Introduction to Drinfeld Modules
and Function Field Arithmetic

Matthew Papanikolas

Texas A&M University

Clemson University

Algebra & Discrete Mathematics Seminar
April 16, 2009

Outline

Arithmetic objects from characteristic 0

- The multiplicative group and $\exp(z)$
- Elliptic curves and elliptic functions
- Abelian extensions of imaginary quadratic fields

The multiplicative group

We have the usual exact sequence of abelian groups

$$0 \to 2\pi i\mathbb{Z} \to \mathbb{C} \stackrel{\exp}{\to} \mathbb{C}^\times \to 0,$$

where

$$\exp(z) = \sum_{i=0}^{\infty} \frac{z^i}{i!} \in \mathbb{Q}[[z]].$$

The multiplicative group

We have the usual exact sequence of abelian groups

$$0 \to 2\pi i\mathbb{Z} \to \mathbb{C} \xrightarrow{\exp} \mathbb{C}^\times \to 0,$$

where

$$\exp(z) = \sum_{i=0}^{\infty} \frac{z^i}{i!} \in \mathbb{Q}[[z]].$$

For any $n \in \mathbb{Z}$,

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\exp} & \mathbb{C}^\times \\ {\scriptstyle z \mapsto nz}\downarrow & & \downarrow{\scriptstyle x \mapsto x^n} \\ \mathbb{C} & \xrightarrow{\exp} & \mathbb{C}^\times \end{array}$$

which is simply a restatement of the functional equation

$$\exp(nz) = \exp(z)^n.$$

Roots of unity

Torsion in the multiplicative group

The *n*-th roots of unity are defined by

$$\mu_n := \{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\} = \{\exp(2\pi i a/n) \mid a \in \mathbb{Z}\}$$

Roots of unity

Torsion in the multiplicative group

The n-th roots of unity are defined by

$$\mu_n := \left\{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\right\} = \left\{\exp\left(2\pi ia/n\right) \mid a \in \mathbb{Z}\right\}$$

Explicit class field theory for $\mathbb{Q}$:

- $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

Roots of unity

Torsion in the multiplicative group

The n-th roots of unity are defined by

$$\mu_n := \{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\} = \{\exp(2\pi ia/n) \mid a \in \mathbb{Z}\}$$

Explicit class field theory for $\mathbb{Q}$:

- $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
- **Kronecker-Weber Theorem:** Every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\mu_n)$ for some n.

Roots of unity

Torsion in the multiplicative group

The n-th roots of unity are defined by

$$\mu_n := \{\zeta \in \mathbb{C}^\times \mid \zeta^n = 1\} = \{\exp(2\pi i a/n) \mid a \in \mathbb{Z}\}$$

Explicit class field theory for $\mathbb{Q}$:

- $\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.
- **Kronecker-Weber Theorem:** Every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\mu_n)$ for some n.
- If ℓ is a prime $\ell \nmid n$, then the Artin automorphism $\sigma_\ell \in \mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$ acts by

$$\sigma_\ell(\zeta) = \zeta^\ell.$$

Elliptic curves over $\mathbb{C}$

- Smooth projective algebraic curve of genus 1.

$$E : y^2 = 4x^3 + ax + b, \quad a, b \in \mathbb{C}$$

- $E(\mathbb{C})$ has the structure of an abelian group through the usual chord-tangent construction.
- The identity element of $E(\mathbb{C})$ is the point O, which lies on the line at infinity in $\mathbb{P}^2$.

Weierstrass uniformization

There exist $\omega_1, \omega_2 \in \mathbb{C}$, linearly independent over $\mathbb{R}$, so that if we consider the lattice

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2,$$

then the *Weierstrass $\wp$-function* is defined by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

The function $\wp(z)$ has double poles at each point in Λ and no other poles.

We obtain an exact sequence of abelian groups,

$$0 \to \Lambda \to \mathbb{C} \stackrel{\exp_E}{\to} E(\mathbb{C}) \to 0,$$

where

$$\exp_E(z) = (\wp(z), \wp'(z)).$$

We obtain an exact sequence of abelian groups,

$$0 \to \Lambda \to \mathbb{C} \stackrel{\exp_E}{\to} E(\mathbb{C}) \to 0,$$

where

$$\exp_E(z) = (\wp(z), \wp'(z)).$$

Moreover, we have a commutative diagram

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\exp_E} & E(\mathbb{C}) \\ {\scriptstyle z \mapsto nz} \downarrow & & \downarrow {\scriptstyle P \mapsto [n]P} \\ \mathbb{C} & \xrightarrow{\exp_E} & E(\mathbb{C}) \end{array}$$

where $[n]P$ is the n-th multiple of a point P on the elliptic curve E.

