Notes on the arithmetic of Drinfeld modules

Dino Festi

These are the notes taken during Lenny Taelman's seminar about Drinfeld Modules, given in Besançon in the autumn 2013. All the useful information is due to Lenny Taelman, all the mistakes are due to me.

Besides the mistakes, I also introduced one exercise for the reader: find (and possibly fix) as many mistakes as you can and let me know.

Finally, I would like to thank Lenny Taelman and Christophe Debry for their corrections, comments and remarks, helping me in improving these notes.

1 Background

Let C be a smooth geometrically irreducible projective curve over the finite field $\mathbb{F}_q$, and let's fix a closed point on C, call it ∞, then we will denote by:
$F := \mathbb{F}_q(C)$, the function field of the curve;
$A := \mathcal{O}(C - \{\infty\}) = \{f \in F \ : \ f \text{ has no poles outside } \infty\}$;
F_∞ the completion of F at ∞.

Example 1.1. The first (non-trivial) example we can consider is given by $C = \mathbb{P}^1(x, y)$, $\infty = (1 : 0)$.
Then we have $F = \mathbb{F}_q(t)$ with $t = \frac{x}{y}$, $A = \mathbb{F}_q[t]$ and $F_\infty = \mathbb{F}_q((t^{-1}))$.

From the above example we can draw a parallelism with the number theory: F plays the same role as $\mathbb{Q}$ in number theory, and hence A is the analogue of $\mathbb{Z}$ and F_∞ of $\mathbb{R}$. Following this analogy we will see that Drinfeld modules of rank 1 are analogous to the group scheme $\mathbb{G}_m$ and Drinfled modules of rank 2 are analogous to elliptic curves. Most of the differences

that break the analogy come from the fact that $|\bar{F}_\infty : F_\infty|$ is infinite while $|\bar{\mathbb{R}} : \mathbb{R}|$ is finite.

Proposition 1.2. *Using the notation set at the beginning of the section, we have that the following equality holds:*

$$A^\times = \mathbb{F}_q^\times.$$

(Proof to be added)

Proposition 1.3. *Keeping the same notation as the beginning of the section, we have that the following statements hold:*
i) $A \subseteq F_\infty$ *is discrete;*
ii) the quotient F_∞/A *is compact.*

(Proof to be added)

2 Algebraic theory of Drinfeld modules

Let K be a field, and consider $f \in K[X]$; we say that f is *additive* if

$$f(X+Y) = f(X) + f(Y).$$

Proposition 2.1. *Let* K *be a field, and* $f \in K[X]$*, then the following statements hold:*
i) if char $K = 0$*, then* f *is additive if and only if*

$$f = aX;$$

ii) if char $K = p > 0$*, then* f *is additive if and only if*

$$f = a_0X + a_1X^p + \ldots + a_dX^{p^d}.$$

Now suppose that $\mathbb{F}_q$ is a subfield of K and consider $f \in K[X]$; we say that f is $\mathbb{F}_q$–linear if it is additive and for any $\lambda \in \mathbb{F}_q$ we have:

$$f(\lambda X) = \lambda f(X).$$

Proposition 2.2. *Let K be a field containing $\mathbb{F}_q$, and let f be an element of $K[X]$. Then f is $\mathbb{F}_q$–linear if and only if*

$$f = a_0X + a_1X^q + \ldots + a_dX^{q^d}.$$

The $\mathbb{F}_q$–linear polynomials form the ring $K[X]_{\mathbb{F}_q}$, where the sum is the usual sum of polynomials and the product is the composition of polynomials.

It is possible to have a different view of this ring. In order to do this we need to introduce the *twisted polynomial ring* over K, denoted by $K\{\tau\}$.
We define $K\{\tau\}$ as the set

$$\{ \sum_{i=0}^{d} a_i\tau^i \mid d \in \mathbb{Z}_{\geq 0}\,,\ a_i \in K \}\,,$$

endowed with the usual sum of polynomial as sum but with the product given by the following rule:

$$a^q\tau = \tau a.$$

With these two operations $K\{\tau\}$ turns out to be a (possibly noncommutative) ring.

