INTRODUCTION TO DRINFELD MODULES

BJORN POONEN

Our goal is to introduce Drinfeld modules and to explain their application to explicit class field theory. First, however, to motivate their study, let us mention some of their applications.

1. Applications

(1) 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 extension of imaginary quadratic fields). Here global function field means $\mathbb{F}_p(T)$ or a finite extension.
(2) Langlands conjectures for GL_n over function fields (Drinfeld modular varieties play the role of Shimura varieties).
(3) Modularity of elliptic curves over function fields: If $E/\mathbb{F}_p(T)$ has split multiplicative reduction at ∞, then E is dominated by a Drinfeld modular curve.
(4) Explicit construction of curves over finite fields with many points, as needed in coding theory, namely reductions of Drinfeld modular curves, which are easier to write equations for than the classical modular curves.

Only the first of these will be treated in these notes.

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 $\Lambda = \mathbb{Z}\omega_1 + \cdots \mathbb{Z}\omega_r$ with $\omega_1, \ldots, \omega_r$ linearly independent over $\mathbb{R}$.

$r = 0$:
$$\mathbb{C}/\Lambda \simeq \mathbb{C} = \mathbb{G}_a(\mathbb{C})$$

$r = 1$:
$$\begin{aligned} \mathbb{C}/\Lambda &\simeq \mathbb{C}^\times = \mathbb{G}_m(\mathbb{C}) \\ z &\mapsto \exp\left(\frac{2\pi i z}{\omega_1}\right). \end{aligned}$$

$r = 2$:
$$\begin{aligned} \mathbb{C}/\Lambda &\simeq E(\mathbb{C}) \qquad \text{elliptic curve} \\ z &\mapsto \left(\wp(z), \wp'(z)\right). \end{aligned}$$

$r > 2$ is impossible since $[\mathbb{C} : \mathbb{R}] = 2$.

Date: May 15, 2017.

This research was supported in part by National Science Foundation grants DMS-841321 and DMS-1601946 and a grant from the Simons Foundation (#402472 to Bjorn Poonen). The exposition draws upon many sources, and in particular, David R. Hayes, A brief introduction to Drinfel'd modules, *The arithmetic of function fields (Columbus, OH, 1991)*, 1–32, Ohio State Univ. Math. Res. Inst. Publ., **2**, de Gruyter, Berlin, 1992.

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 choose a closed point $\infty \in X$. Let $\mathscr{O}(X - \{\infty\})$ denote the affine 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 $a \in A$, define $|a| := \#(A/a) = q^{\deg a}$; extend this to K, K_∞, and C in turn. The field C is algebraically closed as well as complete with respect to $|\ |$.

Finite rank $\mathbb{Z}$-submodules of C are just finite-dimensional $\mathbb{F}_p$-subspaces, not 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 PID, such as $\mathbb{F}_q[T]$, then all such Λ arise as follows: let $\{x_1, \ldots, x_r\}$ be a basis for a K_∞-subspace in C, and take $\Lambda = Ax_1 + \cdots + Ax_r \subset C$.

Note: 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 an surjective $\mathbb{F}_q$-linear map $C \to C$ with kernel Λ. If we require $\alpha_0 = 1$, then 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: if $e(z)$ exists, then

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

(Over $\mathbb{C}$, there would be an ambiguity of multiplication by a function $e^{g(z)}$, but in the nonarchimedean setting there is no entire exponential function.)

- 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.)
- $\ker e = \Lambda$. $\square$

Next: 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

$$\begin{tikzcd} C/\Lambda \arrow[r, "a"] \arrow[d, "e"', "\wr"] & C/\Lambda \arrow[d, "\wr"', "e"] \\ C \arrow[r, dotted, "\phi_a"] & C \end{tikzcd}$$

commute.

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

Proof. 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 makes the diagram above commute, because $\phi_a(e(z))$ and $e(az)$ have the same zeros and same coefficient of z. $\square$

Moreover, $\deg \phi_a = |a|^r$.

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 $c \in \mathbb{F}_q$. 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* must be $\mathbb{F}_q$-linear:

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

where we think of τ as the Frobenius operator $x \mapsto x^q$, and each $a \in L$ acts as $x \mapsto ax$. The ring $L\{\tau\}$ is a twisted polynomial ring: $\tau a = a^q \tau$ for each $a \in L$.