Periods of E

How do we find ω_1 and ω_2?

An elliptic curve E,

$$E : y^2 = 4x^3 + ax + b, \quad a, b \in \mathbb{C},$$

has the geometric structure of a torus in $\mathbb{P}^2(\mathbb{C})$. Let

$$\gamma_1, \gamma_2 \in H_1(E, \mathbb{Z})$$

be generators of the homology of E.

Periods of E

How do we find ω_1 and ω_2?

An elliptic curve E,

$$E : y^2 = 4x^3 + ax + b, \quad a, b \in \mathbb{C},$$

has the geometric structure of a torus in $\mathbb{P}^2(\mathbb{C})$. Let

$$\gamma_1, \gamma_2 \in H_1(E, \mathbb{Z})$$

be generators of the homology of E.

Then we can choose

$$\omega_1 = \int_{\gamma_1} \frac{dx}{\sqrt{4x^3 + ax + b}}, \qquad \omega_2 = \int_{\gamma_2} \frac{dx}{\sqrt{4x^3 + ax + b}}.$$

Multiplication by n on E

- Note that if $P = (x, y)$ is a point on E, then $[n]P$ has the form

$$[n]P = \Big(f_n(x, y), g_n(x, y)\Big),$$

where f_n and g_n are rational functions in x, y, and the coefficients of the defining polynomial for E.

Multiplication by n on E

- Note that if $P = (x, y)$ is a point on E, then $[n]P$ has the form

$$[n]P = \Big(f_n(x,y), g_n(x,y) \Big),$$

where f_n and g_n are rational functions in x, y, and the coefficients of the defining polynomial for E.

- For example,

$$[2]P = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2}, \right.$$
$$\left. \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8y^3} \right)$$

Multiplication by n on E

- Note that if $P = (x, y)$ is a point on E, then $[n]P$ has the form

$$[n]P = \Big(f_n(x, y), g_n(x, y)\Big),$$

where f_n and g_n are rational functions in x, y, and the coefficients of the defining polynomial for E.

- For example,

$$[2]P = \left(\frac{x^4 - 2ax^2 - 8bx + a^2}{4y^2}, \right.$$
$$\left. \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{8y^3}\right)$$

- In particular, if x, y, a, b are all in a field K, then $[n]P$ has coordinates in K.

Torsion points on elliptic curves

The group $E[n]$

- Suppose E is defined over a field $K \subseteq \mathbb{C}$. For a field L with $K \subseteq L \subseteq \mathbb{C}$, we set

$$E(L) := \{(x, y) \in E \mid x, y \in L\}.$$

  Then $E(L)$ is a subgroup of E.

Torsion points on elliptic curves

The group $E[n]$

- Suppose E is defined over a field $K \subseteq \mathbb{C}$. For a field L with $K \subseteq L \subseteq \mathbb{C}$, we set

$$E(L) := \{(x, y) \in E \mid x, y \in L\}.$$

  Then $E(L)$ is a subgroup of E.
- For each $n \in \mathbb{Z}$, we define the torsion subgroup

$$E[n] := \{P \in E(\mathbb{C}) \mid [n]P = O\} \subseteq E(\mathbb{C}).$$

  Then as an abstract group,

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Division fields

- Since $E[n]$ is a finite group, the field $K(E[n])$ satisfies

$$[K(E[n]) : K] < \infty.$$

Division fields

- Since $E[n]$ is a finite group, the field $K(E[n])$ satisfies

$$[K(E[n]):K] < \infty.$$

- Moreover, $K(E[n])/K$ is Galois: for $\sigma \in \mathrm{Gal}(\overline{K}/K)$,

$$[n](\sigma P) = \sigma([n]P) \Rightarrow \sigma(E[n]) \subseteq E[n].$$

Division fields

- Since $E[n]$ is a finite group, the field $K(E[n])$ satisfies
$$[K(E[n]) : K] < \infty.$$

- Moreover, $K(E[n])/K$ is Galois: for $\sigma \in \mathrm{Gal}(\overline{K}/K)$,
$$[n](\sigma P) = \sigma([n]P) \Rightarrow \sigma(E[n]) \subseteq E[n].$$

- Because $E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, we find that
$$\mathrm{Gal}(K(E[n])/K) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}).$$

Abelian extensions of imaginary quadratic fields

Elliptic curves with complex multiplication (CM)

- Consider the example

$$E : y^2 = x^3 - x.$$

- Then for $i = \sqrt{-1}$, the morphism $[i](x, y) := (-x, iy)$ induces and embedding

$$\mathbb{Z}[i] \subseteq \mathrm{End}(E).$$

  In this case we say E has CM by $\mathbb{Z}[i]$.

