THE MATHIEU GROUP M_{23} IS A GALOIS GROUP OVER $\mathbb{Q}$

XIAOYU HUANG, BLAKE JACKSON, KYU-HWAN LEE, BJORN POONEN, RACHEL PRIES, AND SHAOWU ZHANG

Abstract. Researchers studying the inverse Galois problem realized 25 of the 26 sporadic finite simple groups as Galois groups over $\mathbb{Q}$ during 1984–1989. We complete this program by proving that the last remaining sporadic group, the Mathieu group M_{23}, occurs as a Galois group over $\mathbb{Q}$. In fact, we produce an explicit degree 23 polynomial with rational coefficients whose splitting field has Galois group M_{23} over $\mathbb{Q}$. To accomplish this, we use a non-rigid triple of conjugacy classes of M_{23} and compute Belyi maps to construct an explicit regular Galois extension of $\mathbb{Q}(t)$ with Galois group M_{23}. Essential for our computation is the numerical Belyi map algorithm developed and implemented by Klug, Musty, Schiavone, Sijsling, and Voight, inspired by ideas of Hejhal and Stark.

1. Introduction

1.1. **The inverse Galois problem.** The inverse Galois problem asks whether or not every finite group G occurs as the Galois group of some finite Galois extension of $\mathbb{Q}$. In particular, one can ask the question for finite simple groups, which fall into 18 infinite families and 26 "sporadic" groups. During 1984–1989, 25 of the 26 sporadic groups were realized as Galois groups over $\mathbb{Q}$.[1] But the last, the Mathieu group M_{23}, remained unrealized until now, despite many attempts; see Section 1.3.

Theorem 1.1. *There exists a Galois extension of $\mathbb{Q}$ with Galois group M_{23}.*

Example 1.2. The splitting field of

$$\begin{aligned} f(x) := x^{23} &- 184x^{21} - 1150x^{20} + 26151x^{19} + 18400x^{18} - 1808490x^{17} \\ &+ 1545462x^{16} + 67672923x^{15} - 42732528x^{14} - 1333395744x^{13} \\ &+ 290615166x^{12} + 10550424369x^{11} + 3700476348x^{10} + 35123826654x^{9} \\ &- 194398310718x^{8} - 1023887308293x^{7} + 3961650395556x^{6} \\ &+ 1949980486716x^{5} - 28142323927002x^{4} + 53599151839311x^{3} \\ &- 46185312415788x^{2} + 19169943578802x - 3150159884154 \end{aligned}$$

Date: August 8, 2026.

2020 *Mathematics Subject Classification.* Primary 12F12; Secondary 11G32, 11R32, 12F10, 14H30, 14Q05.

Key words and phrases. Inverse Galois problem, Mathieu group, sporadic group, Belyi map, rigidity method.

X.H. was supported by an AMS–Simons Travel Grant. B.J. was supported by ICARM through NSF grant DMS-2425401. B.P. was supported in part by NSF grant DMS-2601551 and Simons Foundation grant #402472. R.P. was supported by NSF grant DMS-2200418.

[1] Strictly speaking, the baby monster B was realized only later, since there was a calculation error in the original construction of [Hun86], according to [MM18, p. 161].

is a Galois extension of $\mathbb{Q}$ with Galois group M_{23}, unramified outside $\{2, 3, 23\}$. We certified these claims with Magma [BCP97].[2]

1.2. **Regular Galois extensions.** A ***G*-extension** of a field k is a Galois field extension L/k, together with an isomorphism $\mathrm{Gal}(L/k) \simeq G$. A finite extension of $k(t)$ is **regular** if it contains no nontrivial algebraic extension of k. If $G \neq \{1\}$ and a regular G-extension of $\mathbb{Q}(t)$ exists, then, by Hilbert's irreducibility theorem, specializing t to different rational numbers yields infinitely many G-extensions of $\mathbb{Q}$. Thus, to prove Theorem 1.1, we prove the following stronger result.

Theorem 1.3. *There exists a regular Galois extension $L/\mathbb{Q}(t)$ with Galois group M_{23}.*

1.3. **Previous work.** The rigidity method, originally developed in [Shi74, Fri77, Bel79, Mat79, Mat84, Mat85, Tho84], was instrumental for constructing regular Galois extensions of $\mathbb{Q}(t)$. Variants of this method, often involving significant new ideas such as the braid group method of [Mat89, Mat91, FV91], were used to construct regular G-extensions of $\mathbb{Q}(t)$ for all the sporadic groups G except M_{23} [Tho84, Mat85, HS85, Hun86, HSM86, MZM86, MZM87, Mal88, Pah88, Pah89]; see [MM18, II.9] for a detailed exposition.

