Rigidity to Non-Rigidity: The Inverse Galois Problem for M_{23} and Beyond

Shaowu Zhang

California Institute of Technology

Joint works

Part	Reference
0–3	Xiaoyu Huang, Blake Jackson, Kyu-Hwan Lee, Bjorn Poonen, Rachel Pries, Shaowu Zhang. *The Mathieu group M_{23} is a Galois group over $\mathbb{Q}$.* arXiv:2608.08538, 2026.
4–5	Shaowu Zhang, Jan Safrata, Brent Kong, Eric Lu, Sathvik Redrouthu, Caiman Moreno-Earle, Tony Yue Yu. *Knowing When to Stop: IGP-Bench and the Multi-Agent System GALOIS for the Inverse Galois Problem.* Preprint, 2026.
Soon	Xiaoyu Huang, Blake Jackson, Kyu-Hwan Lee, Bjorn Poonen, Rachel Pries, Shaowu Zhang. *More cases of Lie type.*

Plan of the talk

Mathematics

AI

0 Galois groups

1 Inverse Galois problem

2 Rigidity method

3 Beyond rigidity: M_{23}

4 IGP-Bench

5 Multi-agent system GALOIS

Galois groups as symmetries of roots

Let $f \in \mathbb{Q}[x]$ have distinct complex roots $\alpha_1, \ldots, \alpha_n$.

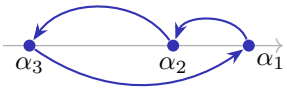
Definition

The splitting field of f over $\mathbb{Q}$ is $K = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$, and the Galois group of f is $\mathrm{Gal}(f) = \mathrm{Aut}(K/\mathbb{Q})$.

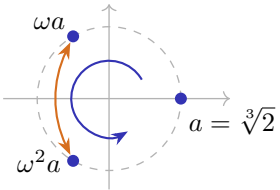
The Galois group $\mathrm{Gal}(f)$ acts on the roots via permutations and a permutation lies in $\mathrm{Gal}(f)$ iff it preserves every polynomial relation among roots with coefficients in $\mathbb{Q}$.



$x^2 - 2$: $\mathrm{Gal} = C_2$



$x^3 - 3x + 1$: $\mathrm{Gal} = A_3$



$x^3 - 2$: $\mathrm{Gal} = S_3$

Classical results

Theorem (Cyclic group C_p, see Stevenhagen, Galois Theory, §24.9.)

For every prime p, the cyclic group C_p is a Galois group over $\mathbb{Q}$ via

$$f_p(x) = \prod_{j=0}^{p-1} \left(x - \sum_{a \in H} \zeta^{(1+jp)a} \right) \in \mathbb{Z}[x], \tag{1}$$

where $\zeta = e^{2\pi i/p^2}$ and $H = \left\{ a \in \left(\mathbb{Z}/p^2\mathbb{Z}\right)^\times : a^{p-1} = 1 \right\}$.

The cyclotomic extension $L = \mathbb{Q}(\xi)$ has Galois group $G = \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/p^2\mathbb{Z})^\times$ of order $p(p-1)$. For the subgroup H, one checks that it is of order $p-1$ and there exists an element $\eta_0 = \sum_{a \in H} \xi^a$ such that $\mathbb{Q}(\eta_0) = L^H$. Since G is abelian, $\mathbb{Q}(\eta_0)/\mathbb{Q}$ is Galois, so the minimal polynomial f_p of η_0 has splitting field $\mathbb{Q}(\eta_0)$, and Galois correspondence gives $\mathrm{Gal}(f_p/\mathbb{Q}) = \mathrm{Gal}(\mathbb{Q}(\eta_0)/\mathbb{Q}) \cong G/H \cong C_p$.

Classical results

Theorem (Hilbert's irreducibility theorem, 1892; see Serre, *Topics in Galois Theory*, §§3.1–3.4)

Let $F \in \mathbb{Q}(t)[x]$ be irreducible of degree n, with Galois group $G \leq S_n$. For all $t_0 \in \mathbb{Q}$ outside a **thin** set, $F(t_0, x)$ is irreducible over $\mathbb{Q}$ with Galois group G.

Thin: contained in $\Omega_0 \cup \bigcup_i \varphi_i(C_i(\mathbb{Q}))$ with Ω_0 finite, C_i irreducible curves, $\varphi_i \colon C_i \to \mathbb{P}^1$ of degree ≥ 2.

Theorem (Hilbert 1892; see Serre, *Topics in Galois Theory*, §§4.4–4.5)

For $n \geq 2$, S_n and A_n are regular over $\mathbb{Q}(t)$, with polynomials given by $h(t, x) = (n-1)x^n - nx^{n-1} + t$:

$$S_n : \ h(t,x) \text{ over } \mathbb{Q}(t); \qquad A_n : \ h\big(t(s), x\big) \text{ over } \mathbb{Q}(s), \quad t(s) = \begin{cases} 1 + (-1)^{n/2}(n-1)s^2, & n \text{ even}, \\ n/\big(n - (-1)^{(n-1)/2}s^2\big), & n \text{ odd}. \end{cases}$$

Classical results

Theorem (Explicit realizations over $\mathbb{Q}$)

Let $L_n^{(\alpha)}(x) = \sum_{k=0}^{n} \binom{n+\alpha}{n-k}(-x)^k/k!$ be the generalized Laguerre polynomials. Then we have

$$\mathrm{Gal}(L_n^{(0)}/\mathbb{Q}) \cong S_n \qquad (n \geq 2),$$

and, for $n \geq 3$, we have

$$\mathrm{Gal}(a_n/\mathbb{Q}) \cong A_n, \qquad a_n(x) = \begin{cases} \sum_{k=0}^{n} x^k/k!, & 4 \mid n, \\ L_n^{(1)}(x), & n \text{ odd}, \\ L_n^{(n)}(x), & n \equiv 2 \pmod 4. \end{cases}$$

See Schur (1930, 1931); Gow (1989); Filaseta–Kidd–Trifonov (2012).

The inverse Galois problem

Conjecture:

For every finite group G, there exists a polynomial $f \in \mathbb{Q}[x]$ such that

$$\mathrm{Gal}(f/\mathbb{Q}) \cong G.$$

In particular, the conjecture asks the cases for all finite simple groups.

Recall: a subgroup $N \leq G$ is **normal** if $gNg^{-1} = N$ for every $g \in G$. A nontrivial group G is **simple** if its only normal subgroups are $\{1\}$ and G.

Examples. C_p (p prime) and A_n ($n \geq 5$) are simple. For $n \geq 3$, S_n is not simple, since

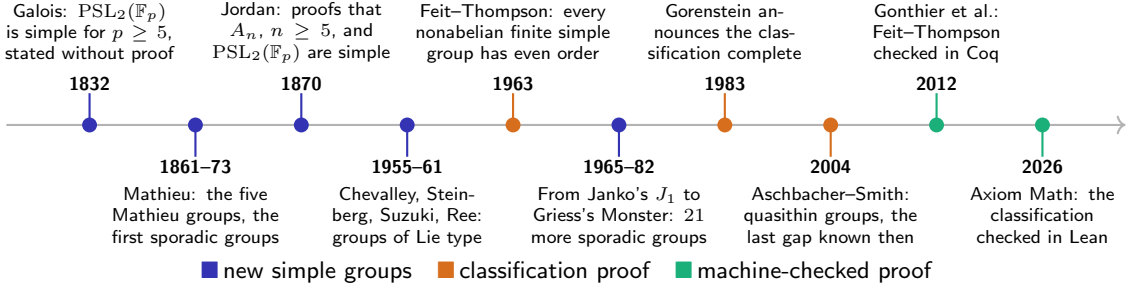
$$\{1\} \subsetneq A_n \lhd S_n.$$

What finite simple groups do we have?

Theorem (Classification of finite simple groups)

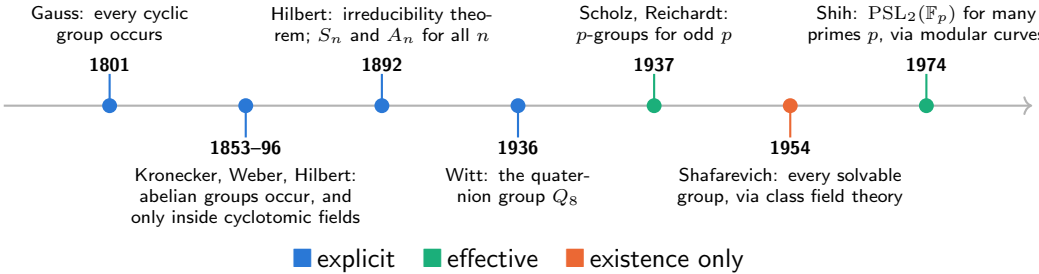
Every finite simple group is isomorphic to one of:

1. a cyclic group C_p, where p is prime;
2. an alternating group A_n, where $n \geq 5$;
3. a simple group of Lie type (16 infinite families);
4. one of the 26 sporadic simple groups.



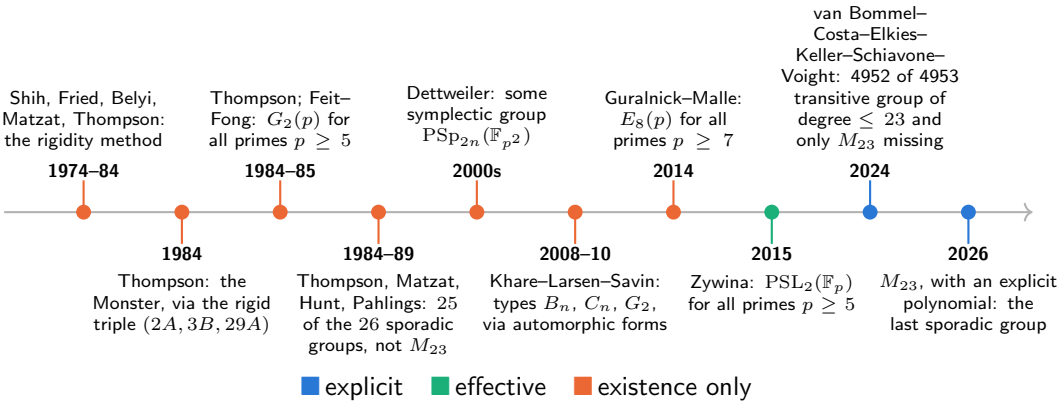
History of the inverse Galois problem, I

A realization is **explicit** if it comes with a polynomial, **effective** if the proof is an algorithm that would produce one, and an **existence** result otherwise.



