A computation on Drinfeld modules

Simon Fraser University

Number Theory & Algebraic Geometry Seminar

Antoine Leudière, University of Calgary

May 29th, 2025

Introduction

Ore polynomials

Drinfeld modules

Computing a group action

Kronecker-Weber theorem

Every abelian number field lies in a cyclotomic field $\mathbb{Q}_n$.

$\mathbb{Q}_n$ is generated by the n-th roots of unity.

Alternative construction

Consider the $\mathbb{Z}$-module

$$\begin{array}{ccc} \mathbb{Z} \times \overline{\mathbb{Q}}^* & \to & \overline{\mathbb{Q}}^* \\ (n, z) & \mapsto & z^n \end{array}$$

The n-th roots of unity are the n-torsion of this $\mathbb{Z}$-module.

Kronecker-Weber theorem

Every abelian number field lies in a cyclotomic field $\mathbb{Q}_n$.

$\mathbb{Q}_n$ is generated by the n-th roots of unity.

Alternative construction

Consider the $\mathbb{Z}$-module

$$\begin{array}{rcl} \mathbb{Z} \times \overline{\mathbb{Q}}^* & \to & \overline{\mathbb{Q}}^* \\ (n, z) & \mapsto & z^n \end{array}$$

The n-th roots of unity are the n-torsion of this $\mathbb{Z}$-module.

Class Field Theory

Class Field Theory

Given a number field $K/\mathbb{Q}$, what can I say about the abelian extensions of K, using only objects defined in K?

Very important object

Hilbert class field (maximal unramified abelian extension).

Some explicit results:

- Kronecker-Weber.
- The case of quadratic imaginary number fields ($\mathbb{Q}(\sqrt{-d})$, where $d < 0$).

The Hilbert class field of $\mathbb{Q}(\sqrt{-d})$ is generated by isomorphism classes of *elliptic curves* with complex multiplication in $\mathbb{Q}(\sqrt{-d})$.

Class Field Theory

Class Field Theory

Given a number field $K/\mathbb{Q}$, what can I say about the abelian extensions of K, using only objects defined in K?

Very important object

Hilbert class field (maximal unramified abelian extension).

Some explicit results:

- Kronecker-Weber.
- The case of quadratic imaginary number fields ($\mathbb{Q}(\sqrt{-d})$, where $d < 0$).

The Hilbert class field of $\mathbb{Q}(\sqrt{-d})$ is generated by isomorphism classes of *elliptic curves* with complex multiplication in $\mathbb{Q}(\sqrt{-d})$.

Class Field Theory

Class Field Theory

Given a number field $K/\mathbb{Q}$, what can I say about the abelian extensions of K, using only objects defined in K?

Very important object

Hilbert class field (maximal unramified abelian extension).

Some explicit results:

- Kronecker-Weber.
- The case of quadratic imaginary number fields ($\mathbb{Q}(\sqrt{-d})$, where $d < 0$).

The Hilbert class field of $\mathbb{Q}(\sqrt{-d})$ is generated by isomorphism classes of *elliptic curves* with complex multiplication in $\mathbb{Q}(\sqrt{-d})$.

Class Field Theory

Class Field Theory

Given a number field $K/\mathbb{Q}$, what can I say about the abelian extensions of K, using only objects defined in K?

Very important object

Hilbert class field (maximal unramified abelian extension).

Some explicit results:

- Kronecker-Weber.
- The case of quadratic imaginary number fields ($\mathbb{Q}(\sqrt{-d})$, where $d < 0$).

The Hilbert class field of $\mathbb{Q}(\sqrt{-d})$ is generated by isomorphism classes of *elliptic curves* with complex multiplication in $\mathbb{Q}(\sqrt{-d})$.

An alternative framework

Common point between the results:

- Number fields (characteristic 0).
- $\mathbb{Z}$-modules.

Can we change these?

Zero characteristic	Positive characteristic
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((1/T))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Roots of unity	Drinfeld modules
Elliptic curves	Drinfeld modules

An alternative framework

Common point between the results:

- Number fields (characteristic 0).
- $\mathbb{Z}$-modules.