Prior attempts to realize M_{23} over $\mathbb{Q}$ resulted only in realizations over other fields:

- Hoyden-Siedersleben [HS85] and Häfner [Häf87] used regular M_{24}-extensions of $k(t)$ to construct regular M_{23}-extensions of $k(t)$ for $k = \mathbb{Q}(\sqrt{-23})$ and $k = \mathbb{Q}(\sqrt{-7})$, respectively.
- Granboulan [Gra96] used another M_{24}-extension to construct a regular M_{23}-extension over $k(t)$ for any field k over which a certain conic C has a k-point. Unfortunately, C has no $\mathbb{Q}$-point.
- Elkies [Elk13] calculated the four degree 23 polynomials $P(x) \in \mathbb{C}[x]$ (up to affine equivalence) such that the Galois group of $P(x) - t$ over $\mathbb{C}(t)$ is M_{23}. Each such $P(x)$ has coefficients in a degree 4 number field F, so one obtains a regular M_{23}-extension of $F(t)$.

For more information and explicit computation of Hurwitz spaces for M_{23}-covers, see [Kön14], [Häf22], and [Seg].

1.4. **Outline of our approach.**

1. The group M_{23} has 17 conjugacy classes, traditionally labeled by the order of a representative element followed by an upper case letter to distinguish classes of the same order. The group $\mathfrak{G}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the set of conjugacy classes of M_{23}. It fixes the class $2 := 2A$, and acts on $23A$ and $23B$ nontrivially through the quotient $\mathrm{Gal}(K/\mathbb{Q})$, where $K := \mathbb{Q}(\sqrt{-23})$.
2. Let S be the finite étale $\mathbb{Q}$-scheme whose geometric points are $0, \sqrt{-23}, -\sqrt{-23}$.
3. The Riemann existence theorem, together with a calculation in M_{23}, shows that there are exactly seven M_{23}-covers $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ ramified only over S with local monodromy $(2, 23A, 23B)$. The quotient of each $Y_{\mathbb{C}}$ by the one-point stabilizer is a genus 4 curve $X_{\mathbb{C}}$.
4. We compute these seven curves $X_{\mathbb{C}}$ numerically using the BelyiDB package of [MSSV19], and recognize coefficients as algebraic numbers to verify the output.
5. One might expect $\mathfrak{G}_{\mathbb{Q}}$ to act transitively on these seven. Miraculously, instead $\mathfrak{G}_{\mathbb{Q}}$ has a fixed point! We do not have a conceptual explanation for this.

[2] Our code is available at `https://github.com/shaowuz/m23isgalois`.

6. The fixed point represents an M_{23}-cover $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ with field of moduli $\mathbb{Q}$. By [CH85, Proposition 2.8(c)] or [DD97, Proposition 3.1(b) and Corollary 3.2], it descends to an M_{23}-cover $Y \to \mathbb{P}^1_{\mathbb{Q}}$.

Details will be given in the subsequent sections.

1.5. **Conclusions.** Let k be a number field. Call a collection of G-extensions of k **mutually independent** if, for any $r \geq 1$, any r distinct extensions from the collection generate a G^r-extension of k.

Corollary 1.4. *Let G be a sporadic finite simple group. Let k be any number field.*

(a) *There exists a regular G-extension of $k(t)$.*
(b) *There exists a G-extension of k.*
(c) *There exists a G-extension of $\mathbb{Q}$ linearly disjoint from k.*
(d) *There exists an infinite collection of mutually independent G-extensions of k.*

Proof. Part (a) over $\mathbb{Q}$ is the combination of Theorem 1.3 and the work cited in Section 1.3. Take a compositum to get (a) over k. For (b,c,d) and other consequences of (a), see [Ser92, §3.3–3.4] and [Ser97, §10.1]. □

2. The rigidity method

2.1. ***G*-covers of the projective line.** Let G be a nonabelian finite simple group, so G has trivial center. Let $\operatorname{Inn}(G)$ be the group of inner automorphisms of G, so $\operatorname{Inn}(G) \simeq G$, and $\operatorname{Inn}(G)$ acts on G. The set $\mathcal{C} := \operatorname{Inn}(G)\backslash G$ is the set of conjugacy classes of G. For $g \in G$, let $[g] \in \mathcal{C}$ be its class. Let $n \geq 1$ be such that $g^n = 1$ for all $g \in G$.