The first 150 years, to 1954: cyclic, abelian, solvable and symmetric groups; the only simple groups realized were C_p and A_n.

History of the inverse Galois problem, II



After 1977 the focus is on finite *simple* groups. A polynomial for the Monster would have degree at least 9.72×10^{19}.

The Mathieu group M_{23}

Definition via permutations

The Mathieu group M_{23} is the subgroup $\langle g_1, g_2 \rangle$ of S_{23} where

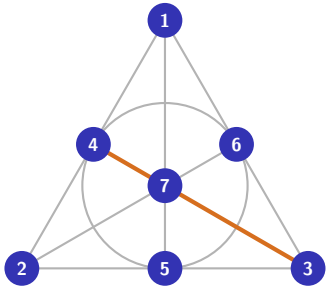
$$g_1 = (1\,2\,\cdots\,23),$$
$$g_2 = (3\,17\,10\,7\,9)(4\,13\,14\,19\,5)(8\,18\,11\,12\,23)(15\,20\,22\,21\,16).$$

Definition via combinatorics

Since M_{23} is 4-transitive, one can prove that

$$M_{23} \cong \mathrm{Aut}\big(S(4,7,23)\big),$$

where $S(4,7,23)$ is the unique Steiner system on 23 points with 7-point blocks in which every 4 points lie in exactly one block.



The smallest Steiner system $S(2,3,7)$: 7 points, 7 blocks of size 3; each pair lies in one block.

Properties of M_{23}

- $M_{23} \subsetneq A_{23} \subsetneq S_{23}$, with $|M_{23}| = 10{,}200{,}960$, $|A_{23}| = 23!/2$ and $|S_{23}| = 23!$.
- M_{23} is nonabelian simple and 4-transitive on 23 points, with point stabilizer M_{22}.
- $Z(M_{23}) = 1$ and $\mathrm{Out}(M_{23}) = 1$, so $\mathrm{Aut}(M_{23}) = \mathrm{Inn}(M_{23}) \cong M_{23}$.
- 17 conjugacy classes: $1, 2, 3, 4, 5, 6, 7A/B, 8, 11A/B, 14A/B, 15A/B, 23A/B$.
- $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes $2A$ and interchanges $23A, 23B$ via $\mathrm{Gal}(\mathbb{Q}(\sqrt{-23})/\mathbb{Q})$.
- For $S = \{0, \sqrt{-23}, -\sqrt{-23}\}$ and $c = (2A, 23A, 23B)$, the Nielsen class has 7 elements, with Galois orbits of sizes 1 and 6. The fixed point yields a cover over $\mathbb{Q}$.

Five Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$

Sporadic simple groups found by Émile Mathieu, 1861 (M_{11}, M_{12}) and 1873 (M_{22}, M_{23}, M_{24}).

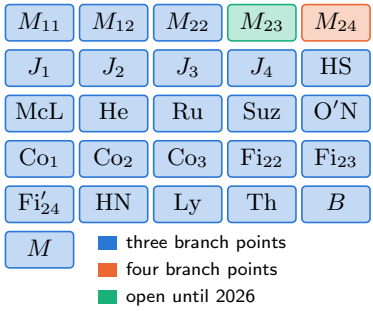
G	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}
transitivity on n points	sharply 4	sharply 5	3	4	5
Steiner system $\mathcal{S}$	$S(4,5,11)$	$S(5,6,12)$	$S(3,6,22)$	$S(4,7,23)$	$S(5,8,24)$
$\mathrm{Aut}(\mathcal{S})$	M_{11}	M_{12}	$M_{22}{:}2$	M_{23}	M_{24}
$\lvert G\rvert$	7920	95 040	443 520	10 200 960	244 823 040

$$\begin{array}{ccccc} M_{24} & \supset & (M_{24})_p = M_{23} & \supset & (M_{23})_q = M_{22} \\ \| & & \| & & \downarrow \text{index } 2 \\ \mathrm{Aut}\big(S(5,8,24)\big) & & \mathrm{Aut}\big(S(4,7,23)\big) & & \mathrm{Aut}\big(S(3,6,22)\big) = M_{22}{:}2 \end{array}$$

- **Stabilizers and derived designs:** restriction gives $\mathrm{Aut}(D)_x \hookrightarrow \mathrm{Aut}(D_x)$, which is an isomorphism for M_{23} and M_{11}, but not M_{22}. The swap $p \leftrightarrow q$ preserves $S(3,6,22)$ but not $S(4,7,23)$.
- **Other sporadic groups:** Co_1, Co_2, Co_3 from the Leech lattice; HS, McL from rank-3 graphs; the Monster from the vertex operator algebra $V^\natural$.

25 sporadic simple groups via the rigidity method and its variants

Year	Groups	Reference
1984	M, rigid triple $(2A, 3B, 29A)$	Thompson [1]
1985	J_1, J_2	Hoyden-Siedersleben [2]
1985–86	M_{11}, M_{12}, M_{22}	Matzat [3, 4]
1985–86	HS, Suz, O′N, Co_1, Co_2, Co_3, Fi_{23}, Fi'_{24}, HN, Th, B	Hunt [5]; Hoyden-S.–Matzat [6]
1988	He, Fi_{22}, J_4	Pahlings [7]
1989	J_3, McL, Ru, Ly	Pahlings [8]
1989	M_{24}	Matzat [9]



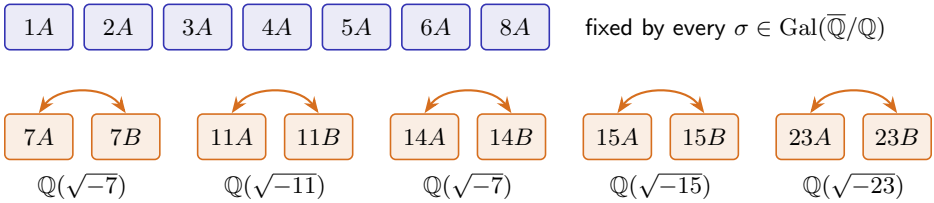
First six rows, 24 groups: rigidity with three branch points, in G, $\mathrm{Aut}(G)$ or an overgroup [10, II.9].
M_{24}: a rigid braid orbit [10, III.7].

Conjugacy classes and the Galois action

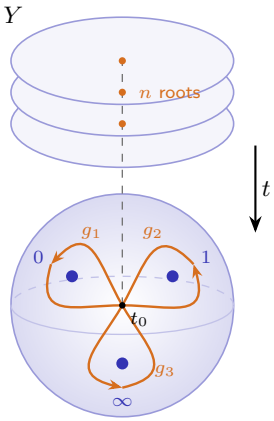
Definition

$\mathcal{C} = G/\operatorname{Inn}(G)$ is the set of **conjugacy classes** of G. For m prime to $|G|$ and $C \in \mathcal{C}$, the set $C^m = \{g^m : g \in C\}$ is another conjugacy class. Each $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $\mathcal{C}$ by $\sigma(C) = C^{\varepsilon(\sigma)^{-1}}$, with $\varepsilon\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/|G|)^\times$ the cyclotomic character. C is **rational** if $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes it.

Example: M_{23}**.** It has 17 conjugacy classes.



Covers of the sphere



the sphere $\mathbb{P}^1(\mathbb{C})$ with branch points $0, 1, \infty$

Definition

Let $F(t, x) \in \mathbb{C}[t, x]$ be irreducible of degree n in x. The curve $Y\colon F(t, x) = 0$ with its projection $t\colon Y \to \mathbb{P}^1$ is a **cover** of degree n. It is **branched** over s if the n roots are not distinct at $t = s$; equivalently, a small loop around s permutes the n points of Y above it nontrivially.

Example: $x^2 = t$ is branched over 0 and ∞: there $\pm\sqrt{t}$ swap.

Monodromy. Let F be branched only over $0, 1, \infty$.

1. Going around the i-th loop permutes the n roots: $g_i \in S_n$.
2. $g_1 g_2 g_3 = 1$: a loop around all three shrinks on the sphere.
3. $\langle g_1, g_2, g_3 \rangle = \mathrm{Gal}(F/\mathbb{C}(t))$, transitive since F is irreducible.

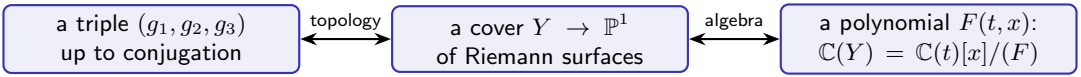
Nielsen classes and covers over $\mathbb{C}$

Definition: the Nielsen class of conjugacy classes $c = (C_1, C_2, C_3)$ of G

$$\overline{\Sigma} = \{(g_1, g_2, g_3) \in C_1 \times C_2 \times C_3 : \ g_1 g_2 g_3 = 1\},$$
$$\Sigma = \{(g_1, g_2, g_3) \in \overline{\Sigma} : \ g_1, g_2, g_3 \text{ generate } G\},$$
$$\mathrm{Ni}(C_1, C_2, C_3) = \Sigma/\text{simultaneous conjugation}.$$

Theorem (Riemann existence theorem)

Galois covers $Y \to \mathbb{P}^1_{\mathbb{C}}$ with group G, branched only over $0, 1, \infty$ with monodromy in C_1, C_2, C_3, are in bijection with $\mathrm{Ni}(C_1, C_2, C_3)$, up to isomorphism.



So $\mathrm{Ni}_c := \mathrm{Ni}(C_1, C_2, C_3)$ is a finite list of covers, defined over $\overline{\mathbb{Q}}$ and permuted by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$: the points of the *Hurwitz scheme* $\mathcal{H}_c$.

