every $P \in N$,

$$\text{the map } \varphi_P \text{ is } \mathcal{F}\text{-linear.} \tag{125}$$

Notice that Assertion $\mathcal{C}_1$ of Theorem 3.72 is identical with Assertion $\mathcal{C}_1$ of Theorem 3.57.

Let us now prove the equivalences $\mathcal{C}_1 \iff \mathcal{D}_1$, $\mathcal{C}_1 \iff \mathcal{D}_2$ and $\mathcal{C}_1 \iff \mathcal{E}_1$. These three equivalences will be derived from Theorem 3.57.

Proof of the equivalence $\mathcal{C}_1 \iff \mathcal{D}_1$: For every $P \in N$, define an endomorphism ψ_P of the $\mathbb{F}_q$-vector space A by

$$\left(\psi_P(a) = (\operatorname{Carl} P)\, a \qquad \text{for every } a \in A\right).$$

The Assumptions 1, 2 and 3 of Theorem 3.57 are satisfied (because they are precisely the Assumptions 1, 2 and 3 of Theorem 3.72). Hence, Proposition 3.59 shows that Assumptions 4 and 5 of Theorem 3.57 are satisfied. Hence, Theorem 3.57 shows that the assertions $\mathcal{C}_1$ and $\mathcal{E}_\psi$ of Theorem 3.57 are equivalent. In other words, $\mathcal{C}_1 \iff \mathcal{E}_\psi$.

But Assertion $\mathcal{D}_1$ can be rewritten as follows:

> *Assertion $\mathcal{D}_1'$:* There exists a family $(z_P)_{P \in N} \in A^N$ of elements of A such that
>
> $$\left(b_P = \sum_{D \mid P} D \cdot \left(\operatorname{Carl} \frac{P}{D}\right) z_D \text{ for every } P \in N\right).$$

Assertion $\mathcal{D}_1'$ is obtained from Assertion $\mathcal{D}_1$ by renaming the family $(x_P)_{P \in N}$ as $(z_P)_{P \in N}$. Hence, we have the equivalence $\mathcal{D}_1 \iff \mathcal{D}_1'$.

But every $P \in N$ and every monic divisor D of P satisfy

$$\begin{aligned} \psi_{P/D}(z_D) &= (\operatorname{Carl}(P/D))\, z_D \qquad \text{(by the definition of } \psi_{P/D}\text{)} \\ &= \left(\operatorname{Carl} \frac{P}{D}\right) z_D. \end{aligned}$$

Thus, Assertion $\mathcal{E}_\psi$ of Theorem 3.57 is equivalent to our Assertion $\mathcal{D}_1'$. In other words, we have the equivalence $\mathcal{E}_\psi \iff \mathcal{D}_1'$. Thus, we have the chain of equivalences $\mathcal{D}_1 \iff \mathcal{D}_1' \iff \mathcal{E}_\psi \iff \mathcal{C}_1$. This proves the equivalence $\mathcal{C}_1 \iff \mathcal{D}_1$.

Proof of the equivalence $\mathcal{C}_1 \iff \mathcal{D}_2$: For every $P \in N$, define an endomorphism ψ_P of the $\mathbb{F}_q$-vector space A by

$$\left(\psi_P(a) = F^{\deg P} a \qquad \text{for every } a \in A\right).$$

The Assumptions 1, 2 and 3 of Theorem 3.57 are satisfied (because they are precisely the Assumptions 1, 2 and 3 of Theorem 3.72). Hence, Proposition 3.60 shows that Assumptions 4 and 5 of Theorem 3.57 are satisfied. Hence, Theorem 3.57 shows that the assertions $\mathcal{C}_1$ and $\mathcal{E}_\psi$ of Theorem 3.57 are equivalent. In other words, $\mathcal{C}_1 \iff \mathcal{E}_\psi$.

But Assertion $\mathcal{D}_2$ can be rewritten as follows:

> *Assertion $\mathcal{D}_2'$:* There exists a family $(z_P)_{P\in N} \in A^N$ of elements of A such that
>
> $$\left(b_P = \sum_{D\mid P} DF^{\deg(P/D)} z_D \text{ for every } P \in N \right).$$

Assertion $\mathcal{D}_2'$ is obtained from Assertion $\mathcal{D}_2$ by renaming the family $(x_P)_{P\in N}$ as $(z_P)_{P\in N}$. Hence, we have the equivalence $\mathcal{D}_2 \iff \mathcal{D}_2'$.

But every $P \in N$ and every monic divisor D of P satisfy

$$\psi_{P/D}(z_D) = F^{\deg(P/D)} z_D \qquad \text{(by the definition of } \psi_{P/D}\text{)}.$$

Thus, Assertion $\mathcal{E}_\psi$ of Theorem 3.57 is equivalent to our Assertion $\mathcal{D}_2'$. In other words, we have the equivalence $\mathcal{E}_\psi \iff \mathcal{D}_2'$. Thus, we have the chain of equivalences $\mathcal{D}_2 \iff \mathcal{D}_2' \iff \mathcal{E}_\psi \iff \mathcal{C}_1$. This proves the equivalence $\mathcal{C}_1 \iff \mathcal{D}_2$.

Proof of the equivalence $\mathcal{C}_1 \iff \mathcal{E}_1$: For every $P \in N$, define an endomorphism ψ_P of the $\mathbb{F}_q$-vector space A by $\psi_P = \varphi_P$. The Assumptions 1, 2 and 3 of Theorem 3.57 are satisfied (because they are precisely the Assumptions 1, 2 and 3 of Theorem 3.72). Hence, Proposition 3.61 shows that Assumptions 4 and 5 of Theorem 3.57 are satisfied. Hence, Theorem 3.57 shows that the assertions $\mathcal{C}_1$ and $\mathcal{E}_\psi$ of Theorem 3.57 are equivalent. In other words, $\mathcal{C}_1 \iff \mathcal{E}_\psi$.

But Assertion $\mathcal{E}_1$ can be rewritten as follows:

> *Assertion $\mathcal{E}_1'$:* There exists a family $(z_P)_{P\in N} \in A^N$ of elements of A such that
>
> $$\left(b_P = \sum_{D\mid P} D\varphi_{P/D}(z_D) \text{ for every } P \in N \right).$$

Assertion $\mathcal{E}_1'$ is obtained from Assertion $\mathcal{E}_1$ by renaming the family $(y_P)_{P\in N}$ as $(z_P)_{P\in N}$. Hence, we have the equivalence $\mathcal{E}_1 \iff \mathcal{E}_1'$.

But every $P \in N$ and every monic divisor D of P satisfy $\psi_{P/D} = \varphi_{P/D}$ (by the definition of $\psi_{P/D}$). Thus, Assertion $\mathcal{E}_\psi$ of Theorem 3.57 is equivalent to our Assertion $\mathcal{E}_1'$. In other words, we have the equivalence $\mathcal{E}_\psi \iff \mathcal{E}_1'$. Thus, we have the chain of equivalences $\mathcal{E}_1 \iff \mathcal{E}_1' \iff \mathcal{E}_\psi \iff \mathcal{C}_1$. This proves the equivalence $\mathcal{C}_1 \iff \mathcal{E}_1$.

Combining the equivalences $\mathcal{C}_1 \iff \mathcal{D}_1$, $\mathcal{C}_1 \iff \mathcal{D}_2$ and $\mathcal{C}_1 \iff \mathcal{E}_1$, we obtain the chain of equivalences $\mathcal{C}_1 \iff \mathcal{D}_1 \iff \mathcal{D}_2 \iff \mathcal{E}_1$. Let us now show some further logical implications. We shall use the notations of Proposition 3.66.

Proof of the implication $\mathcal{E}_1 \implies \mathcal{F}_1$: Assume that Assertion $\mathcal{E}_1$ holds. That is, there exists a family $(y_P)_{P \in N} \in A^N$ of elements of A such that

$$\left(b_P = \sum_{D \mid P} D\varphi_{P/D}\left(y_D\right) \text{ for every } P \in N \right). \tag{126}$$

Consider this family $(y_P)_{P \in N}$. We need to prove that Assertion $\mathcal{F}_1$ holds, i.e., that every $P \in N$ satisfies

$$\sum_{D \mid P} \mu\left(D\right) \varphi_D\left(b_{P/D}\right) \in PA.$$

Fix $P \in N$. Then, every monic divisor D of P satisfies

$$b_{P/D} = \sum_{\substack{E \mid P; \\ DE \mid P}} E\varphi_{(P/E)/D}\left(y_E\right) \tag{127}$$

[70]. Moreover, if D and E are two monic divisors of P satisfying $DE \mid P$, then

$$\varphi_D\left(\varphi_{(P/E)/D}\left(y_E\right)\right) = \varphi_{P/E}\left(y_E\right) \tag{128}$$

[70] *Proof of (127):* Let B be a monic divisor of P. Thus, $P/B \in \mathbb{F}_q\left[T\right]_+$. Moreover, the polynomial P/B is monic (since P and B are monic), and is a divisor of P. Hence, $P/B \in N$ (since N is a q-nest, and since $P \in N$). Thus, (126) (applied to P/B instead of P) yields

$$b_{P/B} = \underbrace{\sum_{D \mid P/B}}_{= \sum\limits_{\substack{D \mid P; \\ BD \mid P}}} D \underbrace{\varphi_{(P/B)/D}}_{= \varphi_{(P/D)/B}} \left(y_D\right) = \sum_{\substack{D \mid P; \\ BD \mid P}} D\varphi_{(P/D)/B}\left(y_D\right)$$

(since the monic divisors D of P/B are precisely the monic divisors D of P satisfying $BD \mid P$)

(since $(P/B)/D = (P/D)/B$)

$$= \sum_{\substack{E \mid P; \\ BE \mid P}} E\varphi_{(P/E)/B}\left(y_E\right) \qquad \left(\begin{array}{c} \text{here, we have renamed the} \\ \text{summation index } D \text{ as } E \end{array} \right).$$

Now, forget that we fixed B. We thus have shown that every monic divisor B of P satisfies $b_{P/B} = \sum\limits_{\substack{E \mid P; \\ BE \mid P}} E\varphi_{(P/E)/B}\left(y_E\right)$. Renaming B as D in this result, we obtain the following: Every monic divisor D of P satisfies $b_{P/D} = \sum\limits_{\substack{E \mid P; \\ DE \mid P}} E\varphi_{(P/E)/D}\left(y_E\right)$. This proves (127).

[71].

Hence, every monic divisor D of P satisfies

$$\varphi_D\left(\underbrace{b_{P/D}}_{\substack{=\sum\limits_{\substack{E\mid P;\\ DE\mid P}} E\varphi_{(P/E)/D}(y_E)\\ \text{(by (127))}}}\right) = \varphi_D\left(\sum_{\substack{E\mid P;\\ DE\mid P}} E\varphi_{(P/E)/D}\left(y_E\right)\right) = \sum_{\substack{E\mid P;\\ DE\mid P}} E\,\underbrace{\varphi_D\left(\varphi_{(P/E)/D}\left(y_E\right)\right)}_{\substack{=\varphi_{P/E}(y_E)\\ \text{(by (128))}}}$$

$$= \sum_{\substack{E\mid P;\\ DE\mid P}} E\varphi_{P/E}\left(y_E\right). \qquad \left(\begin{array}{c}\text{since the map } \varphi_D \text{ is } \mathcal{F}\text{-linear}\\ \text{(by (125), applied to } D \text{ instead of } P)\end{array}\right) \tag{129}$$

[71] *Proof of (128):* Let D and E be two monic divisors of P satisfying $DE \mid P$. We have $E \mid DE \mid P$. Thus, $P/E \in \mathbb{F}_q[T]$. Moreover, the polynomial P/E is monic (since P and E are monic). Hence, P/E is a monic divisor of $P \in N$. Thus, $P/E \in N$ (since N is a q-nest). Moreover, $D \mid P/E$ (since $\dfrac{P/E}{D} = \dfrac{P}{DE} \in \mathbb{F}_q[T]$ (since $DE \mid P$)). Hence, D is a monic divisor of P/E. Thus, (124) (applied to P/E instead of P) yields $\varphi_D \circ \varphi_{(P/E)/D} = \varphi_{P/E}$.

Now, $\varphi_D\left(\varphi_{(P/E)/D}\left(y_E\right)\right) = \underbrace{\left(\varphi_D \circ \varphi_{(P/E)/D}\right)}_{=\varphi_{P/E}}\left(y_E\right) = \varphi_{P/E}\left(y_E\right)$. This proves (128).

Hence,

$$\begin{aligned}
&\sum_{D|P} \mu(D) \underbrace{\varphi_D(b_{P/D})}_{=\sum\limits_{\substack{E|P;\\ DE|P}} E\varphi_{P/E}(y_E)} \\
&\qquad \text{(by (129))} \\
&= \sum_{D|P} \mu(D) \sum_{\substack{E|P;\\ DE|P}} E\varphi_{P/E}(y_E) = \sum_{B|P} \mu(B) \sum_{\substack{E|P;\\ BE|P}} E\varphi_{P/E}(y_E) \\
&\qquad \left(\begin{array}{c} \text{here, we have renamed the summation} \\ \text{index } D \text{ as } B \text{ in the outer sum} \end{array} \right) \\
&= \underbrace{\sum_{B|P} \sum_{\substack{E|P;\\ BE|P}}}_{=\sum\limits_{E|P} \sum\limits_{\substack{B|P;\\ BE|P}}} \mu(B) E\varphi_{P/E}(y_E) = \sum_{E|P} \underbrace{\sum_{\substack{B|P;\\ BE|P}} \mu(B)}_{\substack{=[E=P] \\ \text{(by Corollary 3.67,} \\ \text{applied to } M=P)}} E\varphi_{P/E}(y_E) \\
&= \sum_{E|P} [E=P] E\varphi_{P/E}(y_E) \\
&= \underbrace{[P=P]}_{=1} P \underbrace{\varphi_{P/P}}_{\substack{=\mathrm{id} \\ \text{(by Assumption 1)}}} (y_P) + \sum_{\substack{E|P;\\ E\neq P}} \underbrace{[E=P]}_{\substack{=0 \\ \text{(since } E\neq P\text{)}}} E\varphi_{P/E}(y_E) \\
&\qquad \text{(here, we have split off the addend for } E=P \text{ from the sum)} \\
&= P \underbrace{\mathrm{id}(y_P)}_{=y_P} + \underbrace{\sum_{\substack{E|P;\\ E\neq P}} 0 E\varphi_{P/E}(y_E)}_{=0} = P \underbrace{y_P}_{\in A} \in PA.
\end{aligned}$$

Thus, Assertion $\mathcal{F}_1$ holds. We have thus proven the implication $\mathcal{E}_1 \Longrightarrow \mathcal{F}_1$.

