Introduction to Drinfeld modules

Bjorn Poonen

Abstract. Our goal is to introduce Drinfeld modules and to explain their application to explicit class field theory.

Before introducing Drinfeld modules, let us motivate their study by mentioning some of their applications.

1. Applications

- Explicit class field theory for global function fields (just as torsion of $\mathbb{G}_m$ gives abelian extensions of $\mathbb{Q}$, and torsion of CM elliptic curves gives abelian extensions of imaginary quadratic fields). Here, global function field means $\mathbb{F}_p(T)$ or a finite extension.
- Langlands conjectures for GL_n over global function fields (Drinfeld modular varieties play the role of Shimura varieties).
- Modularity of elliptic curves over global function fields: If E over $\mathbb{F}_p(T)$ has split multiplicative reduction at ∞, then E is dominated by a Drinfeld modular curve.
- Explicit construction of curves over finite fields with many points, as needed in coding theory, namely reductions of Drinfeld modular curves, which have easier-to-write-down equations than the classical modular curves.

Only the first of these will be treated in these notes, though we do also give a very brief introduction to Drinfeld modular curves and varieties. We follow [**Hay92**] as primary reference. For many more details about Drinfeld modules, one can consult the original articles of Drinfeld [**Dri74**, **Dri77**] or any of the following: [**DH87**], [**GHR92**], [**Gos96**], [**Lau96**], [**Lau97**], [**GPRG97**], [**Ros02**], [**Tha04**].

2. Analytic theory

2.1. Inspiration from characteristic 0. Let Λ be a discrete $\mathbb{Z}$-submodule of $\mathbb{C}$ of rank $r \geq 0$, so there exist $\mathbb{R}$-linearly independent $\omega_1, \ldots, \omega_r$ such that $\Lambda = \mathbb{Z}\omega_1 + \cdots \mathbb{Z}\omega_r$. It turns out that the Lie group $\mathbb{C}/\Lambda$ is isomorphic to $G(\mathbb{C})$ for some algebraic group G over $\mathbb{C}$, as we can check for each value of r:

2020 *Mathematics Subject Classification.* Primary 11G09; Secondary 11G45, 11R37,

Key words and phrases. Drinfeld module, class field theory, $\mathbb{F}_q$-linear polynomial, Tate module, good reduction, stable reduction, Carlitz module, Hilbert class field, ray class field, Drinfeld modular variety.

The writing of this article was supported in part by National Science Foundation grants DMS-841321, DMS-1601946, and DMS-2101040 and Simons Foundation grants #402472 and #550033.

r	isomorphism of Lie groups	G
0	$\mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{C}$	the additive group $\mathbb{G}_a$
1	$\mathbb{C}/\Lambda \xrightarrow{\sim} \mathbb{C}^\times$ $z \longmapsto \exp(2\pi i z/\omega_1)$	the multiplicative group $\mathbb{G}_m$
2	$\mathbb{C}/\Lambda \xrightarrow{\sim} E(\mathbb{C})$ $z \longmapsto (\wp(z), \wp'(z))$	an elliptic curve E

(The notation $\wp$ denotes the Weierstrass $\wp$-function associated to the lattice Λ; see [**Sil09**, VI.3], for instance.)

Cases with $r > 2$ do not occur, since $[\mathbb{C} : \mathbb{R}] = 2$.

2.2. Characteristic p analogues. What is a good analogue of the above in characteristic p? Start with a smooth projective geometrically integral curve X over a finite field $\mathbb{F}_q$, and fix a closed point $\infty \in X$. Let $\mathscr{O}(X - \{\infty\})$ denote the coordinate ring of the affine curve $X - \{\infty\}$.

Characteristic 0 ring	Characteristic p analogue	Example
$\mathbb{Z}$	$A := \mathscr{O}(X - \{\infty\})$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$K := \operatorname{Frac} A$	$\mathbb{F}_q(T)$
$\mathbb{R}$	$K_\infty :=$ completion at ∞	$\mathbb{F}_q((1/T))$
$\mathbb{C}$	$C :=$ completion of $\overline{K}_\infty$	

The completions are taken with respect to the ∞-adic absolute value: For nonzero $a \in A$, define $|a| := \#(A/a) = q^{\deg a}$ (and $|0| := 0$); extend $|\ |$ to K, its completion K_∞, an algebraic closure $\overline{K}_\infty$, and *its* completion C, in turn. The field C is algebraically closed as well as complete with respect to $|\ |$. Some authors use the notation $\mathbb{C}$ or $\mathbb{C}_\infty$ instead of C.

Finite rank $\mathbb{Z}$-submodules of C are just finite-dimensional $\mathbb{F}_p$-subspaces, not so interesting, so instead consider this:

Definition 2.1. An *A-lattice* in C is a discrete A-submodule Λ of C of finite rank, where

$$\operatorname{rank} \Lambda := \dim_K(K\Lambda) = \dim_{K_\infty}(K_\infty \Lambda).$$

If A is a principal ideal domain, such as $\mathbb{F}_q[T]$, then all such Λ arise as follows:

> Let $\{x_1, \dots, x_r\}$ be a basis for a finite-dimensional K_∞-subspace in C, and let $\Lambda := Ax_1 + \cdots + Ax_r \subset C$.

Note: In contrast with the characteristic 0 situation, r can be arbitrarily large since $[C : K_\infty]$ is infinite.

Theorem 2.2. *The quotient C/Λ is analytically isomorphic to C!*

This statement can be interpreted using rigid analysis. More concretely, it means that there exists a power series

$$e(z) = \alpha_0 z + \alpha_1 z^q + \alpha_2 z^{q^2} + \cdots$$

defining a surjective $\mathbb{F}_q$-linear map $C \to C$ with kernel Λ. If we require $\alpha_0 = 1$, then such a power series e is unique.

Sketch of proof. Uniqueness follows from the nonarchimedean Weierstrass preparation theorem, which implies that a convergent power series is determined up to a constant multiple by its zeros: explicitly, if $e(z)$ exists, then

$$e(z) = z \prod_{\substack{\lambda \in \Lambda \\ \lambda \neq 0}} \left(1 - \frac{z}{\lambda}\right). \tag{2.1}$$

(Over $\mathbb{C}$, there would be an ambiguity of multiplication by a function $e^{g(z)}$, but in the nonarchimedean setting, every invertible entire function is constant!)

If we take (2.1) as a definition, there are several things to check:

- The infinite product converges. (Proof: Since Λ is a discrete subgroup of a locally compact group $K_\infty \Lambda$, we have $\lambda \to \infty$.)
- $e(z)$ is surjective. (The nonarchimedean Picard theorem says that a nonconstant entire function omits *no* values.)
- $e(x+y) = e(x) + e(y)$. (Proof: Write Λ as an increasing union of finite-dimensional $\mathbb{F}_p$-subspaces, and $e(x)$ as the limit of the corresponding finite products. If $f(x)$ is a polynomial whose zeros are distinct and form a group G under addition, then $f(x+y) = f(x)+f(y)$, because $f(x+y)-f(x)-f(y)$ vanishes on $G \times G$ but is of degree less than $\#G$ in each variable.)
- $e(cx) = ce(x)$ for each $c \in \mathbb{F}_q$. (Use a proof similar to the preceding, or argue directly.)
- $\ker e = \Lambda$. □

Now C/Λ has a natural A-module structure. Carrying this across the isomorphism $C/\Lambda \to C$ gives an *exotic* A-module structure on C. This is essentially what a Drinfeld module is: the additive group with a new A-module structure.

For each $a \in A$, the multiplication-by-a map $a\colon C/\Lambda \to C/\Lambda$ corresponds under the isomorphism to a map $\phi_a\colon C \to C$ making

$$\begin{array}{ccc} C/\Lambda & \xrightarrow{a} & C/\Lambda \\ {\scriptstyle e}\downarrow\wr & & \wr\downarrow{\scriptstyle e} \\ C & \xrightarrow{\phi_a} & C \end{array} \tag{2.2}$$

commute.

Proposition 2.3. *The map ϕ_a is a polynomial!*

Proof. Assume that $a \neq 0$. We have

$$\ker\left(a\colon C/\Lambda \to C/\Lambda\right) = \frac{a^{-1}\Lambda}{\Lambda},$$

which is isomorphic to $\Lambda/a\Lambda = (A/a)^r$, which is finite of order $|a|^r$. So $\ker \phi_a$ should be $e\left(\frac{a^{-1}\Lambda}{\Lambda}\right)$. Define the polynomial

$$\phi_a(z) := az \prod_{t \in \frac{a^{-1}\Lambda}{\Lambda} - \{0\}} \left(1 - \frac{z}{e(t)}\right).$$

Then ϕ_a is the map making (2.2) commute, because the power series $\phi_a(e(z))$ and $e(az)$ have the same zeros and same coefficient of z. □

The proof of Proposition 2.3 shows also that for any nonzero $a \in A$,

$$\deg \phi_a = \# \frac{a^{-1}\Lambda}{\Lambda} = |a|^r.$$

3. Algebraic theory

3.1. $\mathbb{F}_q$-linear polynomials. Let L be a field containing $\mathbb{F}_q$. A polynomial $f(x) \in L[x]$ is called additive if $f(x+y) = f(x) + f(y)$ in $L[x,y]$, and $\mathbb{F}_q$-linear if, in addition, $f(cx) = cf(x)$ in $L[x]$ for all $c \in \mathbb{F}_q$. Think of such polynomials as operators that can be composed: For example, each $a \in L$ defines an operator $x \mapsto ax$ and τ denotes the Frobenius operator $x \mapsto x^p$, so τa is $x \mapsto (ax)^p$ and τ^2 is $x \mapsto x^{p^2}$.

