Belyi maps in number theory: a survey

John Voight
Dartmouth College

VaNTAGe
17 August 2021

Introduction: Branched covers of the projective line

Recall the Riemann–Hurwitz formula.

Let X be a nice curve over $\mathbb{C}$ with genus g, and let $\varphi\colon X \to \mathbb{P}^1$ be a map of degree d. Then

$$2g - 2 = -2d + e(\varphi)$$

where $e(\varphi) := \sum_P (e_P - 1)$ is the ramification degree.

Suppose φ is ramified at $r \geq 0$ points.

- If $r \leq 1$, then in fact $r = 0$ and $d = 1$: φ an isomorphism.
- If $r = 2$, then $g = 0$ and $\varphi(x) = x^d$.
- If $r = 3$, suddenly we see all of math!

Belyi maps

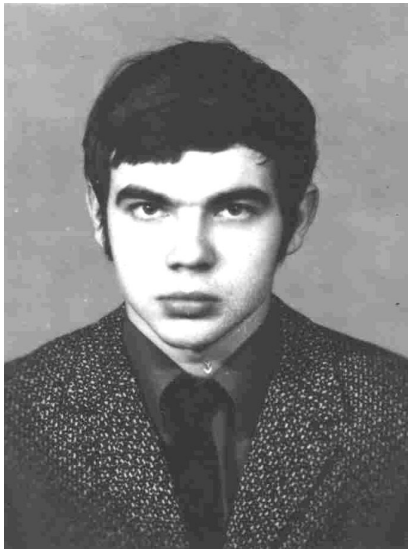
Let X be a nice curve over $\mathbb{C}$. A **Belyi map** (on X) is a nonconstant morphism

$$\varphi\colon X \to \mathbb{P}^1$$

that is unramified away from $\{0, 1, \infty\}$.

An **isomorphism** of Belyi maps is a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{\sim} & X' \\ & {\scriptstyle\varphi}\searrow \quad \swarrow{\scriptstyle\varphi'} & \\ & \mathbb{P}^1 & \end{array} .$$



G.V. Belyi (1951–2001)