Nielsen classes and covers over $\mathbb{Q}$

Branch cycle lemma (Fried 1977)

Suppose a cover with class C_i at the branch point s_i is defined over $\mathbb{Q}$. Then every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ permutes the branch points, and the class at $\sigma(s_i)$ is $\sigma(C_i) = C_i^{\varepsilon(\sigma)^{-1}}$, with ε the cyclotomic character.

- Rational branch points need rational classes.
- Conjugate branch points need conjugate classes.

$$\begin{array}{ccc} s_i & \longmapsto & C_i \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ \sigma(s_i) & \longmapsto & \sigma(C_i) \end{array}$$

Definition

A triple of classes is **Galois-stable** if branch points can be chosen to satisfy the lemma; the map $s_i \mapsto C_i$ is then Galois-equivariant.

Example: M_{23}.

- $(2A, 23A, 23B)$ is Galois-stable: take the branch points $0,\ \sqrt{-23},\ -\sqrt{-23}$.
- $(2A, 4A, 23A)$ is not: if $\sigma(\sqrt{-23}) = -\sqrt{-23}$, some point must carry $\sigma(23A) = 23B$.

The rigidity method

Theorem (Coombes–Harbater 1985; Fried–Völklein 1991)

Let (C_1, C_2, C_3) be Galois-stable and $Z(G) = 1$. If $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ fixes an element of $\mathrm{Ni}(C_1, C_2, C_3)$, then its G-cover is defined over $\mathbb{Q}$, with function field L a regular G-extension of $\mathbb{Q}(t)$: $L \cap \overline{\mathbb{Q}} = \mathbb{Q}$.

Why $Z(G) = 1$? Let $Y \to \mathbb{P}^1$ be the cover corresponding to $x \in \mathrm{Ni}(C_1, C_2, C_3)$, and $\sigma, \tau \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

- $\mathrm{Aut}(Y/\mathbb{P}^1) = G$, and the G-equivariant automorphisms are $\mathrm{Aut}_G(Y/\mathbb{P}^1) = Z(G)$.
- Applying σ to the equations of Y gives a G-cover Y^σ, and $\sigma(x) = x$ means $Y^\sigma \cong Y$ as G-covers.
- If $Z(G) = 1$ this isomorphism f_σ is unique, so $f_{\sigma\tau} = f_\sigma \circ f_\tau^\sigma$ holds automatically. Weil's descent theorem then gives a model of Y over $\mathbb{Q}$.

Corollary (Rigidity)

If $|\mathrm{Ni}(C_1, C_2, C_3)| = 1$, then the triple is called **rigid**, and there is a regular G-extension of $\mathbb{Q}(t)$, so G occurs over $\mathbb{Q}$.

Remark. For four classes, the braid orbits on $\mathrm{Ni}(C_1, \ldots, C_4)$ are the connected components of the Hurwitz space of such covers. An orbit of unique length gives a component over $\mathbb{Q}$, whose $\mathbb{Q}$-points are covers over $\mathbb{Q}$.

Variants of rigidity for M_{11}, M_{12}, M_{22}, M_{24}

G	Class tuple	Why it gives a cover over $\mathbb{Q}(t)$	References
M_{12}	$(4A, 4A, 10A)$	$\lvert \mathrm{Ni} \rvert = 2$, but modulo the symmetry V of the two $4A$ points, $\lvert \mathrm{Ni}/V \rvert = 1$: the twisted rigidity method	Matzat–Zeh-Marschke [4]
M_{11}	the same M_{12}-cover	M_{11} is a point stabilizer in M_{12}, and its fixed field has genus 0	Matzat–Zeh-Marschke [4]
M_{22}	$(2B, 4C, 11A)$ in $\mathrm{Aut}(M_{22})$	$\lvert \mathrm{Ni} \rvert = 1$, rational classes; the fixed field of M_{22} is a rational function field	Matzat [3]; Malle [11]
M_{24}	$(12B, 2A, 2A, 2A)$	a single braid orbit of sizes $\lvert \mathrm{Ni} \rvert = 144$; genus 0 after symmetrizing the three $2A$ points	Matzat [9, 12]; Granboulan [13]; Müller [14]

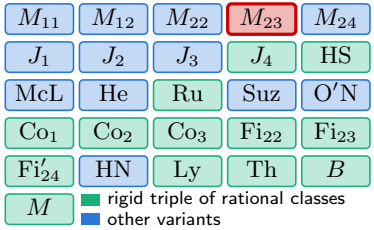
▸ $\mathrm{Aut}(M_{22})$

Variants of rigidity for other sporadic groups

Theorem (Thompson 1984)

For the Monster, $|\mathrm{Ni}(2A, 3B, 29A)| = 1$ and all three classes are rational.

1. The 13 green groups have a rigid triple of rational classes. The rest are handled by Galois-stable triples, 4-tuples, $\mathrm{Aut}(G)$, or a larger group.
2. For M_{23}: of the 86 Galois-stable 3-multisets of nontrivial classes, 30 have $|\mathrm{Ni}| = 0$ and the rest have $|\mathrm{Ni}| \geq 7$, with equality exactly for $\{2A, 23A, 23B\}$. So the classical variants of the rigidity method do not apply.



Earlier results on M_{23}

Year	Authors	Field of definition	Method
1985	Hoyden-Siedersleben [2]	$\mathbb{Q}(\sqrt{-23})(t)$	rigid triple $(2A, 3B, 23A)$ of M_{24}; M_{23} as a point stabilizer
1987	Häfner [15]	$\mathbb{Q}(\sqrt{-7})(t)$	rigid triple $(2B, 3A, 21A)$ of M_{24}; the same descent
1996	Granboulan [13]	$k(t)$ if a conic C has a k-point; $C(\mathbb{Q}) = \emptyset$	M_{24} over $\mathbb{Q}(t)$, four branch points; the fixed field of M_{23} is $\mathbb{Q}(C)$
2013	Elkies [16]	$F(t)$, F a quartic field	the four $P(x)$ with $\mathrm{Gal}(P(x) - t) \cong M_{23}$; type $(2A, 4A, 23A)$ or $(2A, 4A, 23B)$
2014–25	König [17]; Häfner [18]; Seguin [19]	$\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-15})$; not $\mathbb{Q}$	braid orbits and Hurwitz spaces, four and more branch points

Until 2026, M_{23} was the only one of the 4953 transitive groups of degree ≤ 23 not realized over $\mathbb{Q}$, and it was on the FrontierMath list of open problems [20].

four branch points

Non-rigidity method for M_{23}

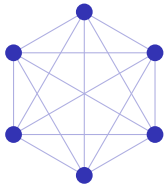
Theorem (Huang–Jackson–Lee–Poonen–Pries–Z. 2026)

For M_{23}, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has a fixed point on the Nielsen class of the Galois-stable triple $(2A, 23A, 23B)$, which gives a regular M_{23}-extension of $\mathbb{Q}(t)$.

The seven elements of $\mathrm{Ni}(2A, 23A, 23B)$, for the branch points $0,\ \sqrt{-23},\ -\sqrt{-23}$, form two Galois orbits. Here L is the sextic field

$$L = \mathbb{Q}[x]/(x^6 - x^5 - 3x^4 - 3x^3 + x^2 + 5x + 4),$$

with Galois closure of group S_6 and discriminant $2^4 \cdot 11 \cdot 23^4$.



one orbit of size 6:
$\mathrm{Spec}\, L$



fixed point:
$\mathrm{Spec}\, \mathbb{Q}$

▸ proof of $1 + 6$ ▸ $\mathrm{Aut}\ Y$

The non-rigidity method in six steps

1. One of the seven elements of $\mathrm{Ni}(2A, 23A, 23B)$ is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. ▸ fixed point
2. It corresponds to an M_{23}-cover $Y \to \mathbb{P}^1$. The quotient $X = Y/M_{22}$ is a non-hyperelliptic curve of genus 4, with a map $t\colon X \to \mathbb{P}^1$ of degree 23. ▸ genus 4
3. Compute X as a complete intersection $P = Q = 0$ in $\mathbb{P}^3$, with $\deg P = 2$ and $\deg Q = 3$, and recognize the coefficients of P, Q in $\mathbb{Q}(\sqrt{-23})$. ▸ Belyi map
4. Find a second rational function v on X and the relation $F(t, v) = 0$, with $F \in \mathbb{Z}[T, V]$ of degree 23 in V. ▸ plane model
5. Specialize t to $\mathsf{q} \in \mathbb{Q}$: by Hilbert's irreducibility theorem, $f_{\mathsf{q}} = F(\mathsf{q}, V)$ has Galois group M_{23} over $\mathbb{Q}$ for infinitely many q. ▸ fibers
6. Verify F exactly: branch points, local monodromy, and $G_{\mathrm{geom}} = G_{\mathrm{arith}} = M_{23}$. So the Galois closure $Y \to \mathbb{P}^1$ of t is an M_{23}-cover over $\mathbb{Q}$. ▸ verification

Two special fibers

Theorem (Huang–Jackson–Lee–Poonen–Pries–Z. 2026)

The set of $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q})$ with $\mathrm{Gal}(f_{\mathsf{q}}) \ncong M_{23}$ is finite: such q lift to rational points of Y/H, $H < M_{23}$ maximal, and all seven quotients have genus ≥ 4 (Faltings).

$t = \mathsf{q}$	$\mathrm{Gal}(f_{\mathsf{q}})$
0 (the rational branch point)	$\mathrm{AGL}_3(\mathbb{F}_2)$, order 1344
$-1545209/264829$	M_{22}, order $443{,}520$
∞ and every other a/b with $\lvert a\rvert, \lvert b\rvert \leq 10^{50}$	M_{23}, order $10{,}200{,}960$

- $\mathsf{q} = 0$: the fiber has 7 unramified points and 8 points of ramification index 2, so $f_0 = g_7\, g_8^2$.
- $\mathsf{q} = -1545209/264829$: the curve X has the rational point $(t, v) = (\mathsf{q}, -1/27)$, found by search. So f_{q} has a rational root, and its factor of degree 22 has Galois group M_{22}, the point stabilizer.

