# Drinfeld modules and Hilbert's 12th problem over function fields

CJ Dowd

December 13, 2024

The references for this talk at Papikian's book *Drinfeld Modules* and Poonen's note *Introduction to Drinfeld Modules*.

# 1 Basics of Drinfeld modules

## 1.1 Algebraic theory

Let $K$ be a characteristic $p$ field, and let $q$ be a power of $p$. We say that a polynomial over $K$ is $\mathbb{F}_q$-linear if $f(\alpha x + \beta y) = \alpha f(x) + \beta f(y)$ for all $\alpha, \beta \in \mathbb{F}_q$. One can easily show that the $\mathbb{F}_q$-linear polynomials are those of the form

$$f(x) = \sum_{i=0}^{n} a_i x^{q^i}.$$

We denote the set of additive polynomials by $K\langle x \rangle$, which we make into a noncommutative unital ring by defining multiplication to be given by composition: $f * g = f(g(x))$. We also define the ring of twisted polynomials $K\{\tau\}$, which is the set of polynomials in $\tau$ with multiplication is given by $\tau a = a^q \tau$ for all $a \in K$. The map sending $\tau^i \mapsto x^{q^i}$ defines an isomorphism between these two noncommutative rings, and we will freely go between whichever notation is easier.

Let $X$ be a a smooth projective geometrically integral curve over $\mathbb{F}_q$, and fix a closed point $\infty \in X$. Let $A := \mathcal{O}(X \setminus \{\infty\}$. For example, if $X = \mathbb{P}^1$, then $A = \mathbb{F}_q[T]$. Fix a field $K$ equipped with a ring homomorphism $\gamma : A \to K$.

**Definition 1.1.** A *Drinfeld $A$-module* over $K$ of rank $r \geq 1$ is a $\mathbb{F}_q$-algebra homomorphism $\phi : A \to K\{\tau\}$ with

$$\phi_a = \gamma(a) + g_1 \tau + \cdots + g_n \tau^n$$

where $n = -r v_\infty(a)$. (For $A = \mathbb{F}_q[T]$, this is just $n = r \deg(a)$.) Taking the constant term $\gamma$ defines a ring homomorphism $\gamma : A \to K$. If $\gamma$ has nonzero (prime) kernel $\mathfrak{p}$, then we say that $\phi$ has characteristic $\mathfrak{p}$; otherwise, if $\gamma$ is injective, we say that $\phi$ has characteristic 0.

To any Drinfeld module $\phi$, there is an associated $A$-module structure on $K$ given by evaluation: we define $a * k = \phi_a(k)$ for any $a \in A, k \in K$, where $\phi_a(x) \in K\langle x \rangle$ is the polynomial that is the image of $a$ under $\phi$. We denote $K$ with its $A$-module structure by ${}^{\phi}K$.

Very easy exercise: $\phi$ is always injective, so its image is an isomorphic copy of $A$ inside $K\{\tau\}$. We will often conflate $A$ with this image.

**Example 1.2.** The simplest Drinfeld $\mathbb{F}_q[T]$-module is the *Carlitz module*, denoted by $\phi = C$ and defined simply by $C_T = t + \tau$, so that $C$ has rank 1. Then we have

$$\begin{aligned} C_{T^2} &= (t+\tau)(t+\tau) = t^2 + (t+t^q)\tau + \tau^2 \\ C_{T^3} &= (t^2 + (t+t^q)\tau + \tau^2)(t+\tau) \\ &= t^3 + (t^{q+1} + t^{2q} + t^2)\tau + (t + t^q + t^{q^2})\tau^2 + \tau^3 \end{aligned}$$

and so on. Even for these small powers, the coefficients already start to look nontrivial.

**Definition 1.3.** Let $\phi, \psi$ be Drinfeld modules over $K$. Then a morphism $\phi \to \psi$ (defined over $K$) is a polynomial $u \in K\{\tau\}$ such that $u\phi_a = \psi_a u$ for all $a \in A$. A nonzero morphism is called an isogeny.

Composition of morphism is defined by multiplication of the corresponding $u \in K\{\tau\}$ (or composition of polynomials if we treat $u \in K\langle x \rangle$). Therefore, a morphism $u$ is an isomorphism if and only if $u \in K\{\tau\}$ is a nonzero constant.

Exercise: show how $A \hookrightarrow \mathrm{End}(\psi)$ and how $\mathrm{Hom}(\phi, \psi)$ is an $A$-module.