Can we change these?

Zero characteristic	Positive characteristic
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((1/T))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Roots of unity	Drinfeld modules
Elliptic curves	Drinfeld modules

An alternative framework

Common point between the results:

- Number fields (characteristic 0).
- $\mathbb{Z}$-modules.

Can we change these?

Zero characteristic	**Positive characteristic**
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((1/T))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Roots of unity	Drinfeld modules
Elliptic curves	Drinfeld modules

An alternative framework

Common point between the results:

- Number fields (characteristic 0).
- $\mathbb{Z}$-modules.

Can we change these?

Zero characteristic	**Positive characteristic**
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((1/T))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Roots of unity	Drinfeld modules
Elliptic curves	Drinfeld modules

An alternative framework

Common point between the results:

- Number fields (characteristic 0).
- $\mathbb{Z}$-modules.

Can we change these?

Zero characteristic	**Positive characteristic**
$\mathbb{Z}$	$\mathbb{F}_q[T]$
$\mathbb{Q}$	$\mathbb{F}_q(T)$
Number fields (finite ext.)	Function fields (finite ext.)
$\mathbb{R}$	$\mathbb{R}_\infty = \mathbb{F}_q((1/T))$
$\mathbb{C}$	$\mathbb{C}_\infty =$ completion of $\overline{\mathbb{R}_\infty}$
Roots of unity	Drinfeld modules
Elliptic curves	Drinfeld modules

Advantages of function fields

- Geometrical interpretation.
- Non-Archimedean valuations.
- Faster algorithms (polynomial derivation and factorization).
- Some unconditional results (GRH).

Broader questions

Elliptic curves	*vs*	Drinfeld modules
Integers	*vs*	Polynomials
Number fields	*vs*	Function fields
Zero characteristic	*vs*	Positive characteristic

Ore polynomials $K\{\tau\}$

Consider an extension $K/\mathbb{F}_q$ and the Frobenius endomorphisms

$$\begin{array}{rccc} \tau^n : & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Finite K-linear combinations of τ^n': ring $K\{\tau\}$ for addition and composition.

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^{n} x_i \tau^i, n \in \mathbb{Z}_{\geqslant 0}, x_i \in K\}$.
- Notion of τ-degree.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.

Ore polynomials $K\{\tau\}$

Consider an extension $K/\mathbb{F}_q$ and the Frobenius endomorphisms

$$\begin{array}{rccc} \tau^n : & \overline{K} & \to & \overline{K} \\ & x & \mapsto & x^{q^n}. \end{array}$$

Finite K-linear combinations of τ^n': ring $K\{\tau\}$ for addition and composition.

Properties

- Representation as polynomials: $K\{\tau\} = \{\sum_{i=0}^{n} x_i \tau^i, n \in \mathbb{Z}_{\geqslant 0}, x_i \in K\}$.
- Notion of τ-degree.
- Noncommutative: for $\lambda \in K$, $\tau^n \lambda = \lambda^{q^n} \tau^n$.

Euclidean divisions

$K\{\tau\}$ is left-euclidean

For all $A(\tau), B(\tau) \in K\{\tau\}$, there exist $Q(\tau), R(\tau) \in K\{\tau\}$ such that:

$$\begin{cases} A(\tau) = Q(\tau)B(\tau) + R(\tau), \\ \deg_\tau(R(\tau)) < \deg_\tau(B(\tau)). \end{cases}$$

Kernels and Ore polynomials

A bijection

$$\left\{ \begin{array}{c} \text{Ore polynomials } f \in K\{\tau\} \\ \text{with constant term } 1 \end{array} \right\} \rightarrow \left\{ \begin{array}{c} \text{finite dimensional } \mathbb{F}_q\text{-linear subspaces} \\ V \subset K^{\mathrm{sep}} \text{ stable by } \operatorname{Gal}(K^{\mathrm{sep}}/K) \end{array} \right\}$$
$$f \mapsto \ker f.$$

$$\begin{array}{rcl} f_1 & \longleftrightarrow & V_1 \\ f_2 & \longleftrightarrow & V_2 \\ \operatorname{rgcd}(f_1, f_2) & \longleftrightarrow & V_1 \cap V_2 \end{array}$$

Introduction

Ore polynomials

Drinfeld modules

Computing a group action

Representing Drinfeld modules

Drinfeld modules ϕ and their morphisms are represented as Ore polynomials.

