2-group Belyi maps

Michael Musty

July 9, 2019

Dartmouth College

Acknowledgements

- Committee: Dave, Tom, Carl, and John
- Family: Mary, Jim, Matt, and Nicole
- Others: Sam, Jeroen, Edgar, Florian, and Richard

Outline

Motivation

Galois representations

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Galois representations

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.
Let $J := \mathrm{Jac}(X)$ be the **Jacobian variety** of X. J is an abelian variety of dimension g.

Galois representations

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.
Let $J := \mathrm{Jac}(X)$ be the **Jacobian variety** of X. J is an abelian variety of dimension g.
G_K acts on the ℓ-torsion points $J[\ell](K^{\mathrm{al}}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X.

Galois representations

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Let $J := \mathrm{Jac}(X)$ be the **Jacobian variety** of X. J is an abelian variety of dimension g.

G_K acts on the ℓ-torsion points $J[\ell](K^{\mathrm{al}}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X.

This action determines a **mod-ℓ Galois representation**

$$\rho\colon G_K \to \mathrm{Aut}(J[\ell]) \cong \mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

Galois representations

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.

Let $J := \mathrm{Jac}(X)$ be the **Jacobian variety** of X. J is an abelian variety of dimension g.

G_K acts on the ℓ-torsion points $J[\ell](K^{\mathrm{al}}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X.

This action determines a **mod-ℓ Galois representation**

$$\rho\colon G_K \to \mathrm{Aut}(J[\ell]) \cong \mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

The geometry of X and the arithmetic of ρ are inimately related.

Galois representations

Let X be an irreducible, smooth projective algebraic curve of genus $g \geq 1$ over a number field K. Let $G_K := \mathrm{Gal}(K^{\mathrm{al}} \mid K)$ be the absolute Galois group of K and let $\ell \in \mathbb{Z}$ be prime.
Let $J := \mathrm{Jac}(X)$ be the **Jacobian variety** of X. J is an abelian variety of dimension g.
G_K acts on the ℓ-torsion points $J[\ell](K^{\mathrm{al}}) \cong (\mathbb{Z}/\ell\mathbb{Z})^{2g}$ of X.
This action determines a **mod-ℓ Galois representation**

$$\rho\colon G_K \to \mathrm{Aut}(J[\ell]) \cong \mathrm{GL}_{2g}(\mathbb{Z}/\ell\mathbb{Z}).$$

The geometry of X and the arithmetic of ρ are inimately related.
For example, if X has good reduction at a prime $\mathfrak{p}$ above $p \neq \ell$, then $\mathfrak{p}$ will be unramified in the ℓ-**torsion field** $K(J[\ell])$.

Belyi's theorem

A **Belyi map** is a morphism $\phi\colon X \to \mathbb{P}^1$ of smooth projective algebraic curves over $\mathbb{C}$ that is unramified outside of $\{0, 1, \infty\}$.

Belyi's theorem

A **Belyi map** is a morphism $\phi\colon X \to \mathbb{P}^1$ of smooth projective algebraic curves over $\mathbb{C}$ that is unramified outside of $\{0, 1, \infty\}$.

Theorem (Belyi 1979)

An algebraic curve (smooth projective) over $\mathbb{C}$ can be defined over a number field if and only if X admits a Belyi map.

Some definitions

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

Some definitions

Let $\phi \colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

Some definitions

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X).$$

Some definitions

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X).$$

ϕ is **geometrically Galois** if $K^{\mathrm{al}}(X)$ is a Galois extension.

Some definitions

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X).$$

ϕ is **geometrically Galois** if $K^{\mathrm{al}}(X)$ is a Galois extension.

The **monodromy group of** ϕ, $\mathrm{Mon}(\phi)$, is the image of the map

$$\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \star) \to S_d$$

obtained by path lifting.

Some definitions

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X).$$

ϕ is **geometrically Galois** if $K^{\mathrm{al}}(X)$ is a Galois extension.

The **monodromy group of** ϕ, $\mathrm{Mon}(\phi)$, is the image of the map

$$\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \star) \to S_d$$

obtained by path lifting.