Remark 2.3. Nevertheless, if $K = \mathbb{F}_q$, then $K\{\tau\}$ is in fact a commutative ring, since $\tau a = a^q\tau = a\tau$.

Example 2.4. For example, multiplying two monomials we get

$$a_i\tau^i \cdot a_j\tau^j = a_i a_j^{q^i}\tau^{i+j}.$$

We can observe how τ simply represents the operation of raising to the q–th power.

Proposition 2.5. *The rings $K\{\tau\}$ and $K[X]_{\mathbb{F}_q}$ are isomorphic via the isomorphism*

$$\sum a_i\tau^i \mapsto \sum a_iX^{q^i}.$$

Definition 2.6. Recalling the definition of A given at the beginning, we define an *A–field* to be a pair (K, i), where K is a field and $i\colon A \to K$ is a ring homomorphism.
Let (K, i) be an A–field; a *Drinfeld A–module over (K, i)* is a ring homomorphism

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

such that $\phi(a) = i(a) + x_1\tau + x_2\tau^2 + \ldots$ for any $a \in A$.

Example 2.7. We give some examples of Drinfeld modules:

i) Take $\phi = i$, then $\phi(a) = i(a)$. This is the trivial Drinfel module and sometimes it is not even considered a Drinfeld module;

ii) let $A = \mathbb{F}_q[t]$ and consider the ring homomorphism $\phi\colon \mathbb{F}_q[t] \to K\{\tau\}$ defined by
$$t \mapsto i(t) + x_1\tau + \ldots + x_d\tau^d.$$
Notice that any choice of the x_i's gives a different Drinfeld A–module.

Exercise 2.8. Give an example of an A that is not isomorphic to $\mathbb{F}_q[t]$ and of a non trivial A–module.

3 Functor of points of a Drinfeld module

Let $\phi\colon A \to K\{t\}$ be a Drinfeld A–module over K, then we define the functor
$$E_\phi\colon K\text{–alg} \to A\text{–mod}$$
by sending a commutative K–algebra R to an A–module $E_\phi(R)$, where $E_\phi(R)$ is the A–module given by considering $(R, +)$ as abelian group with the following action of A:
$$a * r = \phi(a)(r),$$
for any $a \in A$ and $r \in R$.

Example 3.1. Consider the following Drinfeld $\mathbb{F}_q[t]$–module
$$\phi\colon \mathbb{F}_q[t] \to K\{\tau\}$$
with $\phi(t) = i(t) + x_1\tau + \ldots + x_d\tau^d$.
Then the A–module $E_\phi(K\{\tau\})$ is given by the following action of $\mathbb{F}_q[t]$ on K:
$$t * y = i(t)y + x_1y^q + \ldots + x_dy^{q^d},$$
for any element $y \in K$.

We give some notation: let M be an A–module, and $a \in A$, then we define the *a–torsion submodule* of M as the set (infact submodule)
$$M[a] := \{m \in M \mid am = 0\ \}.$$

Theorem 3.2 (Drinfeld)**.** *Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld A–module over K, then there is a unique $r \in \mathbb{Z}_{\geq 0}$ such that for any $a \in A$ with $i(a) \neq 0$ one has that*

$$E_\phi(\bar{K})[a] \cong \left(\frac{A}{aA}\right)^r.$$

The r in the theorem is called the *rank* of ϕ. By this theorem we can note the analogy between the a–torsion elements of Drinfeld modules of rank 2, and n–torsion points on elliptic curves.

Exercise 3.3. Assuming Theorem 3.2, show that $\deg_\tau(\phi(t)) = r$, where $\phi\colon \mathbb{F}_q[t] \to K\{\tau\}$ is the Drinfeld module as in Example 3.1.

