Drinfel′d Modules: Elliptic Modules

Ashwath Rabindranath*

September 29, 2017

We follow [Dri75, §§2–3] and parts of [Poo17]. The algebraic approach to elliptic modules is contained in [Dri75, §2], while [Dri75, §3] describes the analytic approach. We will focus more on the former, but will sketch some things from the latter afterward.

1 Algebraic approach [Dri75, §2]

Let B be a commutative ring of characteristic $p > 0$, and consider the *Frobenius endomorphism*

$$\begin{aligned} \tau\colon B &\longrightarrow B \\ t &\longmapsto t^p \end{aligned}$$

which, in particular, is an endomorphism of additive groups. The multiplication by b endomorphism

$$\begin{aligned} \cdot b\colon B &\longrightarrow B \\ t &\longmapsto tb \end{aligned}$$

is also an additive endomorphism. These endomorphisms generate $B\{\tau\}$, the ring of *additive polynomials*, whose elements are polynomials in τ over B with the usual additive structure, but with a product structure given by composition, e.g., $\tau \cdot b = b^p \cdot \tau$.

There are two maps relating B to $B\{\tau\}$:

$$\begin{aligned} \epsilon\colon B &\longrightarrow B\{\tau\} \\ b &\longmapsto \cdot b \end{aligned} \qquad\qquad \begin{aligned} D\colon B\{\tau\} &\longrightarrow B \\ \sum_{i=0}^{n} b_i\tau^i &\longmapsto b_0 \end{aligned}$$

We will also fix the following notation:

Notation 1.1. We denote by k a global field of characteristic p, and fix a place ∞ of k. The completion of k at a place v will be denoted k_v. There is a normed absolute value $\lvert\cdot\rvert_v$ corresponding to this place v; when $v = \infty$, we will denote $\lvert\cdot\rvert_\infty$ by $\lvert\cdot\rvert$. Finally, we set

$$A = \bigl\{x \in k \bigm| \lvert x\rvert_v \le 1 \text{ for all } v \ne \infty\bigr\},$$

and denote by A_v the completion of A at $v \in \operatorname{Spec} A$.

Now fix an A-field $i\colon A \to K$. Recall that the pullback $i^*(\operatorname{Spec} K) \in \operatorname{Spec} A$ is called the *characteristic* of the field K, and i is an embedding if and only if we have *generic characteristic*.

We can now define elliptic modules over A. Note that these are now known as *Drinfel′d modules*.

Definition 1.2. An *elliptic A-module* over K is a homomorphism

$$\phi\colon A \longrightarrow K\{\tau\}$$

such that $i = D \circ \phi$, but $\phi \ne \epsilon \circ i$.

*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 30, 2017.

The second condition in Definition 1.2 makes the notion non-trivial. These modules are the main object of study in this seminar.

Definition 1.3. There is a *degree map* $\deg\colon K\{\tau\} \to \mathbf{Z}$, where

$$\deg\left(\sum_{i=0}^{n} a_i \tau^i\right) = p^n$$

when $a_n \neq 0$, and $\deg 0 = 0$.

Proposition 1.4 [Dri75, Prop. 2.1(a)]**.** *ϕ is an imbedding.*

Proof. If the kernel of ϕ is nonzero, then it must be maximal, since $K\{\tau\}$ is a domain and A is one-dimensional. Then, the image of ϕ is a subfield of K, i.e., $\operatorname{Im}\phi \subset \epsilon(K)$, which implies $\phi = \epsilon \circ i$, contradicting the second condition in Definition 1.2. □

The following relates the degree to the absolute value associated to the place ∞.

Proposition 1.5 [Dri75, Prop. 2.1(b)]**.** *There exists $d > 0$ such that $\deg\phi(a) = |a|^d$ for all $a \in A$.*

Proof. The proof is just checking a bunch of little details.

- $\deg(ab) = \big(\deg\phi(a)\big)\big(\deg\phi(b)\big)$ (multiplication of τ's works well, even if the ring is non-commutative);
- $\deg\big(\phi(a+b)\big) \leq \max\big\{\deg\phi(a), \deg\phi(b)\big\}$;
- $\deg\phi(a) = 0$ if and only if $a = 0$;
- $\deg\phi(a) \geq 1$ for $a \neq 0$;
- $\deg\phi(a) > 1$ for some $a \in A$.

