Introduction to Drinfeld modules

Jiangxue Fang

January 12, 2021

The goal of this note is to introduce Drinfeld modules and explain their application to explicitly class field theory of function fields.

1 Analytic theory

1.1 Inspiration from characteristic zero

Let Λ be a discrete $\mathbb{Z}$-submodule of $\mathbb{C}$ of finite rank r. We must have $r \leq 2$. Write $\Lambda = \mathbb{Z}\omega_1 + \cdots + \mathbb{Z}\omega_r$.

$r = 0, \mathbb{C}/\Lambda \simeq \mathbb{G}_{\mathrm{a}}(\mathbb{C})$, additive group;

$r = 1, \mathbb{C}/\Lambda \simeq \mathbb{G}_{\mathrm{m}}(\mathbb{C}) = \mathbb{C}^*,\ z \mapsto \exp(2\pi i z/\omega)$, multiplicative group;

$r = 2, \mathbb{C}/\Lambda \simeq E(\mathbb{C}),\ z \mapsto (\mathcal{P}(z), \mathcal{P}'(z))$, elliptic curve.

1.2 Characteristic p analogue

Throughout this note, we keep the following notations.

$\mathbb{F}_q$: a finite field of q-elements of characteristic p;

X: a geometrically connected smooth projective curve over $\mathbb{F}_q$;

K: the function field of X;

∞: a fix closed point of X with residue field $\mathbb{F}_\infty$ and degree $d_\infty = \dim_{\mathbb{F}_q}(\mathbb{F}_\infty)$;

$A = \Gamma(X - \{\infty\}, \mathcal{O}_X)$;

K_∞: the completion of K at the point ∞;

C: the completion of an algebraic closure $\overline{K_\infty}$ of K_∞.

We have a one-to-one correspondence between the set of closed points of X and the set of discrete valuations on K. For any $x \in |X|$, let v_x be the corresponding discrete valuation on K. Then

$$A = \{a \in K | v_x(a) \geq 0 \text{ for any } x \in |X| - \{\infty\}\}.$$

There is a homomorphism $\deg : K^* \to \mathbb{Z}$ such that $\deg(a) = \dim_{\mathbb{F}_q}(A/aA)$ for any $0 \neq a \in A$. By the product formula, $-d_\infty v_\infty(a) = \deg(a)$ for any $a \in K^*$. Actually, we can define $\deg(I)$ to be $\dim_{\mathbb{F}_q}(A/I)$ for any nonzero ideal I of A.

Lemma 1.1. *A is discrete in K_∞ and the quotient K_∞/A is compact.*

Proof. For any $n > 0$, applying $R\Gamma(X, \bullet)$ to the short exact sequence

$$0 \to \mathcal{O}_X \to \mathcal{O}_X(n\infty) \to \mathcal{O}_X(n\infty)/\mathcal{O}_X \to 0,$$

we have an exact sequence

$$0 \to H^0(X, \mathcal{O}_X) \to H^0(X, \mathcal{O}_X(n\infty)) \to H^0(X, \mathcal{O}_X(n\infty)/\mathcal{O}_X) \to H^1(X, \mathcal{O}_X) \to H^1(X, \mathcal{O}_X(n\infty)) \to 0.$$

By taking direct limit and using the fact $H^1(X, \mathcal{O}_X(n\infty)) = 0$ for $n \gg 0$, we get an exact sequence

$$0 \to H^0(X, \mathcal{O}_X) \to A \to K_\infty/\mathcal{O}_\infty \to H^1(X, \mathcal{O}_X) \to 0,$$

where $\mathcal{O}_\infty$ is the discrete valuation ring of K_∞. Then

$$0 \to H^0(X, \mathcal{O}_X) \to \mathcal{O}_\infty \to K_\infty/A \to H^1(X, \mathcal{O}_X) \to 0$$

is also exact. Since $H^i(X, \mathcal{O}_X)$ is finite dimensional over $\mathbb{F}_q$, then K_∞/A is compact. □

Definition 1.2. A lattice in **C** is a discrete A-submodule of **C** of finite rank, where the rank of an A-module M is defined to be $\dim_K(K \otimes_A M)$.

By the following lemma, we have $\mathrm{rank}_A(\Lambda) = \dim_{K_\infty}(K_\infty \Lambda)$ for any lattice Λ in **C**.

Lemma 1.3. *Let L be a local field and R a discrete subring of L such that L/R is compact. Let V be a finitely dimensional L-vector space with the canonical topology and let M be an R-submodule of V. If M is discrete, then the canonical homomorphism $L \otimes_R M \to LM$ is an isomorphism. The converse also holds if M is projective over R. In both cases, M is finitely generated over R and $\dim_F(F \otimes_R M) = \dim_L(LM)$, where F is the fraction field of R.*

Proof. Suppose M is discrete. Choose an L-basis $m_1, \ldots, m_k$ of LM with $m_i \in M$ and set $M_0 = \sum_{i=1}^{k} Rm_i$. Since M is discrete, we can choose a neighborhood U_1 of 0 in V such that $U_1 \cap M = 0$. There is a neighborhood U of 0 in V such that $U - U \subset U_1$. Then for any $x, y \in M$, $x - y \in U$ if and only if $x = y$. It followss that $(U + M_0)/M_0 \cap M/M_0 = 0$ and hence M/M_0 is discrete in V/M_0 and LM/M_0. Since L/R is compact, $LM/M_o = \sum_{i=1}^{k}(L/R)m_i$ is compact and M/M_0 is thus a finite set. We have

$$\dim_L(L \otimes_R M) = \dim_F(F \otimes_R M) = \dim_F(F \otimes_R M_0) = k = \dim_L(LM).$$

Conversely, suppose M is projective over R and we have a canonical isomorphism $L \otimes_R M \simeq LM$. Then M is finitely generated over R and we can find an R-module N such that $M \oplus N$ is a free R-module of finite rank. Hence $M \oplus N$ is discrete in $L \otimes_R (M \oplus N)$ and hence M is discrete in $L \otimes_R M \simeq LM$. □

Remark 1.4. The rank of a lattice in $\mathbf{C}$ can be arbitrary large since $[\mathbf{C} : K_\infty] = +\infty$.

Definition 1.5. Let R be a ring containing $\mathbb{F}_q$. A polynomial $f \in R[z]$ is called $\mathbb{F}_q$-linear if $f(z + w) = f(z) + f(w) \in R[z, w]$ and $f(az) = af(z) \in R[z]$ for any $a \in \mathbb{F}_q$. We can also define $\mathbb{F}_q$-linear power series.

Lemma 1.6. *Let $f \in R[[z]]$. Then f is $\mathbb{F}_q$-linear if and only if $f = \sum_{i=0}^{\infty} a_i z^{q^i}$ for some $a_i \in R$.*

Proof. The if part is trivial. For the only if part, suppose $f = \sum_{n=0}^{\infty} a_n z^n$ is $\mathbb{F}_q$-linear. The equality $f(z+w) = f(z)+f(w)$ means that $a_n \mathrm{C}_n^i = 0$ if $1 \leq i \leq n-1$. If n is not a power of p, we can find $1 \leq i \leq n-1$ such that $p \nmid \mathrm{C}_n^i$ and hence $a_n = 0$. Now suppose n is a power of p. The equality $f(\alpha z) = \alpha f(z)$ means that $a_n(\alpha^n - \alpha) = 0$ for any $\alpha \in \mathbb{F}_q$. If n is not a power of q, we can find $\alpha \in \mathbb{F}_q$ such that $\alpha^n - \alpha \neq 0$ and hence $a_n = 0$. This prove the only if part. □

Theorem 1.7. *Let Λ be an A-lattice in $\mathbf{C}$. There exists an $\mathbb{F}_q$-linear entire power series $e_\Lambda(z) \in \mathbf{C}[[z]]$ which defines an $\mathbb{F}_q$-linear isomorphism $\mathbf{C}/\Lambda \simeq \mathbf{C}$.*

Proof. Define

$$e_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} (1 - \frac{z}{\lambda}).$$

Since Λ is discrete, then $e_\Lambda(z)$ is entire. Let's prove $e_\Lambda(z)$ is $\mathbb{F}_q$-linear.

Write $\Lambda = \bigcup_i \Lambda_i$ for some $\mathbb{F}_q$-subspace of Λ of finite dimension and set $e_i(z) = z \prod_{0 \neq \lambda \in \Lambda_i} (1 - \frac{z}{\lambda})$. Then $e_\Lambda(z) = \lim_i e_i(z)$. To prove $e_\Lambda(z)$ is $\mathbb{F}_q$-linear, we need only to show this for $e_i(z)$. For any $a \in \mathbb{F}_q$, by comparing the degrees, roots and coefficients in z of $e_i(az)$ and $ae_i(z)$, we have $e_i(az) = ae_i(z)$. Let $F(z, w) = e_i(z + w) - e_i(z) - e_i(w) \in \mathbf{C}[z]$. We can write $F(z, w) = \sum_{i=0}^{d-1} f_i z^i$ for some $f_i \in \mathbf{C}[w]$ of degree $< d$, where $d = \#\Lambda_i$. For any $\lambda \in \Lambda_i$, we have

$$F(z, \lambda) = e_i(z + \lambda) - e_i(z) - e_i(\lambda) = 0.$$

This shows each $\lambda \in \Lambda_i$ is a root of $f_i(z)$ for any i. But $\deg f_i < d$, we must have $f_i = 0$ and hence $F(z, w) = 0$. This show that $e_i(z)$ and hence $e_\Lambda(z)$ are $\mathbb{F}_q$-linear.

The entire series $e_\Lambda(z)$ define an $\mathbb{F}_q$-linear map $\mathbf{C} \to \mathbf{C}$ of analytic spaces with kernel Λ. By Weistrass representation theorem, $e_\Lambda(z) : \mathbf{C} \to \mathbf{C}$ is surjective. So we get an isomorphism $e_\Lambda(z) : \mathbf{C}/\Lambda \simeq \mathbf{C}$. □

Corollary 1.8. *For any $a \in A$, there exists a unique polynomial $\phi_a \in \mathbf{C}[z]$ making the following diagram commutes:*

$$\begin{array}{ccc} \mathbf{C}/\Lambda & \xrightarrow{a} & \mathbf{C}/\Lambda \\ \downarrow{\scriptstyle e_\Lambda} & & \downarrow{\scriptstyle e_\Lambda} \\ \mathbf{C} & \xrightarrow{\phi_a} & \mathbf{C}. \end{array}$$

Moreover, ϕ_a is a $\mathbb{F}_q$-linear polynomial of degree $q^{r \deg(a)}$ where r is the rank of the lattice Λ. For any $a, b \in A$, $\phi_a(\phi_b(z)) = \phi_{ab}(z)$.

Proof. Define

$$\phi_a(z) = az \prod_{0 \neq \lambda \in a^{-1}\Lambda/\Lambda} (1 - z/e_\Lambda(\lambda)).$$

Then $e_\Lambda(az)$ and $\phi_a(e_\Lambda(z))$ are two entire series with the same root set $a^{-1}\Lambda$ and with the same derivative a. So these two series only have simple roots and hence $e_\Lambda(az) = \phi_a(e_\Lambda(z))$. Moreover, $\phi_a(z)$ is $\mathbb{F}_q$-linear. The equality $\phi_a(\phi_b(z)) = \phi_{ab}(z)$ holds by the following commutative diagram

$$\begin{array}{ccccc} \mathbf{C}/\Lambda & \xrightarrow{a} & \mathbf{C}/\Lambda & \xrightarrow{b} & \mathbf{C}/\Lambda \\ \downarrow{\scriptstyle e_\Lambda} & & \downarrow{\scriptstyle e_\Lambda} & & \downarrow{\scriptstyle e_\Lambda} \\ \mathbf{C} & \xrightarrow{\phi_a} & \mathbf{C} & \xrightarrow{\phi_b} & \mathbf{C}. \end{array}$$

□

For any $\mathbb{F}_q$-algebra R, denote by τ the q-th power map on R and by $R\{\tau\}$ the twist polynomial ring with relation $\tau r = r^q \tau$ for any $r \in R$. We have a one-to-one correspondence

$$R\{\tau\} \simeq \{\mathbb{F}_q\text{-linear polynomials in } R[z]\},\ f = \sum_i a_i \tau^i \mapsto f(z) = \sum_i a_i z^{q^i}.$$

For any $f = \sum_i a_i \tau^i \in R\{\tau\}$, define $w(f) = \min\{i | a_i \neq 0\}$, $\deg(f) = \max\{i | a_i \neq 0\}$, $\text{c.t.}(f) = a_0$ and $\text{l.c.}(f) = a_{\deg(f)}$.

Thus any lattice Λ in $\mathbf{C}$ defines a ring homomorphism $\phi : A \to \mathbf{C}\{\tau\}$ sending a to ϕ_a whose constant term is a. This leads the definition of Drinfeld modules in the next section.

2 Algebraic theory

In this section, fix a homomorphism ι from A to a field L. The characteristic $\text{char}_A(L)$ of the A-field L is defined to be $\ker(\iota)$.

2.1 Basic definitions

Definition 2.1. A Drinfeld module over L is a ring homomorphism

$$\phi : A \to L\{\tau\},\ a \mapsto \phi_a,$$

such that $\text{c.t.}(\phi_a) = \iota(a)$ for any $a \in A$ and $\phi_a \neq \iota(a)$ for some $a \in A$.

