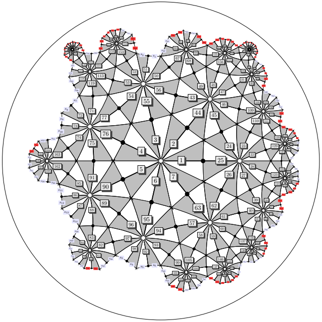
Computing a Database of Belyĭ Maps



Michael Musty (Dartmouth College)
GSCAGT at Temple University
June 4, 2017

Acknowledgements

This is joint work with:

- Mike Klug
- Sam Schiavone
- Jeroen Sijsling
- John Voight

Example 😇

Find $\varphi \in \mathbb{Q}[x]$ of degree 3 such that $\varphi(x)$ and $\varphi(x) - 1$ have a double root.

Example 😇

Find $\varphi \in \mathbb{Q}[x]$ of degree 3 such that $\varphi(x)$ and $\varphi(x) - 1$ have a double root.

$$\varphi(x) = ax^2(x-1), \qquad \varphi(x) - 1 = a(x-b)^2(x-c)$$

implies

$$ax^3 - ax^2 - 1 = ax^3 - a(2b+c)x^2 + ab(b+2c)x - ab^2c$$

Example 😇

Find $\varphi \in \mathbb{Q}[x]$ of degree 3 such that $\varphi(x)$ and $\varphi(x) - 1$ have a double root.

$$\varphi(x) = ax^2(x-1), \qquad \varphi(x) - 1 = a(x-b)^2(x-c)$$

implies

$$ax^3 - ax^2 - 1 = ax^3 - a(2b+c)x^2 + ab(b+2c)x - ab^2c$$

which yields the solution $a, b, c = -27/4, 2/3, -1/3$.

Example 😇

Find $\varphi \in \mathbb{Q}[x]$ of degree 3 such that $\varphi(x)$ and $\varphi(x) - 1$ have a double root.

$$\varphi(x) = ax^2(x-1), \qquad \varphi(x) - 1 = a(x-b)^2(x-c)$$

implies

$$ax^3 - ax^2 - 1 = ax^3 - a(2b+c)x^2 + ab(b+2c)x - ab^2c$$

which yields the solution $a, b, c = -27/4, 2/3, -1/3$.
After a linear change of variables ($x \leftarrow -2x/3$) we get

$$\begin{aligned}\varphi(x) &= 2x^3 + 3x^2 = x^2(2x+3)\\ \varphi(x) - 1 &= 2x^3 + 3x^2 - 1 = (2x-1)(x+1)^2.\end{aligned}$$

Example 😇

Find $\varphi \in \mathbb{Q}[x]$ of degree 3 such that $\varphi(x)$ and $\varphi(x) - 1$ have a double root.

$$\varphi(x) = ax^2(x-1), \qquad \varphi(x) - 1 = a(x-b)^2(x-c)$$

implies

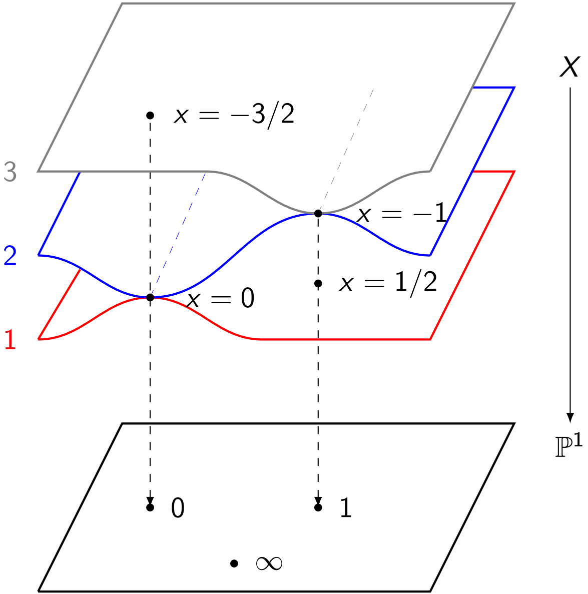
$$ax^3 - ax^2 - 1 = ax^3 - a(2b+c)x^2 + ab(b+2c)x - ab^2c$$

which yields the solution $a, b, c = -27/4, 2/3, -1/3$.
After a linear change of variables ($x \leftarrow -2x/3$) we get

$$\begin{gathered} \varphi(x) = 2x^3 + 3x^2 = x^2(2x+3) \\ \varphi(x) - 1 = 2x^3 + 3x^2 - 1 = (2x-1)(x+1)^2. \end{gathered}$$

We can view φ as a branched (ramified) covering map of Riemann surfaces...