In order to prove Theorem 3.2 we prove the following two lemmas:

Lemma 3.4. *Let a be an alement in A such that $i(a) \neq 0$, then*

$$\#E_\phi(\bar{K})[a] = q^{\deg_\tau \phi(a)}.$$

(proof to be added)

Lemma 3.5. *There exists a rational r such that*

$$q^{\deg_\tau \phi(a)} = \#\left(\frac{A}{aA}\right)^r$$

for any nonzero $a \in A$.

(proof to be added)

4 Analytic theory of Drinfeld moduels

This section can be seen as the analogue of the study of elliptic curves as complex lattices, although this is a non archimedean context. Recall that a norm $|\cdot|$ on a vector space X is said *non-archimedean* if for any $x, y \in X$ we have that the following holds:

$$|x + y| \leq \max\{|x|, |y|\}.$$

Consider the absolute value $|\cdot|_\infty$ on F_∞, where $|x|_\infty = q^{-v_\infty(x)}$. The absolute value $|\cdot|_\infty$ extends uniquely to the absolute value $|\cdot|_\infty$ on $\bar{F}_\infty$.

Warning: The field $\bar{F}_\infty$ is never complete.

Let S be a subset of $\bar{F}_\infty$; we say that S is *strongly discrete* if S is discrete and the index $|\, F_\infty(S) \,:\, F_\infty \,|$ is finite.
Assume 0 is an element of S, then we define

$$e_S(z) := z \prod_{s \in S} \left(1 - \frac{z}{s}\right).$$

Recall the following fact about non-archimedean analysis:

Fact 4.1. *Let R be a ring with a non-archimedean topology, and let*

$$(f_i \colon X \to R)_{i \in I}$$

be a family of functions.
Then the infinite product $\prod_{i \in I} f_i$ converges if and only if $\lim_{i \in I} f_i = 1$.

Using this we can prove the following proposition:

Proposition 4.2. *Let S be a strongly discrete subset of $\bar{F}_\infty$ and let $e_S(z)$ be the infinite product $z \prod_{s \in S} \left(1 - \frac{z}{s}\right)$, then:*

i) the infinite product e_S converges to the function $e_S \colon \bar{F}_\infty \to \bar{F}_\infty$;
ii) $e_S^{-1}(0) = S$;
iii) the function e_S is surjective.

(proof to be added)

Proposition 4.3. *Let $S \subseteq \bar{F}_\infty$ be strongly discrete, and assume S is also a $\mathbb{F}_q$–vector space.*
Then the function e_S is $\mathbb{F}_q$-linear.

The previous propositions yelds the following short exact sequence of $\mathbb{F}_q$–vector spaces:

$$0 \longrightarrow S \hookrightarrow \bar{F}_\infty \xrightarrow{e_S} \bar{F}_\infty \longrightarrow 0\,.$$

Moreover, we define a A–lattice in $\bar{F}_\infty$ to be a strictly discrete sub–A–module $\Lambda \subseteq \bar{F}_\infty$ (this implies that Λ is projective and finitely generated).

Theorem 4.4 (Drinfeld)**.** *Let $\Lambda \subseteq \bar{F}_\infty$ be a A–lattice, and let a be an element of A. Then there is a unique Drinfled A–module $\phi\colon A \to K\{\tau\}$ making the following diagram commute for any $a \in A$:*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \hookrightarrow & \bar{F}_\infty & \xrightarrow{e_\Lambda} & \bar{F}_\infty & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \phi(a)} & & \\ 0 & \longrightarrow & \Lambda & \hookrightarrow & \bar{F}_\infty & \xrightarrow{e_\Lambda} & \bar{F}_\infty & \longrightarrow & 0 \end{array}$$

with the a in the diagram denoting the multiplication by a.
Moreover we have that $\mathrm{rank}_A\Lambda = \mathrm{rank}(\phi)$.

