Do the symmetric functions have a function-field analogue?

Darij Grinberg

draft, version 1.2, February 14, 2016

Contents

0.1. Remark on Borger’s work ........................................... 3

1. Notations ...................................................................... 3
1.1. General number theory .............................................. 3
1.2. Algebra ................................................................. 4
1.3. Carlitz polynomials .................................................. 4

2. The Carlitz-Witt suite .................................................. 6
2.1. The classical ghost-Witt equivalence theorem ............... 6
2.2. Classical Witt vectors .............................................. 7
2.3. The Carlitz ghost-Witt equivalence theorem ................. 10
2.4. Carlitz-Witt vectors ................................................. 12
2.5. $F$-modules .......................................................... 17

3. Proofs .......................................................................... 19
3.1. The skew polynomial ring $\mathcal{M}$ ................................. 19
3.2. The skew polynomial ring $\mathcal{F}$ ................................ 33
3.3. $q$-polynomials ...................................................... 36
3.4. $q$-polynomials from subspaces ................................. 44
3.5. Further consequences of the $F_{q}pol$ isomorphism ........... 49
3.6. Frobenius $F_{q}[T]$-modules .................................... 51
3.7. The Carlitz action ................................................... 57
3.8. “Fermat’s Little Theorem” for the Carlitz action ............. 59

4. Speculations .................................................................. 62
4.1. So what is $\Lambda_{\text{Carl}}$? ........................................... 62
4.2. Some computations in $\Lambda_{\mathcal{F}}$ ................................. 63
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 $\Lambda$ of symmetric functions as $\mathbb{F}_q$ has to the "mythical field $\mathbb{F}_1$"?

This question allows for at least two different interpretation. 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 reinterpretated (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 $\Lambda$ itself (rather than just its structure coefficients). Namely, recall that all (or most) of the usual bases of $\Lambda$ 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 "weakly decreasing" (in the sense that each term divides the preceding one) sequence of monic polynomials in $\mathbb{F}_q[T]$, or, equivalently, a conjugacy class of a matrix in $\text{GL}_n(\mathbb{F}_q)$. 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 $\Lambda$ 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 $\Lambda$ as the coordinate ring of the affine group of Witt vectors ([9, §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 $\Lambda$. But this answer is lacking something very important: the combinatorial bases. The most interesting structure on the ring $\Lambda$ of symmetric functions is not so much its Hopf algebra structure, but its various bases, such as the homogeneous symmetric functions $\left(h_\lambda\right)_{\lambda \in \text{Par}}$, the elementary symmetric functions $\left(e_\lambda\right)_{\lambda \in \text{Par}}$ and the Schur functions $\left(s_\lambda\right)_{\lambda \in \text{Par}}$. I am unable to find a counterpart to any of the bases just mentioned in the $\mathbb{F}_q$-analogue of $\Lambda$ suggested. All I can offer is an analogue of the power-sum functions $\left(p_\lambda\right)_{\lambda \in \text{Par}}$ (which do not even form a basis, although with functoriality they are sufficient for many computational purposes) and of a basis $\left(w_\lambda\right)_{\lambda \in \text{Par}}$ defined in [6, Exercise 2.79 (c)] (which, while having interesting properties, hardly feels at home in combinatorics). So the $\mathbb{F}_q$-analogue of $\Lambda$ I find is somewhat of an empty shell. Still, there are some surprises and my hope is not lost.

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 2.22 and Theorem 2.27), 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 vector 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 (actu-
ally, one of many constructions) of the Witt vectors, and then introduce the $\mathbb{F}_q$-analogue of this construction. In Section 4, we speculate on how this analogue could lead to an $\mathbb{F}_q$-analogue of $\Lambda$. Finally, 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 ([16] or [9] or [10, §1]) and a bit about Carlitz polynomials ([3]). Symmetric functions will only be really used in Section 4.

0.1. 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 $W_N$ given in Corollary 2.25 below is the same as the one for $W^\text{fl}_{R,E} (A)$ 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 $\{0, 1, 2, \ldots\}$, and $\mathbb{N}_+$ the set $\{1, 2, 3, \ldots\}$.

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 [16]).

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

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 $\text{PF} n$ the set of all prime divisors of $n$.

We let $\mu$ denote the Möbius function and $\phi$ 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. 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 \( \sum_{D | M} a_D \) 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 \( \text{PF}_M \) will denote the set of all monic irreducible divisors of \( M \) (rather than all irreducible divisors of \( M \)). Finally, if \( \pi \) 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 \( \pi^m | f \); this is set to be \( +\infty \) if \( f = 0 \).

### 1.2. Algebra

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

We denote by \( \Lambda \) the ring of symmetric functions over \( \mathbb{Z} \). (This is also known as \( \text{Symm} \) or \( \text{Sym} \). See [6, §2] and [17, Chapter 7] for studies of this ring \( \Lambda \).)

### 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 \( \mathbb{F}_p \) will be called \( \mathbb{F}_q \) 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 \( [T^0] = X \) and \( [T^n] = [T^{n-1}]^q + T[T^{n-1}] \) for every \( n \geq 1 \). For example,

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

(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 \( a_0 [T^0] + a_1 [T^1] + \cdots + a_k [T^k] \), where the polynomial \( M \) is written in the form \( M = a_0 T^0 + a_1 T^1 + \cdots + a_k T^k \). (In other words, we define a polynomial

---

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

$$[\pi] (X) \equiv X^{\deg \pi} \mod \pi$$

for any monic irreducible $\pi \in \mathbb{F}_q[T]$. (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

$$\mu (M) = \begin{cases} (-1)^{[PF M]} & \text{if } M \text{ is squarefree;} \\ 0 & \text{if } M \text{ is not squarefree} \end{cases}$$

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

$$\varphi_C (M) = M \prod_{\pi \in PF M} \left( 1 - \frac{1}{\pi} \right) = \sum_{D|M} \mu (D) \frac{M}{D}$$

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

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

$$\varphi (M) = q^{\deg M} \prod_{\pi \in PF M} \left( 1 - \frac{1}{q^{\deg \pi}} \right) = \sum_{D|M} \mu (D) q^{\deg (M/D)}$$

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

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 \( \varphi_n \) is an endomorphism of the ring \( A \).

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

**Assumption 3:** We have \( \varphi_1 = \text{id} \), 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 \( C, D, E, F, G, H, \) and \( J \) are equivalent:

**Assertion \( C \):** Every \( n \in N \) and every \( p \in \mathbb{P} \) satisfies

\[
\varphi_p (b_{n/p}) \equiv b_n \mod p^{\nu_p(n)} A.
\]

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

\[
\left( b_n = \sum_{d | n} dx_d^{n/d} \text{ for every } n \in N \right).
\]

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

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

**Assertion \( F \):** Every \( n \in N \) satisfies

\[
\sum_{d | n} \mu (d) \varphi_d (b_{n/d}) \in nA.
\]

**Assertion \( G \):** Every \( n \in N \) satisfies

\[
\sum_{d | n} \phi (d) \varphi_d (b_{n/d}) \in nA.
\]

**Assertion \( H \):** Every \( n \in N \) satisfies

\[
\sum_{i=1}^{n} \varphi_{n/gcd(i,n)} (b_{gcd(i,n)}) \in nA.
\]

**Assertion \( J \):** There exists a ring homomorphism from the ring \( \Lambda \) 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 \((b_n)_{n \in \mathbb{N}} \subseteq A^N\) which satisfy the equivalent assertions \(C, D, E, F, G, H,\) and \(J\) 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 \(\varphi_n = \text{id}_A\) for all \(n \in \mathbb{N}\), 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 to take the case where \(A\) is a polynomial ring \(\mathbb{Z}[\Xi]\) for some family \(\Xi\) of indeterminates, and the maps \(\varphi_n\) are defined by \(\varphi_n(P) = P(\Xi^n)\) for every \(P \in \mathbb{Z}[\Xi]\) (where \(P(\Xi^n)\) 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 \(C \iff D\).

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 \(J\)) in \([7, \text{Theorem 11}]\). Also, the proof of the whole Theorem 2.1 in the case when \(N = \mathbb{N}_+\) appears in \([6, \text{Exercise 2.82}]\); 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 \(C \iff D\) needs Assumptions 1 and 2 but not 3 (unsurprisingly), and the equivalence \(C \iff E \iff F \iff G \iff H\) needs only Assumption 3 (not 1 and 2; actually, \(A\) can be any additive group rather than a ring for this equivalence). The equivalence \(D \iff J\) 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

\[
w_N \left( (x_n)_{n \in N} \right) = \left( \sum_{d|n} dx_n^{n/d} \right)_{n \in N}
\]

for all \((x_n)_{n \in N} \in A^N\).

This \(N\)-ghost map is (generally) neither additive nor multiplicative.
The following theorem is easily derived from Theorem 2.1 (more precisely, the equivalence $C \iff D$) applied to the case $A = \mathbb{Z}[\Xi]$ and $\varphi_n (P) = P (\Xi^n)$:

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

- We have $W_N (A) = A^N$ as a set for every commutative ring $A$.
- The map $w_N : A^N \to A^N$ regarded as a map $W_N (A) \to A^N$ 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 $W_N (A)$ the $N$-Witt vector ring over $A$. Its zero is the family $(0)_{n \in N}$, and its unity is the family $(\delta_{u,v})_{n \in N}$ (where $\delta_{u,v}$ is defined to be $1$, if $u = v$; $0$, if $u \neq v$ for any two objects $u$ and $v$).

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

Theorem 2.4 appears in [16, 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 $\varphi_n$ satisfying Assumptions 1, 2 and 3 over any commutative ring $A$), but rather requires a detour via $\mathbb{Z}[\Xi]$.

The following theorem ([16, 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” [16, 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 $\sigma_n$ 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 $\sigma_1 = \text{id}$. Finally, assume that $\sigma_p (a) \equiv a^p \mod pA$ 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

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

Now let us describe some known functorial operations on $W_N (A)$. I will follow [16] 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 $f_m : W_N \to W_N$ of set-valued (not ring-valued) functors such that any commutative ring $A$ and any $x \in W_N (A)$ satisfy

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

where $f_m$ is short for $f_m (A)$.

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

(c) We have $f_1 = \text{id}$. Any two positive integers $n$ and $m$ such that $f_n$ and $f_m$ are well-defined satisfy $f_n \circ f_m = f_{nm}$.

(d) Let $p$ be a prime such that every $n \in N$ satisfies $pn \in N$. We have $f_p (x) \equiv x^p \mod p$ (in $W_N (A)$) for every commutative ring $A$ and every $x \in W_N (A)$.

In one or the other form, Theorem 2.7 appears in most sources on Witt vector; for example, it can be pieced together from parts of [16, Theorem 5.7, Proposition 5.9 and Proposition 5.12].

Here is the definition of Verschiebung ([16, 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 $V_m : W_N \to W_N$ of set-valued (not ring-valued) functors such that any commutative ring $A$ and any $x \in W_N (A)$ satisfy

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

where $V_m$ is short for $V_m (A)$.

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

(c) We have $V_1 = \text{id}$. Any two positive integers $n$ and $m$ satisfy $V_n \circ V_m = V_{nm}$.

(d) Actually, $V_m \left( (x_n)_{n \in N} \right) = \left( \begin{array}{ll} x_{n/m}, & \text{if } m \mid n; \\ 0, & \text{if } m \nmid n \end{array} \right)_{n \in N}$ 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 $V_m$ and $f_m$ 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 [16, 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 $AH : W_N \to W_N \circ W_N$ (of functors $\text{CRing} \to \text{CRing}$) such that every commutative ring $A$, every $n \in N$ and every $x \in W_N(A)$ satisfy

$$(n\text{-th coordinate of } w_N(AH(x))) = f_n(x)$$

(where $w_N$ this time stands for the natural transformation $w_N$ evaluated at the ring $W_N(A)$; thus, $w_N(AH(x))$ 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 $x \in W_N(A)$ to the $n$-th coordinate of $w_N(x)$. Then, $W_N(w_n) \circ AH = f_n$.

### 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 $d \in N$, every monic divisor of $d$ lies in $N$.

**Theorem 2.12.** 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 $\varphi_P$ is an endomorphism of the $\mathbb{F}_q[T]$-algebra $A$.

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

**Assumption 3:** We have $\varphi_1 = \text{id}$, 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 $C_1$, $D_1$, $D_2$, $E_1$, $F_1$, $G_1$, and $G_2$ are equivalent:

**Assertion $C_1$:** Every $P \in N$ and every $\pi \in PF P$ satisfies

$$\varphi_\pi(b_P/\pi) \equiv b_P \mod \pi^{\nu_\pi(P)}A.$$

---

\[2\] This is something Hazewinkel, in [16, §16.45], calls Artin-Hasse exponential. I am not sure if I completely understand its relation to the usual Artin-Hasse exponential...
Assertion $D_1$: There exists a family $(x_P)_{P \in N} \in A^N$ of elements of $A$ such that
\[ b_P = \sum_{D \mid P} D \left[ \frac{P}{D} \right] (x_D) \text{ for every } P \in N. \]

Assertion $D_2$: There exists a family $(\tilde{x}_P)_{P \in N} \in A^N$ of elements of $A$ such that
\[ b_P = \sum_{D \mid P} D^{\deg(P/D)} \tilde{x}_D \text{ for every } P \in N. \]

Assertion $E_1$: There exists a family $(y_P)_{P \in N} \in A^N$ of elements of $A$ such that
\[ b_P = \sum_{D \mid P} D \phi_{P/D} (y_D) \text{ for every } P \in N. \]

Assertion $F_1$: Every $P \in N$ satisfies
\[ \sum_{D \mid P} \mu(D) \phi_D (b_{P/D}) \in PA. \]

Assertion $G_1$: Every $P \in N$ satisfies
\[ \sum_{D \mid P} \phi_C(D) \phi_D (b_{P/D}) \in PA. \]

Assertion $G_2$: Every $P \in N$ satisfies
\[ \sum_{D \mid P} \phi(D) \phi_D (b_{P/D}) \in PA. \]

For this Theorem 2.12 to be a complete analogue of Theorem 2.1, two assertions are missing: $H$ and $J$. Finding an analogue of $J$ requires finding an analogue of $\Lambda$, which is the question that I have started this report with; approaches to it will be discussed in Section 4. Two other assertions ($D$ and $G$) have two analogues each due. However, Assertion $G_2$ is clearly equivalent to Assertion $F_1$ because of $\phi(M) \equiv \mu(M) \mod p$ for every $M \in \mathbb{F}_q[T]_+$. I have written out the former assertion merely to produce a clearer view of the analogy.

The proof of Theorem 2.12 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 $D_1 \iff C_1 \iff D_2$, $C_1 \iff F_1 \iff E_1 \implies C_1$, $F_1 \iff G_2$ and $E_1 \iff G_1$. Two different analogues of Hensel’s exponent lifting are used in proving $C_1 \iff D_1$ and $C_1 \iff D_2$.)
**Definition 2.13.** The families \((b_n)_{n \in \mathbb{N}} \in A^N\) which satisfy the equivalent assertions \(C_1, D_1, D_2, E_1, F_1, G_1,\) and \(G_2\) of Theorem 2.12 will be called Carlitz ghost-Witt vectors (over \(A\)).

What is more interesting is the following observation:

**Remark 2.14.** Assumption 1 in Theorem 2.12 can be replaced by the following weaker one:

Assumption 1': For every \(P \in \mathbb{N}\), the map \(\varphi_P\) is an endomorphism of the \(\mathbb{F}_q[T]\)-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

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

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 2.12 are both extremely simple and do not use multiplication in \(A\). It seems that \(A\) being a ring is a red herring in Theorem 2.12.

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?  

### 2.4. Carlitz-Witt vectors

Parroting Definition 2.3, we define:

**Definition 2.15.** 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

---

3Non-rhetorical question. Please let me know! (darijgrinberg[at]gmail.com)
over $N$). The Carlitz $N$-ghost map $w_N : A^N \to A^N$ is the map defined by

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

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

From the equivalence $C_1 \iff D_1$ in Theorem 2.14 we can obtain

**Theorem 2.16.** Let $N$ be a $q$-nest. There exists a unique functor $W_N : \text{CRing}_{\mathbb{F}_q[T]} \to \text{CRing}_{\mathbb{F}_q[T]}$ 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 $\text{CRing}_{\mathbb{F}_q[T]} \to \text{CRing}_{\mathbb{F}_q[T]}$, $A \mapsto A^N$. 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 2.14. This can no longer be proven using Theorem 2.16, 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 2.17.** 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 $(0)_{n \in N}$.