Proof of the implication $\mathcal{F}_1 \Longrightarrow \mathcal{E}_1$: Assume that Assertion $\mathcal{F}_1$ holds. That is, every $P \in N$ satisfies

$$\sum_{D|P} \mu(D) \varphi_D(b_{P/D}) \in PA. \tag{130}$$

Now we need to prove that Assertion $\mathcal{E}_1$ holds, i.e., that there exists a family $(y_P)_{P\in N} \in A^N$ of elements of A such that every $P \in N$ satisfies

$$\left(b_P = \sum_{D|P} D\varphi_{P/D}(y_D) \text{ for every } P \in N \right). \tag{131}$$

We shall construct such a family $(y_P)_{P\in N}$ recursively, by induction over $\deg P$. That is, we fix some $Q \in N$, and we assume that we already have constructed a $y_P \in A$ for every $P \in N$ satisfying $\deg P < \deg Q$; we furthermore assume that

these y_P satisfy

$$b_P = \sum_{D|P} D\varphi_{P/D}\left(y_D\right) \tag{132}$$

for every $P \in N$ satisfying $\deg P < \deg Q$. We now need to construct a $y_Q \in A$ such that (132) is satisfied for $P = Q$. In other words, we need to construct a $y_Q \in A$ satisfying $b_Q = \sum_{D|Q} D\varphi_{Q/D}\left(y_D\right)$.

From (130) (applied to $P = Q$), we obtain $\sum_{D|Q} \mu\left(D\right) \varphi_D\left(b_{Q/D}\right) \in QA$. Thus, there exists a $t \in A$ such that $\sum_{D|Q} \mu\left(D\right) \varphi_D\left(b_{Q/D}\right) = Qt$. Consider this t. Set $y_Q = t$.

For every monic divisor E of Q satisfying $E \neq 1$, we have

$$b_{Q/E} = \sum_{\substack{D|Q; \\ DE|Q}} D\varphi_{(Q/D)/E}\left(y_D\right) \tag{133}$$

[72]. If D and E are two monic divisors of Q satisfying $DE \mid Q$, then

$$\varphi_E\left(\varphi_{(Q/D)/E}\left(y_D\right)\right) = \varphi_{Q/D}\left(y_D\right) \tag{134}$$

[72] *Proof of (133):* Let E be a monic divisor of Q satisfying $E \neq 1$. We have $E \mid Q$ and thus $Q/E \in \mathbb{F}_q\left[T\right]$. The polynomial Q/E is monic (since Q and E are monic) and thus is a monic divisor of $Q \in N$. Hence, $Q/E \in N$ (since N is a q-nest). Also, E is a monic polynomial satisfying $E \neq 1$; therefore, $\deg E > 0$. Hence, $\deg\left(Q/E\right) = \deg Q - \underbrace{\deg E}_{>0} < \deg Q$. Thus, we can apply (132) to $P = Q/E$ (since we have assumed that (132) holds for every $P \in N$ satisfying $\deg P < \deg Q$). As a result, we obtain

$$b_{Q/E} = \underbrace{\sum_{D|Q/E}}_{\substack{= \sum_{\substack{D|Q; \\ DE|Q}} \\ \text{(since the monic divisors } D \text{ of } Q/E \\ \text{are precisely the monic divisors } D \text{ of } Q \\ \text{satisfying } DE|Q \text{ (since } E|Q\text{))}}} D \underbrace{\varphi_{(Q/E)/D}}_{\substack{=\varphi_{(Q/D)/E} \\ \text{(since } (Q/E)/D=(Q/D)/E\text{)}}} \left(y_D\right) = \sum_{\substack{D|Q; \\ DE|Q}} D\varphi_{(Q/D)/E}\left(y_D\right).$$

This proves (133).

[73]. If D is a monic divisor of Q, then

$$\sum_{\substack{E|Q;\\ DE|Q;\\ E\neq 1}} \mu(E) = [D=Q] - 1 \tag{135}$$

[74].

[73] *Proof of (134):* Let D and E be two monic divisors of Q satisfying $DE \mid Q$. We have $D \mid Q$ and thus $Q/D \in \mathbb{F}_q[T]$. The polynomial Q/D is monic (since Q and D are monic), and thus is a monic divisor of $Q \in N$. Hence, $Q/D \in N$ (since N is a q-nest). Moreover, $DE \mid Q$, and thus $\dfrac{Q}{DE} \in \mathbb{F}_q[T]$. Hence, $\dfrac{Q/D}{E} = \dfrac{Q}{DE} \in \mathbb{F}_q[T]$. Thus, E is a divisor of Q/D (since $Q/D \in \mathbb{F}_q[T]$). Hence, (124) (applied to Q/D and E instead of P and D) shows that

$$\varphi_E \circ \varphi_{(Q/D)/E} = \varphi_{Q/D}.$$

Now, $\varphi_E\left(\varphi_{(Q/D)/E}(y_D)\right) = \underbrace{\left(\varphi_E \circ \varphi_{(Q/D)/E}\right)}_{=\varphi_{Q/D}}(y_D) = \varphi_{Q/D}(y_D)$. This proves (134).

[74] *Proof of (135):* Let D be a monic divisor of Q. We must prove (135).

The polynomial 1 is a monic divisor of Q satisfying $D \cdot 1 \mid Q$ (since $D \cdot 1 = D \mid Q$). Hence, we can split off the addend for $E = 1$ from the sum $\sum_{\substack{E|Q;\\ DE|Q}} \mu(E)$. As a result, we obtain

$$\sum_{\substack{E|Q;\\ DE|Q}} \mu(E) = \sum_{\substack{E|Q;\\ DE|Q;\\ E\neq 1}} \mu(E) + \underbrace{\mu(1)}_{=1} = \sum_{\substack{E|Q;\\ DE|Q;\\ E\neq 1}} \mu(E) + 1.$$

Comparing this with

$$\begin{aligned}\sum_{\substack{E|Q;\\ DE|Q}} \mu(E) &= \underbrace{\sum_{\substack{B|Q;\\ DB|Q}}}_{\substack{=\sum\limits_{\substack{B|Q;\\ BD|Q}} \\ \text{(since } DB=BD \\ \text{for every } B|Q\text{)}}} \mu(B) \qquad \text{(here, we have renamed the summation index } E \text{ as } B\text{)} \\ &= \sum_{\substack{B|Q;\\ BD|Q}} \mu(B) = [D=Q] \qquad \left(\begin{array}{c}\text{by Corollary 3.67, applied to } Q \text{ and } D \\ \text{instead of } M \text{ and } E\end{array}\right),\end{aligned}$$

we obtain $\sum_{\substack{E|Q;\\ DE|Q;\\ E\neq 1}} \mu(E) + 1 = [D=Q]$. In other words, $\sum_{\substack{E|Q;\\ DE|Q;\\ E\neq 1}} \mu(E) = [D=Q] - 1$. This proves (135).

Now,

$$Qt = \sum_{D|Q} \mu(D)\, \varphi_D\left(b_{Q/D}\right) = \sum_{E|Q} \mu(E)\, \varphi_E\left(b_{Q/E}\right)$$

(here, we have renamed the summation index D as E)

$$= \underbrace{\mu(1)}_{=1}\, \underbrace{\varphi_1}_{=\mathrm{id}}\left(\underbrace{b_{Q/1}}_{=b_Q}\right) + \sum_{\substack{E|Q;\\ E\neq 1}} \mu(E)\, \varphi_E\left(\underbrace{b_{Q/E}}_{\substack{=\sum\limits_{\substack{D|Q;\\ DE|Q}} D\varphi_{(Q/D)/E}(y_D)\\ \text{(by (133))}}}\right)$$

(here, we have split off the addend for $E = 1$ from the sum)

$$= \underbrace{\mathrm{id}\left(b_Q\right)}_{=b_Q} + \sum_{\substack{E|Q;\\ E\neq 1}} \mu(E)\, \varphi_E\underbrace{\left(\sum_{\substack{D|Q;\\ DE|Q}} D\varphi_{(Q/D)/E}\left(y_D\right)\right)}_{\substack{=\sum\limits_{\substack{D|Q;\\ DE|Q}} D\varphi_E\left(\varphi_{(Q/D)/E}(y_D)\right)\\ \text{(since the map } \varphi_E \text{ is } \mathcal{F}\text{-linear}\\ \text{(by (125), applied to } E \text{ instead of } P)\text{)}}}$$

$$= b_Q + \sum_{\substack{E|Q;\\ E\neq 1}} \mu(E) \sum_{\substack{D|Q;\\ DE|Q}} D\underbrace{\varphi_E\left(\varphi_{(Q/D)/E}\left(y_D\right)\right)}_{\substack{=\varphi_{Q/D}(y_D)\\ \text{(by (134))}}} = b_Q + \sum_{\substack{E|Q;\\ E\neq 1}} \mu(E) \sum_{\substack{D|Q;\\ DE|Q}} D\varphi_{Q/D}\left(y_D\right).$$

Subtracting b_Q from both sides of this equality, we obtain

$$\begin{aligned}
Qt - b_Q &= \sum_{\substack{E|Q; \\ E\neq 1}} \mu(E) \sum_{\substack{D|Q; \\ DE|Q}} D\varphi_{Q/D}(y_D) = \underbrace{\sum_{\substack{E|Q; \\ E\neq 1}} \sum_{\substack{D|Q; \\ DE|Q}}}_{= \sum\limits_{D|Q} \sum\limits_{\substack{E|Q; \\ DE|Q; \\ E\neq 1}}} \mu(E) D\varphi_{Q/D}(y_D) \\
&= \sum_{D|Q} \underbrace{\sum_{\substack{E|Q; \\ DE|Q; \\ E\neq 1}} \mu(E)}_{=[D=Q]-1 \text{ (by (135))}} D\varphi_{Q/D}(y_D) = \sum_{D|Q} ([D=Q]-1) D\varphi_{Q/D}(y_D) \\
&= \underbrace{\sum_{D|Q} [D=Q] D\varphi_{Q/D}(y_D)}_{=[Q=Q]Q\varphi_{Q/Q}(y_Q) + \sum\limits_{\substack{D|Q; \\ D\neq Q}} [D=Q]D\varphi_{Q/D}(y_D)} - \sum_{D|Q} \underbrace{1D}_{=D} \varphi_{Q/D}(y_D) \\
&\qquad \text{(here, we have split off the addend for } D{=}Q \text{ from the sum)} \\
&= \underbrace{[Q=Q]}_{=1} Q \underbrace{\varphi_{Q/Q}}_{=\varphi_1=\mathrm{id}}(y_Q) + \sum_{\substack{D|Q; \\ D\neq Q}} \underbrace{[D=Q]}_{\substack{=0 \\ \text{(since } D\neq Q\text{)}}} D\varphi_{Q/D}(y_D) - \sum_{D|Q} D\varphi_{Q/D}(y_D) \\
&= Q \underbrace{\mathrm{id}(y_Q)}_{=y_Q=t} + \underbrace{\sum_{\substack{D|Q; \\ D\neq Q}} 0D\varphi_{Q/D}(y_D)}_{=0} - \sum_{D|Q} D\varphi_{Q/D}(y_D) \\
&= Qt - \sum_{D|Q} D\varphi_{Q/D}(y_D).
\end{aligned}$$

Subtracting Qt from both sides of this equality, we obtain

$$-b_Q = -\sum_{D|Q} D\varphi_{Q/D}(y_D).$$

In other words, $b_Q = \sum\limits_{D|Q} D\varphi_{Q/D}(y_D)$. In other words, (132) is satisfied for $P = Q$.

Thus, we have constructed a $y_Q \in A$ such that (132) is satisfied for $P = Q$. This completes a step of our recursive construction of the family $(y_P)_{P\in N}$. This family therefore exists. In other words, Assertion $\mathcal{E}_1$ holds. Thus, the implication $\mathcal{F}_1 \Longrightarrow \mathcal{E}_1$ is proven.

We have now proven the two implications $\mathcal{E}_1 \Longrightarrow \mathcal{F}_1$ and $\mathcal{F}_1 \Longrightarrow \mathcal{E}_1$. Combining them, we obtain the equivalence $\mathcal{E}_1 \Longleftrightarrow \mathcal{F}_1$.

Let us define one more notation: For every $P \in N$ and every monic divisor

D of P, we define an element $g_{P,D}$ of A by $g_{P,D} = \varphi_D(b_{P/D})$. (This is well-defined[75].)

Next, let us introduce two more assertions:

Assertion $\mathcal{L}$: Every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \mu(D)\, g_{P,DE} \in PA.$$

Assertion $\mathcal{M}$: Every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \varphi_C(D)\, g_{P,DE} \in PA.$$

Lemma 3.74 shows that these two Assertions $\mathcal{L}$ and $\mathcal{M}$ are equivalent. In other words, we have the equivalence $\mathcal{L} \iff \mathcal{M}$.