(Proof to be added)

Remark 4.5. We hence obtain short exact sequence of A–modules:

$$0 \longrightarrow \Lambda \hookrightarrow \bar{F}_\infty \xrightarrow{e_\Lambda} E_\phi(\bar{F}_\infty) \longrightarrow 0\ .$$

Theorem 4.6 (Drinfeld)**.** *Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld A–module, then i) there is a unique function $e_\phi(z) = z + e_1 z + e_2 z^{q^2} + \ldots$ such that the following diagram commutes for any $a \in A$:*

$$\begin{array}{ccc} \bar{F}_\infty & \xrightarrow{e_\phi} & \bar{F}_\infty \\ \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \phi(a)} \\ \bar{F}_\infty & \xrightarrow{e_\phi} & \bar{F}_\infty \end{array}$$

ii) The kernel of e_ϕ is a A–lattice of rank $\mathrm{rank}(\phi)$.

Definition 4.7. Let A be the ring $\mathbb{F}_q[t]$, the Carlitz module is the Drinfeld module $\phi\colon A \to K\{\tau\}$ given by

$$t \mapsto i(t) + \tau\ .$$

Exercise 4.8. Show that $e_\phi(z) = z + \frac{z^q}{t^q - t} + \frac{z^{q^2}}{(t^{q^2} - t^q)(t^{q^2} - t)} + \cdots$.

Exercise 4.9. Let ϕ be the Carlitz module defined in 4.7 and f a monic irreducible polynomial in $\mathbb{F}_q[t]$. Show that $E_\phi(\mathbb{F}_q[t]/(f))$ is isomorphic to $\mathbb{F}_q[t]/(f-1)$.

5 Morphisms of Drinfeld modules

Let $\phi_i \colon A \to K\{\tau\}$, with $i = 1, 2$, be two Drinfeld modules. We define the ring of *morphisms of Drinfeld modules* from ϕ_1 to ϕ_2 to be the subring of $K\{\tau\}$ given by

$$\mathrm{Hom}(\phi_1, \phi_2) := \{\psi \in K\{\tau\} \mid \phi_2\psi = \psi\phi_1 \} = \mathrm{Hom}(E_{\phi_1}(-), E_{\phi_2}(-)).$$

Notice that with this definition we can talk about the *category* of Drinfeld modules, and we can summarize the analytic theory of Drinfeld modules (see Chapter 4) in the following theorem:

Theorem 5.1. *There is an equivalence of category between the category of the A–lattices in $\bar{F}_\infty$ of rank r and the category of the Drinfeld A–modules over $\bar{F}_\infty$ of rank r.*

Given a Drinfeld module ϕ, we define its ring of endomorphisms $\mathrm{End}(\phi)$ to be the ring $\mathrm{Hom}(\phi, \phi)$. The following theorem gives some information about the rank of $\mathrm{End}(\phi)$.

Theorem 5.2. *Let $\phi \colon A \to K\{\tau\}$ be a Drinfeld A–module of rank r, then:*
i) $\mathrm{End}(\phi)$ *is a finitely generated projective A–module of rank less or equal than r^2;*
ii) if the ring homomorphism $i \colon A \to K$ is injective then $\mathrm{End}(\phi)$ *is commutative and its rank is less or equal than r.*

Exercise 5.3. Find an example of a Drinfeld module ϕ having rank equal to 2 and whose endomorphism ring, $\mathrm{End}(\phi)$, has rank equal to 4.

6 Drinfeld modules over Finite Fields

Let E be an elliptic curve defined over a finite field K; a very classic problem related to E is to compute the number of its rational points. Let now $\phi \colon A \to K\{\tau\}$ be a Drinfeld A–module over K, where K is a finite A–field. If we keep in mind the parallelism we pointed out at the beginning between Drinfeld modules (of rank 2) and elliptic curves, asking the cardinality of the finite A–module $E_\phi(K)$ seems a licit question. On the contrary of the elliptic curves, in this case the answer is trivial: the cardinality $E_\phi(K)$ is always equal to the cardinality of K.