Equivalently, a Drinfeld A-module over L is an A-module scheme over L whose underlying $\mathbb{F}_q$-vector space scheme is isomorphic to $\mathbb{G}_{\mathrm{a},L} = \text{Spec } L[z]$ and the A-module action on $\mathbb{G}_{\mathrm{a},L}$ is given by the ring homomorphism $\phi : A \to \text{End}_{\mathbb{F}_q}(\mathbb{G}_{\mathrm{a},L}) = L\{\tau\}$ satisfying the above conditions. So ϕ defines a functor

$$\phi : \text{Alg}_L \to \text{Mod}_A,\ R \mapsto \phi(R),$$

where $\phi(R) = R$ as abelian groups and the A-module structure on $\phi(R)$ is given by $a.r = \phi_a(r)$ for any $a \in A$ and $r \in R$.

2.2 Rank and height

Proposition 2.2. *Let ϕ be a Drinfeld module over L.*

(1) There exists a positive rational number r such that $\deg(\phi_a) = r \deg(a)$ for any $a \in A$.

(2) Suppose $\mathfrak{p} = \text{char}_A(L)$ is nonzero. Then there exists a positive rational number h such that $w(\phi_a) = h \deg(\mathfrak{p}) v_{\mathfrak{p}}(a)$ for any $a \in A$.

Proof. (1) Define $\mu(a) = -\deg(\phi_a)$ for any $a \in A$ and $\mu(0) = +\infty$. Then $\mu(ab) = \mu(a) + \mu(b)$ and $\mu(a+b) \geq \min\{\mu(a), \mu(b)\}$ for any $a, b \in A$. So we can extend μ to a nontrivial valuation $\bar{\mu} : K \to \mathbb{Z} \cup \{+\infty\}$ on K. As $\bar{\mu}(a) = -\deg(\phi_a) < 0$ for some $a \in A$, $\bar{\mu}$ is the valuation on K defined by $\infty \in X$. Then there exists a positive rational number r such that $\deg(\phi_a) = r \deg(a)$ for any $a \in A$.

(2) Define $\nu(a) = w(\phi_a)$ for any $a \in A$ and $\nu(0) = +\infty$. Then $\nu(ab) = \nu(a) + \nu(b)$ and $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$ for any $a, b \in A$. So we can extend ν to a valuation $\bar{\nu} : K \to \mathbb{Z} \cup \{+\infty\}$ on K. As $\bar{\nu}(a) > 0$ for any $a \in \mathfrak{p}$, $\bar{\nu}$ is the valuation on K corresponding to $\mathfrak{p}$. So there exists a positive rational number h such that $w(\phi_a) = h \deg(\mathfrak{p}) v_{\mathfrak{p}}(a)$ for any $a \in A$. □

Definition 2.3. The numbers r and h in Proposition 2.2 are called the rank and height of ϕ, respectively.

To show r and h are positive integers, we need to study the torsion points of Drinfeld modules.

2.3 Torsion points

Definition 2.4. Let ϕ be a Drinfeld module over L and let $a \in A$. For any L-algebra R, let

$$\phi[a](R) = \{r \in R | \phi_a(r) = 0\}$$

be the a-torsion submodule of the A-module $\phi(R)$. More generally, for any ideal I of A, let $\phi[I](R) = \bigcap_{i \in I} \phi[i](R)$.

Actually, the functor $\phi[a] : \mathrm{Alg}_L \to \mathrm{Mod}_A$ is the A-module scheme $\phi[a] = \ker(\phi_a : \mathbb{G}_{\mathrm{a},L} \to \mathbb{G}_{\mathrm{a},L})$ which is represented by the finite scheme Spec $L[z]/(\phi_a(z))$ over L of degree $q^{r \deg(a)}$.

If I is a nonzero ideal of A, then the left ideal $\sum_{i \in I} L\{\tau\}\phi_i$ of $L\{\tau\}$ is generated by a unique monic polynomial ϕ_I. Then the functor $\phi[I] : \mathrm{Alg}_L \to \mathrm{Mod}_A$ is represented by the finite scheme Spec $L[z]/(\phi_I(z))$ over L.

Lemma 2.5. *Let R be a Dedkind domain and M an R-module.*

(1) For any distinct maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ of R and any $e_1, \ldots, e_n \in \mathbb{N}$, we have

$$M[\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}] = \bigoplus_{i=1}^{n} M[\mathfrak{p}_i^{e_i}].$$

(2) If M is a divisible R-module, then for any maximal ideal $\mathfrak{p}$ of R and $e \in \mathbb{N}$, $M[\mathfrak{p}^e]$ is a free $R/\mathfrak{p}^e$-module of some rank r independent of e. Moreover, $M[\mathfrak{p}^\infty] := \bigcup_{e=1}^{\infty} M[\mathfrak{p}^e]$ is isomorphic to $(K_\mathfrak{p}/\widehat{R}_\mathfrak{p})^r$, where $\widehat{R}_\mathfrak{p}$ is the completion of R at $\mathfrak{p}$ and $L_\mathfrak{p}$ its fraction field.

Proof. (1) is obvious. The homomorphism $M \to M_\mathfrak{p}$ induces an isomorphism $M[\mathfrak{p}^e] \simeq M_\mathfrak{p}[\mathfrak{p}^e R_\mathfrak{p}]$. For (2), we may assume that R is a discrete valuation ring. Fix a uniformizer π of R and choose a free R-module F of rank r and an isomorphism $i_1 : \pi^{-1}F/F \simeq M[\pi]$ of $R/\mathfrak{p}$-modules. Let's construct an isomorphism $i_e : \pi^{-e}F/F \simeq M[\pi^e]$ of $R/\mathfrak{p}^e$-modules by induction on e. Given the isomorphism $i_e : \pi^{-e}F/F \simeq M[\pi^e]$, using divisablity of M, there is an isomorphism $i_{e+1} : \pi^{-e-1}F/F \simeq M[\pi^{e+1}]$ making the following diagram commutes:

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

So i_{e+1} is an isomorphism. The family $\{i_e\}$ is an isomorphism from the direct systems $\{\pi^{-e}F/F\}$ to $\{M[\pi^e]\}$ and hence $M[\mathfrak{p}^\infty] = \varinjlim_e \pi^{-e}F/F = (L_\mathfrak{p}/\widehat{R}_\mathfrak{p})^r$. □

Proposition 2.6. *Let ϕ be a Drinfeld module over an algebraically closed field L of rank r and height h.*

(1) If I is an ideal of A prime to $\mathrm{char}_A(L)$, then $\phi(L)[I]$ is a free A/I-module of rank r. In particular, r is a positive integer.

(2) Suppose $\mathfrak{p} = \mathrm{char}_A(L) \neq 0$. Then for any positive integer $e \in \mathbb{N}$, $\phi(L)[\mathfrak{p}^e]$ is a free $A/\mathfrak{p}^e$-module of rank $r - h$. In particular, h is a positive integer.

Proof. For any $0 \neq a \in A$, $\phi_a : L \to L$ is surjective. Hence $\phi(L)$ is A-divisible. By Lemma 2.5, we only need to show that for any maximal ideal $\mathfrak{p}$ of A, there exists a positive integer e such that $\#\phi(L)[\mathfrak{p}^e] = q^{er\deg(\mathfrak{p})}$ if $\mathfrak{p} \neq \mathrm{char}_A(L)$ and $\#\phi(L)[\mathfrak{p}^e] = q^{e(r-h)\deg(\mathfrak{p})}$ if $\mathfrak{p} = \mathrm{char}_A(L)$. Let e be the class number of A. Then $\mathfrak{p}^e = (a)$ for some $a \in A$. We have $\deg(a) = e\deg(\mathfrak{p})$ and $\deg(\phi_a) = er\deg(\mathfrak{p})$. If $\mathfrak{p} \neq \mathrm{char}_A(L)$, then $a \notin \mathfrak{p}$ and $\phi_a(z)$ is a separable polynomial of degree $q^{r\deg(a)}$, and thus $\#\phi(L)[\mathfrak{p}^e] = \#\phi(L)[a] = q^{r\deg(a)} = q^{er\deg(\mathfrak{p})}$. If $\mathfrak{p} = \mathrm{char}_A(L)$, then $w(\phi_a) = hv_\mathfrak{p}(a)\deg(\mathfrak{p}) = eh\deg(\mathfrak{p})$. In this case, $\#\phi(L)[\mathfrak{p}^e] = \#\phi(L)[a] = q^{e(r-h)\deg(a)} = q^{e(r-h)\deg(\mathfrak{p})}$. □

2.4 Drinfeld modules and lattices in $\mathbf{C}$

Definition 2.7. A morphism $f : \phi \to \psi$ of Drinfeld modules over L is a polynomial $f \in L\{\tau\}$ such that $\psi_a f = f\phi_a$ for any $a \in A$. In other words, a morphism from ϕ to ψ is an endomorphism f of the additive group scheme over L such that for any $a \in A$, the following diagram commutes:

$$\begin{array}{ccc} \mathbb{G}_{\mathrm{a},L} & \xrightarrow{f} & \mathbb{G}_{\mathrm{a},L} \\ \downarrow{\scriptstyle \phi_a} & & \downarrow{\scriptstyle \psi_a} \\ \mathbb{G}_{\mathrm{a},L} & \xrightarrow{f} & \mathbb{G}_{\mathrm{a},L}. \end{array}$$

We denote by $\mathrm{Hom}(\phi, \psi)$ the set of morphisms from ϕ to ψ. A nonzero morphism of Drinfeld modules is called an isogeny.

Proposition 2.8. *Isogenous Drinfeld modules have the same rank and height.*

Proof. For any $f \in \mathrm{Hom}(\phi, \psi)$, we have $\deg(\psi_a)+\deg(f) = \deg(f)+\deg(\phi_a)$ and hence $\deg(\psi_a) = \deg(\phi_a)$ for any $a \in A$. Then ϕ and ψ have the same rank by definition. So is the height. □

Definition 2.9. A morphism from an A-lattice Λ of $\mathbf{C}$ to another one Λ' of the same rank is an element $c \in \mathbf{C}$ such that $c\Lambda \subset \Lambda'$.

Theorem 2.10. *The functor from the categories of lattices in $\mathbf{C}$ to the categories of Drinfeld modules over $\mathbf{C}$ constructed in Corollary 1.8 defines an equivalence of categories. Moreover, any lattice and its corresponding Drinfeld module have the same rank.*

Proof. (1) Given a lattice Λ in $\mathbf{C}$ of rank r, define

$$e_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} (1 - \frac{z}{\lambda}),$$

and for any $0 \neq a \in A$, define

$$\phi_a(z) = az \prod_{0 \neq \lambda \in a^{-1}\Lambda/\Lambda} (1 - z/e_\Lambda(\lambda)).$$

Then $\phi_a(z)$ is an $\mathbb{F}_q$-linear polynomial of degree $q^{r\deg(a)}$ which defines a polynomial $\phi_a \in \mathbf{C}\{\tau\}$ of degree $r\deg(a)$. By Corollary 1.8, we get a Drinfeld module $\phi : A \to \mathbf{C}\{\tau\}$ over $\mathbf{C}$ of rank r.

(2) Let ϕ be a Drinfeld module over $\mathbf{C}$ of rank r. Choose $a \in A\backslash\mathbb{F}_q$ and write $\phi_a = \sum_{i=0}^{d} a_i\tau^i$. There exists a unique series $e_\phi = \sum_{i=0}^{\infty} e_i\tau^i \in \mathbf{C}\{\{\tau\}\}$ with $e_0 = 1$ and $e_\phi a = \phi_a e_\phi$ by the equalites

$$e_n(a^{q^n} - a) = a_d e_{n-d}^{q^d} + \cdots + a_1 e_{n-1}^{q} \ \ (n \geq 0).$$

As $d_\infty v_\infty(a) = -\deg(a) < 0$, we have

$$v_\infty(e_n) \geq \min\{v_\infty(a_d e_{n-d}^{q^d}), \ldots, v_\infty(a_1 e_{n-1}^q)\} - q^n v_\infty(a).$$

Thus there exists a positive real number c such that for $n \gg 0$,

$$\frac{v_\infty(e_n)}{q^n} \geq \min\{\frac{v_\infty(e_{n-1})}{q^{n-1}}, \ldots, \frac{v_\infty(e_{n-d})}{q^{n-d}}\} + c.$$

This proves $\lim_{n\to\infty} \frac{v_\infty(e_n)}{q^n} = +\infty$ and hence $e_\phi(z)$ is an entire function. For any $b \in A$, we have

$$(e_\phi^{-1}\phi_b e_\phi)a = e_\phi^{-1}\phi_b\phi_a e_\phi = e_\phi^{-1}\phi_a\phi_b e_\phi = a(e_\phi^{-1}\phi_b e_\phi) \in \mathbf{C}\{\{\tau\}\}.$$

If we write $e_\phi^{-1}\phi_b e_\phi = \sum_i b_i\tau^i$ for some $b_i \in \mathbf{C}$, then $b_i(a^{q^i} - a) = 0$ for any $i \geq 0$ and hence $b_i = 0$ for any $i \geq 1$. We must have $e_\phi^{-1}\phi_b e_\phi = b$ and $e_\phi b = \phi_b e_\phi$ for any $b \in A$. Let Λ be the kernel of the $\mathbb{F}_q$-linear map $e_\phi : \mathbf{C} \to \mathbf{C}$. Then Λ is a discrete A-submodule of $\mathbf{C}$. The isomorphism $e_\phi : \mathbf{C}/\Lambda \simeq \mathbf{C}$ induces an isomorphism $a^{-1}\Lambda/\Lambda \simeq \ker(e_\phi : \mathbf{C} \to \mathbf{C})$ which is a free A/aA-module of rank r by Proposition 2.6. To show Λ is a lattice, we only need to show it is a finitely generated A-module. By Lemma 1.3, it is sufficient to show $\dim_{K_\infty}(K_\infty\Lambda) < +\infty$. If not, we can find infinitely many elements $\lambda_1, \lambda_2, \ldots$ in Λ which are linearly independent over K_∞. Set $\Lambda_r = \sum_{i=1}^r K_\infty\lambda_i \cap \Lambda$ for each i. By Lemma 1.3, Λ_r is a finitely generated A-module of rank r. The natural monomorphism $a^{-1}\Lambda_r/\Lambda_r \to a^{-1}\Lambda/\Lambda$ implies $\#(a^{-1}\Lambda/\Lambda) > \#(a^{-1}\Lambda_r/\Lambda_r) = \#(A/aA)^r$, which contradicts to $a^{-1}\Lambda/\Lambda \simeq (A/aA)^r$. It follows that Λ is a lattice in $\mathbf{C}$ of rank r.