Example 😇



$$\varphi(x) = \underbrace{2x^3 + 3x^2}_{z}$$

Riemann's Existence Theorem

Let X be a compact connected Riemann surface.

Riemann's Existence Theorem

Let X be a compact connected Riemann surface.

Theorem (Riemann Existence)

There exists a non-constant meromorphic function on X *that represents* X *as a branched cover of* $\mathbb{P}^1$ *(with branch locus a finite subset of* $\mathbb{P}^1$*) as in the previous slide.*

Riemann's Existence Theorem

Let X be a compact connected Riemann surface.

Theorem (Riemann Existence)

There exists a non-constant meromorphic function on X *that represents* X *as a branched cover of* $\mathbb{P}^1$ *(with branch locus a finite subset of* $\mathbb{P}^1$*) as in the previous slide.*

A consequence of this theorem is the equivalence between Riemann surfaces and algebraic curves.

Belyĭ's Theorem

We say X is **defined over** a subfield L of $\mathbb{C}$ if there exists $f(z,w) \in L[z,w]$ such that the field of meromorphic functions on X is isomorphic to

$$\frac{\mathbb{C}(z)[w]}{(f(z,w))}.$$

Belyĭ's Theorem

We say X is **defined over** a subfield L of $\mathbb{C}$ if there exists $f(z,w) \in L[z,w]$ such that the field of meromorphic functions on X is isomorphic to

$$\frac{\mathbb{C}(z)[w]}{(f(z,w))}.$$

For example, $\mathbb{P}^1$ is defined over $\mathbb{Q}$:

Belyĭ's Theorem

We say X is **defined over** a subfield L of $\mathbb{C}$ if there exists $f(z,w) \in L[z,w]$ such that the field of meromorphic functions on X is isomorphic to

$$\frac{\mathbb{C}(z)[w]}{(f(z,w))}.$$

For example, $\mathbb{P}^1$ is defined over $\mathbb{Q}$:
Let $f(z,w) = w \in \mathbb{Q}[z,w]$. Then

$$\frac{\mathbb{C}(z)[w]}{(w)} = \mathbb{C}(z)$$

which is the meromorphic functions on $\mathbb{P}^1$.

Belyĭ's Theorem

We say X is **defined over** a subfield L of $\mathbb{C}$ if there exists $f(z,w) \in L[z,w]$ such that the field of meromorphic functions on X is isomorphic to

$$\frac{\mathbb{C}(z)[w]}{(f(z,w))}.$$

For example, $\mathbb{P}^1$ is defined over $\mathbb{Q}$:
Let $f(z,w) = w \in \mathbb{Q}[z,w]$. Then

$$\frac{\mathbb{C}(z)[w]}{(w)} = \mathbb{C}(z)$$

which is the meromorphic functions on $\mathbb{P}^1$.

Question: How do we know when X is defined over $\overline{\mathbb{Q}}$?

Belyĭ's Theorem

Theorem (G.V. Belyĭ 1979)

A curve X over $\mathbb{C}$ *can be defined over* $\overline{\mathbb{Q}}$ *if and only if there exists a branched covering of compact connected Riemann surfaces* $\varphi : X \to \mathbb{P}^1$ *unramified (unbranched) above* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$*.*

Belyĭ's Theorem

Theorem (G.V. Belyĭ 1979)

A curve X *over* $\mathbb{C}$ *can be defined over* $\overline{\mathbb{Q}}$ *if and only if there exists a branched covering of compact connected Riemann surfaces* $\varphi : X \to \mathbb{P}^1$ *unramified (unbranched) above* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$*.*

Such a map is called a **Belyĭ map**.

Belyĭ's Theorem

Theorem (G.V. Belyĭ 1979)

A curve X *over* $\mathbb{C}$ *can be defined over* $\overline{\mathbb{Q}}$ *if and only if there exists a branched covering of compact connected Riemann surfaces* $\varphi : X \to \mathbb{P}^1$ *unramified (unbranched) above* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Such a map is called a **Belyĭ map**. The **degree** of a Belyĭ map is the number of sheets in the covering.

Belyĭ’s Theorem

Theorem (G.V. Belyĭ 1979)

A curve X *over* $\mathbb{C}$ *can be defined over* $\overline{\mathbb{Q}}$ *if and only if there exists a branched covering of compact connected Riemann surfaces* $\varphi : X \to \mathbb{P}^1$ *unramified (unbranched) above* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$.

