Do the symmetric functions have a function-field analogue?

Darij Grinberg

draft, version 1.2, November 8, 2015

Contents

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

2. The Carlitz-Witt suite
   2.1. The classical ghost-Witt equivalence theorem
   2.2. Classical Witt vectors
   2.3. The Carlitz ghost-Witt equivalence theorem
   2.4. Carlitz-Witt vectors
   2.5. $\mathcal{F}$-modules

3. Speculations
   3.1. So what is $\Lambda_{\text{Carl}}$?
   3.2. Some computations in $\Lambda_{\mathcal{F}}$

4. The logarithm series

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 reinterpreted (i.e., counting sets becomes counting $\mathbb{F}_q$-vector spaces). This naturally leads to Hall algebras, studied e.g. in [7]. 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 \( \mathbb{F}_q \)-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 ([1, §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 \((h_\lambda)_{\lambda \in \text{Par}}\), the elementary symmetric functions \((e_\lambda)_{\lambda \in \text{Par}}\) and the Schur functions \((s_\lambda)_{\lambda \in \text{Par}}\). 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 \((p_\lambda)_{\lambda \in \text{Par}}\) (which do not even form a basis, although with functoriality they are sufficient for many computational purposes) and of a basis \((w_\lambda)_{\lambda \in \text{Par}}\) defined in [8, 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 2.25), 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 [2].

This report is built as follows: In Section 1, we introduce notations and present basic definitions. In Section 2, we remind the reader of a construction (actually, one of many constructions) of the Witt vectors, and then introduce the \( \mathbb{F}_q \)-analogue of this construction. In Section 3, we speculate on how this analogue could lead to an \( \mathbb{F}_q \)-analogue of \( \Lambda \). Finally, in Section 4, 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 ([9] or [11]) and a bit about Carlitz polynomials ([2]). Symmetric functions will only be really used in Section 3.
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 [9]).

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

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 $n = 0$.

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

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 $M \in R[\mathbb{T}]_+$ is a monic polynomial, then a sum like $\sum_{D \mid M} a_D$ is to be read as a sum over all monic divisors of $M$, not over all arbitrary divisors of $M$. Moreover, if $R$ is a field and $M \in R[\mathbb{T}]_+$ 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 $R[\mathbb{T}]_+$ and $f$ is any polynomial in $R[\mathbb{T}]_+$ (for a field $R$), then $v_\pi(f)$ means the largest nonnegative integer $m$ satisfying $\pi^m \mid f$; this is set to be $+\infty$ if $f = 0$.

1.2. Algebra

We denote by $\text{CRing}$ 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 [3, §2] and [6, Chapter 7] for studies of this ring $\Lambda$.)

1.3. Carlitz polynomials

In discussing Carlitz polynomials, I use the notations from Keith Conrad’s [2] (but I’m using blackboard bold instead of boldface for labelling rings; so what

\[1\text{This is a well-known analogy, often taught in number theory classes.}\]
Conrad calls $\mathbb{F}_p$ will be called $\mathbb{F}_p$ here, etc.). In particular, let $q$ be a prime power. For any $M \in \mathbb{F}_q[T]$, the Carlitz polynomial in $\mathbb{F}_q[T][X]$ corresponding to the polynomial $M$ will be denoted by $[M]$. Let us recall how it is defined:

**Definition 1.1.** For every $n \in \mathbb{N}$, define a polynomial $[T^n] \in \mathbb{F}_q[T][X]$ recursively, by setting $[T^0] = X$ 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 $M = a_0T^0 + a_1T^1 + \cdots + a_kT^k$. (In other words, we define a polynomial $[M] \in \mathbb{F}_q[T][X]$ in such a way that $[M]$ depends $\mathbb{F}_q$-linearly on $M$, and that our new definition of $[M]$ does not conflict with our existing definition of $[T^n]$ for $n \in \mathbb{N}$.) We call $[M]$ the **Carlitz polynomial** corresponding to $M$.

