Drinfeld-Stuhler modules

Mihran Papikian

Pennsylvania State University

Arithmetic of Function Fields,
Münster, June 26-30, 2017

Notation

- F= function field of smooth projective curve C over $\mathbb{F}_q$
- ∞ = fixed place of F
- $A \subset F$ = functions regular away from ∞
- L= field equipped with A-algebra structure $\gamma : A \to L$
- A-characteristic of L is $\mathrm{char}_A(L) = \ker(\gamma)$
- $\tau : x \mapsto x^q$
- $L[\tau]$=skew polynomial ring with $\tau b = b^q \tau$, $b \in L$
- $M_d(L[\tau])$= ring of $d \times d$ matrices with entries in $L[\tau] \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,L}^d)$
- Action on the tangent space $\mathrm{Lie}(\mathbb{G}_{a,L}^d)$

$$\partial : M_d(L[\tau]) \longrightarrow M_d(L)$$
$$\sum_{i \geq 0} B_i \tau^i \longmapsto B_0$$

Notation

- D=central division algebra over F of dimension d^2
- $\mathrm{Ram}(D) = \{v \text{ place of } F \mid D \otimes F_v \ncong M_d(F_v)\}$
- Assume $\infty \notin \mathrm{Ram}(D)$
- $\mathfrak{r}(D) = \prod_{\mathfrak{p} \in \mathrm{Ram}(D)} \mathfrak{p}$, discriminant of D
- O_D=maximal A-order in D (note that A is the center of O_D)

Definition of Drinfeld-Stuhler modules

Assume $\mathrm{char}_A(L) \nmid \mathfrak{r}(D)$.

Drinfeld-Stuhler $\mathbf{O_D}$-module over L is an embedding

$$\begin{aligned} \phi : O_D &\longrightarrow M_d(L[\tau]) \\ b &\longmapsto \phi_b \end{aligned}$$

satisfying the following conditions:

(i) For any $0 \neq b \in O_D$ the kernel $\phi[b] := \ker \phi_b$ of the endomorphism ϕ_b of $\mathbb{G}_{a,L}^d$ is a finite group scheme over L of order $\#(O_D/O_D \cdot b)$.

(ii) The composition

$$A \to O_D \xrightarrow{\phi} M_d(L[\tau]) \xrightarrow{\partial} M_d(L)$$

maps $a \in A$ to $\mathrm{diag}(\gamma(a), \dots, \gamma(a))$.

- Morphisms: $\mathrm{Hom}_L(\phi, \psi) := \{u \in M_d(L[\tau]) \mid u\phi_b = \psi_b u \text{ for all } b \in O_D\}$
- Isogeny is a morphism with finite kernel

Comments

1. If $d = 1$, so that $D = F$, we get Drinfeld A-modules of rank 1.
2. The idea of Drinfeld-Stuhler module (in its "shtuka" incarnation) was proposed by Ulrich Stuhler. The modular varieties of these objects were studied by Laumon, Rapoport and Stuhler in

   [LRS] *$\mathcal{D}$-elliptic sheaves and the Langlands correspondence*, Invent. Math. (1993).

   with the aim of proving the local Langlands correspondence for GL_d in positive characteristic.
3. Condition (i) is equivalent to $\#\phi[b] = \#(A/\mathrm{Nr}(b)A)$, where $\mathrm{Nr}(b)$ is the non-reduced norm of b in D.
4. $\phi[b]$ is not necessarily (left) $\phi(O_D)$-invariant, so $\phi[b] \ncong O_D/O_D b$.
5. But it is true that for $a \in A$ coprime to $\mathrm{char}_A(L)$ we have $\phi[a] \cong O_D/O_D a$.