We shall now prove the implications $\mathcal{F}_1 \implies \mathcal{L}$, $\mathcal{L} \implies \mathcal{F}_1$, $\mathcal{G}_1 \implies \mathcal{M}$ and $\mathcal{M} \implies \mathcal{G}_1$:

Proof of the implication $\mathcal{F}_1 \implies \mathcal{L}$: Assume that Assertion $\mathcal{F}_1$ holds. That is, every $P \in N$ satisfies

$$\sum_{D|P} \mu(D)\, \varphi_D(b_{P/D}) \in PA. \tag{136}$$

Now we need to prove that Assertion $\mathcal{L}$ holds, i.e., that every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \mu(D)\, g_{P,DE} \in PA. \tag{137}$$

Let $P \in N$. Let E be a monic divisor of P. Thus, $E \mid P$, so that $P/E \in \mathbb{F}_q[T]$. Moreover, the polynomial P/E is monic (since P and E are monic). Hence, P/E is a monic divisor of $P \in N$. Thus, $P/E \in N$ (since N is a q-nest). Hence, (136) (applied to P/E instead of P) yields

$$\sum_{D|P/E} \mu(D)\, \varphi_D\left(b_{(P/E)/D}\right) \in (P/E)\, A. \tag{138}$$

But the map φ_E is $\mathcal{F}$-linear (by (125), applied to E instead of P). Furthermore, we have

$$\varphi_E \circ \varphi_D = \varphi_{DE} \qquad \text{for every monic divisor } D \text{ of } P/E \tag{139}$$

[75] *Proof.* Let $P \in N$, and let D be a monic divisor of P. Since D is a monic divisor of $P \in N$, we have $D \in N$ (since N is a q-nest). Hence, φ_D is well-defined. Also, $P/D \in \mathbb{F}_q[T]$ (since $D \mid P$). The polynomial P/D is monic (since P and D are monic), and thus is a monic divisor of $P \in N$. Hence, $P/D \in N$ (since N is a q-nest). Thus, $b_{P/D}$ is well-defined. Therefore, $\varphi_D(b_{P/D})$ is well-defined (since φ_D is well-defined). Qed.

[76].

Applying the map φ_E to both sides of the relation (138), we obtain

$$\varphi_E\left(\sum_{D\mid P/E}\mu(D)\,\varphi_D\left(b_{(P/E)/D}\right)\right)\in\varphi_E\left((P/E)\,A\right)\subseteq(P/E)\,\varphi_E(A)$$

(since the map φ_E is $\mathcal{F}$-linear). In view of

$$\begin{aligned}
&\varphi_E\left(\sum_{D\mid P/E}\mu(D)\,\varphi_D\left(b_{(P/E)/D}\right)\right)\\
&=\sum_{D\mid P/E}\mu(D)\,\underbrace{\varphi_E\left(\varphi_D\left(b_{(P/E)/D}\right)\right)}_{=(\varphi_E\circ\varphi_D)\left(b_{(P/E)/D}\right)}\qquad\text{(since the map }\varphi_E\text{ is }\mathcal{F}\text{-linear)}\\
&=\sum_{D\mid P/E}\mu(D)\,\underbrace{(\varphi_E\circ\varphi_D)}_{\substack{=\varphi_{DE}\\(\text{by (139)})}}\left(\underbrace{b_{(P/E)/D}}_{\substack{=b_{P/(DE)}\\(\text{since }(P/E)/D=P/(DE))}}\right)\\
&=\underbrace{\sum_{D\mid P/E}}_{\substack{=\sum\limits_{\substack{D\mid P;\\ DE\mid P}}\\(\text{since the monic divisors }D\text{ of }P/E\\ \text{are exactly the monic divisors }D\text{ of }P\\ \text{satisfying }DE\mid P\text{ (since }E\mid P))}}\mu(D)\,\underbrace{\varphi_{DE}\left(b_{P/(DE)}\right)}_{\substack{=g_{P,DE}\\(\text{since }g_{P,DE}=\varphi_{DE}\left(b_{P/(DE)}\right)\\ \text{(by the definition of }g_{P,DE}))}}\\
&=\sum_{\substack{D\mid P;\\ DE\mid P}}\mu(D)\,g_{P,DE},
\end{aligned}$$

this rewrites as $\sum\limits_{\substack{D\mid P;\\ DE\mid P}}\mu(D)\,g_{P,DE}\in(P/E)\,\varphi_E(A)$. Hence,

$$\underbrace{E\sum_{\substack{D\mid P;\\ DE\mid P}}\mu(D)\,g_{P,DE}}_{\in(P/E)\varphi_E(A)}\in\underbrace{E\,(P/E)}_{=P}\,\underbrace{\varphi_E(A)}_{\subseteq A}\subseteq PA.$$

[76] *Proof of (139):* Let D be a monic divisor of P/E.

We have $D\mid P/E$, thus $\dfrac{P/E}{D}\in\mathbb{F}_q[T]$. Also, the polynomial DE is monic (since D and E are monic) and divides P (since $\dfrac{P}{DE}=\dfrac{P/E}{D}\in\mathbb{F}_q[T]$). Thus, DE is a monic divisor of $P\in N$. Hence, $DE\in N$ (since N is a q-nest). Thus, (123) (applied to E and D instead of D and E) shows that $\varphi_E\circ\varphi_D=\varphi_{ED}=\varphi_{DE}$. This proves (139).

In other words, (137) holds. Thus, Assertion $\mathcal{L}$ holds. We have thus proven the implication $\mathcal{F}_1 \Longrightarrow \mathcal{L}$.

Proof of the implication $\mathcal{F}_1 \Longrightarrow \mathcal{L}$: Assume that Assertion $\mathcal{L}$ holds. That is, every $P \in N$ and every monic divisor E of P satisfy

$$E \sum_{\substack{D|P; \\ DE|P}} \mu(D)\, g_{P,DE} \in PA. \tag{140}$$

Now we need to prove that Assertion $\mathcal{F}_1$ holds, i.e., that every $P \in N$ satisfies

$$\sum_{D|P} \mu(D)\, \varphi_D(b_{P/D}) \in PA. \tag{141}$$

Let $P \in N$. Then, 1 is a monic divisor of P. Hence, (140) (applied to $E = 1$) yields

$$1 \sum_{\substack{D|P; \\ D\cdot 1|P}} \mu(D)\, g_{P,D\cdot 1} \in PA.$$

In view of

$$\begin{aligned} 1 & \underbrace{\sum_{\substack{D|P; \\ D\cdot 1|P}}}_{= \sum_{\substack{D|P; \\ D|P}} = \sum_{D|P}} \mu(D) \underbrace{g_{P,D\cdot 1}}_{\substack{= g_{P,D} = \varphi_D(b_{P/D}) \\ \text{(by the definition of } g_{P,D}\text{)}}} \\ &= 1 \sum_{D|P} \mu(D)\, \varphi_D(b_{P/D}) = \sum_{D|P} \mu(D)\, \varphi_D(b_{P/D}), \end{aligned}$$

this rewrites as $\sum_{D|P} \mu(D)\, \varphi_D(b_{P/D}) \in PA$. In other words, (141) holds. Thus, Assertion $\mathcal{F}_1$ holds. We have thus proven the implication $\mathcal{L} \Longrightarrow \mathcal{F}_1$.

Proof of the implication $\mathcal{G}_1 \Longrightarrow \mathcal{M}$: The implication $\mathcal{G}_1 \Longrightarrow \mathcal{M}$ can be proven in exactly the same way as the implication $\mathcal{F}_1 \Longrightarrow \mathcal{L}$ (except that every appearance of "μ" must be replaced by "φ_C").

Proof of the implication $\mathcal{M} \Longrightarrow \mathcal{G}_1$: The implication $\mathcal{M} \Longrightarrow \mathcal{G}_1$ can be proven in exactly the same way as the implication $\mathcal{L} \Longrightarrow \mathcal{F}_1$ (except that every appearance of "μ" must be replaced by "φ_C").

We now have proven the four implications $\mathcal{F}_1 \Longrightarrow \mathcal{L}$, $\mathcal{L} \Longrightarrow \mathcal{F}_1$, $\mathcal{G}_1 \Longrightarrow \mathcal{M}$ and $\mathcal{M} \Longrightarrow \mathcal{G}_1$. Combining them, we obtain the two equivalences $\mathcal{F}_1 \Longleftrightarrow \mathcal{L}$ and $\mathcal{G}_1 \Longleftrightarrow \mathcal{M}$.

Finally, let us prove the equivalence $\mathcal{F}_1 \Longleftrightarrow \mathcal{G}_2$:

Proof of the equivalence $\mathcal{F}_1 \Longleftrightarrow \mathcal{G}_2$: For every $P \in N$ and $D \in \mathbb{F}_q[T]_+$, we have

$$\underbrace{\varphi(D)}_{\substack{= \mu(D) \text{ in } \mathbb{F}_q \\ \text{(by Proposition 3.70 } \textbf{(d)}\text{,} \\ \text{applied to } M = D\text{)}}} \varphi_D(b_{P/D}) = \mu(D)\, \varphi_D(b_{P/D}).$$

Therefore, Assertion $\mathcal{G}_2$ is equivalent to $\mathcal{F}_1$. In other words, we obtain the equivalence $\mathcal{F}_1 \iff \mathcal{G}_2$.

We now have obtained the following equivalences:

$$\mathcal{C}_1 \iff \mathcal{D}_1 \iff \mathcal{D}_2 \iff \mathcal{E}_1, \qquad \mathcal{E}_1 \iff \mathcal{F}_1, \qquad \mathcal{L} \iff \mathcal{M},$$
$$\mathcal{F}_1 \iff \mathcal{L}, \qquad \mathcal{G}_1 \iff \mathcal{M}, \qquad \mathcal{F}_1 \iff \mathcal{G}_2.$$

Combining them all, we obtain the chain of equivalences

$$\mathcal{C}_1 \iff \mathcal{D}_1 \iff \mathcal{D}_2 \iff \mathcal{E}_1 \iff \mathcal{F}_1 \iff \mathcal{L} \iff \mathcal{M} \iff \mathcal{G}_1 \iff \mathcal{G}_2.$$

In particular, the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ are equivalent. This proves Theorem 3.72. □

3.16. Examples: "Necklace congruences" for $\mathbb{F}_q[T]$

Theorem 3.72 shows the equivalence of several assertions, but we have yet to see a situation in which these assertions hold. Let us now explore a few such situations. We begin with the simplest ones:

Proposition 3.75. Let N be the q-nest $\mathbb{F}_q[T]_+$. Let $A = \mathbb{F}_q[T]$. Notice that A is a commutative $\mathbb{F}_q[T]$-algebra, and thus an $\mathcal{F}$-module (according to Convention 3.29).

For every $P \in N$, define an endomorphism φ_P of the $\mathbb{F}_q$-vector space A by $\varphi_P = \mathrm{id}$.

Fix a polynomial $Q \in \mathbb{F}_q[T]$.

(a) The three Assumptions 1, 2 and 3 of Theorem 3.72 are satisfied.

(b) The assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied for the family $(b_P)_{P\in N} = \left(F^{\deg P} Q\right)_{P\in N} \in A^N$.

(c) The assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied for the family $(b_P)_{P\in N} = ((\mathrm{Carl}\, P)\, Q)_{P\in N} \in A^N$.

(d) The assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied for the family $(b_P)_{P\in N} = (Q)_{P\in N} \in A^N$.

Before we prove this proposition, let us get two simple lemmas out of our way:

Lemma 3.76. Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Set $d = \deg \pi$. Let $P \in \mathbb{F}_q[T]$. Then, $P^{q^d} \equiv P \bmod \pi\mathbb{F}_q[T]$.

Proof of Lemma 3.76. Let $\mathbb{F}_\pi$ denote the field $\mathbb{F}_q[T]/\pi\mathbb{F}_q[T]$. This is a field extension of $\mathbb{F}_q$. Furthermore, it is well-known that $\mathbb{F}_\pi = \mathbb{F}_q[T]/\pi\mathbb{F}_q[T]$ is an $\mathbb{F}_q$-vector space of dimension $\deg \pi = d$. Hence, $|\mathbb{F}_\pi| = \left|\mathbb{F}_q\right|^d = q^d$ (since $\left|\mathbb{F}_q\right| = q$). In particular, $\mathbb{F}_\pi$ is a finite field.

If Q is any element of $\mathbb{F}_q[T]$, then we let $\overline{Q}$ denote the residue class of $Q \in \mathbb{F}_q[T]$ modulo the ideal $\pi\mathbb{F}_q[T]$. This residue class $\overline{Q}$ lies in $\mathbb{F}_q[T]/\pi\mathbb{F}_q[T] =$

$\mathbb{F}_\pi$. Applying this to $Q = P$, we conclude that $\overline{P}$ lies in $\mathbb{F}_\pi$. In other words, $\overline{P} \in \mathbb{F}_\pi$.

But another known fact says that if L is a finite field, then every $a \in L$ satisfies $a^{|L|} = a$. Applying this to $L = \mathbb{F}_\pi$ and $a = \overline{P}$, we obtain $\overline{P}^{|\mathbb{F}_\pi|} = \overline{P}$. Since $q^d = |\mathbb{F}_\pi|$, we have $\overline{P^{q^d}} = \overline{P^{|\mathbb{F}_\pi|}} = \overline{P}^{|\mathbb{F}_\pi|} = \overline{P}$. In other words, $P^{q^d} \equiv P \bmod \pi\mathbb{F}_q[T]$ (because if Q is any element of $\mathbb{F}_q[T]$, then $\overline{Q}$ denotes the residue class of $Q \in \mathbb{F}_q[T]$ modulo the ideal $\pi\mathbb{F}_q[T]$). This proves Lemma 3.76. □

Lemma 3.77. Let $A = \mathbb{F}_q[T]$. Notice that A is a commutative $\mathbb{F}_q[T]$-algebra, and thus an $\mathcal{F}$-module (according to Convention 3.29). Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Let $P \in A$.