Let $\mathbb{G}_a$ be the additive group scheme over L, viewed as an $\mathbb{F}_q$-vector space scheme over L. Endomorphisms of $\mathbb{G}_a$ *as an $\mathbb{F}_q$-vector space scheme* are $\mathbb{F}_q$-linear by definition:

$$\begin{aligned}
\operatorname{End} \mathbb{G}_a &= \{\mathbb{F}_q\text{-linear polynomials in } L[x]\} \\
&= \left\{ \textstyle\sum_{i=0}^n a_i x^{q^i} : a_i \in L \right\} \\
&= \left\{ \left(\textstyle\sum_{i=0}^n a_i \tau^i \right)(x) : a_i \in L \right\} \\
&=: L\{\tau\};
\end{aligned}$$

this is a ring under addition and composition. More specifically, $L\{\tau\}$ is a twisted polynomial ring, twisted in that the elements $a \in L$ do not necessarily commute with the variable τ: instead, $\tau a = a^q \tau$.

For $f \in L\{\tau\}$, let l.c.(f) denote the leading coefficient a_n of f; by convention, l.c.$(0) = 0$. Also, if $f = \sum_{i=0}^n a_i \tau^i$, then the derivative of the $\mathbb{F}_q$-linear polynomial $f(x) \in L[x]$ is the constant $f'(0) = a_0$, which is the "constant term" of f viewed as a twisted polynomial in $L\{\tau\}$.

3.2. Drinfeld modules.

Definition 3.1. An A-field is an A-algebra L that is a field; that is, L is a field equipped with a ring homomorphism $\iota\colon A \to L$. The A-characteristic of L is $\operatorname{char}_A L := \ker \iota$, a prime ideal of A.

We distinguish two cases:

- L is an extension of K and ι is an inclusion; then $\operatorname{char}_A L = 0$. (Example: C.)
- L is an extension of $A/\mathfrak{p}$ for some nonzero prime $\mathfrak{p}$ of A; then $\operatorname{char}_A L = \mathfrak{p}$.

To motivate the following definition, recall that an A-module M is an abelian group M together with a ring homomorphism $A \to \operatorname{End}_{\text{group}} M$.

Definition 3.2. A Drinfeld A-module ϕ over L is the additive group scheme $\mathbb{G}_a$ with a faithful A-module structure for which the induced action on the tangent space at 0 is given by ι. More concretely, ϕ is an injective ring homomorphism

$$\begin{aligned}
A &\longrightarrow \operatorname{End} \mathbb{G}_a = L\{\tau\} \\
a &\longmapsto \phi_a
\end{aligned}$$

such that $\phi_a'(0) = \iota(a)$ for all $a \in A$.

REMARK 3.3. Many authors explicitly disallow ϕ to be the composition $A \xrightarrow{\iota} L \subset L\{\tau\}$, but we allow it when $\operatorname{char}_A L = 0$, since doing so does not seem to break any theorems. Our requirement that ϕ be injective does rule out $A \xrightarrow{\iota} L \subset L\{\tau\}$ when $\operatorname{char}_A L \neq 0$, however; we must rule this out to make Proposition 3.5 below hold.

It turns out that every Drinfeld A-module over C arises from an A-lattice as in Section 2. For a more precise statement, see Theorem 3.11.

3.3. Rank. We could define the rank of a Drinfeld module over C as the rank of the A-lattice it comes from, but it will be nicer to give an *algebraic* definition that makes sense over any A-field.

Let ϕ be a Drinfeld module. For each nonzero $a \in A$, there are nonnegative integers $m(a) \leq M(a)$ such that we may write

$$\phi_a = c_{m(a)}\tau^{m(a)} + \cdots + c_{M(a)}\tau^{M(a)}$$

with exponents in increasing order and $c_{m(a)}, c_{M(a)} \neq 0$. Then $\phi_a(x)$ as a polynomial in x has degree $q^{M(a)}$ and each zero has multiplicity $q^{m(a)}$. In terms of the functions M and m, we will define the rank and height of ϕ, respectively.

For each closed point $\mathfrak{p} \in X$, let $v_\mathfrak{p}$ be the $\mathfrak{p}$-adic valuation on K normalized so that $v_\mathfrak{p}(a)$ is the degree of the $\mathfrak{p}$-component of the divisor (a); thus $v_\mathfrak{p}(K^\times) = (\deg \mathfrak{p})\mathbb{Z}$. Also, define $|a|_\mathfrak{p} := q^{-v_\mathfrak{p}(a)}$. For example, $|\ |_\infty$ is the absolute value $|\ |$ defined earlier.

EXAMPLE 3.4. If $A = \mathbb{F}_q[T]$, then ϕ is determined by ϕ_T, and we define $r = M(T)$. For any nonzero $a \in A$, expanding ϕ_a in terms of ϕ_T shows that $M(a) = (\deg a)r = -rv_\infty(a)$.

A similar result holds for arbitrary A:

PROPOSITION 3.5 (Characterization of rank). *Let ϕ be a Drinfeld module over an A-field L. Then there exists a unique $r \in \mathbb{Q}_{\geq 0}$ such that $M(a) = -rv_\infty(a)$, or equivalently $\deg \phi_a = |a|^r$, for all nonzero $a \in A$. (Proposition 3.13*(a) *will imply that r is an* integer.)

PROOF. After enlarging L to make L perfect, we may define the ring of twisted Laurent series $L((\tau^{-1}))$ whose elements have the form $\sum_{n\in\mathbb{Z}} \ell_n\tau^n$ with $\ell_n = 0$ for sufficiently large *positive* n; multiplication is defined so that $\tau^n\ell = \ell^{q^n}\tau$. Then $L((\tau^{-1}))$ is a division ring with a valuation $v\colon L((\tau^{-1})) \to \mathbb{Z} \cup \{+\infty\}$ sending τ^n to $-n$ (same proof as for usual Laurent series over a field). Thus $\phi\colon A \to L\{\tau\}$ extends to a homomorphism $\phi\colon K \to L((\tau^{-1}))$, and v pulls back to a nontrivial valuation v_K on K. We have $v_K(a) = -M(a) \leq 0$ for all $a \in A - \{0\}$, so $v_K = rv_\infty$ for some $r \in \mathbb{Q}_{\geq 0}$. Then $M(a) = -rv_\infty(a)$ for all $a \in A - \{0\}$. □

Define the rank of ϕ to be r. (This is *not* analogous to the rank of the group of rational points of an elliptic curve.)

3.4. Analogies. Drinfeld modules are *1-dimensional* objects, no matter what the rank is. Comparing with Section 2.1 suggests the following analogies:

rank 0 Drinfeld module $\longleftrightarrow \mathbb{G}_a$

rank 1 Drinfeld module $\longleftrightarrow \mathbb{G}_m$ or CM elliptic curve

(if E has CM by $\mathscr{O}$, view its lattice as rank 1 $\mathscr{O}$-module)

rank 2 Drinfeld module $\longleftrightarrow$ elliptic curve

rank ≥ 3 Drinfeld module $\longleftrightarrow$? (if only such geometric objects existed...)

There is also a higher-dimensional generalization called a t-module [**And86**].

REMARK 3.6. Gekeler [**Gek83**, **Gek91**] developed a theory of Drinfeld modules over *finite* fields analogous to the theory of abelian varieties over finite fields developed by Deuring, Tate, Waterhouse, and others.

3.5. Height.

PROPOSITION 3.7. *Let ϕ be a Drinfeld module over an A-field L of nonzero characteristic $\mathfrak{p}$. Then there exists a unique $h \in \mathbb{Q}_{>0}$ such that $m(a) = hv_{\mathfrak{p}}(a)$ for all nonzero $a \in A$. (Proposition 3.13*(b)* will imply that h is an integer satisfying $0 < h \leq r$.)*

PROOF. Enlarge L to make it perfect and extend ϕ to a homomorphism $K \to L((\tau))$ (twisted Laurent series in τ instead of τ^{-1}) to define a valuation on K. It is positive on $\mathfrak{p}$, hence equal to $hv_{\mathfrak{p}}$ for some $h \in \mathbb{Q}_{>0}$. □

Call h the height of ϕ. It is analogous to the height of the formal group of an elliptic curve over a field of characteristic p.

3.6. Drinfeld modules and lattices. For fixed A and L, Drinfeld A-modules over L form a category, with morphisms as follows:

DEFINITION 3.8. A morphism $f\colon \phi \to \psi$ of Drinfeld modules over L is an element of $\operatorname{End} \mathbb{G}_a$ such that $f \circ \phi_a = \psi_a \circ f$ for all $a \in A$: i.e.,

(3.1)
$$\begin{array}{ccc} \mathbb{G}_a & \xrightarrow{\phi_a} & \mathbb{G}_a \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbb{G}_a & \xrightarrow{\psi_a} & \mathbb{G}_a \end{array}$$

commutes.

