Drinfel′d Modules: The Carlitz Module, Part 2

Shubhodip Mondal*

September 22, 2017

Today is the second part of our discussion of Carlitz modules. Last time, we defined the Carlitz exponential, and described how the Carlitz module structure can be described as a homomorphism to the ring of additive polynomials $k\{\tau\}$.

1 Notation and review from last time

We briefly recall some notation and results we had last time.

Notation 1.1. We denote by $\mathbf{F}_r$ the finite field of order $r = p^m$, and denote $A = \mathbf{F}_r[T]$. We also denote $k = \mathbf{F}_r(T)$, and consider the valuation

$$v_\infty \colon k \longrightarrow \mathbf{R} \cup \{\infty\}$$

where $v_\infty(1/T) = 1$. We can evaluate the valuation of any rational function by first doing a transformation $T \to 1/T$ and then writing it as $(T)^e(P(T)/Q(T))$ for $P(T)$ and $Q(T)$ not divisible by T, in which case this element has valuation e.

The completion of k with respect to v_∞ is denoted K_∞. We fix an algebraic closure $\overline{K_\infty}$ of K_∞ and we define $\mathbf{C}_\infty$ to be its completion.

We also defined $[i] = T^{r^i} - T$, and defined

$$D_0 = 1, \qquad D_i = [i][i-1]^r \cdots [1]^{r^{i-1}}$$

and

$$L_0 = 1, \qquad L_i = [i][i-1] \cdots [1]$$

which are analogues of factorials.

One of our main results last time was the following:

Theorem 1.2 (Carlitz [Gos96, Thm. 3.1.5, Lem. 3.2.5, Cor. 3.2.6])**.** *Let*

$$e_d(x) \coloneqq \prod_{\alpha \in A(d)} (x - \alpha)$$

where $A(d) \coloneqq \{\alpha \in A \mid \deg < d\}$. *Then,*

$$e_d(x) = \sum_{i=0}^{d} (-1)^{d-i} x^{r^i} \frac{D_d}{D_i L_{d-i}^{r^i}}.$$

We will give an alternative proof of this last fact, using Moore determinants [Gos96, p. 45].

[*] Notes were taken by Takumi Murayama, who is responsible for any and all errors. Please e-mail takumim@umich.edu with any corrections. Compiled on September 26, 2017.

2 Additive polynomials [Gos96, §§1.1–1.2]

We start with some preliminaries on $\mathbf{F}_r$-linear polynomials. Let $\mathbf{F}_r \subseteq L$ be a field extension, and let $P(x) \in L[x]$. We then have the following:

Proposition 2.1 (cf. [Gos96, Prop. 1.1.5])**.** *Let L be an infinite field containing $\mathbf{F}_r$. Then, a polynomial $P(x) \in L[x]$ is $\mathbf{F}_r$-linear if and only if $P(x) \in L\{\tau\}$.*

Here, we say that $P(x)$ is $\mathbf{F}_r$-linear if $P(\alpha+\beta) = P(\alpha) + P(\beta)$ for all $\alpha, \beta \in L$, and $P(\lambda\alpha) = \lambda P(\alpha)$ for $\lambda \in \mathbf{F}_r$. The ring $L\{\tau\}$ is the ring of polynomials in $\tau = x^r$, with composition as multiplication. This ring is sometimes called the *ring of Frobenius polynomials* or the *Frobenius algebra*.

We note that for Proposition 2.1 to hold, we must assume that L is infinite. For example, if $L = \mathbf{F}_r$, then $(x^r - x)^2$ evaluates to zero for all $\alpha \in \mathbf{F}_r$, but it is not in $L\{\tau\}$.