Representation

For $a \in \mathbb{F}_q[T]$, the endomorphism of multiplication by a is represented by an Ore polynomial $\phi_a \in K\{\tau\}$.

From now on, K is finite with $[K : \mathbb{F}_q] = d$.

Frobenius endomorphism

One extra endomorphism: $\mathrm{Frob} = \tau^d \in K\{\tau\}$.

Representing Drinfeld modules

Drinfeld modules ϕ and their morphisms are represented as Ore polynomials.

Representation

For $a \in \mathbb{F}_q[T]$, the endomorphism of multiplication by a is represented by an Ore polynomial $\phi_a \in K\{\tau\}$.

From now on, K is finite with $[K : \mathbb{F}_q] = d$.

Frobenius endomorphism

One extra endomorphism: $\mathrm{Frob} = \tau^d \in K\{\tau\}$.

The module of a Drinfeld module

A Drinfeld module is *not* a module!

Let ϕ be a Drinfeld module.

We have an $\mathbb{F}_q[T]$-module law on $\overline{K}$:

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, x) & \mapsto & \phi_a(x). \end{array}$$

Drinfeld module analogue of the $\mathbb{Z}$-module coming from an elliptic curve!

The notion of *point* is ambiguous.

The module of a Drinfeld module

A Drinfeld module is *not* a module!

Let ϕ be a Drinfeld module.

We have an $\mathbb{F}_q[T]$-module law on $\overline{K}$:

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, x) & \mapsto & \phi_a(x). \end{array}$$

Drinfeld module analogue of the $\mathbb{Z}$-module coming from an elliptic curve!

The notion of *point* is ambiguous.

The module of a Drinfeld module

A Drinfeld module is *not* a module!

Let ϕ be a Drinfeld module.

We have an $\mathbb{F}_q[T]$-module law on $\overline{K}$:

$$\begin{array}{rcl} \mathbb{F}_q[T] \times \overline{K} & \to & \overline{K} \\ (a, x) & \mapsto & \phi_a(x). \end{array}$$

Drinfeld module analogue of the $\mathbb{Z}$-module coming from an elliptic curve!

The notion of *point* is ambiguous.

Introduction

Ore polynomials

Drinfeld modules

Computing a group action

Joint-work with P.-J. Spaenlehauer.

Computing a group action from the class field theory of imaginary hyperelliptic function fields.

Journal of symbolic computation, 2024.
`https://doi.org/10.1016/j.jsc.2024.102311`.

Cryptography with group actions

Fix and assume:

- A free-transitive action of an abelian group G on a set X.
- For all $g \in G$, computing g from x and $g \cdot x$ is hard.

$$\text{Alice} \quad \overset{g_A \cdot x}{\longrightarrow} \quad \text{Bob}$$

$$\text{Alice} \quad \underset{g_B \cdot x}{\longleftarrow} \quad \text{Bob}$$

Hard Homogeneous Spaces (Couveignes, 1997)

Alice and Bob can use $(g_A g_B) \cdot x = g_A \cdot (g_B \cdot x) = g_B \cdot (g_A \cdot x)$ as their secret key.

Cryptography with group actions

Fix and assume:

- A free-transitive action of an abelian group G on a set X.
- For all $g \in G$, computing g from x and $g \cdot x$ is hard.

$$\text{Alice} \quad \underset{g_B \cdot x}{\overset{g_A \cdot x}{\rightleftarrows}} \quad \text{Bob}$$

Hard Homogeneous Spaces (Couveignes, 1997)

Alice and Bob can use $(g_A g_B) \cdot x = g_A \cdot (g_B \cdot x) = g_B \cdot (g_A \cdot x)$ as their secret key.

