國家天元數學中部中心

算術幾何短期課程

Introduction to Drinfeld modules and modular varieties

12, 15, 17, 19, 22 . 08 , 2022

余家富

(中研院數學所)

Ref: [L] G. Laumon, Cohomology of Drinfeld modular varieties Vol. I.

[G] D. Goss, Basic structure of function field arithmetic.

Goal: (1) Construction of Drinfeld modular varieties. (Chap. I of [L])

(2) Introduce tools for studying Drinfeld modules particularly over "finite characteristic" fields, e.g. endomorphism rings, Tate modules and Dieudonné modules. (Chap II. of [L]).

Basic parallel analogues between number field world and function field world:

global fields.	# field	function fields.
F	$\mathbb{Q}$	$\mathbb{F}_q(t)$
A	$\mathbb{Z}$	$\mathbb{F}_q[t]$
∞	usual abs. value $\lvert\ \rvert$, or real place	∞, pt at the infinity.
F_∞	$\mathbb{R}$	$\mathbb{F}_q((t^{-1}))$.
$\mathbb{C}_\infty$	$\mathbb{C}$	$\widehat{\overline{F_\infty}}$
E	elliptic curves / $\mathbb{C}$	Drinfeld A-modules of rank 2 / $\mathbb{C}_\infty$

Ω	$\mathbb{H}^{\pm} = \mathbb{C} - \mathbb{R}$ double half plane	$\mathbb{C}_\infty - F_\infty$: Drinfeld upper half plane
$Gl_2(A)$	$GL_2(\mathbb{Z})$	$GL_2(\mathbb{F}_q[t])$.
moduli spaces	$GL_2(\mathbb{Z})\backslash\mathbb{H}^{\pm} \simeq SL_2(\mathbb{Z})\backslash\mathbb{H}^{+}$	$GL_2(A)\backslash\Omega$

$$\mathbb{H} = \{z \in \mathbb{C} : Im(z) > 0\}.$$

$SL_2(\mathbb{Z})\backslash\mathbb{H} \simeq \left\{ \begin{array}{c} \text{isom classes of} \\ \text{elliptic curves} / \mathbb{C} \end{array} \right\}$: $\mathbb{H}$: complex analytic space

$GL_2(A)\backslash\Omega \simeq \left\{ \begin{array}{c} \text{isom classes of} \\ \text{Drinfeld } A\text{-modules} \\ \text{of rank 2} / \mathbb{C}_\infty \end{array} \right\}$ Ω "rigid" analytic space.

analytic construction of moduli spaces

→ Provide an arithmetic construction of $GL_r(A)\backslash\Omega$

for general function fields and any rank.

Notation :

p : prime, q : a power of p.

$\mathbb{F}_q$: the finite field of q elements.

X : geometrically connected smooth projective alg curve $/\mathbb{F}_q$.

1-dim'l reduced closed closed subscheme of $\mathbb{P}^N_{\mathbb{F}_q}$.

geom. connected : $X \otimes_{\mathbb{F}_q} \overline{\mathbb{F}_q} = X \times_{\operatorname{Spec}\mathbb{F}_q} \operatorname{Spec}\overline{\mathbb{F}_q}$: connected.

Smooth : $X \underset{\mathbb{F}_q}{\otimes} \overline{\mathbb{F}_q}$ is non-singular, i.e.

$\forall$ a closed point $x \in X \otimes \overline{\mathbb{F}_q}$ ($\leftrightarrow$ $x \in X(\overline{\mathbb{F}_q})$)

the local ring $\mathcal{O}_x$ is a DVR ($\Leftrightarrow$ $\mathcal{O}_x$: regular)

$F =: \mathbb{F}_q(X)$ the function field of X over $\mathbb{F}_q$.

= the quotient field of the ring of regular functions on an Zariski open subset U.

geom. connected $\Rightarrow$ the constant subfied of $F := \{a \in F : a \text{ alg} / \mathbb{F}_q\}$
$= \mathbb{F}_q$.

∞ : closed point, as the "point at infinity".