For $f \in L\{\tau\}$, let l.c.(f) denote the leading coefficient of f; by convention, l.c.$(0) = 0$.

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 $\iota\colon A \to L$.

So L is an extension of K (e.g., C) and ι is an inclusion, or L is an extension of $A/\mathfrak{p}$ for some nonzero prime $\mathfrak{p}$ of A.

Definition 3.2. The A-characteristic of L is $\operatorname{char}_A L := \ker \iota$, a prime ideal of A.

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

Definition 3.3. 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 3.4. 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 still rules out $A \xrightarrow{\iota} L \subset L\{\tau\}$ when $\operatorname{char}_A L \neq 0$, however; we must rule this out to make Proposition 3.6 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 would be nicer to give an algebraic definition that makes sense over any A-field.

Let ϕ be a Drinfeld module. For each nonzero $a \in A$, 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 3.5. 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 3.6 (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). Thus $\phi \colon A \to L\{\tau\}$ extends to a homomorphism $\phi \colon K \to L((\tau))$, and v pulls back to a nontrivial valuation v_K on K. We have $v_K(a) = -M(a) \le 0$ for all $a \in A - \{0\}$, so $v_K = rv_\infty$ for some $r \in \mathbb{Q}_{\ge 0}$. Then $M(a) = -rv_\infty(a)$ for all $a \in A - \{0\}$. $\square$

Define the rank of ϕ to be r.

Drinfeld modules are 1-dimensional objects. 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 we knew...)

There is a higher-dimensional generalization called a t-module.

3.4. 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 $0 < h \le r$.)*

Proof. 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 $h \in \mathbb{Q}_{>0}$. $\square$

Call h the height of ϕ.

3.5. 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.,

$$\begin{array}{ccc} \mathbb{G}_a & \xrightarrow{\phi_a} & \mathbb{G}_a \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ \mathbb{G}_a & \xrightarrow{\psi_a} & \mathbb{G}_a \end{array} \tag{1}$$

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.

Proposition 3.9. *Isogenous Drinfeld modules have the same rank (just as one cannot have a nonzero algebraic morphism $\mathbb{G}_m \to E$).*

Proof. If $f\colon \phi \to \psi$ is an isogeny between Drinfeld modules of rank r and r', respectively, then (1) gives

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

for all a, so $r = r'$. $\square$

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 nonconstant $a \in A$, 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; one can solve for each α_i in turn. Show 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. $\square$

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

3.6. **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 $\phi[I] := \ker \phi_I$.

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

$$\begin{tikzcd}
0 \arrow[r] & \ell^{-1}F/F \arrow[r] \arrow[d, "i_1"] & \ell^{-(e+1)}F/F \arrow[r, "\ell"] \arrow[d, dotted, "i_{e+1}"] & \ell^{-e}F/F \arrow[r] \arrow[d, "i_e"] & 0 \\
0 \arrow[r] & D[\ell] \arrow[r] & D[\ell^{e+1}] \arrow[r, "\ell"] & D[\ell^e] \arrow[r] & 0.
\end{tikzcd}$$

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

Proposition 3.13. *Let ϕ be a 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 $\operatorname{char}_A L = \mathfrak{p} \neq 0$, 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 $\#\phi[I] = \#\phi[I]^0 \cdot \#\phi[I](L)$ 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), $\phi[\mathfrak{p}](L) = 0$. Since $\phi_{\mathfrak{p}}$ is monic, it 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 $\phi_{\mathfrak{p}} = \tau^{\deg \mathfrak{p}}$. □

3.7. **Tate module.** 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 $K_\ell := \operatorname{Frac} A_\ell$. 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.

Applications:

- 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

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

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.