---

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 $\Xi$ is a family of indeterminates, and define morphisms $\varphi_p$ by $\varphi_p(Q) = Q((P)(\Xi))$, where $(P)(\Xi)$ means the family obtained by applying $(P)$ to each variable in the family $\Xi$. Alternatively, one could define morphisms $\varphi_p$ by $\varphi_p(Q) = Q(\Xi^{\deg(P)})$; these are different morphisms but they also work here.
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 $C_1 \iff D_1$ so far. What about $C_1 \iff D_2$?

**Definition 2.18.** Let $N$ be a $q$-nest. Let $A$ be a commutative $\mathbb{F}_q[T]$-algebra. The Carlitz tilde $N$-ghost map $\tilde{w}_N : A^N \to A^N$ is the map defined by

$$
\tilde{w}_N ((x_P)_{P \in N}) = \left( \sum_{D \mid P} D x_{\deg(P/D)}^q \right)_{P \in N}
$$

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.

From the equivalence $C_1 \iff D_2$ in Theorem 2.12, we get:

**Theorem 2.19.** Let $N$ be a $q$-nest. There exists a unique functor $\tilde{W}_N : \text{CRing}_{\mathbb{F}_q[T]} \to \text{CRing}_{\mathbb{F}_q[T]}$ with the following two properties:

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

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

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

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

**Theorem 2.20.** Let $N$ be a $q$-nest. The functors $W_N$ and $\tilde{W}_N$ are isomorphic by an isomorphism which forms a commutative triangle with $w_N$ and $\tilde{w}_N$.

This is again proven using Theorem 2.12 and universal polynomials.

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

**Theorem 2.21.** 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 $\tilde{w}_N : \tilde{W}_N (A) \to A^N$ are $\mathbb{F}_q[T]$-algebra isomorphisms.
We have an “almost-universal property” again, following from exponent lifting and the implication \( C_1 \implies D_1 \) in Theorem 2.12.

**Theorem 2.22.** 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 \( \sigma_P \) 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 \( \sigma_1 = \text{id} \). Finally, assume that \( \sigma_\pi(a) \equiv [\pi](a) \mod \pi A \) (or, equivalently, \( \sigma_\pi(a) \equiv a^{q^{\deg \pi}} \mod \pi A \)) for every monic irreducible \( \pi \in N \) and every \( a \in A \). Then, there exists a unique \( \mathbb{F}_q \{ T \} \)-algebra homomorphism \( \varphi : A \to \mathbb{W}_N(A) \) satisfying

\[
(w_N \circ \varphi)(a) = (\sigma_P(a))_{P \in N}
\]

for every \( a \in A \). (3)

A similar result holds for \( \mathbb{W}_N \) and \( \mathbb{w}_N \).

What about Frobenius operations?

**Theorem 2.23.** 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 \( f_M : \mathbb{W}_N \to \mathbb{W}_N \) of *set-valued* (not \( \mathbb{F}_q \{ T \} \)-algebra-valued) functors such that any commutative \( \mathbb{F}_q \{ T \} \)-algebra \( A \) and any \( x \in \mathbb{W}_N(A) \) satisfy

\[
(w_N(f_M(x))) = (MP\text{-th coordinate of } w_N(x))_{P \in N},
\]

where \( f_M \) is short for \( f_M(A) \).

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

(c) We have \( f_1 = \text{id} \). Any \( P \in \mathbb{F}_q \{ T \} \) and \( Q \in \mathbb{F}_q \{ T \} \) such that \( f_P \) and \( f_Q \) are well-defined satisfy \( f_P \circ f_Q = f_{PQ} \).

(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 \( f_{\pi}(x) \equiv [\pi](x) \mod \pi \mathbb{W}_N(A) \) (in \( \mathbb{W}_N(A) \)) for every commutative \( \mathbb{F}_q \{ T \} \)-algebra \( A \) and every \( x \in \mathbb{W}_N(A) \).

**Corollary 2.24.** Consider the setting of Theorem 2.22. Then (from Theorem 2.22) we know that there exists a unique \( \mathbb{F}_q \{ T \} \)-algebra homomorphism \( \varphi : A \to \mathbb{W}_N(A) \) satisfying (3). Consider this \( \varphi \). Let \( M \in N \) be such that every \( P \in N \) satisfies \( MP \in N \). Then,

\[
\varphi \circ \sigma_M = f_M \circ \varphi
\]

for every \( M \in N \).
Corollary 2.25. Consider the setting of Theorem 2.22. 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 $\text{proj}_B : W_N(B) \to B$ be the map sending every $u \in W_N(B)$ to the 1-st coordinate of $w_N(u) \in B^N$. This $\text{proj}_B$ 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

$$G \circ \sigma_M = f_M \circ g$$

for every $M \in N$.

This $G$ can be constructed as follows: Theorem 2.22 shows that there exists a unique $\mathbb{F}_q[T]$-algebra homomorphism $\varphi : A \to W_N(A)$ satisfying (3). Consider this $\varphi$. 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 $W_N(f) : W_N(A) \to W_N(B)$. Now, the $G$ is constructed as the composition $W_N(f) \circ \varphi$.

A Verschiebung exists too:

Theorem 2.26. Let $N$ be a $q$-nest.

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

$$w_N(V_M(x)) = \left\{ \begin{array}{ll} M \cdot \left( \frac{P}{M} \right) -\text{th coordinate of } w_N(x), & \text{if } M \mid P; \\ 0, & \text{if } M \nmid P \end{array} \right\}_{P \in N},$$

where $V_M$ is short for $V_M(A)$.

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

(c) We have $V_1 = \text{id}$. Any two $P \in \mathbb{F}_q[T]^+$ and $Q \in \mathbb{F}_q[T]^+$ satisfy $V_P \circ V_Q = V_{PQ}$.

(d) Actually, $V_M((x_P)_{P \in N}) = \left\{ \begin{array}{ll} x_P / M, & \text{if } M \mid P; \\ 0, & \text{if } M \nmid P \end{array} \right\}_{P \in N}$ 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 2.27.** 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 $AH : W_N \to W_N \circ W_N$ (of functors $\text{CRing}_{\mathbb{F}_q[T]} \to \text{CRing}_{\mathbb{F}_q[T]}$) such that every commutative $\mathbb{F}_q[T]$-algebra $A$, every $P \in N$ and every $x \in W_N(A)$ satisfy

$$(P\text{-th coordinate of } w_N(AH(x))) = f_P(x)$$

(where $w_N$ this time stands for the natural transformation $w_N$ evaluated at the $\mathbb{F}_q[T]$-algebra $W_N(A)$; thus, $w_N(AH(x))$ 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 $x \in W_N(A)$ to the $P$-th coordinate of $w_N(x)$. Then, $W_N(w_p) \circ AH = f_P$.

### 2.5. $\mathcal{F}$-modules

The classical $N$-Witt vector functor for $N \subseteq \mathbb{N}_+$ being a nest is a functor $\text{CRing} \to \text{CRing}$, and I don’t see how to extend it to any broader category than $\text{CRing}$. 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 2.14. 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 $\mathbb{F}_q[F,T \mid FT = T^qF]$. This $\mathcal{F}$ can be considered as a skew polynomial ring $\mathbb{F}_q[T] [F; \text{Frob}]$ over the polynomial ring $\mathbb{F}_q[T]$, where $\text{Frob} : \mathbb{F}_q[T] \to \mathbb{F}_q[T]$ 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 $\mathbb{F}_q[T] \rightarrow \mathcal{F}$ and $\mathbb{F}_q[F] \rightarrow \mathcal{F}$, 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 $(F^i)_{i \geq 0}$ and thus torsionfree (this will be useful).
- As right $\mathbb{F}_q[T]$-module, $\mathcal{F}$ is free with basis $(T^iF^j)_{i \geq 0, 0 \leq j < q^i}$.
- As right $\mathbb{F}_q[F]$-module, $\mathcal{F}$ is free with basis $(T^i)_{j \geq 0}$.
- As left $\mathbb{F}_q[F]$-module, $\mathcal{F}$ is free with basis $(T^iF^j)_{i = 0 \text{ or } qj}$.

As a consequence, it is torsionfree (but this also follows from the isomorphism $\mathcal{F} \to \mathbb{F}_q[T] [X]_{q\text{-lin}}$ introduced below).
As \( \mathbb{F}_q[F]-\mathbb{F}_q[T] \)-bimodule, \( \mathcal{F} \) is free with basis \((T^i F^j)\) for \( i = 0 \) or \( q \) and \( 0 \leq j < q^i \) (that is, \( \mathcal{F} = \bigoplus_{(i,j) \in \mathbb{N}^2; \ (i=0 \text{ or } qj) \text{ and } 0 \leq j < q^i} \mathbb{F}_q[F] \cdot (T^i F^j) \cdot \mathbb{F}_q[T] \), and each \( \mathbb{F}_q[F] \cdot (T^i F^j) \cdot \mathbb{F}_q[T] \) 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 \( T^i F^j \) with \((i,j) \in \mathbb{N}^2 \). Actually, this monoid is \( J \)-trivial. Finite \( J \)-trivial monoids have a very nice representation theory \([1]\); does ours? \footnote{\( J \)-trivial means that \( \mathcal{F} \) acts as left multiplication with \( T \) and \( F \) act as taking the \( \deg \) of the \( X \)-degree \( \deg \) of \( F \).}

Every commutative \( \mathbb{F}_q[T] \)-algebra is canonically an \( \mathcal{F} \)-module, by letting \( T \) act as \( \deg \) of \( X \)-degree \( \deg \) of \( F \) and letting \( F \) act as taking the \( q \)-th power in the algebra.

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 \( \text{Carl} : \mathbb{F}_q[T] \to \mathcal{F} \) which sends \( T \) to \( F + T \). This Carl is a very important homomorphism.

There is another interesting, and important, map around here. Let \( \mathbb{F}_q[T][X]_{q-\text{lin}} \) 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 \( X^0, X^q, X^{q^2}, \ldots \) appear (we consider \( T \) as a constant here). Then, \( \mathbb{F}_q[T][X]_{q-\text{lin}} \) 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

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

yields a well-defined \( \mathbb{F}_q \)-algebra isomorphism \( \mathcal{F} \to \mathbb{F}_q[T][X]_{q-\text{lin}} \). 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 \( \pi \in \mathbb{F}_q[T] \),

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

\footnote{\( u(\pi) \) means that \( u \) depends on \( \pi \); it is not meant to imply that \( u(\pi) \) is a polynomial in \( \pi \).}

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

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

Now, the situation described in Remark 2.14 is simply understood as having a left $\mathcal{F}$-module $A$, and for every $P \in \mathbb{N}$, an $\mathcal{F}$-module endomorphism $\varphi_P$ of $A$.

The category of left $\mathcal{F}$-modules has its free objects, which simply are free left $\mathcal{F}$-modules. If $\Xi$ is a set (to be viewed as a set of “indeterminates”), then a family of $\mathcal{F}$-module endomorphisms $\varphi_P$ of the free $\mathcal{F}$-module $\mathcal{F}_\Xi$ satisfying Assumptions 1', 2 and 3 can be easily constructed (namely, $\varphi_P$ 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 $\tilde{W}_N$ will then be functors from $\mathcal{F}\text{-Mod}$ to $\mathcal{F}\text{-Mod}$. 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 [14] and [15] (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 \( K \) be a commutative ring. Let \( r \) be a positive integer. Let \( M \) be the \( K \)-algebra \( K \langle F, T \mid FT = T F \rangle \). There are well-defined \( K \)-algebra homomorphisms \( K [ T ] \to M \) (sending \( T \) to \( T \)) and \( K [ F ] \to M \) (sending \( F \) to \( F \)). These homomorphisms make \( M \) into a left \( K [ T ] \)-module, a right \( K [ F ] \)-module, a left \( K [ F ] \)-module, and a right \( K [ F ] \)-module. Any of these two left module structures can be combined with any of these two right module structures to form a \( \otimes \)-bimodule structure on \( M \) (for example, the left \( K [ T ] \)-module structure and the right \( K [ F ] \)-module structure on \( M \) can be combined to form an \( \otimes \)-bimodule structure on \( M \)). (However, in general, \( M \) is neither a \( K [ T ] \)-algebra nor a \( K [ F ] \)-algebra.)

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

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

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

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

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

(f) As left \( K [ F ] \)-module, \( M \) is free with basis \( (T^i F^j)_{i=0 \text{ or } r|j}, 0 \leq j < ri} \).

(g) As \( K [ F ] \)-\( K [ T ] \)-bimodule, \( M \) is free with basis \( (T^i F^j)_{(i,j) \in \mathbb{N}^2, (i=0 \text{ or } r|j) \text{ and } 0 \leq j < ri} \).

(That is, we have \( M = \bigoplus_{(i,j) \in \mathbb{N}^2, (i=0 \text{ or } r|j) \text{ and } 0 \leq j < ri} \).)

We notice that the \( K \)-algebra \( M \) in Proposition 3.1 is actually the monoid algebra (over \( K \)) of the monoid with generators \( F, T \) and relation \( FT = T F \). From this viewpoint, all of Proposition 3.1 is easily revealed to be a monoid-theoretical statement (with \( K \) being merely a distraction). However, we shall work with \( K \)-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

\[
\ell (\phi (s)) > \ell (s) \quad \text{for every } s \in S. \tag{5}
\]

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

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

Then, \( \rho \) 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 $\phi$.)

**Proof of Lemma 3.2** Let us first prove that the map $\rho$ 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 $\rho$ yields $\rho(s, k) = \phi^k(s)$. Thus, $\phi^k(s) = \rho(s, k) = \rho(s', k') = \phi^{k'}(s')$ (by the definition of $\rho$).

The map $\phi^{k'}$ is injective (since $\phi$ 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, $\phi^k(s) = \phi^{k'+(k-k')}(s) = \phi^{k'}(\phi^{k-k'}(s))$. But the map $\phi^{k'}$ is injective. Therefore, from $\phi^{k'}(\phi^{k-k'}(s)) = \phi^k(s) = \phi^{k'}(s')$, 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 $\phi^{k-k'}(s) = \phi^{k-k'}(s')$. This yields $s = s'$ (since the map $\phi^{k-k'}$ 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 $\rho$ is injective.

Let us now show that the map $\rho$ is surjective. Indeed, we shall prove that

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

**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. 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

---

\footnote{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.}
Function-field analogue for symmetric functions? February 14, 2016

\[ s = \rho(t, k) = \phi^k(t) \text{ (by the definition of } \rho) \text{, and } x = \phi\left( \frac{s}{\phi^k(t)} \right) = \phi\left( \phi^k(t) \right) = \phi^{k+1}(t). \]

Comparing this with \( \rho(t, k + 1) = \phi^{k+1}(t) \) (by the definition of \( \rho \)), 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, \( \ell \) is a map \( S \rightarrow \mathbb{N} \). Hence, \( S = \bigcup_{n \in \mathbb{N}} \ell^{-1}(n) \subseteq \bigcup_{n \in \mathbb{N}} \rho(B \times \mathbb{N}) \subseteq \rho(B \times \mathbb{N}) \).

In other words, the map \( \rho \) is surjective. Hence, the map \( \rho \) is bijective (since we already know that \( \rho \) is injective). This proves Lemma 3.2. \( \Box \)

We record two corollaries of Lemma 3.2.

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

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

Define a map \( \rho : B \times \mathbb{N} \rightarrow \mathbb{N}^2 \) by

\[ \rho((i, j), k) = (i + k, r^k j) \quad \text{for every } ((i, j), k) \in B \times \mathbb{N}. \tag{8} \]

Then, the map \( \rho \) is a bijection.

**Proof of Corollary 3.3** Let \( \phi : \mathbb{N}^2 \rightarrow \mathbb{N}^2 \) be the map defined by

\[ \phi(i, j) = (i + 1, rj) \quad \text{for every } (i, j) \in \mathbb{N}^2. \]
It is clear that this map $\phi$ is injective (since $r > 0$). Moreover, $B = \mathbb{N}^2 \setminus \phi \left( \mathbb{N}^2 \right)$.