Such a map is called a **Belyĭ map**. The **degree** of a Belyĭ map is the number of sheets in the covering.

In the 1980s, Grothendieck spoke of Belyĭ’s result saying: *Never, without a doubt, was such a deep and disconcerting result proved in so few lines!*

Belyĭ's Theorem

Theorem (G.V. Belyĭ 1979)

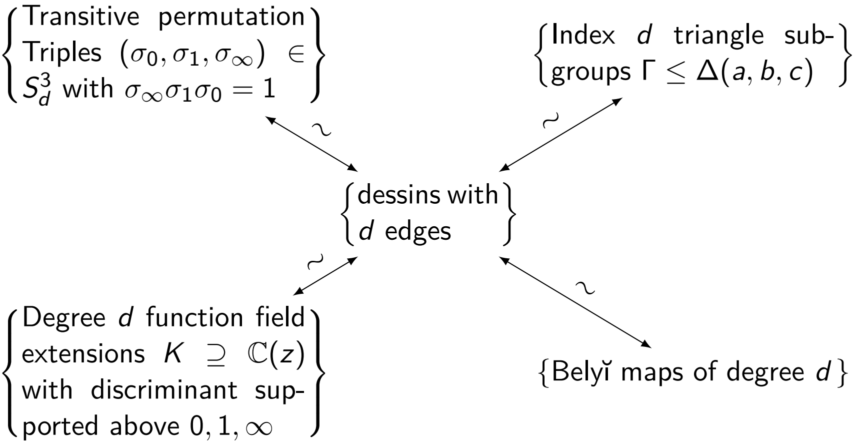
A curve X *over* $\mathbb{C}$ *can be defined over* $\overline{\mathbb{Q}}$ *if and only if there exists a branched covering of compact connected Riemann surfaces* $\varphi : X \to \mathbb{P}^1$ *unramified (unbranched) above* $\mathbb{P}^1 \setminus \{0, 1, \infty\}$*.*

Such a map is called a **Belyĭ map**. The **degree** of a Belyĭ map is the number of sheets in the covering.

In the 1980s, Grothendieck spoke of Belyĭ's result saying: *Never, without a doubt, was such a deep and disconcerting result proved in so few lines!*

There is a zoo of objects in bijection with the set of Belyĭ maps.

A Zoo of Bijections



$\left\{\text{Transitive permutation Triples } (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3 \text{ with } \sigma_\infty\sigma_1\sigma_0 = 1\right\}$

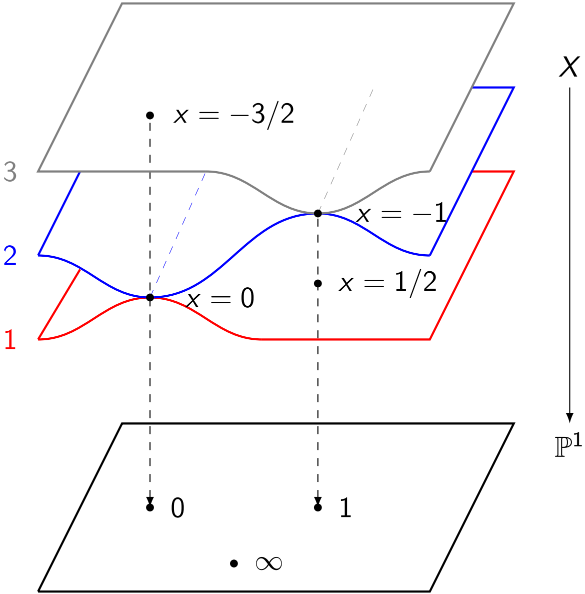
$\left\{\text{Index } d \text{ triangle subgroups } \Gamma \leq \Delta(a, b, c)\right\}$

$\left\{\text{dessins with } d \text{ edges}\right\}$

$\left\{\text{Degree } d \text{ function field extensions } K \supseteq \mathbb{C}(z) \text{ with discriminant supported above } 0, 1, \infty\right\}$