When ϕ is Galois we can identify $\mathrm{Mon}(\phi)$ with $\mathrm{Gal}(K^{\mathrm{al}}(X) \mid K^{\mathrm{al}}(\mathbb{P}^1))$.

Some definitions

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map defined over K.

The **genus** of ϕ is the genus of the curve X.

The **degree** of ϕ is the degree of the field extension

$$K(\mathbb{P}^1) \hookrightarrow K(X).$$

ϕ is **geometrically Galois** if $K^{\mathrm{al}}(X)$ is a Galois extension.

The **monodromy group of** ϕ, $\mathrm{Mon}(\phi)$, is the image of the map

$$\pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}, \star) \to S_d$$

obtained by path lifting.

When ϕ is Galois we can identify $\mathrm{Mon}(\phi)$ with $\mathrm{Gal}(K^{\mathrm{al}}(X) \mid K^{\mathrm{al}}(\mathbb{P}^1))$.

We can now state Beckmann's theorem.

Beckmann's theorem

Theorem (Beckmann 1989)

Let $\phi\colon X \to \mathbb{P}^1$ *be a Galois Belyi map with monodromy group* G*.*
Let p *be a prime not dividing* $\#G$*.*

Theorem (Beckmann 1989)

Let $\phi\colon X \to \mathbb{P}^1$ be a Galois Belyi map with monodromy group G. Let p be a prime not dividing $\#G$. Then there exists a number field M satisfying the following properties.

Beckmann's theorem

Theorem (Beckmann 1989)

Let $\phi\colon X \to \mathbb{P}^1$ be a Galois Belyi map with monodromy group G.
Let p be a prime not dividing $\#G$.
Then there exists a number field M satisfying the following properties.

- *p is unramified in M*
- *ϕ is defined over M*
- *X is defined over M*
- *X has good reduction at all primes $\mathfrak{p}$ of M above p*

Why $p = 2$?

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

Why $p = 2$?

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

$p \geq 11$: existence (Serre), explicit (Edixhoven, Mascot)

$p = 7$: existence (Dieulefait)

$p = 5$: existence (Dembélé, Greenberg, Voight), explicit (Roberts)

$p = 3$: existence (Dembélé, Greenberg, Voight)

$p = 2$: existence (Dembélé)

Why $p = 2$?

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

$p \geq 11$: existence (Serre), explicit (Edixhoven, Mascot)

$p = 7$: existence (Dieulefait)

$p = 5$: existence (Dembélé, Greenberg, Voight), explicit (Roberts)

$p = 3$: existence (Dembélé, Greenberg, Voight)

$p = 2$: existence (Dembélé)

The hope is that an explicit nonsolvable field ramified only at 2 can be obtained as $K(\mathrm{Jac}(X)[2])$ where X is the domain of a Galois Belyi map with monodromy group a 2-group.

Why $p = 2$?

Conjecture (Gross 1998)

For every prime p, there exists a nonsolvable Galois number field ramified only at p.

$p \geq 11$: existence (Serre), explicit (Edixhoven, Mascot)

$p = 7$: existence (Dieulefait)

$p = 5$: existence (Dembélé, Greenberg, Voight), explicit (Roberts)

$p = 3$: existence (Dembélé, Greenberg, Voight)

$p = 2$: existence (Dembélé)

The hope is that an explicit nonsolvable field ramified only at 2 can be obtained as $K(\mathrm{Jac}(X)[2])$ where X is the domain of a Galois Belyi map with monodromy group a 2-group.
We call these Belyi maps 2-**group Belyi maps**.

Main results

Motivated by the applications of 2-group Belyi maps to arithmetic geometry, we now state the main results.

Main results

Motivated by the applications of 2-group Belyi maps to arithmetic geometry, we now state the main results.

- implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps

Main results

Motivated by the applications of 2-group Belyi maps to arithmetic geometry, we now state the main results.

- implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps
- implementation of an algorithm to compute equations for 2-group Belyi maps over finite fields

Main results

Motivated by the applications of 2-group Belyi maps to arithmetic geometry, we now state the main results.

- implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps
- implementation of an algorithm to compute equations for 2-group Belyi maps over finite fields
- implementation of a *method* to compute equations for 2-group Belyi maps over number fields

Main results

Motivated by the applications of 2-group Belyi maps to arithmetic geometry, we now state the main results.