$A = \Gamma(X \setminus \{\infty\}, \mathcal{O}_X)$: the ring of regular functions on $X \setminus \{\infty\}$.
a Dedekind domain.

$|X|$: the set of closed points. $= X(\overline{\mathbb{F}_q}) / \Gamma_{\mathbb{F}_q} = \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$

We identify $|X|$ with the set of places $\left(\begin{array}{l}\text{or valuations} \\ v : F \to \mathbb{Z} \cup \{\infty\}\end{array}\right)$ of F.

For any $v \in |X|$, F_v = the completion of F at v

$\mathcal{O}_v$ = the valuation ring (the ring of integers) of F_v.

$\mathbb{F}_v := \mathcal{O}_v / m_v$, the residue field at v, $[\mathbb{F}_v : \mathbb{F}_q] = \deg(v)$

$[\mathbb{F}_v : \mathbb{F}_p] = \deg_{\mathbb{F}_p}(v)$

$v : F_v \to \mathbb{Z} \cup \{\infty\}$ discrete valuation
normalized by $v(\pi_v) = 1$

π_v : uniformizer of F_v.

$\forall\ a \in A \setminus \{0\}$. define $\deg(a) := \dim_{\mathbb{F}_q} A/(a)$ $\left(\deg_{\mathbb{F}_p}(a) = \dim_{\mathbb{F}_p} A/(a)\right)$

If $u \in A^\times$, $\deg(u) = 0$

Thm 1: (Product formula) $\forall\ a \in F^\times$, one has

$$\sum_{v \in |X|} \deg(v) \cdot v(a) = 0$$

$$(a) = \prod_{v \neq \infty} \mathfrak{P}_v^{v(a)}$$

If $a \neq 0 \in A$. $A/(a) = \prod_{v \neq \infty} A/\mathfrak{P}_v^{v(a)}$, $\dim_{\mathbb{F}_q} A/\mathfrak{P}_v = \deg(v)$

$\Rightarrow \dim_{\mathbb{F}_q} A/(a) = \sum_{v \neq \infty} \deg(v) \cdot v(a)$

$\Rightarrow \boxed{\deg(a) = -\deg(\infty)\ \infty(a).}$

Endomorphisms of the additive groups.

k: any commutative ring of char p. $k \supset \mathbb{F}_p$.

A polynomial $f(t) \in k[t]$ is additive if $f(t_1 + t_2) = f(t_1) + f(t_2)$ in $k[t_1, t_2]$.

Lemma 2 Every additive polynomial $f(t) \in k[t]$ is of the form

$$f(t) = \sum_{i=0}^{n} a_i t^{p^i} = a_0 t + a_1 t^p + \cdots + a_n t^{p^n}$$

Pf: Exercise.

$\mathbb{G}_{a,k} = \operatorname{Spec} k[t]$, the additive group $/k$.

The group law: $m : \mathbb{G}_{a,k} \times \mathbb{G}_{a,k} \to \mathbb{G}_{a,k}$ $\quad (x,y) \mapsto x+y$

$$\iota : \mathbb{G}_{a,k} \to \mathbb{G}_{a,k} \qquad x \mapsto -x.$$

Hopf algebra $k[t]$.

Co-multiplication $\Delta : k[t] \to k[t] \otimes k[t] = k[t_1, t_2]$

$$\Delta(t) = t \otimes 1 + 1 \otimes t \qquad t_1 = t \otimes 1$$
$$= t_1 + t_2 \qquad t_2 = 1 \otimes t_2$$

$$\iota : k[t] \to k[t], \quad \iota(t) = -t.$$

$\operatorname{End}(\mathbb{G}_{a,k})$: the endomorphism ring of $\mathbb{G}_{a,k}$.

$$= \{ f : \mathbb{G}_{a,k} \to \mathbb{G}_{a,k} . \; m \circ (f,f) = f \circ m \}$$

$$\begin{tikzcd} \mathbb{G}_a^2 \arrow[r, "(f,f)"] \arrow[d, "m"] & \mathbb{G}_a^2 \arrow[d] \\ \mathbb{G}_a \arrow[r, "f"] & \mathbb{G}_a \end{tikzcd}$$

$$= \{ f(t) \in k[t] : f(t_1 + t_2) = f(t_1) + f(t_2) \}$$

$a \in k \quad [a] : \mathbb{G}_a \to \mathbb{G}_a, \quad t \mapsto at$

$\tau = \tau_p \quad \mathbb{G}_a \to \mathbb{G}_a, \quad t \mapsto t^p. \quad \Rightarrow \tau \cdot [a] = [a^p] \tau.$