Abelian extensions of imaginary quadratic fields

Elliptic curves with complex multiplication (CM)

- Consider the example

$$E : y^2 = x^3 - x.$$

- Then for $i = \sqrt{-1}$, the morphism $[i](x, y) := (-x, iy)$ induces and embedding

$$\mathbb{Z}[i] \subseteq \mathrm{End}(E).$$

  In this case we say E has CM by $\mathbb{Z}[i]$.
- Let $K = \mathbb{Q}(i)$ and $n \geq 3$.

Abelian extensions of imaginary quadratic fields

Elliptic curves with complex multiplication (CM)

- Consider the example

$$E : y^2 = x^3 - x.$$

- Then for $i = \sqrt{-1}$, the morphism $[i](x, y) := (-x, iy)$ induces and embedding

$$\mathbb{Z}[i] \subseteq \mathrm{End}(E).$$

  In this case we say E has CM by $\mathbb{Z}[i]$.
- Let $K = \mathbb{Q}(i)$ and $n \geq 3$. Then
  - $\mathrm{Gal}(K(E[n])/K)$ is abelian (and explicitly given depending on the primes dividing n),
  - Every abelian extension of K is contained in $K(E[n])$ for some n.
  - For a prime $\ell \nmid 2n$ and $P \in E[n]$, we have

$$\sigma_\ell(P) = [\ell]P.$$

General imaginary quadratic fields

Let $K = \mathbb{Q}(\sqrt{-d})$ for some $d \geq 1$. Let h_K be the class number of K.

- There are exactly h_K isomorphism classes (over $\mathbb{C}$) of elliptic curves with CM by $\mathcal{O}_K$.
- For any such curve $E : y^2 = x^3 + ax + b$, set

$$j_E = \frac{6912a^3}{4a^3 + 27b^2}.$$

- The field $H := K(j_E)$ is the Hilbert class field of K; that is, H is the maximal abelian unramified extension of K.
- Morever, as long as $j_E \neq 0$ or 1728,

$$K^{ab} = \bigcup_n K\left(j_E, x(E[n])\right) = \bigcup_n H\left(x(E[n])\right).$$

Function fields and Drinfeld modules

- Function fields
- Drinfeld modules
  - The Carlitz module
  - Drinfeld modules of rank 1 and abelian extensions
  - Drineld modules of higher rank

Function fields

Let p be a fixed prime; q a fixed power of p.

$A := \mathbb{F}_q[\theta]$	$\longleftrightarrow$	$\mathbb{Z}$
$k := \mathbb{F}_q(\theta)$	$\longleftrightarrow$	$\mathbb{Q}$
$\overline{k}$	$\longleftrightarrow$	$\overline{\mathbb{Q}}$
$k_\infty := \mathbb{F}_q((1/\theta))$	$\longleftrightarrow$	$\mathbb{R}$
$\mathbb{C}_\infty := \widehat{\overline{k_\infty}}$	$\longleftrightarrow$	$\mathbb{C}$
$\lvert f\rvert_\infty = q^{\deg f}$	$\longleftrightarrow$	$\lvert \cdot \rvert$

Twisted polynomials

- Let $\tau : \mathbb{C}_\infty \to \mathbb{C}_\infty$ be the q-th power Frobenius map: $\tau(x) = x^q$.
- For a subfield $\mathbb{F}_q \subseteq K \subseteq \mathbb{C}_\infty$, the ring of *twisted polynomials* over K is

$$K[\tau] = \text{polynomials in } \tau \text{ with coefficients in } K,$$

subject to the conditions

$$\tau c = c^q \tau, \quad \forall\, c \in K.$$

Twisted polynomials

- Let $\tau : \mathbb{C}_\infty \to \mathbb{C}_\infty$ be the q-th power Frobenius map: $\tau(x) = x^q$.
- For a subfield $\mathbb{F}_q \subseteq K \subseteq \mathbb{C}_\infty$, the ring of *twisted polynomials* over K is