For simplicity, let us assume that $\operatorname{Pic} R = 0$; this holds if the A-algebra R is a PID, 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* $\text{l.c.}(\phi_a) \in R^\times$ for all nonzero $a \in A$. The last requirement, which implies injectivity of ϕ, 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 $\text{l.c.}(\phi_a) \in R^\times$ 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 the Drinfeld module $a \mapsto (\phi_a \bmod \mathfrak{m})$ over $\mathbb{F}$ has 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 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 $u^{-1}\phi_{a_i}u$ have nonnegative valuation, and there exist i and $j > 0$ such that the coefficient of τ^j in ϕ_{a_i} has valuation 0. □

Corollary 4.3. *Let ϕ be a rank 1 Drinfeld module over L. If there exists $a \in A - \mathbb{F}_q$ such that $\mathrm{l.c.}(\phi_a) \in R^\times$, then ϕ is a Drinfeld module over R. In particular, ϕ has good reduction.*

Proof. Left as an exercise. □

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

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

Define

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

Carlitz proved in the 1930s, long before Drinfeld, 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. *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 $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \xrightarrow{\sim} (\mathbb{Z}/n)^\times$.)

Theorem 5.2 (Analogue of Kronecker–Weber)**.** *Every abelian extension of K in which the place ∞ splits completely is contained in $K(\phi[a])$ for some a.*

6. Class field theory

6.1. **The class group.** When A is not a PID, class field theory is more complicated. Introduce the following notation:

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

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

6.2. **Rank 1 Drinfeld modules over C.**

Proposition 6.1. *We have bijections*

$$\begin{aligned}\operatorname{Pic} A &\xrightarrow{\sim} \frac{\{\text{rank 1 } A\text{-lattices in } C\}}{\text{homothety}} \xrightarrow{\sim} \frac{\{\text{rank 1 Drinfeld modules over } C\}}{\text{isomorphism}} \\ [I] &\longmapsto (\text{homothety class of } I \text{ in } C)\end{aligned}$$

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

Theorem 6.5. *The set $\mathscr{X}(C)$ 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 abelian 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

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

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 3.6. 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:

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

Lemma 6.9. *If $\phi \in \mathscr{X}^+(L)$, 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, $\eta(\operatorname{sgn} b) = \operatorname{l.c.}(\phi_b) = \operatorname{l.c.}(\phi_I) = 1$, so $\operatorname{sgn} b = 1$. Thus $I \in \mathcal{P}^+$. □

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

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

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

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 $\phi \in \mathscr{X}^+(C)$. 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 $\mathscr{X}^+(C)$, so H^+ is also the extension of K generated by the coefficients of ϕ_a for all $\phi \in \mathscr{X}^+(C)$ 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 $\mathscr{X}^+(C)$, 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 a field obtained by adjoining a $(\#\mathbb{F}_\infty - 1)$th root. The completion K_∞ of a global field K is a separable extension of K, and adjoining $(\#\mathbb{F}_\infty - 1)$th roots produces a field F separable over K_∞ with $F \supseteq H^+$, so H^+ is separable over K.

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

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

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 $\phi \in \mathscr{X}^+(H^+) = \mathscr{X}^+(C)$ is a Drinfeld module over the localization B_P^+, so there is a reduction map

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

By Lemma 6.9, $\operatorname{Pic}^+ A$ acts faithfully on the source and target. Moreover, the map ρ is $\operatorname{Pic}^+ A$-equivariant, and $\mathscr{X}^+(H^+)$ 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 $\mathscr{X}^+(\mathbb{F}_P)$, so σ acts trivially on $\mathscr{X}^+(H^+)$, 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 $\phi \in \mathscr{X}^+(\mathbb{F}_P)$; 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 $\mathscr{X}^+(H^+) \to \mathscr{X}^+(\mathbb{F}_P)$ is injective and $\operatorname{Pic}^+ A$-equivariant, it follows that $\operatorname{Frob}_{\mathfrak{p}}$ acts on $\mathscr{X}^+(H^+)$ 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 $\mathscr{X}^+(C) \twoheadrightarrow \mathscr{X}(C)$ 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 $\mathscr{X}(C)$ is represented by a Drinfeld module over K_∞, so the decomposition group $D_\infty \subseteq \operatorname{Gal}(H^+/K)$ acts trivially on $\mathscr{X}(C)$. 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 $H \subseteq H_A$. Class field theory shows that $\operatorname{Gal}(H_A/K) \simeq \operatorname{Pic} A$, so $H = H_A$.

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:

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

Arguments similar to those in previous sections show the following:

Theorem 6.12.

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

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

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

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.

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

Email address: poonen@math.mit.edu

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