Given an $s \in S$, it is easy to algorithmically check whether $s \not\in \phi \left( \mathbb{N}^2 \right)$ (because of the equivalence $s \not\in \phi \left( \mathbb{N}^2 \right) \iff s \in \mathbb{N}^2 \setminus \phi \left( \mathbb{N}^2 \right) \iff s \in B$), and if $s \in \phi \left( \mathbb{N}^2 \right)$, then it is easy to compute a preimage of $s$ under $\phi$ (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

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

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

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

\[ ^9 \text{Proof.}\] We have

$$\mathbb{N}^2 \setminus \phi \left( \mathbb{N}^2 \right) = \left\{ (i, j) \in \mathbb{N}^2 \mid \text{there exists no } (u, v) \in \mathbb{N}^2 \text{ such that } (i, j) = \phi(u, v) \right\} = (u + 1, rv) \quad \text{(by the definition of } \phi)$$

$$\mathbb{N}^2 \setminus \phi \left( \mathbb{N}^2 \right) = \left\{ (i, j) \in \mathbb{N}^2 \mid \text{there exists no } (u, v) \in \mathbb{N}^2 \text{ such that } (i, j) = (u + 1, rv) \right\}$$

$$\mathbb{N}^2 \setminus \phi \left( \mathbb{N}^2 \right) = \left\{ (i, j) \in \mathbb{N}^2 \mid i - 1 \notin \mathbb{N} \text{ or } j/r \notin \mathbb{N} \right\}$$

$$\mathbb{N}^2 \setminus \phi \left( \mathbb{N}^2 \right) = \left\{ (i, j) \in \mathbb{N}^2 \mid i = 0 \text{ or } r \mid j \right\} = B,$$

$qed.$

\[ ^9 \text{Proof of } (10):\] 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

$$\phi^k(s_{(i, j)}) = \phi^k(i, j) = \left( i + k, r^k j \right) \quad \text{(by } 9)$$

$$\rho(i, j), k = \rho(s, k) \quad \text{(by } 8)$$

This proves $(10).$
Furthermore, define a map \( \ell : \mathbb{N}^2 \to \mathbb{N} \) by
\[
\ell (i, j) = i \quad \text{for every } (i, j) \in \mathbb{N}^2.
\]
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 \( \rho \) is a bijection. This proves Corollary 3.3. \( \square \)

**Corollary 3.4.** Define a subset \( C \) of \( \mathbb{N}^2 \) by
\[
C = \{(i, j) \in \mathbb{N}^2 \mid (i = 0 \text{ or } r \parallel j) \text{ and } 0 \leq j < r^j \}.
\]
Define a map \( \zeta : C \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}^2 \) by
\[
\zeta ((i, j), \ell, k) = \left(i + k, r^k \left(j + r^j \ell \right)\right) \quad \text{for every } ((i, j), k) \in C \times \mathbb{N} \times \mathbb{N}.
\]
Then, the map \( \zeta \) 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
\[
\tau ((i, j), \ell) = \left(i, j + r^j \ell \right) \quad \text{for every } ((i, j), \ell) \in C \times \mathbb{N}.
\]
It is easy to see that this map \( \tau \) is well-defined (i.e., that \((i, j + r^j \ell) \in B \) 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 \( u \div v \) denote the quotient of \( u \) when divided by \( v \) with remainder. Thus, \( u \div v \in \mathbb{Z}, u \% v \in \{0, 1, \ldots, v - 1\} \) and \( u = (u \div v) \times v + u \% v \).

Define a map \( \gamma : B \to C \times \mathbb{N} \) by
\[
\gamma (i, j) = \left(\left((i, j) \% r^j\right), j / r^j \right) \quad \text{for every } (i, j) \in B.
\]
Again, it is easy to see that this map \( \gamma \) is well-defined (i.e., that \(( (i, j) \% r^j), j / r^j ) \in C \times \mathbb{N} \) for every \((i, j) \in B\).

Furthermore, it is easy to see that the maps \( \tau \) and \( \gamma \) are mutually inverse. \( \square \) Hence, the map \( \tau \) 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 \( \tau \times \text{id} : (C \times \mathbb{N}) \times \mathbb{N} \to B \times \mathbb{N} \) can be viewed as a map \( C \times \mathbb{N} \times \mathbb{N} \to B \times \mathbb{N} \). This map \( \tau \times \text{id} \) sends every \(( (i, j), \ell, k) \in C \times \mathbb{N} \times \mathbb{N} \) to \( (\tau ((i, j), \ell), k) \). Clearly, the map \( \tau \times \text{id} \) is a bijection (since \( \tau \) is a bijection).

\( ^{10} \text{Proof. Let us first show that } \tau \circ \gamma = \text{id}. \)
On the other hand, define a map $\rho$ as in Corollary 3.3. Then, Corollary 3.3 shows that the map $\rho$ is a bijection. But every $((i, j), \ell, k) \in C \times N \times N$ satisfies

$$(\rho \circ (\tau \times \text{id}_N)) ((i, j), \ell, k)$$

$$= \rho \left( (\tau \times \text{id}_N) ((i, j), \ell, k) \right) = \rho \left( (\tau ((i, j), \ell), k) \right)$$

$$= \rho \left( (i, j + r^{\ell}) , k \right) = (i + k, r^{j + r^{\ell}})$$

(by the definition of $\rho$)

$$= \zeta ((i, j), \ell, k)$$

(by (12)).

Hence, $\rho \circ (\tau \times \text{id}_N) = \zeta$. Since the map $\rho \circ (\tau \times \text{id}_N)$ is a bijection (because both $\rho$ and $\tau \times \text{id}_N$ are bijections), this shows that the map $\zeta$ is a bijection. This proves Corollary 3.4.

**Proof of Proposition 3.1**

(a) First, we have the equality

$$FT^b = T^{rb}F$$

(13)

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

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

$$(\tau \circ \gamma) (i, j) = \tau \left( \frac{\gamma (i, j)}{(i, j + r^{\ell})} \right) = \tau \left( \left( i, \frac{j}{r^{\ell}} \right), j / r^{\ell} \right) = \left( i, j / r^{\ell} \right) = (i, j) \, .$$

(by the definition of $\tau$

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

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

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

$$= \left( i, \left( \frac{j}{r^{\ell}} \right) % r^\ell \right) \left( \frac{j}{r^{\ell}} / r^\ell \right) = ((i, j), \ell) \, .$$

This proves that $\gamma \circ \tau = \text{id}$. Combining this with $\tau \circ \gamma = \text{id}$, we obtain that the maps $\tau$ and $\gamma$ are mutually inverse, qed.
(b) Let \( \mathcal{N} \) be the free \( \mathbb{K} \)-module with basis \( (a_{i,j})_{i \geq 0, j \geq 0} \). We let \( f \) be the \( \mathbb{K} \)-linear map \( \mathcal{N} \to \mathcal{N} \) which sends every \( a_{i,j} \) to \( a_{i+1,j} \). We let \( t \) 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
\[
f^k(a_{i,j}) = a_{i+k,j} \tag{14}
\]
and
\[
t^k(a_{i,j}) = a_{i,j+k} \tag{15}
\]
(Both of these equalities are easily proven by induction over \( k \).) Using (15), it is easy to see that \( f \circ t = t' \circ f \). Thus, we can define a \( \mathbb{K} \)-algebra homomorphism \( \Phi : \mathcal{M} \to \text{End} \mathcal{N} \) by setting
\[
\Phi(F) = f \quad \text{and} \quad \Phi(T) = t \tag{16}
\]
(where \( \text{End} \mathcal{N} \) denotes the \( \mathbb{K} \)-algebra of all \( \mathbb{K} \)-module endomorphisms of \( \mathcal{N} \)). Consider this \( \Phi \). For every \( i, j \in \mathbb{N} \), we have
\[
\Phi\left( T^i F^j \right) = \Phi(T)^i \circ \Phi(F)^j = t^i \circ f^j \quad \text{(by (16))}
\]
and thus
\[
\left( \Phi\left( T^i F^j \right) \right)(a_{0,0}) = \left( t^i \circ f^j \right)(a_{0,0}) = t^j \left( f^i(a_{0,0}) \right) = t^j \left( a_{i,0} \right) \tag{17}
\]
(by (15)). Hence, the family \( (T^i F^j)_{i \geq 0, j \geq 0} \) of elements of \( \mathcal{M} \) is \( \mathbb{K} \)-linearly independent\(^{11}\).

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 \( (T^i F^j)_{i \geq 0, j \geq 0} \). Then, \( 1 = T^0 F^0 \in \mathcal{M}' \). Moreover,

\(^{11}\)because any linear dependence relation \( \sum_{i \geq 0, j \geq 0} \lambda_{i,j} T^i F^j = 0 \) would yield
\[
\sum_{i \geq 0, j \geq 0} \lambda_{i,j} \underbrace{a_{i,j}}_{= (\Phi(T^i F^j))(a_{0,0}) \tag{by (17)}} = \sum_{i \geq 0, j \geq 0} \lambda_{i,j} \left( \Phi\left( T^i F^j \right) \right)(a_{0,0})
\]
\[
= \Phi\left( \sum_{i \geq 0, j \geq 0} \lambda_{i,j} T^i F^j \right)(a_{0,0}) = 0,
\]
which would lead to \( (\lambda_{i,j})_{i \geq 0, j \geq 0} = (0)_{i \geq 0, j \geq 0} \) since the family \( (a_{i,j})_{i \geq 0, j \geq 0} \) is linearly independent.
the \( K \)-submodule \( M' \) satisfies \( TM' \subseteq M' \) (since \( T \cdot TiFi = Ti+1Fi \) for every \( i,j \in \mathbb{N} \)) and \( FM' \subseteq M' \) (since \( F \cdot TiFi = \frac{FTj}{F} \) \( F = TjFFi = TjFi+1 \) for every \( i,j \in \mathbb{N} \)). Hence, \( M' \) is a left \( M \)-submodule of \( M \). Therefore, \( M \cdot M' \subseteq M' \).

But \( M = M \cdot \frac{1}{\beta} \subseteq M \cdot M' \subseteq M' \). This shows that the family \( (TiFi)_{i\geq0, j\geq0} \)
spans the \( K \)-module \( M \) (since the \( K \)-linear span of this family is \( M' \)). Since we already know that this family is \( K \)-linearly independent, we can thus conclude that this family is a basis of the \( K \)-module \( M \). This proves Proposition 3.1(b).

\( \text{(c)} \) Let \((e_0, e_1, e_2, \ldots)\) be the standard basis of the left \( K [T] \)-module \( K [T]^{|\mathbb{N}|} \). Define a \( K [T] \)-module homomorphism \( \alpha : K [T]^{|\mathbb{N}|} \rightarrow M \) by sending each \( e_i \) to \( F_i \). Define a \( K \)-module homomorphism \( \beta : M \rightarrow K [T]^{|\mathbb{N}|} \) by sending each \( TiFi \) to \( Ti'e_i \). (This \( \beta \) is well-defined, since Proposition 3.1(b) shows that \( (TiFi)_{i\geq0, j\geq0} \) is a basis of the \( K \)-module \( M \).) It is easy to see that \( \beta \) is a \( K [T] \)-module homomorphism. It is straightforward to see that the homomorphisms \( \alpha \) and \( \beta \) are mutually inverse. Thus, \( \alpha \) is a left \( K [T] \)-module isomorphism. As a consequence, the left \( K [T] \)-module \( M \) has a basis
\[
\left\{ \frac{\alpha(e_i)}{F^i} \right\}_{i \geq 0} = \left( \frac{F}{F} \right)_{i \geq 0}.
\]
This proves Proposition 3.1(c).

\( \text{(d)} \) 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 \( u = (u / v) \cdot v + u \% v \).

Let \( G \) be the free right \( K [T] \)-module with basis \((g_{ij})_{i\geq0, 0 \leq j < r'_i} \). Define a right \( K [T] \)-module homomorphism \( \alpha : G \rightarrow M \) by sending each \( g_{ij} \) to \( TiFi \). Define a \( K \)-module homomorphism \( \beta : M \rightarrow G \) by sending each \( TiFi \) to \( g_{i',i \% r'_i}Ti'/r'_i \). (This \( \beta \) is well-defined, since Proposition 3.1(b) shows that \( (TiFi)_{i\geq0, j\geq0} \) is a basis of the \( K \)-module \( M \).) It is easy to see that the homomorphisms \( \alpha \) and \( \beta \) are mutually inverse\( ^{12} \). Thus, \( \alpha \) is a right \( K [T] \)-module isomorphism. Since the right \( K [T] \)-module \( G \) has a basis \((g_{ij})_{i\geq0, 0 \leq j < r'_i} \), this shows that the right \( K [T] \)-module \( M \) has a basis
\[
\left\{ \frac{\alpha(g_{ij})}{TiFi} \right\}_{i \geq 0, 0 \leq j < r'_i} = \left( \frac{TiFi}{F} \right)_{i \geq 0, 0 \leq j < r'_i}.
\]
This proves Proposition 3.1(d).

\( \text{(e)} \) Let \((e_0,e_1,e_2,\ldots)\) be the standard basis of the right \( K [F] \)-module \( K [F]^{|\mathbb{N}|} \). Define a right \( K [F] \)-module homomorphism \( \alpha : K [F]^{|\mathbb{N}|} \rightarrow M \) by sending

\( ^{12} \text{Proof. We need to show that } \alpha \circ \beta = \text{id and } \beta \circ \alpha = \text{id.} \)

To prove that \( \alpha \circ \beta = \text{id} \), we need to show that \( (\alpha \circ \beta) (TiFi) = TiFi \) for every \( i,j \in \mathbb{N} \). So
each $e_j$ to $T^i$. Define a $K$-module homomorphism $\beta : M \to K[T]^{(N)}$ by sending each $T^iF^j$ to $e_jF^i$. (This $\beta$ is well-defined, since Proposition 3.1(b) shows that $(T^iF^j)_{i \geq 0, j \geq 0}$ is a basis of the $K$-module $M$.) It is easy to see that $\beta$ is a right $K[F]$-module homomorphism. It is straightforward to see that the homomorphisms $\alpha$ and $\beta$ are mutually inverse. Thus, $\alpha$ is a right $K[F]$-module isomorphism. As a consequence, the right $K[F]$-module $M$ has a basis

$$
\left( \alpha \left( e_j \right) \right)_{T^i} = \left( T^i \right)_{j \geq 0}.
$$

This proves Proposition 3.1(e).

---

Let us fix $i, j \in \mathbb{N}$. Then,

$$(\alpha \circ \beta) \left( T^iF^j \right) = \alpha \left( \beta \left( T^iF^j \right) \right) = \alpha \left( g_{ij}T^j \right) = \alpha \left( T_i^j \right) = T^iF^j,$$

which is what we wanted to prove.

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

We know that $G$ is spanned by $\left( g_{ij} \right)_{i \geq 0, 0 \leq j < r^i}$ as a right $K[T]$-module (by the definition of $G$). Hence, $G$ is spanned by $\left( g_{ij}T^k \right)_{i \geq 0, 0 \leq j < r^i, k \geq 0}$ as a $K$-module. Hence, in order to prove that $\beta \circ \alpha = \text{id}$, it suffices to show that $\left( (\beta \circ \alpha) \left( g_{ij}T^k \right) = g_{ij}T^k \right)$ 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 $\alpha$ yields $\alpha \left( g_{ij} \right) = T_i^j F^j$. But since $\alpha$ is a right $K[T]$-module homomorphism, we have

$$
\alpha \left( g_{ij}T^k \right) = \alpha \left( g_{ij} \right) T^k = T_i^j F^j = T_i^j T^k F^j = T_i^j T^k F^j.
$$

(by Proposition 3.1(a), applied to $a=i$ and $b=k$)

Now,

$$
(\beta \circ \alpha) \left( g_{ij}T^k \right) = \beta \left( T_i^j T^k F^j \right) = \beta \left( T_i^j+r^k F^j \right) = g_{ij} \left( T_{i+j+r^k} \right) F^j.
$$

But $0 \leq j < r^i$. Hence, $(j+r^k) F^j = j$ and $(j+r^k) / r = k$. In view of these two equalities, (18) rewrites as $\left( (\beta \circ \alpha) \left( g_{ij}T^k \right) = g_{ij}T^k \right)$. This completes our proof of $\beta \circ \alpha = \text{id}$. Thus, we have shown that $\alpha$ and $\beta$ are mutually inverse.
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 $\rho$ is a bijection. Hence, its inverse $\rho^{-1} : \mathbb{N}^2 \to B \times \mathbb{N}$ is well-defined.