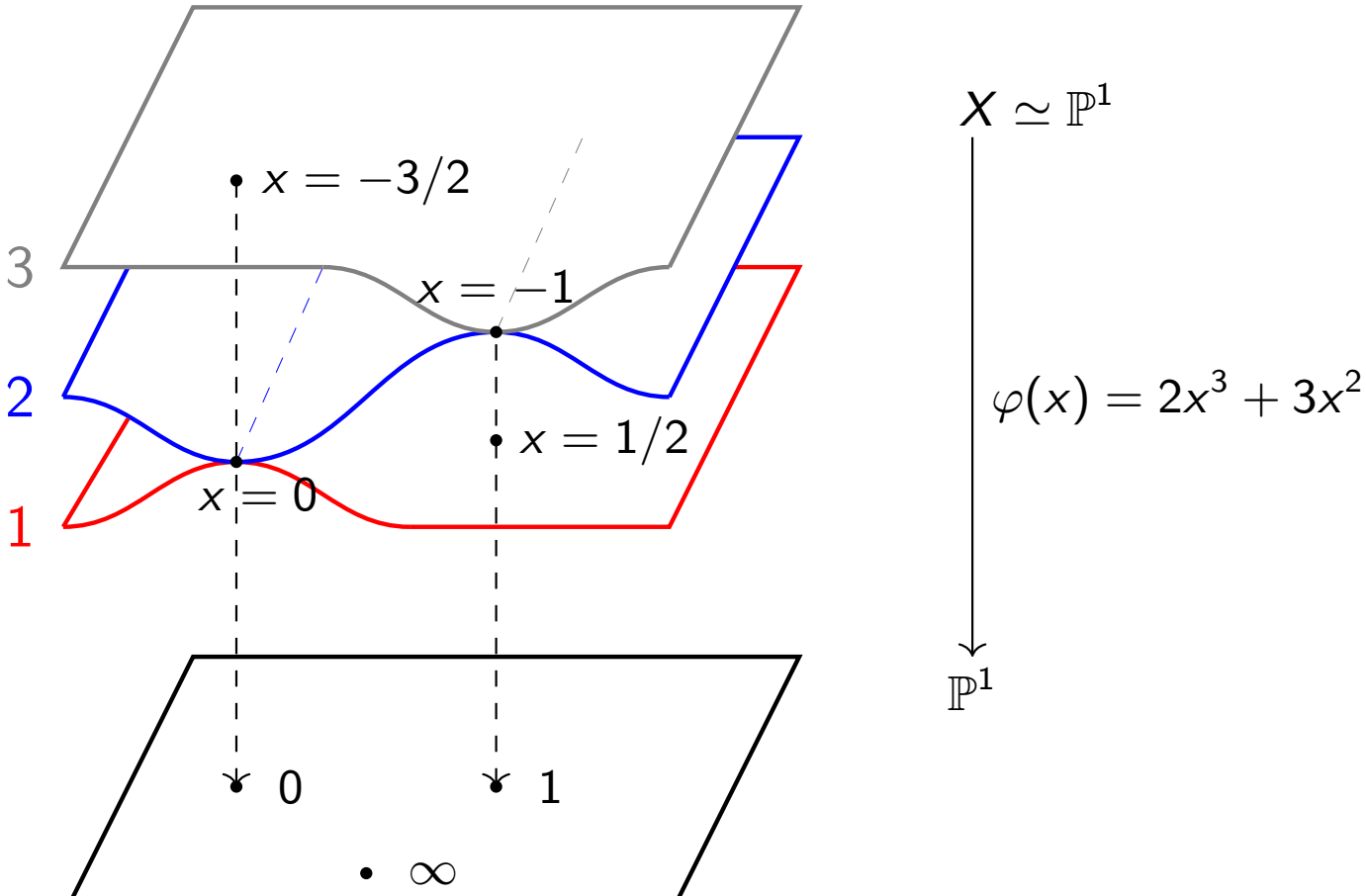
Example

Consider the map $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ defined by:

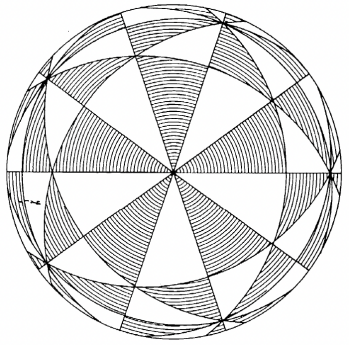
$$\varphi(x) = 2x^3 + 3x^2 = x^2(2x+3)$$

$$\varphi(x) - 1 = 2x^3 + 3x^2 - 1 = (2x-1)(x+1)^2.$$

Since $\varphi'(x) = 6x^2 + 6x = 6x(x+1)$, φ is a Belyi map of degree 3.



Belyi map examples



- An icosahedral map:

$$\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1/A_5 \simeq \mathbb{P}^1$$

$$\phi(x) = \frac{(x^{20} + 228x^{15} + 494x^{10} - 228x^5 + 1)^3}{2^6 3^3 x^5 (x^{10} - 11x^5 - 1)^5}$$

- The Fermat curve has a Belyi map of degree n^2:

$$\varphi\colon (X : x^n + y^n = z^n) \to \mathbb{P}^1$$
$$(x : y : z) \mapsto (x^n : z^n)$$

Belyi's theorem

Theorem (Belyi)

A nice curve X over $\mathbb{C}$ admits a Belyi map if and only if X can be defined over a number field $K \subset \mathbb{C}$.

The implication ($\Rightarrow$) is a consequence of Weil descent.

The implication ($\Leftarrow$) can be proven by:

1. Map $X \to \mathbb{P}^1$ using any nonconstant function;
2. Post-compose with a function to obtain ramification set in $\mathbb{P}^1(\mathbb{Q})$; then
3. Make careful use of the map

$$x \mapsto \frac{(m+n)^{m+n}}{m^m n^n} x^m (1-x)^n$$

which maps $\{0, 1, m/(m+n), \infty\} \mapsto \{0, 1, \infty\}$ for $m, n \in \mathbb{Z}_{\geq 1}$.

Grothendieck

Grothendieck, in his *Esquisse d'un Programme*, says:

Every finite oriented map gives rise to a projective non-singular algebraic curve defined over $\mathbb{Q}^{al}$, and one immediately asks the question: which are the algebraic curves over $\mathbb{Q}^{al}$ obtained in this way—do we obtain them all, who knows? In more erudite terms, could it be true that every projective non-singular algebraic curve defined over a number field occurs as a possible "modular curve" parametrising elliptic curves equipped with a suitable rigidification? Such a supposition seemed so crazy that I was almost embarrassed to submit it to the competent people in the domain. Deligne when I consulted him found it crazy indeed, but didn't have any counterexample up his sleeve. Less than a year later, at the International Congress in Helsinki, the Soviet mathematician Belyi announced exactly that result, with a proof of disconcerting simplicity which fit into two little pages of a letter of Deligne—never, without a doubt, was such a deep and disconcerting result proved in so few lines!