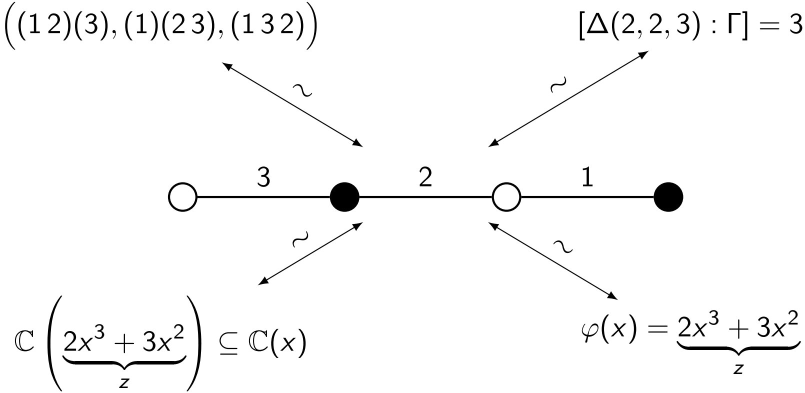
$\{\text{Belyĭ maps of degree } d\}$

Example 😇



$$\varphi(x) = \underbrace{2x^3 + 3x^2}_{z}$$

Example 😇



$$\big((1\,2)(3), (1)(2\,3), (1\,3\,2)\big)$$

$$[\Delta(2,2,3) : \Gamma] = 3$$

$$\mathbb{C}\left(\underbrace{2x^3+3x^2}_{z}\right) \subseteq \mathbb{C}(x)$$

$$\varphi(x) = \underbrace{2x^3+3x^2}_{z}$$

Motivation

Motivation

In his 1984 work *Esquisse d'un Programme*, Grothendieck describes an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of dessins d'enfants.

Motivation

In his 1984 work *Esquisse d'un Programme*, Grothendieck describes an action of Gal$(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of dessins d'enfants.

About this discovery, Grothendieck said: *I do not believe that a mathematical fact has ever struck me quite so strongly as this one.*

Motivation

In his 1984 work *Esquisse d'un Programme*, Grothendieck describes an action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the set of dessins d'enfants.

About this discovery, Grothendieck said: *I do not believe that a mathematical fact has ever struck me quite so strongly as this one.*

This yields a Galois action on everything in the zoo.

Database

Database

Also in Grothendieck's Esquisse d'un Programme, he writes about the computation of specific examples of Belyĭ maps:

Exactly which are the conjugates of a given oriented map? (Visibly, there is only a finite number of these.) I considered some concrete cases (for coverings of low degree) by various methods, J. Malgoire considered some others–I doubt there is a uniform method for solving the problem by computer.

Database

Also in Grothendieck's Esquisse d'un Programme, he writes about the computation of specific examples of Belyĭ maps:
Exactly which are the conjugates of a given oriented map? (Visibly, there is only a finite number of these.) I considered some concrete cases (for coverings of low degree) by various methods, J. Malgoire considered some others–I doubt there is a uniform method for solving the problem by computer.

In 2014, KMSV provide a general purpose numerical method for computing Belyĭ maps using power series expansions of modular forms.

Database

We are currently tabulating a database of *all* Belyĭ maps in low degree to be included in the LMFDB `www.lmfdb.org`.

Database

We are currently tabulating a database of *all* Belyĭ maps in low degree to be included in the LMFDB `www.lmfdb.org`.

Below is a table detailing how many Belyĭ maps (up to isomorphism) there are of given degree and genus.

d	$g = 0$	$g = 1$	$g = 2$	$g = 3$	$g > 3$	total
2	1	0	0	0	0	1
3	2	1	0	0	0	3
4	6	2	0	0	0	8
5	12	6	2	0	0	20
6	38	29	7	0	0	74
7	89	50	13	3	0	155
8	261	217	84	11	0	573
9	583	427	163	28	6	1207

Galois action for example
`7T5-[3,4,4]-331-421-421-g0`

Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the element interchanging $\pm\sqrt{7}$...

Galois action for example

7T5-[3,4,4]-331-421-421-g0

Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the element interchanging $\pm\sqrt{7}$...

$$\lambda = \left(\frac{1}{3087}\left(173\sqrt{7} + 343\right)\right)$$

Galois action for example
7T5-[3,4,4]-331-421-421-g0

Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the element interchanging $\pm\sqrt{7}$...

$$\lambda = \left(\frac{1}{3087}\left(173\sqrt{7} + 343\right)\right)$$

$$\varphi = \lambda \cdot \frac{x^3\left(x - \frac{1}{729}(68\sqrt{7} + 236)\right)^1 \left(x - \frac{1}{9}(20 - 4\sqrt{7})\right)^3}{\left(x - \frac{4}{21}(\sqrt{7} + 3)\right)^2 \left(x - \frac{4}{21}(\sqrt{7} + 1)\right)^4}$$