For a more challenging question we introduce the notion of *Fitting ideals*. Let A be a Dedekind domain and let M be a finite A–module, then there is a (finite) family $(I_i)_i$ of ideals of A such that $M \cong \oplus A/I_i$. We define the Fitting ideal of M in A to be the ideal

$$\mathrm{Fitt}_A M := \prod_i I_i \ \subseteq \ A \ .$$

Here is a list of some facts about Fitting ideals.

Facts 6.1. *Using the previous notation, the following statements hold:*
i) The Fitting ideal $\mathrm{Fitt}_A M$ *is independent of the decomposition of* M*;*
ii) the cardinality of M *is equal to the cardinality of* $A/\mathrm{Fitt}_A M$*;*
iii) if we have the following short exact sequence of finite A*–modules*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

then we have that

$$\mathrm{Fitt}_A M_2 = (\mathrm{Fitt}_A M_1)(\mathrm{Fitt}_A M_3).$$

Remark 6.2. With the anlogous definition for finite modules we would find that if M is a finite abelian group then $\mathrm{Fitt}_{\mathbb{Z}} M = (\#M)\mathbb{Z}$.

Our goal is now to get more information about the ideals $\mathrm{Fitt}_A K$ and $\mathrm{Fitt}_A E_\phi(K)$.

Theorem 6.3 (Gekeler, Debry)**.** *Let* $\phi\colon A \to K\{\tau\}$ *be a Drinfeld module of positive rank, with* K *a finite* A*-field, then*
i) the ideal $\mathrm{Fitt}_A E_\phi(K)$ *is principal;*
ii) the ideal $\mathrm{Fitt}_A K$ *is principal;*
iii) there is a unique element $u \in \hat{\mathcal{O}}_\infty^\times$ *such that* $u \equiv 1 \ mod\ \mathfrak{m}_\infty$ *and* $\mathrm{Fitt}_A K = u \cdot \mathrm{Fitt}_A E_\phi(K)$*.*

In order to prove this theorem we need to introduce the notion of K_0 group of the finitely generated A–modules.
Let fgA–mod be the category of the finitely generated A–modules, then we define the group

$$K_0(\text{fgA–mod})$$

to be the abelian group generated by the isomorphism classes of finitely generated A–modules M modulo the relation

$$[M_2] = [M_1] + [M_3]$$

for any short exact sequence

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \ .$$

Example 6.4. Let K be a field. It is easy to see that if fdK–vs denotes the category of the finite dimensional K–vector spaces, then

$$K_0(\text{fdK–vs}) \cong \mathbb{Z}$$

via the group isomorphism $[V] \mapsto \dim V$.
Also, if K–vs denotes the category of the K–vector spaces (without any restriction on their dimension) then it turns out that

$$K_0(\text{K–vs}) \cong 0.$$

Proposition 6.5. *Let* $\text{FracId}(A)$ *denote the group of fractional ideals of* A *and* fin A–mod *the category of finite* A*–modules. Then the group* $K_0(\text{fin A–mod})$ *is isomorphic to* $\text{FracId}(A)$ *via the group isomorphism*

$$[M] \mapsto \text{Fitt}_A M \ .$$

Furthermore, we have the following exact commutative diagram of groups:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \text{FracId}(A) & \xrightarrow{\sim} & K_0(\text{fin A–mod}) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \text{Pic}\, A & \longrightarrow & K_0(\text{fgA–mod}) & \xrightarrow{\text{rk}} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

where $\text{rk}\colon [M] \mapsto \text{rk}_A M$,
the horizontal map from $\text{FracId}(A)$ *sends the ideal* I *to the class* $[A/I]$ *in* $K_0(\text{fin A–mod})$,
the horizontal map from $\text{Pic}\, A$ *sends the class* $[I]$ *to the class* $[A/I]$ *in* $K_0(\text{fgA–mod})$.