$$K[\tau] = \text{polynomials in } \tau \text{ with coefficients in } K,$$

subject to the conditions

$$\tau c = c^q \tau, \quad \forall\, c \in K.$$

- In this way,

$$K[\tau] \cong \{\mathbb{F}_q\text{-linear endomorphisms of } K^+\}.$$

For $x \in K$ and $\phi = a_0 + a_1\tau + \cdots a_r\tau^r \in K[\tau]$, we write

$$\phi(x) := a_0 x + a_1 x^q + \cdots + a_r x^{q^r}.$$

Functions on algebraic curves

- Let X be a smooth projective curve over $\mathbb{F}_q$, with function field $K = \mathbb{F}_q(X)$.
- Suppose we have fixed maps,

$$X \to \mathbb{P}^1 \quad \Leftrightarrow \quad \mathbb{F}_q(\theta) \hookrightarrow K.$$

Functions on algebraic curves

- Let X be a smooth projective curve over $\mathbb{F}_q$, with function field $K = \mathbb{F}_q(X)$.
- Suppose we have fixed maps,

$$X \to \mathbb{P}^1 \quad \Leftrightarrow \quad \mathbb{F}_q(\theta) \hookrightarrow K.$$

- Fix a point ∞ on X that sits above the infinite point on $\mathbb{P}^1$.
- Throughout the following we set

$$A := \{f \in K \mid f \text{ is regular on } X \text{ away from } \infty\}.$$

- So if $X = \mathbb{P}^1$, then $A = \mathbb{F}_q[\theta]$.

Drinfeld modules

Function field analogues of $\mathbb{G}_m$ and elliptic curves

Fix a curve $X/\mathbb{F}_q$ and ring $A \subseteq K = \mathbb{F}_q(X)$ as above.

Definition

A *Drinfeld A-module* is an $\mathbb{F}_q$-algebra homomorphism,

$$\rho : A \to \mathbb{C}_\infty[\tau],$$

such that

$$\rho_f = f + a_1\tau + \cdots a_s\tau^s, \quad \forall f \in A.$$

Drinfeld modules

Function field analogues of $\mathbb{G}_m$ and elliptic curves

Fix a curve $X/\mathbb{F}_q$ and ring $A \subseteq K = \mathbb{F}_q(X)$ as above.

Definition

A *Drinfeld A-module* is an $\mathbb{F}_q$-algebra homomorphism,

$$\rho : A \to \mathbb{C}_\infty[\tau],$$

such that

$$\rho_f = f + a_1\tau + \cdots a_s\tau^s, \quad \forall f \in A.$$

- ρ makes $\mathbb{C}_\infty$ into an A-module in the following way:

$$f * x := \rho_f(x), \quad \forall f \in A, x \in \mathbb{C}_\infty.$$

- If $a_1, \ldots, a_r \in K \subseteq \mathbb{C}_\infty$ for all $f \in A$, we say ρ is *defined over K*.
- $s = r\deg(f)$, where r is called the *rank* of ρ.

The Carlitz module

The analogue of $\mathbb{G}_m$

- We define a Drinfeld $\mathbb{F}_q[\theta]$-module $C : \mathbb{F}_q[t] \to \mathbb{C}_\infty[\tau]$ by

$$C_\theta := \theta + \tau.$$

Thus, for any $x \in \mathbb{C}_\infty$,

$$C_\theta(x) = \theta x + x^q.$$

The Carlitz module

The analogue of $\mathbb{G}_m$

- We define a Drinfeld $\mathbb{F}_q[\theta]$-module $C : \mathbb{F}_q[t] \to \mathbb{C}_\infty[\tau]$ by

$$C_\theta := \theta + \tau.$$

Thus, for any $x \in \mathbb{C}_\infty$,

$$C_\theta(x) = \theta x + x^q.$$

- And for example,

$$C_{\theta^2} = C_\theta C_\theta = (\theta + \tau)(\theta + \tau) = \theta^2 + (\theta + \theta^q)\tau + \tau^2,$$
$$C_{\theta^2}(x) = \theta^2 x + (\theta + \theta^q)x^q + x^{q^2}.$$

Carlitz exponential

We set

$$\exp_C(z) = z + \sum_{i=1}^{\infty} \frac{z^{q^i}}{(\theta^{q^i} - \theta)(\theta^{q^i} - \theta^q) \cdots (\theta^{q^i} - \theta^{q^{i-1}})}.$$