This means $\deg \circ \phi$ gives a nontrivial absolute value on k. This absolute value is not a finite place since $\operatorname{Im}\phi \not\subset \epsilon(K)$ (see the proof of Proposition 1.4), hence $\deg\phi(a) = |a|^d$. □

Definition 1.6. The number d in Proposition 1.5 is the *rank* of the elliptic A-module ϕ.

We now construct an example of an elliptic A-module when A is the polynomial ring over a finite field.

Example 1.7. Let $A = \mathbf{F}_q[x]$, and let K be its function field. Let $\phi|_{\mathbf{F}_q} = \epsilon \circ i|_{\mathbf{F}_q}$, and let

$$\phi(x) = \sum_{i=0}^{d} a_j \tau^{j \log_p q}$$

for some $a_j \in K$. If $d \geq 1$ and $a_d \neq 0$, then the rank of ϕ is d.

In this manner, we can give the function field $K = \mathbf{F}_q(x)$ an interesting structure as a module over $A = \mathbf{F}_q[x]$, and in general, elliptic modules allow us to put interesting A-module structures on A-fields K.

Theorem 1.8 [Dri75, Cor. to Prop. 2.2]**.** *The rank of an elliptic A-module is a positive integer.*

We outline the proof of Theorem 1.8 first. First, we look for certain finite subgroups of the algebraic clousre of K, given by the roots of a polynomial $\phi(a)$ for suitable $a \in A$, thought of as a polynomial with variable τ. We can then count the number of roots of $\phi(a)$ in multiple ways, forcing d to be a positive integer.

Proof. Let $\beta \in \operatorname{Spec} A$ such that $\beta \neq i^*(\operatorname{Spec} K)$, i.e., such that β is not the characteristic of K. Since A is a Dedekind domain, it has a class number h, and so $\beta^h = (a)$ is a principal ideal. Now let $\overline{K}$ be the algebraic closure of K, and consider the finite subgroup of roots of $\phi(a)$, which we denote by $\phi[a] \subset \overline{K}$. Note that $\#\phi[a] = p^{d \deg a}$. On the other hand,

$$\phi[a] \simeq \bigoplus_{i=1}^{t} A/\beta^{e_i},$$

hence a counting argument shows that $e_i = h$ and $t = d$. This forces d to be an integer. □

We pause to connect elliptic modules to the material we have been covering so far in this seminar.

Example 1.9 (Carlitz modules)**.** In the situation of Example 1.7, let

$$\phi(x) = x + \tau.$$

Since $\phi(a) = C_a$ matches the homomorphism defining a Carlitz module, we see that Carlitz modules are examples of rank one elliptic A-modules.

We will see later that elliptic curves are analogous to rank two elliptic A-modules.

Definition 1.10 (Morphisms)**.** Let $\phi\colon A \to K\{\tau\}$ and $\psi\colon A \to K\{\tau\}$ be two elliptic A-modules. Then, a morphism $\phi \to \psi$ is an element $P \in K\{\tau\}$ such that $\phi_a P = P\psi_a$ for all $a \in A$.

If $P \neq 0$, then we say that P is an *isogeny* and that the elliptic modules are *isogenous*.

Following [Poo17, Def. 3.8], if we think about $K\{\tau\}$ as the endomorphisms of $\mathbf{G}_a$, then we can think of a morphism of elliptic modules as an endomorphism P of $\mathbf{G}_a$ making the diagram

$$\begin{tikzcd} \mathbf{G}_a \arrow[r, "\phi_a"] \arrow[d, "P"'] & \mathbf{G}_a \arrow[d, "P"] \\ \mathbf{G}_a \arrow[r, "\psi_a"] & \mathbf{G}_a \end{tikzcd}$$

commute.