We will also need the following result:

Theorem 2.2 (cf. [Gos96, Cor. 1.2.2])**.** *Let L be an algebraically closed field containing $\mathbf{F}_r$. Let $P(x) \in L[x]$ be a separable polynomial. Then, $P(x)$ is $\mathbf{F}_r$-linear if and only if roots of $P(x)$ form an $\mathbf{F}_r$-vector space.*

Since the roots of $e_d(x)$ form an $\mathbf{F}_r$-vector space by definition, we can conclude the following:

Corollary 2.3. *The polynomial $e_d(x)$ is $\mathbf{F}_r$-linear.*

3 The Moore determinant [Gos96, §1.3 and p. 45]

One of the key elements of the induction-free proof of Theorem 1.2 is that the polynomial $e_d(x)$ can be written in terms of Moore determinants.

Definition 3.1. The *Moore determinant* is

$$\Delta(w_0, \ldots, w_d) \coloneqq \det \begin{pmatrix} w_0 & \cdots & w_d \\ w_0^r & \cdots & w_d^r \\ \vdots & & \\ w_0^{r^d} & \cdots & w_d^{r^d} \end{pmatrix}.$$

The Moore determinant can detect linear independence of elements over $\mathbf{F}_r$.

Proposition 3.2 [Gos96, Lem. 1.3.3]**.** *Let L be a field containing $\mathbf{F}_r$. The, the set $\{w_0, \ldots, w_d\}$ is linearly independent over $\mathbf{F}_r$ if and only if $\Delta(w_0, \ldots, w_d) \neq 0$.*

In our case, we have

$$e_d(x) = \prod_{\alpha \in A(d)} (x + \alpha) = \frac{\Delta(1, \ldots, T^{d-1}, x)}{\Delta(1, \ldots, T^{d-1})},$$

since $e_d(x)$ is zero if and only if x is a polynomial of degree $< d$, and the constant in the denominator is there to get the correct scaling; see [Gos96, Prop. 1.3.5.2]. This equality is the analogue of how the Vandermonde determinant of $1, 2, 3, \ldots, n, x$ is a constant multiple of $(x-1)\cdots(x-n)$.

This expression of $e_d(x)$ in terms of the Moore determinant shows the expression for $e_d(x)$ in Theorem 1.2 by writing out the Moore determinants in the numerator and denominator; see [Gos96, p. 45].

4 The Carlitz module and the Carlitz exponential [Gos96, §§3.2–3.3]

Last time, to prove the convergence statement in Theorem 1.2, we did some rescaling: Choose an $(r-1)$th root λ of $-[1]$ from $\overline{K_\infty}$, and let

$$\xi_* \coloneqq \prod_{j=1}^{\infty} \left(1 - \frac{[j]}{[j+1]}\right),$$

which we can think of as an analogue of $\pi \in \mathbf{R}$. Set $\xi \coloneqq \lambda\xi_*$, which we can think of as an analogue of $2\pi i \in \mathbf{C}$. Then, we showed that

$$e_C(x) \coloneqq \sum_{j=0}^{\infty} \frac{x^{r^j}}{D_j},$$

is an entire function [Gos96, Lem. 3.2.5], such that [Gos96, Thm. 3.2.8]

$$\frac{1}{\xi} e_C(\xi x) = x \prod_{0 \neq \alpha \in A} \left(1 - \frac{x}{\alpha}\right).$$

Note that this implies $e_C(\cdot)$ is $\mathbf{F}_r$-linear. Replacing $x \mapsto x/\xi$, we get the expression

$$x \prod_{\alpha \in L \smallsetminus \{0\}} \left(1 - \frac{x}{\alpha}\right) = e_C(x),$$

where $L \coloneqq \xi A$ [Gos96, Cor. 3.2.9].

Last time, we also saw:

Proposition 4.1 [Gos96, Prop. 3.3.1]**.** *Let $x \in \mathbf{C}_\infty$. Then,*

$$e_C(Tx) = Te_C(x) + (e_C(x))^r.$$

This shows that the action of T on $\mathbf{C}_\infty$ via the A-module structure induced by e_C is the same as the usual action of T, added with a Frobenius twist by τ, since $(e_C(x))^r = \tau(e_C(x))$.