Cryptography with group actions

Fix and assume:

- A free-transitive action of an abelian group G on a set X.
- For all $g \in G$, computing g from x and $g \cdot x$ is hard.

$$\text{Alice} \quad \begin{array}{c} \xrightarrow{\qquad g_A \cdot x \qquad} \\ \xleftarrow[\qquad g_B \cdot x \qquad]{} \end{array} \quad \text{Bob}$$

Hard Homogeneous Spaces (Couveignes, 1997)

Alice and Bob can use $(g_A g_B) \cdot x = g_A \cdot (g_B \cdot x) = g_B \cdot (g_A \cdot x)$ as their secret key.

Isogeny-based cryptography

- Quadratic imaginary number field $\mathbb{Q}(\sqrt{-d})$.
- Its ring of integers $\mathcal{O}$, and the class group $\mathrm{Cl}(\mathcal{O})$.
- The set $X_{\mathcal{O}}$ isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}$.

Fix an ideal $\mathfrak{a} \subset \mathcal{O}$ and an elliptic curve E. There is a curve $E_{\mathfrak{a}}$ and morphism $E \to E_{\mathfrak{a}}$ with kernel

$$\bigcap_{f \in \mathfrak{a}} \ker f.$$

We define

$$\overline{\mathfrak{a}} * \overline{E} = \overline{E_{\mathfrak{a}}}.$$

Free and transitive group action of $\mathrm{Cl}(\mathcal{O})$ on $X_{\mathcal{O}}$.

Too slow for cryptography (de Feo-Kieffer-Smith, 2018)!

Isogeny-based cryptography

- Quadratic imaginary number field $\mathbb{Q}(\sqrt{-d})$.
- Its ring of integers $\mathcal{O}$, and the class group $\mathrm{Cl}(\mathcal{O})$.
- The set $X_{\mathcal{O}}$ isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}$.

Fix an ideal $\mathfrak{a} \subset \mathcal{O}$ and an elliptic curve E. There is a curve $E_{\mathfrak{a}}$ and morphism $E \to E_{\mathfrak{a}}$ with kernel

$$\bigcap_{f \in \mathfrak{a}} \ker f.$$

We define

$$\overline{\mathfrak{a}} * \overline{E} = \overline{E_{\mathfrak{a}}}.$$

Free and transitive group action of $\mathrm{Cl}(\mathcal{O})$ on $X_{\mathcal{O}}$.

Too slow for cryptography (de Feo-Kieffer-Smith, 2018)!

Isogeny-based cryptography

- Quadratic imaginary number field $\mathbb{Q}(\sqrt{-d})$.
- Its ring of integers $\mathcal{O}$, and the class group $\mathrm{Cl}(\mathcal{O})$.
- The set $X_{\mathcal{O}}$ isomorphism classes of elliptic curves with endomorphism ring $\mathcal{O}$.

Fix an ideal $\mathfrak{a} \subset \mathcal{O}$ and an elliptic curve E. There is a curve $E_{\mathfrak{a}}$ and morphism $E \to E_{\mathfrak{a}}$ with kernel

$$\bigcap_{f \in \mathfrak{a}} \ker f.$$

We define

$$\overline{\mathfrak{a}} * \overline{E} = \overline{E_{\mathfrak{a}}}.$$

Free and transitive group action of $\mathrm{Cl}(\mathcal{O})$ on $X_{\mathcal{O}}$.

Too slow for cryptography (de Feo-Kieffer-Smith, 2018)!

The Drinfeld module analogue

Same action for Drinfeld modules!

- Order $\mathcal{O}$ in an imaginary quadratic number field.
- Elliptic curves E such that $\mathrm{End}(E) \simeq \mathcal{O}$.
- Ideal $\mathfrak{a}$ of $\mathrm{End}(E)$.
- Compute $\bigcap_{f \in \mathfrak{a}} \ker f$.

