Drinfel′d Modules: The Carlitz Module, Part 1

Alex Horawa*

September 15, 2017

Today, we will discuss Carlitz modules, which are the first examples of Drinfel′d modules.

1 Motivation

We start with some motivation for what we will do today.

Recall from last time that we want an analogue for function fields of elliptic curves, which arise out of studying the Langlands correspondence over $\mathbf{Q}$. We had the following process for producing elliptic curves:

$$\mathbf{Q} \xrightarrow[\left(\substack{\text{with respect to}\\ \text{standard metric}}\right)]{\text{completion}} \mathbf{R} \xrightarrow{\text{algebraic closure}} \mathbf{C} \twoheadrightarrow \mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C})$$

where $L \simeq \mathbf{Z}^2 \subset \mathbf{C}$ is a lattice, and $E(\mathbf{C})$ is a complex elliptic curve. The inclusion $\mathbf{Z} \subset \mathbf{Q}$ gives $E(\mathbf{C})$ the structure of an abelian group.

Today, we will consider the function field $k = \mathbf{F}_r(T)$ of $\mathbf{P}^1_{\mathbf{F}_r}$, where $r = p^{m_0}$ is a power of a prime p. Let v_∞ denote the valuation which is the order of vanishing at infinity, so that $v_\infty(1/T) = 1$. We will then consider the following process analogous to the above:

$$k \xrightarrow[\left(\substack{\text{with respect to}\\ \text{the valuation } v_\infty}\right)]{\text{completion}} K \xrightarrow[\text{and completion}]{\text{algebraic closure}} \mathbf{C}_\infty \twoheadrightarrow \mathbf{C}_\infty/L \xrightarrow{\sim} \mathbf{C}_\infty$$

where $L \subset C_\infty$ is a lattice, and the last isomorphism will be defined later. The inclusion $A \coloneqq \mathbf{F}_r[T] \subset k$ gives $\mathbf{C}_\infty$ the structure of an A-module. The resulting $\mathbf{C}_\infty$, with its extra A-module structure, is what is called a *Drinfel′d module*.

In this talk, we will only give the first, simplest example of this process, when $L = A$. The $\mathbf{Q}$-analogue of this would be taking $L = \mathbf{Z}$ in the process above, in which case the last isomorphism is replaced by the exponential map

$$\exp(2\pi i \cdot -) \colon \mathbf{C}/\mathbf{Z} \xrightarrow{\sim} \mathbf{C}^*.$$

For $n \in \mathbf{Z}$, the module structure $z \mapsto nz$ on $\mathbf{C}/\mathbf{Z}$ translates to the n-power map $z \mapsto z^n$. In the function field case, we take $L = A$, and will construct an isomorphism

$$e_C \colon \mathbf{C}_\infty/A \xrightarrow{\sim} \mathbf{C}_\infty.$$

For $a \in A$, the map $x \mapsto ax$ on $\mathbf{C}_\infty/A$ translates to $x \mapsto C_a(x)$ for some map C_a to be defined later. This mapping $a \mapsto C_a$ gives the A-module structure on $\mathbf{C}_\infty$, which we will call the *Carlitz module*.

Our goal is therefore the following:

Goal 1.1. Construct a surjective map $e_C \colon \mathbf{C}_\infty \twoheadrightarrow \mathbf{C}_\infty$ with kernel A.

The naïve idea is as follows: Take

$$x \longmapsto \prod_{\alpha \in A} (\alpha - x),$$

*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 18, 2017.

which has the required kernel. However, if you plug in $x = 0$, you get

$$\prod_{\alpha \in A} \alpha,$$

which does not really make sense since it does not converge. Instead, a naïve fix is to consider the function

$$x \longmapsto x \prod_{\alpha \in A \smallsetminus \{0\}} \left(1 - \frac{x}{\alpha}\right),$$

which looks like a Weierstrass or Hadamard product, except we are working over a function field instead of over the complex numbers. Surprisingly, this actually works! This is despite the fact that we can't *literally* define it this way; once we formalize this idea, though, it will work.

2 The Carlitz Exponential [Gos96, §§3.1–3.2]

Let us now go step by step. We first start with a finite product. In this case, we do not have to worry about convergence, and we can just look at the resulting sum.

Definition 2.1 [Gos96, Def. 3.1.3]**.** Let $A(d) \coloneqq \{f(T) \in A \mid \deg f(T) < d\}$. Then,

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

which is a finite product. Expanding out the product, we obtain a polynomial that defines a map $\mathbf{C}_\infty \to \mathbf{C}_\infty$.

Note that although any polynomial of degree > 1 is not linear in characteristic zero, the polynomial $e_d(x)$ *does* define an $\mathbf{F}_r$-linear function, since we are working in positive characteristic. To check this linearity property, just use the defining formula, or see [Gos96, Cor. 1.2.2].