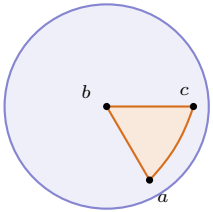
Conjecture

The only exceptions are $\mathsf{q} = 0$ and $\mathsf{q} = -1545209/264829$.

▸ the M_{22} polynomial ▸ sieve

What we've tried in 8 weeks

1. **LLMs end to end.** ChatGPT 5.6 Sol and Claude Fable 5, run end to end: no result.
2. **Four branch points.** Braid orbits and genera for 4-tuples of classes, recovering and extending Häfner's data [18]. The covers most likely to descend to a number field of low degree were pullbacks of three-point covers along a map $\mathbb{P}^1 \to \mathbb{P}^1$ of degree 2.
3. **Three branch points.** To compute the image of X in $\mathbb{P}^3$, we used the analytic coordinate q and the numerical expansions of the holomorphic differentials from BelyiDB. This coordinate is not adapted to the number field E' over which X and the point of expansion are defined, and the coefficients were not recognized at 40, 60 or even 90 digits. Later we used a local parameter τ defined over E', which agrees with a scaling λq of q up to degree 23. With it, a 40-digit computation of BelyiDB suffices.



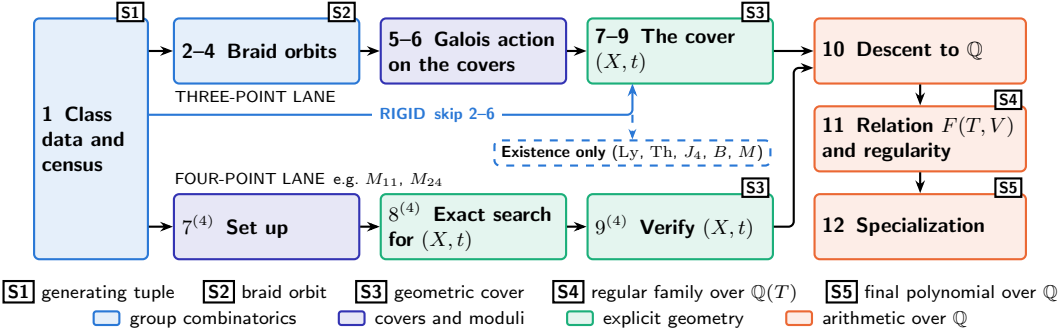
the disc D with coordinate q, $q(b) = 0$

four branch points | braid orbit data | how we succeeded

Measuring how AI fails: IGP-Bench

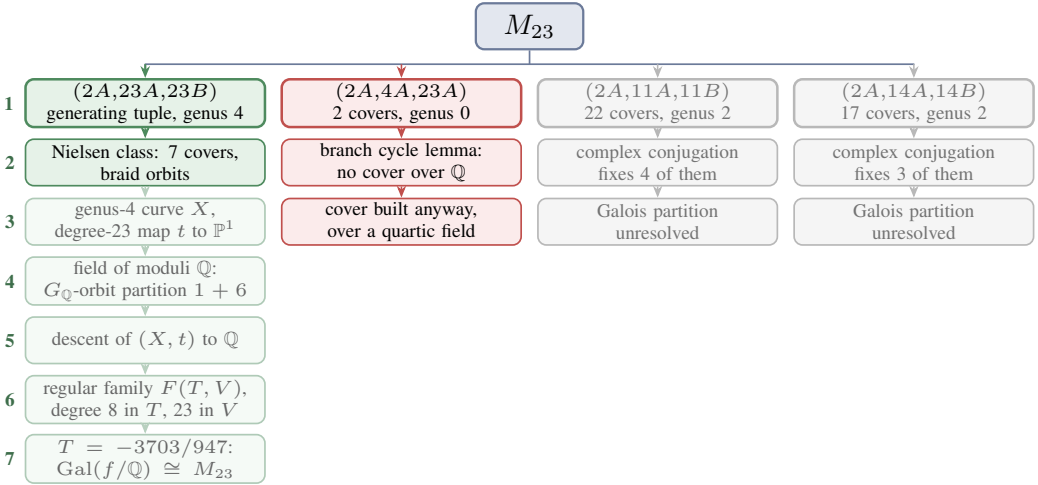
Z.–Safrata–Kong–Lu–Redrouthu–Moreno-Earle–Yu, *Knowing When to Stop* (preprint, 2026)

- **IGP-Bench** has 200 long-horizon tasks: given a finite group G, find $f \in \mathbb{Q}[V]$ with $\mathrm{Gal}(f/\mathbb{Q}) \cong G$.
- Deterministic GAP and Magma verifiers check the generic checkpoints S1–S5, with no LLM judge.
- From the agent's artifact graph: the progress score P and the knowing-when-to-stop metric K_r.



How agents fail on M_{23}

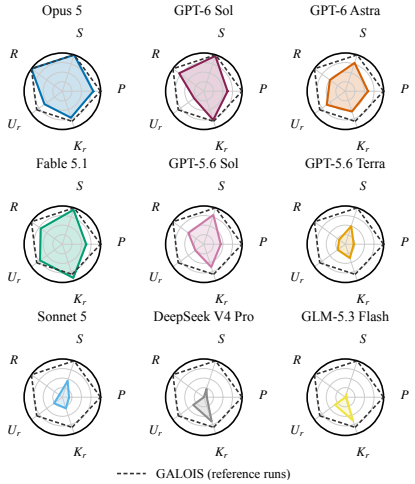
16 of the 18 single-agent runs reach checkpoint 2 and none goes further; K_r ranges from 4.7 to 98.2.



Frontier agents on IGP-Bench

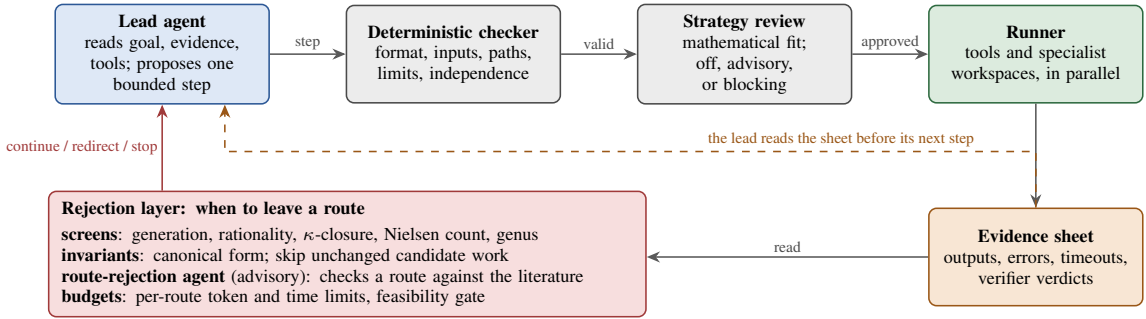
Problem. Stronger models are sometimes more stubborn and stay on a wrong route longer.

System	S	R	C	P	POLY	U_r	K_r
Claude Opus 5	100.0	100.0	52.5	**81.0**	50.0	57.7	72.8
GPT-6 Sol	97.0	80.0	22.5	**62.1**	20.0	31.4	79.1
GPT-6 Astra	78.0	50.0	52.5	**59.4**	50.0	60.3	55.9
Claude Fable 5.1	94.7	70.0	32.5	**62.4**	30.0	72.2	92.7
GPT-5.6 Sol	80.7	50.0	12.5	**44.2**	10.0	27.5	62.9
GPT-5.6 Terra	49.7	20.0	2.5	**21.9**	0.0	24.6	38.2
Claude Sonnet 5	45.0	10.0	2.5	**17.5**	0.0	26.9	30.6
DeepSeek V4 Pro	22.7	0.0	2.5	**7.8**	0.0	34.4	66.6
GLM-5.3 Flash	8.7	0.0	0.0	**2.6**	0.0	33.5	63.9
GALOIS	100.0	100.0	100.0	100.0	100.0	82.8	82.8



An open-source human-centered multi-agent system: GALOIS

Top row: the lead agent proposes one resource-limited step; a deterministic checker validates it.



- Rejection layer: a route is rejected only on an exact certificate; a resource limit only defers it.
- Failed exact recognition requires a justified precision increase, a coordinate change, another resource-limited test, or deferral, "since more digits do not repair unsuitable coordinates".

Ten hours against 126 minutes

Budget per single-agent run: 10 hours wall-clock, $500{,}000$ output tokens, eight CPUs.

Single agents: verified polynomials out of 2 runs

	M_{11}	M_{12}	M_{22}	M_{23}	M_{24}
Claude Opus 5	**1**	**2**	**2**	0	0
GPT-6 Sol	0	**1**	**1**	0	0
GPT-6 Astra	**1**	**2**	**2**	0	0
Claude Fable 5.1	**1**	0	**2**	0	0
GPT-5.6 Sol	0	0	**1**	0	0
GPT-5.6 Terra	0	0	0	0	0
Claude Sonnet 5	0	0	0	0	0
DeepSeek V4 Pro	0	0	0	0	0
GLM-5.3 Flash	0	0	0	0	0

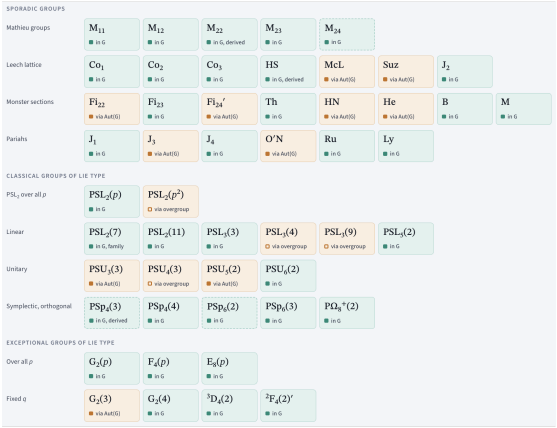
GALOIS reference runs

Task	Finished route	Minutes run 1 / run 2
M_{11}	$(2A, 2A, 3A, 4A)$	78 / 78
M_{12}	$(3A, 3A, 6A)$	13 / 10
M_{22}	$(2A, 11A, 11B)$	126 / 59
M_{23}	$(2A, 23A, 23B)$	43 / 41
M_{24}	$(2A, 2A, 2A, 12B)$	79 / 43

No single-agent run produced a verified polynomial for M_{23} or M_{24}. The ten GALOIS reference runs (Claude Opus 5.5 lead at medium effort, strategy review disabled) all reach a Magma-verified polynomial, in 10 to 126 minutes. Caveats: a different protocol; no controlled ablations of GALOIS.