Now, let $H$ be the free left $K[F]$-module with basis $(h(i,j))_{(i,j) \in B}$. Define a left $K[F]$-module homomorphism $\alpha : H \to M$ by sending each $h(i,j)$ to $T^i F^j$. Define a $K$-module homomorphism $\beta : M \to H$ by sending each $T^i F^j$ to $F^k h(u,v)$, where $((u,v),k) = \rho^{-1}(i,j)$. (This $\beta$ is well-defined, since Proposition 3.1(b) shows that $(T^i F^j)_{i \geq 0, j \geq 0}$ is a basis of the $K$-module $M$.) It is straightforward to see
that the homomorphisms $\alpha$ and $\beta$ are mutually inverse\footnote{Proof.}. Thus, $\alpha$ is a left $K[F]$-module homomorphism. Hence, the definition of $\beta$ shows that $\beta(T^iF^j) = F^k h_{(i,j)}$. Now,

\[
(\alpha \circ \beta) (T^iF^j) = \alpha \left( \beta(T^iF^j) \right) = \alpha \left( F^k h_{(i,j)} \right) = F^k \alpha(h_{(i,j)}) = T^iF^j,
\]

which is what we wanted to prove.

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

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

\[
\alpha(F^k h_{(i,j)}) = F^k \alpha(h_{(i,j)}) = F^k \left( T^iF^j \right) = T^i F^j F^k = T^i F^{k+i}.
\]

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

\[
(\beta \circ \alpha)(F^k h_{(i,j)}) = \beta \left( \alpha(F^k h_{(i,j)}) \right) = \beta \left( T^i F^{k+i} \right) = F^k h_{(i,j)}.\]

This completes our proof of $\beta \circ \alpha = id$. Thus, we have shown that $\alpha$ and $\beta$ are mutually inverse.
module isomorphism. As a consequence, the left $\mathbb{K} [F]$-module $\mathcal{M}$ has a basis
\[
\left( a \left( h_{(i,j)} \right) \right)_{(i,j) \in B} = \left( T^i F^j \right) \quad \text{for } i \geq 0 \text{ or } r \mid j
\]
(since $B = \{(i, j) \in \mathbb{N}^2 \mid i = 0 \text{ or } r \not| j\}$). This proves Proposition 3.1 (f).

(g) Define $\zeta$ and $\zeta'$ 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 $\zeta$ is a bijection. In other words, the map
\[
C \times \mathbb{N} \times \mathbb{N} \to \mathbb{N}^2, \quad ((i, j), \ell, k) \mapsto (i + k, r^k \left(j + r^\ell \ell\right)) \quad (19)
\]
is a bijection (since this is the map $\zeta$).

Proposition 3.1 (b) shows that $\left( T^i F^j \right)_{i \geq 0, j \geq 0}$ is a basis of the $\mathbb{K}$-module $\mathcal{M}$. We can reindex this basis using the bijection (19); thus, we conclude that $\left( T^{r^k (i + r^\ell \ell)} F^{i \ell + k} \right)_{(i, j), \ell, k \in \mathbb{C} \times \mathbb{N} \times \mathbb{N}}$ 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,
\[
\left( r_{(i,j)} \otimes F^k \otimes T^\ell \right)_{(i, j), \ell, k \in \mathbb{C} \times \mathbb{N} \times \mathbb{N}}
\]
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
\[
\eta \left( r_{(i,j)} \otimes F^k \otimes T^\ell \right) = T^{r^k (i + r^\ell \ell)} F^{i \ell + k}.
\]
Consider this map $\eta$. It sends the basis $\left( r_{(i,j)} \otimes F^k \otimes T^\ell \right)_{(i,j), \ell, k \in \mathbb{C} \times \mathbb{N} \times \mathbb{N}}$ of $\mathcal{R} \otimes \mathbb{K} [F] \otimes \mathbb{K} [T]$ to the basis $\left( T^{r^k (i + r^\ell \ell)} F^{i \ell + k} \right)_{(i,j), \ell, k \in \mathbb{C} \times \mathbb{N} \times \mathbb{N}}$ of $\mathcal{M}$. Thus, $\eta$ 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 $\eta$ is a left $\mathbb{K} [F]$-module homomorphism and a right

\[\text{Proof.} \quad \text{It suffices to show that } \eta (fz) = f \eta (z) \text{ for every } f \in \mathbb{K} [F] \text{ and } z \in \mathcal{R} \otimes \mathbb{K} [F] \otimes \mathbb{K} [T]. \]

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 $\left( r_{(i,j)} \otimes F^k \otimes T^\ell \right)_{((i,j), \ell, k) \in \mathbb{C} \times \mathbb{N} \times \mathbb{N}}$ 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 $((i,j), \ell, k) \in \mathbb{C} \times \mathbb{N} \times \mathbb{N}$. 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 \text{ and }
Thus, \( \eta \) is a \( \mathbb{K}[F] \)-\( \mathbb{K}[T] \)-bimodule homomorphism. 

Now, recall that \( (r_{(i,j)})_{(i,j) \in C} \) is a basis of the free \( \mathbb{K} \)-module \( \mathcal{R} \). Hence, \( \mathcal{R} = \)

\[
\frac{F^p F^k \otimes T^\ell}{=F^{p+k}} = r_{(i,j)} \otimes F^{p+k} \otimes T^\ell. 
\]

Hence,

\[
\eta(fz) = \eta \Bigg( r_{(i,j)} \otimes F^{p+k} \otimes T^\ell \Bigg) = T^{p+k} (j+r\ell) F^{i+k}.
\]

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

\[
f = F^p \quad \eta(z) = \underbrace{F^p T^k (j+r\ell)}_{=F^{p+k}} = F^{i+k} = \underbrace{F^p = F^{p+k}}_{=F^{p+k}}.
\]

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

15 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.

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 \( (T^\ell)_{\ell \in \mathbb{N}} \) of \( \mathbb{K}[T] \), and that \( z \) belongs to the basis \( (r_{(i,j)} \otimes F^k \otimes T^\ell)_{((i,j), k) \in C \times \mathbb{N} \times \mathbb{N}} \) 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 \( ((i,j), k, \ell) \in C \times \mathbb{N} \times \mathbb{N} \). Consider these \( p \) and \( ((i,j), k, \ell) \).

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

\[
\eta(zt) = \eta \Bigg( r_{(i,j)} \otimes F^k \otimes T^{\ell+p} \Bigg) = T^{k} (j+r(\ell+p)) F^{i+k},
\]

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

\[
\eta(z) t = T^{k} (j+r\ell) F^{i+k} = \underbrace{T^{k} (j+r\ell) T^{p+i+k}}_{=T^{k} (j+r\ell+i+p)} = \underbrace{T^{k} (j+r\ell+i+p)}_{=T^{k} (j+r(\ell+p))},
\]

Comparing this with \( \eta(zt) = T^{k} (j+r(\ell+p)) F^{i+k} \), we obtain \( \eta(zt) = \eta(z) t \), qed.
$\bigoplus_{(i,j) \in C} r_{(i,j)} K$. Since direct sums commute with tensor products, this yields

$$\mathcal{R} \otimes K[F] \otimes K[T] = \bigoplus_{(i,j) \in C} r_{(i,j)} K \otimes K[F] \otimes K[T]$$

$$= K[F] \cdot (r_{(i,j)} \otimes F^0 \otimes T^0) \cdot K[T]$$

(this follows easily from the definition of the $K[F] \cdot K[T]$-bimodule structure on $\mathcal{R} \otimes K[F] \otimes K[T]$)

$$= \bigoplus_{(i,j) \in C} K[F] \cdot \left( r_{(i,j)} \otimes F^0 \otimes T^0 \right) \cdot K[T].$$

We can apply the map $\eta$ to this equality. The left hand side becomes $\mathcal{M}$ (since $\eta$ is an isomorphism of $K$-modules), and the direct sum on the right hand side remains direct (for the same reason). Hence, we obtain

$$\mathcal{M} = \bigoplus_{(i,j) \in C} \eta \left( K[F] \cdot \left( r_{(i,j)} \otimes F^0 \otimes T^0 \right) \cdot K[T] \right)$$

$$= K[F] \cdot \eta \left( r_{(i,j)} \otimes F^0 \otimes T^0 \right) \cdot K[T]$$

(by the definition of $\eta$)

$$= \bigoplus_{(i,j) \in C} K[F] \cdot \left( r_{(i,j)} \otimes F^0 \otimes T^0 \right) \cdot K[T]$$

$$= \bigoplus_{(i,j) \in \mathbb{N}^2; (i=0 \text{ or } r|j) \text{ and } 0 \leq j < r^i} K[F] \cdot \left( T^i F^j \right) \cdot K[T].$$

It remains to show that each $K[F] \cdot \left( T^i F^j \right) \cdot K[T]$ is isomorphic to $K[F] \otimes K[T]$ as an $K[F] \cdot K[T]$-bimodule. This follows from $\eta$ 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 $\text{Frob}_A : A \rightarrow A$ be the map which sends every $a \in A$ to $a^q$. This map $\text{Frob}_A$ is called the Frobenius endomorphism.
of \( A \). It is well-known that \( \text{Frob}_A \) is an \( \mathbb{F}_q \)-algebra homomorphism. We will often denote the \( \mathbb{F}_q \)-algebra homomorphism \( \text{Frob}_A \) by \( \text{Frob} \) when no confusion can arise from the omission of \( A \). A rather important particular case is the endomorphism \( \text{Frob} = \text{Frob}_\mathbb{F}_q[T] \) of the commutative \( \mathbb{F}_q \)-algebra \( \mathbb{F}_q[T] \).

We let \( \mathcal{F} \) be the \( \mathbb{F}_q \)-algebra \( \mathbb{F}_q \langle F, T \mid FT = T^q F \rangle \). 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 \( \text{Finc}_F : \mathbb{F}_q[F] \to \mathcal{F} \) by \( \text{Finc}_F(F) = F \). Thus, \( \text{Finc}_F(p) = p(F) \) for every \( p \in \mathbb{F}_q[F] \) (where \( p(F) \) means the result of substituting \( F \) into the polynomial \( p \)).

- We define an \( \mathbb{F}_q \)-algebra homomorphism \( \text{Finc}_T : \mathbb{F}_q[T] \to \mathcal{F} \) by \( \text{Finc}_T(T) = T \). Thus, \( \text{Finc}_T(p) = p(T) \) 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 \( \text{Carl} : \mathbb{F}_q[T] \to \mathcal{F} \) by \( \text{Carl}(T) = F + T \). Thus, \( \text{Carl}(p) = p(F + T) \) 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 \( \text{Fpro}_F : \mathcal{F} \to \mathbb{F}_q[F] \) by \( \text{Fpro}_F(F) = F \) and \( \text{Fpro}_F(T) = 0 \). It is easy to see that \( \text{Fpro}_F \circ \text{Finc}_F = \text{id} \). Hence, the \( \mathbb{F}_q \)-algebra homomorphism \( \text{Finc}_F \) is injective. Thus, we shall regard \( \text{Finc}_F \) 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 \( \text{Fpro}_T : \mathcal{F} \to \mathbb{F}_q[T] \) by \( \text{Fpro}_T(F) = 0 \) and \( \text{Fpro}_T(T) = T \). It is easy to see that \( \text{Fpro}_T \circ \text{Finc}_T = \text{id} \). Hence, the \( \mathbb{F}_q \)-algebra homomorphism \( \text{Finc}_T \) is injective. Thus, we shall regard \( \text{Finc}_T \) 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 \( \text{Fscal}_{a,b} : \mathcal{F} \to \mathcal{F} \) by \( \text{Fscal}_{a,b}(F) = a F \) and \( \text{Fscal}_{a,b}(T) = b T \). (This is well-defined, since \( (a F)(b T) = (b T)^q (a F) \).) If \( a \) and \( b \) are nonzero, then \( \text{Fscal}_{a,b} \) is invertible (with inverse \( \text{Fscal}_{a^{-1}, b^{-1}} \)).

\[ \text{This follows from the fact that } (\lambda a)^q = \lambda^q a^q \text{ for every } a \in A \text{ and } \lambda \in \mathbb{F}_q, \text{ and } \text{the fact that } (a + b)^q = a^q + b^q \text{ for every } a, b \in A. \]
Now, we shall derive some structural properties of \( \mathcal{F} \) straight from Proposition 3.1.

**Proposition 3.5.** The homomorphisms \( \text{Finc}_T \) and \( \text{Finc}_F \) 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 \( F^a T^b = T^{qb} F^a \) 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 \( \{ T^i F^j \}_{i \geq 0, j \geq 0} \).

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

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

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

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

(g) As \( \mathbb{F}_q [F] \)-\( \mathbb{F}_q [T] \)-bimodule, \( \mathcal{F} \) is free with basis \( \{ T^i F^j \}_{(i,j) \in \mathbb{N}^2, (i=0 \text{ or } q/ j) \text{ and } 0 \leq j < q^i} \).

Then, \( \mathcal{F} = \bigoplus_{(i,j) \in \mathbb{N}^2} \mathbb{F}_q [F] \cdot (T^i F^j) \cdot \mathbb{F}_q [T] \), and each \( \mathbb{F}_q [F] \cdot (T^i F^j) \cdot \mathbb{F}_q [T] \) is isomorphic to \( \mathbb{F}_q [F] \otimes \mathbb{F}_q [T] \) as a \( \mathbb{F}_q [F] \)-\( \mathbb{F}_q [T] \)-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 \( K = \mathbb{F}_q \) and \( r = q \).

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

**Proposition 3.6.** Let \( P \in \mathbb{F}_q [T] \). Then, \( FP = P^q F \) in \( \mathcal{F} \).

**Proof of Proposition 3.6.** We are going to prove that \( FP = (\text{Frob} \ P) \ F \). Since both sides of this equality are \( \mathbb{F}_q \)-linear in \( P \) (because \( \text{Frob} \) is an \( \mathbb{F}_q \)-linear map), we can WLOG assume that \( P \) belongs to the basis \( \{ T^i \}_{i \geq 0} \) 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 \( \text{Frob} \) yields \( \text{Frob} \ P = \left( \begin{array}{c} P \\ = T^i \end{array} \right)^q = (T^i)^q = T^{q^i} \).

Now, \( \left( \begin{array}{c} F \\ = T^i \end{array} \right)^P = F^1 T^i = T^{q^i} F^1 \) (by Proposition 3.5(a)), so that \( FP = \left( \begin{array}{c} T^{q^i} \\ = T^q = \text{Frob} \ P \end{array} \right) \left( \begin{array}{c} F \\ = F \end{array} \right) = (\text{Frob} \ P) \ F \).

Thus, \( FP = (\text{Frob} \ P) \ F \) is proven. Hence, \( FP = (\text{Frob} \ P) \ F = P^q F \). This proves Proposition 3.6. 

\( \square \)
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

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

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, $F^n P \in P \cdot \mathcal{F}$.

Now, $F^{n+1} P = F F^n P \in P \cdot \mathcal{F}$ (by Proposition 3.6).

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

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

Now, we shall prove that

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

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 $(T^i F^j)_{i \geq 0, j \geq 0}$ of the $\mathbb{F}_q$-module $\mathcal{F}$. Assume this. Thus, $u = T^i F^j$ for some $(i, j) \in \mathbb{N}^2$. Consider this $(i, j)$. Now,

$$u = T^i F^j P = T^i P \in P \cdot \mathcal{F} \quad \text{(by (20))}$$

This proves (21).

Now, (21) immediately yields $\mathcal{F} \cdot P \subseteq P \cdot \mathcal{F}$. Hence, $\mathcal{F} \cdot \mathcal{F} \subseteq P \cdot \mathcal{F}$. 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 $A \left[ X \right]$ is said to be a $q$-polynomial if it is an $A$-linear combination of the monomials $X^q, X^q^1, X^q^2, \ldots$. We let $A \left[ X \right]_{q \text{-lin}}$ be the set of all $q$-polynomials in $A \left[ X \right]$. Thus, $A \left[ X \right]_{q \text{-lin}}$ is an $A$-submodule of $A \left[ X \right]$; as an $A$-submodule, it has basis $(X^q, X^q^1, X^q^2, \ldots)$.