Basic properties

- $0 \neq u \in \mathrm{Hom}_L(\phi, \psi)$ is an isogeny.
- $\phi[b]$ is étale if and only if $\mathrm{Nr}(b)$ is not divisible by $\mathrm{char}_A(L)$.
- Let $\partial_\phi = \partial \circ \phi : O_D \to M_d(L)$ be the action on the tangent space. Then

  $$\partial_{\phi,L} = \partial_\phi \otimes_A L : O_D \otimes_A L \to M_d(L)$$

  is an isomorphism.
  $\Rightarrow$ Drinfeld-Stuhler modules can be defined only over fields that split D. In particular, Drinfeld-Stuhler module cannot be defined over F itself, even if $F = \mathbb{F}_q(T)$.
  (If $[L : F] = d$, then L splits D if and only if L embeds into D.)
- If $\mathrm{char}_A(L) = 0$, then $\partial : \mathrm{Hom}_L(\phi, \psi) \to M_d(L)$ is injective.
  $\Rightarrow$ $\mathrm{End}_L(\phi)$ is commutative and is isomorphic to an A-subalgebra of L.

Example

By Grunwald-Wang theorem, there is a Galois extension K/F with $\mathrm{Gal}(K/F) \cong \mathbb{Z}/d\mathbb{Z}$, a generator σ of $\mathrm{Gal}(K/F)$, and $f \in A$ such that

$$D \cong (K/F, \sigma, f) = \bigoplus_{i=0}^{d-1} Kz^i, \qquad z \cdot y = \sigma(y)z, \quad z^d = f, \quad y \in K.$$

- Assume K is imaginary (i.e., ∞ does not split in K/F), and let O_K be the integral closure of A in K.
- Assume the A-order

  $$O_D = \bigoplus_{i=0}^{d-1} O_K z^i$$

  is maximal in D.

Remark

O_D might or might not be maximal in general. This can be verified in a given case by comparing the discriminant $f^{d(d-1)}\mathrm{disc}(K/F)^d$ of O_D with the discriminant of a maximal order. For prime d the discriminant of maximal order is $\mathfrak{r}(D)^{d(d-1)}$.

Example (cont.)

Let $\varphi : O_K \to L[\tau]$ be a Drinfeld O_K-module of rank 1 defined over some field L. Let

$$\phi : O_D = \bigoplus_{i=0}^{d-1} O_K z^i \longrightarrow M_d(L[\tau])$$

be defined as follows:

$$\phi_\alpha = \mathrm{diag}(\varphi_\alpha, \varphi_{\sigma\alpha}, \dots, \varphi_{\sigma^{d-1}\alpha}), \quad \alpha \in O_K,$$

$$\phi_z = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ \varphi_f & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Note that $\phi_z \phi_\alpha = \phi_{\sigma\alpha}\phi_z$ and $\phi_z^d = \phi_f$, so ϕ is an embedding. It is not hard to check that (i) and (ii) hold, so ϕ is a Drinfeld-Stuhler O_D-module.

Example (explicit version)

- Let $A = \mathbb{F}_q[T]$, $F = \mathbb{F}_q(T)$, $K = \mathbb{F}_{q^d}(T)$.
- Then $O_K = \mathbb{F}_{q^d}[T]$ and $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q)$.
- Let $\mathfrak{r} = \mathfrak{p}_1 \cdots \mathfrak{p}_m$ product of distinct primes of degrees coprime to d.
- Let $D = (K/F, \mathrm{Frob}_q, \mathfrak{r})$.
  If $\sum_{i=1}^m \deg(\mathfrak{p}_i)$ is divisible by d, then D splits at ∞ and $\mathfrak{r}(D) = \mathfrak{r}$.
- $O_D = \bigoplus_{i=0}^{d-1} O_K z^i$ is maximal in this case.
- Let L be an O_K-field and $\gamma : A \to O_K \to L$ be the composition homomorphism.
- Let $\varphi : O_K \to L[\tau]$ be defined by $\varphi_T = \gamma(T) + \tau^d$.

Example (explicit version)

$$\phi : \bigoplus_{i=0}^{d-1} \mathbb{F}_{q^d}[T]z^i \longrightarrow M_d(L[\tau])$$

is defined by

$$\phi_T = \mathrm{diag}(\varphi_T, \dots, \varphi_T), \qquad \varphi_T = \gamma(T) + \tau^d$$

$$\phi_h = \mathrm{diag}(h, h^q, \dots, h^{q^{d-1}}), \qquad h \in \mathbb{F}_{q^d},$$

$$\phi_z = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ \varphi_{\mathfrak{r}} & 0 & 0 & \cdots & 0 \end{pmatrix}.$$