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

Notice that

$$
[M](X) \equiv X^{\deg M} \pmod{\pi} \quad \text{for any monic irreducible } \pi \in \mathbb{F}_q[T]. \quad (1)
$$

(This is proven in [2] 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 $\mathfrak{N}_q[T]_+$ (whose partial order is the divisibility relation). In other words, it is the function $\mu : \mathfrak{N}_q[T]_+ \rightarrow \{-1, 0, 1\}$ defined by

$$
\mu(M) = \begin{cases}
(-1)^{|\mathfrak{P} M|}, & \text{if } M \text{ is squarefree;} \\
0, & \text{if } M \text{ is not squarefree}
\end{cases}
$$

for all $M \in \mathfrak{N}_q[T]_+$.

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 [2]):

1. The first analogue is the function $\varphi_C : \mathfrak{N}_q[T]_+ \rightarrow \mathfrak{N}_q[T]_+$ defined by

$$
\varphi_C(M) = M \prod_{\pi \in \mathfrak{P} M} \left( 1 - \frac{1}{\pi} \right) = \sum_D \frac{\mu(D) M}{D} \quad \text{for all } M \in \mathfrak{N}_q[T]_+.
$$


Some properties of this $\varphi_C$ are shown in [2, 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

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

This function appears in [2, 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:

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

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

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

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

- **Assertion C:** Every $n \in N$ and every $p \in PF$ satisfies
  $$\varphi_p(b_{n/p}) \equiv b_n \mod p^{\varphi_p(n)} A.$$

- **Assertion D:** There exists a family $(x_n)_{n \in N} \in A^N$ of elements of $A$ such that
  $$b_n = \sum_{d|n} d x_{n/d} \text{ for every } n \in N.$$

- **Assertion E:** There exists a family $(y_n)_{n \in N} \in A^N$ of elements of $A$ such that
  $$b_n = \sum_{d|n} d \varphi_{n/d}(y_d) \text{ for every } n \in N.$$
Assertion $\mathcal{F}$: Every $n \in N$ satisfies
\[ \sum_{d|n} \mu(d) \varphi_d\left( b_{n/d}\right) \in nA. \]

Assertion $\mathcal{G}$: Every $n \in N$ satisfies
\[ \sum_{d|n} \phi(d) \varphi_d\left( b_{n/d}\right) \in nA. \]

Assertion $\mathcal{H}$: Every $n \in N$ satisfies
\[ \sum_{i=1}^{n} \varphi_{n/gcd(i,n)}\left( b_{gcd(i,n)}\right) \in nA. \]

Assertion $\mathcal{J}$: There exists a ring homomorphism from the ring $\Lambda$ 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 $(b_n)_{n \in N} \in A^N$ which satisfy the equivalent assertions $\mathcal{C}, \mathcal{D}, \mathcal{E}, \mathcal{F}, \mathcal{G}, \mathcal{H},$ and $\mathcal{J}$ of Theorem 2.1 will be called ghost-Witt vectors (over $A$).

There are many variations on Theorem 2.1. An easy way to get a more intuitive particular case of Theorem 2.1 is to set $\varphi_n = \text{id}_A$ for all $n \in N$, after which Assumptions 1 and 3 become tautologies. However, Assumption 2 is not guaranteed to hold in this setting; but it holds in $\mathbb{Z}$, and more generally in binomial rings, and in some non-torsionfree rings as well. Unfortunately, this case is in some sense too simple: it is too weak to yield the basic properties of Witt vectors (such as the well-definedness of addition, multiplication, Frobenius and Verschiebung). Instead one needs the case when $A$ is a polynomial ring $\mathbb{Z}[\Xi]$ 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 $\mathcal{C} \iff \mathcal{D}$.