Future direction: a systematic study of IGP

Goal. Understand which class tuples are special.



GROUP	ROUTE	TUPLE IN	ATLAS CLASSES	R	FIELD	LABELS	SOURCE, LOCATION
M_{11}	G itself	G	(2A, 3A, 3A, 3A)	4	$\mathbb{Q}$	as in source	König, J. Symbolic Comput. 2017, section 2, citing Dettweiler Theorem 3.10
M_{11}	G itself	G	(2A, 2A, 3A, 5A)	4	$\mathbb{Q}$	as in source	König, J. Symbolic Comput. 2017, section 3.1, Theorems 1 and 3
M_{11}	G itself	G	(2A, 2A, 3A, 4A)	4	$\mathbb{Q}$	as in source	König, J. Symbolic Comput. 2017, section 3.3, Theorem 5
M_{12}	via Aut(G)	$\mathrm{Aut}(M_{12})$	(2C, 3A, 12A)	3	$\mathbb{Q}$	as in source	Malle–Matzat 2018, II.9 Proposition 9.1(a)
M_{12}	G itself	G	(4B, 4B, 10A)	3	$\mathbb{Q}$	as in source	Roberts 2016, Table 3.1, cover B; section 3.3
M_{12}	G itself	G	(4A, 4A, 10A)	3	$\mathbb{Q}$	as in source	Roberts 2016, Table 3.1, cover B*t; section 3.3
M_{12}	G itself	G	(3A, 3A, 6A)	3	$\mathbb{Q}$	as in source	Roberts 2016, Table 3.1, cover E; section 3.5
M_{12}	G itself	G	(2B, 2B, 2A, 8B)	4	$\mathbb{Q}(a)$ family	computed	Malle 2000, Theorem 10.1 and its proof
M_{22}	via Aut(G)	$\mathrm{Aut}(M_{22})$	(2B, 4C, 11A)	3	$\mathbb{Q}$	as in source	Malle–Matzat 2018, II.9 Proposition 9.1(b)
M_{22}	via Aut(G)	$\mathrm{Aut}(M_{22})$	(2B, 2A, 2C, 6A)	4	$\mathbb{Q}$	computed	König, Math. Comp. 2017, section 8, Theorem 12
M_{22}	derived	M_{22}	(2A, 2A, 6A, 6A)	4	$\mathbb{Q}$	computed	König, Math. Comp. 2017, section 8, Theorem 12, polynomial $g(s,x)$
M_{22}	via Aut(G)	$\mathrm{Aut}(M_{22})$	(11AB, 2B, 4C)	3	$\mathbb{Q}$	computed	Barth–Wenz 2017, section 2, pp.6–7
M_{23}	G itself	G	(2A, 23A, 23B)	3	$\mathbb{Q}$	as in source	Huang–Jackson–Lee–Poonen–Pries–Zhang 2026, Theorem 1.3; sections 2–3
M_{24}	G itself	G	(12B, 2A, 2A, 2A)	4	$\mathbb{Q}(\sqrt{})$ family	as in source	Häfner 2022, Theorem 10.1

See more literature on successful class vectors: `https://shaowuz.github.io/new-frontiers/IGP/`

More cases of Lie type

More cases are coming in Blake Jackson's talk.

The M_{23} paper	`https://arxiv.org/abs/2608.08538`
Code for the M_{23} paper	`https://github.com/shaowuz/m23isgalois`
IGP-Bench and GALOIS	`https://www.shaowuzhang.com/files/knowing-when-to-stop.pdf`
Inverse Galois Atlas	`https://shaowuz.github.io/new-frontiers/IGP/`

References I

[1] John G. Thompson. Some finite groups which appear as $\mathrm{Gal}(L/K)$, where $K \subseteq \mathbb{Q}(\mu_n)$. *J. Algebra*, 89(2):437–499, 1984.

[2] Gudrun Hoyden-Siedersleben. Realisierung der Jankogruppen J_1 und J_2 als Galoisgruppen über $\mathbb{Q}$. *J. Algebra*, 97(1):17–22, 1985.

[3] B. Heinrich Matzat. Zwei aspekte konstruktiver Galoistheorie. *Journal of Algebra*, 96(2):499–531, 1985.

[4] B. Heinrich Matzat and Andreas Zeh-Marschke. Realisierung der Mathieugruppen M_{11} und M_{12} als Galoisgruppen über $\mathbb{Q}$. *J. Number Theory*, 23(2):195–202, 1986.

[5] David C. Hunt. Rational rigidity and the sporadic groups. *J. Algebra*, 99(2):577–592, 1986.

[6] Gudrun Hoyden-Siedersleben and B. Heinrich Matzat. Realisierung sporadischer einfacher Gruppen als Galoisgruppen über Kreisteilungskörpern. *J. Algebra*, 101(1):273–286, 1986.

[7] H. Pahlings. Some sporadic groups as Galois groups. *Rend. Sem. Mat. Univ. Padova*, 79:97–107, 1988.

[8] H. Pahlings. Some sporadic groups as Galois groups. II. *Rend. Sem. Mat. Univ. Padova*, 82:163–171, 1989. Errata corrige: Rend. Sem. Mat. Univ. Padova 85 (1991), 309–310.

[9] B. Heinrich Matzat. Rationality criteria for Galois extensions. In *Galois groups over $\mathbb{Q}$ (Berkeley, CA, 1987)*, volume 16 of *Math. Sci. Res. Inst. Publ.*, pages 361–383. Springer, New York, 1989.

[10] Gunter Malle and B. Heinrich Matzat. *Inverse Galois Theory*. Springer Monographs in Mathematics. Springer, 2 edition, 2018.

[11] Gunter Malle. Polynomials with Galois groups $\mathrm{Aut}(M_{22})$, M_{22}, and $\mathrm{PSL}_3(\mathbb{F}_4) \cdot 2_2$ over $\mathbb{Q}$. *Mathematics of Computation*, 51(184):761–768, 1988.

References II

[12] B. Heinrich Matzat. Zöpfe und Galoissche Gruppen. *J. Reine Angew. Math.*, 420:99–159, 1991.

[13] Louis Granboulan. Construction d'une extension régulière de $\mathbb{Q}(T)$ de groupe de Galois M_{24}. *Experiment. Math.*, 5(1):3–14, 1996.

[14] Peter Müller. A one-parameter family of polynomials with Galois group M_{24} over $\mathbb{Q}(t)$, 2012. arXiv:1204.1328.

[15] Frank Häfner. Realisierung der Mathieugruppen M_{23} und M_{24} als Galoisgruppen, 1987. Diplomarbeit, Universität Karlsruhe.

[16] Noam D. Elkies. The complex polynomials $P(x)$ with $\mathrm{Gal}(P(x) - t) \cong M_{23}$. In *ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium*, volume 1 of *Open Book Ser.*, pages 359–367. Math. Sci. Publ., Berkeley, CA, 2013.

[17] Joachim König. *The inverse Galois problem and explicit computation of families of covers of $\mathbb{P}^1\mathbb{C}$ with prescribed ramification*. PhD thesis, Universität Würzburg, 2014.

[18] Frank Häfner. Braid orbits and the Mathieu group M_{23} as Galois group, 2022. arXiv:2202.08222v3.

[19] Béranger Seguin. Fields of definition of components of Hurwitz spaces. *Annali della Scuola Normale Superiore - Classe di Scienze*, pages 1–26, 2025.

[20] Epoch AI. FrontierMath: Open problems, 2026. `https://epoch.ai/frontiermath/open-problems`, accessed 2026-08-11.

[21] Issai Schur. Gleichungen ohne Affekt. *Sitzungsberichte der Preussischen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse*, pages 443–449, 1930.

[22] Issai Schur. Affektlose Gleichungen in der Theorie der Laguerreschen und Hermiteschen Polynome. *Journal für die reine und angewandte Mathematik*, 165:52–58, 1931.

References III

[23] R. Gow. Some generalized Laguerre polynomials whose Galois groups are the alternating groups. *Journal of Number Theory*, 31(2):201–207, 1989.

[24] Michael Filaseta, Travis Kidd, and Ognian Trifonov. Laguerre polynomials with Galois group A_m for each m. *Journal of Number Theory*, 132(4):776–805, 2012.

[25] Xiaoyu Huang, Blake Jackson, Kyu-Hwan Lee, Bjorn Poonen, Rachel Pries, and Shaowu Zhang. The Mathieu group M_{23} is a Galois group over $\mathbb{Q}$, 2026. arXiv:2608.08538.

[26] Shaowu Zhang, Jan Safrata, Brent Kong, Eric Lu, Sathvik Redrouthu, Caiman Moreno-Earle, and Tony Yue Yu. Knowing When to Stop: IGP-Bench and the Multi-Agent System GALOIS for the Inverse Galois Problem. Preprint, 2026.

[27] Xiaoyu Huang, Blake Jackson, Kyu-Hwan Lee, Bjorn Poonen, Rachel Pries, and Shaowu Zhang. A regular Galois realization of the unitary group $\mathrm{PSU}_3(\mathbb{F}_4)$ over $\mathbb{Q}(t)$. Unpublished draft, revised 16 October 2026, 2026.

[28] Inverse Galois atlas, 2026. Literature snapshot, 5 October 2026; repository revision `0f054b7`. Interactive atlas.

[29] Axiom Math. Formalizing the enormous theorem, October 2026. 26 October 2026. Project announcement; Lean source.

[30] Bernat Plans and Núria Vila. Galois covers of $\mathbb{P}^1$ over $\mathbb{Q}$ with prescribed local or global behavior by specialization. *Journal de théorie des nombres de Bordeaux*, 17(1):271–282, 2005.