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

The $A$-submodule $A \left[ X \right]_{q \text{-lin}}$ of $A \left[ X \right]$ is not a subring of $A \left[ X \right]$ (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 $f \in A \left[ X \right]$ and $g \in A \left[ X \right]$. Then, $f \circ g$ denotes the polynomial $f \left( g \right) \in A \left[ X \right]$. (This is the polynomial obtained from $f$ by substituting $g$ for $X$.) This defines a binary operation $\circ$ on the set $A \left[ X \right]$.

Proposition 3.10. Let $A$ be a commutative ring.

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

(b) Assume that $A$ is a commutative $\mathbb{F}_q$-algebra. Then, $A \left[ X \right]_{q \text{-lin}}$ is a submonoid of the monoid $(A \left[ X \right], \circ)$. Moreover, $(A \left[ X \right]_{q \text{-lin}}, +, \circ)$ is a (noncommutative) $\mathbb{F}_q$-algebra with unity $X$ (where the $\mathbb{F}_q$-module structure is the one obtained by restricting the $A \left[ X \right]$-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 $\varphi : A \left[ X \right] \to B$ satisfying $\varphi \left( X \right) = b$. \[\text{[17]}\] We shall denote this homomorphism $\varphi$ by $ev_b$. It has the property that
\[ev_b \left( f \right) = f \left( b \right) \quad \text{for every } f \in A \left[ X \right].\] \hspace{1cm} (22)

Now, every $f, g \in A \left[ X \right]$ satisfy
\[ev_g \left( f \right) = f \left( g \right) \quad \text{(by (22), applied to } B = A \left[ X \right] \text{ and } b = g)\]
\[= f \circ g \quad \text{(since } f \circ g = f \left( g \right)) .\] \hspace{1cm} (23)

Let $f, g, h \in A \left[ X \right]$. Then, (23) yields $ev_g \left( f \right) = f \circ g$. Furthermore, (23) (applied to $f \circ g$ and $h$ instead of $f$ and $g$) yields $ev_h \left( f \circ g \right) = (f \circ g) \circ h$. But (23) (applied to $g$ and $h$ instead of $f$ and $g$) yields $ev_h \left( g \right) = g \circ h$. Finally, (23) (applied to $g \circ h$ instead of $g$) yields $ev_{g \circ h} \left( f \right) = f \circ (g \circ h)$.

\[\text{[17]}\] This is simply the universal property of the polynomial ring $A \left[ X \right]$.
The defining property of \( ev_{g \circ h} \) yields \( ev_{g \circ h} (X) = g \circ h \). But the defining property of \( ev_{g} \) yields \( ev_{g} (X) = g \). Now,

\[
(ev_h \circ ev_g) (X) = ev_h \left( ev_g (X) \right) = ev_h (g) = g \circ h.
\]

Comparing this with \( ev_{g \circ h} (X) = g \circ h \), we obtain \( (ev_h \circ ev_g) (X) = ev_{g \circ h} (X) \). The two maps \( ev_h \circ ev_g \) and \( ev_{g \circ h} \) 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 \( ev_{g \circ h} \) are \( A \)-algebra homomorphisms), this shows that these two maps are equal. In other words, \( ev_h \circ ev_g = ev_{g \circ h} \). Hence, \( (ev_h \circ ev_g) (f) = ev_{g \circ h} (f) = f \circ (g \circ h) \). Thus,

\[
f \circ (g \circ h) = (ev_h \circ ev_g) (f) = ev_h \left( ev_g (f) \right) = ev_h (f \circ g) = (f \circ g) \circ h.
\]

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

\[
\text{Frob}^n (f) = f^{q^n} \quad \text{for every } f \in A[X] \text{ and } n \in \mathbb{N}.
\]  

(24)

It is easy to see that

\[
\text{Frob} \left( A[X]_{q-\text{lin}} \right) \subseteq A[X]_{q-\text{lin}}
\]  

(25)

Using this fact, it is straightforward to see (by induction over \( n \)) that

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

(26)

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

Indeed, \( g \in A[X]_{q-\text{lin}}. \text{ Thus, } g \text{ is an } A \text{-linear combination of } \left( X^{q^0}, X^{q^1}, X^{q^2}, \ldots \right) \text{ (since the } A \text{-module } A[X]_{q-\text{lin}} \text{ has basis } \left( X^{q^0}, X^{q^1}, X^{q^2}, \ldots \right)). \text{ In other words, there exists a sequence } (a_0, a_1, a_2, \ldots) \in A^{\mathbb{N}} \text{ of elements of } A \text{ such that } g = \sum_{n \in \mathbb{N}} a_n X^{q^n}, \text{ and such that all but finitely many } n \in \mathbb{N} \text{ satisfy } a_n = 0. \text{ Consider this sequence.}\]
Step 2: Now, let us prove that
\[ f \circ (\lambda_1 g_1 + \lambda_2 g_2) = \lambda_1 (f \circ g_1) + \lambda_2 (f \circ g_2) \] (27)

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

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

We have \( f \in A [X]_{q-\text{lin}} \). Thus, \( f \) is an \( A \)-linear combination of \( \left( X^{q^0}, X^{q^1}, X^{q^2}, \ldots \right) \) (since the \( A \)-module \( A [X]_{q-\text{lin}} \) 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 \( \hat{f} \) denote the element \( \sum_{n \in \mathbb{N}} a_n \text{Frob}^n \) of \( \text{End} (A [X]) \). (This is well-defined, since \( \text{Frob}^n \in \text{End} (A [X]) \) for every \( n \in \mathbb{N} \).) Now, every \( h \in A [X] \) satisfies
\[ f \circ h = \hat{f} (h) \] (28)

Applying the map \( \text{Frob} \) to the equality \( g = \sum_{n \in \mathbb{N}} a_n X^{q^n} \), we obtain
\[ \text{Frob} g = \text{Frob} \left( \sum_{n \in \mathbb{N}} a_n X^{q^n} \right) = \sum_{n \in \mathbb{N}} \text{Frob} \left( a_n X^{q^n} \right) \quad \text{(since the map \( \text{Frob} \) is \( \mathbb{F}_q \)-linear)} \]
\[ = \sum_{n \in \mathbb{N}} a_n^q \left( X^{q^n} \right)^{\frac{q^n}{q}} \in \sum_{n \in \mathbb{N}} a_n^q A [X]_{q-\text{lin}} \subseteq A [X]_{q-\text{lin}} \]
\[ \left( \text{since } A [X]_{q-\text{lin}} \text{ is an } A \text{-module}. \right) \]

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

19 Proof of (28): Let \( h \in A [X] \). Then,
\[ f \circ h = f (h) = \sum_{n \in \mathbb{N}} a_n h^{q^n} \quad \text{(since } f = \sum_{n \in \mathbb{N}} a_n X^{q^n}) \].

Comparing this with
\[ \hat{f} (h) = \sum_{n \in \mathbb{N}} a_n \text{Frob}^n (h) \quad \text{(by \ref{sec:proof_of_24}, applied to } h) \]
\[ = \sum_{n \in \mathbb{N}} a_n h^{q^n} \]
this yields \( f \circ h = \hat{f} (h) \), qed.
Comparing this with $\lambda$ for every operation we obtain
$$f \circ (\lambda_1 g_1 + \lambda_2 g_2) = \hat{f} (\lambda_1 g_1 + \lambda_2 g_2) = \lambda_1 \hat{f} (g_1) + \lambda_2 \hat{f} (g_2)$$
(since $\hat{f} \in \text{End} (A \langle X \rangle)$). Comparing this with
$$\lambda_1 \hat{f} (g_1) + \lambda_2 \hat{f} (g_2) = \hat{f} (\lambda_1 g_1) + \lambda_2 \hat{f} (g_2) \quad \text{(by (28))}$$
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
$$\lambda_1 f_1 + \lambda_2 f_2 \circ g = \lambda_1 (f_1 \circ g) + \lambda_2 (f_2 \circ g) \quad \text{(29)}$$
for every $f_1, f_2 \in A \langle X \rangle$ and $\lambda_1, \lambda_2 \in \mathbb{F}_q$.

**Proof of (29):** Let $f_1, f_2 \in A \langle X \rangle$, $g \in A \langle X \rangle$, $\lambda_1, \lambda_2 \in \mathbb{F}_q$. Then,
$$\lambda_1 f_1 + \lambda_2 f_2 \circ g = \lambda_1 f_1 (g) + \lambda_2 f_2 (g).$$
Comparing this with $\lambda_1 (f_1 \circ g) + \lambda_2 (f_2 \circ g) = \lambda_1 f_1 (g) + \lambda_2 f_2 (g)$, we obtain
$$\lambda_1 f_1 (g) = f_1 (g) \quad \text{(by (28))}$$
and
$$\lambda_2 f_2 (g) = f_2 (g) \quad \text{(by (28)).}$$
This proves (29).

**Step 4:** Now, let us show that
$$f \circ g \in A \langle X \rangle_{	ext{q-lin}}$$
for every $f, g \in A \langle X \rangle_{	ext{q-lin}}$.

**Proof of (30):** Let $f, g \in A \langle X \rangle_{	ext{q-lin}}$. Define the sequence $(a_0, a_1, a_2, \ldots) \in A^\mathbb{N}$ and the element $\hat{f} \in \text{End} (A \langle X \rangle)$ as in the proof of (27). Then, (28) holds. Applying (28) to $h = g$, we obtain
$$f \circ g = \hat{f} (g) = \sum_{n \in \mathbb{N}} a_n \text{Frob}^n \left( g \right) \quad \text{(since } f = \sum_{n \in \mathbb{N}} a_n \text{Frob}^n)$$
and
$$f \circ g \in A \langle X \rangle_{\text{q-lin}} \quad \text{(by (28))}$$
(since $A \langle X \rangle_{\text{q-lin}}$ is an $A$-module). Thus, we have proven (30).

**Step 5:** We have $X = X^1 \in A \langle X \rangle_{\text{q-lin}}$. This, combined with (30), shows that $A \langle X \rangle_{\text{q-lin}}$ is a submonoid of the monoid $(A \langle X \rangle, \circ)$. Furthermore, the binary operation $\circ$ on $A \langle X \rangle_{\text{q-lin}}$ is $\mathbb{F}_q$-bilinear (by (27) and (29)) and associative (since $(A \langle X \rangle, \circ)$ is a monoid) and has neutral element $X$ (since $(A \langle X \rangle, \circ)$ is a monoid with neutral element $X$). Thus, $(A \langle X \rangle_{\text{q-lin}}, +, \circ)$ 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 \( \left( A[X]_{q-\text{lin}}, +, \circ \right) \) constructed in Proposition 3.10 will be called the Ore polynomial ring over \( A \), and simply denoted by \( A[X]_{q-\text{lin}} \) (since there are no other \( \mathbb{F}_q \)-algebra structures on \( A[X]_{q-\text{lin}} \) 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 over \( \mathbb{F}_q [T] [X]_{q-\text{lin}} \) (recall that this is the \( \mathbb{F}_q \)-algebra \( \left( \mathbb{F}_q [T] [X]_{q-\text{lin}}, +, \circ \right) \)). (Notice that polynomials in \( \mathbb{F}_q [T] [X]_{q-\text{lin}} \) contain arbitrary powers of \( T \), but the only powers of \( X \) they can contain are \( X^q, X^{q^2}, X^{q^3}, \ldots \)) Define an \( \mathbb{F}_q \)-algebra homomorphism \( \text{Fqpol} : \mathcal{F} \rightarrow \mathbb{F}_q [T] [X]_{q-\text{lin}} \) by \( \text{Fqpol} (F) = X^q \) and \( \text{Fqpol} (T) = TX \).

(a) This homomorphism \( \text{Fqpol} \) is well-defined.

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

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

(d) We have \( \text{Fqpol} t = t \cdot X \) 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
\[
(TX)^\circ n = T^n X \quad \text{in} \quad \mathbb{F}_q [T] [X]_{q-\text{lin}}.
\] (This follows by a straightforward induction on \( n \).) Furthermore, for every \( n \in \mathbb{N} \), we have
\[
(X^q)^\circ n = X^{q^n} \quad \text{in} \quad \mathbb{F}_q [T] [X]_{q-\text{lin}}.
\] (Again, this is easy to prove by induction.)

(a) In \( \mathbb{F}_q [T] [X]_{q-\text{lin}} \), 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 \( (TX)^\circ q \circ X^q = T^q X \) (by (31), applied to \( n=q \))). 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 \( \mathcal{F} \rightarrow \mathcal{U} \) sending \( F \) and \( T \) to \( u \) and \( v \), respectively. Applying this to \( \mathcal{U} = \mathbb{F}_q [T] [X]_{q-\text{lin}} \), \( u = X^q \) and \( v = TX \), we thus conclude that there exists a unique \( \mathbb{F}_q \)-algebra homomorphism \( \mathcal{F} \rightarrow \mathcal{U} \) sending \( F \) and \( T \) to \( X^q \) and \( TX \),
respectively. In other words, the homomorphism $F_{q\text{pol}}$ is well-defined. This proves Theorem 3.13 \((a)\).

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

$$F_{q\text{pol}} \left( T^i F^j \right) = \left( \frac{F_{q\text{pol}} T}{=TX} \right)^{\circ j} \circ \left( \frac{F_{q\text{pol}}}{=X^q} \right)^{\circ i}$$

(since $F_{q\text{pol}}$ is an $F_q$-algebra homomorphism)

$$= \left( TX \right)^{\circ j} \circ \left( X^q \right)^{\circ i} = \left( T^i X \right) \circ X^q = T^i X^q.$$  

This proves Theorem 3.13 \(c\).

\(b\) The $F_q [T]$-module $F_q [T] [X]_{q\text{--lin}}$ has basis $(X^q^0, X^q^1, X^q^2, \ldots) = \left( X^q \right)_{i \geq 0}$.

Thus, as an $F_q$-module, it has basis $(T^i X^q)_{i \geq 0, j \geq 0}$.

On the other hand, Proposition 3.14 \(b\) says that the $F_q$-module $F$ is free with basis $(T^i F^j)_{i \geq 0, j \geq 0}$.

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

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

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

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

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

**Proof of Proposition 3.14** Let $\text{End} B$ denote the $F_q$-algebra of all endomorphisms of the $F_q$-vector space $B$. It is easy to see that $\text{Frob} = \text{Frob}_B \in \text{End} B$. Hence,
Frob^n ∈ End B for every n ∈ N. It is straightforward to see (by induction over n) that
\[ \text{Frob}^n (b) = b q^n \quad \text{for every } b ∈ B \text{ and } n ∈ N. \quad (33) \]

We have f ∈ A [X]_{q - \text{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 - \text{lin}} has basis \( \left( X q^0, X q^1, X q^2, \ldots \right) \)). In other words, there exists a sequence \( (a_0, a_1, a_2, \ldots) ∈ A^N \) of elements of A such that \( f = \sum_{n∈N} a_n X q^n \), and such that all but finitely many \( n ∈ N \) satisfy \( a_n = 0 \). Consider this sequence.

Recall that

Let \( \hat{f} \) denote the element \( \sum_{n∈N} a_n \text{Frob}^n \) of End B. (This is well-defined, since Frob^n ∈ End B for every n ∈ N.) Now, every b ∈ B satisfies
\[ f (b) = \hat{f} (b) \quad (34) \]

Hence, the map \( B → B, \ b → f (b) \) equals the map \( B → B, \ b → \hat{f} (b) \). But the latter map is simply the map \( \hat{f} ∈ \text{End } B \), 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 \( f ∈ A [X] \) be such that, for every commutative A-algebra B, the map \( B → B, \ b → f (b) \) is \( \mathbb{F}_q \)-linear. Then, \( f ∈ A [X]_{q - \text{lin}}. \)

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 \( A [X]_{q - \text{lin}} \)) 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).

**Proof of (34):** Let b ∈ B. From \( f = \sum_{n∈N} a_n X q^n \), we obtain \( f (b) = \sum_{n∈N} a_n b q^n \). Comparing this with
\[ \hat{f} (b) = \sum_{n∈N} a_n \text{Frob}^n (b) \quad \text{(since } \hat{f} = \sum_{n∈N} a_n \text{Frob}^n \text{)} \]
\[ = \sum_{n∈N} a_n b q^n, \]
this yields \( f (b) = \hat{f} (b) \), qed.

43
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 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 [13, (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 an \( \mathbb{F}_q \)-vector subspace of \( A \). Then, \( f_V \) is a \( q \)-polynomial.