- implementation of an algorithm to enumerate isomorphism classes of 2-group Belyi maps
- implementation of an algorithm to compute equations for 2-group Belyi maps over finite fields
- implementation of a *method* to compute equations for 2-group Belyi maps over number fields
- computational and theoretical evidence supporting a conjecture that every 2-group Belyi map is defined over an abelian extension of the rationals

Background

Isomorphism of Belyi maps

Let $\phi\colon X \to \mathbb{P}^1$ and $\phi'\colon X' \to \mathbb{P}^1$ be Belyi maps of degree d.

Isomorphism of Belyi maps

Let $\phi\colon X \to \mathbb{P}^1$ and $\phi'\colon X' \to \mathbb{P}^1$ be Belyi maps of degree d. ϕ and ϕ' are **isomorphic** (respectively **lax isomorphic**) if the diagrams

$$\begin{tikzcd} X \arrow[rr, "\sim"] \arrow[dr, "\phi"'] & & X' \arrow[dl, "\phi'"] \\ & \mathbb{P}^1 & \end{tikzcd}, \text{ respectively } \begin{tikzcd} X \arrow[r, "\sim"] \arrow[d, "\phi"'] & X' \arrow[d, "\phi'"] \\ \mathbb{P}^1 \arrow[r, "\sim", "\beta"'] & \mathbb{P}^1 \end{tikzcd}$$

commute where $\beta(\{0,1,\infty\}) = \{0,1,\infty\}$.

Permutation Triples

A **transitive permutation triple of degree** d is a triple

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$$

such that

- $\sigma_\infty \sigma_1 \sigma_0 = 1$
- σ generates a transitive subgroup of S_d

Permutation Triples

A **transitive permutation triple of degree** d is a triple

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3$$

such that

- $\sigma_\infty \sigma_1 \sigma_0 = 1$
- σ generates a transitive subgroup of S_d

The set of degree d Belyi maps up to isomorphism is in bijection with the set of degree d transitive permutation triples up to **simultaneous conjugation** and the group $\langle \sigma \rangle$ is the monodromy group of ϕ.

Passports

A **passport** $\mathcal{P}$ consists of the data (g, G, λ) where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a triple of partitions of d.

Passports

A **passport** $\mathcal{P}$ consists of the data (g, G, λ) where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a triple of partitions of d.

The **passport of a Belyi map** $\phi : X \to \mathbb{P}^1$ is $(g(X), \mathrm{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$ with $g(X)$ the genus of X, $\mathrm{Mon}(\phi)$ the monodromy group of ϕ, and the partitions specified by ramification.

Passports

A **passport** $\mathcal{P}$ consists of the data (g, G, λ) where $g \geq 0$ is an integer, $G \leq S_d$ is a transitive subgroup, and $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ is a triple of partitions of d.

The **passport of a Belyi map** $\phi : X \to \mathbb{P}^1$ is $(g(X), \mathrm{Mon}(\phi), (\lambda_0, \lambda_1, \lambda_\infty))$ with $g(X)$ the genus of X, $\mathrm{Mon}(\phi)$ the monodromy group of ϕ, and the partitions specified by ramification.

The **passport of a permutation triple** σ is $(g(\sigma), \langle\sigma\rangle, \lambda(\sigma))$ where

$$g(\sigma) = 1 - d + (e(\sigma_0) - e(\sigma_1) - e(\sigma_\infty))/2$$

with

$$e(\tau) = d - \#\text{cycles of } \tau,$$

and $\lambda(\sigma)$ is specified by cycle structures.

Function fields

Let $\phi\colon X \to \mathbb{P}^1$ be a Belyi map

Fields of moduli and fields of definition

The Galois setting

Computing permutation triples

General idea

Outline of algorithm

Results

Computing equations

A motivating example

Algorithm in characteristic $p \geq 3$

Implementation in characteristic zero

Results

A refined conjecture

Refined passports

A refined conjecture

Examples

Notation

`4T1-4,1,4-g0`

An

4T1-4,1,4-g0

Backup slides