Three equivalent categories

1. An O_D-**motive** is a left $O_D^{\mathrm{opp}} \otimes_{\mathbb{F}_q} L[\tau]$-module M, which is free $L[\tau]$-module of rank d, locally free $O_D^{\mathrm{opp}} \otimes_{\mathbb{F}_q} L$-module of rank 1, and for all $a \in A$, $(a \otimes 1 - 1 \otimes \gamma(a))\overline{M} \subset \tau\overline{M}$, where $\overline{M} := M \otimes_L L^{\mathrm{alg}}$.
2. $\mathcal{D}$-**elliptic sheaf** over L is essentially a vector bundle of rank d^2 on $C \times_{\mathrm{Spec}(\mathbb{F}_q)} \mathrm{Spec}(L)$ equipped with an action of O_D and with a meromorphic O_D-linear Frobenius satisfying certain conditions.
3. Let $\mathbb{C}_\infty = \widehat{F_\infty^{\mathrm{alg}}}$. For a Drinfeld-Stuhler module ϕ over $\mathbb{C}_\infty$ there is a discrete O_D-submodule Λ_ϕ of $\mathbb{C}_\infty^d$, which is locally free of rank 1, and an entire $\mathbb{F}_q$-linear function $\exp_\phi : \mathbb{C}_\infty^d \to \mathbb{C}_\infty^d$, such that for any $b \in O_D$ the following diagram is commutative:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \Lambda_\phi & \longrightarrow & \mathbb{C}_\infty^d & \xrightarrow{\exp_\phi} & \mathbb{C}_\infty^d & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \partial_\phi(b)} & & \downarrow{\scriptstyle \partial_\phi(b)} & & \downarrow{\scriptstyle \phi_b} & & \\
0 & \longrightarrow & \Lambda_\phi & \longrightarrow & \mathbb{C}_\infty^d & \xrightarrow{\exp_\phi} & \mathbb{C}_\infty^d & \longrightarrow & 0.
\end{array}$$

Three equivalent categories (cont.)

- Drinfeld-Stuhler O_D-modules $\Longleftrightarrow$ O_D-motives (Anderson)
- O_D-motives $\Longleftrightarrow$ $\mathcal{D}$-elliptic sheaves mod $\mathbb{Z}$ (Taelman and [LRS])
- Uniformization $\mathbb{C}_\infty^d/\Lambda_\phi$ (Taelman)

Endomorphism rings of Drinfeld-Stuhler modules

Theorem

Let ϕ be a Drinfeld-Stuhler O_D-module over L. Then:

1. $\mathrm{End}_L(\phi)$ *is a projective A-module of rank $\leq d^2$.*
2. *If $\mathrm{char}_A(L) = 0$, then $\mathrm{End}_L(\phi)$ is an A-order in an imaginary field extension of F which embeds into D. In particular, $\mathrm{End}_L(\phi)$ is commutative and its rank over A divides d.*
3. *The automorphism group $\mathrm{Aut}_L(\phi) := \mathrm{End}_L(\phi)^\times$ is isomorphic to $\mathbb{F}_{q^r}^\times$ for some r dividing d.*

Proof.

Proof uses O_D-motives, $\mathcal{D}$-elliptic sheaves, and the uniformization of ϕ. □

Complex multiplication (Example)

Let K/F be imaginary extension of degree d.
$\varphi : O_K \to \mathbb{C}_\infty[\tau]$ is a Drinfeld O_K-module of rank 1.
Let $\phi : O_D = \bigoplus_{i=0}^{d-1} O_K z^i \to M_d(\mathbb{C}_\infty[\tau])$ be defined by

$$\phi_\alpha = \mathrm{diag}(\varphi_\alpha, \varphi_{\sigma\alpha}, \dots, \varphi_{\sigma^{d-1}\alpha}), \quad \alpha \in O_K,$$

$$\phi_z = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ \varphi_f & 0 & 0 & \cdots & 0 \end{pmatrix},$$

Then

$$O_K \xrightarrow{\sim} \{\mathrm{diag}(\varphi_\alpha, \dots, \varphi_\alpha) \mid \alpha \in O_K\} \subset M_d(L[\tau]).$$

commutes with ϕ_α and ϕ_z. Therefore $O_K \cong \mathrm{End}(\phi)$.