(a) We have $(\operatorname{Carl}\pi)\, P \equiv P \bmod \pi A$. Here, $(\operatorname{Carl}\pi)\, P$ denotes the image of P under the action of $\operatorname{Carl}\pi \in \mathcal{F}$ on the $\mathcal{F}$-module A.

(b) We have $F^{\deg\pi} P \equiv P \bmod \pi A$.

Proof of Lemma 3.77. **(b)** Set $d = \deg\pi$. Observe that $P \in A = \mathbb{F}_q[T]$. Thus, Lemma 3.76 yields $P^{q^d} \equiv P \bmod \pi\mathbb{F}_q[T]$. In other words, $P^{q^d} \equiv P \bmod \pi A$ (because $\mathbb{F}_q[T] = A$).

Now, (49) (applied to $k = d$ and $m = P$) yields $F^d \cdot P = P^{q^d} \equiv P \bmod \pi A$. Since $d = \deg\pi$, this rewrites as $F^{\deg\pi} \cdot P \equiv P \bmod \pi A$. In other words, $F^{\deg\pi} P \equiv P \bmod \pi A$. This proves Lemma 3.77 **(b)**.

(a) Corollary 3.42 (applied to $a = P$) yields $(\operatorname{Carl}\pi)\, P \equiv F^{\deg\pi} P \equiv P \bmod \pi A$ (by Lemma 3.77 **(b)**). Lemma 3.77 **(a)** is thus proven. □

Proof of Proposition 3.75. **(a)** Assumptions 1 and 3 of Theorem 3.72 are clearly satisfied (since $\varphi_P = \mathrm{id}$ for each $P \in N$). It thus remains to prove that Assumption 2 of Theorem 3.72 is satisfied.

Proof of Assumption 2 of Theorem 3.72: Let $a \in A$. Let $\pi \in N$ be monic irreducible. We must prove that $\varphi_\pi(a) \equiv (\operatorname{Carl}\pi)\, a \bmod \pi A$. Here, $(\operatorname{Carl}\pi)\, a$ denotes the image of a under the action of $\operatorname{Carl}\pi \in \mathcal{F}$ on the $\mathcal{F}$-module A.

Proposition 3.35 shows that there exists a unique $u(\pi) \in \mathcal{F}$ such that $\operatorname{Carl}\pi = F^{\deg\pi} + \pi \cdot u(\pi)$. Consider this $u(\pi)$. We have

$$\underbrace{(\operatorname{Carl}\pi)}_{=F^{\deg\pi}+\pi\cdot u(\pi)}\, a = \left(F^{\deg\pi} + \pi \cdot u(\pi)\right) a = F^{\deg\pi} a + \pi \cdot \underbrace{u(\pi)\, a}_{\in A} \in F^{\deg\pi} a + \pi A.$$

In other words, $(\operatorname{Carl}\pi)\, a \equiv F^{\deg\pi} a \bmod \pi A$. Thus,

$$(\operatorname{Carl}\pi)\, a \equiv F^{\deg\pi} a \equiv a \bmod \pi A \tag{142}$$

(by Lemma 3.77 **(b)**, applied to $P = a$).

But $\varphi_\pi = \mathrm{id}$ (by the definition of φ_π), and thus $\varphi_\pi(a) = \mathrm{id}(a) = a \equiv (\operatorname{Carl}\pi)\, a \bmod \pi A$ (by (142)). This completes our proof of Assumption 2 of Theorem 3.72.

Thus, all three Assumptions 1, 2 and 3 of Theorem 3.72 are satisfied. This proves Proposition 3.75 **(a)**.

(b) Define a family $(b_P)_{P\in N} \in A^N$ by $(b_P)_{P\in N} = \left(F^{\deg P}Q\right)_{P\in N}$. Thus,

$$b_P = F^{\deg P}Q \qquad \text{for every } P \in N. \tag{143}$$

We now must prove that the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied for this family.

We shall first show that Assertion $\mathcal{C}_1$ is satisfied:

Proof of Assertion $\mathcal{C}_1$: Let $P \in N$ and $\pi \in \operatorname{PF} P$. We must prove that $\varphi_\pi\left(b_{P/\pi}\right) \equiv b_P \bmod \pi^{v_\pi(P)}A$.

We have $\pi \in \operatorname{PF} P$, thus $P/\pi \in \mathbb{F}_q[T]$. The polynomial P/π is monic (since P and π are monic), and thus belongs to $\mathbb{F}_q[T]_+ = N$. Hence, the equality (143) (applied to P/π instead of P) yields $b_{P/\pi} = F^{\deg(P/\pi)}Q$. But $\varphi_\pi = \mathrm{id}$ (by the definition of φ_π), and thus

$$\varphi_\pi\left(b_{P/\pi}\right) = \mathrm{id}\left(b_{P/\pi}\right) = b_{P/\pi} = F^{\deg(P/\pi)}Q. \tag{144}$$

Lemma 3.77 **(b)** (applied to Q instead of P) yields $F^{\deg\pi}Q \equiv Q \bmod \pi A$. Thus, Corollary 3.48 **(a)** (applied to P/π, $F^{\deg\pi}Q$ and Q instead of N, a and b) yields

$$F^{\deg(P/\pi)}F^{\deg\pi}Q \equiv F^{\deg(P/\pi)}Q \bmod \pi^{v_\pi(P/\pi)+1}A.$$

Since

$$F^{\deg(P/\pi)}F^{\deg\pi} = F^{\deg(P/\pi)+\deg\pi} = F^{\deg P}$$
$$\left(\text{since } \deg(P/\pi) + \deg\pi = \deg\underbrace{\left((P/\pi)\,\pi\right)}_{=P} = \deg P\right)$$

and

$$\underbrace{v_\pi(P/\pi)}_{=v_\pi(P)-v_\pi(\pi)} + 1 = v_\pi(P) - \underbrace{v_\pi(\pi)}_{=1} + 1 = v_\pi(P) - 1 + 1 = v_\pi(P),$$

this rewrites as

$$F^{\deg P}Q \equiv F^{\deg(P/\pi)}Q \bmod \pi^{v_\pi(P)}A.$$

Now, (143) becomes

$$b_P = F^{\deg P}Q \equiv F^{\deg(P/\pi)}Q = \varphi_\pi\left(b_{P/\pi}\right) \bmod \pi^{v_\pi(P)}A$$

(by (144)). In other words, $\varphi_\pi\left(b_{P/\pi}\right) \equiv b_P \bmod \pi^{v_\pi(P)}A$. Thus, Assertion $\mathcal{C}_1$ is proven.

We now have shown that Assertion $\mathcal{C}_1$ is satisfied. Thus, all the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied (since Theorem 3.72 says that these assertions are equivalent). This proves Proposition 3.75 **(b)**.

(c) Define a family $(b_P)_{P\in N} \in A^N$ by $(b_P)_{P\in N} = ((\operatorname{Carl} P)\, Q)_{P\in N}$. Thus,

$$b_P = (\operatorname{Carl} P)\, Q \qquad \text{for every } P \in N. \tag{145}$$

We now must prove that the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied for this family.

We shall first show that Assertion $\mathcal{C}_1$ is satisfied:

Proof of Assertion $\mathcal{C}_1$: Let $P \in N$ and $\pi \in \operatorname{PF} P$. We must prove that $\varphi_\pi(b_{P/\pi}) \equiv b_P \bmod \pi^{v_\pi(P)} A$.

We have $\pi \in \operatorname{PF} P$, thus $P/\pi \in \mathbb{F}_q[T]$. The polynomial P/π is monic (since P and π are monic), and thus belongs to $\mathbb{F}_q[T]_+ = N$. Hence, the equality (145) (applied to P/π instead of P) yields $b_{P/\pi} = (\operatorname{Carl}(P/\pi))\, Q$. But $\varphi_\pi = \operatorname{id}$ (by the definition of φ_π), and thus

$$\varphi_\pi(b_{P/\pi}) = \operatorname{id}(b_{P/\pi}) = b_{P/\pi} = (\operatorname{Carl}(P/\pi))\, Q. \tag{146}$$

Lemma 3.77 **(a)** (applied to Q instead of P) yields $(\operatorname{Carl}\pi)\, Q \equiv Q \bmod \pi A$. Thus, Corollary 3.48 **(b)** (applied to P/π, $(\operatorname{Carl}\pi)\, Q$ and Q instead of N, a and b) yields

$$(\operatorname{Carl}(P/\pi))\,(\operatorname{Carl}\pi)\, Q \equiv (\operatorname{Carl}(P/\pi))\, Q \bmod \pi^{v_\pi(P/\pi)+1} A.$$

Since

$$\begin{aligned}(\operatorname{Carl}(P/\pi))\,(\operatorname{Carl}\pi) &= \operatorname{Carl}\left(\underbrace{(P/\pi)\,\pi}_{=P}\right) \qquad \left(\begin{array}{c}\text{since Carl is an } \mathbb{F}_q\text{-algebra}\\ \text{homomorphism}\end{array}\right)\\ &= \operatorname{Carl} P\end{aligned}$$

and

$$\underbrace{v_\pi(P/\pi)}_{=v_\pi(P)-v_\pi(\pi)} + 1 = v_\pi(P) - \underbrace{v_\pi(\pi)}_{=1} + 1 = v_\pi(P) - 1 + 1 = v_\pi(P),$$

this rewrites as

$$(\operatorname{Carl} P)\, Q \equiv (\operatorname{Carl}(P/\pi))\, Q \bmod \pi^{v_\pi(P)} A.$$

Now, (145) becomes

$$b_P = (\operatorname{Carl} P)\, Q \equiv (\operatorname{Carl}(P/\pi))\, Q = \varphi_\pi(b_{P/\pi}) \bmod \pi^{v_\pi(P)} A$$

(by (146)). In other words, $\varphi_\pi(b_{P/\pi}) \equiv b_P \bmod \pi^{v_\pi(P)} A$. Thus, Assertion $\mathcal{C}_1$ is proven.

We now have shown that Assertion $\mathcal{C}_1$ is satisfied. Thus, all the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied (since Theorem 3.72 says that these assertions are equivalent). This proves Proposition 3.75 **(c)**.

(d) Define a family $(b_P)_{P\in N} \in A^N$ by $(b_P)_{P\in N} = (Q)_{P\in N}$. Thus,

$$b_P = Q \qquad \text{for every } P \in N. \tag{147}$$

We now must prove that the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied for this family.

We shall first show that Assertion $\mathcal{C}_1$ is satisfied:

Proof of Assertion $\mathcal{C}_1$: Let $P \in N$ and $\pi \in \operatorname{PF} P$. We must prove that $\varphi_\pi\left(b_{P/\pi}\right) \equiv b_P \bmod \pi^{v_\pi(P)} A$.

We have $\pi \in \operatorname{PF} P$, thus $P/\pi \in \mathbb{F}_q[T]$. The polynomial P/π is monic (since P and π are monic), and thus belongs to $\mathbb{F}_q[T]_+ = N$. Hence, the equality (143) (applied to P/π instead of P) yields $b_{P/\pi} = Q$. But $\varphi_\pi = \mathrm{id}$ (by the definition of φ_π), and thus

$$\varphi_\pi\left(b_{P/\pi}\right) = \mathrm{id}\left(b_{P/\pi}\right) = b_{P/\pi} = Q. \tag{148}$$

Now, (143) becomes $b_P = Q = \varphi_\pi\left(b_{P/\pi}\right)$ (by (148)). Hence,

$$b_P \equiv \varphi_\pi\left(b_{P/\pi}\right) \bmod \pi^{v_\pi(P)} A.$$

In other words, $\varphi_\pi\left(b_{P/\pi}\right) \equiv b_P \bmod \pi^{v_\pi(P)} A$. Thus, Assertion $\mathcal{C}_1$ is proven.

We now have shown that Assertion $\mathcal{C}_1$ is satisfied. Thus, all the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied (since Theorem 3.72 says that these assertions are equivalent). This proves Proposition 3.75 **(d)**. □

Spelling out the claims of Theorem 3.72 in basic terms provides a plethora of congruences between polynomials in $\mathbb{F}_q[T]$. We will not list of all them, but only give one example, conjectured by the math.stackexchange user "Levent" in [13]:

Corollary 3.78. Let $Q \in \mathbb{F}_q[T]$. Then,

$$P \mid \sum_{D\mid P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}} \qquad \text{for every } P \in \mathbb{F}_q[T]_+.$$

First proof of Corollary 3.78. Define N, A and φ_P (for all $P \in N$) as in Proposition 3.75. Define a family $(b_P)_{P\in N} \in A^N$ by $(b_P)_{P\in N} = \left(F^{\deg P} Q\right)_{P\in N}$. Then, every $P \in N$ satisfies

$$b_P = F^{\deg P} Q = F^{\deg P} \cdot Q = Q^{q^{\deg P}} \tag{149}$$

(by (49), applied to $k = \deg P$ and $m = Q$).

Proposition 3.75 **(b)** shows that the assertions $\mathcal{C}_1$, $\mathcal{D}_1$, $\mathcal{D}_2$, $\mathcal{E}_1$, $\mathcal{F}_1$, $\mathcal{G}_1$, and $\mathcal{G}_2$ of Theorem 3.72 are satisfied for this family $(b_P)_{P\in N} = \left(F^{\deg P} Q\right)_{P\in N}$. In particular, Assertion $\mathcal{G}_2$ is satisfied. In other words, every $P \in N$ satisfies

$$\sum_{D\mid P} \varphi(D)\, \varphi_D\left(b_{P/D}\right) \in PA. \tag{150}$$

Now, let $P \in \mathbb{F}_q[T]_+$. Thus, $P \in \mathbb{F}_q[T]_+ = N$ (since N was defined to be $\mathbb{F}_q[T]_+$).