We shall prove Theorem 3.17 following an idea that appears in [13, proof of (7.15)]; but first, let us slightly generalize it:

**Definition 3.18.** Let \( A \) be a commutative \( \mathbb{F}_q \)-algebra. For every set \( V \) and every map \( \varphi : V \rightarrow A \), 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 an \( \mathbb{F}_q \)-vector space, and let \( \varphi : V \rightarrow A \) 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 \( \mathbb{F}_q \)-vector spaces. Let \( \varphi : V \rightarrow A \) and \( \psi : W \rightarrow A \) be two \( \mathbb{F}_q \)-linear maps. Assume that \( f_{W,\psi} \) is a \( q \)-polynomial. Let \( h : A \rightarrow A \) be an \( \mathbb{F}_q \)-linear map such that every \( a \in A \) satisfies

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

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

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

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

$$f_{W, \varphi} (X + \varphi (v)) = f_{W, \varphi} (X) + f_{W, \varphi} (\varphi (v)).$$

Comparing this with (37), we obtain

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

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

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

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

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

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

$$f_{V \oplus W, X} = \prod_{v \in V \oplus W} (X + \chi (v)) = \prod_{(v, w) \in V \oplus W} \left( X + \chi (v, w) \right) = \prod_{v \in V} \prod_{w \in W} (X + \chi (v, w)) \tag{here, we renamed the index $v$ as $(v, w)$ in the product}

= \prod_{v \in V} \prod_{w \in W} (X + \varphi (v) + \psi (w)) = \prod_{v \in V} (f_{W, \varphi} + (h \circ \varphi) (v))$$

(by (38))

$$= f_{V, h \circ \varphi} (f_{W, \varphi}) \quad \text{(by (39))}$$

This proves Lemma 3.20. □
Lemma 3.21. We have
\[
\prod_{\lambda \in \mathbb{F}_q} (X - \lambda Y) = X^q - X Y^{q-1}
\] (40)
in the polynomial ring \( \mathbb{F}_q [X, Y] \).

Proof of Lemma 3.21. It is well-known that
\[
\prod_{\lambda \in \mathbb{F}_q} (X - \lambda) = X^q - X
\] (41)
in the polynomial ring \( \mathbb{F}_q [X] \).

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

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 \( |\mathbb{F}_q| = q \) 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
\[
\prod_{\lambda \in \mathbb{F}_q} (\mu - \lambda) = \begin{cases} 
\mu^q & \text{if } \mu \in \mathbb{F}_q \\
0 & \text{if } \mu \not\in \mathbb{F}_q 
\end{cases}
\]

(since one of the factors of this product is \( \lambda = \lambda \) 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).
Hence,

\[ X^q - XY^{q-1} = Y^q \prod_{\lambda \in F_q} \left( X/Y - \lambda \right) = \prod_{\lambda \in F_q} \left( Y \left( X/Y - \lambda \right) \right) = \prod_{\lambda \in F_q} \left( X - \lambda Y \right). \]

(since \(|F_q| = q\))

This proves Lemma 3.21.

**Lemma 3.22.** Let \( A \) be a commutative \( F_q \)-algebra. Let \( V \) be a one-dimensional \( F_q \)-vector space. Let \( \varphi : V \to A \) be an \( F_q \)-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 \( F_q \)-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 \( F_q \to V, \lambda \mapsto \lambda \cdot (-e) \) is a bijection. Now, the definition of \( f_{V,\varphi} \) yields

\[
f_{V,\varphi} = \prod_{v \in V} (X + \varphi(v)) = \prod_{\lambda \in F_q} \left( X + \varphi \left( \lambda \cdot (-e) \right) \right) \]

(here, we have substituted \( \lambda (-e) \) for \( v \) in the product, since the map \( F_q \to V, \lambda \mapsto \lambda (-e) \) is a bijection)

\[
= \prod_{\lambda \in F_q} \left( X + \varphi(-\lambda e) \right) = \prod_{\lambda \in F_q} \left( X - \lambda \varphi(e) \right) \]

(since \( \varphi \) is \( F_q \)-linear)

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

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

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 \( \dim V = 0 \).

This 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

\[
f_{V,\varphi} = \prod_{v \in V} (X + \varphi(v)) = X + \varphi(0) \quad \text{(since} \ V = 0) \]

(since \( \varphi \) is \( F_q \)-linear)

\[
= X. \]

Thus, \( f_{V,\varphi} \) is a \( q \)-polynomial (since \( X \) is a \( q \)-polynomial). Thus, Theorem 3.19 is proven in the case when \( \dim V = 0 \).
Proposition 3.14 (applied to $V$) is one of the basic theorems of linear algebra). Then, Theorem 3.19 can be applied to $U \oplus W = V$. We shall identify $V$ with the external direct sum of $U$ and $W$ (that is, we shall identify each element 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 $\gamma = \varphi |_U$ and $\psi = \varphi |_W$. Then, the $\mathbb{F}_q$-linear map $\varphi : U \oplus W \to A$ sends every $(v, w) \in U \oplus W$ to $\gamma (v) + \psi (w)$.

From $V = U \oplus W$, we obtain $\dim V = \dim U + \dim W$, so that $\dim W = \dim V - \dim U = N + 1 - 1 = N$. Thus, (according to the induction hypothesis) Theorem 3.19 can be applied to $W$ and $\psi$ instead of $V$ and $\varphi$. As a consequence, we obtain that $f_{W, \psi}$ is a $q$-polynomial. In other words, $f_{W, \psi} \in A [X]_{q-\text{lin}}$. 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 $U$, $\gamma$ and $\varphi$ instead of $V$, $\varphi$ and $\chi$) 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 $\varphi$) 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, $f_{U, h \circ \gamma} \in A [X]_{q-\text{lin}}$.

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

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 $\varphi = \varphi |_U$). We have $w \in W$, and thus $\psi (w) = \varphi (w)$ (since $\psi = \varphi |_W$). The map $\varphi$ is $\mathbb{F}_q$-linear, and thus $\varphi (v + w) = \varphi (v) + \varphi (w) = \gamma (v) + \psi (w)$. 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.

23 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 $\varphi = \varphi |_U$). We have $w \in W$, and thus $\psi (w) = \varphi (w)$ (since $\psi = \varphi |_W$). The map $\varphi$ is $\mathbb{F}_q$-linear, and thus $\varphi (v + w) = \varphi (v) + \varphi (w) = \gamma (v) + \psi (w)$. 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.
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.

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

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

**Proof of Corollary 3.23** Theorem 3.19 (applied to $W$ and $\psi$ instead of $V$ and $\varphi$) 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 $\iota$ be the canonical inclusion map $V \rightarrow A$. Thus, $\iota$ 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

$$f_{V,\iota} = \prod_{v \in V} \left( X + \iota(v) \right) = \prod_{v \in V} (X + v) = f_V$$

(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 $\mathbb{F}_q\text{-pol}$ isomorphism

Let us return to $\mathcal{F}$. We shall now exploit the isomorphism $\mathbb{F}_q\text{-pol}$ to obtain properties of $\mathcal{F}$.

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

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

We shall write this $\mathbb{F}_q[\![T]\!]$-module structure on the left (i.e., we use it to make $\mathbb{F}_q[\![T]\!] [\![X]\!]_{q-\text{lin}}$ 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 $F_{q\text{pol}} : \mathcal{F} \to \mathbb{F}_q[T][X]_{q\text{-lin}}$ 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 $(T^j F^i)_{i \geq 0, j \geq 0}$.

Theorem 3.13 (b) shows that $F_{q\text{pol}}$ is an $\mathbb{F}_q$-algebra isomorphism. Thus, it remains to prove that $F_{q\text{pol}}$ is a homomorphism of left $\mathbb{F}_q[T]$-modules. In other words, it remains to prove that $F_{q\text{pol}}(uf) = f F_{q\text{pol}}(u)$ 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 $F_{q\text{pol}}(uf) = f F_{q\text{pol}}(u)$. This equality is $\mathbb{F}_q$-linear in $u$. Hence, we can WLOG assume that $u$ belongs to the basis $(T^j F^i)_{i \geq 0, j \geq 0}$ 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 $F_{q\text{pol}}(fu) = f F_{q\text{pol}}(u)$. This equality is $\mathbb{F}_q$-linear in $f$. Hence, we can WLOG assume that $f$ belongs to the basis $(T^k)_{k \geq 0}$ of the $\mathbb{F}_q$-module $\mathbb{F}_q[T]$. Assume this. Thus, $f = T^k$ for some $k \in \mathbb{N}$ and $j \in \mathbb{N}$. Consider this $k$.

Multiplying the equalities $f = T^k$ and $u = T^j F^i$, we obtain $fu = T^k T^j F^i = T^{k+j} F^i$. Hence, $F_{q\text{pol}}(fu) = F_{q\text{pol}}(T^{k+j} F^i) = T^{k+j} X^q^i$ (by Theorem 3.13 (c), applied to $k+j$ instead of $j$). On the other hand, $u = T^j F^i$, so that $F_{q\text{pol}}(u) = F_{q\text{pol}}(T^j F^i) = T^j X^q^i$ (by Theorem 3.13 (b)). Multiplying the equalities $f = T^k$ and $F_{q\text{pol}}(u) = T^j X^q^i$, we obtain $f F_{q\text{pol}}(u) = T^k T^j X^q^i = T^{k+j} X^q^i$. Comparing this with $F_{q\text{pol}}(fu) = T^{k+j} X^q^i$, we obtain $F_{q\text{pol}}(fu) = f F_{q\text{pol}}(u)$. 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 $\mathcal{F} \cong \mathbb{F}_q[T][X]_{q\text{-lin}}$ as left $\mathbb{F}_q[T]$-modules, via the isomorphism $F_{q\text{pol}}$. Since the left $\mathbb{F}_q[T]$-module $\mathbb{F}_q[T][X]_{q\text{-lin}}$ has basis $(X^{q^0}, X^{q^1}, X^{q^2}, \ldots)$, we can therefore conclude that the left $\mathbb{F}_q[T]$-module $\mathcal{F}$ has basis $\left\{ F_{q\text{pol}}^{-1}\left(X^{q^0}\right), F_{q\text{pol}}^{-1}\left(X^{q^1}\right), F_{q\text{pol}}^{-1}\left(X^{q^2}\right), \ldots \right\}$. Since $F_{q\text{pol}}^{-1}\left(X^{q^i}\right) = F^i$ for every $i \in \mathbb{N}$, this rewrites as follows: The left $\mathbb{F}_q[T]$-module $\mathcal{F}$ has basis $(F^i)_{i \geq 0}$. This proves Proposition 3.5 (c) again.

24 Proof. Let $i \in \mathbb{N}$. Theorem 3.13 (c) (applied to $j = 0$) yields $F_{q\text{pol}}\left(T^0 F^i\right) = T^0 \overset{1}{\overset{1}{=}} X^q^i = X^{q^i}$. Thus, $F_{q\text{pol}}^{-1}\left(X^{q^i}\right) = T^0 \overset{1}{\overset{1}{=}} F^i$, qed.
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 \( F_q[T] \)-module structure on \( \mathcal{F} \) to \( F_q[T][X]_{q\text{-lin}} \) via the isomorphism \( \text{Fqpol} : \mathcal{F} \to F_q[T][X]_{q\text{-lin}} \), then we obtain the left \( F_q[T] \)-module structure on \( F_q[T][X]_{q\text{-lin}} \) constructed in (42). Of course, we can also use the isomorphism \( \text{Fqpol} \) to transport all the other module structures from \( \mathcal{F} \) to \( F_q[T][X]_{q\text{-lin}} \) along \( \text{Fqpol} \). In more detail:

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

- If \( t \in F_q[T] \), then the action of \( t \) on the right \( F_q[T] \)-module \( F_q[T][X]_{q\text{-lin}} \) sends every \( m \in F_q[T][X]_{q\text{-lin}} \) to \( m \circ \text{Fqpol} t = m \circ (t \cdot X) = t \cdot X (m) \) (that is, the result of substituting \( t \cdot X \) for \( X \) in \( m \)).

- If \( f \in F_q[F] \), then the action of \( f \) on the left \( F_q[F] \)-module \( F_q[T][X]_{q\text{-lin}} \) sends every \( m \in F_q[T][X]_{q\text{-lin}} \) to \( \text{Fqpol} f \circ m = f \left( \text{Frob}_{F_q[T][X]} \right) \circ m \).

3.6. Frobenius \( F_q[T] \)-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 \( F_q \)-algebra):

**Lemma 3.25.** Let \( M \) and \( N \) be two \( \mathcal{F} \)-modules. Let \( f : M \to N \) be an \( F_q \)-linear map. Assume that

\[
f(Tu) = Tf(u) \quad \text{for every } u \in M.
\]

Assume also that

\[
f(Fu) = Ff(u) \quad \text{for every } u \in M.
\]

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 \( \mathcal{F} \)-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 \((M, f)\), where \( M \) is an \( \mathbb{F}_q [T] \)-module, and where \( f : M \to M \) is an \( \mathbb{F}_q \)-linear map satisfying

\[
f (Tm) = T^n f (m) \quad \text{for every } m \in M.
\]

This map \( f \) is called the Frobenius map of the Frobenius \( \mathbb{F}_q [T] \)-module \((M, f)\). 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 \((M, f)\)”, leaving the Frobenius map \( f \) implicit; in this situation, the Frobenius map \( f \) will be denoted by \( f_M \).

(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 \( f_N \circ h = h \circ f_M \)).

(c) We let \( \text{FrobMod}_{\mathbb{F}_q[T]} \) 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 \( \text{FrobMod}_{\mathbb{F}_q[T]} \) is isomorphic to the category of \( \mathcal{F} \)-modules:

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

Recall that we are regarding the \( \mathbb{F}_q \)-algebra homomorphism \( \text{Finc}_T : \mathbb{F}_q [T] \to \mathcal{F} \) 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

\[
F \cdot m = f_M (m) \quad \text{for every } m \in M.
\]

(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 \( f \) 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, \((N, f)\) is a Frobenius \( \mathbb{F}_q [T] \)-module.

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

**Proof of Proposition 3.27 (a)** We let $\text{End} M$ 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

$$F \cdot m = f_M(m) \quad \text{for every } m \in M$$  \hspace{1cm} (44)

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

As usual, we abbreviate $f_M$ as $f$.

Let $t$ 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

$$t^n(m) = T^n \cdot m. \quad \hspace{1cm} (45)$$

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

For every $m \in M$, we have

$$(f \circ t)(m) = f \left( t \left( \frac{m}{T \cdot m} \right) \right) = f(T \cdot m) = T^q f(m) \quad \text{(by (43))}$$

$$= t^q(f(m)) \quad \text{(because (45) (applied to $q$ and $f(m)$ instead of $n$ and $m$)) shows that $t^q(f(m)) = T^q \cdot f(m) = T^{qq} f(m)$)}$$

$$= (t^q \circ f)(m).$$

Hence, $f \circ t = t^q \circ f$.

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

We have

$$(\Phi(f))(m) = f \cdot m \quad \text{for every } f \in \mathbb{F}_q[T] \text{ and } m \in M \quad \hspace{1cm} (46)$$

\[25\] 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 (43) 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.
Thus, the $F$-module structure on $M$ obtained from the map $Φ : F → \text{End} M$ extends the $F_q [T]$-module structure on $M$.

Furthermore, $Φ (F) (m) = f_M (m)$ for every $m ∈ M$. Thus, the $F$-module structure on $M$ obtained from the map $Φ : F → \text{End} M$ satisfies (44).

Hence, there exists at least one $F$-module structure on $M$ which extends the $F_q [T]$-module structure on $M$ and satisfies (44) (namely, the $F$-module structure on $M$ obtained from the map $Φ : F → \text{End} M$). This completes the proof of Proposition 3.27 (a).

(b) We need to show that $(N, f)$ is a Frobenius $F_q [T]$-module. In other words, we need to show that $N$ is an $F_q [T]$-module, that $f : N → N$ is an $F_q$-linear map, and that this map $f$ satisfies

$$f (Tm) = T^q f (m) \quad \text{for every } m ∈ N.$$  \hspace{1cm} (47)

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

So let $m ∈ N$. The definition of $f$ yields $f (m) = F m$ and $f (Tm) = F · Tm = F T m = T^q F m = T^q f (m)$. 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 $\text{FrobMod}_{F_q [T]} → \text{Mod} F$ first and then the functor $\text{Mod} F → \text{FrobMod}_{F_q [T]}$, then we get back to where we started. It is somewhat less obvious, but still easy, to prove that if we apply the functor $\text{Mod} F → \text{FrobMod}_{F_q [T]}$ first and then the functor $\text{FrobMod}_{F_q [T]} → \text{Mod} F$, then we get back to where we started.\hspace{1cm} (27) Thus, the functors $\text{FrobMod}_{F_q [T]} → \text{Mod} F$ and $\text{Mod} F → \text{FrobMod}_{F_q [T]}$ are mutually inverse. This proves Proposition 3.27 (c).