An isogeny between Drinfeld modules ϕ and ψ is a surjective morphism f with finite kernel, or equivalently (since $\mathbb{G}_a$ is 1-dimensional), a nonzero morphism. If such an f exists, ϕ and ψ are called isogenous.

Over $\mathbb{C}$, there is no nonzero algebraic homomorphism from $\mathbb{G}_m$ to an elliptic curve; analogously:

PROPOSITION 3.9. *Isogenous Drinfeld modules have the same rank.*

PROOF. If $f\colon \phi \to \psi$ is an isogeny between Drinfeld modules of rank r and r', respectively, then (3.1) gives

$$(\deg f)|a|^r = |a|^{r'}(\deg f)$$

for all $a \in A$, so $r = r'$. □

Because of Proposition 3.9, we fix the rank in the following.

DEFINITION 3.10. A morphism of rank r A-lattices Λ, Λ' in C is a number $c \in C$ such that $c\Lambda \subseteq \Lambda'$.

THEOREM 3.11. *For each $r \geq 0$, the analytic construction*

$$\{A\text{-lattices in } C \text{ of rank } r\} \xrightarrow{\sim} \{\text{Drinfeld modules over } C \text{ of rank } r\}$$

of Section 2 is an equivalence of categories.

SKETCH OF PROOF. Given a rank r Drinfeld module ϕ over C, choose a non-constant $a \in A$, and consider a power series

$$e(z) = z + \alpha_1 z^q + \alpha_2 z^{q^2} + \cdots$$

with unknown coefficients α_i. The condition $e(az) = \phi_a(e(z))$ determines the α_i uniquely; solve for each α_i in turn. Check that the resulting power series converges everywhere, and that its kernel is an A-lattice in C giving rise to ϕ. The proof of Proposition 2.3 shows more generally that a morphism of A-lattices corresponds to a polynomial map $C \to C$ defining a morphism of Drinfeld modules, and vice versa. □

In particular, homothety classes of rank r A-lattices in C are in bijection with isomorphism classes of rank r Drinfeld modules over C.

3.7. Torsion points. The additive polynomial ϕ_a plays the role of the multiplication-by-n map on an elliptic curve, or the n^{th} power map on $\mathbb{G}_m$.

For $a \neq 0$, the a-torsion subscheme of a Drinfeld module ϕ is $\phi[a] := \ker \phi_a$, viewed as subgroup scheme of $\mathbb{G}_a$. It is a finite group scheme of order $\deg \phi_a = q^{M(a)} = |a|^r$. Let ${}^{\phi}L$ denote the additive group of L viewed as an A-module via ϕ. Then $\phi[a](L)$ is an A-submodule of ${}^{\phi}L$, but its order may be less than $|a|^r$ if L is not algebraically closed or $\phi[a]$ is not reduced.

More generally, if I is a nonzero ideal of A, let $\phi[I]$ be the scheme-theoretic intersection $\bigcap_{a \in I} \phi[a]$. Equivalently, one can define ϕ_I as the monic generator of the left ideal of $L\{\tau\}$ generated by $\{\phi_a : a \in I\}$, and define $\phi[I] := \ker \phi_I$. To understand the structure of $\phi[I](L)$, we need the following basic lemma about modules over Dedekind rings.

LEMMA 3.12. *Let A be a Dedekind ring. Let D be an A-module.*

(a) *If $\ell_1, \ldots, \ell_n$ are distinct nonzero prime ideals of A, and $e_1, \ldots, e_n \in \mathbb{Z}_{\geq 0}$, then*

$$D[\ell_1^{e_1} \cdots \ell_n^{e_n}] \simeq D[\ell_1^{e_1}] \oplus \cdots \oplus D[\ell_n^{e_n}].$$

(b) *If D is divisible, then for each fixed nonzero prime ℓ of A, the A/ℓ^e-module $D[\ell^e]$ is free of rank independent of e.*

PROOF. Localize to assume that A is a discrete valuation ring. Then (a) is trivial. In proving (b), we write ℓ also for a generator of ℓ. Since $D[\ell]$ is an A/ℓ-vector space, we can choose a free A-module F and an isomorphism $i_1 \colon \ell^{-1}F/F \xrightarrow{\sim} D[\ell]$. We construct isomorphisms $i_e \colon \ell^{-e}F/F \xrightarrow{\sim} D[\ell^e]$ for all $e \geq 1$ by induction: given the isomorphism i_e, use divisibility of D to lift i_e to a

homomorphism $i_{e+1}\colon \ell^{-(e+1)}F/F \to D[\ell^{e+1}]$ fitting in a commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ell^{-1}F/F & \longrightarrow & \ell^{-(e+1)}F/F & \xrightarrow{\ell} & \ell^{-e}F/F & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle i_1} & & \downarrow{\scriptstyle i_{e+1}} & & \downarrow{\scriptstyle i_e} & & \\ 0 & \longrightarrow & D[\ell] & \longrightarrow & D[\ell^{e+1}] & \xrightarrow{\ell} & D[\ell^e] & \longrightarrow & 0. \end{array}$$

The diagram shows that i_{e+1} is an isomorphism too. □

PROPOSITION 3.13. *Let ϕ be a rank r Drinfeld module over an algebraically closed A-field L.*

(a) *If I is an ideal of A such that $\operatorname{char}_A L \nmid I$, then the A/I-module $\phi[I](L)$ is free of rank r. The same holds even if L is only separably closed.*
(b) *If $\operatorname{char}_A L = \mathfrak{p} \neq 0$, let h be the height of ϕ; then the $A/\mathfrak{p}^e$-module $\phi[\mathfrak{p}^e](L)$ is free of rank $r-h$.*

PROOF. When L is algebraically closed, $\phi_a\colon L \to L$ is surjective for every nonzero $a \in A$. In other words, the A-module ${}^{\phi}L$ is divisible. By Lemma 3.12, the claims for algebraically closed L follow if for each nonzero prime ℓ of A, there exists $e \geq 1$ such that

$$\#\phi[\ell^e](L) = \begin{cases} \#(A/\ell^e)^r, & \text{if } \ell \neq \operatorname{char}_A L; \\ \#(A/\ell^e)^{r-h}, & \text{if } \ell = \operatorname{char}_A L. \end{cases}$$

The class group of A is finite, so we may choose e so that ℓ^e is principal, say generated by a. If $\ell \neq \operatorname{char}_A L$, then ϕ_a is separable, so $\#\phi[\ell^e](L) = \deg \phi_a = |a|^r = \#(A/a)^r$. If $\ell = \operatorname{char}_A L$, then each zero of ϕ_a has multiplicity $q^{m(a)} = q^{hv_{\mathfrak{p}}(a)} = \#(A/a)^h$, so $\#\phi[\ell^e](L) = \#(A/a)^{r-h}$.

Now suppose that L is only separably closed, with algebraic closure $\overline{L}$. If $\operatorname{char}_A L \nmid I$, the proof above shows that $\phi[I](\overline{L})$ consists of L-points, so the structure of $\phi[I](L)$ is the same. □

COROLLARY 3.14. *If ϕ is a rank r Drinfeld module over any A-field L, and I is a nonzero ideal of A, then $\deg \phi_I = \#\phi[I] = \#(A/I)^r$.*

PROOF. The underlying scheme of $\phi[I]$ is $\operatorname{Spec} L[x]/(\phi_I(x))$, so $\#\phi[I] = \deg \phi_I$. For the second equality, assume without loss of generality that L is algebraically closed. For a group scheme G, let G^0 denote its connected component. Define $m(I) := \min\{m(a) : a \in I - \{0\}\}$. If $a \in A - \{0\}$, then $\phi[a]^0 = \ker \tau^{m(a)}$, so $\phi[I]^0 = \ker \tau^{m(I)}$. Thus $\#\phi[I]^0 = q^{m(I)}$, which is multiplicative in I. On the other hand, Proposition 3.13 shows that $\#\phi[I](L)$ is multiplicative in I. Thus the integers $\#\phi[I] = \#\phi[I]^0 \cdot \#\phi[I](L)$ and $\#(A/I)^r$ are both multiplicative in I. They are equal for any power of I that is principal, so they are equal for I. □

COROLLARY 3.15. *Let ϕ be a rank 1 Drinfeld module over a field L of nonzero A-characteristic $\mathfrak{p}$. Then $\phi_{\mathfrak{p}} = \tau^{\deg \mathfrak{p}}$.*

PROOF. Without loss of generality, L is algebraically closed. Since $0 < h \leq r = 1$, we have $h = r = 1$. By Proposition 3.13(b), $\phi[\mathfrak{p}](L) = 0$. On the other hand, $\phi_{\mathfrak{p}}$ is monic, by the general definition of ϕ_I. The previous two sentences show that $\phi_{\mathfrak{p}}$ is a power of τ. By Corollary 3.14, $\deg \phi_{\mathfrak{p}} = \#(A/\mathfrak{p}) = q^{\deg \mathfrak{p}} = \deg \tau^{\deg \mathfrak{p}}$, so $\phi_{\mathfrak{p}} = \tau^{\deg \mathfrak{p}}$. □

COROLLARY 3.16. *In the context of Corollary 3.15, if* $\mathfrak{p} = (\pi)$ *for some* $\pi \in A$, *then* $\phi_\pi = c\tau^{\deg \mathfrak{p}}$ *for some* $c \in L^\times$.