Let k be a field of characteristic 0. For each $m \geq 1$, let $\mu_m = \{x \in \overline{k}^\times : x^m = 1\}$. Let $\mathfrak{G}_k = \operatorname{Gal}(\overline{k}/k)$. Let $\epsilon \colon \mathfrak{G}_k \to \operatorname{Aut} \mu_n \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ be the cyclotomic character describing the $\mathfrak{G}_k$-action on nth roots of unity. A choice of generator $\zeta \in \mu_n$ determines a bijection $\operatorname{Hom}(\mu_n, G) \simeq \operatorname{Hom}(\mathbb{Z}/n\mathbb{Z}, G) = G$. To make this bijection $\mathfrak{G}_k$-*equivariant*, we let $\sigma \in \mathfrak{G}_k$ act trivially on the G in $\operatorname{Hom}(\mu_n, G)$ and as $g \mapsto g^{\epsilon(\sigma)^{-1}}$ on the G on the right. Taking $\operatorname{Inn}(G)$-orbits, the latter action induces a $\mathfrak{G}_k$-action on $\mathcal{C}$.

A **curve** over k is a 1-dimensional smooth projective geometrically connected scheme of finite type over k. A ***G*-cover of $\mathbb{P}^1_k$** is a (ramified) Galois morphism of curves $Y \to \mathbb{P}^1_k$ together with an isomorphism $\operatorname{Gal}(k(Y)/k(\mathbb{P}^1)) \simeq G$. An **isomorphism of *G*-covers** $Y \to \mathbb{P}^1_k$ and $Y' \to \mathbb{P}^1_k$ is a G-equivariant isomorphism $Y \to Y'$ over $\mathbb{P}^1_k$.

2.2. **Local monodromy.** Let $D \subset \mathbb{C}$ be the open unit disk. Let $D^\times = D - \{0\}$. We have $\mathbb{Z} \xrightarrow{\sim} \pi_1(D^\times)$ sending 1 to the standard counterclockwise generator.

Suppose that $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ is a G-cover with branch locus S. For each $s \in S$, we have an analytic open embedding $D \to \mathbb{P}^1_{\mathbb{C}}$ sending 0 to s, such that s is the only point of S in the image; ignoring basepoints, this induces

$$\mathbb{Z} \simeq \pi_1(D^\times) \to \pi_1(\mathbb{P}^1(\mathbb{C}) - S) \twoheadrightarrow G$$

sending 1 to a generator of the local monodromy group (inertia group) at s. Changing basepoints conjugates the generator by an element of G, so we obtain a well-defined conjugacy class for each s, hence a map $\mathfrak{c} \colon S \to \mathcal{C}$, which we call the **local monodromy**.

Algebraically, if u is an analytic uniformizer at $s \in \mathbb{P}^1(\mathbb{C})$, the completion of $\mathbb{C}(\mathbb{P}^1)$ at s is $\mathbb{C}((u))$, and we have analogous homomorphisms involving étale fundamental groups

$$\hat{\mathbb{Z}}(1) \simeq \pi_1^{\text{ét}}(\operatorname{Spec}\mathbb{C}((u))) \to \pi_1^{\text{ét}}(\mathbb{P}^1_{\mathbb{C}} - S) \twoheadrightarrow G,$$

factoring through μ_n, defined up to conjugation by elements of G. Thus we get a canonical map $\mathfrak{c}\colon S \to \operatorname{Inn}(G)\backslash \operatorname{Hom}(\mu_n, G) \simeq \mathcal{C}$, where the last isomorphism is induced by the choice $\zeta := e^{2\pi i/n}$.

If $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ is the base change of a G-cover $Y \to \mathbb{P}^1_{\mathbb{Q}}$, then S may be viewed as a finite étale subscheme of $\mathbb{P}^1_{\mathbb{Q}}$, and $\mathfrak{c}\colon S(\overline{\mathbb{Q}}) \to \mathcal{C}$ is $\mathfrak{G}_{\mathbb{Q}}$-equivariant. This is the branch cycle argument of Fried.

2.3. **Rigidity.** See [FV91], especially Corollary 1, for details on the theory in this section. Now fix a finite étale subscheme $S \subset \mathbb{P}^1_{\mathbb{Q}}$ and a $\mathfrak{G}_{\mathbb{Q}}$-equivariant map $\mathfrak{c}\colon S(\overline{\mathbb{Q}}) \to \mathcal{C}$. Write $S(\mathbb{C}) = \{s_1, \ldots, s_r\}$, and $C_i := \mathfrak{c}(s_i)$ for $i = 1, \ldots, r$.