Corollary 4.2 [Gos96, Cor. 3.3.2]**.** *If $a = \sum_{i=0}^{d} a_i T^i$ for $a_i \in \mathbf{F}_r$. Then,*

$$e_C(ax) = ae_C(x) + \sum_{j=1}^{d} C_a^{(j)} e_C(x)^{r^j}$$

where $\{C_a^{(j)}\} \subset A$, and $C_a^{(d)} = a_d$.

We will later talk about how we can define Carlitz modules by choosing a similar collection of elements of A first. Also we will discuss how the fact that $C_a^{(j)} \subset A$ allows us to replace our ground field k with an arbitrary A-field.

Proof Idea. By $\mathbf{F}_r$-linearity, it suffices to note that for $i \geq 1$, we have

$$e_C(T^i x) = e_c(T(T^{i-1}x)),$$

and then use induction. For example,

$$e_C(T^2 x) = T^2 e_C(x) + (T^r + T)e_C^r(x) + e_C(x)^{r^2}. \qquad \square$$

Later on, we will also see how to iteratively compute $C_a^{(j)}$ from $C_a^{(j-1)}$.

We also saw that we can define, for $a \in A = \mathbf{F}_r[T]$, the polynomial

$$C_a(x) = a\tau^0 + \sum_{j=1}^{d} C_a^{(j)} \tau^j \in k\{\tau\},$$

where $d = \deg a$. From the relation above, it follows that

$$e_C(ax) = c_a(e_C(x)),$$

and we have the following:

Theorem 4.3 [Gos96, Thm. 3.3.4]**.** *The mapping*

$$\begin{aligned} A &\longrightarrow k\{\tau\} \\ a &\longmapsto C_a \end{aligned}$$

is an injective homomorphism of $\mathbf{F}_r$*-algebras, and in particular,*

$$C_{ab} = C_a \circ C_b = C_b \circ C_a = C_{ba}.$$

So although the codomain $k\{\tau\}$ is not commutative, the image of A *is* commutative. In any case, the non-commutativity of the ring $k\{\tau\}$ is quite tractable: $\tau a = a^r x^r$, while $a\tau = ax^r$.

Definition 4.4. This map $A \to k\{\tau\}$ is called the *Carlitz module*. This defines a new A-module structure on $\mathbf{C}_\infty$: if $x \in \mathbf{C}_\infty$, then $a \cdot x = C_a(x)$, and in particular, for $m \in \mathbf{F}_r$, we have $m \cdot x = mx$.

Remark 4.5. The Carlitz module is the unique map taking $T \mapsto T + \tau$ which is identity on elements of $\mathbf{F}_r$. Therefore, in principle, we could use this as our definition and avoid having to talk about the exponential. However, while computing the torsions of the Carlitz module, we will see the importance of the exponential. In the more general case, while defining the Drinfeld module associated to a lattice, its often convenient to start with an exponential function associated to the lattice.

Since the Carlitz exponential is surjective (see [Gos96, Prop. 2.13], whose proof uses Newton polygons), the Carlitz exponential induces an isomorphism

$$e_C \colon \mathbf{C}_\infty / L \xrightarrow{\sim} \mathbf{C}_\infty,$$

where $L \coloneqq \xi A$ as before. Thus, the Carlitz exponential e_C is transporting the A-module on the left-hand side to the Carlitz module structure on the right-hand side.

We now define the analogue of roots of unity for complex numbers (which are in other words, the $\mathbf{Z}$ torsion elements in $\mathbf{C}^*$) in the case of Carlitz modules.

Definition 4.6. The *division values* of the Carlitz module are the values

$$\{e_C(a\xi) \mid a \in k\} \subset \mathbf{C}_\infty,$$

where $e_C(a\xi) \in \mathbf{C}_\infty$ since writing $a = b/f \in k$, we have

$$C_f(e_C(a\xi)) = e_C(b\xi) = 0,$$

i.e., $e_C(a\xi)$ is a root of $C_f(x) = 0$, hence in $\mathbf{C}_\infty$.