PROOF. By definition, $\phi_\mathfrak{p}$ is the monic generator of the left ideal generated by $\{\phi_a : a \in I\}$, which is the left ideal generated by ϕ_π. □

3.8. Tate modules. Let $\ell \subset A$ be a prime ideal not equal to 0 or $\operatorname{char}_A L$. Define the completions $A_\ell := \varprojlim_n A/\ell^n$ and $K_\ell := \operatorname{Frac} A_\ell$. Let L_s be a separable closure of L. Then the Tate module

$$T_\ell\phi := \operatorname{Hom}(K_\ell/A_\ell, {}^\phi L_\mathrm{s})$$

is a free A_ℓ-module of rank r.

Its applications are analogous to those for elliptic curves:

- The endomorphism ring $\operatorname{End}\phi$ is a projective A-module of rank $\le r^2$. In particular, if $r = 1$, then $\operatorname{End}\phi = A$ and $\operatorname{Aut}\phi = A^\times = \mathbb{F}_q^\times$.
- The Galois action on torsion points yields an ℓ-adic representation

$$\rho_\ell \colon \operatorname{Gal}(L_\mathrm{s}/L) \longrightarrow \operatorname{Aut}_{A_\ell}(T_\ell\phi) \simeq \mathrm{GL}_r(A_\ell).$$

4. Reduction theory

4.1. Drinfeld modules over rings. So far we considered Drinfeld modules over A-fields. One can also define Drinfeld modules over arbitrary A-algebras R or even A-schemes. In such generality, the underlying $\mathbb{F}_q$-vector space scheme need only be *locally* isomorphic to $\mathbb{G}_a$, so it could be the $\mathbb{F}_q$-vector space scheme associated to a nontrivial line bundle on the base.

To avoid this complication, let us assume that $\operatorname{Pic} R = 0$; this holds if the A-algebra R is a principal ideal domain, for instance. Then a Drinfeld A-module over R is given by a ring homomorphism

$$\begin{aligned} A &\longrightarrow \operatorname{End}\mathbb{G}_{a,R} = R\{\tau\} \\ a &\longmapsto \phi_a \end{aligned}$$

such that $\phi_a'(0) = a$ in R for all $a \in A$ *and* $\operatorname{l.c.}(\phi_a) \in R^\times$ for all nonzero $a \in A$. The last requirement, which implies injectivity of ϕ (if R is nonzero), guarantees that for any maximal ideal $\mathfrak{m} \subset R$, reducing all the ϕ_a modulo $\mathfrak{m}$ yields a Drinfeld module over $R/\mathfrak{m}$ *of the same rank*.

4.2. Good and stable reduction. Let us now specialize to the following setting:

R: an A-discrete valuation ring
(a discrete valuation ring with a ring homomorphism $A \to R$)
$\mathfrak{m}$: the maximal ideal of R
$L := \operatorname{Frac} R$, the fraction field
$v \colon L \to \mathbb{Z} \cup \{+\infty\}$, the discrete valuation
$\mathbb{F} := R/\mathfrak{m}$, the residue field
ϕ: a Drinfeld module over L of rank $r \ge 1$.

Then

- ϕ has good reduction if ϕ is isomorphic over L to a Drinfeld module over R, that is, if after replacing ϕ by an isomorphic Drinfeld module over L, all the ϕ_a have coefficients in R, and $\mathrm{l.c.}(\phi_a) \in R^\times$ for all nonzero $a \in A$.
- ϕ has stable reduction if after replacing ϕ by an isomorphic Drinfeld module over L, all the ϕ_a have coefficients in R, and $a \mapsto (\phi_a \bmod \mathfrak{m})$ is a Drinfeld module over $\mathbb{F}$ of positive rank.

EXAMPLE 4.1. Let $A = \mathbb{F}_q[T]$. A rank 2 Drinfeld module over L is determined by

$$\phi_T = T + c_1\tau + c_2\tau^2;$$

here $c_1, c_2 \in L$ and $c_2 \neq 0$. Isomorphic Drinfeld modules are given by

$$u^{-1}\phi_T\, u = T + u^{q-1}c_1\tau + u^{q^2-1}c_2\tau^2$$

for any $u \in L^\times$. The condition for stable reduction is satisfied if and only if $v(u^{q-1}c_1) \geq 0$ and $v(u^{q^2-1}c_2) \geq 0$, with at least one of them being an equality. This condition uniquely specifies $v(u) \in \mathbb{Q}$. An element u of this valuation might not exist in L, but u can be found in a suitable ramified finite extension of L.

THEOREM 4.2 (Potential stability). *Let ϕ be a Drinfeld module over L of rank $r \geq 1$. There exists a finite ramified extension L' of L such that ϕ over L' has stable reduction.*

PROOF. Choose generators $a_1, \ldots, a_m$ of the ring A. As in Example 4.1, find L' and $u \in L'$ of valuation "just right" so that all coefficients of $u^{-1}\phi_{a_i}u$ for all i have nonnegative valuation, and there exist i and $j > 0$ such that the coefficient of τ^j in $u^{-1}\phi_{a_i}u$ has valuation 0. □

COROLLARY 4.3. *Let ϕ be a rank 1 Drinfeld module over L. If there exists $a \in A$ such that $\deg \phi_a > 1$ and $\mathrm{l.c.}(\phi_a) \in R^\times$, then ϕ is a Drinfeld module over R.*

Note: Saying that ϕ *is* a Drinfeld module over R is stronger than saying that ϕ is *isomorphic over L to* a Drinfeld module over R, which would be saying that ϕ has good reduction.

PROOF. By enlarging R and L, we may assume that ϕ has stable reduction, so there exists u such that $(u^{-1}\phi u) \bmod \mathfrak{m}$ is a Drinfeld module of positive rank. This reduction has rank at most the rank of ϕ, so it too has rank 1, so ϕ_a and $(u^{-1}\phi_a u) \bmod \mathfrak{m}$ have the same degree. Thus $v(\mathrm{l.c.}(\phi_a))$ and $v(\mathrm{l.c.}(u^{-1}\phi_a u))$ are 0, so $v(u^{\deg \phi_a - 1}) = 0$, so $v(u) = 0$. Now $u^{-1}\phi u$ is a Drinfeld module of rank 1 over R, so ϕ is too. □

5. Example: The Carlitz module

The Drinfeld module analogue of $\mathbb{G}_m$ is the Carlitz module

$$\begin{aligned} \phi\colon A = \mathbb{F}_q[T] &\longrightarrow K\{\tau\} \\ T &\longmapsto T + \tau \end{aligned}$$

(i.e., $\phi_T(x) = Tx + x^q$). This is a Drinfeld module of rank 1 since

$$\deg \phi_T = q = |T|^1.$$

Define

$$\begin{aligned}
[n] &:= T^{q^n} - T \\
[n]! &:= [1]\,[2]\cdots[n] \\
e(z) &:= \sum_{n\geq 0} z^{q^n}/[n]! \\
\pi &:= \prod_{n\geq 1}\left(1 - \frac{[n]}{[n+1]}\right) \quad \in K_\infty \\
i &:= \sqrt[q-1]{-[1]} \quad \in C.
\end{aligned}$$

Carlitz [**Car35**], long before Drinfeld, proved that e induces an isomorphism

$$C/\pi i A \longrightarrow (C \text{ with the Carlitz } A\text{-module action}).$$

This is analogous to $\exp\colon \mathbb{C}/2\pi i\mathbb{Z} \xrightarrow{\sim} \mathbb{C}^\times$.

THEOREM 5.1 ([**Car38**, Theorem 9]). *Fix $a \in A$ with $a \neq 0$. Then $K(\phi[a])$ is an abelian extension of K, and $\mathrm{Gal}(K(\phi[a])/K) \simeq (A/a)^\times$.*

Theorem 5.1 is analogous to $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n\mathbb{Z})^\times$, and can be proved in the same way.

THEOREM 5.2 (Analogue of Kronecker–Weber, implicit in [**Hay74**, §7] and [**Dri74**, §8]). *Every abelian extension of K in which the place ∞ splits completely is contained in $K(\phi[a])$ for some a.*

6. Class field theory

The theory of elliptic curves with complex multiplication leads to an explicit construction of the abelian extensions of an imaginary quadratic number field. In this section, we explain work of Drinfeld [**Dri74**] and Hayes [**Hay79**] that adapts this classical theory to construct the abelian extensions of an arbitrary global function field $K = \mathrm{Frac}\, A$.

6.1. The class group. When A is not a principal ideal domain, class field theory is more complicated than Theorem 5.2 would suggest. Introduce the following notation:

$$\begin{aligned}
\mathcal{I} &:= \text{the group of nonzero fractional } A\text{-ideals in } K \\
\mathcal{P} &:= \{(c) : c \in K^\times\}, \quad \text{the group of principal fractional } A\text{-ideals} \\
\mathrm{Pic}\, A &:= \mathcal{I}/\mathcal{P}, \quad \text{the class group of } A.
\end{aligned}$$

For a nonzero fractional ideal I, let $[I]$ denote its class in $\mathrm{Pic}\, A$.