[31] An explicit degree-65 polynomial for $\mathrm{PSU}_3(\mathbb{F}_4)$, October 2026. Unpublished computational note, 27 October 2026.

[32] B. Heinrich Matzat. Konstruktion von Zahlkörpern mit der Galoisgruppe M_{11} über $\mathbb{Q}(\sqrt{-11})$. *Manuscripta Math.*, 27(1):103–111, 1979.

References IV

[33] M. Fried. Fields of definition of function fields and Hurwitz families—groups as Galois groups. *Comm. Algebra*, 5(1):17–82, 1977.

[34] Kevin Coombes and David Harbater. Hurwitz families and arithmetic Galois groups. *Duke Math. J.*, 52(4):821–839, 1985.

[35] Michael D. Fried and Helmut Völklein. The inverse Galois problem and rational points on moduli spaces. *Math. Ann.*, 290(4):771–800, 1991.

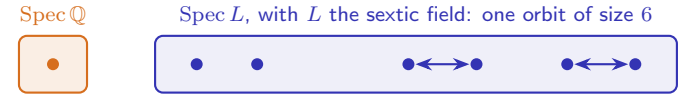
[36] Jean-Pierre Serre. *Topics in Galois theory*, volume 1 of *Research Notes in Mathematics*. Jones and Bartlett, Boston, MA, 1992.

[37] Raymond van Bommel, Edgar Costa, Noam D. Elkies, Timo Keller, Sam Schiavone, and John Voight. The constructive inverse Galois problem via Hilbert modular forms: realizing the transitive group 17T7, 2026. arXiv:2411.07857v4.

Step 1: one of the seven covers is fixed by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$

Section 3.7: Hurwitz scheme $\mathcal{H}_c$ of M_{23}-covers, $c = (2A, 23A, 23B)$ at $0, \pm\sqrt{-23}$

$\mathcal{H}_c = \operatorname{Spec} \mathbb{Q} \sqcup \operatorname{Spec} L$, so $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ has orbits of sizes 1 and 6 on $\mathrm{Ni}(2A, 23A, 23B) = \mathcal{H}_c(\overline{\mathbb{Q}})$.



seven dots: $\mathrm{Ni}(2A, 23A, 23B)$;
arrows: complex conjugation,
orbits of sizes $1, 1, 1, 2, 2$;
L has signature $(2, 2)$

- **A $\mathbb{Q}$-point of $\mathcal{H}_c$:** the cover $t\colon X \to \mathbb{P}^1_{\mathbb{Q}}$ defined by F (Step 4) and verified exactly in Step 6.
- **An L-point of $\mathcal{H}_c$:** Steps 3, 4 and 6 for a second element of the class give a cover $\mathcal{X} \to \mathbb{P}^1_L$.
- **Proposition 3.14:** the curve $\mathcal{X}$ does not descend to $\mathbb{Q}$, since $\#\mathcal{X}(\mathbb{F}_{\mathfrak{p}_1}) = 45$ and $\#\mathcal{X}(\mathbb{F}_{\mathfrak{p}_2}) = 52$ at two degree-1 primes $\mathfrak{p}_1, \mathfrak{p}_2$ of L above 53; over $\mathbb{Q}$, both would equal $\#\mathcal{X}(\mathbb{F}_{53})$.
- **Count:** the only subfields of L are $\mathbb{Q}$ and L (Galois closure of group S_6), and $\deg \mathcal{H}_c = 7 = 1 + 6$.

We have no conceptual explanation for the split $7 = 1 + 6$.

the field L | Step 6 | return to talk

Step 2: the curve X has genus 4 and is not hyperelliptic

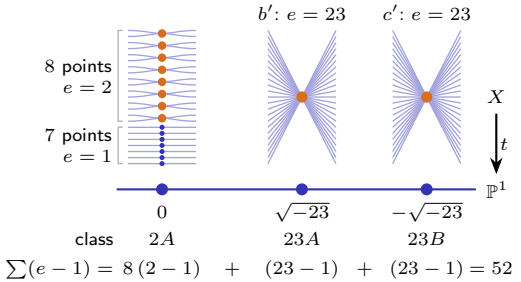
Over $\mathbb{C}$: $Y \to \mathbb{P}^1$ is the M_{23}-cover of the fixed element of $\mathrm{Ni}(2A, 23A, 23B)$, $M_{22} = \mathrm{Stab}_{M_{23}}(1)$, and $X = Y/M_{22}$. Then $t\colon X \to \mathbb{P}^1$ has degree 23 and is not Galois; its Galois closure is $Y \to \mathbb{P}^1$.

Lemmas 3.1 and 3.4

The genus g_X of X is 4, and X is non-hyperelliptic.

Genus. The ramification indices e of t are the cycle lengths of the monodromy. Riemann–Hurwitz:

$$2g_X - 2 = 23 \cdot (-2) + \sum (e-1) = -46 + 52 = 6.$$



Not hyperelliptic. The space of quadrics vanishing on the canonical image of X in $\mathbb{P}^3$ has dimension $\binom{4-1}{2} = 3$ if X is hyperelliptic and $\binom{4-2}{2} = 1$ otherwise (van Bommel–Costa–Poonen–Srinivasan). We compute numerically, without controlling errors, that it is 1; Step 6 restores rigor by verifying F. So the canonical model of X is a complete intersection $P = Q = 0$ in $\mathbb{P}^3$, $\deg P = 2$, $\deg Q = 3$.

Step 3 Step 6 return to talk

Step 3: equations for X in $\mathbb{P}^3$

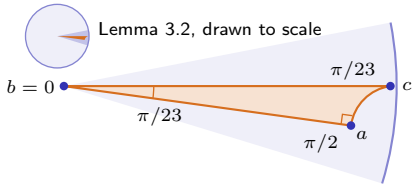
In the unit disc D with coordinate q, let $\delta_a, \delta_b, \delta_c$ be the counterclockwise hyperbolic rotations by $2\pi/2$, $2\pi/23$, $2\pi/23$ around a, b, c; let (g_1, g_2, g_3) represent the element of $\mathrm{Ni}(2A, 23A, 23B)$ from Step 1.

$$\Delta := \langle \delta_a, \delta_b, \delta_c \mid \delta_a^2 = \delta_b^{23} = \delta_c^{23} = \delta_a\delta_b\delta_c = 1 \rangle \quad \text{(right action)},$$

$$\psi\colon \Delta \twoheadrightarrow M_{23}, \quad (\delta_a, \delta_b, \delta_c) \mapsto (g_1, g_2, g_3),$$

$$\Gamma := \psi^{-1}(M_{22})\colon \quad D/\Gamma \to D/\Delta \text{ is } t\colon X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}},$$

basis of $H^0(X_{\mathbb{C}}, \Omega^1) \xrightarrow{\text{pullback to } D} f_0\,dq, \ldots, f_3\,dq, \quad f_i \in \mathbb{C}[[q]]$.



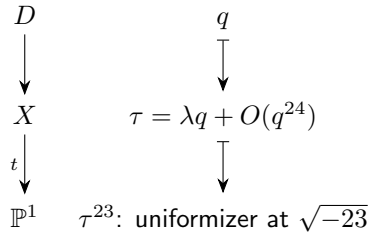
- BelyiDB (algorithm of Klug–Musty–Schiavone–Voight and Musty–Schiavone–Sijsling–Voight) computes the first $N = 19$ coefficients of each f_i numerically, to 40 digits.
- For R homogeneous of degree $d \le 3$: $R(f_0, \ldots, f_3) \equiv 0 \pmod{q^{19}}$ implies $R(f_0, \ldots, f_3) = 0$, since a nonzero section of $(\Omega^1)^{\otimes d}$ has at most $(2g_X - 2)d = 6d \le 18$ zeros.
- Numerical linear algebra gives a quadric P_1 and a cubic $Q_1 \notin (P_1)$ vanishing at $(f_0 : \cdots : f_3)$. After rescaling q and normalizing, lattice reduction recognizes the coefficients in $K = \mathbb{Q}(\sqrt{-23})$.
- Errors are not controlled at this stage; rigor returns at the end, by algebraic verification (Step 6).

recognition | details | return to talk

Backup: how we succeeded in one day

We replaced the disc coordinate q by the scaled parameter $q' = \lambda q$, which agrees to order 24 with a uniformizer τ at b' defined over the number field E' (Lemmas 3.5 and 3.6 of the paper).

- The rotation δ_b acts by $q \mapsto \zeta q$ and $\tau \mapsto \zeta\tau$, $\zeta = e^{2\pi i/23}$, so $\tau = \lambda q + O(q^{24})$.
- Scaling by λ multiplies a monomial of weight w by λ^{-w}, with x_i of weight i. Choose λ so that x_0x_2 and x_0x_3 have equal coefficients in P_λ.
- Normalize P_λ and Q_λ. At 40 digits, lattice reduction recognizes the coefficients of P, but not those of Q.
- Replace λ by λ/α, α small in a fractional ideal of E': Q is recognized too, with coefficients in $\mathbb{Q}(\sqrt{-23})$.



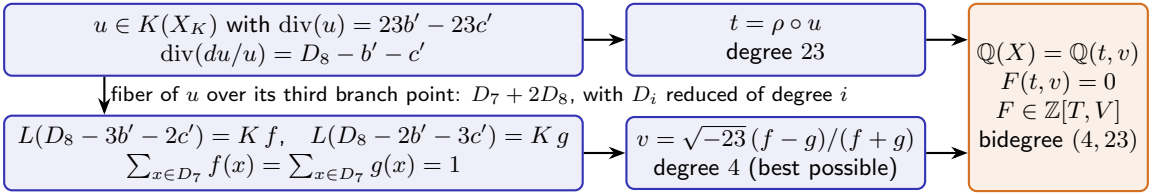
$E' = E(\sqrt{-23})$; the cover is defined over E, with $[E : \mathbb{Q}] \leq 7$.