(3) Let Λ_1 and Λ_2 be two lattices in $\mathbf{C}$ of the same rank r, and let c be a nonzero element in $\mathbf{C}$ such that $c\Lambda_1 \subset \Lambda_2$. As $\Lambda_1 \subset c^{-1}\Lambda_2$, consider

$$f(z) = cz \prod_{0\neq\lambda\in c^{-1}\Lambda_2/\Lambda_1} (1 - z/e_{\Lambda_1}(\lambda)).$$

Then $f(z)$ is an $\mathbb{F}_q$-linear polynomial. Comparing the roots and coefficients of the entire series $e_{\Lambda_2}(cz)$ and $f(e_{\Lambda_1}(z))$, they must be equal. Let ϕ and ψ be the Drinfeld modules over $\mathbf{C}$ corresponding to Λ_1 and Λ_2, respectively. Then $f \in \mathrm{Hom}(\phi, \psi)$.

(4) Given a nonzero morphism $f : \phi \to \psi$ of Drinfeld modules over $\mathbf{C}$. Let Λ and W be their corresponding lattices. We have $e_\Lambda a = \phi_a e_\Lambda$, $e_W a = \psi_a e_W$ and $f\phi_a = \psi_a f$ for any $a \in A$. Then $(e_w^{-1} f e_\Lambda)a = a(e_W^{-1} f e_\Lambda) \in \mathbf{C}\{\{\tau\}\}$. We must have $e_w^{-1} f e_\Lambda = c \in \mathbf{C}^\times$ and then $c\Lambda \subset W$. $\square$

2.5 Endomorphism ring of Drinfeld modules

Given a Drinfeld module ϕ over L of rank r, denote by $\mathrm{End}(\phi)$ the ring of endomorphisms of ϕ. More precisely,

$$\mathrm{End}(\phi) = \{P \in L\{\tau\} | P\phi_a = \phi_a P \text{ for any } a \in A\}.$$

The ring homomorphism $A \to \mathrm{End}(\phi)$ by sending a to ϕ_a gives an A-module structure on $\mathrm{End}(\phi)$.

Proposition 2.11. *(1)* $\mathrm{End}(\phi)$ *is a projective A-module of rank* $\leq r^2$.

(2) If $r = 1$, the above ring homomorphism $A \to \mathrm{End}(\phi)$ is an isomorphism.

Proof. Fix some $a \in A \backslash \mathbb{F}_q$ and $a \notin \mathrm{char}_A(L)$. Claim that $\mathrm{End}(\phi) \otimes_A A/(a) \to \mathrm{End}_A(\phi[a](\overline{L}))$ is injective.

Indeed, suppose that $P \in \mathrm{End}(\phi)$ give rise to the trivial endomorphism on $\phi[a](\overline{L})$. Write $P = Q\phi_a + R$ for some $Q, R \in L\{\tau\}$ with $\deg(R) < \deg(\phi_a)$. Hence R acts trivial on $\phi[a](\overline{L})$. Since $a \notin \mathrm{char}_A(L)$, by Proposition 2.6 $\#\phi[a](\overline{L}) = q^{r\deg(a)}$. As $\deg(R(z)) < \deg(\phi_a(z)) = q^{r\deg(a)}$, we must have $R = 0$ and hence $P = Q\phi_a$. One can easily check that $Q \in \mathrm{End}(\phi)$. This proves the claim.

Define $\delta : \mathrm{End}(\phi) \to \mathbb{Z} \cup \{+\infty\}$ by $\delta(P) = -\deg(P)$. The mapping δ satisfies

1. $\delta(P) = \infty$ if and only if $P = 0$.
2. $\delta(PQ) = \delta(P) + \delta(Q)$ for any $P, Q \in \mathrm{End}(\phi)$.
3. $\delta(P + Q) \geq \min\{\delta(P), \delta(Q)\}$ for any $P, Q \in \mathrm{End}(\phi)$.
4. $\delta(a.P) = rd_\infty v_\infty(a) + \delta(P)$ for any $a \in A$ and $P \in \mathrm{End}(\phi)$.

Denote $M = \mathrm{End}(\phi)$. The mapping δ thus gives rise to a norm on the K_∞-vector space $K_\infty \otimes_A M$. Note that $\mathrm{End}(\phi)$ is discrete in $K_\infty \otimes_A M$.

Suppose $\dim_K(K \otimes_A M) = \infty$. Choose infinitely many $P_1, P_2, \ldots \in \mathrm{End}(\phi)$ which are linearly independent over K. Let $V_n = \sum_{i=1}^{n} K_\infty P_i$ and $M_n = V_n \cap M$. By Lemma 1.3, M_n is a projective A-module of rank n. The canonical monomorpshim $a^{-1}M_n/M_n \to a^{-1}M/M$ implies that $\#(a^{-1}M/M) \geq \#(a^{-1}M_n/M_n) = q^{n\deg(a)}$ for each n. This contradicts to the claim that $\#(a^{-1}M/M) \leq q^{r^2\deg(a)}$. Hence $\dim_K(K \otimes_A M)A \leq r^2$ and (1) holds.

If $r = 1$, $\mathrm{End}(\phi)$ is an invertible A-module. The monomorphism $A \to \mathrm{End}(\phi)$ induces an isomorphism $K \simeq K \otimes_A \mathrm{End}(\phi)$. So $\mathrm{End}(\phi)$ can be viewed as a subring of K which is integral over A. But A is integrally closed in K, we must have $A = \mathrm{End}(\phi)$. □

3 Carlitz module and cyclotomic function fields

In this section, we will construct the cyclotomic extensions of the rational function field $\mathbb{F}_q(t)$ by the Carlitz module.

Let ϕ be a Drinfeld module over an A-field L of rank r. Fix an algebraic closure $\overline{L}$ of L. Recall that $\phi[I](\overline{L}) = \{x \in \overline{L} | \phi_i(x) = 0 \text{ for any } i \in I\}$ for any nonzero ideal I of A. Let L_I be the field extension of L by adding $\phi[I](\overline{L})$. For any $\sigma \in \mathrm{Gal}(\overline{L}/L)$, σ preserves $\phi[I](\overline{L})$ and L_I/L is thus a finite normal extension.

Suppose I is prime to $\mathrm{char}_A(L)$. Then $I^e = (a)$ for some positive integer e and some $a \in A$ with $\iota(a) \neq 0$. In other words, $\phi_a(z) \in L[z]$ is separable and $L_{(a)}/L$ is separable. So L_I/L is Galois and we also have a canonical monomorphism

$$\chi : \mathrm{Gal}(L_I/L) \hookrightarrow \mathrm{Aut}_A(\phi[I]) \simeq \mathrm{GL}_r(A/I). \tag{3.1}$$

In particular, L_I/L is an abelian extension if $r = 1$.

In the remainder of this section, suppose $A = \mathbb{F}_q[t]$ and consider the Carlitz module

$$C : A \to K\{\tau\},\ t \mapsto t + \tau$$

over $K = \mathbb{F}_q(t)$. For any $0 \neq a \in A$, let $C[a] = \{\lambda \in \mathbf{C} | C_a(\lambda) = 0\}$ and $K_a = K(C[a])$. Then $C[a]$ is a free A/aA-module of rank one.

Theorem 3.1. *(1) K_a/K is an abelian Galois extension of Galois group $(A/aA)^\times$.*

(2) For any maximal ideal $\mathfrak{p}$ of A, K_a/K is ramified at $\mathfrak{p}$ if and only if $a \in \mathfrak{p}$.

(3) Let $\mathcal{O}_a$ be the integral closure of A in K_a and let λ be a generator of the A-module $C[a]$. We have $\mathcal{O}_a = A[\lambda]$.

Proof. First suppose $a = p^e$ for some positive integer e and some monic irreducible polynomial $p(z)$ of degree d. The composition $A \xrightarrow{C} A\{\tau\} \to A/pA\{\tau\}$ defines a Drinfeld module $\overline{C} : A \to A/pA\{\tau\}$ over A/pA of rank 1 and height 1. So $\overline{C}_{p^e} = \tau^{de} \in A/pA\{\tau\}$ and hence $C_{p^e} - \tau^{de} \in pA\{\tau\}$. Define

$\phi_{p^e}(z) = C_{p^e}(z)/C_{p^{e-1}}(z)$. Then $\phi_{p^e}(z) = C_p(C_{p^{e-1}}(z))/C_{p^{e-1}}(z) \in A[z]$ and $\phi_{p^e}(z) \equiv z^{q^{de}-q^{d(e-1)}}$ (mod $pA[z]$). The constant term of $\phi_{p^e}(z)$ is p. In other words, $\phi_{p^e}(z)$ is an Eisenstein polynomial over A with respect to the prime ideal pA and so it is irreducible over K. For any generator λ of the A-module $C[p^e]$, we have $C_{p^e}(\lambda) = 0$ but $C_{p^{e-1}}(\lambda) \neq 0$. Thus $\phi_{p^e}(z)$ is the minimal polynomial over K of any generator of $C[p^e]$ and $K_{p^e} = K(\lambda)$. So for any $0 \neq b \in A$ prime to p, we have an isomorphism of fields

$$\sigma_b : K_{p^e} \simeq K_{p^e} \text{ by } \sigma_b(\lambda) = C_b(\lambda).$$

This proves that

$$\chi : \mathrm{Gal}(K_{p^e}/K) \simeq \mathrm{Aut}_A(C[p^e]) \simeq (A/(p^e))^\times.$$

Moreover, K_{p^e}/K is totally ramified at pA.

Let's compute the discriminant $\delta = d(1, \lambda, \ldots, \lambda^{\phi(p^e)-1})$ where $\phi(b) = \#(A/bA)^\times$ for any $b \in A$. By the definition of discriminant,

$$\pm\delta = \pm\det(\sigma\lambda^i)_{\substack{\sigma\in\mathrm{Gal}(K_{p^e}/K)\\ 0\le i<\phi(p^e)}} = \prod_{x\neq y\in(A/p^eA)^\times} (C_x(\lambda) - C_y(\lambda)).$$

Differenting both sides of $C_{p^e}(z) = C_{p^{e-1}}(z)\phi_{p^e}(z)$ and substituting $z = \lambda$, we have $p^e = C_{p^{e-1}}(\lambda)\phi'_{p^e}(\lambda)$. Differenting $\phi_{p^e}(z) = \prod_{y\in(A/p^eA)^\times} (z - C_y(\lambda))$ and substituting $z = C_x(\lambda)$, we have

$$\phi'_{p^e}(C_x(\lambda)) = \prod_{y\in(A/p^eA)^\times,\, y\neq x} (C_x(\lambda) - C_y(\lambda)).$$

Then

$$\begin{aligned}
\pm\delta &= \prod_{x\in(A/pA)^\times} \phi'_{p^e}(C_x(\lambda)) \\
&= \prod_{\sigma\in\mathrm{Gal}(K_{p^e}/K)} \sigma(\phi'_{p^e}(\lambda)) = N_{K_{p^e}/K}(\phi'_{p^e}(\lambda)) \\
&= N_{K_{p^e}/K}(p^e)/N_{K_{p^e}/K}(C_{p^{e-1}}(\lambda)) \\
&= N_{K_{p^e}/K}(p^e)/N_{K_{p^e}/K_p}(N_{K_p/K}(C_{p^{e-1}}(\lambda))) \\
&= \pm p^{q^{(e-1)d}(eq^d-e-1)}.
\end{aligned}$$

Let $w \in \mathcal{O}_{p^e}$. Then $w = \sum_{i=0}^{\phi(p^e)-1} a_i\lambda^i$ for some $a_i \in K$. Hence

$$\mathrm{Tr}_{K_{p^e}/K}(w\lambda^j) = \sum_{i=0}^{\phi(p^e)-1} a_i \mathrm{Tr}_{K_{p^e}/K}\lambda^{i+j}) \in A \text{ for any } 0 \le j < \phi(p^e).$$

Set $T = (\mathrm{Tr}_{K_{p^e}/K}(\lambda^{i+j}))_{0\le i,j<\phi(p^e)}$, $a = (a_0, \dots, a_{\phi(p^e)-1})$ and $b = (\mathrm{Tr}w, \dots, \mathrm{Tr}(w\lambda^{\phi(p^e)-1}))$. We have $b = aT$ and $bT^* = \delta a$. This shows $\delta a_i \in A$. Since δ is a power of p, we have $p^n w = \sum_{i=0}^{\phi(p^e)-1} b_i\lambda^i$ for some $n \in \mathbb{N}$ and $b_i \in A$ such that at least one b_i not divided by p. Let i_0 be the smallest integer such that $v_p(b_{i_0}) = 0$. Since $v_p(\lambda) = 1/\phi(p^e)$, we have $v_p(b_{i_0}\lambda^{i_0}) < v_p(b_i\lambda^i)$ for any $i \ne i_0$. So

$$n \le v_p(p^n w) = v(\sum_{i=0}^{\phi(p^e)-1} b_i\lambda^i) = v_p(b_{i_0}\lambda^{i_0}) = i_0/\phi(p^e) < 1.$$

We must have $n = 0$ and then $w \in A[\lambda]$. So $\mathcal{O}_{p^e} = A[\lambda]$ and $1, \lambda, \dots, \lambda^{\phi(p^e)-1}$ is an integral basis of $\mathcal{O}_{p^e}/A$. Hence $\delta_{\mathcal{O}_{p^e}/A}$ is a power of p. As a consequence, K_{p^e}/K is unramified at any prime ideal of A not equal to pA. We prove the theorem for $a = p^e$.