But the polynomial P is monic. Hence, the map

$$\begin{aligned}(\text{the set of all monic divisors of } P) &\to (\text{the set of all monic divisors of } P), \\ D &\mapsto P/D\end{aligned}$$

is well-defined and a bijection (actually, it is an involution). Thus, we can substitute P/D for D in the sum $\sum_{D|P} \varphi(D)\,\varphi_D(b_{P/D})$. We thus obtain

$$\begin{aligned}&\sum_{D|P} \varphi(D)\,\varphi_D(b_{P/D}) \\ &= \sum_{D|P} \varphi\left(\underbrace{P/D}_{=\frac{P}{D}}\right) \underbrace{\varphi_{P/D}}_{\substack{=\mathrm{id} \\ \text{(by the definition of } \varphi_{P/D}\text{)}}} \left(\underbrace{b_{P/(P/D)}}_{\substack{=b_D=Q^{q^{\deg D}} \\ \text{(by (149), applied} \\ \text{to } D \text{ instead of } P\text{)}}}\right) \\ &= \sum_{D|P} \varphi\left(\frac{P}{D}\right) \underbrace{\mathrm{id}\left(Q^{q^{\deg D}}\right)}_{=Q^{q^{\deg D}}} = \sum_{D|P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}}.\end{aligned}$$

Hence,

$$\sum_{D|P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}} = \sum_{D|P} \varphi(D)\,\varphi_D(b_{P/D}) \in PA$$

(by (150)). In other words, $P \mid \sum_{D|P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}}$. This proves Corollary 3.78. □

This said, it is not much harder to prove Corollary 3.78 without any reference to Theorem 3.72, using just the results of Subsection 3.14:

Second proof of Corollary 3.78. Let Frob denote the Frobenius endomorphism of the $\mathbb{F}_q$-algebra $\mathbb{F}_q[T]$. This is the map $\mathbb{F}_q[T] \to \mathbb{F}_q[T]$ that sends each $P \in \mathbb{F}_q[T]$ to P^q. It is well-known that Frob is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_q[T]$.

We make a few auxiliary observations:

> *Observation 1:* Let $u \in \mathbb{N}$, $a \in \mathbb{F}_q[T]$ and $b \in \mathbb{F}_q[T]$. Then, $a^{q^u} - b^{q^u} = (a-b)^{q^u}$.

[*Proof of Observation 1:* We have

$$\mathrm{Frob}^k c = c^{q^k} \qquad \text{for every } k \in \mathbb{N} \text{ and } c \in \mathbb{F}_q[T]. \tag{151}$$

(Indeed, this is easy to prove by induction over k, using the definition of Frob.)

Now, recall that Frob is an $\mathbb{F}_q$-algebra endomorphism of $\mathbb{F}_q[T]$. Hence, so is its u-th power Frob^u. Thus,

$$\mathrm{Frob}^u(a-b) = \underbrace{\mathrm{Frob}^u a}_{\substack{=a^{q^u} \\ \text{(by (151), applied to } c=a\text{)}}} - \underbrace{\mathrm{Frob}^u b}_{\substack{=b^{q^u} \\ \text{(by (151), applied to } c=b\text{)}}} = a^{q^u} - b^{q^u}.$$

Thus,

$$a^{q^u} - b^{q^u} = \mathrm{Frob}^u(a-b) = (a-b)^{q^u}$$

(by (151), applied to $c = a-b$). This proves Observation 1.]

> *Observation 2:* Let π be a monic irreducible polynomial in $\mathbb{F}_q[T]$. Let a and b be two elements of $\mathbb{F}_q[T]$ such that $a \equiv b \bmod \pi\mathbb{F}_q[T]$. Let $N \in \mathbb{F}_q[T]$ be nonzero. Then, $a^{q^{\deg N}} \equiv b^{q^{\deg N}} \bmod \pi^{v_\pi(N)+1}\mathbb{F}_q[T]$.

[*Proof of Observation 2:* We can regard Observation 2 as a particular case of Corollary 3.48 **(a)** (applied to $A = \mathbb{F}_q[T]$). But let us give a self-contained proof instead.

We have $a - b \in \pi\mathbb{F}_q[T]$ (since $a \equiv b \bmod \pi\mathbb{F}_q[T]$). In other words, $a - b = \pi c$ for some $c \in \mathbb{F}_q[T]$. Consider this c. Now, define $u \in \mathbb{N}$ by $u = \deg N$.

But every nonnegative integer m satisfies $2^m \geq m+1$ (this is easy to prove). Applying this to $m = u$, we find $2^u \geq u+1$. But $\pi^{v_\pi(N)} \mid N$ and thus $\deg\left(\pi^{v_\pi(N)}\right) \leq \deg N = u$. Hence, $u \geq \deg\left(\pi^{v_\pi(N)}\right) = v_\pi(N)\underbrace{\deg\pi}_{\geq 1} \geq v_\pi(N)$. But $q \geq 2$ and thus $q^u \geq 2^u \geq \underbrace{u}_{\geq v_\pi(N)} + 1 \geq v_\pi(N) + 1$.

But Observation 1 yields $a^{q^u} - b^{q^u} = \left(\underbrace{a-b}_{=\pi c}\right)^{q^u} = (\pi c)^{q^u} = \pi^{q^u} c^{q^u}$. Hence, $\pi^{q^u} \mid a^{q^u} - b^{q^u}$ in $\mathbb{F}_q[T]$. But $q^u \geq v_\pi(N) + 1$, and thus $\pi^{v_\pi(N)+1} \mid \pi^{q^u} \mid a^{q^u} - b^{q^u}$. In other words, $a^{q^u} \equiv b^{q^u} \bmod \pi^{v_\pi(N)+1}\mathbb{F}_q[T]$. Since $u = \deg N$, this rewrites as $a^{q^{\deg N}} \equiv b^{q^{\deg N}} \bmod \pi^{v_\pi(N)+1}\mathbb{F}_q[T]$. Thus, Observation 2 is proven.]

Next, fix $P \in \mathbb{F}_q[T]_+$. Let $\mathbf{S}$ be the set of all squarefree monic divisors of P.

> *Observation 3:* We have
>
> $$\sum_{D \mid P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}} = \sum_{D \in \mathbf{S}} \mu(D)\, Q^{q^{\deg(P/D)}}.$$

[*Proof of Observation 3:* Let $\mathbf{D}$ be the set of all monic divisors of P. Then, the map

$$\mathbf{D} \to \mathbf{D}, \qquad D \mapsto P/D$$

is well-defined (since P itself is monic) and invertible (since it is its own inverse). Thus, this map is a bijection. Hence, we can substitute P/D for D in the sum $\sum_{D\in\mathbf{D}} \varphi\left(\frac{P}{D}\right) Q^{\deg D}$. We thus obtain

$$\begin{aligned}
&\sum_{D\in\mathbf{D}} \varphi\left(\frac{P}{D}\right) Q^{\deg D} \\
&= \sum_{D\in\mathbf{D}} \varphi\left(\frac{P}{\underbrace{P/D}_{=D}}\right) Q^{\deg(P/D)} = \sum_{D\in\mathbf{D}} \underbrace{\varphi(D)}_{\substack{=\mu(D) \text{ in } \mathbb{F}_q \\ \text{(by Proposition 3.70 \textbf{(d)}} \\ \text{(applied to } D \text{ instead of } M))}} Q^{\deg(P/D)} \\
&= \underbrace{\sum_{D\in\mathbf{D}}}_{\substack{=\sum_{D\mid P} \\ \text{(since } \mathbf{D} \text{ is the set of all} \\ \text{monic divisors of } P)}} \mu(D)\, Q^{\deg(P/D)} = \sum_{D\mid P} \mu(D)\, Q^{\deg(P/D)} \\
&= \underbrace{\sum_{\substack{D\mid P; \\ D \text{ is squarefree}}}}_{\substack{=\sum_{D\in\mathbf{S}} \\ \text{(since } \mathbf{S} \text{ is the set} \\ \text{of all squarefree} \\ \text{monic divisors of } P)}} \mu(D)\, Q^{\deg(P/D)} + \sum_{\substack{D\mid P; \\ D \text{ is not squarefree}}} \underbrace{\mu(D)}_{\substack{=0 \\ \text{(by the definition} \\ \text{of } \mu, \text{ since } D \\ \text{is not squarefree)}}} Q^{\deg(P/D)} \\
&= \sum_{D\in\mathbf{S}} \mu(D)\, Q^{\deg(P/D)} + \underbrace{\sum_{\substack{D\mid P; \\ D \text{ is not squarefree}}} 0 Q^{\deg(P/D)}}_{=0} = \sum_{D\in\mathbf{S}} \mu(D)\, Q^{\deg(P/D)}.
\end{aligned}$$

Comparing this with

$$\underbrace{\sum_{D\in\mathbf{D}}}_{\substack{=\sum_{D\mid P} \\ \text{(since } \mathbf{D} \text{ is the set of all} \\ \text{monic divisors of } P)}} \varphi\left(\frac{P}{D}\right) Q^{\deg D} = \sum_{D\mid P} \varphi\left(\frac{P}{D}\right) Q^{\deg D},$$

this yields

$$\sum_{D\mid P} \varphi\left(\frac{P}{D}\right) Q^{\deg D} = \sum_{D\in\mathbf{S}} \mu(D)\, Q^{\deg(P/D)}.$$

This proves Observation 3.]

Observation 4: Let $P \in \mathbb{F}_q[T]_+$. Let $\pi \in \operatorname{PF} P$. Let D be a monic divisor of P such that $\pi \nmid D$. Then,

$$Q^{q^{\deg(P/D)}} \equiv Q^{q^{\deg(P/(\pi D))}} \bmod \pi^{v_\pi(P)} \mathbb{F}_q[T].$$

[*Proof of Observation 4:* Observe that $P/D \in \mathbb{F}_q[T]$ (since D is a divisor of P). Also, $\pi \nmid D$ and thus $v_\pi(D) = 0$. But $\pi \in \operatorname{PF} P$, so that $\pi \mid P$ and thus $v_\pi(P) > 0$. Now, $v_\pi(P/D) = v_\pi(P) - \underbrace{v_\pi(D)}_{=0} = v_\pi(P) > 0$. In other words, $\pi \mid P/D$. Hence, $(P/D)/\pi \in \mathbb{F}_q[T]$.

Set $d = \deg \pi$. Lemma 3.76 (applied to Q instead of P) yields

$$Q^{q^d} \equiv Q \bmod \pi \mathbb{F}_q[T].$$

Hence, Observation 2 (applied to $a = Q^{q^d}$, $b = Q$ and $N = (P/D)/\pi$) yields

$$\left(Q^{q^d}\right)^{q^{\deg((P/D)/\pi)}} \equiv Q^{q^{\deg((P/D)/\pi)}} \bmod \pi^{v_\pi((P/D)/\pi)+1} \mathbb{F}_q[T].$$

Since

$$\left(Q^{q^d}\right)^{q^{\deg((P/D)/\pi)}} = Q^{q^d q^{\deg((P/D)/\pi)}} = Q^{q^{d+\deg((P/D)/\pi)}}$$
$$\left(\text{since } q^d q^{\deg((P/D)/\pi)} = q^{d+\deg((P/D)/\pi)}\right)$$

and

$$\underbrace{v_\pi((P/D)/\pi)}_{=v_\pi(P/D)-v_\pi(\pi)} + 1 = \underbrace{v_\pi(P/D)}_{=v_\pi(P)} - \underbrace{v_\pi(\pi)}_{=1} + 1 = v_\pi(P) - 1 + 1 = v_\pi(P),$$

this rewrites as

$$Q^{q^{d+\deg((P/D)/\pi)}} \equiv Q^{q^{\deg((P/D)/\pi)}} \bmod \pi^{v_\pi(P)} \mathbb{F}_q[T].$$

Since

$$\underbrace{d}_{=\deg\pi} + \deg((P/D)/\pi) = \deg\pi + \deg((P/D)/\pi)$$
$$= \deg\left(\underbrace{\pi \cdot ((P/D)/\pi)}_{=P/D}\right) = \deg(P/D)$$

and

$$\deg\left(\underbrace{(P/D)/\pi}_{=P/(\pi D)}\right) = \deg(P/(\pi D)),$$

this rewrites as

$$Q^{q^{\deg(P/D)}} \equiv Q^{q^{\deg(P/(\pi D))}} \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T].$$

This proves Observation 4.]

Recall that $\mathbf{S}$ is the set of all squarefree monic divisors of P. Each of these squarefree monic divisors has the form $\prod_{\eta\in I}\eta$ for some subset I of $\operatorname{PF} P$. More precisely, the map

$$\begin{aligned}\{I \subseteq \operatorname{PF} P\} &\to \mathbf{S},\\ I &\mapsto \prod_{\eta\in I}\eta\end{aligned} \tag{152}$$

is a bijection. Moreover, every subset I of $\operatorname{PF} P$ satisfies

$$\begin{aligned}\mu\left(\prod_{\eta\in I}\eta\right) &= (-1)^{\left|\operatorname{PF}\left(\prod_{\eta\in I}\eta\right)\right|} \qquad \left(\text{since } \prod_{\eta\in I}\eta \text{ is squarefree}\right)\\ &= (-1)^{|I|} \qquad \left(\text{since } \operatorname{PF}\left(\prod_{\eta\in I}\eta\right) = I\right).\end{aligned} \tag{153}$$

Now, we claim the following:

Observation 5: Let $\pi \in \operatorname{PF} P$. Let $I \subseteq \operatorname{PF} P$ be such that $\pi \notin I$. Then,

$$Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}} \equiv Q^{q^{\deg\left(P/\left(\prod_{\eta\in I\cup\{\pi\}}\eta\right)\right)}} \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T].$$

[*Proof of Observation 5:* From $\pi \notin I$, we obtain

$$\prod_{\eta\in I\cup\{\pi\}}\eta = \pi\prod_{\eta\in I}\eta. \tag{154}$$

We have $I \subseteq \operatorname{PF} P$. Thus, the elements of I are monic irreducible divisors of P. In particular, the elements of I are monic irreducible polynomials in $\mathbb{F}_q[T]$. These monic irreducible polynomials are all distinct from π (since $\pi \notin I$), and therefore coprime to π (since π is irreducible). Hence, the elements of I are polynomials coprime to π. Therefore, $\prod_{\eta\in I}\eta$ is a product of polynomials coprime to π. Thus, $\prod_{\eta\in I}\eta$ itself is coprime to π. Consequently, $\pi \nmid \prod_{\eta\in I}\eta$.