Belyi map details | return to talk

Step 4: a plane model $F(t, v) = 0$ over $\mathbb{Q}$

Descent assumption (Section 3.4); Step 6 verifies F independently

There exists a degree 23 cover $t\colon X \to \mathbb{P}^1_{\mathbb{Q}}$ with Galois group M_{23} and local monodromy $(2A, 23A, 23B)$ above $S = \{0, \pm\sqrt{-23}\}$ whose base change to $K = \mathbb{Q}(\sqrt{-23})$ is $X_K \subset \mathbb{P}^3_K$, such that $\mathrm{Gal}(K/\mathbb{Q})$ interchanges b' and c'. Here $b', c' \in X_K(K)$ are the totally ramified points of the cover.

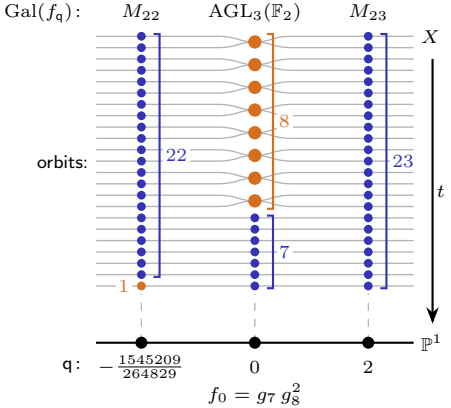


- t: scale u so that $u = 1$ on D_8; $\rho \in \mathrm{Aut}(\mathbb{P}^1_K)$ sends $1, 0, \infty$ to $0, \sqrt{-23}, -\sqrt{-23}$.
- v: for the intended $\mathbb{Q}$-structure, $\mathrm{Gal}(K/\mathbb{Q})$ fixes D_8 and interchanges b', c' and f, g.
- F: linear algebra modulo many primes $p \approx 10^7$ split in K; reconstruct over $\mathbb{Q}$; clear denominators.

Step 6 | details | return to talk

Step 5: Hilbert irreducibility and the fibers of $t\colon X \to \mathbb{P}^1$

For $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q})$ let X_q be the fiber of t above q; put $f_\mathsf{q} = F(\mathsf{q}, V)$ for $\mathsf{q} \in \mathbb{Q}$ and $f_\infty = \tau^4 F(1/\tau, V)|_{\tau=0}$. The roots of f_q correspond to the points of $X_\mathsf{q}(\overline{\mathbb{Q}})$, and its irreducible factors to the $\mathrm{Gal}(f_\mathsf{q})$-orbits.



Proposition (Proposition 3.18 (b), (c))

For each $\mathsf{q} \in \mathbb{P}^1(\mathbb{Q})$, complex conjugation gives an element of order 2 in $\mathrm{Gal}(f_\mathsf{q})$, and

$$\mathrm{Gal}(f_\mathsf{q}) \cong M_{23} \iff f_\mathsf{q} \text{ is irreducible over } \mathbb{Q}.$$

- Hilbert's irreducibility theorem: f_q is irreducible for all q outside a thin set.
- By regularity: infinitely many M_{23}-extensions of $\mathbb{Q}$.
- Certified by `GaloisProof`: $\mathsf{q} = 2$ and $-3703/947$, unramified outside $\{2, 3, 23\}$ and $\{2, 7, 23\}$.

special fibers | lowest-height polynomial | return to talk

Step 6: exact verification of F

Prop. 3.10. The closure X_0 of $F = 0$ in $\mathbb{P}^1 \times \mathbb{P}^1$ has exactly 62 singular points: a node above each root of h_{62}, where $\operatorname{disc}_V F = e\,T^8(T^2+23)^{22}h_{62}^2$, $e \in \mathbb{Z} \setminus \{0\}$, $h_{62} \in \mathbb{Z}[T]$ irreducible of degree 62.

Prop. 3.11. On the normalization X of X_0, $t\colon X \to \mathbb{P}^1$ is ramified only above 0 (cycle type $1^7 2^8$) and above each of $\pm\sqrt{-23}$ (a 23-cycle), so X is geometrically irreducible. Genus: $(4-1)(23-1) - 62 = 4$.

Prop. 3.12. $G_{\mathrm{geom}} = M_{23}$, where $G_{\mathrm{geom}} \lhd G_{\mathrm{arith}} \leq S_{23}$ are the geometric and arithmetic monodromy groups of $F(t,V) \in \mathbb{Q}(t)[V]$, and $G_{\mathrm{geom},p}$, $G_{\mathrm{arith},p}$ those of $F \bmod p$, $p = 411000011$:

$$M_{23} \overset{(1)}{\subseteq} G_{\mathrm{geom}} \overset{(2)}{=} G_{\mathrm{geom},p} \subseteq G_{\mathrm{arith},p} \overset{(3)}{=} M_{23}.$$

(1) Local monodromy (Prop. 3.11) and the classification of transitive groups of degree 23. (2) $p \nmid e$, and $t(t^2+23)h_{62} = 0$ stays étale modulo p, so the prime-to-p fundamental groups specialize isomorphically (SGA 1, XIII.2). (3) Appendix A: the group is M_{23} or A_{23}, and a character sum over Frobenius elements excludes A_{23}.

Cor. 3.13. $G_{\mathrm{arith}} = M_{23}$, since $G_{\mathrm{geom}} \lhd G_{\mathrm{arith}}$ and M_{23} is self-normalizing in S_{23}. So $G_{\mathrm{geom}} = G_{\mathrm{arith}}$: the splitting field of F over $\mathbb{Q}(t)$ is a regular M_{23}-extension (Theorem 1.3).

Verified in Magma 2.29-9 and PARI/GP 2.17.4 without the use of AI.

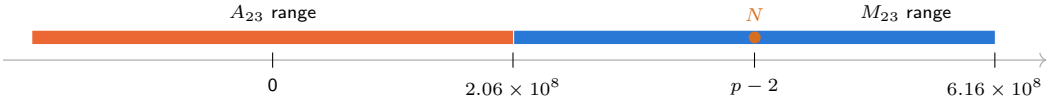
certification return to talk

Backup: certifying $G_{\text{geom}} = M_{23}$ over $\mathbb{F}_p(t)$

`GaloisProof` did not terminate over $\mathbb{Q}(t)$ and appears unavailable over $\mathbb{F}_p(t)$. Reduce mod $p = 411000011$ (tame: G_{geom} unchanged); local monodromy and the square discriminant leave $G = \mathrm{Gal}(F \bmod p)$ in $\{M_{23}, A_{23}\}$. Following an approach of Elkies (2013), use $\eta = \chi_5 - \chi_4$, with χ_r the permutation character on r-subsets: $\langle \eta, 1 \rangle = 1$ for M_{23} (two orbits on 5-sets: inside a block of $S(4, 7, 23)$ or not), 0 for A_{23}. Weil's bound for Artin L-functions gives, for $N = \sum_{u \in U(\mathbb{F}_p)} \eta(\mathrm{Frob}_u)$, $U = \mathbb{P}^1_{\mathbb{F}_p} \setminus \{0, \pm\sqrt{-23}\}$,

$$\begin{aligned} G = M_{23} &\Rightarrow |N - (p-2)| \le 10110\sqrt{p} + 14683, \\ G = A_{23} &\Rightarrow |N| \le 10108\sqrt{p} + 14686. \end{aligned}$$

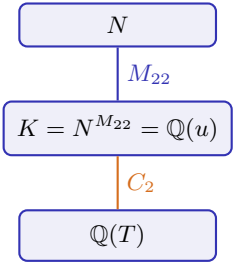
Computed in 40 CPU-hours: $N = 411207463$, in the M_{23} range.



return

Backup: M_{22} through $\mathrm{Aut}(M_{22})$

$H = \mathrm{Aut}(M_{22}) = M_{22}{:}2$ acts on 22 points; the classes $2B$ ($2^7 1^8$), $4C$ ($4^4 2^3$) lie outside M_{22} and $11A$ (11^2) inside. All three are rational and $|\mathrm{Ni}_H(2B, 4C, 11A)| = 1$: rigidity gives a regular H-extension $N/\mathbb{Q}(T)$ branched at three rational points.



$K/\mathbb{Q}(T)$ is branched at exactly two rational points, so $K = \mathbb{Q}(u)$ has genus 0. Malle's model:

$$F(T, X) = p(X)^4 q(X)^2 - 2^{22} T\, r(X)^{11}, \quad \deg p, q, r = 4, 3, 2,$$

$p = 5X^4 + 34X^3 - 119X^2 + 212X - 164$, $q = 19X^3 - 12X^2 + 28X + 32$, $r = X^2 - X + 3$. Substituting $T = u^2/(u^2 + 11)$ gives group M_{22} over $\mathbb{Q}(u)$, and Hilbert irreducibility gives M_{22}-extensions of $\mathbb{Q}$.

[3]; [10], II.9.1 and II.9.6; [11]; equation checked in [30], Proposition 2.5.

return to talk

Vocabulary I: simple groups

Definition

A subgroup $N \leq G$ is **normal** if $gNg^{-1} = N$ for all $g \in G$; then G/N is a group. A group $G \neq 1$ is **simple** if its only normal subgroups are 1 and G.

Theorem (Jordan–Hölder)

Every finite group G has a composition series $1 = G_0 \lhd G_1 \lhd \cdots \lhd G_r = G$ in which every factor G_i/G_{i-1} is simple. Any two composition series of G have the same length and the same factors, up to order and isomorphism.

Examples: C_p (p prime) and A_5 are simple; S_4 is not, since $V_4 \lhd S_4$. Galois introduced normal subgroups in 1832; the theorem is named after Camille Jordan and Otto Hölder. It makes the finite simple groups the building blocks of all finite groups.

return to talk

Backup: a detour through four branch points

Early in the research, an LLM survey of the literature suggested using four branch points.

- With four branch points the covers form a curve (Fried–Völklein). The braid group acts on Nielsen 4-tuples; each orbit is a component. An orbit that is the only one of its length gives a component over $\mathbb{Q}$; with genus 0 and a rational point, its rational points are covers over $\mathbb{Q}$. This is how M_{24} was realized over $\mathbb{Q}$ (Matzat 1989).
- For $(23A, 23A, 23B, 23B)$ the pure braid orbits have lengths $373{,}026{,}124$ (genus $121{,}077{,}255$), $29{,}693$ (genus $6{,}032$), and **seven of length 2 and genus 0**.
- With seven orbits of the same length, nothing forces a component over $\mathbb{Q}$. Pulling back a $(2A, X, Y)$ cover along $t \mapsto t^2$ gives an (X, X, Y, Y) cover; the seven small orbits are the pullbacks of the seven $(2A, 23A, 23B)$ covers.