For general a, write $a = p_1^{e_1}\cdots p_t^{e_t}$ for some pairwise different irreducible polynomials p_i and some $e_i \in \mathbb{N}$. We prove our theorem by induction on t. Let $b = p_1^{e_1}\cdots p_{t-1}^{e_{t-1}}$ and λ a generator of $C[a]$. Then $C_b(\lambda)$ is a generator of $C[p_t^{e_t}]$ and $C_{p_t^{e_t}}(\lambda)$ is a generator of $C[b]$. By induction, our theorem holds for b and $p_t^{e_t}$. Choose $f, g \in A$ such that $fb + gp_t^{e_t} = 1$. We have $\lambda = C_f(C_b(\lambda)) + C_g(C_{p_t^{e_t}}(\lambda))$ and thus $K_a = K_b \cdot K_{p_t^{e_t}}$. Now $K_b \cap K_{p_t^{e_t}} = K$, because K_b is unramified at p_tA and $K_{p_t^{e_t}}$ is totally ramified at p_tA. As a consequence,

$$[K_a : K] = [K_b : K] \cdot [K_{p_t^{e_t}} : K] = \phi(b)\phi(p_t^{e_t}) = \phi(a).$$

So the monomorphism $\chi : \mathrm{Gal}(K_a/K) \hookrightarrow (A/aA)^\times$ given in (3.1) is an isomorphism. □

Corollary 3.2. *For any $b \in A$ prime to a, there exists a unique $\sigma_b \in \mathrm{Gal}(K_a/K)$ such that $\sigma_b(\lambda) = C_b(\lambda)$ for any generator λ of $C[a]$. In particular, if b is a monic irreducible polynomial furthermore, $\sigma_b = (bA, K_a/K)$.*

4 Reduction theory

4.1 Drinfeld modules over rings

We can also define Drinfeld modules over arbitrary A-algebras or even A-schemes. In such generalizing, the underlying $\mathbb{F}_q$-vector space scheme need only be locally isomorphic to $\mathbb{G}_a$, so it should be the $\mathbb{F}_q$-vector space scheme associated to a line bundle on the base scheme.

For simplicity, let R be an A-algebra with $\mathrm{Pic}R = 0$. This holds if R is a principle ideal domain. Then a Drinfeld module over R is a ring homomorphism

$$\phi : A \to R\{\tau\},\ a \to \phi_a$$

such that c.t.$(\phi_a) = a \in R$ and l.c.$(\phi_a) \in R^\times$ for any $0 \neq a \in A$ and $\phi_a \neq a$ for some $a \in A$. Then for any maximal ideal $\mathfrak{m}$ of R, $\phi \mod \mathfrak{m}$ yields a Drinfeld module over $R/\mathfrak{m}$ of the same rank.

4.2 Reduction theory of Drinfeld modules

Let R be a discrete valuation ring with fraction field L, maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}$. Let $v : K^\times \to \mathbb{Z}$ be the discrete valuation.

Definition 4.1. Let ϕ be a Drinfeld module over L of rank r.

(1) We say ϕ has integral coefficients if $\phi(A) \subset R\{\tau\}$ and the composition $A \xrightarrow{\phi} R\{\tau\} \to \mathbb{F}\{\tau\}$ defines a Drinfeld module over $\mathbb{F}$ of rank $0 < r_1 \leq r$.

(2) We say ϕ has stable reduction if it is isomorphic to a Drinfeld module ψ over L which has integral coefficients.

(3) We say ϕ has good reduction if ϕ is isomorphic to a Drinfeld module ψ over L such that $\psi(A) \subset R\{\tau\}$ and l.c.$(\psi_a) \in R^\times$ for any $0 \neq a \in A$.

(4) We say ϕ has potentially stable (resp. good) reduction if there exists a finite extension (L', v') of (L, v) such that ϕ has stable (resp. good) reduction on L'.

Lemma 4.2. *Let ϕ and ψ be two Drinfeld modules over L of the same rank. If ϕ and ψ have integral coefficients, then for any isomorphism $c : \phi \simeq \psi$, we have $c \in R^\times$.*

Proof. Choose $a \in A \backslash \mathbb{F}_q$ such that $\deg(\phi_a \mod \mathfrak{m}) > 0$. Write $\phi_a = \sum_i a_i \tau^i$ for some $a_i \in R$. There exists $n > 0$ such that $a_n \in R^\times$ and $a_i \in \mathfrak{m}$ for any $i > m$. As $\psi_a = c\phi_a c^{-1} \in R\{\tau\}$, we have $c^{1-q^n} a_n \in R$. This implies $c^{-1} \in R$. Similarly, $\psi = c^{-1}\phi c$ implies $c \in R$. This proves $c \in R^\times$. □

Corollary 4.3. *If ϕ has stable reduction which is isomorphic to a Drinfeld module ψ having integral coefficients, then the isomorphic class of ψ* mod $\mathfrak{m}$ *does not depend on the choice of ψ.*

Lemma 4.4. *Let ϕ be a Drinfeld module over K. Then ϕ has stable reduction on some finite extension L' of K.*

Proof. Choose $a_1, \ldots, a_n \in A$ which generates A as an $\mathbb{F}_q$-algebra. Write each $\phi_{a_i} = \sum_j a_{ij} \tau^j$ for some $a_{ij} \in L$ and set $c = \min_{i,j \geq 1} \frac{v(a_{ij})}{q^j - 1}$. Let n be the denominator of the rational number c. Let L' be a totally ramifeld extension of L of index n and let $\alpha \in L'$ with $v(\alpha) = c$. Put $\psi_a = \alpha \phi_a \alpha^{-1}$ for any $a \in A$. Then $\psi_{a_i} = \sum_j a_{ij} \alpha^{1-q^j} \tau^j \in R'\{\tau\}$ for any $1 \leq i \leq n$ and $a_{ij} \alpha^{1-q^j} \in R'^\times$ for some

$1 \leq i \leq n$ and $j \geq 1$ where R' is the valuation ring of L'. This shows that $\psi : A \to L'\{\tau\}$ has integral coefficients. In other words, ϕ has stable reduction over L'. □

Corollary 4.5. *Let ϕ be a Drinfeld module over L of rank 1. If there exists $a \in A \backslash \mathbb{F}_q$ 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. By Lemma 4.4, there exists a finite ramifield extension L' of L and $\alpha \in L'$ such that $\alpha\phi\alpha^{-1}(A) \subset R'\{\tau\}$ and the composition $A \xrightarrow{\alpha\phi\alpha^{-1}} R'\{\tau\} \to R'/\mathfrak{m}'\{\tau\}$ defines a rank one Drinfeld module over $R'/\mathfrak{m}'$, where R' is the discrete valuation ring of L' and $\mathfrak{m}'$ is the maximal ideal of R'. So $\deg(\alpha\phi_b\alpha^{-1}) = \deg(\alpha\phi_b\alpha^{-1} \bmod \mathfrak{m}') = \deg(b)$ and hence $\mathrm{l.c.}(\alpha\phi_b\alpha^{-1}) = \mathrm{l.c.}(\phi_b)\alpha^{1-q^{\deg a}} \in R'^\times$ for any $b \in A$. In particular, $\mathrm{l.c.}(\phi_a)\alpha^{1-q^{\deg(a)}} \in R'^\times$. Since $\mathrm{l.c.}(\phi_a) \in R^\times$, we have $\alpha \in R'^\times$. So $\phi_b \in R\{\tau\}$ and $\mathrm{l.c.}(\phi_b) \in R^\times$ for any $b \in R$. In other words, ϕ is a Drinfeld module over R. □

5 Class field theory

Let $\mathcal{I}$ be the group of fractional A-ideals in K, $\mathcal{P}$ the group of principle fractional A-ideals in K, and $\mathrm{Pic}A = \mathcal{I}/\mathcal{P}$ the ideal class group of A. In this section, fix an A-field L.

5.1 Rank one Drinfeld modules over C

Proposition 5.1. *We have bijections*

$$\mathrm{Pic}A \simeq \{\textit{rank 1 lattices in } \mathbf{C}\}/\textit{homothety} \simeq \{\textit{rank 1 Drinfeld modules over } \mathbf{C}\}/\textit{isomorphism}.$$

Proof. We need only to consider the first map. For injectivity, let I and I' be two fractional ideals of K such that they are homothety in $\mathbf{C}$. That is $I = cI'$ for some $c \in \mathbf{C}$. We must have $c \in K^\times$. For surjectivity, take a lattice Λ in $\mathbf{C}$ of rank 1 and $0 \neq \lambda \in \Lambda$. Replacing Λ by $\lambda^{-1}\Lambda$, we may assume that $1 \in \Lambda$. The injective homomorphism $\Lambda \to K \otimes_A \Lambda = K$ implies that Λ is a fractional ideal of K. □

Proposition 5.2. *Every rank 1 Drinfeld module ϕ over $\mathbf{C}$ is isomorphic to one defined over K_∞.*

Proof. Let Λ be the corresponding lattice in $\mathbf{C}$ to ϕ. By Proposition 5.1, we may assume $\Lambda \subset K \subset K_\infty$. By the construction of $e_\Lambda(z)$ in Theorem 1.7 and $\phi_a(z)$ in Corollary 1.8, we have $e_\Lambda(z) \in K_\infty[[z]]$ and $\phi_a \in K_\infty\{\tau\}$ for any $a \in A$. □

5.2 The action of ideals on Drinfeld modules

Let ϕ be a Drinfeld module over L of rank r and height h. For any nonzero ideal I of A, the left ideal $\sum_{i\in I} L\{\tau\}\phi_i$ of $L\{\tau\}$ is generated by a unique monic polynomial ϕ_I. The scheme Spec $L[z]/(\phi_I(z))$ represents the functor

$$\phi[I] : \mathrm{Alg}_L \to \mathrm{Mod}_A, \quad R \mapsto \phi(R)[I].$$

We have $\#\phi[I](\overline{L}) = q^{\deg(\phi_I)-w(\phi_I)}$.

Lemma 5.3. *(1)* $\deg(\phi_I) = r\deg(I)$.

(2) $w(\phi_I) = 0$ *if* $0 = \mathrm{char}_A(L)$ *and* $w(\phi_I) = hv_{\mathfrak{p}}(I)\deg(\mathfrak{p})$ *if* $0 \neq \mathfrak{p} = \mathrm{char}_A(L)$.

Proof. First claim that there exists an ideal J of A prime to I such that $J \nsubseteq \mathfrak{p}$ and $IJ = (a)$ for some $a \in A$.

Indeed, choose $a_{\mathfrak{q}} \in \mathfrak{q}^{v_{\mathfrak{p}}(I)} \backslash \mathfrak{q}^{v_{\mathfrak{q}}(I)+1}$ for each maximal ideal $\mathfrak{q}$ of A dividing I or $\mathfrak{q} = \mathfrak{p}$. By strong approximation theorem, there exists $a \in K^\times$ such that $v_{\mathfrak{q}}(a - a_{\mathfrak{q}}) > v_{\mathfrak{q}}(I)$ for any maximal ideal $\mathfrak{q}$ of A dividing I or $\mathfrak{q} = \mathfrak{p}$ and $v_{\mathfrak{q}}(a) \geq 0$ otherwise. Thus $a \in I$ and $v_{\mathfrak{q}}(a) = v_{\mathfrak{q}}(I)$ when $\mathfrak{q}|I$ or $\mathfrak{q} = \mathfrak{p}$. Take $J = aI^{-1}$. Then J is an ideal of A satisfying the required conditions.

So we have an isomorphism $\phi[a] \simeq \phi[I] \oplus \phi[J] : \mathrm{Alg}_L \to \mathrm{Mod}_A$ of functors and hence

$$\mathrm{Spec}\, L[z]/(\phi_a(z)) = \mathrm{Spec}\, L[z]/(\phi_I(z)) \times_L \mathrm{Spec}\, L[z]/(\phi_J(z)) = \mathrm{Spec}\, L[z]/(\phi_I(z)) \otimes_L L[z]/(\phi_J(z)).$$

So $\deg(\phi_a(z)) = \deg(\phi_I(z)) \cdot \deg(\phi_J(z))$ and $\deg(\phi_a) = \deg(\phi_I) + \deg(\phi_J)$. By counting elements of both sides of $\phi[a](\overline{L}) = \phi[I](\overline{L}) \oplus \phi[J](\overline{L})$, we have $q^{\deg(\phi_a)-w(\phi_a)} = q^{\deg(\phi_I)-w(\phi_I)} q^{\deg(\phi_J)-w(\phi_J)}$ and hence $\deg(\phi_a) - w(\phi_a) = \deg(\phi_I) - w(\phi_I) + \deg(\phi_J) - w(\phi_J)$. So $w(\phi_a) = w(\phi_I) + w(\phi_J)$. By $\deg(a) = \deg(I) + \deg(J)$ and $v_{\mathfrak{p}}(a) = v_{\mathfrak{p}}(I) + v_{\mathfrak{p}}(J)$, it suffices to prove the lemma for (a) and J.