- Order $\mathcal{O}$ in an imaginary quadratic function field.
- Drinfeld modules ϕ such that $\mathrm{End}(\phi) \simeq \mathcal{O}$.
- Ideal $\mathfrak{a}$ of $\mathrm{End}(\phi)$.
- Compute $\bigcap_{f \in \mathfrak{a}} \ker f$.

The hyperelliptic case

Imaginary hyperelliptic curve $\mathcal{H}$ defined by $\chi \in \mathbb{F}_q[T][X]$, and its *coordinate ring*

$$\mathbb{F}_q[\mathcal{H}] = \mathbb{F}_q[T][X]/(\chi).$$

Mumford coordinates

Elements of $\mathrm{Cl}(\mathbb{F}_q[\mathcal{H}])$ are represented by couples $(u, v) \in \mathbb{F}_q[T]^2$ with:

$$(u, v) \longleftrightarrow \left(\overline{u(T)}, \overline{X - v(T)}\right)$$

For a Drinfeld module ϕ such that $\mathrm{End}(\phi) = \mathbb{F}_q[\mathcal{H}]$, we have an isomorphism

$$\begin{array}{rcl} \mathbb{F}_q[\mathcal{H}] & \to & \mathrm{End}(\phi) \\ P(T, X) & \mapsto & P(\phi_T, \mathrm{Frob}). \end{array}$$

The hyperelliptic case

Imaginary hyperelliptic curve $\mathcal{H}$ defined by $\chi \in \mathbb{F}_q[T][X]$, and its *coordinate ring*

$$\mathbb{F}_q[\mathcal{H}] = \mathbb{F}_q[T][X]/(\chi).$$

Mumford coordinates

Elements of $\mathrm{Cl}(\mathbb{F}_q[\mathcal{H}])$ are represented by couples $(u, v) \in \mathbb{F}_q[T]^2$ with:

$$(u, v) \longleftrightarrow \left(\overline{u(T)}, \overline{X - v(T)}\right)$$

For a Drinfeld module ϕ such that $\mathrm{End}(\phi) = \mathbb{F}_q[\mathcal{H}]$, we have an isomorphism

$$\begin{array}{rcl} \mathbb{F}_q[\mathcal{H}] & \to & \mathrm{End}(\phi) \\ P(T, X) & \mapsto & P(\phi_T, \mathrm{Frob}). \end{array}$$

Practical computation

We rely on:

- Mumford coordinates.
- The correspondence between kernels and Ore polynomials.

Computing the action essentially goes down to computing

$$\operatorname{rgcd}\left(\phi_u, \mathrm{Frob} - \phi_v\right).$$

Computation time on cryptographic sizes goes from ~ 10 min. to 400 ms.
Highly insecure though! (Wesolowski)

Practical computation

We rely on:

- Mumford coordinates.
- The correspondence between kernels and Ore polynomials.

Computing the action essentially goes down to computing

$$\mathrm{rgcd}\left(\phi_u, \mathrm{Frob} - \phi_v\right).$$

Computation time on cryptographic sizes goes from ~ 10 min. to 400 ms.
Highly insecure though! (Wesolowski)

Conclusive remarks

Applications of Drinfeld modules

- Geometric Langlands program, Class Field Theory of function fields, GRH for function fields.
- State of the art polynomial factorization (Doliskani-Narayanan-Schost, 2018).

Tools for Drinfeld modules

- Inspiration from elliptic curves.
- Function fields arithmetics.
- Ore polynomial arithmetics.
- Anderson motives.

Conclusive remarks

Applications of Drinfeld modules

- Geometric Langlands program, Class Field Theory of function fields, GRH for function fields.
- State of the art polynomial factorization (Doliskani-Narayanan-Schost, 2018).

Tools for Drinfeld modules

- Inspiration from elliptic curves.
- Function fields arithmetics.
- Ore polynomial arithmetics.
- Anderson motives.