The proof of Theorem 2.1 is everywhere and nowhere: it is a straightforward generalization of arguments easily found in literature, but I haven’t seen it explicit in this generality anywhere. I’ve written it up (save for Assertion $\mathcal{J}$) in [11, Theorem 11]. Also, the proof of the whole Theorem 2.1 in the case when $N = N_+$ appears in [8, 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 $\mathcal{C} \iff \mathcal{D}$ needs Assumptions 1 and 2 but not 3 (unsurprisingly), and the equivalence $\mathcal{C} \iff \mathcal{E} \iff \mathcal{F} \iff \mathcal{G} \iff \mathcal{H}$ needs only Assumption 3 (not 1 and 2; actually, $A$ can be any additive group rather than a ring for this equivalence). The equivalence $\mathcal{D} \iff \mathcal{J}$ needs nothing. This is all old news.
2.2. Classical Witt vectors

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

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

$$w_N \left((x_n)_{n \in N}\right) = \left(\sum d \frac{dx^N}{d} \right)_{n \in N}$$

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 $\phi_n (P) = P (\Xi^n)$:

**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 $(\delta_n, 1)_{n \in N}$ (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 [9, 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 $\phi_n$ satisfying Assumptions 1, 2 and 3 over any commutative ring $A$), but rather requires a detour via $\mathbb{Z}[\Xi]$.

The following theorem ([9, 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” [9, 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 $n, m \in N$ 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

$$(w_N \circ \varphi)(a) = (\sigma_n(a))_{n \in N}$$

for every $a \in A$.

Now let us describe some known functorial operations on $W_N(A)$. I will follow [9] 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 [9, Theorem 5.7, Proposition 5.9 and Proposition 5.12].

Here is the definition of Verschiebung ([9, 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

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

for every $n \in N$. 

---

8
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 \textit{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 \textit{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, $V_m((x_n)_{n \in N}) = \left(\begin{array}{ll} x_{n \div m}, & \text{if } m \mid n; \\ 0, & \text{if } m \nmid n \end{array}\right)_{n \in N}$ 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\textsuperscript{2} ([9 Corollary 6.3]):

\textbf{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, $W_N(w_n) \circ AH = f_n$.

\section*{2.3. The Carlitz ghost-Witt equivalence theorem}

Now, let us move to the Carlitz case.

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

\textbf{Definition 2.11.} A \textit{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 $N$.

\textsuperscript{2}This is something Hazewinkel, in [11 §16.45], calls Artin-Hasse exponential. I am not sure if I completely understand its relation to the usual Artin-Hasse exponential...
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

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

Assertion $D_1$: There exists a family $(x_P)_{P \in N} \in A^N$ of elements of $A$ such that

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

Assertion $D_2$: There exists a family $(\tilde{x}_P)_{P \in N} \in A^N$ of elements of $A$ such that

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

Assertion $E_1$: There exists a family $(y_P)_{P \in N} \in A^N$ of elements of $A$ such that

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

Assertion $F_1$: Every $P \in N$ satisfies

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

Assertion $G_1$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \varphi_{\mathcal{C}(D)} \varphi_D (b_P / D) \in PA.$$  

Assertion $G_2$: Every $P \in N$ satisfies

$$\sum_{D \mid P} \varphi_{D} (b_P / D) \in PA.$$
For this Theorem 2.12 to be a complete analogue of Theorem 2.1, two assertions are missing: $\mathcal{H}$ and $\mathcal{J}$. Finding an analogue of $\mathcal{J}$ requires finding an analogue of $\Lambda$, which is the question that I have started this report with; approaches to it will be discussed in Section 3. Two other assertions ($\mathcal{D}$ and $\mathcal{G}$) have two analogues each due. However, Assertion $G_2$ is clearly equivalent to Assertion $F_1$ because of $\varphi(M) \equiv \mu(M) \mod p$ 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 $D_1 \iff C_1 \iff D_2$, $C_1 \implies F_1 \implies E_1 \iff C_1$, $F_1 \iff G_2$ 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 $\left( b_n \right)_{n \in \mathbb{N}} \in A$ 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 $A \rightarrow A$, $a \mapsto a^q$.

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 $F : A \rightarrow A$ which satisfies

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

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.

---

11
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 over $N$). The **Carlitz $N$-ghost map** $w_N : A^N \to A^N$ is the map defined by

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

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 2.12 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.

---

3Non-rhetorical question. Please let me know! (darijgrinberg[at]gmail.com)

4I’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.
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 $(0)_{n \in N}$.