Definition 4.7. Let $g \in A$. We set

$$C[g] \coloneqq \left\{ e_C\left(\frac{b\xi}{g}\right) \;\middle|\; b \in A \right\} \subset \mathbf{C}_\infty,$$

which are all the roots of $C_g(x)$. They are the $g-$torsion elements in the Carlitz module. This sub-A-module (as Carlitz modules) of $\mathbf{C}_\infty$ is isomorphic to $A/(g)$.

We now prove something quite analogous to the computation of Galois groups for cyclotomic fields.

Proposition 4.8 [Gos96, Prop. 3.3.8]**.** *Let* $L \subseteq \mathbf{C}_\infty$ *be an extension of* k*. Let* $a \in k$ *and let* $L_1 = L(e_C(a\xi))$*. Then,* L_1 *is an abelian extension of* L*.*

Proof. If $a = b/f$, then

$$e_C\left(\frac{b}{f}\xi\right) = C_b\left(e_C\left(\frac{\xi}{f}\right)\right),$$

and so $L_1 \subseteq L(e_C(\xi/f))$. We can therefore reduce to the case when $b = 1$, since if $L(e_C(\xi/f))$ is an abelian extension of L, then $\mathrm{Aut}(L_1/L)$ is a quotient of $\mathrm{Aut}(L(e_C(\xi/f))/L)$, hence is abelian as well.

We therefore assume that $L_1 = L(e_C(\xi/f))$. In this case, since $e_C\left(\frac{b}{f}\xi\right) = C_b\left(e_C\left(\frac{\xi}{f}\right)\right)$, we see that L_1 contains all the f-torsion points, which are all the roots of $C_f(x)$, and therefore L_1 is a splitting field for $C_f(x)$ which is a separable polynomial. The extension is therefore Galois, and the f-torsion points are isomorphic to $A/(f)$ as Carlitz modules.

Let G be the Galois group, and let $x \in L_1$. If $\sigma \in G$ and $g \in A$, then we have $C_g(\sigma(x)) = \sigma(C_g(x))$ since

$$\sum_j a_j(\sigma(x))^{r^j} = \sum_j \sigma(a_j x^{r^j}) = \sigma C_g(x),$$

i.e., the Galois group G commutes with the Carlitz module structure since the module structure is defined by a polynomial with coefficients in A. We then claim that $\sigma(e_C(\xi/f))$ is a generator for f-torsion points. Indeed,

$$C_g\left(\sigma\left(e_c\left(\frac{\xi}{f}\right)\right)\right) = \sigma\left(C_g\left(e_C\left(\frac{\xi}{f}\right)\right)\right) = \sigma\left(e_c\left(\frac{g\xi}{f}\right)\right).$$

We note that σ permutes f-torsion points, since they are all the roots of $C_f(x)$. Now by varying g one can obtain all f-torsion points. So the above equality implies that,

$$\sigma(e_C(\xi/f))$$

is an A-module generator for f-torsion points as well. We therefore see that we can embed $G \hookrightarrow (A/f)^*$. □

Before moving on to Carlitz modules for arbitrary A-fields, we will go back a little bit and try to compute the $C_a^{(j)}$ in terms of a recursion. Let

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{d} C_a^{(j)}\tau^j$$

as before. Defining $a_j := c_a^{(j)}$, we have

Proposition 4.9 [Gos96, Prop. 3.3.10]**.**

$$a_1 = \frac{a^r - a}{T^r - T},\ a_2 = \frac{a_1^r - a_1}{T^{r^2} - T},\ \dots\ , a_i = \frac{a_{i-1}^r - a_{i-1}}{T^{r^i} - T},\ \dots$$