- $\exp_C : \mathbb{C}_\infty \to \mathbb{C}_\infty$ is entire, surjective, and $\mathbb{F}_q$-linear.
- Functional equation:

$$\exp_C(\theta z) = \theta \exp_C(z) + \exp_C(z)^q,$$
$$\exp_C(f(\theta)z) = C_f(\exp_C(z)), \quad \forall f(t) \in \mathbb{F}_q[t].$$

Carlitz uniformization and the Carlitz period

We have a commutative diagram of $\mathbb{F}_q[t]$-modules,

$$\begin{array}{ccc}
\mathbb{C}_\infty & \xrightarrow{\exp_C} & \mathbb{C}_\infty \\
{\scriptstyle z \mapsto \theta z}\downarrow & & \downarrow{\scriptstyle x \mapsto \theta x + x^q} \\
\mathbb{C}_\infty & \xrightarrow{\exp_C} & \mathbb{C}_\infty
\end{array}$$

Carlitz uniformization and the Carlitz period

We have a commutative diagram of $\mathbb{F}_q[t]$-modules,

$$\begin{array}{ccc} \mathbb{C}_\infty & \xrightarrow{\exp_C} & \mathbb{C}_\infty \\ {\scriptstyle z\mapsto\theta z}\downarrow & & \downarrow{\scriptstyle x\mapsto\theta x+x^q} \\ \mathbb{C}_\infty & \xrightarrow{\exp_C} & \mathbb{C}_\infty \end{array}$$

The kernel of $\exp_C(z)$ is

$$\ker(\exp_C(z)) = \mathbb{F}_q[\theta]\widetilde{\pi},$$

where

$$\widetilde{\pi} = \theta \sqrt[q-1]{-\theta} \prod_{i=1}^{\infty} \left(1 - \theta^{1-q^i}\right)^{-1}.$$

Torsion points on the Carlitz module

Recall $k = \mathbb{F}_q(\theta)$, $A = \mathbb{F}_q(\theta)$.

- For $f \in \mathbb{F}_q[\theta]$, we set

$$C[f] = \{x \in \mathbb{C}_\infty \mid C_f(x) = 0\},$$
$$= f\text{-torsion submodule of } C.$$

Torsion points on the Carlitz module

Recall $k = \mathbb{F}_q(\theta)$, $A = \mathbb{F}_q(\theta)$.

- For $f \in \mathbb{F}_q[\theta]$, we set

$$\begin{aligned} C[f] &= \{x \in \mathbb{C}_\infty \mid C_f(x) = 0\}, \\ &= f\text{-torsion submodule of } C. \end{aligned}$$

- For example,

$$\begin{aligned} C[\theta] &= \{x \in \mathbb{C}_\infty \mid \theta x + x^q = 0\} \\ &= \{\exp_C\left(\frac{a}{\theta}\right) \mid a \in \mathbb{F}_q\} \\ &= \{\zeta \sqrt[q-1]{-\theta} \mid \zeta \in \mathbb{F}_q\}. \end{aligned}$$

- Preliminary observations:
  - $C[\theta] \cong A/\theta$ as an A-module;
  - $k(\mathbb{C}_\infty[\theta])/k$ is an abelian extension.

Explicit class field theory for $\mathbb{F}_q(\theta)$

- For every $f \in A$,

$$\mathrm{Gal}(k(C[f])/k) \cong (A/f)^\times.$$

- Indeed, given $\ell \in A$ irreducible with $\ell \nmid f$, the Frobenius automorphism $\sigma_\ell \in \mathrm{Gal}(k(C[f])/k)$ acts by

$$\sigma_\ell(\zeta) = C_\ell(\zeta), \quad \zeta \in C[f].$$

- Moreover, every abelian extension of k that is unramified away from ∞ is contained in $k(C[f])$ for some $f \in A$.

Drinfeld A-modules for general A

- Do they always exist? In general, defining a ring homomorphism $A \to S$ to some target ring S is non-trivial.

Drinfeld A-modules for general A

- Do they always exist? In general, defining a ring homomorphism $A \to S$ to some target ring S is non-trivial.
- Yes, in fact for any A, there are Drinfeld A-modules of every possible rank.
- Example (Thakur): Let $A = \mathbb{F}_3[\theta, \eta]/(\eta^2 - \theta^3 + \theta + 1)$. Then there is a rank 1 Drinfeld A-module,

$$\rho : A \to \mathbb{C}_\infty[\tau],$$

with

$$\rho_\theta = \theta + \eta(\theta^3 - \theta)\tau + \tau^2,$$
$$\rho_\eta = \eta + \eta(\eta^3 - \eta)\tau + (\eta^9 + \eta^3 + \eta)\tau^2 + \tau^3.$$

In fact ρ is defined over the fraction field of A.