The unity of the $\mathbb{F}_q[T]$-algebra $W_N(A)$ is not as simple as it was in Theorem 2.18.

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

$$\tilde{w}_N((x_p)_{p \in N}) = \left(\sum_{D|p} D x_p^{\deg(p/D)}\right)_{p \in N} \quad \text{for all } (x_p)_{p \in N} \in A^N.$$ 

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

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 $\varphi : A \to W_N (A)$ satisfying

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

A similar result holds for $\tilde{W}_N$ and $\tilde{w}_N$.

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 $f_M : W_N \to W_N$ 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

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

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

(b) This natural transformation $f_M$ is actually a natural transformation $W_N \to W_N$ of $\mathbb{F}_q [T]$-algebra-valued functors as well. That is, $f_M : W_N (A) \to W_N (A)$ is an $\mathbb{F}_q [T]$-algebra homomorphism for every commutative $\mathbb{F}_q [T]$-algebra $A$. (Here, again, $f_M$ 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 $P \in \mathbb{F}_q [T]_+$ 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 $f_\pi (x) \equiv [\pi] (x) \mod \pi W_N (A)$ (in $W_N (A)$) for every commutative $\mathbb{F}_q [T]$-algebra $A$ and every $x \in W_N (A)$. 

14
A Verschiebung exists too:

**Theorem 2.24.** Let \( N \) be a \( q \)-nest.

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

\[
w_N (\mathbf{V}_M (x)) = \begin{cases} M \cdot \left( \frac{P}{M} \right) \text{-th coordinate of } w_N (x) & \text{if } M \mid P; \\ 0 & \text{if } M \nmid P \end{cases},
\]

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

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

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

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

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

**Theorem 2.25.** Let \( N \) be a \( q \)-nest. Assume that \( PQ \in N \) for all \( P \in N \) and \( Q \in \mathbb{N} \).

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

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

(where \( w_N \) this time stands for the natural transformation \( w_N \) evaluated at the \( \mathbb{F}_q [T] \)-algebra \( W_N (A) \); thus, \( w_N (\mathbf{AH}(x)) \) 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, \( W_N (w_P) \circ \mathbf{AH} = f_P \).

### 2.5. \( \mathcal{F} \)-modules

The classical \( N \)-Witt vector functor for \( N \subseteq \mathbb{N}_+ \) being a nest is a functor \( \mathbb{CRing} \to \mathbb{CRing} \), and I don’t see how to extend it to any broader category than \( \mathbb{CRing} \). 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 \( \mathbb{F}_q \langle F, T \mid FT = T^q F \rangle \). This \( \mathcal{F} \) can be considered as a skew polynomial ring \( \mathbb{F}_q [T] [F; \text{Frob}] \) 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 \( \mathbb{F}_q [T] \to \mathcal{F} \) and \( \mathbb{F}_q [F] \to \mathcal{F} \), which make \( \mathcal{F} \) into a left \( \mathbb{F}_q [T] \)-module, a right \( \mathbb{F}_q [T] \)-module, a left \( \mathbb{F}_q [F] \)-module, and a right \( \mathbb{F}_q [F] \)-module. The left \( \mathbb{F}_q [T] \)-module structure on \( \mathcal{F} \) is probably the most useful one.

- As left \( \mathbb{F}_q [T] \)-module, \( \mathcal{F} \) is free with basis \( (F^i)_{i \geq 0} \) and thus torsionfree (this will be useful).
- As right \( \mathbb{F}_q [T] \)-module, \( \mathcal{F} \) is free with basis \( (T^jF^i)_{i \geq 0, 0 \leq j < q^i} \).
- As right \( \mathbb{F}_q [F] \)-module, \( \mathcal{F} \) is free with basis \( (T^j)_{j \geq 0} \).
- As left \( \mathbb{F}_q [F] \)-module, \( \mathcal{F} \) is free with basis \( (T^jF^i)_{i = 0 \text{ or } qj, 0 \leq j < q^i} \). As a consequence, it is torsionfree (but this also follows from the isomorphism \( \mathcal{F} \to \mathbb{F}_q [T] [X]_{\text{lin}} \) introduced below).
- As \( \mathbb{F}_q [F] \)-\( \mathbb{F}_q [T] \)-bimodule, \( \mathcal{F} \) is free with basis \( (T^jF^i)_{(i,j) \in \mathbb{N}^2; (i = 0 \text{ or } qj) \text{ and } 0 \leq j < q^i} \)
  \( (T^jF^i) \cdot \mathbb{F}_q [T] \) 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 \( T^jF^i \) with \( (i, j) \in \mathbb{N}^2 \). Actually, this monoid is \( J \)-trivial. Finite \( J \)-trivial monoids have a very nice representation theory \( 4 \); does ours?\(^5\)