Proposition 1.11. *Isogenous modules have the same rank.*

Proof. We have $(\deg P)|a|^{\operatorname{rank}\phi} = |a|^{\operatorname{rank}\psi} \cdot \deg P$, hence $\operatorname{rank}\phi = \operatorname{rank}\psi$. □

For elliptic curves, every isogeny has a dual; one can prove the same statement for elliptic modules:

Fact 1.12 (Dual isogenies [Dri75, Cor. to Prop. 2.3])**.** *Every isogeny has a dual, i.e., can be composed with another isogeny to obtain an endomorphism which is multiplication by some nonzero $a \in A$.*

We will not prove this, since it is a bit tangential to what we are doing. Proving Fact 1.12 takes a bit of work: The idea is that you want to understand the structure of the torsion points when multiplying by an element $a \in A$, and thereby understand the kernel of these isogenies. You can then characterize what these kernels can or can't be. One of the characterizations is that there is a morphism that goes in the other direction whose composition is multiplication by an element $a \in A$; you can then check that this is an isogeny. The a that shows up in Fact 1.12 can then be thought of as the degree of the isogeny.

2 Analytic approach [Dri75, §2]

We adopt the same notation as in Notation 1.1. In addition, we denote k_∞ to be the completion of k at ∞, and let L be a finite extension of k_∞ that is also a A-field with separable closure L^s.

Definition 2.1. A *lattice over L* is a finitely generated discrete A-submodule in L^s that is invariant under the Galois group $\operatorname{Gal}(L^s/L)$. If Γ_1, Γ_2 are two lattices of dimension d, then a morphism $\phi\colon \Gamma_1 \to \Gamma_2$ is a number $\alpha \in L^s$ such that $\alpha\Gamma_1 \subset \Gamma_2$.

This is like the usual notion of a lattice in $\mathbf{C}$.

Theorem 2.2 [Dri75, Prop. 3.1]**.** *The category of elliptic A-modules of rank d over L is equivalent to the category of lattices of dimension d over L.*

The crux of the argument relies on constructing a surjective, k-linear map $e(z)\colon L \to L$ with kernel Γ, inducing a bijection

$$e(z)\colon L/\Gamma \xrightarrow[\text{analytic}]{\sim} L$$

that is similar to the Carlitz exponential from before. This map is defined as

$$e(z) = z \prod_{\substack{\gamma \in \Gamma \\ \gamma \neq 0}} \left(1 - \frac{z}{\gamma}\right).$$

You can then prove the following, which would take some time (see [Poo17, Thm. 2.2]):

1. Uniqueness: use the Weierstrass preparation theorem;
2. Convergence;
3. Surjectivity;
4. k-linearity: $e(x + y) = e(x) + e(y)$;
5. $e(cx) = c \cdot e(x)$ for all $c \in k$;
6. $\ker(e) = \Gamma$.

The proofs are similar to the material about Carlitz modules we have already seen.

Now given such an isomorphism

$$L/\Gamma \xrightarrow[e]{\sim} L,$$

we obtain an "exotic" A-module structure on L: for $a \in A$, the action of a on L is given by

$$\begin{tikzcd} L/\Gamma \arrow[r, "\cdot a"] \arrow[d, "e"', "\wr"] & L/\Gamma \arrow[d, "e"', "\wr"] \\ L \arrow[r, dashed, "\phi_a"] & L \end{tikzcd}$$

Claim 2.3 [Poo17, Prop. 2.3]**.** *ϕ_a is a polynomial.*

Proof. First, $\ker(a) = (a^{-1}\Gamma)/\Gamma \cong \Gamma/a\Gamma$. But Γ is an A-module, hence

$$\Gamma/a\Gamma \cong (A/aA)^r$$

is a finite group of order $|a|^r$. The kernel of ϕ_a is just the image of the kernel upstairs $e(a^{-1}\Gamma/\Gamma)$, and

$$\phi_a(z) = az \prod_{\substack{t \in a^{-1}\Gamma/\Gamma \\ t \neq 0}} \left(1 - \frac{z}{e(t)}\right)$$

One needs to check that $\phi_a(e(z))$ and $e(az)$ have the same zeroes, and that the coefficient of z is the same. $\square$

This shows that you can reconstruct these polynomials ϕ_a from the exotic A-module structure.

References

[Dri75] V. G. Drinfel′d. "Elliptic modules." Trans. by M. B. Nathanson. *Math. USSR-Sb.* 23.4 (1974), pp. 561–592. DOI: 10.1070/SM1974v023n04ABEH001731. MR: 0384707.

[Poo17] B. Poonen. *Introduction to Drinfeld modules.* Notes from a four lecture mini-course. Version from May 17, 2017. URL: https://math.mit.edu/~poonen/papers/drinfeld.pdf.