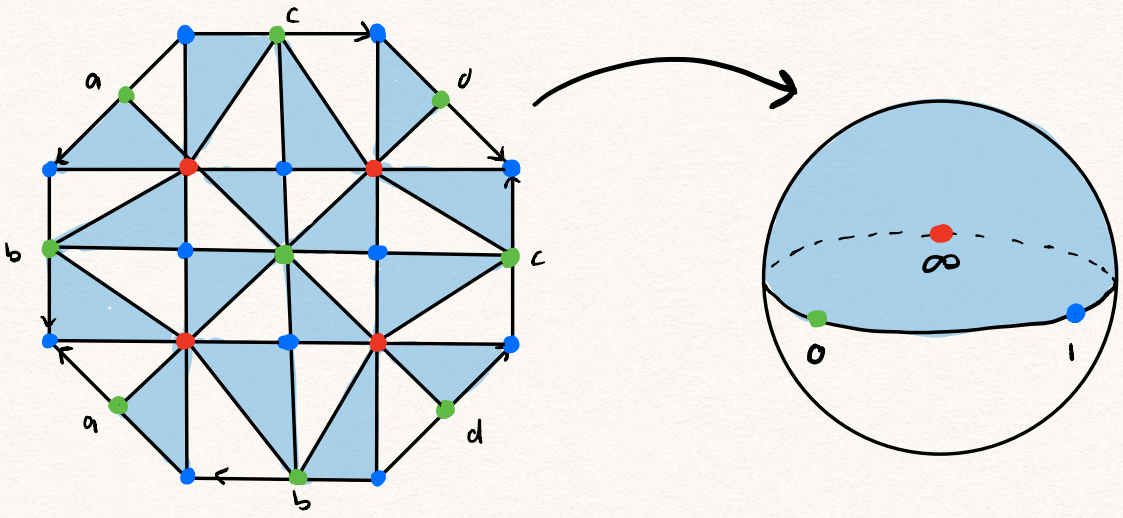
Genus 2 surface with a "Dessin"



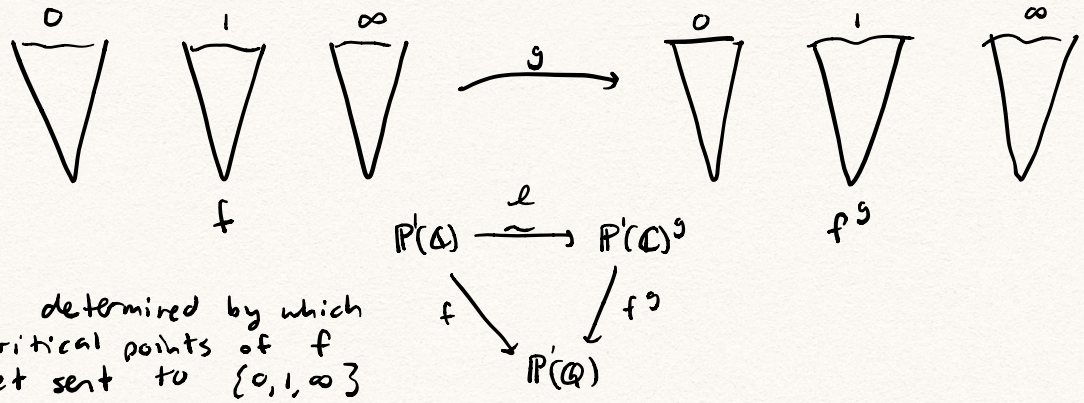
- This doodle on a genus 2 surface topologically determines a degree 16 branched covering of the sphere ramified over 3 points.
- Riemann: Any topological branched cover of the sphere described by a doodle like this can be upgraded to a meromorphic function on a Riemann surface, and an algebraic map between algebraic curves / $\mathbb{C}$.

Claim: Any algebraic curve $\mathcal{C}$ with a map $f : \mathcal{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$ branched over $\mathbb{Q}$-rat'l pts can be defined over $\overline{\mathbb{Q}}$

Sketch: $G = Gal(\mathbb{C}/\mathbb{Q})$ acts on on f and fixes critical values.

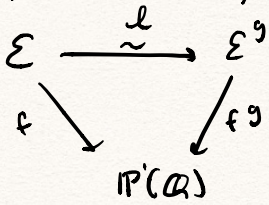
- Suffices to show that, up to an aut of the cover, f has finite G-orbit.
- Action preserves monodromy group and ramification type.
  (But not necessarily monodromy action!)
  ↳ only fin. many possibilities
  ↳ suffices to show stabilizer of isom class has finite orbit
- If $\mathcal{C}$ has genus > 2, $Aut(\mathcal{C})$ finite. ✓

- If $\mathcal{C}$ has genus = 0, can choose coordinates to assume $0, 1, \infty$ among critical points.