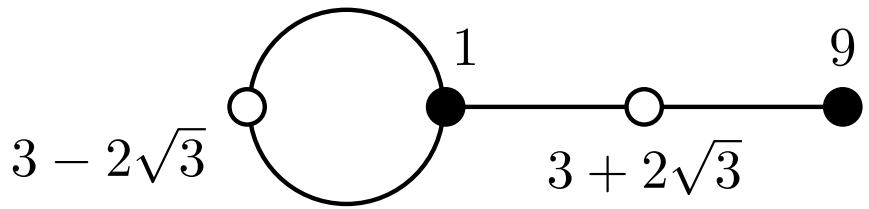
Dessins

Given a Belyi map $\varphi\colon X \to \mathbb{P}^1$, the preimage $\varphi^{-1}([0,1])$ is a **dessin**: a connected bicolored graph such that two vertices of an edge are colored differently and such that edges around each vertex are given a cyclic ordering. Conversely, a dessin determines a Belyi map, providing an equivalence of categories.

For example, the Belyi map $\varphi\colon \mathbb{P}^1 \to \mathbb{P}^1$ of degree 4 defined by

$$\varphi(x) = -\frac{(x-1)^3(x-9)}{64x} = 1 - \frac{(x^2-6x-3)^2}{64x}$$

has dessin:



Galois acting on dessins

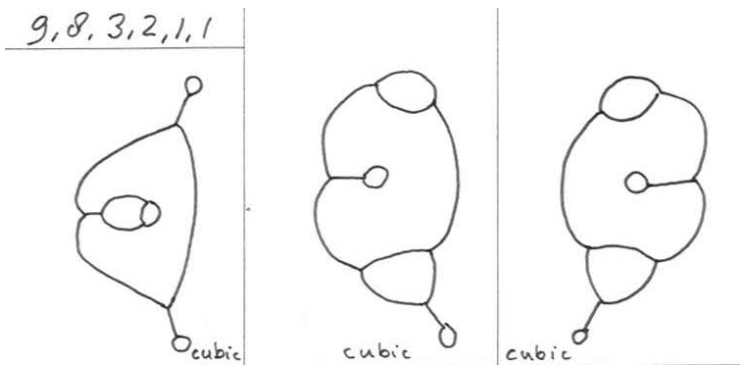
In general, Belyi maps are defined over number fields, e.g.

$$\varphi(x) = \left(2\sqrt{2}x^3 - 2(2\sqrt{2}+1)x^2 + (-4+7\sqrt{2})x + 1\right)^2 \cdot \left(14x^2 + 6(\sqrt{2}+4)x - 8\sqrt{2} + 31\right).$$

So $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ acts faithfully on the set of dessins.

The idea that one can study the action of $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ using topology (staring at drawings) is striking!

However, this Galois action on dessins is mysterious and highly unpredictable, and nontrivial invariants are difficult to find.



(Frits Beukers)

Combinatorial description of Belyi maps

The combinatorial description of Belyi maps is particularly simple: there is a bijection between

$$\text{Belyi maps } \varphi\colon X \to \mathbb{P}^1 \text{ of degree } d$$

up to isomorphism over $\mathbb{Q}^{\mathrm{al}}$ and **transitive permutation triples**

$$\sigma = (\sigma_0, \sigma_1, \sigma_\infty) \in S_d^3 \text{ that satisfy } \sigma_\infty\sigma_1\sigma_0 = 1$$
$$\text{and generate a transitive subgroup } \langle\sigma\rangle \leq S_d$$

up to simultaneous conjugation in S_d.

In particular, there are only finitely many $\mathbb{Q}^{\mathrm{al}}$-isomorphism classes of curves X with a Belyi map of given degree d.

For the previous examples, we had

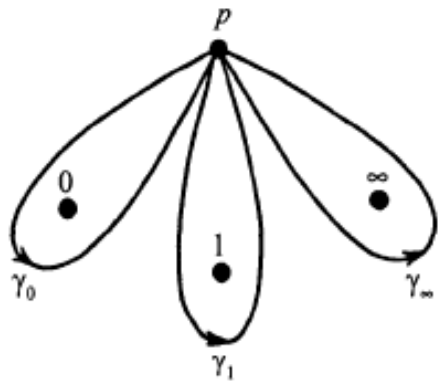
$$\sigma_0 = (1\ 2), \quad \sigma_1 = (2\ 3), \quad \sigma_\infty = (1\ 3\ 2)$$
$$\sigma_0 = (1\ 2\ 3), \quad \sigma_1 = (1\ 2)(3\ 4), \quad \sigma_\infty = (2\ 3\ 4).$$

Monodromy

If $\sigma \in S_d^3$ corresponds to $\varphi\colon X \to \mathbb{P}^1$, we say φ has **monodromy** σ. If $G = \langle\sigma\rangle \leq S_d$ is the subgroup generated by σ, then we say that the corresponding Belyi map has **monodromy group** G. The cover $\varphi\colon X^o \to \mathbb{P}^1 \setminus \{0, 1, \infty\}$ corresponds to a subgroup

$$\Gamma \leq \pi_1(\mathbb{P}^1 \setminus \{0, 1, \infty\}) \simeq F_2$$

of index d in the free group on 2 generators γ_0, γ_1.