Notation 2.2 [Gos96, Def. 3.1.4]**.** Let $i > 0$. We set

$$[i] \coloneqq \prod_{\substack{f \text{ monic, prime} \\ \deg f | i}} f = T^{r^i} - T \in A,$$

which we think of as the A-analogue of $i \in \mathbf{Z}$. The equality is by [Gos96, Prop. 3.1.6.1].

We also define A-analogues of factorials. We set

$$L_i \coloneqq [i] L_{i-1} \qquad \text{and} \qquad L_0 \coloneqq 1,$$

and to play nicely with $\mathbf{F}_r$-linearity, we also consider only r-powers by setting

$$D_i \coloneqq [i] D_{i-1}^r \qquad \text{and} \qquad D_0 \coloneqq 1.$$

We can then write down an expression for $e_d(x)$ as a sum.

Theorem 2.3 (Carlitz [Gos96, Thm. 3.1.5])**.** *We have*

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

There are two proofs of this, of which we will do the easier one. The other proof uses Moore determinants; see [Gos96, p. 45]. Note that the coefficients look a lot like binomial coefficients.

Proof [Gos96, pp. 46–47]. We will show the following recurrence relation:

$$e_d(x) = \big(e_{d-1}(x)\big)^r - (D_{d-1})^{r-1} \cdot e_{d-1}(x). \tag{2.1}$$

Since both sides of this equation are monic polynomials of the same degree, it suffices to show that they have the same set of zeroes. The left-hand side is

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

which has zeroes $A(d)$. To check that the right-hand side also has zeroes $A(d)$, we first note that any $\alpha \in A(d-1)$ is already a zero by definition of $e_{d-1}(x)$. One can check that plugging in $\alpha \in A(d) \smallsetminus A(d-1)$ makes the right-hand side vanish as well. Once we have the recurrence relation (2.1), the theorem follows by induction on d. $\square$

So far, we had an expression with $(x-\alpha)$'s. We saw before that we actually wanted factors like $(1 - \frac{x}{\alpha})$ to show up, so it looks like we should just divide by the product of all $\alpha \in A(d) \smallsetminus \{0\}$ to obtain

$$x \prod_{\alpha \in A(d) \smallsetminus \{0\}} \left(1 + \frac{x}{\alpha}\right) = \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \frac{L_d}{(L_{d-j})^{r^j}}, \tag{2.2}$$

where we used the fact $e_d(x) = \prod_{\alpha \in A(d)} (x + \alpha)$ since $\alpha \mapsto -\alpha$ is a bijection on $A(d)$, and the identity

$$\prod_{\alpha \in A(d) \smallsetminus \{0\}} \alpha = (-1)^d \frac{D_d}{L_d},$$

which follows from another calculation using recurrence relations [Gos96, p. 47].

We now pass to the limit $d \to \infty$ in (2.2). Essentially, what we need to do is to control the growth of the coefficient $L_d/(L_{d-j})^{r^j}$ to ensure the series actually converges. To simplify notation, we set

$$\beta_d \coloneqq [1]^{\frac{r^d - 1}{r-1}} \qquad \text{and} \qquad \xi_d \coloneqq \frac{\beta_d}{L_d}$$

so that [Gos96, Lem. 3.2.3]

$$\frac{L_d}{(L_{d-j})^{r^j}} = \frac{\beta_j (\xi_{d-j})^{r^j}}{\xi_d}.$$

One can show [Gos96, Lem. 3.2.1]

$$\xi_d = \prod_{j=0}^{d-1} \left(1 - \frac{[j]}{[j+1]}\right).$$

The limit of this as $d \to \infty$ is

$$\prod_{j=0}^{\infty} \left(1 - \frac{[j]}{[j+1]}\right) =: \xi_* \in K.$$

Theorem 2.4 Carlitz [Gos96, Lem. 3.2.5, Cor. 3.2.6]**.** *For any $x \in \mathbf{C}_\infty$, the series*

$$\frac{1}{\xi_*} \sum_{j=0}^{\infty} (-1)^j \frac{x^{r^j}}{D_j} \beta_j \xi_*^{r^j}$$

converges to an element in $\mathbf{C}_\infty$, and is equal to

$$x \prod_{\alpha \in A \smallsetminus \{0\}} \left(1 - \frac{x}{\alpha}\right).$$

Sketch of Proof. By Theorem 2.3 and (2.2), we have

$$
\begin{aligned}
x \prod_{\alpha \in A(d) \setminus \{0\}} \Bigl(1 + \frac{x}{\alpha}\Bigr) &= \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \beta_j \frac{(\xi_{d-j})^{r^j}}{\xi_d} \\
&= \frac{1}{\xi_d} \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \beta_j \bigl((\xi_{d-j} - \xi_*)^{r^j} + \xi_*^{r^j}\bigr) \\
&= \frac{1}{\xi_d} \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \beta_j (\xi_{d-j} - \xi_*)^{r^j} + \frac{1}{\xi_d} \sum_{j=0}^{d} (-1)^j \frac{x^{r^j}}{D_j} \beta_j \xi_*^{r^j}.
\end{aligned}
$$

By calculating v_∞-norms of these two terms, one can show that as $d \to \infty$, the first sum tends to zero [Gos96, Lem. 3.2.4] and the second sum tends to what we wanted. $\square$

We now define the analogue of the exponential function $\exp \colon \mathbf{C} \to \mathbf{C}^*$.