But $\prod_{\eta\in I}\eta \in \mathbf{S}$ (since $\prod_{\eta\in I}\eta$ is the image of I under the bijection (152)). In other words, $\prod_{\eta\in I}\eta$ is a squarefree monic divisor of P. Hence, Observation 4 (applied

to $D = \prod_{\eta \in I} \eta$) yields

$$Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}} \equiv Q^{q^{\deg\left(P/\left(\pi\prod_{\eta\in I}\eta\right)\right)}} \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T].$$

In view of (154), this rewrites as

$$Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}} \equiv Q^{q^{\deg\left(P/\left(\prod_{\eta\in I\cup\{\pi\}}\eta\right)\right)}} \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T].$$

This proves Observation 5.]

Observation 6: Let $\pi \in \operatorname{PF} P$. Then,

$$\sum_{D\in\mathbf{S}} \mu(D)\, Q^{q^{\deg(P/D)}} \equiv 0 \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T].$$

[*Proof of Observation 6:* Recall that (152) is a bijection. Thus, we can substitute $\prod_{\eta\in I}\eta$ for D in the sum $\sum_{D\in\mathbf{S}} \mu(D)\, Q^{q^{\deg(P/D)}}$. Thus, we obtain

$$\begin{aligned}
&\sum_{D\in\mathbf{S}} \mu(D)\, Q^{q^{\deg(P/D)}} \\
&= \sum_{I\subseteq \operatorname{PF} P} \underbrace{\mu\left(\prod_{\eta\in I}\eta\right)}_{\substack{=(-1)^{|I|} \\ \text{(by (153))}}} Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}} = \sum_{I\subseteq \operatorname{PF} P} (-1)^{|I|}\, Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}} \\
&= \sum_{\substack{I\subseteq \operatorname{PF} P; \\ \pi\in I}} (-1)^{|I|}\, Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}} + \sum_{\substack{I\subseteq \operatorname{PF} P; \\ \pi\notin I}} (-1)^{|I|}\, Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}} \qquad (155)
\end{aligned}$$

(since every $I \subseteq \operatorname{PF} P$ satisfies either $\pi \in I$ or $\pi \notin I$ (but not both)).

But we have $\pi \in \operatorname{PF} P$. Hence, the map

$$\begin{aligned}
\{I \subseteq \operatorname{PF} P \mid \pi \notin I\} &\to \{I \subseteq \operatorname{PF} P \mid \pi \in I\}, \\
J &\mapsto J \cup \{\pi\}
\end{aligned}$$

is well-defined and a bijection[77]. Hence, we can substitute $J \cup \{\pi\}$ for I in the

[77] This is a particular case (obtained by setting $G = \operatorname{PF} P$ and $g = \pi$) of the following fact:

sum $\sum\limits_{\substack{I \subseteq \operatorname{PF} P; \\ \pi \in I}} (-1)^{|I|} Q^{q^{\deg\left(P/\prod\limits_{\eta\in I}\eta\right)}}$. We thus obtain

$$\begin{aligned}
&\sum_{\substack{I \subseteq \operatorname{PF} P; \\ \pi \in I}} (-1)^{|I|} Q^{q^{\deg\left(P/\prod\limits_{\eta\in I}\eta\right)}} \\
&= \sum_{\substack{J \subseteq \operatorname{PF} P; \\ \pi \notin J}} \underbrace{(-1)^{|J\cup\{\pi\}|}}_{\substack{=-(-1)^{|J|} \\ \text{(since } |J\cup\{\pi\}|=|J|+1 \\ \text{(since } \pi\notin J))}} Q^{q^{\deg\left(P/\prod\limits_{\eta\in J\cup\{\pi\}}\eta\right)}} = -\sum_{\substack{J \subseteq \operatorname{PF} P; \\ \pi \notin J}} (-1)^{|J|} Q^{q^{\deg\left(P/\prod\limits_{\eta\in J\cup\{\pi\}}\eta\right)}} \\
&= -\sum_{\substack{I \subseteq \operatorname{PF} P; \\ \pi \notin I}} (-1)^{|I|} Q^{q^{\deg\left(P/\prod\limits_{\eta\in I\cup\{\pi\}}\eta\right)}} \qquad (156)
\end{aligned}$$

(here, we have renamed the summation index J as I).

Let G be a set. Let $g \in G$. Then, the map

$$\begin{aligned}
\{I \subseteq G \mid g \notin I\} &\to \{I \subseteq G \mid g \in I\}, \\
J &\mapsto J \cup \{g\}
\end{aligned}$$

is well-defined and a bijection. (Its inverse is the map

$$\begin{aligned}
\{I \subseteq G \mid g \in I\} &\to \{I \subseteq G \mid g \notin I\}, \\
J &\mapsto J \setminus \{g\}.
\end{aligned}$$

This is all straightforward to check.)

Now, (155) becomes

$$\sum_{D\in\mathbf{S}} \mu(D)\, Q^{q^{\deg(P/D)}}$$

$$= \underbrace{\sum_{\substack{I\subseteq \operatorname{PF} P;\\ \pi\in I}} (-1)^{|I|}\, Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}}}_{=-\sum_{\substack{I\subseteq \operatorname{PF} P;\\ \pi\notin I}} (-1)^{|I|} Q^{q^{\deg\left(P/\prod_{\eta\in I\cup\{\pi\}}\eta\right)}} \text{ (by (156))}} + \sum_{\substack{I\subseteq \operatorname{PF} P;\\ \pi\notin I}} (-1)^{|I|} \underbrace{Q^{q^{\deg\left(P/\prod_{\eta\in I}\eta\right)}}}_{\equiv Q^{q^{\deg\left(P/\left(\prod_{\eta\in I\cup\{\pi\}}\eta\right)\right)}} \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T] \text{ (by Observation 5)}}$$

$$\equiv -\sum_{\substack{I\subseteq \operatorname{PF} P;\\ \pi\notin I}} (-1)^{|I|}\, Q^{q^{\deg\left(P/\prod_{\eta\in I\cup\{\pi\}}\eta\right)}} + \sum_{\substack{I\subseteq \operatorname{PF} P;\\ \pi\notin I}} (-1)^{|I|}\, Q^{q^{\deg\left(P/\left(\prod_{\eta\in I\cup\{\pi\}}\eta\right)\right)}}$$

$$= 0 \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T].$$

Thus, Observation 6 is proven.]

Recall that P is a monic polynomial. Hence, $\prod_{\pi\in\operatorname{PF} P} \pi^{v_\pi(P)}$ is the factorization of P into monic irreducible factors. Thus, $\prod_{\pi\in\operatorname{PF} P} \pi^{v_\pi(P)} = P$.

But the polynomials $\pi^{v_\pi(P)}$ for distinct $\pi \in \operatorname{PF} P$ are mutually coprime. Hence, their least common multiple is their product. In other words, the least common multiple of the polynomials $\pi^{v_\pi(P)}$ (where π ranges over $\operatorname{PF} P$) is $\prod_{\pi\in\operatorname{PF} P} \pi^{v_\pi(P)} = P$.

Now, define a polynomial $Z \in \mathbb{F}_q[T]$ by

$$Z = \sum_{D|P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}}.$$

Then, for every $\pi \in \operatorname{PF} P$, we have

$$Z = \sum_{D|P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}} = \sum_{D\in\mathbf{S}} \mu(D)\, Q^{q^{\deg(P/D)}} \qquad \text{(by Observation 3)}$$

$$\equiv 0 \bmod \pi^{v_\pi(P)}\mathbb{F}_q[T] \qquad \text{(by Observation 6)},$$

and thus $\pi^{v_\pi(P)} \mid Z$. Therefore, the least common multiple of the polynomials $\pi^{v_\pi(P)}$ (where π ranges over $\operatorname{PF} P$) divides Z. In other words, P divides Z (since the least common multiple of the polynomials $\pi^{v_\pi(P)}$ (where π ranges over $\operatorname{PF} P$) is P). Thus,

$$P \mid Z = \sum_{D|P} \varphi\left(\frac{P}{D}\right) Q^{q^{\deg D}}.$$

This proves Corollary 3.78 again. □

3.17. (More sections to be added here!)

[...]

XTODO: Conclude torsionfreeness in two ways.

XTODO: polynomial ring example.

[...]

4. Speculations

4.1. So what is Λ_{Carl} ?

So what is the Carlitz analogue of the ring of symmetric functions?

I'm still groping in the dark here. But at least I'm seeing some hints of why this isn't as simple as in the classical case (although I guess the theory of symmetric functions can only be called "simple" with the wisdom of hindsight anyway). After Subsection 2.5 it appears to me that the multiplication isn't crucial to the functor W_N, but rather an extra structure that gets carried along (whatever this means).[78] This suggests that I shouldn't be looking at the representing object of the functor $W_N : \mathbf{CRing}_{\mathbb{F}_q[T]} \to \mathbf{CRing}_{\mathbb{F}_q[T]}$, but at the representing object of the functor $W_N : {}_{\mathcal{F}}\mathbf{Mod} \to {}_{\mathcal{F}}\mathbf{Mod}$, or at least that the latter is more fundamental than the former. To begin with, it's smaller.

A representing object of a functor ${}_{\mathcal{F}}\mathbf{Mod} \to {}_{\mathcal{F}}\mathbf{Mod}$ is the same as an $\mathcal{F}$-$\mathcal{F}$-bimodule[79]. The $\mathcal{F}$-$\mathcal{F}$-bimodule which represents the functor $W_N : {}_{\mathcal{F}}\mathbf{Mod} \to {}_{\mathcal{F}}\mathbf{Mod}$ is the free left $\mathcal{F}$-module $\Lambda_{\mathcal{F}}$ with basis $(x_P)_{P \in N}$, and with right $\mathcal{F}$-module structure defined as follows: Let $p_P = \sum_{D|P} D\left[\frac{P}{D}\right](x_D)$ for every $P \in N$. (The intuition is that x_P are analogues of the "Witt vector coordinates" of Λ [80] and p_P are "power sum symmetric functions".) Then, set $p_P f = f p_P$ for every $P \in N$ and $f \in \mathcal{F}$. This uniquely determines a right $\mathcal{F}$-module structure (since it has to commute with the left one), although its existence is not really obvious. Thus $\Lambda_{\mathcal{F}}$ is defined.

When N is the whole set $\mathbb{F}_q[T]_+$, the $\mathcal{F}$-$\mathcal{F}$-bimodule $\Lambda_{\mathcal{F}}$ has some claims to be the Carlitz analogue of the ring of symmetric functions, although it is an $\mathcal{F}$-$\mathcal{F}$-bimodule rather than a ring. Nevertheless, I don't feel able to realize it as an actual set of symmetric power series. The Carlitz structure is way too additive for that. In some sense, what made the power sums algebraically independent over the integers was the fact that $(x+y)^2 \neq x^2 + y^2$ etc.; but in the Carlitz

[78] What about Lie algebras? What properties should a Lie algebra structure on an $\mathcal{F}$-module A satisfy so that $W_N(A)$ also is a Lie algebra? Will $W_N(A)$ then also share these properties?

[79] This is a particular case of the following general fact: If A and B are two algebras, then any A-B-bimodule M gives rise to a representable functor $\mathrm{Hom}_{{}_A\mathbf{Mod}}({}_AM, -) : {}_A\mathbf{Mod} \to {}_B\mathbf{Mod}$.

[80] These are the symmetric functions w_n in [6, Exercise 2.9.3]. Their name stems from their relation to the Witt vectors; from a combinatorial viewpoint, they are a rather exotic family.

case, $[P]$ is additive and even $\mathbb{F}_q$-linear for every $P \in \mathbb{F}_q[T]$, so that if we would define the "P-th power sum polynomial" in some variables ξ_i to mean $\sum_i [P](\xi_i)$, then all these polynomials would be linearly dependent over $\mathcal{F}$ simply because $\sum_i [P](\xi_i) = [P]\left(\sum_i \xi_i\right) = (\operatorname{Carl}(P))\left(\sum_i \xi_i\right)$.

The absence of multiplicative structure makes it hard to even guess what "elementary symmetric functions" or "complete homogeneous symmetric functions" would be in the Carlitz situation. But Carlitz exponential and Carlitz logarithm are well-defined on every left $\mathcal{F}$-module on which $\mathbb{F}_q[T]$ acts invertibly (i. e., whose $\mathbb{F}_q[T]$-module structure extends to an $\mathbb{F}_q(T)$-module structure) and which has appropriate closure properties. We might try to use them to construct the "elementary symmetric functions" by some analogue of the classical $\sum_{n\in\mathbb{N}} (-1)^n e_n T^n = \exp\left(-\sum_{n\geq 1} \frac{1}{n} p_n T^n\right)$ formula from the theory of symmetric functions.[81] The problem is that this is an identity in power series, and we would first have to find out what the right analogue of power series is in this context.

There is other stuff to do as well. One can look for explicit formulas for the right $\mathcal{F}$-action on the x_P in $\Lambda_{\mathcal{F}}$. And one can try to define the analogue of plethysm (which, as far as I understand, should be an $\mathcal{F}$-$\mathcal{F}$-bilinear map from $\Lambda_{\mathcal{F}} \otimes_{\mathcal{F}} \Lambda_{\mathcal{F}}$ to $\Lambda_{\mathcal{F}}$ making $\Lambda_{\mathcal{F}}$ into what would be an $\mathcal{F}$-algebra if it were commutative?).