So we returned to three branch points and computed the seven curves.

▸ braid orbit data ▸ return: earlier results

Backup: descent and certification details

Descent. On the K-model ($K = \mathbb{Q}(\sqrt{-23})$), u has divisor $23b' - 23c'$, and $t = \rho \circ u$ is the descended parameter, where $\rho \in \mathrm{Aut}(\mathbb{P}^1_K)$ sends $1, 0, \infty$ to $0, \sqrt{-23}, -\sqrt{-23}$. Let f, g generate the one-dimensional spaces $L(D_8 - 3b' - 2c')$ and $L(D_8 - 2b' - 3c')$, normalized on D_7; conjugation swaps them. Set $v = \sqrt{-23}(f-g)/(f+g)$, of degree 4. Compute $F(T, V)$ modulo many primes near 10^7 and reconstruct; largest coefficient: 63 digits. Substituting $V = (37W - 40)/(49W + 32)$ gives a model whose largest coefficient has 21 digits.

Ramification. $\mathrm{disc}_V F = e\, T^8 (T^2 + 23)^{22} h_{62}^2$; the 62 roots of h_{62} give nodes of the bidegree model in $\mathbb{P}^1 \times \mathbb{P}^1$. Its genus is $(4-1)(23-1) - 62 = 4$.

Certification. Magma's `GaloisProof` did not terminate over $\mathbb{Q}(t)$ or $L(t)$ and appears not to be implemented over $\mathbb{F}_p(t)$. Reduce modulo $p = 411{,}000{,}011$ (tame; the geometric group is unchanged), loop over all $p - 2$ points of $U(\mathbb{F}_p)$, and sum a class function η of the Frobenius cycle types. The Weil bounds give disjoint ranges for M_{23} and A_{23}; the sum lands in the M_{23} range. 40 CPU-hours per curve.

The $6 + 1$ split. A second cover has coefficients in $L = \mathbb{Q}[x]/(x^6 - x^5 - 3x^4 - 3x^3 + x^2 + 5x + 4)$, whose Galois closure has group S_6; point counts at two primes above 53 (45 vs. 52) show it does not descend to $\mathbb{Q}$. Hence the Hurwitz scheme is $\mathrm{Spec}\,\mathbb{Q} \sqcup \mathrm{Spec}\,L$.

return

Backup: the lowest-height specialization we found

$$
\begin{aligned}
f(x) = x^{23} &+ 46x^{21} - 598x^{20} + 1679x^{19} - 21620x^{18} + 127420x^{17} \\
&- 361974x^{16} + 2223732x^{15} - 9392096x^{14} + 17344116x^{13} \\
&- 71999476x^{12} + 320807726x^{11} - 436105484x^{10} + 83587888x^{9} \\
&- 2463757240x^{8} + 9451874955x^{7} - 5728074376x^{6} - 26037806834x^{5} \\
&+ 63691532334x^{4} - 67357061907x^{3} + 38754121124x^{2} \\
&- 11217790920x + 1243077066
\end{aligned}
$$

Its splitting field is an M_{23}-extension of $\mathbb{Q}$ unramified outside $\{2, 7, 23\}$; this is the specialization $t = -3703/947$. Certified with `GaloisProof`.

return

Backup: the M_{22} polynomial

At $t = -1545209/264829$ the degree-22 factor, after `polredbest`, is

$$\begin{aligned} & x^{22} - 10x^{21} - 171x^{20} + 4948x^{19} - 3160x^{18} - 878184x^{17} \\ & + 1612816x^{16} + 57499538x^{15} - 104404974x^{14} - 1334363150x^{13} \\ & + 222611762x^{12} + 13957937472x^{11} + 44873894586x^{10} + 48162643482x^{9} \\ & - 396850048164x^{8} - 2898168029276x^{7} - 8595497273752x^{6} \\ & - 12865403779026x^{5} - 5309597045808x^{4} + 12770814291390x^{3} \\ & + 19223398109406x^{2} + 8150987444096x + 212425572022 \end{aligned}$$

and its splitting field is an M_{22}-extension of $\mathbb{Q}$. Certified with `GaloisProof`.

return

Backup: braid orbits for M_{23} with four branch points

The pure braid group acts on Nielsen classes of 4-tuples. Each orbit is a component of the Hurwitz curve, with genus given by the cycle counts of $\beta_{12}, \beta_{13}, \beta_{14}$ (Häfner).

class vector	orbit length	genus
$(23A, 23A, 23B, 23B)$	373,026,124	121,077,255
	29,693	6,032
	2 (seven orbits, three real)	0
$(4A, 4A, 4A, 4A)$	85,599,672	26,562,979
	2,456 (three orbits)	459
$(8A, 8A, 8A, 8A)$	25,381,871,824	8,417,057,661
	198,488 (three orbits)	39,505
	2 (84 orbits)	0

Häfner's Theorem 5.1 builds, from each element of $\mathrm{Ni}(2A, X, Y)$ (pullback along $t \mapsto t^2$), one length-2 genus-0 orbit in each of (X, X, Y, Y), (X, Y, X, Y), (X, Y, Y, X); for $X = Y = 8A$ these coincide, so $|\mathrm{Ni}(2A, 8A, 8A)| = 28$ gives the $84 = 3 \cdot 28$ small orbits.

return

Backup: the numerical Belyi map

In the unit disk D with coordinate q, for $\theta = \pi/23$ the points $a = e^{-i\theta}\sqrt{\tan(\pi/4-\theta)}$, $b = 0$, $c = \sqrt{\cos 2\theta}$ are the vertices of a hyperbolic triangle with angles $\pi/2, \theta, \theta$. Let $\Delta = \langle \delta_a, \delta_b, \delta_c \rangle$ be the triangle group of rotations about them, and $\psi\colon \Delta \to M_{23}$ send $\delta_a, \delta_b, \delta_c$ to g_1, g_2, g_3. With $\Gamma = \psi^{-1}(M_{22})$, the cover is $D/\Gamma \to D/\Delta$.

- q is a uniformizer at the image b' of b on X. A basis of holomorphic differentials pulls back to $f_0\,dq, \ldots, f_3\,dq$ with $f_i \in \mathbb{C}[[q]]$; the algorithm of Klug–Musty–Schiavone–Voight (BelyiDB, in Magma) computes the first N coefficients numerically; $N = 19$, to 40 digits.
- A form R of degree $d \le 3$ with $R(f_0, \ldots, f_3) \equiv 0 \bmod q^{19}$ vanishes identically, since a section of $(\Omega^1)^{\otimes d}$ has at most $(2g-2)d \le 18$ zeros.
- The space of quadrics through $(f_0 : \cdots : f_3)$ has dimension 1, not 3, so X is not hyperelliptic and is the intersection of a quadric P and a cubic Q. Normalize P, Q and the scaling of q, then recognize the coefficients by lattice reduction: they lie in $\mathbb{Q}(\sqrt{-23})$.

return

Backup: the Galois closure Y and its automorphisms

Y is the M_{23}-cover of $\mathbb{P}^1$ whose quotient by M_{22} is X. The Euler characteristic of the quotient stack is

$$\chi([Y/M_{23}]) = 2 - \tfrac{1}{2} - \tfrac{22}{23} - \tfrac{22}{23} = -\tfrac{19}{46}, \qquad 2 - 2g_Y = |M_{23}| \cdot \chi([Y/M_{23}]),$$

so $g_Y = 2{,}106{,}721$. **Proposition.** $\operatorname{Aut} Y = \operatorname{Aut} Y_{\mathbb{C}} = M_{23}$.

- Every finite-index overgroup of $\Delta(2, 23, 23)$ is a triangle group, and the only one is $\Delta(2, 4, 23)$, of index 2 (Singerman). So $(\operatorname{Aut} Y_{\mathbb{C}} : M_{23}) \leq 2$.
- Index 2 would give an involution swapping the points with monodromy $23A$ and $23B$, hence an outer automorphism of M_{23} swapping the classes. There is none.

Consequence: Y is not also an M_{24}-cover of $\mathbb{P}^1$; the $\mathbb{Q}(\sqrt{-23})$-realizations of Malle–Matzat come from M_{24}-covers, and ours cannot.

return to talk

Backup: local arguments and the sieve

- **Real points.** $\mathbb{P}^1(\mathbb{R}) - \{0\}$ contains no branch point, so complex conjugation acts on $X_{\mathsf{q}}(\mathbb{C})$ in the same conjugacy class for all real $\mathsf{q} \neq 0$; it is the class $2A$. So every $\mathrm{Gal}(f_{\mathsf{q}})$ has even order, and $(23{:}11)\backslash Y$ has no real point. Also: $\mathrm{Gal}(f_{\mathsf{q}}) = M_{23}$ if and only if f_{q} is irreducible.
- **23-adic points.** The Newton polygon of $F(\mathsf{q}, V)$ at 23 depends only on $v_{23}(\mathsf{q})$ and forces the inertia group to contain an element of order 7, 15, or 23. M_{11} has none, so $M_{11}\backslash Y$ has no $\mathbb{Q}_{23}$-point.
- **The sieve.** Write $\mathsf{q} = a/b$. If $a^2 + 23b^2$ is not of the form $2^i 3^j 23^k w^{23}$, then some prime $p \neq 2, 3, 23$ is totally ramified of degree 23 in $\mathbb{Q}[V]/(f_{\mathsf{q}})$, so $\mathrm{Gal}(f_{\mathsf{q}}) = M_{23}$. Enumerate the numbers of that form of the relevant size, represent each as $a^2 + 23b^2$ by Cornacchia's algorithm, and test irreducibility of f_{q}. This handles all q with $|a|, |b| \leq 10^{50}$.

return to talk