Corollary 6.6. *Let*

$$0 \longrightarrow P \longrightarrow P \longrightarrow M \longrightarrow 0$$

be a short exact sequence of finitely generated A*–modules.*
Then M *is finite and* $\text{Fitt}_A M$ *is principal.*

(Proof of Thorem 6.3 to be added)

Consider now a finite A–field K and let $\phi\colon A \to K\{\tau\}$ be a Drinfeld module of positive rank. We can then give $K\{\tau\}$ the structure of a left A–module, by defining the following multiplication:

$$a * f \ = \ \phi(a) \cdot f \ ,$$

for any $a \in A$ and $f \in K\{\tau\}$.

Proposition 6.7. *With the above notation, $K\{\tau\}$ is a finitely generated A–module.*
In fact, it is free of rank $|K : \mathbb{F}_q| \cdot \mathrm{rk}\phi$.

(Proof to be added)

Theorem 6.3 is a very important theorem. The first two points tell us that the ideals $\mathrm{Fitt}_A E_\phi(K)$ and $\mathrm{Fitt}K$ are principals.
Theorem 6.3, in its third point, also tells us that there is a unique element $u \in \hat{\mathcal{O}}_\infty^\times$ such that $u \equiv 1 \bmod \mathfrak{m}_\infty$ and $\mathrm{Fitt}_A K = u \cdot \mathrm{Fitt}_A E_\phi(K)$.
Notice that, going on with the parallelism between Drinfeld modules (of rank 2) and Elliptic curves, the u in 6.3.*iii* is the analogue of the quantity $\frac{q}{\#E(\mathbb{F}_q)} \in \mathbb{R}$ for an elliptic curve E defined over the finite field $\mathbb{F}_q$.
Exercise 6.8. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. Show that

$$u = L(E, s = 1).$$

Theorem 6.9 (Gekeler)**.** *Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld module of positive rank $r > 0$, with K a finite A-field. Let u be as in 6.3.iii . Then we have that the following inequality holds:*

$$|1 - u|_\infty \leq (\#K)^{-\frac{1}{r}}.$$

Remark 6.10. Notice that if the rank equals $r = 2$ then, applying the theorem, we get that $|1 - u|_\infty \leq \frac{1}{\sqrt{\#K}}$, that is exactly analogous to the Hasse-Weil bound for Elliptic curves.

To every elliptic curve is attached a particular L function. The parallelism between elliptic curves and Drinfeld modules suggest us that we could define an analogous object for a Drinfeld Module, and Theorem 6.3 gives us exactly what we need.
Let $\phi\colon A \to K\{\tau\}$ be a Drinfeld module of positive rank, with K a finite A-field and let u be as in 6.3.*iii* . Then we define

$$L(\phi/K, 1) := u.$$

Corollary 6.11. *Let k be a finite extension of the function field F and $\mathcal{O}_k$ the integral closure of A in k.*
Let $\phi\colon A \to k\{\tau\}$ be a Drinfeld A–module.
Let $\tilde{\phi}\colon A \to \mathcal{O}_k\{\tau\}$ be a model of ϕ.
Then

$$L(\tilde{\phi}/\mathcal{O}_k, 1) = \prod_{\mathfrak{m} \subseteq \mathcal{O}_k} L(\tilde{\phi} \bmod \mathfrak{m}, 1) \in F_\infty,$$

where $\mathfrak{m}$ runs through all the maximal ideals of $\mathcal{O}_K$.

7 Drinfeld modules over global fields

In this section we develop the theory of Drinfeld modules as in the setting of Corollary 6.11, that is, Drinfeld modules over global fields.