4.2. Some computations in $\Lambda_{\mathcal{F}}$

Let me see if I'm able to get something concrete out of the above reveries. How about computing the right $\mathcal{F}$-action on concrete basis elements of $\Lambda_{\mathcal{F}}$?

Assume that N is the whole $\mathbb{F}_q[T]_+$.

By definition, $p_1 = x_1$, so that $\boxed{x_1 f = f x_1 \text{ for every } f \in \mathcal{F}}$ (since $p_1 f = f p_1$ for every $f \in \mathcal{F}$). That is, x_1 is central with respect to the two $\mathcal{F}$-actions. Nothing to see here.

By definition, $p_T = \underbrace{[T](x_1)}_{=(F+T)x_1} + T x_T = (F+T)x_1 + T x_T$. Now, $p_T f = f p_T$ for every $f \in \mathcal{F}$. Apply this to $f = T$ and substitute $p_T = (F+T)x_1 + T x_T$; you obtain

$$((F+T)x_1 + T x_T)\, T = T\,((F+T)x_1 + T x_T).$$

[81] Another suggestion by James Borger.

Since

$$\begin{aligned}((F+T)\,x_1+Tx_T)\,T &= (F+T)\underbrace{x_1T}_{\substack{=Tx_1\\ \text{(since } x_1 \text{ is central)}}}+Tx_TT = \underbrace{(F+T)\,Tx_1}_{=T\left(T^{q-1}F+T\right)x_1}+Tx_TT\\ &= T\left(\left(T^{q-1}F+T\right)x_1+x_TT\right),\end{aligned}$$

this rewrites as $T\left(\left(T^{q-1}F+T\right)x_1+x_TT\right) = T\left((F+T)\,x_1+Tx_T\right)$. Since T is a left non-zero-divisor in $\mathcal{F}$ and thus also in $\Lambda_{\mathcal{F}}$ (as $\Lambda_{\mathcal{F}}$ is a free left $\mathcal{F}$-module), we can cancel the T out of this, and obtain $\left(T^{q-1}F+T\right)x_1+x_TT = (F+T)\,x_1+Tx_T$. Hence, $x_TT = (F+T)\,x_1+Tx_T-\left(T^{q-1}F+T\right)x_1$. This simplifies to

$$\boxed{x_TT = Tx_T-\left(T^{q-1}-1\right)Fx_1}.$$

Let's do x_TF. Apply $p_Tf = fp_T$ to $f = F$, and substitute $p_T = (F+T)\,x_1+Tx_T$ again; the result is

$$((F+T)\,x_1+Tx_T)\,F = F\left((F+T)\,x_1+Tx_T\right).$$

Subtraction of $(F+T)\,x_1F$ turns this into

$$\begin{aligned}Tx_TF &= F\left((F+T)\,x_1+Tx_T\right)-(F+T)\,x_1F\\ &= FFx_1+\underbrace{FT}_{=T^qF}x_1+\underbrace{FT}_{=T^qF}x_T-F\underbrace{x_1T}_{\substack{=Fx_1\\ \text{(since } x_1 \text{ is central)}}}-Tx_1F\\ &= FFx_1+T^qFx_1+T^qFx_T-FFx_1-Tx_1F = T^qFx_1+T^qFx_T-Tx_1F\\ &= T\left(T^{q-1}Fx_1+T^{q-1}Fx_T-x_1F\right).\end{aligned}$$

Cancelling T, we obtain

$$x_TF = T^{q-1}Fx_1+T^{q-1}Fx_T-\underbrace{x_1F}_{\substack{=Fx_1\\ \text{(since } x_1 \text{ is central)}}}T^{q-1}Fx_1+T^{q-1}Fx_T-Fx_1.$$

This simplifies to $\boxed{x_TF = \left(T^{q-1}-1\right)Fx_1+T^{q-1}Fx_T}$.

Let's be more bold and try a general irreducible polynomial, just to see how far we can simplify. Let $\pi\in\mathbb{F}_q[T]_+$ be irreducible. What is $x_\pi T$? As usual, $p_\pi = (\operatorname{Carl}\pi)\,x_1+\pi x_\pi$ satisfies $p_\pi f = fp_\pi$ for every $f\in\mathcal{F}$. Applying this to $f = T$ and substituting $p_\pi = (\operatorname{Carl}\pi)\,x_1+\pi x_\pi$, we get

$$((\operatorname{Carl}\pi)\,x_1+\pi x_\pi)\,T = T\left((\operatorname{Carl}\pi)\,x_1+\pi x_\pi\right).$$

Subtracting $(\operatorname{Carl}\pi)\, x_1 T$ from here, we get

$$\begin{aligned}\pi x_\pi T &= T\left((\operatorname{Carl}\pi)\, x_1 + \pi x_\pi\right) - (\operatorname{Carl}\pi)\, x_1 T \\ &= T\,(\operatorname{Carl}\pi)\, x_1 + T\pi x_\pi - (\operatorname{Carl}\pi) \underbrace{x_1 T}_{\substack{=Tx_1 \\ \text{(since } x_1 \text{ is central)}}} \\ &= T\,(\operatorname{Carl}\pi)\, x_1 + T\pi x_\pi - (\operatorname{Carl}\pi)\, Tx_1 \\ &= T\pi x_\pi + [T, \operatorname{Carl}\pi]\, x_1.\end{aligned}$$

Thus, $[T, \operatorname{Carl}\pi]$ must lie in $\pi\mathcal{F}$, and an explicit formula for the quotient would be very useful. Well, the fact that $[T, \operatorname{Carl}\pi]$ lies in $\pi\mathcal{F}$ is easily derived from (4), but there seems to be no way to write the quotient in finite terms. Let us rather introduce a notation for it: Let $\eth_T(\pi)$ denote the (unique) $f \in \mathcal{F}$ satisfying $[T, \operatorname{Carl}\pi] = \pi f$ (for π irreducible monic). In more elementary (and commutative) terms, $\eth_T(\pi) = \dfrac{T[\pi](X) - [\pi](TX)}{\pi}$. Now,

$$\pi x_\pi T = \underbrace{T\pi}_{=\pi T} x_\pi + \underbrace{[T, \operatorname{Carl}\pi]}_{=\pi\eth_T(\pi)} x_1 = \pi T x_\pi + \pi \eth_T(\pi)\, x_1.$$

Cancelling π, we obtain $\boxed{x_\pi T = T x_\pi + \eth_T(\pi)\, x_1}$.

The question is: Do we get $x_\pi F$ explicitly using $\eth_T(\pi)$, or will we have to introduce another new operator? Apply $p_\pi f = f p_\pi$ to $f = F$ and substitute $p_\pi = (\operatorname{Carl}\pi)\, x_1 + \pi x_\pi$. The result is

$$\left((\operatorname{Carl}\pi)\, x_1 + \pi x_\pi\right) F = F\left((\operatorname{Carl}\pi)\, x_1 + \pi x_\pi\right).$$

Subtracting $(\operatorname{Carl}\pi)\, x_1 F$ from here, we get

$$\begin{aligned}\pi x_\pi F &= F\left((\operatorname{Carl}\pi)\, x_1 + \pi x_\pi\right) - (\operatorname{Carl}\pi)\, x_1 F \\ &= F\,(\operatorname{Carl}\pi)\, x_1 + F\pi x_\pi - (\operatorname{Carl}\pi) \underbrace{x_1 F}_{\substack{=Fx_1 \\ \text{(since } x_1 \text{ is central)}}} \\ &= F\,(\operatorname{Carl}\pi)\, x_1 + F\pi x_\pi - (\operatorname{Carl}\pi)\, Fx_1 \\ &= F\pi x_\pi + [F, \operatorname{Carl}\pi]\, x_1.\end{aligned}$$

Oh, but $[F, \operatorname{Carl}\pi] + [T, \operatorname{Carl}\pi] = \left[\underbrace{F+T}_{=\operatorname{Carl}T}, \operatorname{Carl}\pi\right] = [\operatorname{Carl}T, \operatorname{Carl}\pi] = \operatorname{Carl}\underbrace{[T,\pi]}_{=0} =$ 0, so that $[F, \operatorname{Carl}\pi] = -\underbrace{[T, \operatorname{Carl}\pi]}_{=\pi\eth_T(\pi)} = -\pi\eth_T(\pi)$. Hence,

$$\pi x_\pi F = F\pi x_\pi + \underbrace{[F, \operatorname{Carl}\pi]}_{=-\pi\eth_T(\pi)} x_1 = \underbrace{F\pi}_{=\pi^q F} x_\pi - \pi\eth_T(\pi)\, x_1 = \pi^q F x_\pi - \pi\eth_T(\pi)\, x_1.$$

Cancelling π, we obtain $\boxed{x_\pi F = \pi^{q-1} F x_\pi - \eth_T(\pi)\, x_1}$.

5. The logarithm series

Here is my result on the logarithm series, which so far has not found any application.

Theorem 5.1. Let q be a prime power. Consider the Carlitz logarithm $\log_C \in \mathbb{F}_q(T)[[X]]$ defined in [3, Section 7] (but with q instead of p). Then, in the power series ring $\mathbb{F}_q(T)[[X, S]]$, we have

$$\log_C(SX) = \sum_{N \in \mathbb{F}_q[T]_+} (-1)^{\deg N} S^{q^{\deg N}} \frac{[N](X)}{N}. \tag{157}$$

(The right hand side of this converges in the usual topology on $\mathbb{F}_q[[X, S]]$.)

Let us recall the definition of $\log_C$ for the sake of completeness: For every $j \in \mathbb{N}$, let L_j be the polynomial $\left(T^{q^j} - T\right)\left(T^{q^{j-1}} - T\right)...\left(T^{q^1} - T\right) \in \mathbb{F}_q[T]$. Then, $\log_C \in \mathbb{F}_q(T)[[X]]$ is defined by

$$\log_C(X) = \sum_{j \in \mathbb{N}} (-1)^j \frac{X^{q^j}}{L_j}. \tag{158}$$

It should be noticed that it is possible to specialize S to 1 in (157), but then the right hand side will only be convergent in a rather weak sense (it will only converge if all terms with N having a given degree are first added up, and then the sums are being summed over the degree rather than the single terms).

In contrast to the preceding results, Theorem 5.1 seems to be neither straightforward nor provable by translating some classical argument. So let me sketch a proof (which is rather roundabout and hopefully simplifiable). First, I need an auxiliary result which itself seems rather interesting:

Proposition 5.2. Let q be a prime power. Let A be a commutative $\mathbb{F}_q$-algebra. Let $n \in \mathbb{N}$. Let $P \in A[X]$ be a polynomial such that $\deg P < q^n - 1$. Let e_1, e_2, ..., e_n be n elements of A. Then,

$$\sum_{(\lambda_1, \lambda_2, ..., \lambda_n) \in \mathbb{F}_q^n} P(\lambda_1 e_1 + \lambda_2 e_2 + ... + \lambda_n e_n) = 0.$$

Proof of Proposition 5.2 (sketch). We can WLOG assume that $P = X^k$ for some $k \in \{0, 1, ..., q^n - 2\}$. Assume this and consider this k. Since $k < q^n - 1$, we can write k in the form $k = k_{n-1}q^{n-1} + k_{n-2}q^{n-2} + ... + k_0 q^0$ with $k_i < q$ and with $k_0 + k_1 + ... + k_{n-1} \leq n(q-1) - 1$. Thus,

$$P = X^k = X^{k_{n-1}q^{n-1} + k_{n-2}q^{n-2} + ... + k_0 q^0} = \prod_{i=0}^{n-1} X^{k_i q^i} = \prod_{i=0}^{n-1} \left(X^{q^i}\right)^{k_i}.$$

Hence,

$$\sum_{(\lambda_1,\lambda_2,...,\lambda_n)\in\mathbb{F}_q^n} P\left(\lambda_1 e_1+\lambda_2 e_2+...+\lambda_n e_n\right)$$

$$= \sum_{(\lambda_1,\lambda_2,...,\lambda_n)\in\mathbb{F}_q^n} \prod_{i=0}^{n-1} \left(\underbrace{\left(\lambda_1 e_1+\lambda_2 e_2+...+\lambda_n e_n\right)^{q^i}}_{\substack{=\lambda_1 e_1^{q^i}+\lambda_2 e_2^{q^i}+...+\lambda_n e_n^{q^i} \\ \text{(since we are over } \mathbb{F}_q\text{)}}} \right)^{k_i}$$

$$= \sum_{(\lambda_1,\lambda_2,...,\lambda_n)\in\mathbb{F}_q^n} \prod_{i=0}^{n-1} \left(\lambda_1 e_1^{q^i}+\lambda_2 e_2^{q^i}+...+\lambda_n e_n^{q^i}\right)^{k_i}.$$

Now, consider the product $\prod_{i=0}^{n-1} \left(\lambda_1 e_1^{q^i}+\lambda_2 e_2^{q^i}+...+\lambda_n e_n^{q^i}\right)^{k_i}$ **as a polynomial (over A) in the variables** λ_1, λ_2, ..., λ_n. Then, it is a polynomial of degree $k_0+k_1+...+k_{n-1} \leq n(q-1)-1$. It is well-known (e. g., from the proof of the Chevalley-Warning theorem) that any such polynomial yields 0 when summed over all $(\lambda_1,\lambda_2,...,\lambda_n) \in \mathbb{F}_q^n$ (because each of its monomials has at least one exponent $< q-1$, and then summing the variable which has this exponent over $\mathbb{F}_q$ already gives 0 with all other variables remaining fixed). This proves Proposition 5.2.