**Example 1.4.** All rank 1 Drinfeld modules (of a given characteristic) become isomorphic over $\overline{K}$. Rank 1 Drinfeld $\mathbb{F}_q[T]$-modules are always of the form $\phi_T = t + c\tau$. Letting $u = c^{1/(q-1)}$, we have

$$\begin{aligned} (t+\tau)u &= c^{q/(q-1)}t + c^{q/(q-1)}\tau \\ &= u(t + c\tau) \end{aligned}$$

so that $u : C \to \phi$ is an isogeny, which has an evident inverse.

As in the case of abelian varieties, isogeny is an equivalence relation due to the existence of the dual isogeny: for any isogeny $u : \phi \to \psi$, there exists an isogeny $\hat{u}$ such that $\hat{u}u = u\hat{u} = \phi_a$ for some $a \in A$ (which we can to require to be monic and of minimal degree to make the choice of $\hat{u}$ unique).

**Definition 1.5.** Let $a \in A$. We write $\phi[a] = \{k \in K : \phi_a(k) = 0\}$, the "$a$-torsion submodule" of $K$. More generally, if $I$ is an ideal in $A$, we write $\phi[I] = \bigcap_{a \in I} \phi[a]$, or equivalently $\phi[I]$ is the set of roots of the unique monic polynomial in $L\langle x \rangle$ generating the principal left ideal $\{\phi_a : a \in I\}$.

In characteristic 0 or if the characteristic does not divide $A$, one can show that $\phi_a$ is a separable polynomial, in the sense that its roots generate a separable extension of $K$. Hence, $\phi[a]$ comes with a $A/(a)$-linear $\mathrm{Gal}(K^{sep}/K)$-action. Moreover, one can show that $\phi[I]$ is isomorphic to $(A/I)^r$ as an $A$-module.

**Definition 1.6.** Let $\mathfrak{l}$ be a nonzero prime ideal. Then the $\mathfrak{l}$-adic Tate module is

$$T_{\mathfrak{l}}\phi = \varprojlim_n \phi[\mathfrak{l}^n]$$

with transition maps given by multiplication by $\phi_{\mathfrak{l}}$. That means $\phi[\mathfrak{l}^{n+1}] \to \phi[\mathfrak{l}^n]$ is given by sending an element $\alpha \in \phi[\mathfrak{l}^{n+1}] \subseteq K$ to its evaluation under $\phi_{\mathfrak{l}}$.

As long as $\mathfrak{l} \neq \mathfrak{p}$, $T_{\mathfrak{l}}\phi$ is a free $A_{\mathfrak{l}}$-module of rank $2r$. Therefore we can attach a $2r$-dimensional $\mathfrak{l}$-adic Galois representation to $\phi$ as long as $\mathfrak{l}$ is not the characteristic.

## 1.2 Analytic theory

Perhaps surprisingly, the theory of Drinfeld modules admits an "analytic" theory very similar to the abelian varieties case that "uniformizes" the algebraic construction.

**Definition 1.7.** Let $X$ be a nice complete curve over $\mathbb{F}_q$. We write $\mathbb{C}_\infty$ for the completion of the algebraic closure of $F = K(X)$ with respect to the place $\infty$.

$\mathbb{C}_\infty$ is again algebraically closed, and it will play the role of the complex numbers for us. Again let $A = \mathcal{O}(X \setminus \{\infty\}$.

**Definition 1.8.** A lattice $\Lambda \subset \mathbb{C}_\infty$ is a submodule such that $\{\lambda \in \Lambda : |\lambda| < r\}$ is finite for all $r \in \mathbb{R}_{\geq 0}$. If $F = \mathrm{Frac}(A)$, the rank of $\Lambda$ is

$$\mathrm{rk}\,\Lambda := \dim_F(F\Lambda) = \dim_{F_\infty}(F_\infty\Lambda)$$

A surprising difference from the classical case:

**Theorem 1.9.** *Let $\Lambda \subset \mathbb{C}_\infty$ be an $A$-module of finite rank. Then $\mathbb{C}_\infty/\Lambda$ is analytically isomorphic to $\mathbb{C}_\infty$, in the sense that there exists a power series $e(z) = a_0 z + \alpha_1 z^q + \alpha_2 z^{q^2} + \ldots$ with a local inverse defining a surjective $\mathbb{F}_q$-linear map $\mathbb{C}_\infty \to \mathbb{C}_\infty$ with kernel $\Lambda$.*