<u>Define</u>: $k\{\tau\} = \{ a_0 + a_1\tau + \cdots + a_n\tau^n : a_i \in k, \; \tau a = a^p \tau \}$

Then $\operatorname{End}(\mathbb{G}_{a,k}) \simeq k\{\tau\}$

$$[a] \longleftarrow a$$
$$t \mapsto t^p \longleftarrow \tau$$

Suppose $k \supset \mathbb{F}_q$ say $f(t) \in \mathrm{End}(\mathbb{G}_{a,k})$ is $\mathbb{F}_q$-linear if

it commutes with $[a]$, $\forall a \in \mathbb{F}_q$. i.e. $f(at) = a f(t)$ $\forall a \in \mathbb{F}_q$.

Easy to show $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,k}) := \left\{ \begin{array}{l} \mathbb{F}_q\text{-linear endomorphisms} \\ \text{on } \mathbb{G}_{a,k} \end{array} \right\}$

$$= k\{\tau_q\} \subseteq k\{\tau\}$$

$$\tau_q(z) = z^q, \quad \tau_q a = a^q \tau_q$$

If $f = \sum_{i=0}^{n} a_i \tau^i \in k\{\tau\}$

$\partial f = a_0$, the derivative of f.

$$\begin{array}{ccc} \mathbb{G}_a & \xrightarrow{f} & \mathbb{G}_a \\ \mathrm{Lie}(\mathbb{G}_a) & \longrightarrow & \mathrm{Lie}(\mathbb{G}_a) \\ \| & & \| \\ k & & k \\ X & \longmapsto & a_0 X. \end{array}$$

Drinfeld modules

Def (1) An **A-field** is (L, γ), where L: a field, $\gamma: A \to L$ ring homo. The **A-characteristic of (L,γ)** is defined to be $\nu = \ker \gamma$. If $\nu = 0$, then we say (L,γ) of **generic characteristic**, otherwise, we say (L,γ) is of **(finite) characteristic ν**

(2) (L,γ) A-field, a Drinfeld A-module $/L$ is a ring monomorphism $\phi : A \to \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,L}) = L\{\tau\}$, $\tau(z) = z^q$

$$a \longmapsto \phi_a = a_0 + a_1\tau + \cdots + a_n\tau^n.$$

s.t. $(*)$ $a_0 =: \partial\phi_a = \gamma(a)$ $\forall a \in A$ and $\phi(A) \not\subseteq L$ (ϕ is not const)

Thus, $\forall$ L-alg R $\mathbb{G}_a(R) = R$ is endowed with an A-module by ϕ.

$$a \in A,\ r \in R \qquad a \underset{\phi}{\times} r = \phi_a(r)$$

$\because$ A : commutative $\phi_{a_1}\cdot\phi_{a_2} = \phi_{a_2}\phi_{a_1}$, $\phi_a(z)$: q-poly in z

$$\phi_a \circ \phi = \phi \circ \phi_a.$$

(3) ϕ_1, ϕ_2 Drinfeld A-modules $/L$. A morphism from ϕ_1 to ϕ_2 is a homomorphism $f : \mathbb{G}_a \to \mathbb{G}_a$ over L s.t $\phi_{2,a}\circ f = f\circ\phi_{1,a}$ $\forall a \in A$

$\mathrm{Hom}(\phi_1,\phi_2)$ = the group of morphisms
$f : \phi_1 \to \phi_2$ over L.