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

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 \( P \in \mathbb{F}_q [T] \).

\(^5\)I wouldn’t hope for much; the representation theory of \( \langle F, T \mid FT = TF \rangle \) is supposedly ugly.
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 \( \text{Carl} \) 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 \( X^q, X^{q^2}, \ldots \) 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

\[
\mathcal{F} \to \mathbb{F}_q [T] [X]_{q - \text{lin}},
\]

\[
F \mapsto X^q,
\]

\[
T \mapsto TX
\]

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 \( \pi \in \mathbb{F}_q [T] \),

there exists a unique \( u (\pi) \in \mathcal{F} \) such that \( \text{Carl} \pi = F^{\deg \pi} + \pi \cdot u \). (3)

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

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

Now, the situation described in Remark 2.14 is simply understood as having a left \( \mathcal{F} \)-module \( A \), and for every \( P \in N \), 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 (3)).
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. Speculations

3.1. 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 \( W_N : \text{CRing}_{\mathbb{F}_q[T]} \to \text{CRing}_{\mathbb{F}_q[T]} \), but at the representing object of the functor \( W_N : \mathcal{F} \text{-Mod} \to \mathcal{F} \text{-Mod} \), or at least that the latter is more fundamental than the former. To begin with, it’s smaller.

A representing object of a functor \( \mathcal{F} \text{-Mod} \to \mathcal{F} \text{-Mod} \) is the same as an \( \mathcal{F} \text{-}\mathcal{F} \)-bimodule (please correct me if I’m doing anything wrong). The \( \mathcal{F} \text{-}\mathcal{F} \)-bimodule \( \Lambda_{\mathcal{F}} \) with basis \( (x_P)_{P \in \mathbb{N}} \), and with right \( \mathcal{F} \)-module structure defined as follows:

Let \( p_P = \sum_{D \mid P} \frac{P}{D} (x_D) \) for every \( P \in \mathbb{N} \). (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 \( P \in \mathbb{N} \) 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 \( \mathcal{F} \text{-}\mathcal{F} \)-bimodule \( \Lambda_{\mathcal{F}} \) has some claims to be the Carlitz analogue of the ring of symmetric functions, although it is an \( \mathcal{F} \text{-}\mathcal{F} \)-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

---

6What 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?

7These are the symmetric functions \( w_n \) in [8 Exercise 2.79]. Their name stems from their relation to the Witt vectors; from a combinatorial viewpoint, they are a rather exotic family.
\[
\sum_i [P](\xi_i) = [P]\left(\sum_i \xi_i\right) = (\text{Carl}(P))\left(\sum_i \xi_i\right).
\]

The absence of multiplicative structure makes it hard to even guess what “elementary symmetric functions” or “complete homogeneous symmetric functions” would be in the Carlitz situation. But Carlitz exponential and Carlitz logarithm are well-defined on every left \( \mathcal{F} \)-module on which \( \mathbb{F}_q[T] \) acts invertibly (i.e., whose \( \mathbb{F}_q[T] \)-module structure extends to an \( \mathbb{F}_q(T) \)-module structure) and which has appropriate closure properties. We might try to use them to construct the “elementary symmetric functions” by some analogue of the classical
\[
\sum_{n \in \mathbb{N}} (-1)^n e_n T^n = \exp\left(-\sum_{n \geq 1} \frac{1}{n} p_n T^n\right)
\]
formula from the theory of symmetric functions.