This power series ends up being the *Carlitz-Drinfeld exponential*

$$e_\Lambda(x) := x \prod_{\lambda \in \Lambda}{}' \left(1 - \frac{x}{\lambda}\right)$$

which converges absolutely and is $\Lambda$-periodic. (Sort of analogous to a Hadamard product expansion, except nicer in the non-archimedean setting because we don't need to worry about exponential factors.) This power series is $\mathbb{F}_q$-linear. Consequently, the (standard) $A$-module structure on $\mathbb{C}_\infty/\Lambda$ transfers to a new $A$-module structure on $\mathbb{C}_\infty$, much in the same way a Drinfeld module defines a new $A$-module structure on a field $K$. In fact, this is more than just a similarity:

**Proposition 1.10.** (Uniformization.) *Let $\Lambda$ have rank $r$ over $A$. Then multiplication by $a$ on $\mathbb{C}_\infty/\Lambda$ transfers to a map $\phi_a : \mathbb{C} \to \mathbb{C}$ given by an $\mathbb{F}_q$-linear polynomial of degree $r \deg(a)$. Consequently, the map $a \mapsto \phi_a \in \mathbb{C}_\infty\langle x\rangle$ defines a Drinfeld module over $\mathbb{C}_\infty$ of rank $r$, with the homomorphism $\gamma : A \to \mathbb{C}_\infty$ given simply by inclusion $A \hookrightarrow \mathbb{C}_\infty$, so that the characteristic is 0.*

*Conversely, every Drinfeld module over $\mathbb{C}_\infty$ (with $\gamma : A \to \mathbb{C}_\infty$ the standard embedding) arises in this way. Given Drinfeld modules $\phi, \psi$ over $\mathbb{C}_\infty$ with corresponding lattices $\Lambda, \Lambda' \subset \mathbb{C}_\infty$, morphisms $\phi \to \psi$ correspond bijectively to elements $c \in \mathbb{C}_\infty$ such that $c\Lambda \subseteq \Lambda'$, so isomorphisms correspond to homotheties of lattices.*

# 2 Explicit geometric class field theory

## 2.1 Actions of ideals

Let $K$ be a global function field (for a curve $X$) with ring of integers $A = \mathcal{O}(X \setminus \infty)$. Let $\mathcal{I}, \mathcal{P}$, and $\operatorname{Pic} A := \mathcal{I}/\mathcal{P}$ denote groups of nonzero fractional ideals, principal fractional ideals, and class group, respectively.

**Proposition 2.1.** $\operatorname{Pic} A$ *is in bijection with rank* 1 *$A$-lattices in $\mathbb{C}_\infty$ up to homothety, sending an ideal class $[I]$ to the homothety class of the lattice $I \subset \mathbb{C}_\infty$. hence with rank* 1 *Drinfeld modules over $\mathbb{C}_\infty$ up to isomorphism.*

Now let $\gamma : A \to L$ be an $A$-field, let $I$ be a nonzero ideal in $A$, and let $A$ be a Drinfeld $A$-module over $L$. Then we can define a new Drinfeld module, denoted $I * \phi$, over $L$, characterized by $\phi_I : L\{\tau\} \to L\{\tau\}$ being an isogeny $\phi \to I * \phi$, where $\phi_I$ is the monic generator of the left ideal in $L\{\tau\}$ generated by $\{\phi_a : a \in I\}$. We can also think of this as the quotient of $\mathbb{G}_a$ by $\phi[I]$.

If $I = (a)$ is principal, then $\phi_I = u^{-1}\phi_a$ is monic for some $u \in L$. Then $I * \phi$ is $u^{-1}\phi u$, which is isomorphic to $\phi$ over $L$.

**Proposition 2.2.** *The operation $*$ defines an action of $\mathcal{I}$ on the set of Drinfeld modules over $L$, which descends to an action of* $\operatorname{Pic} A$ *on the set of isomorhpism classes of Drinfeld modules over $L$.*

**Example 2.3.** If $\mathbb{C}_\infty/\Lambda$ corresponds analytically to $\phi$, then $\phi[I] \simeq I^{-1}\Lambda/\Lambda$, and so $I * (\mathbb{C}_\infty/\Lambda) \simeq \mathbb{C}_\infty/I^{-1}\Lambda$.