6.2. Rank 1 Drinfeld modules over C.

PROPOSITION 6.1. *We have bijections*

$$\begin{array}{ccccc}
\mathrm{Pic}\, A & \xrightarrow{\sim} & \dfrac{\{\text{rank 1 } A\text{-lattices in } C\}}{\text{homothety}} & \xrightarrow{\sim} & \dfrac{\{\text{rank 1 Drinfeld modules over } C\}}{\text{isomorphism}} \\
{[I]} & \longmapsto & (\text{homothety class of } I \text{ in } C) & &
\end{array}$$

PROOF. The second bijection comes from the $r = 1$ case of Theorem 3.11. Thus we need only consider the first map.

Surjectivity: Any rank 1 A-lattice Λ in C can be scaled so that $K\Lambda = K$. Then Λ is a nonzero fractional ideal I.

Injectivity: I is homothetic to I' in C if and only if there exists $c \in K^\times$ such that $I = cI'$. □

COROLLARY 6.2. *Every rank* 1 *Drinfeld module over* C *is isomorphic to one defined over* K_∞.

PROOF. When the lattice Λ is contained in K_∞, the power series e and polynomials ϕ_a constructed in Section 2 will have coefficients in K_∞. □

6.3. The action of ideals on Drinfeld modules. The bijection between $\operatorname{Pic} A$ and the set of isomorphism classes of rank 1 Drinfeld modules over C is analytic, not canonical from the algebraic point of view. But a weaker form of this structure exists algebraically, as will be described in Theorem 6.5.

Fix any A-field L. If I is a nonzero ideal of A and ϕ is a Drinfeld module over any A-field L, we can define a new Drinfeld module $I * \phi$ over L isomorphic to the quotient of $\mathbb{G}_a$ by $\phi[I]$; more precisely, there exists a unique Drinfeld module ψ over L such that $\phi_I \colon \mathbb{G}_a \to \mathbb{G}_a$ is an isogeny $\phi \to \psi$, and we define $I * \phi := \psi$.

Suppose that $I = (a)$ for some nonzero $a \in A$. Then ϕ_I is ϕ_a made monic; that is, if $u := \text{l.c.}(\phi_a)$, then $\phi_I = u^{-1}\phi_a$. Therefore ϕ_I is the composition

$$\phi \xrightarrow{\phi_a} \phi \xrightarrow{u^{-1}} u^{-1}\phi u,$$

so $(a) * \phi = u^{-1}\phi u$, which is isomorphic to ϕ, but not necessarily equal to ϕ. This suggests that we define $(a^{-1}) * \phi = u\phi u^{-1}$. Finally, every $I \in \mathcal{I}$ is $(a^{-1})J$ for some $a \in A - \{0\}$ and integral ideal J, and we define $I * \phi = u(J * \phi)u^{-1}$. The following is now easy to check:

PROPOSITION 6.3. *The operation* $*$ *defines an action of* $\mathcal{I}$ *on the set of Drinfeld modules over* L. *It induces an action of* $\operatorname{Pic} A$ *on the set of isomorphism classes of Drinfeld modules over* L.

EXAMPLE 6.4. Suppose that ϕ is over C, and I is a nonzero integral ideal of A. If we identify ϕ analytically with C/Λ, then $\phi[I] \simeq I^{-1}\Lambda/\Lambda$, so

$$I * (C/\Lambda) \simeq (C/\Lambda)/(I^{-1}\Lambda/\Lambda) \simeq C/I^{-1}\Lambda.$$

Let $\mathscr{Y}(C)$ be the set of isomorphism classes of rank 1 Drinfeld A-modules over C.

THEOREM 6.5. *The set* $\mathscr{Y}(C)$ *is a principal homogeneous space under the action of* $\operatorname{Pic} A$.

PROOF. This follows from Proposition 6.1 and the calculation in Example 6.4 showing that the corresponding action of I on lattices is by multiplication by I^{-1}. □

6.4. Sgn-normalized Drinfeld modules. We will eventually construct abe-12lian extensions of a global function field K by adjoining the coefficients appearing in rank 1 Drinfeld modules. For this, it will be important to have *actual* Drinfeld modules, and not just *isomorphism classes* of Drinfeld modules. Therefore we will choose a (not quite unique) "normalized" representative of each isomorphism class.

Let $\mathbb{F}_\infty$ be the residue field of $\infty \in X$. Since ∞ is a closed point, $\mathbb{F}_\infty$ is a finite extension of $\mathbb{F}_q$. A choice of uniformizer $\pi \in K_\infty$ defines an isomorphism $K_\infty \simeq \mathbb{F}_\infty((\pi))$, and we define sgn as the composition

$$K_\infty^\times \xrightarrow{\sim} \mathbb{F}_\infty((\pi))^\times \overset{\text{l.c.}}{\twoheadrightarrow} \mathbb{F}_\infty^\times.$$

The function sgn is an analogue of the classical sign function $\operatorname{sgn}\colon \mathbb{R}^\times \to \{\pm 1\}$.

From now on, we fix (A, sgn).

Definition 6.6. A rank 1 Drinfeld module ϕ over L is sgn-normalized if there exists an $\mathbb{F}_q$-algebra homomorphism $\eta\colon \mathbb{F}_\infty \to L$ such that $\text{l.c.}(\phi_a) = \eta(\operatorname{sgn} a)$ for all nonzero $a \in A$.

Example 6.7. Suppose that $A = \mathbb{F}_q[T]$ and $\operatorname{sgn}(1/T) = 1$. For a Drinfeld A-module ϕ over L, the following are equivalent:

- ϕ is sgn-normalized;
- $\text{l.c.}(\phi_T) = 1$;
- $\phi_T = T + \tau$ (the Carlitz module).

Theorem 6.8. *Every rank 1 Drinfeld module ϕ over C is isomorphic to a sgn-normalized Drinfeld module. More precisely, the set of sgn-normalized Drinfeld modules isomorphic to ϕ is a principal homogeneous space under $\mathbb{F}_\infty^\times/\mathbb{F}_q^\times$.*

Proof. When A is generated over $\mathbb{F}_q$ by one element T, then it suffices to choose u so that $u^{-1}\phi_T u$ is monic. The idea in general is that even if A is not generated by one element, its completion will be (topologically).

First, extend ϕ to a homomorphism $K \to C((\tau^{-1}))$ as in the proof of Proposition 3.5. The induced valuation on K is v_∞, so there exists a unique extension to a continuous homomorphism $K_\infty \to C((\tau^{-1}))$, which we again denote by $a \mapsto \phi_a$. Also, l.c. extends to a map $C((\tau^{-1}))^\times \to C^\times$ (not a homomorphism). Let $\pi \in K_\infty$ be a uniformizer with $\operatorname{sgn}(\pi) = 1$. Replacing ϕ by $u^{-1}\phi u$ multiplies $\text{l.c.}(\phi_\pi)$ by $u^{|\pi|-1}$, so we can choose $u \in C^\times$ to make $\text{l.c.}(\phi_\pi) = 1$.

We claim that the new ϕ is sgn-normalized. Define $\eta\colon \mathbb{F}_\infty \to C$ by $\eta(c) := \text{l.c.}(\phi_c)$. For any $a = c\pi^n \in K_\infty^\times$, with $c \in \mathbb{F}_\infty$ and $n \in \mathbb{Z}$, we have

$$\text{l.c.}(\phi_a) = \text{l.c.}(\phi_c \phi_\pi^n) = \text{l.c.}(\phi_c) = \eta(c) = \eta(\operatorname{sgn} a),$$

as required.

The u was determined up to a $(\#\mathbb{F}_\infty - 1)$th root of unity, but $\operatorname{Aut}\phi = A^\times = \mathbb{F}_q^\times$, so $u^{-1}\phi u$ depends only on the image of u modulo $\mathbb{F}_q^\times$. This explains the principal homogeneous space claim. □

Introduce the following notation:

$$\mathscr{Y}^+(L) := \text{the set of sgn-normalized rank 1 Drinfeld } A\text{-modules over } L$$
$$\mathcal{P}^+ := \{(c) : c \in K^\times \text{ and } \operatorname{sgn} c = 1\} \subseteq \mathcal{P}$$
$$\operatorname{Pic}^+ A := \mathcal{I}/\mathcal{P}^+, \quad \text{the narrow class group of } A.$$

Lemma 6.9. *If $\phi \in \mathscr{Y}^+(L)$, then $\operatorname{Stab}_{\mathcal{I}} \phi = \mathcal{P}^+$.*

Proof. The following are equivalent for a nonzero integral ideal I not divisible by $\operatorname{char}_A \phi$:

- $I * \phi = \phi$;
- $\phi_I \phi_a = \phi_a \phi_I$ for all $a \in A$;

- $\phi_I \in \operatorname{End}\phi$;
- $\phi_I \in A$;
- $\phi_I = \phi_b$ for some $b \in A$.

In particular, if I is an integral ideal in $\mathcal{P}^+$, then $I = (b)$ for some $b \in A$ with $\operatorname{sgn} b = 1$, so $\phi_I = \phi_b$, so $I \in \operatorname{Stab}_{\mathcal{I}} \phi$. Using weak approximation, one can show that the integral ideals in $\mathcal{P}^+$ generate the group $\mathcal{P}^+$, and that a general ideal I can be multiplied by an ideal in $\mathcal{P}^+$ to make it integral and not divisible by $\operatorname{char}_A \phi$.