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 \( \Lambda_\mathcal{F} \otimes \mathcal{F} \) to \( \Lambda_\mathcal{F} \) making \( \Lambda_\mathcal{F} \) into what would be an \( \mathcal{F} \)-algebra if it were commutative?).

### 3.2. 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, \( p_T = \left[ T \right] (x_1) + T x_T = (F + T) x_1 + T x_T \). 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
\[
((F + T) x_1 + T x_T) T = (F + T) \underbrace{x_1 T}_{= T x_1} + T x_T T = (F + T) \underbrace{T x_1}_{= T x_1} + T x_T T
\]

(since \( x_1 \) is central)
\[
= T \left( (T^{q-1} F + T) x_1 + x_T T \right),
\]
this rewrites as \( T \left( (T^{q-1} F + T) x_1 + x_T T \right) = T ((F + T) x_1 + T x_T) \). 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),

---

8 Another suggestion by James Borger.
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 

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

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 

$$Tx_T F = F ((F + T) x_1 + T x_T) - (F + T) x_1 F$$

$$= F F x_1 + \frac{F T}{T^q F} x_1 + \frac{F T}{T^q F} x_T - F x_1 T$$

$$= F F x_1 + T^q F x_1 + T^q F x_T - F F x_1 - T x_1 F = T^q F x_1 + T^q F x_T - T x_1 F$$

$$= T \left( T^{q-1} F x_1 + T^{q-1} F x_T - x_1 F \right).$$

Cancelling $T$, we obtain 

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

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 

$$\pi x_\pi T = T ((\text{Carl } \pi) x_1 + \pi x_\pi) - (\text{Carl } \pi) x_1 T$$

$$= T (\text{Carl } \pi) x_1 + T\pi x_\pi - (\text{Carl } \pi) x_1 T$$

$$= T (\text{Carl } \pi) x_1 + T\pi x_\pi - (\text{Carl } \pi) T x_1$$

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 [3], but there seems to be no way to write the quotient in finite terms. Let us rather introduce a notation for it: Let $\delta_T (\pi)$ denote the (unique) $f \in \mathcal{F}$
satisfying $[T, \text{Carl } \pi] = \pi f$ (for $\pi$ irreducible monic). In more elementary (and commutative) terms, $\partial_T (\pi) = T \frac{[\pi] (X) - [\pi] (TX)}{\pi}$. Now,

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

Cancelling $\pi$, we obtain $x_{\pi} T = T x_{\pi} + \pi \partial_T (\pi) x_1$.

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

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

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

$$\pi x_{\pi} F = F ((\text{Carl } \pi) x_1 + \pi x_{\pi}) - (\text{Carl } \pi) x_1 F$$

$$= F (\text{Carl } \pi) x_1 + F \pi x_{\pi} - (\text{Carl } \pi) F x_1$$

$$= F \pi x_{\pi} + [F, \text{Carl } \pi] x_1.$$  

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

$$\pi x_{\pi} F = F \pi x_{\pi} + [F, \text{Carl } \pi] x_1 = F \pi x_{\pi} - \pi \partial_T (\pi) x_1 = \pi^q F x_{\pi} - \pi \partial_T (\pi) x_1.$$  

Cancelling $\pi$, we obtain $x_{\pi} F = \pi^{q-1} F x_{\pi} - \pi \partial_T (\pi) x_1$.

### 4. The logarithm series

Here is my result on the logarithm series, which so far has not found any application.

**Theorem 4.1.** Let $q$ be a prime power. Consider the Carlitz logarithm $\log_C \in \mathbb{F}_q (T) [[X]]$ defined in [2, Section 7] (but with $q$ instead of $p$). Then, in the power series ring $\mathbb{F}_q (T) [[X, S]]$, we have

$$\log_C (SX) = \sum_{N \in \mathbb{F}_q [T]} (-1)^{\deg N} s_N^{\deg N} \frac{[N] (X)}{N}. (4)$$
(The right hand side of this converges in the usual topology on $F_q[[X, S]]$.)