Proof. Write $C_a = a\tau^0 + \chi_a$, where $\chi_a \in A\{\tau\}$; for example, $\chi_T = \tau$. We can write $C_aC_T = C_TC_a$, hence

$$(a\tau^0 + \chi_a)C_T = C_T(a\tau^0 + \chi_a).$$

In terms of the commutator $[\cdot,\cdot]$, this is equivalent to

$$[C_T, a\tau^0] = -[C_T, x_a].$$

Equating coefficients of τ^j on both sides gives the desired formulas. We also note that since $v \mapsto [u,v]$ is a derivation of $k\{\tau\}$ where $u, v \in k\{\tau\}$, we obtain a derivational equation for the Carlitz module structure. □

5 The Carlitz Logarithm [Gos96, §3.4]

We can define

$$\log(x) = \sum_{i=0}^{\infty}(-1)^i\frac{x^{r^i}}{L_i},$$

which converges at α if $v_\infty(\alpha) > \frac{r}{1-r}$. One can also calculate

$$v_\infty(\xi) = \frac{r}{1-r},$$

and so the logarithm converges ”up to the smallest non-zero period of $e_C(x)$”.

6 Carlitz modules over arbitrary A-fields [Gos96, §3.6]

Definition 6.1. We say that L is an *A-field* if there is a homomorphism $\iota\colon A \to L$. We define $\wp := \ker(\iota)$. We say that L has *generic characteristic* if $\wp = \{0\}$.

To define a Carlitz module structure on L, we do the following: we define

$$\hat{C}_a = \sum_j \iota(C_a^{(j)})\tau^j,$$

and define the A-module structure by $a \cdot x = \hat{C}_a x$ for $x \in L$. We will abuse the notation and write C_a in place of $\hat{C}_a$.

Taking the derivative with respect to x, we get

$$C_a'(x) = \iota(a),$$

that is, c_a is separable if and only if $a \notin \wp$.

From now on, we assume that L is algebraically closed (by extending to $\overline{L}$). We can then define $C[a] \subset \overline{L}$ to be the roots of $C_a(x)$, which are the same as the a-torsion points.

We want to describe the a-torsion points of C as an A-module.

Theorem 6.2 [Gos96, Thm. 3.6.2.1]**.** *Let $a \notin \wp = \ker(\iota)$. Then, $C[a] \simeq A/(a)$.*

Proof. First, note that $C[a]$ is an A-module with $r^{\deg(a)}$ elements. We also have that

$$C[a] \simeq \bigoplus_i A/(h_i)^{b_i} \tag{6.1}$$

since A is a PID, where the h_i-s are prime and $b_i > 0$. We then use the following:

Lemma 6.3. *Let $a, f \in A$. Assume that at least one the elements a, f does not belong to $\wp$. Then C_f acts as automorphisms on $C[a]$ if and only if $\gcd_A(f, a) = 1$.*

Proof. C_f clearly acts on $C[a]$ since we have $C_f(C_a(x)) = C_a(C_f(x))$. Since $C[a]$ is finite, this action is an automorphism iff C_f has a trivial kernel, i.e., C_f and C_a has no common non-zero root. Now if $\gcd(a, f) = 1$ then we have an equation of the form $uf + va = 1$. But that implies that $C_uC_f + C_vC_a = \mathrm{id}$, which allows us to conclude that there cannot be a common non-zero root. Conversely if $\gcd(a, f) = t$, where $\deg t \geq 1$, we have $a = pt$ and $f = qt$. So $C_a = C_pC_t$ and $C_f = C_qC_t$. Now $C_a' \neq 0$ ($C_f' \neq 0$) implies that $C_t' \neq 0$. Now $\deg C_t = r^{\deg t} \geq r$. So C_t has a non-zero root, implying that C_a and C_f has a non-zero common root. □