Thus it remains to show that when I is an integral ideal not divisible by $\operatorname{char}_A \phi$, the condition $\phi_I = \phi_b$ implies $I \in \mathcal{P}^+$. Suppose that $\phi_I = \phi_b$. Taking kernels yields $\phi[I] = \phi[b]$. Since $\operatorname{char}_A \phi \nmid I$, the group scheme $\phi[I]$ is reduced, so $\operatorname{char}_A \phi \nmid b$. By Proposition 3.13, $I = \operatorname{Ann}_A \phi[I] = \operatorname{Ann}_A \phi[b] = (b)$. Also, $\eta(\operatorname{sgn} b) = \text{l.c.}(\phi_b) = \text{l.c.}(\phi_I) = 1$, so $\operatorname{sgn} b = 1$. Thus $I \in \mathcal{P}^+$. □

THEOREM 6.10. *The action of $\mathcal{I}$ on Drinfeld modules makes $\mathscr{Y}^+(C)$ a principal homogeneous space under* $\operatorname{Pic}^+ A$.

PROOF. Lemma 6.9 implies that $\mathscr{Y}^+(C)$ is a disjoint union of principal homogeneous spaces under $\operatorname{Pic}^+ A$, so it suffices to check that $\mathscr{Y}^+(C)$ and $\#\operatorname{Pic}^+ A$ are finite sets of the same size. Theorems 6.8 and 6.5 imply

$$\#\mathscr{Y}^+(C) = \#\mathscr{Y}(C) \cdot \#(\mathbb{F}_\infty^\times/\mathbb{F}_q^\times) = \#\operatorname{Pic} A \cdot \#(\mathbb{F}_\infty^\times/\mathbb{F}_q^\times).$$

On the other hand, the exact sequence

$$1 \longrightarrow \mathcal{P}/\mathcal{P}^+ \longrightarrow \mathcal{I}/\mathcal{P}^+ \longrightarrow \mathcal{I}/\mathcal{P} \longrightarrow 1$$

and the isomorphism $\mathcal{P}/\mathcal{P}^+ \xrightarrow{\sim} \mathbb{F}_\infty^\times/\mathbb{F}_q^\times$ induced by sgn show that

$$\#\operatorname{Pic}^+ A = \#\operatorname{Pic} A \cdot \#(\mathbb{F}_\infty^\times/\mathbb{F}_q^\times).$$ □

6.5. The narrow Hilbert class field. Choose $\phi \in \mathscr{Y}^+(C)$. Define

$$H^+ := K(\text{all coefficients of } \phi_a \text{ for all } a \in A) \subseteq C.$$

Then ϕ is a Drinfeld module over H^+, and so is $I * \phi$ for any $I \in \mathcal{I}$. By Theorem 6.10, these are all the objects in $\mathscr{Y}^+(C)$, so H^+ is also the extension of K generated by the coefficients of ϕ_a for *all* $\phi \in \mathscr{Y}^+(C)$ and all $a \in A$. In particular, H^+ is independent of the choice of ϕ. It is called the narrow Hilbert class field of (A, sgn).

THEOREM 6.11.

(a) *The field H^+ is a finite abelian extension of K.*
(b) *The extension $H^+ \supseteq K$ is unramified above every finite place ("finite" means not ∞).*
(c) *We have* $\operatorname{Gal}(H^+/K) \simeq \operatorname{Pic}^+ A$.

PROOF.

(a) The group $\operatorname{Aut}(C/K)$ acts on $\mathscr{Y}^+(C)$, so it maps H^+ to itself. Also, H^+ is finitely generated over K. These imply that H^+ is a finite normal extension of K.

By Corollary 6.2, each rank 1 Drinfeld module over C is isomorphic to one over K_∞, and it can be made sgn-normalized over the field F obtained by adjoining to K_∞ the $(\#\mathbb{F}_\infty - 1)$th root of some element. Then $H^+ \subset F$. On the other hand, the extensions $K \subseteq K_\infty \subseteq F$ are separable, so H^+ is separable over K.

The automorphism group of $\mathscr{Y}^+(C)$ as a principal homogeneous space under $\operatorname{Pic}^+ A$ equals $\operatorname{Pic}^+ A$, so we have an injective homomorphism

$$\chi\colon \operatorname{Gal}(H^+/K) \hookrightarrow \operatorname{Aut} \mathscr{Y}^+(C) \simeq \operatorname{Pic}^+ A.$$

Thus $\operatorname{Gal}(H^+/K)$ is a finite abelian group.

(b) Let B^+ be the integral closure of A in H^+. Let $P \subset B^+$ be a nonzero prime ideal, lying above $\mathfrak{p} \subset A$. Let $\mathbb{F}_P = B^+/P$. By Corollary 4.3, each $\phi \in \mathscr{Y}^+(H^+) = \mathscr{Y}^+(C)$ is a Drinfeld module over the localization B_P^+, so there is a reduction map

$$\rho\colon \mathscr{Y}^+(H^+) \to \mathscr{Y}^+(\mathbb{F}_P).$$

By Lemma 6.9, $\operatorname{Pic}^+ A$ acts faithfully on the source and target. Moreover, the map ρ is $(\operatorname{Pic}^+ A)$-equivariant, and $\mathscr{Y}^+(H^+)$ is a principal homogeneous space under $\operatorname{Pic}^+ A$ by Theorem 6.10, so ρ is injective.

If an automorphism $\sigma \in \operatorname{Gal}(H^+/K)$ belongs to the inertia group at P, then σ acts trivially on $\mathscr{Y}^+(\mathbb{F}_P)$, so σ acts trivially on $\mathscr{Y}^+(H^+)$, so $\sigma = 1$. Thus $H^+ \supseteq K$ is unramified at P.

(c) Let $\operatorname{Frob}_\mathfrak{p} := \operatorname{Frob}_P \in \operatorname{Gal}(\mathbb{F}_P/\mathbb{F}_\mathfrak{p}) \hookrightarrow \operatorname{Gal}(H^+/K)$ be the Frobenius automorphism. The key point is the formula

$$\operatorname{Frob}_\mathfrak{p} \ \phi = \mathfrak{p} * \phi$$

for any $\phi \in \mathscr{Y}^+(\mathbb{F}_P)$; let us now prove this. By definition, if $\psi := \mathfrak{p} * \phi$, then $\psi_a \phi_\mathfrak{p} = \phi_\mathfrak{p} \phi_a$ for all $a \in A$. By Corollary 3.15, $\phi_\mathfrak{p} = \tau^{\deg \mathfrak{p}}$, so $\psi_a \tau^{\deg \mathfrak{p}} = \tau^{\deg \mathfrak{p}} \phi_a$. Compare coefficients; since $\tau^{\deg \mathfrak{p}}$ acts on $\mathbb{F}_P$ as $\operatorname{Frob}_\mathfrak{p}$, we obtain $\psi = \operatorname{Frob}_\mathfrak{p} \ \phi$.

Since $\mathscr{Y}^+(H^+) \to \mathscr{Y}^+(\mathbb{F}_P)$ is injective and $(\operatorname{Pic}^+ A)$-equivariant, it follows that $\operatorname{Frob}_\mathfrak{p}$ acts on $\mathscr{Y}^+(H^+)$ too as $\phi \mapsto \mathfrak{p} * \phi$. Thus $\chi\colon \operatorname{Gal}(H^+/K) \hookrightarrow \operatorname{Pic}^+ A$ maps $\operatorname{Frob}_\mathfrak{p}$ to the class of $\mathfrak{p}$ in $\operatorname{Pic}^+ A$. Such classes generate $\operatorname{Pic}^+ A$, so χ is surjective. □

6.6. The Hilbert class field. Because of the exact sequence

$$0 \longrightarrow \mathcal{P}/\mathcal{P}^+ \longrightarrow \operatorname{Pic}^+ A \longrightarrow \operatorname{Pic} A \longrightarrow 0,$$

the extension $H^+ \supseteq K$ decomposes into two abelian extensions

$$\begin{array}{c} H^+ \\ \big| \ \mathcal{P}/\mathcal{P}^+ \\ H \\ \big| \ \operatorname{Pic} A \\ K \end{array}$$

with Galois groups as shown. The map of sets $\mathscr{Y}^+(C) \twoheadrightarrow \mathscr{Y}(C)$ is compatible with the surjection of groups $\operatorname{Pic}^+ A \twoheadrightarrow \operatorname{Pic} A$ acting on the sets. By Corollary 6.2, each element of $\mathscr{Y}(C)$ is represented by a Drinfeld module over K_∞, so the decomposition group $D_\infty \subseteq \operatorname{Gal}(H^+/K)$ acts trivially on $\mathscr{Y}(C)$. Thus $D_\infty \subseteq \mathcal{P}/\mathcal{P}^+$. In other words, ∞ splits completely in $H \supseteq K$.

The Hilbert class field H_A of A is defined as the maximal unramified abelian extension of K in which ∞ splits completely. Thus $H \subseteq H_A$. On the other hand,

$\mathrm{Gal}(H/K) \simeq \mathrm{Pic}\, A \simeq \mathrm{Gal}(H_A/K)$, the latter isomorphism coming from class field theory. Hence $H = H_A$.

