

Computations in positive and zero characteristic

Antoine Leudière, for Alberta Number Theory Days XVI

University of Calgary

May 3rd, 2025

Introduction

Drinfeld modules

Computing a group action

Introduction

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

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

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 ?

Some explicit results:

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

The *Hilbert class field* (maximal unramified abelian extension) of an **imaginary quadratic number field** $\mathbb{Q}(\sqrt{-d})$ is generated by: the j -invariants of **elliptic curves** with complex multiplication in $\mathbb{Q}(\sqrt{-d})$.

Looking for an alternative framework

Common point between these 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}	$\mathbb{R}_\infty = \mathbb{F}_q((\frac{1}{T}))$
\mathbb{C}	$\mathbb{C}_\infty = \text{completion of } \overline{\mathbb{R}_\infty}$
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).

Introduction

Drinfeld modules

Computing a group action

Ore polynomials $K\{\tau\}$

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

$$\begin{aligned}\tau^n : K &\rightarrow K \\ x &\mapsto x^{q^n}.\end{aligned}$$

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

Properties

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

Kernels and Ore polynomials

$K\{\tau\}$ is left-euclidean: $\forall A(\tau), B(\tau) \in K\{\tau\}, \exists Q(\tau), R(\tau) \in K\{\tau\}$ such that:

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

A bijection

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

$$\begin{aligned} V_1 &\longleftrightarrow f_1 \\ V_2 &\longleftrightarrow f_2 \\ V_1 \cap V_2 &\longleftrightarrow \text{rgcd}(f_1, f_2) \end{aligned}$$

Representing Drinfeld modules

Drinfeld modules ϕ and their morphisms are represented in terms of $K\{\tau\}$.

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: $\text{Frob} = \tau^d \in K\{\tau\}$.

Introduction

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>.

The case of elliptic curves

- Quadratic imaginary number field $\mathbb{Q}(\sqrt{-d})$.
- Its ring of integers \mathcal{O} .
- The class group $\text{Cl}(\mathcal{O})$ of \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 $E \rightarrow E_{\mathfrak{a}}$ with kernel

$$\bigcap_{f \in \mathfrak{a}} \text{Ker}(f).$$

We define

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

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

Relevance of the problem

Theoretical applications

Class field theory.

Practical applications

Isogeny-based cryptography (Couveignes, 2006; Rostovtsev-Stolbunov, 2006).

Very slow computation! See de Feo-Kieffer-Smith, 2018.

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

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

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

$$\begin{aligned} \mathbb{F}_q[\mathcal{H}] &\rightarrow \text{End}(\phi) \\ P(\textcolor{red}{T}, \textcolor{red}{X}) &\mapsto P(\phi_{\textcolor{red}{T}}, \textcolor{red}{\text{Frob}}). \end{aligned}$$

Practical computation

We rely on:

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

Computing the action essentially goes down to computing

$$\text{rgcd}(\phi_u, \text{Frob} - \phi_v).$$

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.