Definition 2.5. The *Carlitz exponential* is

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

Note that $e_C(x)$ is $\mathbf{F}_r$-linear.

Note that the D_j play the role that factorials play in the series expression

$$
\exp(x) = \sum_{j=0}^{\infty} \frac{x^j}{j!}.
$$

We will next show that $e_C(x)$ is an entire function. This will follow from Theorem 2.4 by putting all the coefficients inside x^{r^j}. There is a clean way to do this: letting $\xi \coloneqq \lambda \xi_*$ for λ the $(r-1)$st root of $-[1]$ in $\overline{K} \subset \mathbf{C}_\infty$, we have

$$
\xi^{r^j - 1} = \lambda^{r^j - 1} \cdot \xi_*^{r^j - 1} = \bigl(-[1]\bigr)^{\frac{r^j - 1}{r-1}} \xi_*^{r^j - 1} = (-1)^j \cdot \beta_j \xi_*^{r^j - 1},
$$

where we note

$$
(-1)^{\frac{r^j - 1}{r-1}} = (-1)^{r^{j-1} + r^{j-2} + \cdots + 1} = (-1)^j
$$

trivially in characteristic two (since $1 = -1$), and otherwise since there are j terms in $r^{j-1} + r^{j-2} + \cdots + 1$, each of which is odd. Now the expression in Theorem 2.4 can be rewritten using $e_C(x)$ as

$$
x \prod_{\alpha \in A \setminus \{0\}} \Bigl(1 - \frac{x}{\alpha}\Bigr) = \sum_{j=0}^{\infty} \frac{x^{r^j}}{D_j} \bigl((-1)^j \beta_j \xi_*^{r^j - 1}\bigr) = \frac{1}{\xi} e_C(\xi \cdot x).
$$

This is the map we were seeking from the very start.

3 The Carlitz Module [Gos96, §3.3]

We have defined a map

$$
\begin{aligned}
\mathbf{C}_\infty &\longrightarrow \mathbf{C}_\infty \\
x &\longmapsto \frac{1}{\xi} e_C(\xi \cdot x)
\end{aligned}
$$

which is entire, hence surjective [Gos96, Rem. 3.3.6.2]. Thus, we get the isomorphism

$$
\mathbf{C}_\infty / A \xrightarrow{\sim} \mathbf{C}_\infty
$$

that we were looking for. For $a \in A$, there is an action $x \mapsto ax$, which gives an action on the other side:

$$e_C(ax) = C_a(e_C(x)).$$

We want to write down C_a explicitly. We first write down what $e_C(Tx)$ is.

Proposition 3.1 [Gos96, Prop. 3.3.1]**.** *For all $x \in \mathbf{C}_\infty$, we have $e_C(Tx) = Te_C(x) + (e_C(x))^r$.*

Proof. We have

$$e_C(Tx) - Te_C(x) = \sum_{j=0}^{\infty} (T^{r^j} - T)\frac{x^{r^j}}{D_j} = \sum_{j=0}^{\infty} \frac{[j]}{D_j} x^{r^j} = \sum_{j=1}^{\infty} \frac{x^{r^j}}{(D_{j-1})^r} = \big(e_C(x)\big)^r. \qquad \square$$

Using this, one can show the following:

Corollary 3.2 [Gos96, Cor. 3.3.2]**.** *For $x \in \mathbf{C}_\infty$ and $a \in A$ where $\deg a = d$, we can write*

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

for some $C_a^{(j)} \in A$.

Definition 3.3. Let $C_a^{(j)}$ be as in Corollary 3.2. Let $\tau(x) = x^r$ be the generating $\mathbf{F}_r$-linear polynomial. Then, we set

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

Finally, we state the following:

Theorem 3.4 [Gos96, Thm. 3.3.4]**.** *The map*

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

where $k\{\tau\}$ is a (non-commutative) ring under $+$ and composition, is an injective map of $\mathbf{F}_r$-algebras.

Proof. The map is injective since the coefficient of τ^0 is a. To check that $C_{ab} = C_a \circ C_b$, one uses the relation $e_C(ax) = C_a(e_C(x))$. $\square$

Finally, we can do what we advertised at the beginning:

Definition 3.5. The *Carlitz module* is the map

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

Next week, we will talk about how to compute these things and how to work with them more explicitly.

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.