6.7. Ray class fields. In this section, we generalize the constructions to obtain *all* the abelian extensions of K, even the ramified ones. Introduce the following notation:

$$\begin{aligned}
\mathfrak{m}: &\quad \text{a nonzero ideal of } A\\
\mathcal{I}_{\mathfrak{m}} &:= \text{the subgroup of } \mathcal{I} \text{ generated by primes not dividing } \mathfrak{m}\\
\mathcal{P}_{\mathfrak{m}} &:= \{(c) : c \in K \text{ and } c \equiv 1 \bmod \mathfrak{m}\}\\
\mathcal{P}^+_{\mathfrak{m}} &:= \{(c) : c \in K \text{ and } \operatorname{sgn} c = 1 \text{ and } c \equiv 1 \bmod \mathfrak{m}\}\\
\mathrm{Pic}_{\mathfrak{m}} A &:= \mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}, \text{ the ray class group modulo } \mathfrak{m} \text{ of } A\\
\mathrm{Pic}^+_{\mathfrak{m}} A &:= \mathcal{I}_{\mathfrak{m}}/\mathcal{P}^+_{\mathfrak{m}}, \text{ the narrow ray class group modulo } \mathfrak{m} \text{ of } (A, \operatorname{sgn})\\
\mathscr{Y}^+_{\mathfrak{m}}(C) &:= \{(\phi, \lambda) : \phi \in \mathscr{Y}^+(C) \text{ and } \lambda \text{ generates the } A/\mathfrak{m}\text{-module } \phi[\mathfrak{m}](C)\}\\
H^+_{\mathfrak{m}} &:= H^+(\lambda) \text{ for any } (\phi, \lambda) \in \mathscr{Y}^+_{\mathfrak{m}}(C)\\
&\qquad (\text{the narrow ray class field modulo } \mathfrak{m} \text{ of } (A, \operatorname{sgn}))\\
H_{\mathfrak{m}} &:= \text{the subfield of } H^+_{\mathfrak{m}} \text{ fixed by } \mathcal{P}_{\mathfrak{m}}/\mathcal{P}^+_{\mathfrak{m}}\\
&\qquad (\text{the ray class field modulo } \mathfrak{m} \text{ of } A).
\end{aligned}$$

Arguments similar to those in previous sections show the following:

THEOREM 6.12.

(a) *There is an action of* $\mathcal{I}_{\mathfrak{m}}$ *on* $\mathscr{Y}^+_{\mathfrak{m}}(C)$ *making* $\mathscr{Y}^+_{\mathfrak{m}}(C)$ *a principal homogeneous space under* $\mathrm{Pic}^+_{\mathfrak{m}} A$.

(b) *The field* $H^+_{\mathfrak{m}}$ *is a finite abelian extension of* K*, unramified outside* $\mathfrak{m}$*, and* $\mathrm{Gal}(H^+_{\mathfrak{m}}/K) \simeq \mathrm{Pic}^+_{\mathfrak{m}} A$.

(c) *The extension* $H_{\mathfrak{m}}$ *is the ray class field modulo* $\mathfrak{m}$ *of* A *as classically defined, with* $\mathrm{Gal}(H_{\mathfrak{m}}/K) \simeq \mathrm{Pic}_{\mathfrak{m}} A$.

6.8. The maximal abelian extension. Theorem 6.12 implies that $\bigcup_{\mathfrak{m}} H_{\mathfrak{m}}$ equals $K^{\mathrm{ab},\infty}$, the maximal abelian extension of K in which ∞ splits completely. Finally, if ∞' is a second closed point of X, then the compositum $K^{\mathrm{ab},\infty}K^{\mathrm{ab},\infty'}$ is the maximal abelian extension of K.

6.9. Example of an explicit Hilbert class field. We follow [**Hay91**, Example 3]; see [**Hay91**, **DH94**] for other examples similar to this one.

Let $q = 2$. Let X be the elliptic curve over $\mathbb{F}_2$ associated to the equation $y^2 + y = x^3$. Let ∞ be the point at infinity on X. Then $A = \mathbb{F}_2[x, y]/(y^2 + y - x^3)$. Since $\mathbb{F}_\infty^\times = \{1\}$, there is only one possible sgn, and $\mathcal{P}/\mathcal{P}^+ \simeq \mathbb{F}_\infty^\times/\mathbb{F}_q^\times \simeq \{1\}$, so $\mathrm{Pic}^+ A \simeq \mathrm{Pic}\, A \simeq \mathrm{Pic}^0 X \simeq X(\mathbb{F}_2)$, which is of order 3. Thus $H^+ = H$ and $[H : K] = 3$.

Our goal is to use Drinfeld modules to find an explicit equation defining H as an extension of K. By definition, to give a sgn-normalized rank 1 Drinfeld A-module over a given field extension L of K is to give elements $a, c_1, c_2 \in L$ such that the elements

$$\begin{aligned}
\phi_x &= x + aT + T^2\\
\phi_y &= y + c_1 T + c_2 T^2 + T^3
\end{aligned}$$

of $L\{\tau\}$ satisfy $\phi_x\phi_y = \phi_y\phi_x$ and $\phi_y^2 + \phi_y = \phi_x^3$. In fact, the second condition is redundant: if ϕ_x commutes with ϕ_y, then ϕ_x commutes with $\phi_y^2 + \phi_y - \phi_x^3$, but in $L\{\tau\}$ if an element with nonzero constant term commutes with an element with zero constant term, the second element is 0, as one sees by equating coefficients.

Thus the only condition is $\phi_x\phi_y = \phi_y\phi_x$, which amounts to the system

$$\begin{aligned} xc_1 + ay^2 &= ay + c_1x^2 \\ xc_2 + ac_1^2 + y^4 &= y + c_1a^2 + c_2x^4 \\ x + ac_2^2 + c_1^4 &= c_1 + c_2a^4 + x^8 \\ a + c_2^4 &= c_2 + a^8 \end{aligned}$$

in the unknowns a, c_1, c_2. The first two equations let us eliminate c_1 and c_2 in turn (remember that x and y are constants in K), so we are left with two polynomials in $K[a]$ that must vanish. Their gcd turns out to be $a^3+(x^2+x)a^2+(x+1)^2a+(x+1)^4$, so H is the extension of K generated by a root of this cubic polynomial.

Remark 6.13. One could also find an equation for H by working analytically, just as one can use lattices in $\mathbb{C}$ to compute CM j-invariants numerically. In both settings, the result can be made rigorous by invoking integrality properties.

Remark 6.14. Yet another way to find H would be to use geometric class field theory: Let F be the Frobenius endomorphism of X; then the extension of function fields $H \supseteq K$ arises from the finite étale covering $X \xrightarrow{F-1} X$.

Similar calculations can be done when $\deg\infty > 1$, but they are more complicated.

7. Drinfeld modular varieties

7.1. Classical modular curves. The classical modular curve $Y(1)$ is a coarse moduli space whose points over any algebraically closed field k are in bijection with isomorphism classes of elliptic curves over k. Over $\mathbb{C}$, the analytic description of elliptic curves as $\mathbb{C}/\Lambda$ with $\Lambda = \mathbb{Z}\tau + \mathbb{Z}$ for some $\tau \in \mathbb{C} - \mathbb{R}$ shows that

$$Y(1)(\mathbb{C}) \simeq \Gamma\backslash\Omega$$

where $\Omega := \mathbb{C} - \mathbb{R}$ (the union of the upper and lower half planes in $\mathbb{C}$) and $\Gamma := \mathrm{GL}_2(\mathbb{Z})$. (Equivalently, one could replace Ω with the upper half plane, and Γ by the index-2 subgroup $\mathrm{SL}_2(\mathbb{Z})$, but our formulation will be easier to adapt.)

Similarly, the modular curve $Y_1(N)$ is a coarse moduli space whose k-points over any algebraically closed field k of characteristic not dividing N are in bijection with isomorphism classes of pairs (E, P) where E is an elliptic curve over k, and $P \in E(k)$ is a point of exact order N. One can extend this description to define a functor on $\mathbb{Z}[1/N]$-schemes, and this functor is representable by a smooth relative affine curve over $\mathbb{Z}[1/N]$ once $N \geq 4$. Over $\mathbb{C}$, one has

$$Y_1(N)(\mathbb{C}) \simeq \Gamma_1(N)\backslash\Omega$$

where

$$\Gamma_1(N) := \left\{ \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \right\}.$$

(Since we are working in $\mathrm{GL}_2(\mathbb{Z})$ instead of $\mathrm{SL}_2(\mathbb{Z})$, it is not OK to replace the lower right * with 1.)

7.2. Drinfeld modular curves. Elliptic curves over $\mathbb{C}$ are described analytically by rank 2 lattices, so elliptic curves are analogous to rank 2 Drinfeld modules. Drinfeld modular curves classify rank 2 Drinfeld modules with level structure.

For simplicity, let us assume that $A = \mathbb{F}_q[T]$. Each rank 2 Drinfeld module has the form

$$\begin{aligned} \phi^{(a,b)} \colon A &\longrightarrow L\{\tau\} \\ T &\longmapsto T + a\tau + b\tau^2 \end{aligned}$$

for some $a \in L$ and $b \in L^\times$. The definition of morphism shows that $\phi^{(a,b)} \simeq \phi^{(a',b')}$ if and only if there exists $u \in L^\times$ such that $a' = u^{q-1}a$ and $b' = u^{q^2-1}b$. So $j := a^{q+1}/b$ is invariant under isomorphism, like the j-invariant of an elliptic curve.