In particular, the cycles of the permutation correspond to the points of X above $0, 1, \infty$ and the length of the cycle corresponds to to its multiplicity.

Passports

We organize basic Galois invariants of a Belyi map as follows.

A **passport** is the data (g, G, λ) consisting of a nonnegative integer $g \in \mathbb{Z}_{\geq 0}$, a transitive permutation group $G \leq S_d$, and three partitions $\lambda = (\lambda_0, \lambda_1, \lambda_\infty)$ of d.

The **passport** of a Belyi map is given by its genus, its monodromy group, and the ramification degrees of the points above $0, 1, \infty$.

The passport of the first example is $(0, S_3, (2+1, 2+1, 3))$.

So far

- A **Belyi map** is a map of curves $\varphi\colon X \to \mathbb{P}^1$ unramified away from $\{0, 1, \infty\}$.
- Belyi proved that curve over $\mathbb{C}$ admits a Belyi map if and only if it can be defined over $\mathbb{Q}^{\mathrm{al}}$.
- There are bijections between equivalence classes of:
  - Belyi maps,
  - dessins (bicolored graphs equipped with a cyclic orientation),
  - transitive permutation triples, and
  - Permutation representations of F_2 as a fundamental group.

  And $\mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ acts on all of these sets!

Modular curves and Belyi maps

Let $X(\Gamma) := \Gamma\backslash\mathcal{H}^*$ be the modular curve attached to a finite index subgroup $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$. Then we obtain a Belyi map

$$J\colon X(\Gamma) \to \mathbb{P}^1$$

from $J(z) := j(z)/1728 = (q^{-1} + 744 + \dots)/1728$.

The "deep and disconcerting" corollary: Every curve over a number field is a modular curve.

For example, taking $\Gamma = \Gamma_0(2) \leq \mathrm{SL}_2(\mathbb{Z})$ of index 3, we obtain the map in our first example.

But this also applies to noncongruence subgroups (those not containing $\Gamma(N)$ for some N): Will Chen has given a moduli interpretation for noncongruence modular curves.

This approach also works to compute equations for certain Shimura curves (e.g. work of Elkies) and certain elliptic K3 surfaces (Beukers–Montanus).

Inverse Galois theory

Inverse Galois problem: does every transitive group $G \leq S_d$ occur as a Galois group over $\mathbb{Q}$?

A Belyi map $\varphi\colon X \to \mathbb{P}^1$ defined over K and with monodromy group G can be thought of as a family of number fields with geometric generic Galois group G. (See e.g. Malle–Matzat and Jensen–Ledet–Yui.)

The method of **rational rigidity** (Thompson, ...) can be used to ensure that $K = \mathbb{Q}$, showing that the monster group arises as the (full) Galois group of a Belyi map over $\mathbb{Q}$!

By Hilbert irreducibility, for all $t \in K$ outside of a thin set, the specialized Galois group is equal to the generic Galois group. Carefully choosing a specialization, one obtains number fields with large Galois group but constrained ramification (e.g. Malle, Roberts, ...).

Inverse Galois theory: example

The polynomial

$$f_t(x) = 2^6 a(x)^5 b(x) - 5^{10} t c(x)^7 \in \mathbb{Q}(t)[x]$$

of degree 50, where

$$a(x) = (x^4 + 11x^3 - 29x^2 + 11x + 1)(64x^5 - 100x^4 + 150x^3 - 25x^2 + 5x + 1)$$

$$b(x) = 196x^5 - 430x^4 + 485x^3 - 235x^2 + 30x + 4$$

$$c(x) = x(x+1)(2x^2 - 3x + 2)(8x^3 - 32x^2 + 10x + 1)$$

has discriminant

$$\operatorname{disc}(f_t(x)) = \frac{5^{560}7^{1092}}{2^{1918}} t^{36}(t-1)^{20};$$

the Galois group of $f(x)$ over $\mathbb{Q}(\sqrt{-7})(t)$ is

$$\mathrm{PSU}_3(\mathbb{F}_5) = \{g \in \mathrm{SL}_3(\mathbb{F}_{25}) : g\sigma(g)^t = 1\}/\text{scalars}$$

where σ is the entry-wise (5th power) Frobenius. We have $\#\,\mathrm{PSU}_3(\mathbb{F}_5) = 126000 = 2^4 3^2 5^3 7$. Specializing at $t = 2$ yields a number field L ramified only at $2, 5, 7$ with $\mathrm{Gal}(L \mid \mathbb{Q}) \simeq \mathrm{PSU}_3(\mathbb{F}_5){:}2$. See e.g. Monien and Barth–Wenz for more!