- ℓ determined by which critical points of f get sent to $\{0, 1, \infty\}$
  ↳ fin. many options. ✓

- If $\mathcal{C}$ has genus = 1, can choose coords. w/ @ least one rat'l point (eg. Weierstrass eqn.) Say $\mathcal{C} = \mathcal{E}$ elliptic curve w/ rat'l identity.



$\ell(P) = aP + Q$, $a \in \mu_4 \cup \mu_6$.

- ℓ determined up to fin. many options by which critical p.t. of f maps to the identity. ✓

■

Grothendieck, Sketch of a Program

> This discovery, which is technically so simple, made a very strong impression on me, and it represents a decisive turning point in the course of my reflections, a shift in particular of my centre of interest in mathematics, which suddenly found itself strongly focused. I do not believe that a mathematical fact has ever struck me quite so strongly as this one, nor had a comparable psychological impact ([2]). This is surely because of the very familiar, non-technical nature of the objects considered, of which any child's drawing scrawled on a bit of paper (at least if the drawing is made without lifting the pencil) gives a perfectly explicit example. To such a dessin, we find associated subtle arithmetic invariants, which are completely turned topsy-turvy as soon as we add one more stroke.

• • •

Every finite oriented map gives rise to a projective non-singular algebraic curve defined over $\overline{\mathbb{Q}}$, and one immediately asks the question: which are the algebraic curves over $\overline{\mathbb{Q}}$ 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 Bielyi 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!

Thm (Belyi, 1979) Let X be a compact RS. Then $X \cong \mathcal{C}/\bar{\mathbb{Q}}$ if and only if there exists a meromorphic function $f: X \to \mathbb{P}^1(\mathbb{C})$ with critical values $\subseteq \{0, 1, \infty\}$.

Pf of remaining direction:

Suppose $\mathcal{C} \xrightarrow{f} \mathbb{P}^1(\bar{\mathbb{Q}})$ defined over $\bar{\mathbb{Q}}$.

Idea: Post compose w/ rational functions that compress critical values into $\{0, 1, \infty\}$.

1. Compress to $\mathbb{Z} \cup \{\infty\}$ critical values.

Let $V \subseteq \mathbb{P}^1(\bar{\mathbb{Q}})$ be the criti vals of f, let $\bar{V}$ be union of all Galois conjugates of V.

$$g(x) := \prod_{\alpha \in \bar{V}} (x - \alpha) \in \bar{\mathbb{Q}}[x].$$

Crit. vals. of $g \circ f$ closed under Galois.

↳ so can assume f has this property. (*)

Say f has d rat'l crit. vals and e irrat'l crit vals, V.

Let $h(x) := \prod_{\alpha \in V} (x - \alpha) \in \mathbb{Q}[x]$. ← by (*)

$\deg h = e$, so has $\leq e$ irrat'l crit vals.

crit vals of $h \circ f$ = crit vals of h $\cup$ h(crit vals of f)

$\therefore$ $h \circ f$ has $\leq e$ irrat'l crit vals.

$\therefore$ Proceed inductively till we get $\tilde{f}: \mathbb{C} \to \mathbb{P}^1(\mathbb{Q})$ w/ all rat'l crit. vals; now clear denoms. ✓

2. Clever / Mysterious Trick.

Say $\{m_1, m_2, \ldots, m_d\} \subseteq \mathbb{Q}$ are the finite crit. vals of f.

$$r(x) = \prod_{i=1}^{d} (x - m_i)^{e_i}, \quad e_i \in \mathbb{Z} \text{ indeterminate.}$$

Idea: Choose e_i so that $\{m_i\}$ are the only finite critical points.