The Drinfeld modular curve $Y(1)$ classifying rank 2 Drinfeld modules without level structure is a coarse moduli space isomorphic to $\mathbb{A}^1$ with coordinate j. Analytically,

$$Y(1)(C) \simeq \Gamma \backslash \Omega$$

where $\Omega := C - K_\infty$ (the Drinfeld upper half plane) and $\Gamma := \mathrm{GL}_2(A)$.

Similarly, for each nonzero $n \in A$, the Drinfeld modular curve $Y_1(n)$ classifies rank 2 Drinfeld modules equipped with a torsion point of exact order n. One can make this more precise by specifying a functor on $A[1/n]$-schemes. The functor is representable by a smooth relative curve over $A[1/n]$ when n is nonconstant.

EXAMPLE 7.1. Let us describe $Y_1(T^2)$ explicitly. First consider triples (a, b, z) where $\phi_{T^2}(z) = 0$ and $\phi_T(z) \neq 0$. These are described by the equations $\phi_T(z) = y$ and $\phi_T(y) = 0$ with $y \neq 0$. In other words,

$$\begin{aligned} Tz + az^q + bz^{q^2} &= y \\ T + ay^{q-1} + by^{q^2-1} &= 0. \end{aligned}$$

Eliminating y rewrites this system as the single equation

$$T + a(Tz + az^q + bz^{q^2})^{q-1} + b(Tz + az^q + bz^{q^2})^{q^2-1} = 0.$$

Another triple (a', b', z') gives rise to an isomorphic Drinfeld module with torsion point if and only if there exists an invertible u such that $a' = u^{q-1}a$, $b' = u^{q^2-1}b$, $z' = u^{-1}z$. So $Y_1(T^2)$ is the quotient of the above affine scheme by an action of $\mathbb{G}_m$. The quotient can be obtained simply by setting $z = 1$, to obtain

$$T + a(T + a + b)^{q-1} + b(T + a + b)^{q^2-1} = 0.$$

So $Y_1(T^2)$ is the relative curve defined by this equation in $\mathbb{A}^2_{A[1/T]} = \operatorname{Spec} A[1/T][a, b]$.

For much more on Drinfeld modular curves, see [**Gek86**].

7.3. Drinfeld modular varieties and stacks. More generally, given any $r \geq 1$ and nonzero ideal $\mathfrak{n} \leq A$, Drinfeld [**Dri74**, §5] defined the notion of (full) level $\mathfrak{n}$ structure on a rank r Drinfeld A-module, and he proved that the functor

$$\begin{aligned} \boldsymbol{A}\textbf{-schemes} &\longrightarrow \textbf{Sets} \\ S &\longmapsto \{\text{Drinfeld } A\text{-modules over } S \text{ with level } \mathfrak{n} \text{ structure}\}/\text{isomorphism} \end{aligned}$$

is representable by an A-scheme Y, provided that $\mathfrak{n}$ is not too small (Drinfeld assumes that $\mathfrak{n}$ is divisible by at least two distinct primes of A). Applying deformation theory to analogues of formal groups and p-divisible groups, he proved also that

$Y \to \operatorname{Spec} A$, after removing the fibers above primes dividing $\mathfrak{n}$, is smooth of relative dimension $r-1$.

Without any restriction on $\mathfrak{n}$, one can define a moduli *stack* $\mathscr{Y}$ and take its coarse space Y. Like classical modular curves and Shimura varieties, these can also be compactified.

EXAMPLE 7.2 ([**Dri74**, §8]). Suppose that $r = 1$ and $\mathfrak{n} = (1)$ (no level structure). Then $\mathscr{Y}$ is of relative dimension 0 over $\operatorname{Spec} A$, and its coarse space Y is a finite A-scheme.

- For $A = \mathbb{F}_q[T]$, there is only one rank 1 Drinfeld module over C up to isomorphism (the Carlitz module). We have $Y = \operatorname{Spec} A$.
- For more general A, define

$$H := \text{the Hilbert class field of } A$$
$$\mathcal{O}_H := \text{the integral closure of } A \text{ in } H.$$

  Then $Y = \operatorname{Spec} \mathcal{O}_H$, so we have bijections

$$Y(C) \longleftrightarrow \{A\text{-embeddings } \mathcal{O}_H \to C\} \longleftrightarrow \{K\text{-embeddings } H \to C\}.$$

  These are principal homogeneous spaces under $\operatorname{Pic} A \simeq \operatorname{Gal}(H/K)$, in accordance with Theorem 6.5.

Acknowledgements

I thank Francesc Fité and the referees for comments.

References

[And86] Greg W. Anderson, *t-motives*, Duke Math. J. **53** (1986), no. 2, 457–502, DOI 10.1215/S0012-7094-86-05328-7. MR850546 ↑3.4

[Car35] Leonard Carlitz, *On certain functions connected with polynomials in a Galois field*, Duke Math. J. **1** (1935), no. 2, 137–168, DOI 10.1215/S0012-7094-35-00114-4. MR1545872 ↑5

[Car38] Leonard Carlitz, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), no. 2, 167–182, DOI 10.2307/1990037. MR1501937 ↑5.1

[DH87] Pierre Deligne and Dale Husemoller, *Survey of Drinfel'd modules*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, pp. 25–91, DOI 10.1090/conm/067/902591. MR902591 ↑1

[Dri74] V. G. Drinfel'd, *Elliptic modules*, Mat. Sb. (N.S.) **94(136)** (1974), 594–627, 656 (Russian). MR0384707 ↑1, 5.2, 6, 7.3, 7.2

[Dri77] V. G. Drinfel'd, *Elliptic modules. II*, Mat. Sb. (N.S.) **102(144)** (1977), no. 2, 182–194, 325 (Russian). MR0439758 ↑1

[DH94] D. S. Dummit and David Hayes, *Rank-one Drinfel'd modules on elliptic curves*, Math. Comp. **62** (1994), no. 206, 875–883, DOI 10.2307/2153547. With microfiche supplement. MR1218342 ↑6.9

[Gek83] Ernst-Ulrich Gekeler, *Zur Arithmetik von Drinfel'd-Moduln*, Math. Ann. **262** (1983), no. 2, 167–182, DOI 10.1007/BF01455309 (German). MR690193 ↑3.6

[Gek86] Ernst-Ulrich Gekeler, *Drinfel'd modular curves*, Lecture Notes in Mathematics, vol. 1231, Springer-Verlag, Berlin, 1986. MR874338 ↑7.2

[Gek91] Ernst-Ulrich Gekeler, *On finite Drinfel'd modules*, J. Algebra **141** (1991), no. 1, 187–203, DOI 10.1016/0021-8693(91)90211-P. MR1118323 ↑3.6

[GPRG97] E.-U. Gekeler, M. van der Put, M. Reversat, and J. Van Geel (eds.), *Drinfeld modules, modular schemes and applications*, World Scientific Publishing Co., Inc., River Edge, NJ, 1997. MR1630594 ↑1

[Gos96] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996. MR1423131 ↑1

[GHR92] David Goss, David R. Hayes, and Michael I. Rosen (eds.), *The arithmetic of function fields*, Ohio State University Mathematical Research Institute Publications, vol. 2, Walter de Gruyter & Co., Berlin, 1992. MR1196508 ↑1

[Hay74] D. R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91, DOI 10.2307/1996848. MR330106 ↑5.2

[Hay79] David R. Hayes, *Explicit class field theory in global function fields*, Studies in algebra and number theory, Adv. in Math. Suppl. Stud., vol. 6, Academic Press, New York-London, 1979, pp. 173–217. MR535766 ↑6

[Hay91] David R. Hayes, *On the reduction of rank-one Drinfel'd modules*, Math. Comp. **57** (1991), no. 195, 339–349, DOI 10.2307/2938678. MR1079021 ↑6.9

[Hay92] David R. Hayes, *A brief introduction to Drinfel'd modules*, The arithmetic of function fields (Columbus, OH, 1991), Ohio State Univ. Math. Res. Inst. Publ., vol. 2, de Gruyter, Berlin, 1992, pp. 1–32. MR1196509 ↑1

[Lau96] Gérard Laumon, *Cohomology of Drinfeld modular varieties. Part I*, Cambridge Studies in Advanced Mathematics, vol. 41, Cambridge University Press, Cambridge, 1996. Geometry, counting of points and local harmonic analysis. MR1381898 ↑1

[Lau97] Gérard Laumon, *Cohomology of Drinfeld modular varieties. Part II*, Cambridge Studies in Advanced Mathematics, vol. 56, Cambridge University Press, Cambridge, 1997. Automorphic forms, trace formulas and Langlands correspondence; With an appendix by Jean-Loup Waldspurger. MR1439250 ↑1

[Ros02] Michael Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657 ↑1

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005) ↑2.1

[Tha04] Dinesh S. Thakur, *Function field arithmetic*, World Scientific Publishing Co., Inc., River Edge, NJ, 2004. MR2091265 ↑1

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA

Email address: poonen@math.mit.edu

URL: http://math.mit.edu/~poonen/