Let k be a finite extension of the function field F and $\mathcal{O}_k$ the integral closure of A in k. Let $\phi\colon A \to \mathcal{O}_k\{\tau\}$ be a Drinfeld A–module over k.
If $\mathfrak{m}$ is a maximal ideal of $\mathcal{O}_k$ then we denote by K the field $\mathcal{O}_k/\mathfrak{m}$ and we define the Drinfeld A–module $\bar{\phi}$ as

$$\bar{\phi} = \phi \bmod \mathfrak{m}\colon A \to K\{\tau\}.$$

Recall that by Theorem 6.3.*iii* there is a unique element $u \in \hat{\mathcal{O}}_\infty^\times$ such that $u \equiv 1 \bmod \mathfrak{m}_\infty$ and $\mathrm{Fitt}_A K = u \cdot \mathrm{Fitt}_A E_{\bar{\phi}}(K)$.
Notice that the previous equality is an equality of A–lattices of rank 1 in F_∞.
Also recall that we defined $L(\phi/K, 1) := u$ and that by Corollary 6.11 we have that

$$L(\phi/\mathcal{O}_k, 1) = \prod_{\mathfrak{m}\subseteq\mathcal{O}_k} L(\phi \bmod \mathfrak{m}, 1) \in F_\infty.$$

Example 7.1. Consider the Carlitz module (see Definition 4.7)

$$\phi\colon A \to A\{\tau\},\ t \mapsto t + \tau,$$

where $A = \mathbb{F}_q[t] = \mathcal{O}_k$.
Let $\mathfrak{m} \subseteq A$ be a maximal ideal, then there is a monic and irreducible element $f \in A$ such that $\mathfrak{m} = (f)$.
By Exercise 4.9 we have that $E_\phi(A/\mathfrak{m})$ is isomorphic to the ring $A/(f-1)A$.
Then it follows that

$$\mathrm{Fitt}_A E_\phi(A/\mathfrak{m}) = (f-1)A$$

and

$$\mathrm{Fitt}_A A/\mathfrak{m} = fA.$$

Then by Theorem 6.3 there is a unique element $u \in \hat{\mathcal{O}}_\infty^\times = \mathbb{F}_q[[t^{-1}]]^\times$ such that $u \equiv 1 \bmod \mathfrak{m}_\infty$ and $\mathrm{Fitt}_A K = u \cdot \mathrm{Fitt}_A E_{\bar{\phi}}(K)$, and it is $\frac{f}{f-1}$.

It follows that

$$\begin{aligned} L(\phi/A,1) &= \prod_{f \text{ monic and irreducible}} \frac{f}{f-1} \\ &= \prod_{f \text{ monic and irreducible}} \frac{1}{1-f^{-1}} \\ &= \sum_{g \text{ monic}} \frac{1}{g} \\ &= \zeta(1) \in 1 + t^{-1}\mathbb{F}_q[[t^{-1}]]. \end{aligned}$$

Theorem 7.2 (Poonen)**.** *Using the notation at the beginning of the section, we have that*

$$E_\phi(\mathcal{O}_k) \cong T \oplus A^{(\mathbb{N})},$$

where T is a finite A-module.

Remark 7.3. Note that this is quite different from the Mordell-Weil theorem for elliptic curves, in that the rank of $E_\phi(\mathcal{O}_k)$ is infinite. There is however a finiteness theorem, quite similar to the Dirichlet unit theorem, which we explain next.

Consider the Drinfled module $\phi : A \to \mathcal{O}_k\{\tau\}$ and define

$$k_\infty = k \otimes_F F_\infty = \prod_{v|\infty} k_v.$$

Let n be the degree $|k : F|$, then k_∞ is a F_∞–vector space of dimension n. Recalling Theorem 4.6 we have the following diagram:

$$\begin{array}{ccc} k_\infty & \xrightarrow{e_\phi} & E_\phi(k_\infty) \\ \uparrow & & \uparrow \\ e_\phi^{-1}E_\phi(\mathcal{O}_k) & \longrightarrow & E_\phi(\mathcal{O}_k) \end{array}$$