**Corollary 2.4.** *The set $\mathscr{Y}(\mathbb{C}_\infty)$ of isomorphism classes of rank* 1 *Drinfeld $A$-modules over $\mathbb{C}_\infty$ is a principal homogeneous space under the action of* $\operatorname{Pic} A$*, where $[I]$ acts by multiplication by $I^{-1}$ on rank* 1 *$\mathbb{C}_\infty$-lattices.*

## 2.2 sgn normalization

We'll mostly blackbox the following discussion. It is useful to pick out a specific Drinfeld module from each isomorphism class. sgn-normalization is the way of doing this. One can

define a homomorphism $\operatorname{sgn} : K_\infty^+ \to \mathbb{F}_\infty^\times$, depending on a choice of uniformizer at $\infty$, and a sgn-normalized Drinfeld module is essentially a Drinfeld module whose coefficients are compatible with this homomorphism.

Some facts:

**Theorem 2.5.** *Every rank* 1 *Drinfeld module over* $\mathbb{C}_\infty$ *is isomorphic to a sgn-normalized one.*

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

**Theorem 2.6** ((a))**.** *1. For any subfield* $L \subset \mathbb{C}_\infty$*, if* $\phi \in \mathscr{Y}^+(L)$*, then* $\operatorname{Stab}_{\mathcal{I}}\phi = \mathcal{P}$*.*

*2. Moreover, the action of* $\mathcal{I}$ *on Drinfeld modules makes* $\mathscr{Y}^+(\mathbb{C}_\infty)$ *into a principal homogeneous space under* $\operatorname{Pic}^+ A$*.*

## 2.3 Narrow Hilbert class field

Let $\phi \in \mathscr{Y}^+(\mathbb{C}_\infty)$ be a sgn-normalized Drinfeld module. Let $H^+$ be the field extension of $K$ obtained by adjoining all coefficients of $\phi_a$ for $a \in A$, i.e. the "minimal field of definition" for $\phi$. Since the action of $\mathcal{I}$ is transitive on $\mathscr{Y}^+(C)$, and $I * \phi$ is also defined over $H^+$, we conclude that $H^+$ is independent of the particular choice of $\phi$, so it is intrinsically defined from $(A, \operatorname{sgn})$.

**Definition 2.7.** $H^+$ is the narrow Hilbert class field of $(A, \operatorname{sgn})$.

**Theorem 2.8.** (Explicit narrow Hilbert class field theory for function fields.)

*(a)* $H^+$ *is a finite abelian extension of* $K$ *unramified above every place except possibly* $\infty$*.*

*(b) There is an isomorphism* $\operatorname{Gal}(H^+/K) \to \operatorname{Pic}^+(A)$ *sending* $\operatorname{Frob}_{\mathfrak{p}} \mapsto [\mathfrak{p}]$*. This map agrees with the map* $\operatorname{Gal}(H^+/K) \hookrightarrow \operatorname{Aut}(\mathscr{Y}^+(C)) \simeq \operatorname{Pic}^+ A$*.*

*Proof.*

$\operatorname{Aut}(\mathbb{C}_\infty/K)$ acts on $\mathscr{Y}^+(\mathbb{C}_\infty)$, so this maps $H^+$ to itself. Since we can define $H^+$ using the coefficients of one particular Drinfeld module, $H^+$ is finitely generated over $K$, so it must be a finite normal extension, and we can show that this is separable.

We get an injective homomorphism

$$\chi : \operatorname{Gal}(H^+/K) \hookrightarrow \operatorname{Aut}_{\operatorname{Pic}^+ A} \mathscr{Y}^+(\mathbb{C}_\infty) \simeq \operatorname{Pic}^+ A$$

which shows that $\operatorname{Gal}(H^+/K)$ is abelian.

Let $B^+$ be the integral closure of $A$ in $H^+$ and $P \subset B^+$ a nonzero prime lying above $\mathfrak{p} \subset A$. There is a reduction theory that lets us define a reduction map $\rho : \mathscr{Y}^+(H^+) \to \mathscr{Y}^+(\mathbb{F}_p)$ that is $\operatorname{Pic}^+ A$-equivariant. The $\operatorname{Pic}^+ A$ action is faithful on both source and target. $\mathscr{Y}^+(H^+)$

is a PHS for $\mathrm{Pic}^+ A$, so we conclude that the reduction map is injective. Therefore, if $g \in \mathrm{Gal}(H^+/K)$ lies in the inertia subgroup for $P$, then $g$ acts trivially downstairs, hence it acts trivially upstairs, so $g = 1$. Therefore $H^+/K$ is unramified at $P \neq \infty$.