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

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

It should be noticed that it is possible to specialize $S$ to 1 in (4), 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 4.1 seems to be neither straightforward nor provable by translating some classical argument. So let me sketch a proof (which is rather roundabout and hopefully simplifiable). First, I need an auxiliary result which itself seems rather interesting:

**Proposition 4.2.** Let $q$ be a prime power. Let $A$ be a commutative $F_q$-algebra. Let $n \in \mathbb{N}$. Let $P \in A[X]$ be a polynomial such that $\text{deg} P < q^n - 1$. Let $e_1, e_2, ..., e_n$ be $n$ elements of $A$. Then,

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

**Proof of Proposition 4.2 (sketch).** We can WLOG assume that $P = X^k$ for some $k \in \{0, 1, ..., q^n - 2\}$. Assume this and consider this $k$. Since $k < q^n - 1$, we can write $k$ in the form $k = k_{n-1}q^{n-1} + k_{n-2}q^{n-2} + ... + k_0 q^0$ with $k_i < q$ and with $k_0 + k_1 + ... + k_{n-1} \leq n (q - 1) - 1$. Thus,

$$P = X^k = X^{k_{n-1}q^{n-1} + k_{n-2}q^{n-2} + ... + k_0 q^0} = \prod_{i=0}^{n-1} X^{k_i q^i} = \prod_{i=0}^{n-1} \left(X^{q^i}\right)^{k_i}.$$  

22
Hence,

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

Now, consider the product \( \prod_{i=0}^{n-1} \left( \lambda_1 e_1^{q^i} + \lambda_2 e_2^{q^i} + \ldots + \lambda_n e_n^{q^i} \right)^{k_i} \) as a polynomial (over \( A \)) in the variables \( \lambda_1, \lambda_2, \ldots, \lambda_n \). Then, it is a polynomial of degree \( k_0 + k_1 + \ldots + k_{n-1} \leq n(q-1)-1 \). It is well-known (e.g., from the proof of the Chevalley-Warning theorem) that any such polynomial yields 0 when summed over all \( (\lambda_1, \lambda_2, \ldots, \lambda_n) \in \mathbb{F}_q^n \) (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 4.2.

Another auxiliary result:

**Proposition 4.3.** 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 4.3 (sketched).** Let \( W \) be the polynomial \( \prod_{v \in V} (X + v) \in L[X] \). This polynomial is a \( q \)-polynomial (by [2] Theorem A.1 2) and Corollary A.3); 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

$$W' = \sum_{w \in V} (X + w)' \cdot \prod_{v \in V; v \neq w} (X + v) = \sum_{w \in V} \prod_{v \in V; v \neq w} (X + v) = \sum_{w \in V} \prod_{v \in V} \frac{X + v}{X + w}$$

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

Applying this to $X = t$, we obtain

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

so that

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

Rename the index $w$ as $v$ and obtain the claim of Proposition 4.3.

**Proof of Theorem 4.1 (sketched).** By (5), we have

$$\log C (SX) = \sum_{j \in \mathbb{N}} (-1)^j (SX)^{q^j} L_j = \sum_{j \in \mathbb{N}} (-1)^j q^j X^{q^j} L_j.$$  

Hence, it is clearly enough to show that every $m \in \mathbb{N}$ satisfies

$$\frac{X^{q^m}}{L_m} = \sum_{\substack{N \in \mathbb{F}_q[T], \deg N = m \\text{and} \\mathbb{F}_q[T]_+}} \frac{[N] (X)}{N}.$$  

(6)

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 [2, Section 7], but with $q$ instead of $p$. Let’s spell out their definition: With $e_C$ denoting the Carlitz exponential, the power series $e_C (Y \log C X) \in \mathbb{F}_q (T) [[X, Y]]$ is a $q$-power series, i. e., its coefficient before $X^\alpha Y^\beta$ can only be nonzero if both $\alpha$ and $\beta$ are powers of $q$. Now, for every $j \in \mathbb{N}$, define $E_j (Y)$ to be the coefficient of this power series $e_C (Y \log C X)$, **regarded as a power series in $X$ over $\mathbb{F}_q (T) [Y]$**, before $X^{q^j}$. Of course, this $E_j (Y)$ is a $q$-polynomial in $\mathbb{F}_q (T) [Y]$. Moreover, $\deg (E_j) = q^j$ and $E_j (0) = 0$ for all $j \in \mathbb{N}$. Furthermore, $E_j (M) = 0$
for every $M \in \mathbb{F}_q [T]$ satisfying $\deg M < j$. Finally, $E_j (M) = 1$ for every $M \in \mathbb{F}_q [T]$ satisfying $\deg M = j$. But most importantly, $[M] (X) = \sum_{j \in \mathbb{N}} E_j (M) X^j$ 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