Definition

Drinfeld-Stuhler module ϕ over L with $\mathrm{char}_A(L) = 0$ has *complex multiplication* by O_K if $O_K \cong \mathrm{End}(\phi)$. Note that in that case K necessarily splits D.

Complex multiplication

Theorem

Let K be an imaginary extension of F of degree d, which splits D. Then:

1. *Up to isomorphism, the number of Drinfeld-Stuhler modules over $\mathbb{C}_\infty$ having CM by O_K is finite and non-zero. (There is an explicit formula for this number.)*
2. *A Drinfeld-Stuhler module having CM by O_K can be defined over the Hilbert class field of K.*

Proof.

1. Compute the number of lattices in $\mathbb{C}_\infty^d$ having CM by O_K.
2. The corresponding motive is an $O_D^{\mathrm{opp}} \otimes_A O_K$-module. But $O_D^{\mathrm{opp}} \otimes_A O_K$ is a maximal order in $M_d(K)$, so Morita equivalence reduces the problem to the case of Drinfeld O_K-modules of rank 1.

□

Supersingularity (Example)

- $L =$ degree d extension of $A/TA \cong \mathbb{F}_q$
- Fix a generator h of $L \cong \mathbb{F}_{q^d}$ over $\mathbb{F}_q$
- $O_K = \mathbb{F}_{q^d}[T]$
- $O_D = \bigoplus_{i=0}^{d-1} O_K z^i$
- $\varphi : O_K \longrightarrow L[\tau]$, $\qquad \varphi_T = \tau^d \quad$ (since $\gamma(T) = 0$)
- $\phi : O_D = \bigoplus_{i=0}^{d-1} O_K z^i \longrightarrow M_d(L[\tau])$ is generated over $\mathbb{F}_q$ by

$$\phi_T = \mathrm{diag}(\tau^d, \dots, \tau^d), \quad \phi_h = \mathrm{diag}(h, h^q, \dots, h^{q^{d-1}}),$$

$$\phi_z = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \\ \varphi_{\mathfrak{r}} & 0 & 0 & \cdots & 0 \end{pmatrix},$$

Supersingularity (Example)

Let

$$\tau^i := \mathrm{diag}(\tau^i, \dots, \tau^i),$$
$$h := \mathrm{diag}(h, \dots, h),$$
$$\kappa_i = \phi_z^i \tau^{d-i}, \quad 1 \leq i \leq d-1.$$

Then:

- $E := \mathbb{F}_q[\phi_T, h, \kappa_1, \dots, \kappa_{d-1}] \subset \mathrm{End}_L(\phi)$.
- $\overline{D} := E \otimes_A F \cong (K/F, \mathrm{Frob}_q, \mathfrak{r}^{-1} T)$ is a central division algebra over F with $\mathrm{inv}_T(\overline{D}) = 1/d$, $\mathrm{inv}_\infty(\overline{D}) = -1/d$, $\mathrm{inv}_v(\overline{D}) = -\mathrm{inv}_v(D)$ for other places.
- E is a maximal A-order in $\overline{D}$
  $\Longrightarrow \mathrm{End}_L(\phi)$ is a maximal A-order in $\overline{D}$.
- $\mathbb{F}_{q^d}^\times \cong \mathbb{F}_q(h)^\times \subset \mathrm{Aut}_L(\phi)$
  $\Longrightarrow \mathrm{Aut}_L(\phi) \cong \mathbb{F}_{q^d}^\times$.
- Note that $\phi[T] = \ker \mathrm{diag}(\tau^d, \dots, \tau^d)$ is connected.

Supersingularity

Theorem

Let L be a finite extension of $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$. Let ϕ be Drinfeld-Stuhler module over L. The following conditions are equivalent:

- $\dim_F(\mathrm{End}_{L^{\mathrm{alg}}}(\phi) \otimes_A F) = d^2$.
- *$\phi[\mathfrak{p}]$ is connected.*
- *Some power of $\mathrm{diag}(\tau, \dots, \tau)$ lies in $\phi(A)$.*

If ϕ satisfies these conditions, then it is called **supersingular**.