$$\begin{array}{ccc} \mathbb{G}_a & \xrightarrow{f} & \mathbb{G}_a \\ \downarrow{\scriptstyle \phi_{1,a}} & & \downarrow{\scriptstyle \phi_{2,a}} \\ \mathbb{G}_a & \xrightarrow{f} & \mathbb{G}_a \end{array}$$

$$f \in \mathrm{Hom}(\phi_1,\phi_2)$$

$$a\cdot f = \phi_{2,a}\circ f$$

Then $\phi_2 \circ (\phi_{2,a}\circ f) = \phi_{2,a}\circ\phi_2\circ f = (\phi_{2,a}\circ f)\circ\phi_1 \Rightarrow \mathrm{Hom}(\phi_1,\phi_2)$: A-module

$$\left(\begin{array}{ccc} R & \xrightarrow{f} & R \\ \phi_1 & & \phi_2 \end{array} , \quad \begin{array}{c} a \underset{\phi_1}{*} r \\ \parallel \\ \phi_{1,a}(r) \end{array} \quad a \underset{\phi_2}{*} r = \phi_{2,a}(r) \quad (a\cdot f)(r) = a \underset{\phi_2}{*} f(r) = \phi_{2,a}(f(r)) \right)$$

One can show that $\mathrm{Hom}(\phi_1,\phi_2)$ is a projective A-module of finite rank.

Ranks and heights :

Notation $f = \sum a_i \tau^i = a_0 + \cdots + a_n \tau^n \in k\{\tau\}$, $a_n \neq 0$ $k = \mathbb{F}_q$-alg

$a_0 = $ const term $=: c.t.(f)$

$a_n = $ leading term $=: l.t.(f)$

$\deg(f) = \max\{i : a_i \neq 0\} = n.$

$w(f) = \min\{i : a_i \neq 0\} = \mathrm{ord}_\tau(f)$

If k is a field. $\#\{z \in \bar{k},\ f(z) = 0\} = q^{n - w(f)}$

Prop 3 : ϕ: Drinfeld A-module / an A-field L.

(1) There exists an $r \in \mathbb{Z}_{>0}$ s.t. $\deg(\phi_a) = r \cdot \deg(a)$ $\forall\ a \in A \setminus \{0\}$

(2) Suppose L has finite char v. Then exists an $h \in \mathbb{Z}_{>0}$

s.t. $w(\phi_a) = h \cdot \deg(v) \cdot v(a)$, $\forall\ a \in A \setminus \{a\}$.

Def The integers r and h in Prop 3 are called the rank and height of ϕ, respectively.

$$\left(1 \leq h \leq r, \quad \begin{cases} h = 1. & \phi : \text{ordinary} \\ h = r & \phi : \text{supersingular} \end{cases} \right)$$

I-torsion submodules :

Def : ϕ : Drinfeld A-module / L (A-field). $\forall a \in A$. define

$$\phi[a] := \ker \phi_a \subseteq \mathbb{G}_a, \text{ subgp scheme of } \mathbb{G}_a.$$

which is stable under A-action and called the a-torsion submodule of ϕ.

$\forall$ L-alg R, $\phi[a](R) = \{ x \in R : \phi_a(x) = 0 \}$.

$\because$ $\phi_a \phi_b = \phi_b \phi_a$, $\phi_a(\phi_b(x)) = \phi_b(\phi_a(x)) = 0 \Rightarrow \phi_b(x) \in \phi[a](R)$

$\Rightarrow \phi[a](R) \subseteq R$: A-module, in fact $A/(a)$-module.

Similarly, for any ideal $I \subseteq A$, define

$$\phi[I] := \bigcap_{a \in I} \phi[a],$$

called the I-torsion submodule of ϕ. $\phi[I]$: A/I-module scheme.

Note : $\because$ A: Dedekind domain. $I = (a_1, a_2)$ for $a_1, a_2 \in I$

$\therefore$ $\phi[I] = \phi[a_1] \cap \phi[a_2]$

$\deg(\phi_a) = r \cdot \deg(a)$

$\deg(\phi_a(z)) = \underline{q}^{r \cdot \deg(a)}$

Explictly $\phi[a] = \operatorname{Spec} L[z]/(\phi_a(z))$.

finite subgp scheme of order ($\dim_L$) $\underline{q}^{r \cdot \deg(a)}$

Similarly. $\phi[I] = \operatorname{Spec} L[z]/(\phi_a(z))_{a \in I} = \operatorname{Spec} L[z]/(\phi_{a_1}(z), \phi_{a_2}(z))$

$\because$ $L[z]$: PID, $\exists!$ monic poly $f_I(z)$ st $(f_I(z)) = (\phi_{a_1}(z), \phi_{a_2}(z))$

Suppose $\deg f_I(z) = q^d$, then $\phi[I]$ has order $\underline{q}^d$.