Let $\mathcal{H}$ be the 0-dimensional Hurwitz scheme over $\mathbb{Q}$ parameterizing G-covers of $\mathbb{P}^1$ unramified outside S with local monodromy $\mathfrak{c}$. Because G has trivial center, $\mathcal{H}$ is a fine moduli space. Define

$$\begin{aligned}
\bar{\Sigma}_{\mathfrak{c}} &:= \{(g_1, \ldots, g_r) \in C_1 \times \cdots \times C_r : g_1 \cdots g_r = 1\} \\
\Sigma_{\mathfrak{c}} &:= \{(g_1, \ldots, g_r) \in \bar{\Sigma}_{\mathfrak{c}} : g_1, \ldots, g_r \text{ generate } G\} \\
\mathrm{Ni}_{\mathfrak{c}} &:= \operatorname{Inn}(G)\backslash\Sigma_{\mathfrak{c}};
\end{aligned}$$

here $g \in G \simeq \operatorname{Inn}(G)$ acts on r-tuples by simultaneous conjugation. The set $\mathrm{Ni}_{\mathfrak{c}}$ is called the **Nielsen class**. By the Riemann existence theorem, $\mathcal{H}(\mathbb{C})$ is in bijection with $\mathrm{Ni}_{\mathfrak{c}}$.

The size $|\bar{\Sigma}_{\mathfrak{c}}|$ can be computed from the character table of G; an inclusion–exclusion gives $|\Sigma_{\mathfrak{c}}|$; and dividing by $|G|$ gives $|\mathrm{Ni}_{\mathfrak{c}}|$, which depends only on the multiset $\{C_1, \ldots, C_r\}$; see [Ser92, §7.2 and §7.3] for an exposition.

We restrict to the case $r = 3$. If $|\mathrm{Ni}_{\mathfrak{c}}| = 1$, then the triple (C_1, C_2, C_3) is called **rigid**; in that case, $\mathcal{H} \simeq \operatorname{Spec}\mathbb{Q}$ and the unique point corresponds to a G-cover $Y \to \mathbb{P}^1_{\mathbb{Q}}$ with local monodromy $\mathfrak{c}$.

3. The Mathieu group M_{23}

The Mathieu group M_{23} is a finite simple group of order $10{,}200{,}960 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$. It is a 4-transitive subgroup of S_{23}, generated by the permutations g_1, g_2 below. It has 17 conjugacy classes:

1, 2, 3, 4, 5, 6, 7A, 7B, 8, 11A, 11B, 14A, 14B, 15A, 15B, 23A, 23B

(we drop the A in the label when there is a unique conjugacy class of elements of a particular order). We calculate $|\mathrm{Ni}_{\mathfrak{c}}|$ for every $\mathfrak{G}_{\mathbb{Q}}$-stable 3-element multiset in $\mathcal{C}$, using character tables as in Section 2.3. The value of $|\mathrm{Ni}_{\mathfrak{c}}|$ is never 1, so the rigidity method fails.

We next investigate the multiset for which $|\mathrm{Ni}_{\mathfrak{c}}|$ has smallest positive size. This is $\{2, 23A, 23B\}$, with $|\mathrm{Ni}_{\mathfrak{c}}| = 7$. In fact, M_{23} is small enough that a computer can quickly list triples representing the elements of $\mathrm{Ni}_{\mathfrak{c}}$. We fix the following such triple of permutations in

S_{23}.[3]

$$\begin{aligned}
g_1 &:= (1,11)(2,23)(3,8)(4,16)(5,21)(7,20)(15,19)(18,22)\\
g_2 &:= (1,2,11,10,16,9,6,3,23,19,20,14,21,17,4,8,22,5,18,15,13,7,12)\\
g_3 &:= (1,2,3,4,10,11,12,7,19,18,8,6,9,16,17,21,22,5,14,20,13,15,23).
\end{aligned}$$

Let S be the finite étale $\mathbb{Q}$-scheme whose geometric points are $0, \sqrt{-23}, -\sqrt{-23}$. Let $\mathfrak{c}\colon S(\overline{\mathbb{Q}}) \to \mathcal{C}$ send these points to classes 2, 23A, 23B, respectively. This $\mathfrak{c}$ is $\mathfrak{G}_{\mathbb{Q}}$-equivariant. We have $(g_1, g_2, g_3) \in \Sigma_{\mathfrak{c}}$, representing a class in $\mathrm{Ni}_{\mathfrak{c}}$.