Theorem

Let ϕ be a supersingular Drinfeld-Stuhler module over $\overline{\mathbb{F}}_\mathfrak{p}$. Then:

1. *$\mathrm{End}(\phi)$ is a maximal A-order in $\overline{D}$.*
2. *ϕ can be defined over the extension of $\mathbb{F}_\mathfrak{p}$ of degree $d \cdot \#\mathrm{Pic}(A)$.*
3. *Up to isomorphism, the number of supersingular Drinfeld-Stuhler modules over $\overline{\mathbb{F}}_\mathfrak{p}$ is equal to the class number of $\mathrm{End}(\phi)$.*

Rational points on modular varieties

It is known that in general the fields of moduli for abelian varieties are not necessarily fields of definition.
This does not happen for elliptic curves (thanks to j-invariant), but does happen for abelian surfaces with quaternionic multiplication:

Example

Let B be the indefinite quaternion algebra over $\mathbb{Q}$ of discriminant 6. Let X^B be the associated Shimura curve. Then

$$X^B : x^2 + y^2 + 3 = 0.$$

Since $(\sqrt{-7})^2 + 2^2 + 3 = 0$, $X^B(\mathbb{Q}(\sqrt{-7})) \neq \emptyset$. But $K = \mathbb{Q}(\sqrt{-7})$ does not split B so there are no abelian surfaces with multiplication by B defined over K.

Remark

A necessary condition for this phenomenon is that B ramifies at 2.

Rational points on modular varieties

Let $A = \mathbb{F}_q[T]$, $F = \mathbb{F}_q(T)$, and $d = 2$.
Then the modular curve X^D of Drinfeld-Stuhler O_D-modules is the function field analogue of X^B. However:

Theorem

For any finite extension L of F_v, $v \in \mathrm{Ram}(D)$, which does not split D we have $X^D(L) = \emptyset$.

For $d \geq 2$ the coarse moduli scheme X^D of Drinfeld-Stuhler modules is smooth projective of dimension $(d-1)$ over F.

Theorem

Assume d and $q^d - 1$ are coprime. If L is a field extension of F which does not split D, then $X^D(L) = \emptyset$.

Remark

If $d \neq p$ is prime, then the assumption is satisfied if and only if $d \nmid q - 1$.

Proof

Let K/L be a finite Galois extension. Let ϕ be a Drinfeld-Stuhler module over K such that for any $\sigma \in \mathrm{Gal}(K/L)$ we have $\phi \cong \phi^\sigma$, where

$$\phi^\sigma : O_D \xrightarrow{\phi} M_d(K[\tau]) \xrightarrow{\sigma} M_d(K[\tau]).$$

We need to show that ϕ can be defined over L.

- For each σ choose an isomorphism $c_\sigma : \phi \to \phi^\sigma$. Then $c_{\sigma\delta} = \sigma(c_\delta) c_\sigma \alpha_{\sigma,\delta}$ with $\alpha_{\sigma,\delta} \in \mathrm{Aut}(\phi) \cong \mathbb{F}_{q^r}^\times$, $r \mid d$.
- If d and $q^d - 1$ are coprime then

  $$\mathrm{GL}_d(K[\tau]) \xrightarrow{\partial} \mathrm{GL}_d(K) \xrightarrow{\det} K^\times$$

  maps $\mathrm{Aut}(\phi)$ isomorphically onto its image. Using Hilbert 90 for $K^\times$, one can modify the isomorphism c_σ so that now they satisfy cocycle condition $c_{\sigma\delta} = \sigma(c_\delta) c_\sigma$.
- Prove Hilbert 90 for $\mathrm{GL}_d(K[\tau])$: we can find $S \in \mathrm{GL}_d(K[\tau])$ such that $c_\sigma = (\sigma S)^{-1} S$.
- $\psi = S\phi S^{-1}$ is defined over L.

References

- M. Papikian, *Drinfeld-Stuhler modules*, http://arxiv.org/abs/1701.00738
- M. Papikian, *Local diophantine properties of modular curves of $\mathcal{D}$-elliptic sheaves*, Journal für die reine und angewandte Mathematik **664** (2012), 115-140.
- M. Papikian, *Endomorphisms of exceptional $\mathcal{D}$-elliptic sheaves*, Mathematische Zeitschrift **266** (2010), 407-423.
- http://www.math.psu.edu/papikian/Research/research.html