As $\mathrm{l.c.}(\phi_a)\phi_{(a)} = \phi_a$, the lemma holds for (a) by the definitions of rank and height. By Proposition 2.6, we have $\#\phi[J](\overline{L}) = q^{r\deg(J)}$. Choose positive integer n such that $J^n = (b)$ for some $b \in A$. T $\iota(b) \neq 0$ and $\phi_b(z)$ is a separable polynomial over L and so is $\phi_I(z)$. This implies that $\#\phi[J](\overline{L}) = \deg(\phi_J(z))$ and hence $\deg(\phi_J) = r\deg(J)$ and $w(\phi_J) = 0 = hv_{\mathfrak{p}}(J)\deg(\mathfrak{p})$. □

Lemma 5.4. *Let I be a nonzero ideal of A. For any $a \in A$, $\phi_I\phi_a \in L\{\tau\}\phi_I$ and $\phi_I\phi_a = (I*\phi)_a\phi_I$ for a unique $(I*\phi)_a \in L\{\tau\}$. Then*

$$I*\phi : A \to L\{\tau\}, \ a \mapsto (I*\phi)_a$$

is a Drinfeld module over L and $\phi_I : \phi \to I * \phi$ is a isogeny.

Proof. Since ϕ_I is a generator of $\sum_{i\in I} L\{\tau\}\phi_i$, then $\phi_I = \sum_{i\in I} f_i\phi_i$ for some $f_i \in L\{\tau\}$. Hence $\phi_I\phi_a = \sum_{i\in I} f_i\phi_i\phi_a = \sum_{i\in I} f_i\phi_a\phi_i$ and hence $\phi_I\phi_a = (I*\phi)_a\phi_I$ for a unique $(I*\phi)_a \in L\{\tau\}$. Obviously, $I*\phi : A \to L\{\tau\},\ a \mapsto (I*\phi)_a$ is a ring homomorphism. By $\phi_I\phi_a = (I*\phi)_a\phi_I$, the constant term of $(I*\phi)_a$ is $\iota(a)^{q^{w(\phi_a)}}$. To show $I*\phi$ is a Drinfeld module, we need only to show that $\iota(a)^{q^{w(\phi_a)}} = \iota(a)$. If $w(\phi_a) = 0$, there is nothing to prove. Otherwise, by Lemma 5.3 we have $\mathrm{char}_A(L) = 0$ and $\mathfrak{p} = \mathrm{char}_A(L) \neq 0$ and $w(\phi_a) = hv_{\mathfrak{p}}(a)\deg(\mathfrak{p}) > 0$. In this case, $\iota(a)^{q^{\deg(\mathfrak{p})}} = \iota(a)$ and hence $\iota(a)^{q^{w(\phi_a)}} = \iota(a)$. □

Lemma 5.5. *(1) For any two nonzero ideals I and J of A, we have $(IJ)*\phi = J*(I*\phi)$.*

(2) For any $0 \neq a \in A$, we have $(a)*\phi = u^{-1}\phi u$ where $u = \mathrm{l.c.}(\phi_a)$.

Proof. We have

$$L\{\tau\}\phi_{IJ} = \sum_{i\in I, j\in J} L\{\tau\}\phi_i\phi_j = \sum_{j\in J} L\{\tau\}\phi_I\phi_j = \sum_{j\in J}(I*\phi)_j\phi_I = L\{\tau\}(I*\phi)_J\phi_I$$

and then $\phi_{IJ} = (I*\phi)_J\phi_I$. For any $b \in A$, we have

$$((IJ)*\phi)_b\phi_{IJ} = \phi_{IJ}\phi_b = (I*\phi)_J\phi_I\phi_b = (I*\phi)_J(I*\phi)_b\phi_I = (J*(I*\phi))_b(I*\phi)_J\phi_I = (J*(I*\phi))_b\phi_{IJ}$$

So $((IJ)*\phi)_b = (J*(I*\phi))_b$ for any $b \in A$ and hence $(IJ)*\phi = J*(I*\phi)$.

If $I = (a)$ for some $a \in A$, then $\phi_a = u\phi_I$. For any $b \in A$,

$$(I*\phi)_b u^{-1}\phi_a = (I*\phi)_b\phi_I = \phi_I\phi_b = u^{-1}\phi_a\phi_b = u^{-1}\phi_b\phi_a$$

and $I*\phi_b = u^{-1}\phi_b u$. Then u^{-1} defines an isomorphism $\phi \to I*\phi$. □

If $\mathrm{l.c.}(\phi_a)$ has an $q^{r\deg(a)}$-th root v in L, define the action of the fractional ideal (a^{-1}) on ϕ to be $(a^{-1})*\phi := v\phi v^{-1}$. Then $(a)*(a^{-1})*\phi = \phi$. For any nonzero ideal I of A, the action of the fractional idea $a^{-1}I$ on ϕ is given by $(a^{-1}I)*\phi := I*((a^{-1})*\phi)$.

Corollary 5.6. *Fix a perfect subfield L_0 of L. Let $\mathfrak{X}$ be the set of Drinfeld modules ϕ over L such that $\mathrm{l.c.}(\phi_a) \in L_0$ for each $a \in A$. The operation $*$ defines an action of the group $\mathcal{I}$ on $\mathfrak{X}$. It induces an action of $\mathrm{Pic}A$ on the set of isomorphic classes of Drinfeld modules in $\mathfrak{X}$.*

Proposition 5.7. *Let $\mathfrak{X}(\mathbf{C})$ be the set of isomorphic classes of Drinfeld modules over $\mathbf{C}$ of rank one. Then $\mathfrak{X}(\mathbf{C})$ is a principle homogeneous space under the action of $\mathrm{Pic}A$.*

Proof. Suppose ϕ is a Drinfeld module over $\mathbf{C}$ of rank one. Let Λ and $I * \Lambda$ be the corresponding lattices of ϕ and $I * \phi$, respectively. By Theorem 5.4, we have a commutative diagram

$$\begin{array}{ccc} \mathbf{C}/\Lambda & \longrightarrow & \mathbf{C}/(I * \Lambda) \\ \downarrow{\scriptstyle e_\Lambda} & & \downarrow{\scriptstyle e_{I*\Lambda}} \\ \phi(\mathbf{C}) & \xrightarrow{\phi_I} & (I * \phi)(\mathbf{C}) \end{array}$$

of A-modules whose vertical arrows are isomorpshims. Since $\ker(\phi_I)$ is the I-torsion submodule of $\phi(\mathbf{C})$, we have $I * \Lambda = I^{-1}\Lambda$ and our assertion holds. □

5.3 Sgn-normalized Drinfeld modules

Recall that $\mathbb{F}_\infty$ is the residue field of $\infty \in X$ and $d_\infty = \dim_{\mathbb{F}_q}(\mathbb{F}_\infty)$.

Definition 5.8. A sgn function on $K_\infty^\times$ is a homomorphism $\mathrm{sgn} : K^\times \to \mathbb{F}_\infty^\times$ such that $\mathrm{sgn}|_{\mathbb{F}_\infty^\times} = \mathrm{id}$.

There are exactly $q^{d_\infty} - 1$ sgn functions on $K_\infty^\times$. From now on, fix a sgn function $\mathrm{sgn} : K_\infty^\times \to \mathbb{F}_\infty^\times$ and a uniformizer $\pi \in K_\infty$ with $\mathrm{sgn}(\pi) = 1$.

Let $U_1 = \{x \in K_\infty | v_\infty(x-1) > 0\}$. Then $\mathrm{sgn}(U_1) = 1$ because U_1 is a pro-p-group. The uniformizer $\pi \in K_\infty$ defines an isomorphism $K_\infty \simeq \mathbb{F}_\infty((\pi))$. Any $a \in K_\infty^\times$ can be uniquely written as $a = \zeta\pi^n u$ for some $\zeta \in \mathbb{F}_\infty^\times$, $n \in \mathbb{Z}$ and $u \in U_1$, then $\mathrm{sgn}(a) = \zeta$.

Definition 5.9. A rank one Drinfeld module ϕ over L is called sgn-normalized if there exists an $\mathbb{F}_q$-algebra homomorphism $\eta : \mathbb{F}_\infty \to L$ such that $\mathrm{l.c.}(\phi_a) = \eta(\mathrm{sgn}(a))$ for any $0 \neq a \in A$.

Example 5.10. Suppose $A = \mathbb{F}_q[t]$ and $\mathrm{sgn}(t) = 1$. The sgn-normalized Drinfeld module over L is just the Carlitz module given by $C : A \to L\{\tau\},\ t \mapsto t + \tau$.

Theorem 5.11. *(1) Every rank one Drinfeld module ϕ over $\mathbf{C}$ is isomorphic to a sgn-normalized Drinfeld module.*

(2) The set of sgn-normalized Drinfeld modules over $\mathbf{C}$ isomorphic to ϕ is a principle homogeneous space under $\mathbb{F}_\infty^\times/\mathbb{F}_q^\times$.

Proof. (1) Extend $\phi : A \to \mathbf{C}\{\tau\}$ to a ring homomorphism from K to the ring $\mathbf{C}\{\{\tau^{-1}\}\}$ of twist Laurent series which is still denoted by ϕ. For any $a \in A$, we have $-\deg(\phi_a) = v_{\tau^{-1}}(\phi_a) = d_\infty v_\infty(a)$. So we can extend $\phi : K \to \mathbf{C}\{\{\tau^{-1}\}\}$ to a continuous homomorphism $K_\infty \to \mathbf{C}\{\{\tau^{-1}\}\}$ denoted by ϕ again. Choose $\alpha \in \mathbf{C}$ such that $\alpha^{1-q^{d_\infty}} = \mathrm{l.c.}(\phi_{\pi^{-1}})$. Replacing ϕ by $\alpha^{-1}\phi\alpha$, we may assume $\mathrm{l.c.}(\phi_{\pi^{-1}}) = 1$. Define $\eta : \mathbb{F}_\infty \to L$ by $\eta(c) = \mathrm{l.c.}(\phi_c)$ for any $c \in \mathbb{F}_\infty^\times$ and $\eta(0) = 0$. If we write any $0 \neq a \in A$ as $a = c\pi^n u$ for some $c \in \mathbb{F}_\infty^\times$, $n \in \mathbb{Z}$ and $u \in U_1$, then we have

$$\mathrm{l.c.}(\phi_a) = \mathrm{l.c.}(\phi_c \phi_\pi^n \phi_u) = \mathrm{l.c.}(\phi_c) = \eta(c) = \eta(\mathrm{sgn}(a)).$$

So ϕ is sgn-normalized.

(2) We may assume that ϕ is sgn-normalized. Let $\alpha \in \mathbf{C}^\times$. Then $\alpha^{-1}\phi\alpha$ is sgn-normalized if and only if $1 = \mathrm{l.c.}(\alpha^{-1}\phi_{\pi^{-1}}\alpha) = \alpha^{q^{\deg(\mathbb{F}_\infty)}-1}$ if and only if $\alpha \in \mathbb{F}_\infty^\times$. By Proposition 5.20, $\mathrm{Aut}(\phi) = A^\times = \mathbb{F}_q^\times$ and then $\alpha^{-1}\phi\alpha = \phi$ implies $\alpha \in \mathbb{F}_q^\times$. This proves (2). □

Definition 5.12. Let $\mathfrak{X}^+(L)$ be the set of sgn-normalized Drinfeld modules over L. Let $\mathcal{P}^+$ be the subgroup of $\mathcal{I}$ generated by (c) for those $c \in K^\times$ such that $\mathrm{sgn}(c) = 1$ and let $\mathrm{Pic}^+ A = \mathcal{I}/\mathcal{P}^+$.

Proposition 5.13. *The set $\mathfrak{X}^+(L)$ is stable under $\mathcal{I}$. For any $\phi \in \mathfrak{X}^+(L)$, $\mathrm{Stab}_{\mathcal{I}}(\phi) = \mathcal{P}^+$.*

Proof. By definition, there exists $\eta : \mathbb{F}_\infty \to L$ such that $\mathrm{l.c.}(\phi_a) = \eta(\mathrm{sgn}(a))$ for any $a \in A$. For any nonzero ideal I of A, $(I*\phi)_a\phi_I = \phi_I\phi_a$ implies $\mathrm{l.c.}((I*\phi)_a) = \mathrm{l.c.}(\phi_a)^{q^{\deg(\phi_I)}} = \mathrm{l.c.}(\phi_a)^{q^{\deg(I)}} = \eta(\mathrm{sgn}(a))^{q^{\deg(I)}}$. This shows $I*\phi \in \mathfrak{X}^+(L)$. By Corollary 5.6, $\mathfrak{X}^+(L)$ is stable under $\mathcal{I}$.