Theorem 7.4 (Taelman)**.** *Keeping the notation above, we have that the following statements hold:*
i) The ring $\mathcal{O}_k$ is an A–lattice in k_∞ of rank n;
ii) The A–module $U(\phi) := e_\phi^{-1}E_\phi(\mathcal{O}_k)$ is an A–lattice on k_∞ of rank n;
iii) The A–module $H(\phi) = \frac{E_\phi(k_\infty)}{e_\phi(k_\infty)+E_\phi(\mathcal{O}_k)}$ is a finite A–module.

Notice that, using the theorem, we get three A–lattices of rank 1 in one-dimensional F_∞–vector space:
i) $\Lambda^n\mathcal{O}_k$ in $\Lambda^n k_\infty$;
ii) $\Lambda^n U(\phi)$ in $\Lambda^n k_\infty$;
iii) $\mathrm{Fitt}_A H(\phi)$ in F_∞.

Conjecture 7.5.

$$\Lambda^n U(\phi) \cdot \mathrm{Fitt}_A H(\phi) = L(\phi, 1) \cdot \Lambda^n \mathcal{O}_k$$

as A–lattices of rank 1 in $\Lambda^n k_\infty$.

Conjecture 7.5 implies the following.

Corollary-Conjecture 7.6.

$$[\mathcal{O}_k] + [H(\phi)] = [U(\phi)]$$

in $K_0(\mathrm{fgA\text{–}mod})$.

Notice that this conjecture is (almost trivially) true if A is a PID.

Theorem 7.7 (Taelman)**.** *Conjecture 7.5 holds for $A = \mathbb{F}_q[t]$.*

Example 7.8. Consider $A = \mathcal{O}_K$ and the Drinfeld A–modules $\phi\colon A \to A\{\tau\}$ given by $t \mapsto t + \tau$.
We have already seen that in this case we have that

$$L(\phi, 1) = \sum_{g \text{ monic}} \frac{1}{g} \in 1 + t^{-1}\mathbb{F}_q[[t^{-1}]].$$

We can explicitely express the map $e_\phi\colon F_\infty \to E_\phi(F_\infty)$ and its formal inverse ℓ_ϕ. Namely:

$$e_\phi\colon z \mapsto z + \frac{z^q}{t^q - t} + \frac{z^{q^2}}{(t^{q^2} - t)(t^{q^2} - t^q)} + \cdots$$

and

$$\ell_\phi\colon z \mapsto z + \frac{z^q}{t - t^q} + \frac{z^{q^2}}{(t - t^q)(t - t^{q^2})} + \cdots .$$

Exercises 7.9. Show that:
i) $e_\phi \circ \ell_\phi = \mathrm{id}_{\mathrm{E}_\phi(\mathrm{F}_\infty)}$ and $\ell_\phi \circ e_\phi = \mathrm{id}_{\mathrm{F}_\infty}$;
ii) the series ℓ_ϕ converges on $\mathbb{F}_q[[t^{-1}]]$;
iii) $e_\phi^{-1} E_\phi(A) = A \cdot \ell_\phi(1)$;
iv) $H(\phi) = 0$;
v) $\mathcal{O}_K = A \cdot 1$;
vi) $\zeta(1) = \ell_\phi(1)$.
Remark 7.10. The formula $\zeta(1) = \ell_\phi(1)$ was already known by Carlitz.

References

[1] Vladimir Gershonovich Drinfel'd. Elliptic modules. *Mathematics of the USSR-Sbornik*, 23(4):561, 1974.

[2] E.-U. Gekeler. Drinfeld moduels. *Enciclopedia of Mathematics*, 2001.

[3] David Goss. *Basic structures of function field arithmetic*, volume 35. Springer, 1998.

[4] G Laumon. Cohomology of drinfeld modular varieties, volumes i et ii. *Cambridge UP*, 1996.