An ample supply of Frobenius $F_q [T]$-modules (and thus, $F$-module) is given by commutative $F_q [T]$-algebras and their Frobenius homomorphisms:

\hspace{1cm} (45). Hence, $(Φ (f)) (m) = T^n · m = f · m$. This proves (45).

\hspace{1cm} In order to prove this, it suffices to observe that an $F$-module structure on a given $F_q$-vector space is uniquely determined by the actions of $F$ and $T$ (because the $F_q$-algebra $F$ is generated by $F$ and $T$).
**Proposition 3.28.** (a) If $A$ is a commutative $\mathbb{F}_q[T]$-algebra, then $(A, \text{Frob}_A)$ 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 $(A, \text{Frob}_A)$ to $(B, \text{Frob}_B)$.

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

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

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

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

for every $m \in A$. Hence, $(A, \text{Frob}_A)$ 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 $F$-module structure on $A$ extends the $\mathbb{F}_q[T]$-module structure on $A$ and has the property that

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

is a consequence of Proposition 3.27 (a).)

Restricted Lie algebras (see, e.g., [12]) 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, $(A, \text{Frob}_A)$ 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 $F$-module structure on $A$. In the

---

28Proof. Let $m \in A$. Then, the definition of $\text{Frob}_A$ shows that $\text{Frob}_A(m) = m^q$ and $\text{Frob}_A(Tm) = (Tm)^q = T^q m^q = T^q \text{Frob}_A(m)$, qed.
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

$$F \cdot m = \text{Frob}_A(m) = m^q \quad \text{(by the definition of Frob}_A)$$

for every $m \in A$.

**Proposition 3.30.** 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 $\overline{\text{Fpol}}$ denote the map $\overline{\text{Fpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]$ considered as a map $\mathcal{F} \to \mathbb{F}_q[T][X]$ (this is well-defined because $\mathbb{F}_q[T][X]_{\text{lin}} \subseteq \mathbb{F}_q[T][X]$). Then, this map $\overline{\text{Fpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]$ is an $\mathcal{F}$-module homomorphism.

**Proof of Proposition 3.30** Proposition 3.24 shows that the map $\overline{\text{Fpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]_{\text{lin}}$ is an isomorphism of left $\mathbb{F}_q[T]$-modules. Thus, the map $\overline{\text{Fpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]$ (which differs from $\overline{\text{Fpol}} : \mathcal{F} \to \mathbb{F}_q[T][X]_{\text{lin}}$ only in its target) is also a homomorphism of left $\mathbb{F}_q[T]$-modules. In other words, $\overline{\text{Fpol}}(fu) = f\overline{\text{Fpol}}(u)$ for every $f \in \mathbb{F}_q[T]$ and $u \in \mathcal{F}$. Applying this to $f = T$, we obtain

$$\overline{\text{Fpol}}(Tu) = T\overline{\text{Fpol}}(u) \quad \text{for every } u \in \mathcal{F}. \quad (49)$$

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

$$\overline{\text{Fpol}}(F u) = \overline{\text{Fpol}}(F u) \quad \text{(by the definition of Fpol)}$$

$$= (\overline{\text{Fpol}}(F)) \circ (\overline{\text{Fpol}}(u))$$

$$= X^q \quad \text{(since Fpol is an $\mathbb{F}_q$-algebra homomorphism $\mathcal{F} \to (\mathbb{F}_q[T][X]_{\text{lin}}, +, \circ)$)}$$

$$= X^q \circ (\overline{\text{Fpol}}(u)) = (\overline{\text{Fpol}}(u))^q.$$

Comparing this with

$$\overline{\overline{\text{Fpol}}}(u) = F \cdot \overline{\text{Fpol}}(u) = \left( \overline{\text{Fpol}}(u) \right)^q \quad \text{(by (48), applied to } A = \mathbb{F}_q[T][X] \text{ and } m = \overline{\text{Fpol}}(u))$$

$$= (\overline{\text{Fpol}}(u))^q,$$
we obtain \( F_{q \text{pol}}(Fu) = FF_{q \text{pol}}(u) \). Let us now forget that we fixed \( u \). We thus have shown that

\[
F_{q \text{pol}}(Fu) = FF_{q \text{pol}}(u) \quad \text{for every } u \in \mathcal{F}.
\]  

(50)

Now, Lemma 3.25 (applied to \( M = \mathcal{F}, N = F_q[T][X] \) and \( f = F_{q \text{pol}} \)) shows that \( F_{q \text{pol}} \) is an \( \mathcal{F} \)-module homomorphism (because of (49) and (50)). This proves Proposition 3.30.

\[ \square \]

### 3.7. The Carlitz action

Now, let us recall the Carlitz polynomials \([M]\) defined in Definition 1.1. We can connect these polynomials to \( \mathcal{F} \) in the following way:\footnote{Recall that Carl is the \( F_q \)-algebra homomorphism \( F_q[T] \to \mathcal{F} \) sending \( T \) to \( F + T \).}

**Proposition 3.31.** Let \( A \) be a commutative \( F_q[T] \)-algebra. Thus, \( A \) becomes an \( \mathcal{F} \)-module (by Convention 3.29).

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

**Proof of Proposition 3.31.** We first claim that

\[
[T^n](a) = (F + T)^n a \quad \text{for every } n \in \mathbb{N} \text{ and } a \in A.
\]  

(51)

**Proof of (51):** We shall prove (51) by induction over \( n \):

*Induction base:* We have \([T^0] = X\), thus \([T^0](a) = X(a) = a\). Comparing this with \((F + T)^0 a = a\), we obtain \([T^0](a) = (F + T)^0 a\). In other words, (51) holds for \( n = 0 \). This completes the induction base.

*Induction step:* Fix a positive integer \( N \). Assume that (51) holds for \( n = N - 1 \). We now need to show that (51) holds for \( n = N \).

We have assumed that (51) holds for \( n = N - 1 \). In other words, we have

\[
[T^{N-1}](a) = (F + T)^{N-1} a \quad \text{for every } a \in A.
\]  

(52)

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

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

(53)
The recursive definition of \( [T^N] \) yields \( [T^N] = [T^{N-1}]^q + T [T^{N-1}] \). Hence,

\[
[T^N](a) = \left( [T^{N-1}]^q + T [T^{N-1}] \right)(a) = \left( [T^{N-1}](a) \right)^q + T [T^{N-1}](a)
\]

\[
= F \cdot [T^{N-1}](a) + T \cdot [T^{N-1}](a) = (F + T) [T^{N-1}](a)
\]

\[
= (F + T)(F + T)^{N-1} a = (F + T)^N a.
\]

Now, let us forget that we fixed \( a \). We thus have shown that \( [T^N](a) = (F + T)^N a \)
for every \( a \in A \). In other words, (51) holds for \( n = N \). This completes the induction step, and thus (51) 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

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

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

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

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

\[
\text{Carl } M = \sum_{n=0}^{k} a_n (F + T)^n.
\]
Hence,

\[(\text{Carl } M) \cdot a = \left( \sum_{n=0}^{k} a_n (F + T)^n \right) \cdot a = \sum_{n=0}^{k} a_n (F + T)^n a = \sum_{n=0}^{[T^n](a)} a_n (F + T)^n a \]

\[= \sum_{n=0}^{k} a_n \left[ T^n \right] (a) = \left( \sum_{n=0}^{k} a_n \left[ T^n \right] \right) (a) = [M] (a) .\]

This proves Proposition 3.31.

Corollary 3.32. Let \( M \in \mathbb{F}_q[T] \). Then, the homomorphism \( \mathbb{F}_q \text{pol} : \mathcal{F} \to \mathbb{F}_q[T] [X]_{q-\text{lin}} \) satisfies \( [M] = \mathbb{F}_q \text{pol} (\text{Carl } M) \).

Corollary 3.32 yields, in particular, that every \( M \in \mathbb{F}_q[T] \) satisfies \( [M] = \mathbb{F}_q \text{pol} (\text{Carl } M) \in \mathbb{F}_q \text{pol} \mathcal{F} \subseteq \mathbb{F}_q[T] [X]_{q-\text{lin}} \).

Proof of Corollary 3.32. Let \( M \in \mathbb{F}_q[T] \).

Consider the map \( \mathbb{F}_q \text{pol} : \mathcal{F} \to \mathbb{F}_q[T] [X] \) defined in Proposition 3.30. This map \( \mathbb{F}_q \text{pol} \) is an \( \mathcal{F} \)-module homomorphism (according to Proposition 3.30).

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

But the definition of \( \mathbb{F}_q \text{pol} \) shows that \( \mathbb{F}_q \text{pol} (\text{Carl } M) = \mathbb{F}_q \text{pol} (\text{Carl } M) \), so that

\[\mathbb{F}_q \text{pol} (\text{Carl } M) = \mathbb{F}_q \text{pol} \left( \frac{\text{Carl } M}{(\text{Carl } M) \cdot 1} \right) = \mathbb{F}_q \text{pol} \left( (\text{Carl } M) \cdot 1 \right) = \text{Carl } M \cdot \mathbb{F}_q \text{pol} (1) = \text{Carl } M \cdot X .\]

(54)

On the other hand, Proposition 3.31 (applied to \( A = \mathbb{F}_q[T] [X] \) and \( a = X \)) yields \( [M] (X) = (\text{Carl } M) \cdot X \). Comparing this with (54), we obtain \( \mathbb{F}_q \text{pol} (\text{Carl } M) = [M] (X) = [M] \). This proves Corollary 3.32.

3.8. “Fermat’s Little Theorem” for the Carlitz action

Let us first state a simple fact:
Lemma 3.33. 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 \( u \in A [X] \) be such that \( f u \in A [X]_{q-\text{lin}} \). Then, \( u \in A [X]_{q-\text{lin}} \).

Proof of Lemma 3.33. We have \( f u \in A [X]_{q-\text{lin}} \). In other words, the polynomial \( f u \in A [X] \) is a \( q \)-polynomial, that is, an \( A \)-linear combination of the monomials \( X^0, X^1, X^2, \ldots \). In other words, for every \( k \in \mathbb{N} \setminus \{q^0, q^1, q^2, \ldots\} \), we have

\[
\left( \text{the } X^k\text{-coefficient of } f u \right) = 0. \tag{55}
\]

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

\[
 f \cdot \left( \text{the } X^k\text{-coefficient of } u \right) = \left( \text{the } X^k\text{-coefficient of } f u \right) = 0
\]
(by (55)), and thus \( \left( \text{the } X^k\text{-coefficient of } u \right) = 0 \) (because \( f \neq 0 \), and because \( A \) is torsionfree as an \( \mathbb{F}_q [T] \)-module). In other words, the polynomial \( u \) is an \( A \)-linear combination of the monomials \( X^0, X^1, X^2, \ldots \). In other words, \( u \) is a \( q \)-polynomial; that is, \( u \in A [X]_{q-\text{lin}} \). This proves Lemma 3.33. \( \square \)

We now shall prove a crucial fact:

Proposition 3.34. Let \( \pi \) be a monic irreducible polynomial in \( \mathbb{F}_q [T] \). Then, there exists a unique \( u (\pi) \in \mathcal{F} \) such that \( \text{Carl } \pi = F^{\deg \pi} + \pi \cdot u (\pi) \). (The notation \( u (\pi) \) means that \( u \) depends on \( \pi \); it is not meant to imply that \( u (\pi) \) is a polynomial in \( \pi \).)

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

First proof of Proposition 3.34. 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 \( \pi (X) \in \mathbb{F}_q [T] [X] \) onto \( (\mathbb{F}_q [T] / \pi) [X] \). In other words, \( \overline{\pi} (X) \equiv X^{q^{\deg \pi}} \mod K \), where \( K \) is the kernel of the projection \( \mathbb{F}_q [T] [X] \to (\mathbb{F}_q [T] / \pi) [X] \). Since this kernel \( K \) is simply \( \pi \mathbb{F}_q [T] [X] \), this rewrites as follows: \( \overline{\pi} (X) \equiv X^{q^{\deg \pi}} \mod \pi \mathbb{F}_q [T] [X] \).

Thus, \( \overline{\pi} = \overline{\pi} (X) \equiv X^{q^{\deg \pi}} \mod \pi \mathbb{F}_q [T] [X] \). In other words, \( \pi \mid \overline{\pi} - X^{q^{\deg \pi}} \) in the ring \( \mathbb{F}_q [T] [X] \). Hence, \( \frac{1}{\pi} \left( \overline{\pi} - X^{q^{\deg \pi}} \right) \) 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 \( u \).
We have

\[ [\pi] = \text{Fqpol} \left( \text{Carl} \pi \right) \]  

(by Corollary 3.32, applied to \( M = \pi \))

\[ \in \text{Carl} \mathcal{F} \subseteq \mathbb{F}_q[ T ][X]_{q-\text{lin}}. \]

But \( u = \frac{1}{\pi} \left( [\pi] - X^{\deg \pi} \right) \), so that \( \pi u = [\pi] - X^{\deg \pi} \in \mathbb{F}_q[ T ][X]_{q-\text{lin}} \) (since both \([\pi]\) and \(X^{\deg \pi}\) belong to \(\mathbb{F}_q[ T ][X]_{q-\text{lin}}\)). Therefore, \( u \in \mathbb{F}_q[ T ][X]_{q-\text{lin}} \) (by Lemma 3.33, applied to \( A = \mathbb{F}_q[ T ] \) and \( f = \pi \)).

Theorem 3.13 (c) (applied to \( j = 0 \) and \( i = \deg \pi \)) yields \( \text{Fqpol} \left( T^0 \mathbb{F}^{\deg \pi} \right) = \sum_{\ell = 1}^{\deg \pi} X^{q^{\deg \pi}} \), so that \( X^{q^{\deg \pi}} = \text{Fqpol} \left( T^0 \mathbb{F}^{\deg \pi} \right) = \text{Fqpol} \left( \mathbb{F}^{\deg \pi} \right). \)

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

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

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

\[ \text{Fqpol} (\pi \tilde{u}) = \pi \text{Fqpol} (\tilde{u}) = \pi u = \frac{[\pi]}{\text{Fqpol} (\text{Carl} \pi )} - \frac{X^{q^{\deg \pi}}}{\text{Fqpol} (\mathbb{F}^{\deg \pi})} \]

(by Corollary 3.32, applied to \( M = \pi \))

\[ = \text{Fqpol} (\text{Carl} \pi ) - \text{Fqpol} (\mathbb{F}^{\deg \pi}) = \text{Fqpol} (\text{Carl} \pi - \mathbb{F}^{\deg \pi}) \]

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

Hence, there exists at least one \( u (\pi) \in \mathcal{F} \) such that \( \pi \cdot u (\pi) = \text{Carl} \pi - \mathbb{F}^{\deg \pi} \) (namely, \( u (\pi) = \tilde{u} \)). 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 \( \text{Carl} \pi = \mathbb{F}^{\deg \pi} + \pi \cdot u (\pi) \). This proves Proposition 3.34.

We shall soon give another proof of Proposition 3.34, which does not rely on Carlitz polynomials.

[...]  
XTODO: Conclude torsionfreeness in two ways.  
XTODO: \pi-theorem.  
XTODO: examples.  
[...]
4. Speculations

4.1. So what is $\Lambda_{\text{Carl}}$?

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). This suggests that I shouldn’t be looking at the representing object of the functor $W_N : \text{CRing}_{\mathbb{F}_q[T]} \rightarrow \text{CRing}_{\mathbb{F}_q[T]}$, but at the representing object of the functor $W_N : \mathcal{F}\text{-Mod} \rightarrow \mathcal{F}\text{-Mod}$, or at least that the latter is more fundamental than the former. To begin with, it’s smaller.