Now let $I \in \mathcal{I}$ such that $I*\phi = \phi$. Then $I = b^{-1}J$ for some $b \in A$ and some ideal J of A. Hence $\phi = I*\phi = (b^{-1})*(J*\phi)$ and $(b)*\phi = J*\phi$. The composition $\phi \xrightarrow{\phi_J} J*\phi = (b)*\phi \xrightarrow{\mathrm{l.c.}(\phi_b)} \phi$ is an endomorphism of ϕ. By Proposition 5.20, $\mathrm{End}(\phi) = A$ and hence $\mathrm{l.c.}(\phi_b)\phi_J = \phi_c$ for some $c \in A$. Set $J' = J + (c)$. Then $\phi_{J'} = \phi_J = \mathrm{l.c.}(\phi_c)^{-1}\phi_c$ and by Lemma 5.3, we have $\deg J = \deg J' = \deg c$ and hence $J = (c)$. By $\mathrm{l.c.}(\phi_b)\phi_J = \phi_c$, we have $\eta(\mathrm{sgn}(b)) = \mathrm{l.c.}(\phi_c) = \mathrm{l.c.}(\phi_b) = \eta(\mathrm{sgn}(b))$ and hence $\mathrm{sgn}(b^{-1}c) = 1$. So $I = (b^{-1}c) \in \mathcal{P}^+$. □

Theorem 5.14. *The action of $\mathcal{I}$ on Drinfeld modules makes $\mathfrak{X}^+(\mathbf{C})$ a principle homogeneous space under $\mathrm{Pic}^+ A$.*

Proof. By Proposition 5.13, $\mathfrak{X}^+(\mathbf{C})$ is a disjoint union of principle homogeneous spaces under $\mathrm{Pic}^+ A$. So we need only to check that $\#\mathfrak{X}^+(\mathbf{C}) = \#\mathrm{Pic}A$. By Proposition 5.1 and Theorem 5.11, we have $\#\mathfrak{X}^+(\mathbf{C}) = \#\mathrm{Pic}A \cdot \#\mathbb{F}_\infty^\times/\mathbb{F}_q^\times$. On the other hand, the short exact sequence

$$1 \to \mathcal{P}/\mathcal{P}^+ \to \mathcal{I}/\mathcal{P}^+ = \mathrm{Pic}^+ A \to \mathcal{I}/\mathcal{P} = \mathrm{Pic}A \to 1$$

and the isomorphism $\mathcal{P}/\mathcal{P}^+ \simeq \mathbb{F}_\infty^\times/\mathbb{F}_q^\times$ induced by sgn show that $\#\mathrm{Pic}^+ A = \#\mathrm{Pic}A \cdot \#\mathbb{F}_\infty^\times/\mathbb{F}_q^\times$. □

5.4 The narrow Hilbert class field

Fix $\phi \in \mathfrak{X}^+(\mathbf{C})$. Define

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

Then ϕ is a Drinfeld module over H^+, so is $I * \phi$ for any $I \in \mathcal{I}$. By Theorem 5.14, these are objects in $\mathfrak{X}^+(\mathbf{C})$. So H^+ is independent of the choice of ϕ, which is called the narrow Hilbert class field of (A, sgn).

Theorem 5.15. *(1) The field H^+ is a finite abelian extension of K.*

(2) The extension H^+/K is unramified outside $\infty \in X$.

(3) We have $\mathrm{Gal}(H^+/K) \simeq \mathrm{Pic}^+ A$.

Proof. (1) The group $\mathrm{Aut}(\mathbf{C}/K)$ of automorphisms of $\mathbf{C}$ fixing K acts on $\mathfrak{X}^+(\mathbf{C})$, 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 Proposition 5.2, ϕ is isomorphic to Drinfeld module ψ over K_∞. Extend $\psi : A \to K_\infty\{\{\tau^{-1}\}\}$ to $\psi : K_\infty \to K_\infty\{\{\tau^{-1}\}\}$ as in the proof of Theorem 5.11 and let $c \in \mathbf{C}$ such that $c^{1-q^{d_\infty}} = \mathrm{l.c.}(\psi_{\pi^{-1}}) \in K_\infty$. Then $c^{-1}\psi c$ is a sgn-normalized Drinfeld module over a finite separable extension $K_\infty(c)$ of K_∞ isomorphic to ϕ. The completion K_∞ of a global field K is a separable extension of K, hence H^+ is separable over K. The automorphism group of $\mathfrak{X}^+(\mathbf{C})$ as a principal homogeneous space under $\mathrm{Pic}^+ A$ is equal to $\mathrm{Pic}^+ A$, so we have a monomorphism $\chi : \mathrm{Gal}(H^+/K) \to \mathrm{Aut}\mathfrak{X}^+(\mathbf{C}) \simeq \mathrm{Pic}^+ A$. So $\mathrm{Gal}(H^+/K)$ is a finite abelian group.

(2) Let B^+ be the integral closure of A in H^+. Let $\mathfrak{P}$ be a nonzero prime ideal of B^+ lying above $\mathfrak{p}$ of A. Let $\mathbb{F}_\mathfrak{P} = B^+/\mathfrak{P}$. By Corollary 4.5, each $\phi \in \mathfrak{X}^+(H^+) = \mathfrak{X}^+(\mathbf{C})$ is a Drinfeld module over the localization $B^+_\mathfrak{P}$, so there is a reduction map $\rho : \mathfrak{X}^+(H^+) \to \mathfrak{X}^+(\mathbb{F}_\mathfrak{P})$. By Proposition 5.13, $\mathrm{Pic}^+ A$ acts faithfully on the source and target. Moreover, the map ρ is $\mathrm{Pic}^+ A$-equivariant, and by Theorem 5.14 $\mathfrak{X}^+(H^+)$ is a principal homogeneous space under $\mathrm{Pic}^+ A$, so ρ is injective. If some $\sigma \in \mathrm{Gal}(H^+/K)$ belongs to the inertia group at $\mathfrak{P}$, then σ acts trivially on $\mathfrak{X}^+(\mathbb{F}_\mathfrak{P})$, so σ acts trivially on $\mathfrak{X}^+(H^+)$ and $\sigma = 1$. Thus H^+/K is unramified at $\mathfrak{P}$.

(3) Let $D_\mathfrak{P} = \{\sigma \in \mathrm{Gal}(H^+/K) | \sigma(\mathfrak{P}) = \mathfrak{P}\}$. By (2), $D_\mathfrak{P} \simeq \mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$. The Frobenius element in $\mathrm{Gal}(\mathbb{F}_\mathfrak{P}/\mathbb{F}_\mathfrak{p})$ defines an elment $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(H^+/K)$. For any $\bar{\phi} \in \mathfrak{X}^+(\mathbb{F}_\mathfrak{P})$, we have $\bar{\phi}_\mathfrak{p} = \tau^{\deg \mathfrak{p}}$ by Lemma 5.3. For any $a \in A$, the equality $(\mathfrak{p} * \bar{\phi})_a \bar{\phi}_\mathfrak{p} = \bar{\phi}_\mathfrak{p} \bar{\phi}_a$ implies that $(\mathfrak{p} * \bar{\phi})_a = \mathrm{Frob}_\mathfrak{p} \bar{\phi}_a$ and hence $\mathfrak{p} * \bar{\phi} = \mathrm{Frob}_\mathfrak{p} \bar{\phi}$.

Since $\rho : \mathfrak{X}^+(H^+) \to \mathfrak{X}^+(\mathbb{F}_{\mathfrak{P}})$ is injective and $\mathrm{Pic}^+ A$-equivariant, then the action of $\mathrm{Frob}_{\mathfrak{p}}$ and $\mathfrak{p}$ on $\mathfrak{X}^+(H^+)$ coincide. Thus $\chi : \mathrm{Gal}(H^+/K) \to \mathrm{Pic}^+ A$ maps $\mathrm{Frob}_{\mathfrak{p}}$ to the class of $\mathfrak{p}$ in $\mathrm{Pic}^+ A$. Such class generates $\mathrm{Pic}^+ A$, so χ is surjective. □

5.5 Hilbert class field

By the short exact sequence

$$1 \to \mathcal{P}/\mathcal{P}^+ \to \mathrm{Pic}^+ A \to \mathrm{Pic} A \to 1,$$

the extension $K \subset H^+$ decomposes into two abelian extensions $K \xrightarrow{\mathrm{Pic} A} H \xrightarrow{\mathcal{P}/\mathcal{P}^+} H^+$ with Galois group as shown. The surjective map $\mathfrak{X}^+(\mathbf{C}) \to \mathfrak{X}(\mathbf{C})$ is compatible with the epimorphism of groups $\mathrm{Pic}^+ A \to \mathrm{Pic} A$. By Proposition 5.2, each element of $\mathfrak{X}(\mathbf{C})$ is represented by a Drinfeld module over K_∞, so the decomposition group D_∞ of H^+/K at $\infty \in X$ acts trivially on $\mathfrak{X}(\mathbf{C})$. So $D_\infty \subset \mathcal{P}/\mathcal{P}^+$. In other words, ∞ splits completely in H/K. The Hilbert class field H_A of A is defined as the maximal unramified extension of K in which ∞ splits completely. Thus $H \subset H_A$. Class field theory shows that $\mathrm{Pic} A \simeq \mathrm{Gal}(H_A/K)$. So $H_A = H$.

5.6 Ray class fields

In this section, we generalize the construction to obtain all the abelian extensions of K, even the ramified ones. Fix notations as follows.

$\mathfrak{m}$: a nonzero ideal of A.

$\mathcal{I}_{\mathfrak{m}}$: the subgroup of $\mathcal{I}$ generated by maximal ideals of A not dividing $\mathfrak{m}$.

$\mathcal{P}_{\mathfrak{m}}$: the subgroup of $\mathcal{I}$ generated by (c) for those $c \in K^\times$ with $c \equiv 1 \pmod{\mathfrak{m}}$.

$\mathcal{P}^+_{\mathfrak{m}}$: the subgroup of $\mathcal{I}$ generated by (c) for those $c \in K^\times$ with $c \equiv 1 \pmod{\mathfrak{m}}$ and $\mathrm{sgn}(c) = 1$.

$\mathrm{Pic}_{\mathfrak{m}} A := \mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}$, the ray class group modulo $\mathfrak{m}$ of A.

$\mathrm{Pic}^+_{\mathfrak{m}} A := \mathcal{I}_{\mathfrak{m}}/\mathcal{P}^+_{\mathfrak{m}}$, the narrow ray class group modulo $\mathfrak{m}$ of A.

$\mathfrak{X}^+_{\mathfrak{m}}(\mathbf{C}) := \{(\phi, \lambda) | \phi \in \mathfrak{X}^+(\mathbf{C})$ and λ generates the $A/\mathfrak{m}$-module $\phi[\mathfrak{m}](\mathbf{C})\}$.

Here $c \equiv 1 \pmod{\mathfrak{m}}$ means that c is quotient b/c of two elements of A relative prime to $\mathfrak{m}$ such that $a \equiv b \pmod{\mathfrak{m}}$.

Lemma 5.16. *We have the following commutative diagram*

$$
\begin{array}{ccccccccc}
 & & & & 0 & & 0 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & 0 & \longrightarrow & (\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}^+)/\mathcal{P}_{\mathfrak{m}}^+ & \longrightarrow & (\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P})/\mathcal{P}_{\mathfrak{m}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{P}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}^+ & \longrightarrow & \mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}^+ & \longrightarrow & \mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{P}/\mathcal{P}^+ & \longrightarrow & \mathcal{I}/\mathcal{P}^+ & \longrightarrow & \mathcal{I}/\mathcal{P} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

with exact rows and lines. Moreover, we have canonical isomorphisms $\mathcal{P}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}^+ \simeq \mathcal{P}/\mathcal{P}^+ \simeq \mathbb{F}_\infty^\times/\mathbb{F}_q^\times$ *and* $(\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}^+)/\mathcal{P}_{\mathfrak{m}}^+ \simeq (\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P})/\mathcal{P}_{\mathfrak{m}} \simeq (A/\mathfrak{m})^\times$.

Proof. The second and third lines are obviously exact. By the snake lemma, to prove exactness of lines and rows in the above diagram, we need only to show that $\mathcal{P}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}^+ \to \mathcal{P}/\mathcal{P}^+$ is an isomorphism and $\mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}} \to \mathcal{I}/\mathcal{P}$ is surjective.

(1) Recall in Theorem 5.14 that the sgn function induces an isomorphism $\mathcal{P}/\mathcal{P}^+ \simeq \mathbb{F}_\infty^\times/\mathbb{F}_q^\times$. Obviously, the sgn function induces a monomorphism $\mathcal{P}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}^+ \to \mathbb{F}_\infty^\times/\mathbb{F}_q^\times$. To show it is surjective, we need find $c \in 1 + \mathfrak{m}$ such that $\mathrm{sgn}(c) = \alpha$ for any $\alpha \in \mathbb{F}_\infty^\times$. Choose $x \in K_\infty^\times$ with $\mathrm{sgn}(x) = \alpha$. Then $v_\infty(x - a/b) > v_\infty(x)$ for some $a, b \in A$. We have $a/bx \in U_1$ and hence

$$\mathrm{sgn}(ab^{q^{d_\infty}-2}) = \mathrm{sgn}(a/b)\mathrm{sgn}(b)^{q^{d_\infty}-1} = \mathrm{sgn}(a/b) = \mathrm{sgn}(x)\mathrm{sgn}(a/bx) = \mathrm{sgn}(x) = \alpha.$$

Take $0 \neq y \in \mathfrak{m}$ and set $c = 1 + ab^{q^{d_\infty}-2}y^{q^{d_\infty}-1}$. Then $c \equiv 1 \pmod{\mathfrak{m}}$ and $\mathrm{sgn}(c) = \alpha$.

(2) The surjectivity of $\mathcal{I}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}} \to \mathcal{I}/\mathcal{P}$ is equivalent to $\mathcal{I} = \mathcal{I}_{\mathfrak{m}}\mathcal{P}$. Let I be a nonzero ideal of A. For each maximal ideal $\mathfrak{p}$ of A dividing $I\mathfrak{m}$, choose $a_{\mathfrak{p}} \in \mathfrak{p}^{v_{\mathfrak{p}}(I)} \backslash \mathfrak{p}^{v_{\mathfrak{p}}(I)+1}$. By strong approximation theorem, there exists $a \in K^\times$ such that $v_{\mathfrak{p}}(a - a_{\mathfrak{p}}) > v_{\mathfrak{p}}(I)$ for any maximal ideal $\mathfrak{p}$ dividing $I\mathfrak{m}$ and $v_{\mathfrak{p}}(a) \geq 0$ for any $\mathfrak{p} \nmid I\mathfrak{m}$. Take $J = aI^{-1}$. Then J is an ideal of A prime to $\mathfrak{m}$ and $I = aJ^{-1} \in \mathcal{I}_{\mathfrak{m}}\mathcal{P}$.