One can show $d = r \cdot \deg(I)$

Note $\because$ roots of $f_I(z)$ form an $\mathbb{F}_q$-linear subspace in $\bar{L}$

$\therefore$ $f_I(z)$: q-polynomial in z, $f_I \in L\{\tau\}$

Lemma 4 : R : Dedekind domain with $K = \mathrm{Frac}(R)$, M : R-module.

(1) Let $I \neq (0) \subseteq R$ an ideal and write $I = P_1^{e_1} \cdots P_r^{e_r}$ into the product of prime ideals P_i. Then $M[I] := \{ m \in M : I \cdot x = 0 \} = \bigoplus_{i=1}^{r} M[P_i^{e_i}]$.

(2) If M is A-divisible (i.e. $\forall a \neq \in R$, $a : M \to M$ surjective) then $\forall$ non-zero prime ideal $p \subseteq A$ and $e \geq 1 \in \mathbb{N}$.

$M[p^e]$ is a free A/p^e - module of rank indep of e. Moreover, if the common rank r is finite, then $M[p^\infty] := \bigcup_{e \geq 1} M[p^e]$

$\simeq (K_p / \hat{R}_p)^r$, where K_p and $\hat{R}_p$ the completions of K & R at p, respectively.

Pf. (1) Chinese Remainder Theorem.

(2) For each non-zero prime p of R, replacing R by R_p,

we may assume that R : DVR, $p = (\pi)$, π: uniformizer.

$\Rightarrow M[\pi]$: $R/\pi R$ - vector space. (say of dim r, r maybe ∞).

Choose a free R-module N of rank $\dim M[\pi]$ and

an isom $\alpha_1 : \pi^{-1} N / N \simeq M[\pi]$ of R/π - modules.

Idea : construct a compatible system of isoms

$$\alpha_e : \pi^{-e} N / N \simeq M[\pi^e] \text{ of } R/\pi^e\text{-modules}$$

by induction.

Consider the following diagram

x_β

$$\begin{tikzcd}
0 \arrow[r] & \pi^{-1}N/N \arrow[r] \arrow[d, "\alpha_1"] & \pi^{-(e+1)}N/N \arrow[r, "\pi"] \arrow[d, dashed, "\alpha_{e+1}"] \arrow[dr] & \pi^{-e}N/N \arrow[r] \arrow[d, "\alpha_e"] & 0 \\
0 \arrow[r] & M[\pi] \arrow[r] & M[\pi^{e+1}] \arrow[r, "\pi"] & M[\pi^e] \arrow[r] & 0
\end{tikzcd}$$

$m_\beta \longmapsto \alpha_e(\pi x_\beta)$

Let $\{x_\beta\}_{\beta \in B}$ be an R-basis of N.

$$\alpha_e(\pi x_\beta) \in M[\pi^e],$$

$\because$ M : π-divisible

$\therefore$ $\exists\, m_\beta \in M[\pi^{e+1}]$ st $\pi \cdot m_\beta = \alpha_e(\pi \cdot x_\beta)$

define $\alpha_{e+1}(x_\beta) = m_\beta$ and yields an R-linear homo

$$\alpha_{e+1} : \pi^{-(e+1)} N/N \longrightarrow M[\pi^{e+1}].$$

$\because$ α_1, α_e : Isom. $\therefore$ α_{e+1} : Isom (the five lemma).

Finally $M[p^\infty] = \bigcup_{e \geq 1} M[p^e] \overset{(\alpha_e)}{\simeq} \bigcup_{e \geq 1} \pi^{-e} N/N = (K_p / \hat{R}_p)^r$.

$r = \operatorname{rank}_R N$.