Let $Y_{\mathbb{C}} \xrightarrow{\phi} \mathbb{P}^1_{\mathbb{C}}$ be the corresponding M_{23}-cover. Let $X_{\mathbb{C}}$ be the (variety) quotient of $Y_{\mathbb{C}}$ by $\mathrm{Stab}_{M_{23}}(1) \leq M_{23}$, so ϕ factors as $Y_{\mathbb{C}} \to X_{\mathbb{C}} \xrightarrow{t} \mathbb{P}^1_{\mathbb{C}}$. Then $X_{\mathbb{C}} \xrightarrow{t} \mathbb{P}^1_{\mathbb{C}}$ is a *non-Galois* degree 23 cover branched over $S(\mathbb{C})$, and its Galois closure is $Y_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$.

Lemma 3.1. *The genus of $X_{\mathbb{C}}$ is 4.*

Proof. There are three ramified fibers of t, one with eight points of ramification index 2 and seven unramified points, and two that are totally ramified. The degree of the ramification divisor of t is $8(2-1)+2(23-1)$, so the genus of $X_{\mathbb{C}}$ is 4 by the Riemann–Hurwitz formula. □

Model the hyperbolic plane by the open unit disk D. Let q be the standard coordinate on D. Let $d(z,w)$ be the metric on D. Given $\theta \in (0, \pi/4)$, define

$$a := e^{-i\theta}\sqrt{\tan\left(\frac{\pi}{4} - \theta\right)}, \qquad b := 0, \qquad c := \sqrt{\cos 2\theta}.$$

Lemma 3.2. *The points a, b, c are the vertices of a hyperbolic triangle in D with corresponding interior angles $\pi/2$, θ, θ.*

Proof. Note that $|a|^2 < 1$ and $|c|^2 < 1$, so $a, b, c \in D$. Since $b = 0$, we have $\angle b = \arg(c) - \arg(a) = \theta$. The hyperbolic law of cosines gives $\cosh d(a,c) = \cot\theta$. A formula for the cosines of the angles in terms of the side lengths of a hyperbolic triangle gives $\cos(\angle a) = 0$ and $\cos(\angle c) = \cos\theta$, so $\angle a = \pi/2$ and $\angle c = \theta$. □

Set $\theta := \pi/23$. Let Δ be the triangle group generated by counterclockwise hyperbolic rotations by angles $2\pi/2$, $2\pi/23$, $2\pi/23$ around a, b, c:

$$\Delta := \langle\, \delta_a, \delta_b, \delta_c \mid \delta_a^2 = \delta_b^{23} = \delta_c^{23} = \delta_a\delta_b\delta_c = 1 \,\rangle.$$

Let $\psi\colon \Delta \to M_{23}$ be the surjection sending $\delta_a, \delta_b, \delta_c$ to g_1, g_2, g_3, respectively. Let $\Gamma := \psi^{-1}(\mathrm{Stab}_{M_{23}}(1)) \leq \Delta$. Then $\Gamma\backslash D \to \Delta\backslash D$ is the desired cover $X_{\mathbb{C}} \xrightarrow{t} \mathbb{P}^1_{\mathbb{C}}$ with monodromy given by (g_1, g_2, g_3). Let a', b', c' be the images of a, b, c under $D \twoheadrightarrow X_{\mathbb{C}}$. The map $D \twoheadrightarrow X_{\mathbb{C}}$ is unramified at b since the ramification indices of b and b' over $\mathbb{P}^1$ are both 23. Thus q corresponds to an analytic uniformizer at $b' \in X_{\mathbb{C}}$.

A basis of $\mathrm{H}^0(X_{\mathbb{C}}, \Omega^1)$ pulls back to a 4-tuple $(f_0\, dq, \ldots, f_3\, dq)$ for some $f_0, \ldots, f_3 \in \mathbb{C}[[q]]$. Given (g_1, g_2, g_3) and $n \geq 1$, the algorithm in [KMSV14], inspired by work of Hejhal [Hej99] and Stark [Sta84], computes the first n coefficients of each f_i numerically. The BelyiDB Magma package [MSSV19] implements this algorithm. We run it! Below, we work numerically without controlling errors, so the intermediate steps of the calculation are not rigorous, but we return to rigor at the end by verifying algebraically that the claimed polynomials define M_{23}-extensions of $\mathbb{Q}$ and a regular M_{23}-extension of $\mathbb{Q}(t)$.