(3) It remains to show $(A/\mathfrak{m})^\times \simeq (\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P})/\mathcal{P}_{\mathfrak{m}}$. Define a map $\mu : \mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}^+ \to (A/\mathfrak{m})^\times$ as follows. Any element of $\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}^+$ is of the form (c) for some $c \in K^\times$ with $\mathrm{sgn}(c) = 1$ and $(c) \in \mathcal{I}_{\mathfrak{m}}$. So there exist ideals I and J of A prime to $\mathfrak{m}$ such that $(c) = IJ^{-1}$. Then $I^n = (a)$ for some positive integer n and some $a \in A$ prime to $\mathfrak{m}$. As $(c) = I^n(I^{n-1}J)^{-1} = (a)(I^{n-1}J)^{-1}$,

we have $(ac^{-1}) = I^{n-1}J$ and then $ac^{-1} \in A$ prime to $\mathfrak{m}$. Define $\mu((c)) = (a \mod \mathfrak{m}) \cdot (ac^{-1} \mod \mathfrak{m})^{-1} \in (A/\mathfrak{m})^{\times}$. Obviously, μ is a well defined homomorphism of groups. If $\mu((c)) = 1$, then $a \equiv ac^{-1} \pmod{\mathfrak{m}}$ and hence $(c) = \mathcal{P}_{\mathfrak{m}}^{+}$. It follows that $\ker(\mu) = \mathcal{P}_{\mathfrak{m}}^{+}$. Given $x \in A$ prime to $\mathfrak{m}$, we can find $y \in \mathfrak{m}$ such that $\deg(y) > \deg(x)$ and $\mathrm{sgn}(y) = 1$. Then $\mathrm{sgn}(x+y) = \mathrm{sgn}(y) = 1$, $(x+y) \in \mathcal{P}_{\mathfrak{m}}^{+}$ and $\mu((x+y)) = x \mod \mathfrak{m} \in (A/\mathfrak{m})^{\times}$. This shows that μ is surjective and hence it induces an isomorphism $(\mathcal{I}_{\mathfrak{m}} \cap \mathcal{P}^{+})/\mathcal{P}_{\mathfrak{m}}^{+} \simeq (A/\mathfrak{m})^{\times}$. □

Lemma 5.17. *If* $\mathfrak{m}$ *is prime to* $\mathrm{char}_A(L)$*, let*

$$\mathfrak{X}_{\mathfrak{m}}^{+}(L) = \{(\phi, \lambda) | \phi \in \mathfrak{X}^{+}(L) \text{ and } \lambda \text{ generates the } A/\mathfrak{m}\text{-module } \phi[\mathfrak{m}](\overline{L})\}.$$

Then we have an action of $\mathcal{I}_{\mathfrak{m}}$ *on* $\mathfrak{X}_{\mathfrak{m}}^{+}(L)$ *such that the stabilizer of each* (ϕ, λ) *is* $\mathcal{P}_{\mathfrak{m}}^{+}$*.*

Proof. Let $(\phi, \lambda) \in \mathfrak{X}_{\mathfrak{m}}^{+}(L)$ and let I be an ideal of A prime to $\mathfrak{m}$. The isogeny $\phi_I : \phi \to I * \phi$ induces an A-linear map $\phi_I^* : \phi[\mathfrak{m}](L) \to (I*\phi)[\mathfrak{m}](L)$ with source and target are free $A/\mathfrak{m}$-modules of rank one. As I is prime to $\mathfrak{m}$, ϕ_I^* is injective and hence bijective. So $\phi_I^*(\lambda)$ is a generator of $(I*\phi)[\mathfrak{m}](L)$. Define $I*(\phi, \lambda) = (I*\phi, \phi_I^*(\lambda))$, which can be extended to an action of $\mathcal{I}_{\mathfrak{m}}$ on $\mathfrak{X}_{\mathfrak{m}}^{+}(L)$.

Suppose $I * (\phi, \lambda) = (\phi, \lambda)$ for some $I \in \mathcal{I}_{\mathfrak{m}}$. By Theorem 5.14, $I = (c)$ for some $c \in K^{\times}$ with $\mathrm{sgn}(c) = 1$. As $(c) \in \mathcal{I}_{\mathfrak{m}}$, then $(c) \cap A$ is an ideal of A prime to $\mathfrak{m}$. Choose $x \in (1+\mathfrak{m}) \cap (c) \cap A$ and take $a = x^{q^{d_\infty}-1}$. Then $a \in A$ and $\mathrm{sgn}(a) = 1$ and $a = cb$ for some $b \in A$. Hence $a \in 1+\mathfrak{m}$ and $\mathrm{sgn}(b) = 1$. The equality $\phi_{(c)}^*(\lambda) = \lambda$ means that $\phi_a(\lambda) = \phi_b(\lambda)$, and hence $a - b \in \mathfrak{m}$. This shows that $I = (c) \in \mathcal{P}_{\mathfrak{m}}^{+}$ and $\mathrm{Stab}_{\mathcal{I}_{\mathfrak{m}}}(\phi, \lambda) = \mathcal{P}_{\mathfrak{m}}^{+}$. □

Theorem 5.18. *Fix* $(\phi, \lambda) \in \mathfrak{X}^{+}(\mathbf{C})$*. Define the narrow ray class field* $H_{\mathfrak{m}}^{+}$ *modulo* $\mathfrak{m}$ *of* (A, sgn) *to be* $H^{+}(\lambda)$*.*

(1) The action of $\mathcal{I}_{\mathfrak{m}}$ *on* $\mathfrak{X}_{\mathfrak{m}}^{+}(\mathbf{C})$ *makes it to be a principle homogeneous space under* $\mathrm{Pic}_{\mathfrak{m}}^{+}A$*.*

(2) The field $H_{\mathfrak{m}}^{+}$ *is independent of the choice of* (ϕ, λ)*, and the extension* $H_{\mathfrak{m}}^{+}/K$ *is finite abelian, unramified at each prime of* A *not dividing* $\mathfrak{m}$*.*

(3) We have $\mathrm{Gal}(H_{\mathfrak{m}}^{+}/K) \simeq \mathrm{Pic}_{\mathfrak{m}}^{+}A$*.*

(4) Let $H_{\mathfrak{m}}$ *be the subfield of* $H_{\mathfrak{m}}^{+}$ *fixed by* $\mathcal{P}_{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}^{+}$*. Then* $H_{\mathfrak{m}}/K$ *splits at* ∞ *and* $\mathrm{Gal}(H_{\mathfrak{m}}/K) = \mathrm{Pic}_{\mathfrak{m}}A$*.*

Proof. By Lemma 5.17, $\mathfrak{X}_{\mathfrak{m}}^{+}(\mathbf{C})$ is a disjoint of principle homogeneous spaces under $\mathrm{Pic}_{\mathfrak{m}}^{+}A$. To prove (1), we need only to show that $\#\mathrm{Pic}_{\mathfrak{m}}^{+}A = \#\mathfrak{X}_{\mathfrak{m}}^{+}(\mathbf{C})$. By Theorem 5.14, $\#\mathfrak{X}_{\mathfrak{m}}^{+}(\mathbf{C}) = \#\mathfrak{X}^{+}(\mathbf{C}) \cdot$

$\#(A/\mathfrak{m})^\times = \#\mathrm{Pic}^+ A \cdot \#(A/\mathfrak{m})^\times$. By Lemma 5.16, $\#\mathrm{Pic}^+_{\mathfrak{m}} A = \#\mathrm{Pic}^+ A \cdot \#(A/\mathfrak{m})^\times$. So (1) holds.

(2) For any $I \in \mathcal{I}_{\mathfrak{m}}$, $I * (\phi, \lambda) = (I * \phi, \phi_I^*(\lambda))$. So $H^+_{\mathfrak{m}}$ is independent of the choice of (ϕ, λ). The group $\mathrm{Aut}(\mathbf{C}/K)$ also acts on $\mathfrak{X}^+_{\mathfrak{m}}(\mathbf{C})$, so $H^+_{\mathfrak{m}}$ is stable under $\mathrm{Aut}(\mathbf{C}/K)$. This shows that $H^+_{\mathfrak{m}}/K$ is a finite Galois extension. The automorphism group of $\mathfrak{X}^+_{\mathfrak{m}}(\mathbf{C})$ as a principle homogeneous space under $\mathrm{Pic}^+_{\mathfrak{m}} A$ is equal to $\mathrm{Pic}^+_{\mathfrak{m}} A$. So we have a monomorphism

$$\chi : \mathrm{Gal}(H^+_{\mathfrak{m}}/K) \to \mathrm{Aut}\mathfrak{X}^+_{\mathfrak{m}}(\mathbf{C}) \simeq \mathrm{Pic}^+_{\mathfrak{m}} A.$$

Thus $H^+_{\mathfrak{m}}/K$ is a finite abelian extension.

Let B be the integral closure of A in $H^+_{\mathfrak{m}}$, and let $\mathfrak{P}$ be a maximal ideal of B lying above a maximal ideal $\mathfrak{p}$ of A not dividing $\mathfrak{m}$. By Corollary 4.5, for each $(\phi, \lambda) \in \mathfrak{X}^+_{\mathfrak{m}}(H^+_{\mathfrak{m}}) = \mathfrak{X}^+_{\mathfrak{m}}(\mathbf{C})$, ϕ is a Drinfeld module over the localization $B_{\mathfrak{P}}$. So there is a reduction map $\rho : \mathfrak{X}^+_{\mathfrak{m}}(H^+_{\mathfrak{m}}) \to \mathfrak{X}^+_{\mathfrak{m}}(\mathbb{F}_{\mathfrak{P}})$ of principle homogeneous spaces under $\mathrm{Pic}^+_{\mathfrak{m}} A$. By (1), ρ is injective. If some $\sigma \in \mathrm{Gal}(H^+_{\mathfrak{m}}/K)$ belongs to the inertia group at $\mathfrak{P}$, then σ acts trivially on $\mathfrak{X}^+_{\mathfrak{m}}(\mathbb{F}_{\mathfrak{P}})$. Hence σ acts trivially on $\mathfrak{X}^+_{\mathfrak{m}}(H^+_{\mathfrak{m}})$ and $\sigma = 1$. Thus $H^+_{\mathfrak{m}}/K$ is unramified at $\mathfrak{P}$.

(3) The Frobenius element in $\mathrm{Gal}(\mathbb{F}_{\mathfrak{P}}/\mathbb{F}_{\mathfrak{p}})$ defines an elment $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(H^+_{\mathfrak{m}}/K)$. For any $\bar{\phi} \in \mathfrak{X}^+_{\mathfrak{m}}(\mathbb{F}_{\mathfrak{P}})$, we have $\bar{\phi}_{\mathfrak{p}} = \tau^{\deg \mathfrak{p}}$ by Lemma 5.3. For any $a \in A$, the equality $(\mathfrak{p} * \bar{\phi})_a \bar{\phi}_{\mathfrak{p}} = \bar{\phi}_{\mathfrak{p}} \bar{\phi}_a$ implies that $(\mathfrak{p} * \bar{\phi})_a = \mathrm{Frob}_{\mathfrak{p}} \bar{\phi}_a$ and hence $\mathfrak{p} * \bar{\phi} = \mathrm{Frob}_{\mathfrak{p}} \bar{\phi}$.

Since $\rho : \mathfrak{X}^+_{\mathfrak{m}}(H^+) \to \mathfrak{X}^+_{\mathfrak{m}}(\mathbb{F}_{\mathfrak{P}})$ is injective and $\mathrm{Pic}^+ A$-equivariant, it follows that the actions of $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(H^+_{\mathfrak{m}})$ and $\mathfrak{p} \in \mathcal{I}_{\mathfrak{m}}$ on $\mathfrak{X}^+_{\mathfrak{m}}(H^+_{\mathfrak{m}})$ coincide. Thus $\chi : \mathrm{Gal}(H^+_{\mathfrak{m}}/K) \to \mathrm{Pic}^+_{\mathfrak{m}} A$ sends $\mathrm{Frob}_{\mathfrak{p}}$ to the class of $\mathfrak{p}$ in $\mathrm{Pic}^+_{\mathfrak{m}} A$. Such class generates $\mathrm{Pic}^+_{\mathfrak{m}} A$, so χ is surjective.

(4) Let $\mathfrak{X}_{\mathfrak{m}}(\mathbf{C})$ be the set of isomorphic classes in $\mathfrak{X}^+_{\mathfrak{m}}(\mathbf{C})$. Then $\mathfrak{X}_{\mathfrak{m}}(\mathbf{C})$ is a principle homogeneous space under $\mathrm{Pic}_{\mathfrak{m}} A$. The surjective map $\mathfrak{X}^+_{\mathfrak{m}}(\mathbf{C}) \to \mathfrak{X}_{\mathfrak{m}}(\mathbf{C})$ is compatible with the epimorphism of groups $\mathrm{Pic}^+_{\mathfrak{m}} A \to \mathrm{Pic}_{\mathfrak{m}} A$. By Proposition 5.2, each element of $\mathfrak{X}(\mathbf{C})$ is represented by a Drinfeld module over K_∞, so the decomposition group D_∞ of $H^+_{\mathfrak{m}}/K$ at ∞ acts trivially on $\mathfrak{X}_{\mathfrak{m}}(\mathbf{C})$. So $D_\infty \subset \mathcal{P}_{\mathfrak{m}}/\mathcal{P}^+_{\mathfrak{m}}$. In other words, ∞ splits completely in $H_{\mathfrak{m}}/K$. The equality $\mathrm{Gal}(H_{\mathfrak{m}}/K) = \mathrm{Pic}_{\mathfrak{m}} A$ holds by Lemma 5.16. □

5.7 The maximal abelian extension of K

In this subsection, we construct the maximal abelian extension K^{ab} of K.