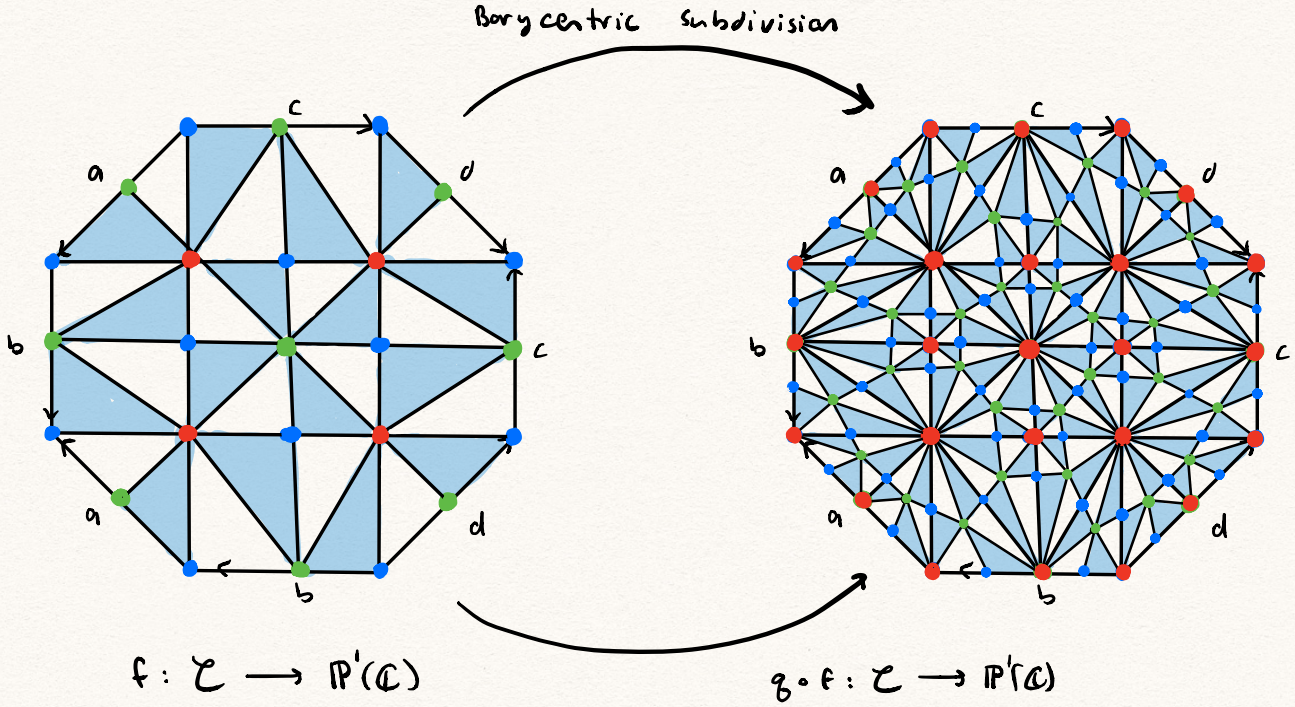
$$\frac{r'(x)}{r(x)} = \sum_{i=1}^{d} \frac{e_i}{(x - m_i)} = \frac{C}{(x-m_1)(x-m_2)\cdots(x-m_d)}$$

Can solve (explicitly) for integral e_i (partial fractions!)

$\therefore$ crit vals of $r \circ f \subseteq$ crit vals of $r(x) \subseteq \{0, 1, \infty\}$. ■

This result seems to have remained more or less unobserved. Yet it appears to me to have considerable importance. To me, its essential message is that there is a profound identity between the combinatorics of finite maps on the one hand, and the geometry of algebraic curves defined over number fields on the other. This deep result, together with the algebraic-geometric interpretation of maps, opens the door onto a new, unexplored world – within reach of all, who pass by without seeing it.

Realizing curves over $\overline{\mathbb{Q}}$ as "modular curves"



$f : \mathcal{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$

$g \circ f : \mathcal{C} \longrightarrow \mathbb{P}^1(\mathbb{C})$

All green fibers have ram. index 3, all blue fibers have ram. index 2.

↳ Monodromy action factors through modular group $PSL_2(\mathbb{Z})$.

$g : \mathbb{P}^1(\mathbb{C}) \longrightarrow \mathbb{P}^1(\mathbb{C})$ quotient by S_3.

$\left(g(x) = -\frac{4x^3}{(x^3-1)^2} \right.$ if f branched over μ_3 $\left.\right)$

Hence the map described by this picture factors the j-invariant map $j : \mathcal{H} \longrightarrow \mathbb{P}^1(\mathbb{C})$!

One last word from Grothendieck:

> There are people who, faced with this, are content to shrug their shoulders with a disillusioned air and to bet that all this will give rise to nothing, except dreams. They forget, or ignore, that our science, and every science, would amount to little if since its very origins it were not nourished with the dreams and visions of those who devoted themselves to it.