A representing object of a functor $\mathcal{F}\text{-Mod} \rightarrow \mathcal{F}\text{-Mod}$ is the same as an $\mathcal{F}$-$\mathcal{F}$-bimodule. The $\mathcal{F}$-$\mathcal{F}$-bimodule which represents the functor $W_N : \mathcal{F}\text{-Mod} \rightarrow \mathcal{F}\text{-Mod}$ 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 $p_P = \sum_{D \mid P} D \left[ \frac{P}{D} \right] (x_D)$ for every $P \in N$.

(The intuition is that $x_P$ are analogues of the “Witt vector coordinates” of $\Lambda$ 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 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 $\xi_i$ to mean $\sum_i [P] (\xi_i)$, then all these polynomials would be linearly dependent over $\mathcal{F}$ simply because

$$\sum_i [P] (\xi_i) = [P] \left( \sum_i \xi_i \right) = (\text{Carl} (P)) \left( \sum_i \xi_i \right).$$

The absence of multiplicative structure makes it hard to even guess what “elementary symmetric functions” or “complete homogeneous symmetric func-

---

30 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?

31 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 $\text{Hom}_{\mathcal{F}\text{-Mod}} (\lambda M, -) : \lambda \text{Mod} \rightarrow \psi \text{Mod}$.

32 These are the symmetric functions $w_n$ in [6, Exercise 2.79]. Their name stems from their relation to the Witt vectors; from a combinatorial viewpoint, they are a rather exotic family.
Function-field analogue for symmetric functions?  

February 14, 2016

tions” 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. 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 $x_1 f = f x_1$ 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, $p_T = \frac{[T]}{(F + T)x_1} + T x_T = (F + T) x_1 + T x_T$. 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

$$
((F + T) x_1 + T x_T) T = T ((F + T) x_1 + T x_T).
$$

Since

$$
((F + T) x_1 + T x_T) T = (F + T) x_1 T + T x_T T = T (T^{q-1} F + T) x_1 + T x_T T = T (T^{q-1} F + T) x_1 + x_T T,
$$

this rewrites as $T (T^{q-1} F + T) x_1 + x_T T = T ((F + T) x_1 + T x_T)$. 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 $(T^{q-1} F + T) x_1 + x_T T = (F + T) x_1 + T x_T$. Hence, $x_T T = (F + T) x_1 + T x_T - (T^{q-1} F + T) x_1$. This simplifies to

$$
x_T T = T x_T - (T^{q-1} - 1) F x_1.
$$

\[33\text{Another suggestion by James Borger.}\]
Let’s do \( x_T F \). Apply \( p_T f = f p_T \) to \( f = F \), and substitute \( p_T = (F + T) x_1 + T x_T \) again; the result is

\[
((F + T) x_1 + T x_T) F = F ((F + T) x_1 + T x_T) .
\]

Subtraction of \( (F + T) x_1 F \) turns this into

\[
T x_T F = F ( (F + T) x_1 + T x_T ) - (F + T) x_1 F = F F x_1 + \frac{T^q F}{T^q} x_1 + \frac{T^q}{T^q} x_T F - F x_1 F - T x_1 F = T^{q-1} F x_1 + T^{q-1} F x_T - x_1 F.
\]

Cancelling \( T \), we obtain

\[
x_T F = T^{q-1} F x_1 + T^{q-1} F x_T - \frac{x_1 F}{F x_1} T^{q-1} F x_1 + T^{q-1} F x_T - F x_1.
\]

This simplifies to \( x_T F = (T^{q-1} - 1) F x_1 + T^{q-1} F x_T \).

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, \( p_\pi = (\text{Carl } \pi) x_1 + \pi x_\pi \) satisfies \( p_\pi f = f p_\pi \) for every \( f \in \mathcal{F} \). Applying this to \( f = T \) and substituting \( p_\pi = (\text{Carl } \pi) x_1 + \pi x_\pi \), we get

\[
((\text{Carl } \pi) x_1 + \pi x_\pi) T = T ((\text{Carl } \pi) x_1 + \pi x_\pi).
\]

Subtracting \( (\text{Carl } \pi) x_1 T \) from here, we get

\[
\pi x_\pi T = T ((\text{Carl } \pi) x_1 + \pi x_\pi) - (\text{Carl } \pi) x_1 T = T (\text{Carl } \pi) x_1 + T \pi x_\pi - (\text{Carl } \pi) x_1 T = T (\text{Carl } \pi) x_1 + T \pi x_\pi - (\text{Carl } \pi) T x_1 = T \pi x_\pi + [T, \text{Carl } \pi] x_1 .
\]

Thus, \([T, \text{Carl } \pi]\) must lie in \( \pi \mathcal{F} \), and an explicit formula for the quotient would be very useful. Well, the fact that \([T, \text{Carl } \pi]\) 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 \( \partial_T (\pi) \) denote the (unique) \( f \in \mathcal{F} \) satisfying \([T, \text{Carl } \pi] = \pi f\) for \( \pi \) irreducible monic. In more elementary (and commutative) terms, \( \partial_T (\pi) = \frac{T [\pi] (X) - [\pi] (TX)}{\pi} \). Now,

\[
\pi x_\pi T = \frac{T \pi x_\pi}{\pi T} + \frac{T, \text{Carl } \pi}{\pi \partial_T (\pi)} x_1 = \pi T x_\pi + \pi \partial_T (\pi) x_1 .
\]
Cancelling \( \pi \), we obtain

\[
\begin{align*}
x_\pi T &= T x_\pi + \partial_T (\pi) x_1 \\
\text{The question is: Do we get } x_\pi F \text{ explicitly using } \partial_T (\pi), \text{ or will we have to introduce another new operator? Apply } p_\pi f = f p_\pi \text{ to } f = F \text{ and substitute } p_\pi = (\text{Carl } \pi) x_1 + \pi x_\pi. \text{ The result is }
\end{align*}
\]

\[
((\text{Carl } \pi) x_1 + \pi x_\pi) F = F ((\text{Carl } \pi) x_1 + \pi x_\pi).
\]

Subtracting \((\text{Carl } \pi) x_1 F\) from here, we get

\[
\begin{align*}
\pi x_\pi F &= F ((\text{Carl } \pi) x_1 + \pi x_\pi) - (\text{Carl } \pi) x_1 F \\
&= F (\text{Carl } \pi) x_1 + F \pi x_\pi - (\text{Carl } \pi) x_1 F \\
&= F (\text{Carl } \pi) x_1 + F \pi x_\pi - (\text{Carl } \pi) F x_1 \\
&= F \pi x_\pi + [F, \text{Carl } \pi] x_1.
\end{align*}
\]

Oh, but \([F, \text{Carl } \pi] + [T, \text{Carl } \pi] = \left[ F + T, \text{Carl } \pi \right] = [\text{Carl } T, \text{Carl } \pi] = \text{Carl } [T, \pi] = 0\), so that \([F, \text{Carl } \pi] = -[T, \text{Carl } \pi] = -\pi \partial_T (\pi)\). Hence,

\[
\begin{align*}
\pi x_\pi F &= F \pi x_\pi + [F, \text{Carl } \pi] x_1 \\
&= F \pi x_\pi - \pi \partial_T (\pi) x_1 = \pi^q F x_\pi - \pi \partial_T (\pi) x_1.
\end{align*}
\]

Cancelling \(\pi\), we obtain

\[
\begin{align*}
x_\pi F &= \pi^{q-1} F x_\pi - \partial_T (\pi) x_1.
\end{align*}
\]

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

\[
\log_C (SX) = \sum_{N \in \mathbb{F}_q[T]_+} (-1)^{\deg N} S^{q^{\deg N}} \frac{[N]}{N} (X). \quad (56)
\]

(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 \((T^{q^j} - T) (T^{q^j-1} - T) \ldots (T^{q^1} - T) \in \mathbb{F}_q[T]\).
Then, \( \log_C \in \mathbb{F}_q ( T ) [[X]] \) is defined by

\[
\log_C ( X ) = \sum_{j \in \mathbb{N}} (-1)^j \frac{X^{q^j}}{L_j} .
\]  

(57)

It should be noticed that it is possible to specialize \( S \) to 1 in (56), 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 straight-forward 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 \( e_1, e_2, \ldots, e_n \) be \( n \) elements of \( A \). Then,

\[
\sum_{(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_q^n} P ( \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n ) = 0.
\]

**Proof of Proposition 5.2 (sketch).** We can WLOG assume that \( P = X^k \) for some \( k \in \{0, 1, \ldots, q^n - 2\} \). Assume this and consider this \( k \). Since \( k < q^n - 1 \), we can write \( k \) in the form \( k = k_{n-1}q^{n-1} + k_{n-2}q^{n-2} + \ldots + k_0q^0 \) with \( k_i < q \) and with \( k_0 + k_1 + \ldots + k_{n-1} \leq n ( q - 1 ) - 1 \). Thus,

\[
P = X^k = X^{k_{n-1}q^{n-1} + k_{n-2}q^{n-2} + \ldots + k_0q^0} = \prod_{i=0}^{n-1} X^{k_i} = \prod_{i=0}^{n-1} (X^{q^i})^{k_i}.
\]

Hence,

\[
\sum_{(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_q^n} P ( \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n )
\]

\[
= \sum_{(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_q^n} \prod_{i=0}^{n-1} \left( \frac{(\lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n)^{q^i}}{=\lambda_1 e_1^{q^i} + \lambda_2 e_2^{q^i} + \ldots + \lambda_n e_n^{q^i} (since we are over \mathbb{F}_q)} \right)^{k_i}
\]

\[
= \sum_{(\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_q^n} \prod_{i=0}^{n-1} \left( \lambda_1^{e_1^{q^i}} e_1^{q^i} + \lambda_2^{e_2^{q^i}} e_2^{q^i} + \ldots + \lambda_n^{e_n^{q^i}} e_n^{q^i} \right)^{k_i}.
\]
Now, consider the product \( \prod_{i=0}^{n-1} \left( \lambda_1 e_1^q + \lambda_2 e_2^q + ... + \lambda_n e_n^q \right)^{k_i} \) as a polynomial (over \( A \)) in the variables \( \lambda_1, \lambda_2, ..., \lambda_n \). 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

\[
W' = \sum_{w \in V} \left( \sum_{v \in V; v \neq w} (X + w)' \cdot (X + v) \right) = \sum_{w \in V} \prod_{v \in V; v \neq w} (X + v) = \prod_{v \in V} (X + v)
\]

\[
= \left( \prod_{v \in V} (X + v) \right) \cdot \left( \sum_{w \in V} \frac{1}{X + w} \right).
\]

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

$$\sum_{w \in V} \frac{1}{t + w} = \prod_{v \in V} \frac{1}{t + v} \cdot W'(t) = \prod_{v \in V} \frac{1}{t + v} \cdot \left( \prod_{v \in V \setminus 0} v \right) = \left( \prod_{v \in V} \frac{1}{t + v} \right) \cdot \left( \prod_{v \in V \setminus 0} v \right).$$

Rename the index $w$ as $v$ and obtain the claim of Proposition 5.3.

**Proof of Theorem 5.1 (sketched).** By (57), 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

$$\frac{X^{q^m}}{L_m} = \sum_{\substack{N \in \mathbb{F}_q[T] \mid ; \\
\deg N = m}} \frac{[N](X)}{N}. \tag{58}$$

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 $\epsilon_C$ denoting the Carlitz exponential, the power series $\epsilon_C(Y \log_C X) \in \mathbb{F}_q(T)[[X,Y]]$ is a $q$-power series, i.e., its coefficient before $X^a Y^b$ can only be nonzero if both $a$ and $b$ are powers of $q$. Now, for every $j \in \mathbb{N}$, define $E_j(Y)$ to be the coefficient of this power series $\epsilon_C(Y \log_C X)$, **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

\[
\frac{[M](X)}{M} = \sum_{j \in \mathbb{N}} \frac{E_j(M)}{M} X^{q^j} = \sum_{j \in \mathbb{N}} E_j(M) X^{q^j} = \sum_{j=0}^{\deg M} \frac{E_j(M)}{M} X^{q^j}
\]

(since \(E_j(M) = 0\) whenever \(\deg M < j\))

\[
= \sum_{j=0}^{\deg M - 1} \frac{E_j(M)}{M} X^{q^j} + \frac{E_{\deg M}(M)}{M} X^{q^{\deg M}}
\]

(since \(E_j(M) = 1\) whenever \(\deg M = j\))

\[
= \sum_{j=0}^{\deg M - 1} \frac{E_j(M)}{M} X^{q^j} + \frac{1}{M} X^{q^{\deg M}}
\]  

(59)

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 \(\deg(E_j) = q^j\)). 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 \(j \in \{0, 1, \ldots, m - 1\}\), 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

\[
\sum_{(\lambda_1, \lambda_2, \ldots, \lambda_m) \in \mathbb{F}_q} \frac{E_j(\lambda_1 T^0 + \lambda_2 T^1 + \ldots + \lambda_m T^{m-1} + T^m)}{\lambda_1 T^0 + \lambda_2 T^1 + \ldots + \lambda_m T^{m-1} + T^m} = 0
\]

(since \(j < m\) and thus \(q^j - 1 < q^m - 1\)). Since the sums of the form \(\lambda_1 T^0 + \lambda_2 T^1 + \ldots + \lambda_m T^{m-1} + T^m\) with \((\lambda_1, \lambda_2, \ldots, \lambda_m) \in \mathbb{F}_q\) are precisely the monic polynomials in \(\mathbb{F}_q[T]\) with degree \(m\) (each appearing exactly once), this rewrites as

\[
\sum_{N \in \mathbb{F}_q[T]_+; \deg N = m} \frac{E_j(N)}{N} = 0 \quad \text{for every } j \in \{0, 1, \ldots, m - 1\}. \tag{60}
\]
Now,
\[
\sum_{N \in \mathbb{F}_q[T] \mid \deg N = m} \frac{[N](X)}{N} \cdot \left( \sum_{j=0}^{\deg (N-1)} \frac{E_j(N)}{N} X^{q^j} + \frac{1}{N} X^{q^{\deg N}} \right)
\]

(here we applied (59) to \( M = N \))
\[
= \sum_{j=0}^{m-1} \left( \sum_{N \in \mathbb{F}_q[T] \mid \deg N = m} \frac{E_j(N)}{N} X^{q^j} \right) + \sum_{N \in \mathbb{F}_q[T] \mid \deg N = m} \frac{1}{N} X^{q^m}
\]

(by (60))
\[
\sum_{N \in \mathbb{F}_q[T] \mid \deg N = m} \frac{1}{N} X^{q^m} = \sum_{v \in \mathbb{F}_q[T] \mid \deg v = m} \frac{1}{T^m + v} X^{q^m}
\]

(since the monic polynomials in \( \mathbb{F}_q[T] \) of degree \( m \) are exactly the sums of the form \( T^m + v \) with \( v \) being a polynomial in \( \mathbb{F}_q[T] \) of degree \( < m \))
\[
= \left( \prod_{v \in \mathbb{F}_q[T] \mid \deg v < m; v \neq 0} \frac{1}{T^m + v} \right) \cdot \left( \prod_{v \in \mathbb{F}_q[T] \mid \deg v < m; v \neq 0} v \right) X^{q^m}
\]

(by Proposition 5.3, applied to \( L = \mathbb{F}_q(T) \), \( t = T^m \) and \( V = \{ v \in \mathbb{F}_q[T] \mid \deg v < m \} \))
\[
= \left( \prod_{N \in \mathbb{F}_q[T] \mid \deg N = m} \frac{1}{N} \right) \cdot \left( \prod_{v \in \mathbb{F}_q[T] \mid \deg v < m; v \neq 0} v \right) X^{q^m} = \frac{X^{q^m}}{L_m}.
\]

(This is relatively straightforward to prove using standard results on finite fields)

This proves (58) and thus Theorem 5.1.

I hope there is a better proof.
References


http://arxiv.org/abs/math/0407227v1

http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/carlitz.pdf


http://www.math.uni-bonn.de/people/dyckerho/notes.pdf

http://www.math.umn.edu/~reiner/Classes/HopfComb.pdf


http://arxiv.org/abs/0804.3888v1


http://www.math.nagoya-u.ac.jp/~larsh/papers/s03/wittsurvey.pdf


71
http://www.emis.de/journals/SLC/opapers/s28macdonald.html

http://www.ams.org/journals/tran/1933-035-03/
S0002-9947-1933-1501703-0/

http://www.ams.org/journals/tran/1934-036-02/
S0002-9947-1934-1501741-9/

http://www.math.harvard.edu/~rabinoff/misc/witt.pdf