Theorem 5.19. *Let $K^{\mathrm{ab},\infty}=\bigcup_{\mathfrak{m}} H_{\mathfrak{m}}$ when $\mathfrak{m}$ runs over all nonzero ideals of $A=\Gamma(X-\{\infty\},\mathcal{O}_X)$ and let $K_{\mathrm{c}}:=\bigcup_{n\geq 1}\mathbb{F}_{q^n}K$ be the constant extension of K.*

(1) Then $K^{\mathrm{ab},\infty}$ is the maximal abelian extension of K in which ∞ splits completely.

(2) Choose another closed point ∞' of X. Then K^{ab} is the compositum K_{c}, $K^{\mathrm{ab},\infty}$ and $K^{\mathrm{ab},\infty'}$.

Before proving the theorem, first recall the class field theory for function fields.

For any closed point $\mathfrak{p}$ of X, denote by $K_{\mathfrak{p}}$ the completion of K at $\mathfrak{p}$, $\mathcal{O}_{\mathfrak{p}}$ the discrete valuation ring of $K_{\mathfrak{p}}$ and $v_{\mathfrak{p}}$ the discrete valuation. Define the idèle group of K to be

$$\mathbb{A}_K^\times=\{(a_{\mathfrak{p}})\in\prod_{\mathfrak{p}\in|X|}K_{\mathfrak{p}}^\times \mid a_{\mathfrak{p}}\in\mathcal{O}_{\mathfrak{p}}^\times \text{ for almost all } \mathfrak{p}\}.$$

For any effective divisor $D=\sum_{\mathfrak{p}\in|X|}n_{\mathfrak{p}}\mathfrak{p}$ of X, let $U_D=\prod_{\mathfrak{p}\in|X|}U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}$, where $U_{\mathfrak{p}}^{(0)}=\mathcal{O}_{\mathfrak{p}}^\times$ and $U_{\mathfrak{p}}^{(n_{\mathfrak{p}})}=\{a\in K_{\mathfrak{p}}|v_{\mathfrak{p}}(a-1)\geq n_{\mathfrak{p}}\}$ if $n_{\mathfrak{p}}>0$. Equip the idèle group a canonical topology by taking a basic system of neighborhoods of $1\in\mathbb{A}_K^\times$ to be the sets U_D where D runs over all the effective divisors of X. Therefore $\mathbb{A}_K^\times$ is a locally compact group. The inclusion $K\subset K_{\mathfrak{p}}$ defines the diagonal embedding $K^\times\to\mathbb{A}_K^\times$ which makes $K^\times$ to be a discrete subgroup of $\mathbb{A}_K^\times$. We call the quotient group $C_K=\mathbb{A}_K^\times/K^\times$ the idèle class group of K. For any finite field extension L/K, we have the norm map

$$N_{L/K}:\mathbb{A}_L^\times\to\mathbb{A}_K^\times,\ \ N_{L/K}((a_{\mathfrak{P}}))_{\mathfrak{p}}=\prod_{\mathfrak{P}|\mathfrak{p}}N_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}(a_{\mathfrak{P}}).$$

The thrust of class field theory is that there exists a continuous homomorphism

$$(\bullet,K^{\mathrm{ab}}/K):\mathbb{A}_K^\times\to\mathrm{Gal}(K^{\mathrm{ab}}/K),$$

which satisfies the following properties:

(i) $(\bullet,K^{\mathrm{ab}}/K)$ has dense image and its kenel is $K^\times$.

(ii) For each $\mathfrak{p}\in|X|$, $(\bullet,K^{\mathrm{ab}}/K)$ is compatible with the local reciprocity map for $K_{\mathfrak{p}}$. In particular, if $\pi_{\mathfrak{p}}\in K_{\mathfrak{p}}$ is a uniformizer, then $(\pi_{\mathfrak{p}},K^{\mathrm{ab}}/K)$ is a Frobenius element for $\mathfrak{p}$.

(iii) For any finite abelian extension L/K, $(\bullet,K^{\mathrm{ab}}/K)$ induces an isomorphism

$$\mathbb{A}_K^\times/K^\times N_{L/K}(\mathbb{A}_L^\times)\simeq\mathrm{Gal}(L/K).$$

(iv) The map $L \mapsto \mathcal{N}_L := K^\times N_{L/K}(\mathbb{A}_L^\times)$ is a one-to-one correspondence between finite abelian extensions of K and open subgroups of $\mathbb{A}_K^\times$ of finite index containing $K^\times$. Moreover, $\mathcal{N}_{LL'} = \mathcal{N}_L \cap \mathcal{N}_{L'}$ and $\mathcal{N}_{L\cap L'} = \mathcal{N}_L \mathcal{N}_{L'}$ for any two finite abelian extensions L, L' of K.

Observe that any open subgroup of $\mathbb{A}_K^\times$ contains U_D for some effective divisor D of X. To specify an open subgroup of finite index in C_K, it suffices to give an effective divisor D of X and an open subgroup N of $\mathbb{A}_K^\times$ of finite index containing $K^\times U_D$. The corresponding abelian extension K_N/K should have these properties:

(a) K_N/K is unramified outside $\mathrm{Supp}(D)$.

(b) There is an isomorphism $\mathbb{A}_K^\times/N \simeq \mathrm{Gal}(K_N/K)$, which carries a uniformizer at $\mathfrak{p} \notin \mathrm{Supp}(D)$ to the Frobenius element $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(K_N/K)$.

The ray class field K_D is the compositum of all finite extensions obtained this way. Then $\mathrm{Gal}(K_D/K)$ is isomorphic to the profinite completion of the ray class group $C_D := \mathbb{A}_K^\times/K^\times U_D$.

Suppose $\infty \notin \mathrm{Supp}(D)$. The divisor $D = \sum_\mathfrak{p} n_\mathfrak{p}\mathfrak{p}$ gives an ideal $\mathfrak{m}$ of A such that $v_\mathfrak{p}(\mathfrak{m}) = n_\mathfrak{p}$ for any $\mathfrak{p} \neq \infty$. Let $\pi_\infty \in K_\infty$ be a uniformizer.

Lemma 5.20. *Suppose $\infty \notin \mathrm{Supp}(D)$. We have $\mathbb{A}_K^\times/K^\times U_D \pi_\infty^\mathbb{Z} \simeq \mathrm{Pic}_\mathfrak{m} A$. In particular, $K^\times U_D \pi_\infty^\mathbb{Z}$ is a subgroup of $\mathbb{A}_K^\times$ of finite index. Any open subgroup of $\mathbb{A}_K^\times$ of finite index containing $K^\times U_D$ must contains $K^\times U_D \pi_\infty^{n\mathbb{Z}}$ for some positive integer n.*

Proof. Let

$$U'_D = \{(a_\mathfrak{p}) \in \mathbb{A}_K^\times | v_\mathfrak{p}(a_\mathfrak{p} - 1) \geq n_\mathfrak{p} \text{ for any } \mathfrak{p} \in \mathrm{Supp}(D)\}.$$

By the weak approximation theorem, we have $\mathbb{A}_K^\times = K^\times U'_D$ and hence

$$\mathbb{A}_K^\times/K^\times U_D\pi_\infty^\mathbb{Z} = K^\times U'_D/K^\times U_D\pi_\infty^\mathbb{Z} \simeq U'_D/(U'_D \cap K^\times U_D\pi_\infty^\mathbb{Z}) \simeq U'_D/((K^\times \cap U'_D)U_D\pi_\infty^\mathbb{Z}).$$

Any $\mathfrak{p} \in |X| - \{\infty\}$ defines a maximal ideal of A which is still denoted by $\mathfrak{p}$. The canonical homomorphism

$$U'_D \to \mathcal{I}_\mathfrak{m}, \ (a_\mathfrak{p}) \mapsto \prod_{\mathfrak{p}\neq\infty} \mathfrak{p}^{v_\mathfrak{p}(a_\mathfrak{p})}$$

induces an isomorphism

$$U'_D/((K^\times \cap U'_D)U_D\pi_\infty^\mathbb{Z}) \simeq \mathcal{I}_\mathfrak{m}/\mathcal{P}_\mathfrak{m} = \mathrm{Pic}_\mathfrak{m} A.$$

Let N be an open subgroup of $\mathbb{A}_K^\times$ of finite index containing $K^\times U_D$ and let $\mathcal{N} = N/K^\times U_D$. So $\mathcal{N}$ is a subgroup of C_D of finite index. The short exact sequence

$$1 \to \pi_\infty^{\mathbb{Z}} \to C_D \to \mathrm{Pic}_{\mathfrak{m}} A \to 1$$

shows that $\mathcal{N} \cap \pi_\infty^{\mathbb{Z}} = \pi_\infty^{n\mathbb{Z}}$ for some $n > 0$ and hence $K^\times U_D \pi_\infty^{n\mathbb{Z}} \subset N$. □

Corollary 5.21. *If $\infty \notin \mathrm{Supp}(D)$, then the subgroup $K^\times U_D \pi_\infty^{\mathbb{Z}} \subset \mathbb{A}_K^\times$ gives the extension $H_{\mathfrak{m}}/K$ defined in section 5.6.*

Proof. By Theorem 5.18, $H_{\mathfrak{m}}$ is unramified outside $\mathrm{Supp}(D)$ and splits at ∞. The assertion follows by the following commutative diagram

$$\begin{array}{ccc} \mathbb{A}_K^\times & \xrightarrow{(\bullet, H_{\mathfrak{m}}/K)} & \mathrm{Gal}(H_{\mathfrak{m}}/K) \\ \downarrow & & \downarrow \simeq \\ \mathbb{A}_K^\times / K^\times U_D \pi_\infty^{\mathbb{Z}} & \xrightarrow{\simeq} & \mathrm{Pic}_{\mathfrak{m}} A. \end{array}$$

□

Lemma 5.22. *If $\infty \notin \mathrm{Supp}(D)$, then the ray class field K_D is the compositum of $H_{\mathfrak{m}}$ and K_{c}.*

Proof. Consider the degree map

$$\deg : \mathbb{A}_K^\times \to \mathbb{Z}, \quad \deg((a_{\mathfrak{p}})) = \sum_{\mathfrak{p} \in |X|} v_{\mathfrak{p}}(a_{\mathfrak{p}}) \deg(\mathfrak{p}).$$

Then $\deg(K^\times U_0) = 1$ and the inverse image of $n\mathbb{Z}$ in $\mathbb{A}_K^\times$ gives the constant extension $K_n := K \cdot \mathbb{F}_{q^n}$ of K of degree n. Let L be a finite extension of K containing in K_D. By Lemma 5.20, we may assume $\mathcal{N}_L = K^\times U_D \pi_\infty^{n\mathbb{Z}}$ for some $n \geq 1$. Then $\mathcal{N}_L \supset K^\times U_D \pi_\infty^{\mathbb{Z}} \cap \deg^{-1}(n d_\infty \mathbb{Z})$ and hence $L \subset H_{\mathfrak{m}} K_{n d_\infty}$.

□

Lemma 5.23. *For any two effective divisors $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}} \mathfrak{p}$ and $D' = \sum_{\mathfrak{p}} n'_{\mathfrak{p}} \mathfrak{p}$ of X, let $\min(D, D') = \sum_{\mathfrak{p}} \min(n_{\mathfrak{p}}, n'_{\mathfrak{p}}) \mathfrak{p}$ and $\max(D, D') = \sum_{\mathfrak{p}} \max(n_{\mathfrak{p}}, n'_{\mathfrak{p}}) \mathfrak{p}$. Then*

$$K_D \cap K_{D'} = K_{\min(D,D')} \textit{ and } K_D \cdot K_{D'} = K_{\max(D,D')}.$$

Proof. We may assume $\infty \notin \mathrm{Supp}(D + D')$. Obviously, $K_D \cap K_{D'} \supset K_{\min(D,D')}$. Let L be a finite extension of K containing in $K_D \cap K_{D'}$. By Lemma 5.20, there exists $n \geq 1$ such that

$\mathcal{N}_L \supset K^\times U_D \pi_\infty^{n\mathbb{Z}}$ and $\mathcal{N}_L \supset K^\times U_{D'} \pi_\infty^{n\mathbb{Z}}$. Hence $\mathcal{N}_L \supset K^\times U_{\min(D,D')} \pi_\infty^{n\mathbb{Z}}$ and $L \subset K_{\min(D,D')}$. This proves $K_D \cap K_{D'} \subset K_{\min(D,D')}$. The proof of $K_D \cdot K_{D'} = K_{\max(D,D')}$ is similar. □

We are ready to prove Theorem 5.19.

Recall that $K^{\rm ab} = \bigcup_E K_E$ when E runs over all effective divisors of X. To prove $K^{\rm ab} = K_{\rm c} K^{{\rm ab},\infty} K^{{\rm ab},\infty'}$, it suffices to show that $K_E \subset K_{\rm c} K^{{\rm ab},\infty} K^{{\rm ab},\infty'}$ for each E. Write $E = D + D'$ for some effective divisors D and D' such that $\mathrm{Supp}(D) \cap \mathrm{Supp}(D') = \emptyset$, $\infty \notin \mathrm{Supp}(D)$ and $\infty' \notin \mathrm{Supp}(D')$. By Lemma 5.23, $K_E = K_D K_{D'}$ and by Lemma 5.22, $K_D \subset K^{{\rm ab},\infty} K_{\rm c}$ and $K_{D'} \subset K^{{\rm ab},\infty'} K_{\rm c}$. This completes the proof of Theorem 5.19.