Another auxiliary result:

Proposition 5.3. Let q be a prime power. Let L be a field extension of $\mathbb{F}_q$. Let V be a finite $\mathbb{F}_q$-vector subspace of L. Let $t \in L \setminus V$. Then,

$$\sum_{v\in V} \frac{1}{t+v} = \left(\prod_{v\in V} \frac{1}{t+v}\right) \cdot \left(\prod_{v\in V\setminus 0} v\right).$$

Proof of Proposition 5.3 (sketched). Let W be the polynomial $\prod_{v\in V} (X+v) \in L[X]$. This polynomial is a q-polynomial (indeed, Theorem 3.17 (applied to $L=A$) shows that f_V is a q-polynomial, but clearly $f_V = W$); hence, its derivative equals its coefficient in front of X^1 (because the derivative of any q-polynomial in characteristic $p \mid q$ equals its coefficient in front of X^1). But this coefficient is $\prod_{v\in V\setminus 0} v$. Thus, we know that the derivative of W equals $\prod_{v\in V\setminus 0} v$. Hence, $W'(t) = \prod_{v\in V\setminus 0} v$.

On the other hand, since $W = \prod_{v \in V} (X + v)$, the Leibniz formula yields

$$W' = \sum_{w \in V} \underbrace{(X+w)'}_{=1} \cdot \prod_{\substack{v \in V; \\ v \neq w}} (X+v) = \sum_{w \in V} \prod_{\substack{v \in V; \\ v \neq w}} (X+v) = \sum_{w \in V} \frac{\prod_{v \in V} (X+v)}{X+w}$$
$$= \left(\prod_{v \in V} (X+v) \right) \cdot \left(\sum_{w \in V} \frac{1}{X+w} \right).$$

Applying this to $X = t$, we obtain

$$W'(t) = \left(\prod_{v \in V} (t+v) \right) \cdot \left(\sum_{w \in V} \frac{1}{t+w} \right),$$

so that

$$\sum_{w \in V} \frac{1}{t+w} = \frac{1}{\prod_{v \in V} (t+v)} \cdot \underbrace{W'(t)}_{= \prod_{v \in V \setminus 0} v} = \frac{1}{\prod_{v \in V} (t+v)} \cdot \left(\prod_{v \in V \setminus 0} v \right)$$
$$= \left(\prod_{v \in V} \frac{1}{t+v} \right) \cdot \left(\prod_{v \in V \setminus 0} v \right).$$

Rename the index w as v and obtain the claim of Proposition 5.3.

Proof of Theorem 5.1 (sketched). By (158), we have

$$\log_C (SX) = \sum_{j \in \mathbb{N}} (-1)^j \frac{(SX)^{q^j}}{L_j} = \sum_{j \in \mathbb{N}} (-1)^j S^{q^j} \frac{X^{q^j}}{L_j}.$$

Hence, it is clearly enough to show that every $m \in \mathbb{N}$ satisfies

$$\frac{X^{q^m}}{L_m} = \sum_{\substack{N \in \mathbb{F}_q[T]_+; \\ \deg N = m}} \frac{[N](X)}{N}. \tag{159}$$

So let $m \in \mathbb{N}$. Introduce the polynomials $E_j(Y) \in \mathbb{F}_q(T)[Y]$ for all $j \in \mathbb{N}$ as in [3, Section 7], but with q instead of p. Let's spell out their definition: With e_C denoting the Carlitz exponential, the power series $e_C(Y \log_C X) \in \mathbb{F}_q(T)[[X, Y]]$ is a q-power series, i. e., its coefficient before $X^\alpha Y^\beta$ can only be nonzero if both α and β are powers of q. Now, for every $j \in \mathbb{N}$, define $E_j(Y)$ to be the coefficient of this power series $e_C(Y \log_C X)$, **regarded as a power series in** X **over** $\mathbb{F}_q(T)[Y]$, before X^{q^j}. Of course, this $E_j(Y)$ is a q-polynomial in $\mathbb{F}_q(T)[Y]$. Moreover, $\deg(E_j) = q^j$ and $E_j(0) = 0$ for all $j \in \mathbb{N}$. Furthermore, $E_j(M) = 0$

for every $M \in \mathbb{F}_q[T]$ satisfying $\deg M < j$. Finally, $E_j(M) = 1$ for every $M \in \mathbb{F}_q[T]$ satisfying $\deg M = j$. But most importantly, $[M](X) = \sum_{j \in \mathbb{N}} E_j(M) X^{q^j}$ in $\mathbb{F}_q(T)[X]$ for every $M \in \mathbb{F}_q[T]$. Hence, for every nonzero $M \in \mathbb{F}_q(T)[X]$, we have

$$\begin{aligned}
\frac{[M](X)}{M} &= \frac{\sum_{j \in \mathbb{N}} E_j(M) X^{q^j}}{M} = \sum_{j \in \mathbb{N}} \frac{E_j(M)}{M} X^{q^j} = \sum_{j=0}^{\deg M} \frac{E_j(M)}{M} X^{q^j} \\
&\qquad \left(\text{since } E_j(M) = 0 \text{ whenever } \deg M < j\right) \\
&= \sum_{j=0}^{\deg M - 1} \frac{E_j(M)}{M} X^{q^j} + \underbrace{\frac{E_{\deg M}(M)}{M}}_{\substack{= \frac{1}{M} \\ (\text{since } E_j(M) = 1 \text{ whenever } \deg M = j)}} X^{q^{\deg M}} \\
&= \sum_{j=0}^{\deg M - 1} \frac{E_j(M)}{M} X^{q^j} + \frac{1}{M} X^{q^{\deg M}} \qquad (160)
\end{aligned}$$

But since $E_j(0) = 0$ for all $j \in \mathbb{N}$, we know that for every $j \in \mathbb{N}$, the polynomial $E_j(Y)$ is divisible by Y. Thus, $\frac{E_j(Y)}{Y}$ is a polynomial of degree $q^j - 1$ for every $j \in \mathbb{N}$ (since $\deg\left(E_j\right) = q^j$). Renaming Y as X, we see that $\frac{E_j(X)}{X}$ is a polynomial of degree $q^j - 1$ for every $j \in \mathbb{N}$. Hence, $\frac{E_j(X + T^m)}{X + T^m} \in \mathbb{F}_q(T)[X]$ also is a polynomial of degree $q^j - 1$ for every $j \in \mathbb{N}$. Hence, for every $j \in \{0, 1, ..., m-1\}$, we can apply Proposition 5.2 to $A = \mathbb{F}_q(T)$, $n = m$, $P = \frac{E_j(X + T^m)}{X + T^m}$ and $e_i = T^{i-1}$, and conclude that

$$\sum_{(\lambda_1, \lambda_2, ..., \lambda_m) \in \mathbb{F}_q} \frac{E_j\left(\lambda_1 T^0 + \lambda_2 T^1 + ... + \lambda_m T^{m-1} + T^m\right)}{\lambda_1 T^0 + \lambda_2 T^1 + ... + \lambda_m T^{m-1} + T^m} = 0$$

(since $j < m$ and thus $q^j - 1 < q^m - 1$). Since the sums of the form $\lambda_1 T^0 + \lambda_2 T^1 + ... + \lambda_m T^{m-1} + T^m$ with $(\lambda_1, \lambda_2, ..., \lambda_m) \in \mathbb{F}_q$ are precisely the monic polynomials in $\mathbb{F}_q[T]$ with degree m (each appearing exactly once), this rewrites as

$$\sum_{\substack{N \in \mathbb{F}_q[T]_+; \\ \deg N = m}} \frac{E_j(N)}{N} = 0 \qquad \text{for every } j \in \{0, 1, ..., m-1\}. \qquad (161)$$

Now,

$$\sum_{\substack{N\in\mathbb{F}_q[T]_+;\\ \deg N=m}} \frac{[N](X)}{N}$$

$$= \sum_{\substack{N\in\mathbb{F}_q[T]_+;\\ \deg N=m}} \left(\sum_{j=0}^{\deg N-1} \frac{E_j(N)}{N} X^{q^j} + \frac{1}{N} X^{q^{\deg N}} \right)$$

(here we applied (160) to $M = N$)

$$= \sum_{j=0}^{m-1} \underbrace{\sum_{\substack{N\in\mathbb{F}_q[T]_+;\\ \deg N=m}} \frac{E_j(N)}{N}}_{\substack{=0\\ \text{(by (161))}}} X^{q^j} + \sum_{\substack{N\in\mathbb{F}_q[T]_+;\\ \deg N=m}} \frac{1}{N} X^{q^m}$$

$$= \sum_{\substack{N\in\mathbb{F}_q[T]_+;\\ \deg N=m}} \frac{1}{N} X^{q^m} = \sum_{\substack{v\in\mathbb{F}_q[T];\\ \deg v<m}} \frac{1}{T^m+v} X^{q^m}$$

$$\left(\begin{array}{c} \text{since the monic polynomials in } \mathbb{F}_q[T] \text{ of degree } m \text{ are exactly} \\ \text{the sums of the form } T^m+v \text{ with } v \text{ being a polynomial in} \\ \mathbb{F}_q[T] \text{ of degree } < m \end{array} \right)$$

$$= \left(\prod_{\substack{v\in\mathbb{F}_q[T];\\ \deg v<m}} \frac{1}{T^m+v} \right) \cdot \left(\prod_{\substack{v\in\mathbb{F}_q[T];\\ \deg v<m;\\ v\neq 0}} v \right) X^{q^m}$$

$$\left(\begin{array}{c} \text{by Proposition 5.3, applied to } L=\mathbb{F}_q(T),\ t=T^m \\ \text{and } V=\left\{v\in\mathbb{F}_q[T] \mid \deg v<m\right\} \end{array} \right)$$

$$= \underbrace{\left(\prod_{\substack{N\in\mathbb{F}_q[T]_+;\\ \deg N=m}} \frac{1}{N} \right) \cdot \left(\prod_{\substack{v\in\mathbb{F}_q[T];\\ \deg v<m;\\ v\neq 0}} v \right)}_{\substack{=\frac{1}{L_m}\\ \text{(this is relatively straightforward to prove}\\ \text{using standard results on finite fields)}}} X^{q^m} = \frac{X^{q^m}}{L_m}.$$

This proves (159) and thus Theorem 5.1.

I hope there is a better proof.

References

[1] James Borger, *The basic geometry of Witt vectors, I: The affine case*, Algebra & Number Theory 5 (2011), no. 2, pp 231–285. Also available as preprint arXiv:0801.1691v6.
http://arxiv.org/abs/0801.1691v6

[2] James Borger, Ben Wieland, *Plethystic algebra*, arXiv:math/0407227v1.
http://arxiv.org/abs/math/0407227v1

[3] Keith Conrad, *Carlitz extensions*.
http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/carlitz.pdf

[4] Tom Denton, Florent Hivert, Anne Schilling, Nicolas M. Thiéry, *On the representation theory of finite $\mathcal{J}$-trivial monoids*, arXiv:1010.3455v3. http://arxiv.org/abs/1010.3455v3

[5] Tobias Dyckerhoff, *Hall Algebras - Bonn, Wintersemester 14/15*, lecture notes, February 5, 2015.
http://www.math.uni-bonn.de/people/dyckerho/notes.pdf

[6] Darij Grinberg, Victor Reiner, *Hopf algebras in Combinatorics*, version of 11 May 2018, arXiv:1409.8356v5.
See also http://www.cip.ifi.lmu.de/~grinberg/algebra/HopfComb-sols.pdf for a version that gets updated.

[7] Darij Grinberg, *Witt#5: Around the integrality criterion 9.93*, sidenote to Michiel Hazewinkel's "Witt vectors. Part 1".
http://mit.edu/~darij/www/algebra/witt5.pdf

[8] Darij Grinberg, *Witt#5c: The Chinese Remainder Theorem for Modules*, sidenote to Michiel Hazewinkel's "Witt vectors. Part 1".
http://mit.edu/~darij/www/algebra/witt5c.pdf

[9] Darij Grinberg, *Witt#5f: Ghost-Witt integrality for binomial rings*, sidenote to Michiel Hazewinkel's "Witt vectors. Part 1".
http://mit.edu/~darij/www/algebra/witt5f.pdf

[10] Michiel Hazewinkel, *Witt vectors. Part 1*, arXiv:0804.3888.
http://arxiv.org/abs/0804.3888v1

[11] Lars Hesselholt, *The big de Rham-Witt complex*, Acta Math. 214 (2015), pp. 135–207.
A preprint is also available as arXiv:1006.3125v3: http://arxiv.org/abs/1006.3125v3

[12] Lars Hesselholt, *Lecture notes on Witt vectors*, MIT, Cambridge, Massachusetts, USA, 2005.
http://www.math.nagoya-u.ac.jp/~larsh/papers/s03/wittsurvey.pdf

[13] Levent, *math.stackexchange post #1824797 ("Show that* $\sum_{d|f} \varphi\left(\frac{f}{d}\right) a^{|d|} \equiv 0 \bmod f$*")*. http://math.stackexchange.com/q/1824797

[14] Nathan Jacobson, *Restricted Lie algebras of characteristic p*, Trans. Amer. Math. Soc. **50** (1941), pp. 15–25.
http://www.ams.org/journals/tran/1941-050-01/
S0002-9947-1941-0005118-0/home.html

[15] I. G. Macdonald, *Schur functions: Theme and variations*, Séminaire Lotharingien de Combinatoire 28, B28a (1992).
http://www.emis.de/journals/SLC/opapers/s28macdonald.html

[16] Oystein Ore, *On a Special Class of Polynomials*, Trans. Amer. Math. Soc. **35** (1933), pp. 559–584.
http://www.ams.org/journals/tran/1933-035-03/
S0002-9947-1933-1501703-0/

[17] Oystein Ore, *Errata in my paper: "On a special class of polynomials" [Trans. Amer. Math. Soc. 35 (1933), no. 3, 559-584; 1501703]*, Trans. Amer. Math. Soc. **36** (1934), p. 275.
http://www.ams.org/journals/tran/1934-036-02/
S0002-9947-1934-1501741-9/

[18] Joseph Rabinoff, *The Theory of Witt Vectors*.
http://www.math.harvard.edu/~rabinoff/misc/witt.pdf

[19] Richard Stanley, *Enumerative Combinatorics, volume 2*, Cambridge University Press 2001.