Rank 1 Drinfeld A-modules

Let A be given, K its fraction field. For simplicity, assume the point ∞ has degree 1.

- Let h be the class number of A. Let H be the Hilbert class field of A (maximal abelian unramified extension).
- Then there exist h isomorphism classes of rank 1 Drinfeld A-modules. Moreover, representatives $\rho^1, \ldots, \rho^h$ for these classes can be chosen (uniquely) so that each is defined over H:

$$\rho^i : A \to H[\tau].$$

(Uniqueness arises from normalizing the leading coefficients to be specific constants.)

Explicit class field theory for K

Fix such a rank 1 Drinfeld A-modules, $\rho : A \to H[\tau]$.

- For any ideal $\mathfrak{f} \subseteq A$, the extension $H(\rho[\mathfrak{f}])/H$ is abelian and
$$\mathrm{Gal}(H(\rho[\mathfrak{f}])/H) \cong (A/\mathfrak{f})^{\times}.$$
- Moreover, $H(\rho[\mathfrak{f}])/K$ is abelian. (Recall that $\mathrm{Gal}(H/K)$ is isomorphic to the class group of A, so we can pin down the total Galois group precisely.)
- As in previous cases, the Artin automorphisms act via the ρ-action on the torsion points:
$$\sigma_\ell(\zeta) = \rho_\ell(\zeta), \quad \zeta \in \rho[\mathfrak{f}], \ell \nmid \mathfrak{f}.$$

Drinfeld modules of arbitrary rank

- Suppose $\rho : A \to \mathbb{C}_\infty[\tau]$ is a rank r Drinfeld A-module.
- Then there is an unique, entire, $\mathbb{F}_q$-linear function

$$\exp_\rho : \mathbb{C}_\infty \to \mathbb{C}_\infty,$$

so that

$$\exp_\rho(fz) = \rho_f(\exp_\rho(z)), \quad \forall f \in A.$$

Periods of Drinfeld modules

- Furthermore, there are $\omega_1, \ldots, \omega_r \in \mathbb{C}_\infty$ and ideals $I_1, \ldots, I_r \subseteq A$, so that
$$\ker(\exp_\rho(z)) = I_1\omega_1 + \cdots + I_r\omega_r =: \Lambda,$$
where Λ is a discrete A-submodule of $\mathbb{C}_\infty$ of projective rank r.

Periods of Drinfeld modules

- Furthermore, there are $\omega_1, \ldots, \omega_r \in \mathbb{C}_\infty$ and ideals $I_1, \ldots, I_r \subseteq A$, so that
$$\ker(\exp_\rho(z)) = I_1\omega_1 + \cdots + I_r\omega_r =: \Lambda,$$
where Λ is a discrete A-submodule of $\mathbb{C}_\infty$ of projective rank r.
- **Chicken vs. Egg:**
$$\exp_\rho(z) = z \prod_{0 \neq \omega \in \Lambda} \left(1 - \frac{z}{\omega}\right).$$
- Again we have a uniformizing exact sequence of $\mathbb{F}_q[t]$-modules
$$0 \to \Lambda \to \mathbb{C}_\infty \stackrel{\exp_\rho}{\to} \mathbb{C}_\infty \to 0.$$
- How do we find the periods?

Torsion points on higher rank modules

- In reality, $\exp_\rho$ is the unique power series that makes the following diagram commute for $f \in A$:

$$\begin{array}{ccc} \mathbb{C}_\infty & \xrightarrow{\exp_\rho} & \mathbb{C}_\infty \\ {\scriptstyle z \mapsto fz} \downarrow & & \downarrow {\scriptstyle x \mapsto \rho_f(x)} \\ \mathbb{C}_\infty & \xrightarrow{\exp_\rho} & \mathbb{C}_\infty \end{array}$$

- Furthermore, the f-torsion submodule is isomorphic to r copies of A/f, which leads to a Galois representation

$$\mathrm{Gal}(L^{sep}/L) \to \mathrm{GL}_r(A/f),$$

  where L is a field of definition for ρ.
- One can develop a theory of "ℓ-adic" Galois representations (see Pink, Taguchi, Tamagawa, et al.)