Finally, we want to show that $\chi$ is actually an isomorphism. Now that we know that $H^+/K$ is unramified at $P$, let $\sigma = \mathrm{Frob}_P = \mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(H^+/K)$. We want to show that

$$\sigma\phi = \mathfrak{p} * \phi$$

for any $\phi \in \mathscr{Y}^+(\mathbb{F}_P)$. If we can show this, then this shows that the Frobenius action on $\mathscr{Y}^+(\mathbb{F}_P)$ lifts to $Y^+(H^+)$ as $\phi \mapsto \mathfrak{p} * \phi$, i.e. $\chi$ sends $\mathrm{Frob}_{\mathfrak{p}}$ to the class of $\mathfrak{p}$ in $\mathrm{Pic}^+(A)$.

To prove the claim, let $\psi := \mathfrak{p} * \phi$. Then by the definition of the ideal action, $\psi_a \phi_{\mathfrak{p}} = \phi_{\mathfrak{p}} \phi_a$. The characteristic of $\phi$ over $\mathbb{F}_p$ is $\mathfrak{p}$, and one can show that this means that $\phi_{\mathfrak{p}} = \tau^{\deg \mathfrak{p}}$, hence $\psi_a \tau^{\deg \mathfrak{p}} = \tau^{\deg \mathfrak{p}} \phi_a$. But this just means that $\mathfrak{p}$ acts by raising coefficients to the power of $q^{\deg \mathfrak{p}}$, which is exactly the action of $\mathrm{Frob}_{\mathfrak{p}}$. ■

This theorem solves a case of Hilbert's 12th problem by explicitly describing one of the ray class fields of $A$. It is not too hard to generalize the arguments from the previous section to make them work more generally for ray class fields of an arbitrary modulus (including the standard class field). See Poonen's notes for the precise statement.

## 2.4 Explicit example

We end by giving an explicit example of a construction of the narrow Hilbert class field.

**Example 2.9.** Let $q = 2$ and let $X$ be the elliptic curve over $\mathbb{F}_2$ defined by $y^2 + y = x^3$, and let $\infty$ be the point at infinity, so that $A = \mathbb{F}_2[x, y]/(y^2 + y - x^3)$. The residue field at $\infty$ is just $\mathbb{F}_2$, which means that there is only one choice of uniformizer for $K_\infty$, and we have $\mathrm{Pic}^+ A \simeq \mathrm{Pic}\, A \simeq \mathrm{Pic}^0 X \simeq X(\mathbb{F}_2)$, which is a group of order 3. Consequently, the narrow Hilbert class field $H^+$ and the Hilbert class field coincide $H$, and $[H : K] = 3$.

To construct $H$ explicitly, we need only write down *one* sgn-normalized Drinfeld module over a finite extension of $K$. Then the coefficients of this Drinfeld module generate $H$. I haven't really told you exactly what sgn-normalized means, but in this case giving a sgn-normalized rank 1 Drinfeld module over $L$ means giving elements $a, c_1, c_2 \in L$ such that

$$\phi_x = x + a\tau + \tau^2 \in L\{\tau\}$$
$$\phi_y = y + c_1\tau + c_2\tau^2 + \tau^3 \in L\{\tau\}$$

such that $\phi_x \phi_y = \phi_y \phi_x$ and $\phi_y^2 + \phi_y = \phi_x^3$. The second condition turns out to be redundant, since the first condition tells us that $\phi_x$ commutes with $f = \phi_y^2 + \phi_y - \phi_x^3$. But $\phi_x$ has a nonzero constant term $x$ and $\phi_y^2 + \phi_y - \phi_x^3$ has a trivial constant term. This means if $f$ is nonzero that the lowest degree term of $\phi_x f$ has coefficient $x$ but the lowest degree term of $f\phi_x$ has coefficient $x^{q^i} \neq x$ for $i \geq 1$, so in fact we must have $f = 0$.

Doing out the multiplication and matching coefficients, the condition $\phi_x\phi_y = \phi_y\phi_x$ is equivalent to

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

The first two equations let us eliminate the variables $c_1$ and $c_2$, so we end up with two polynomial conditions on $a$. The gcd of these two polynomials ends up being $a^3 + (x^2 + x)a^2 + (x+1)^2a + (x+1)^4 = 0$, so $H$ is the extension generated by a root of this polynomial, since $c_1, c_2$ are rational functions of $x, y$, and $a$.