Galois Belyi maps

When a Belyi map $\varphi\colon X \to \mathbb{P}^1$ corresponds to a *Galois* extension of function fields over $\mathbb{C}$, the Riemann surface X is sometimes called **quasiplatonic**, and its dessin is said to be **regular**.

Quasiplatonic surfaces are equivalently the curves X where the map $[X] \mapsto \#\operatorname{Aut}(X)$ achieves a local maximum on $\mathcal{M}_g$.

Hurwitz proved that in general $\#\operatorname{Aut}(X) \leq 84(g-1)$. If *equality* holds, then $\varphi\colon X \to X/\operatorname{Aut}(X) \simeq \mathbb{P}^1$ is a Belyi map. So the Klein quartic has a Belyi map of degree 168.

Jones–Wolfart:

5.2.2 Genus 3

Here we have eight non-isomorphic quasiplatonic curves, which can be described by the models

$$y^2 = x^8 - x \tag{5.4}$$
$$y^2 = x^7 - x \tag{5.5}$$
$$y^2 = x^8 - 1 \tag{5.6}$$
$$y^2 = x^8 - 14x^4 + 1 \tag{5.7}$$
$$y^3 = x(1-x^3) \tag{5.8}$$
$$y^4 + x^3 = 1 \tag{5.9}$$
$$y^4 + x^4 = 1 \tag{5.10}$$
$$x^3y + y^3z + z^3x = 0\,. \tag{5.11}$$

abc conjecture

Specializing Belyi maps can give good *abc* triples: taking $x = t = 1$ in the degree 50 example above gives

$$5^2 \cdot 19^5 + 618 \cdot 103^2 = 13^7.$$

Indeed, Elkies proved using Belyi maps that the *abc* conjecture implies Mordell's conjecture.

Recall also the *abc* theorem for polynomials (the Mason–Stothers theorem): if $f(x) + g(x) = h(x) \in \mathbb{C}[x]$ are relatively prime then

$$\deg h \leq \deg \operatorname{rad}(fgh) - 1.$$

Equality holds exactly when $\varphi(x) = f(x)/g(x)$ is a (rescaled) Belyi map.

This includes **Hall polynomials** (also called **Davenport–Stothers triples**), coprime solutions to

$$x(t)^3 - y(t)^2 = z(t)$$

with $\deg x(t) = 2m$, $\deg(y(t)) = 3m$, and $\deg(z(t)) = m + 1$.

Belyi degree

Let X be a curve over $\mathbb{Q}^{\mathrm{al}}$. The **Belyi degree** of X, denoted $\mathrm{Beldeg}(X)$, is the minimal degree of a Belyi map $X \to \mathbb{P}^1$.

The Belyi degree behaves "like a height" (Liţcanu). It arises naturally in Arakelov theory, for example one can bound the Faltings height of a curve polynomially in terms of the Belyi degree (Javanpeykar).

Theorem (Javanpeykar–V)

The Belyi degree of a curve is computable.

For example, the Fermat curve $x^4 + y^4 = z^4$ has Belyi degree 8.

A computational *Esquisse*

Jeroen Sijsling and I wrote a survey on computing Belyi maps (though this misses developments in the past 7 years!).

Grothendieck asks:

> *Exactly which are the conjugates of a given oriented map? I considered some concrete cases (for coverings of low degree) by various methods... I doubt that there is a uniform method for solving the problem by computer.*

Open question: Is there an algorithm that takes as

input: a permutation triple $\sigma \in S_d^3$

and produces

output: a model for the associated Belyi map $\varphi\colon X \to \mathbb{P}^1$ over $\mathbb{Q}^{\mathrm{al}}$

that runs in time doubly exponential in d?

Conclusion

The study of Belyi maps has links to a wide range of areas of mathematics, and greater understanding may have profound implications in number theory and arithmetic geometry.
We just skimmed the surface, missing numerous applications.

But please join us for the talks to come:
Edray Goins, Ozlem Ejder, Sam Schiavone, Irene Bouw!