Returning to the proof of Theorem 6.2, we write $a = \prod_j f_j^{e_j}$, and apply Lemma 6.3 to see that exactly the irreducible factors of a appear in the decomposition (6.1), since these are the only elements of A that cannot act by automorphisms on $C[a]$. Also, the LHS of (6.1) has elements that are $f_j^{e_j}$ torsions but not f_j^t torsion for any $t < e_j$.That implies that the decomposition (6.1) must contain factors of the form $A/(f_j)^{b_j}$, where $b_j \geq e_j$. Now we just count: we have

$$r^{\deg a} = \#C[a] \geq r^{\sum b_j \deg f_j} \geq r^{\sum e_j \deg f_j} = r^{\deg a},$$

hence $b_j = e_j$, and therefore

$$C[a] \simeq \bigoplus_i A/(f_j)^{e_j} \simeq A/a.$$

□

We can also show the following:

Theorem 6.4 [Gos96, Thm. 3.6.2.2]**.** *Let $(f) = \wp$. Then, $C[f^i] = \{0\} \subset L$.*

Proof. Since $C'_f(x) = \iota(f) = 0$, we see that $C_f(x)$ is not separable, hence it has $< r^{\deg(f)}$ roots in L. An argument similar to that of Theorem 6.2 says that $C[f] \simeq A/(f)^j$ for some j. Indeed, for any prime $h \neq f$, $h \notin \wp$ and by the above lemma, C_h acts as an automorphism on $C[f]$. Now,

$$r^{j \deg f} = \#(A/f^j) = \#C[f] < r^{\deg(f)}.$$

Therefore, $j = 0$. This also says something abut C_f:

$$C_f \equiv x^{r^{\deg f}} \mod \wp A[x],$$

and moreover,

$$C_{f^i} = x^{r^{i \deg f}} \mod \wp A[x].$$

□

One can also interpret the results above in terms of finite group schemes, since

$$C[f^i] \simeq L[x]/x^{r^{i \deg f}}.$$

We now formulate a generalization of Lemma 6.3.

Corollary 6.5. *Let $a, b \in A$. Then C_b acts as an automorphism on $C[a]$ iff $\gcd(a, b) = f^i$ for some $i \geq 0$, where $(f) = \wp$.*

Proof. Let a' be such that $\gcd(a', f) = 1$ and $f^m a' = a$. Then $C[a] = C[a']$ and $a' \notin \wp$. Now by the lemma, C_b acts as automorphism on $C[a']$ iff $\gcd(a', b) = 1$, implying that $\gcd(a, b) = f^i$ for some $i \geq 0$. Converse is also clear. □

Now suppose we have a prime element f of A. We define $\wp := (f)$. Then, we have a map

$$A \longrightarrow A/\wp = \mathbf{F}_\wp.$$

Let $\mathbf{F}_{\wp^n}$ be the extension of $\mathbf{F}_\wp$ of degree n. It is an A-field of characteristic $\wp$ and can be equipped with a Carlitz module structure. We then have

Proposition 6.6 [Gos96, Thm. 3.6.3]**.** *Via C, we have $\mathbf{F}_{\wp^n} \simeq A/(f^n - 1)$ as Carlitz A-modules.*

Proof. The left-hand side is a finite set and an A-module. Since A is infinite, there exists $m \neq 0$ in A such that m annihilates $\mathbf{F}_{p^n}$. This implies that $\mathbf{F}_{p^n}$ is an A-submodule of a cyclic module. Since A is a PID, this implies that $\mathbf{F}_{p^n}$ is cyclic. Now we already saw that $C_{f^n} = x^{r^{n \deg f}} \mod \wp A[x]$. This implies that $f^n - 1$ annihilates $\mathbf{F}_{p^n}$ as an A-module. Now as before, we can count number of points on either side to show that it must be isomorphic to $A/(f^n - 1)$. □

References

[Gos96] D. Goss. *Basic structures of function field arithmetic.* Ergeb. Math. Grenzgeb. (3), Vol. 35. Berlin: Springer-Verlag, 1996. DOI: 10.1007/978-3-642-61480-4. MR: 1423131.