$$\frac{[M] (X)}{M} = \sum_{j \in \mathbb{N}} \frac{E_j (M) X^j}{M} = \sum_{j \in \mathbb{N}} \frac{E_j (M) X^j}{M} = \sum_{j=0}^{\deg M} \frac{E_j (M) X^j}{M} Y^j (\text{since } E_j (M) = 0 \text{ whenever } \deg M < j)$$

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

$$(\text{since } E_j (M) = 1 \text{ whenever } \deg M = j)$$

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

(7)

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 $j \in \{0, 1, ..., m - 1\}$, we can apply Proposition 4.2 to $A = \mathbb{F}_q (T)$, $n = m$, $P = \frac{E_j (X + T^m)}{X + T^m}$ and $e_i = T^{i-1}$, and conclude that

$$\sum_{(\lambda_1, \lambda_2, ..., \lambda_m) \in \mathbb{F}_q} E_j \left( \lambda_1 T^0 + \lambda_2 T^1 + ... + \lambda_m T^{m-1} + T^m \right) \left( \frac{\lambda_1 T^0 + \lambda_2 T^1 + ... + \lambda_m T^{m-1} + T^m}{\lambda_1 T^0 + \lambda_2 T^1 + ... + \lambda_m T^{m-1} + T^m} \right) = 0$$

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

$$\sum_{N \in \mathbb{F}_q [T]_+; \deg N = m} \frac{E_j (N)}{N} = 0$$

for every $j \in \{0, 1, ..., m - 1\}$. (8)
Now,

$$\sum_{\substack{N \in F_q[T]_+; \\
\deg N = m}} \frac{[N](X)}{N} \frac{E_j(N)}{N} X^{q^j} + \frac{1}{N} X^{q^\deg N}$$

(here we applied (7) to $M = N$)

$$= \sum_{j=0}^{m-1} \sum_{\substack{N \in F_q[T]_+; \\
\deg N = m}} \frac{E_j(N)}{N} X^{q^j} + \sum_{\substack{N \in F_q[T]_+; \\
\deg N = m}} \frac{1}{N} X^{q^m}$$

(by [8])

$$= \sum_{\substack{N \in F_q[T]_+; \\
\deg N = m}} \frac{1}{N} X^{q^m} = \sum_{\substack{v \in F_q[T]; \\
\deg v < m; \ v \neq 0}} \frac{1}{T^{m+v}} X^{q^m}$$

since the monic polynomials in $F_q[T]$ of degree $m$ are exactly the sums of the form $T^{m+v}$ with $v$ being a polynomial in $F_q[T]$ of degree $< m$

$$= \left( \prod_{\substack{v \in F_q[T]; \\
\deg v < m; \ v \neq 0}} \frac{1}{T^{m+v}} \right) \cdot \left( \prod_{\substack{v \in F_q[T]; \\
\deg v < m; \ v \neq 0}} v \right) X^{q^m}$$

(by Proposition 4.3 applied to $L = F_q(T), t = T^m$ and $V = \{ v \in F_q[T] \mid \deg v < m \}$)

$$= \left( \prod_{\substack{N \in F_q[T]_+; \\
\deg N = m}} \frac{1}{N} \right) \cdot \left( \prod_{\substack{v \in F_q[T]; \\
\deg v < m; \ v \neq 0}} v \right) X^{q^m} = \frac{X^{q^m}}{L_m}.$$

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

This proves (6) and thus Theorem 4.1.
I hope there is a better proof.
References

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

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

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


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

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

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

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