Galois action for example
7T5-[3,4,4]-331-421-421-g0

Let $\tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ be the element interchanging $\pm\sqrt{7}$...

$$\lambda = \left(\frac{1}{3087}\left(173\sqrt{7} + 343\right) \right)$$

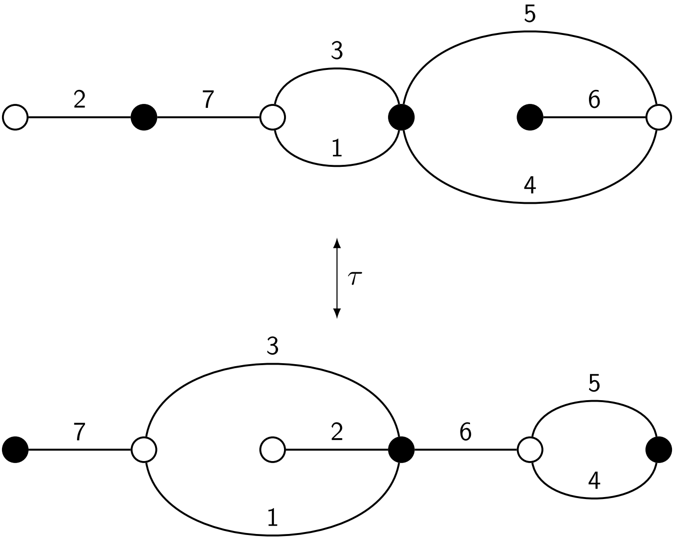
$$\varphi = \lambda \cdot \frac{x^3 \left(x - \frac{1}{729}(68\sqrt{7} + 236)\right)^1 \left(x - \frac{1}{9}(20 - 4\sqrt{7})\right)^3}{\left(x - \frac{4}{21}(\sqrt{7} + 3)\right)^2 \left(x - \frac{4}{21}(\sqrt{7} + 1)\right)^4}$$

$$\varphi - 1 = \lambda \cdot \frac{\left(x - \frac{1}{189}\left(44\sqrt{7} + 140\right)\right)^4 \left(x - \frac{1}{7}\left(12\sqrt{7} - 28\right)\right)^2 \left(x - \frac{1}{14}\left(3\sqrt{7} + 7\right)\right)^1}{\left(x - \frac{4}{21}\left(\sqrt{7} + 3\right)\right)^2 \left(x - \frac{4}{21}\left(\sqrt{7} + 1\right)\right)^4}$$

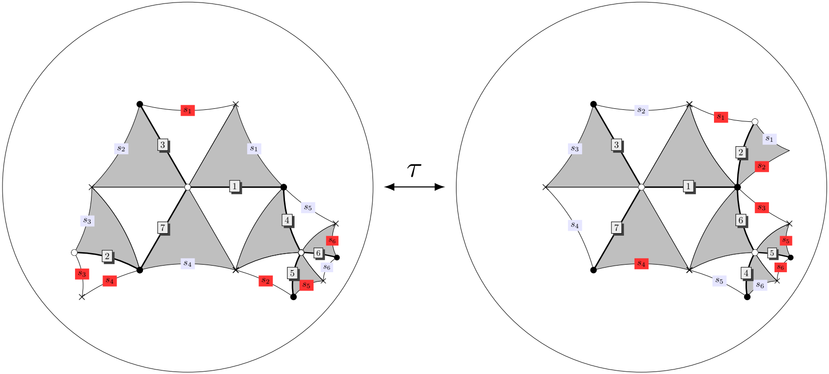
Galois action for example
7T5-[3,4,4]-331-421-421-g0

$$\begin{aligned}\sigma_0 &= (1\,3\,7)(2)(4\,5\,6)\\ \sigma_1 &= (1\,4\,5\,3)(2\,7)(6)\\ \sigma_\infty &= (1\,2\,7\,5)(3)(4\,6)\end{aligned} \quad \xleftrightarrow{\qquad\tau\qquad} \quad \begin{aligned}\sigma_0 &= (1\,3\,7)(2)(4\,5\,6)\\ \sigma_1 &= (1\,6\,3\,2)(4\,5)(7)\\ \sigma_\infty &= (1\,7\,6\,4)(2\,3)(5)\end{aligned}$$

Galois action for example
`7T5-[3,4,4]-331-421-421-g0`



Galois action for example 7T5-[3,4,4]-331-421-421-g0



Thanks for listening!