[3] Our convention is that S_{23} acts on the left on $\{1, \ldots, 23\}$, but Magma has S_{23} acting on the right.

We echelonize the basis. This calculation shows that no nonzero 1-form vanishes at b' to order greater than 3 (that is, b' is not a Weierstrass point). In other words, we obtain $f_i = q^i + O(q^4)$.

Lemma 3.3. *The genus 4 curve $X_{\mathbb{C}}$ is non-hyperelliptic.*

Proof. The dimension of the space of quadratic forms $P(x_0, \dots, x_3)$ vanishing at $(f_0 : \cdots : f_3)$ is $\binom{4-1}{2} = 3$ if $X_{\mathbb{C}}$ is hyperelliptic, and $\binom{4-2}{2} = 1$ otherwise [vBCPS26, Lemma 4.3]. We compute that the dimension is 1. $\square$

The canonical model of a non-hyperelliptic curve of genus 4 is a complete intersection $P = Q = 0$ in $\mathbb{P}^3$, where P and Q are homogeneous of degrees 2 and 3, respectively. To make P unique, not just up to a scalar, we require that its leading coefficient be 1 (with respect to some monomial order). To make Q unique, we require that Q be orthogonal to $x_0P, \dots, x_3P$ with respect to the Hermitian pairing associated to the monomial basis and require Q to have leading coefficient 1.

Since $|\mathrm{Ni}_{\mathfrak{c}}| = 7$, the cover $t\colon X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ associated to (g_1, g_2, g_3) is defined over a number field L of degree ≤ 7 over $\mathbb{Q}$. We expanded the 1-forms around the unique ramification point of $t\colon X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ above $\sqrt{-23} \in \mathbb{P}^1(L(\sqrt{-23}))$, so the theory says that P and Q have coefficients in $L(\sqrt{-23})$.

Using the PSLQ algorithm [FBA99], we recognize the coefficients of P and Q as algebraic numbers. Miraculously, they lie in $K := \mathbb{Q}(\sqrt{-23})$! The exact P and Q define a canonically embedded genus 4 curve $X_K \subset \mathbb{P}^3_K$. Evaluating $(f_0 : \cdots : f_3)$ at a, b, c gives $a', b', c' \in X_K(\mathbb{C}) \subset \mathbb{P}^3(\mathbb{C})$ with $b' = (1 : 0 : 0 : 0)$, and PSLQ recognizes $c' \in X_K(K) \subset \mathbb{P}^3(K)$.

From now on, our calculations are algebraic. We seek a morphism $t\colon X \to \mathbb{P}^1_{\mathbb{Q}}$ which is ramified over 0, $\sqrt{-23}$, $-\sqrt{-23}$, with ramification index 23 above $\pm\sqrt{-23}$. First we will construct a variant morphism u ramified over $1, 0, \infty$ instead. A Riemann–Roch space computation produces $u \in K(X_K)$ such that $\operatorname{div}(u) = 23b' - 23c'$. We compute the zeros of du other than b' (the 8 points with ramification index 2) and impose the condition that u maps one of them to 1, to obtain the correct scaling of u. Let $\alpha \in \operatorname{Aut}(\mathbb{P}^1_K)$ send $1, 0, \infty$ to $0, \sqrt{-23}, -\sqrt{-23}$, respectively. We compute $t = \alpha \circ u$.

We seek a second rational function $v \in K(X_K)$ such that $\mathbb{Q}(t, v)$ is the function field of a curve X over $\mathbb{Q}$ whose base change is X_K. Then the minimal polynomial of v over $\mathbb{Q}(t)$ is the degree 23 polynomial whose splitting field is a regular M_{23}-extension of $\mathbb{Q}(t)$.

Let σ be the generator of $\operatorname{Gal}(K/\mathbb{Q})$, which acts also on $K(t)$, fixing t. The K-vector space $L(5b' - c')$ turns out to be 1-dimensional, and a Riemann–Roch space computation produces a nonzero function y in it. We have $\deg y = 5$. By linear algebra, we find $H(T, Y) \in K[T, Y]$ with $\deg_T H = 5$ and $\deg_Y H = 23$ such that $H(t, y) = 0$. We factor ${}^{\sigma}H(t, Y)$ over $K(X_K) = K(t, y)$ and find $y' \in K(X_K)$ such that $({}^{\sigma}H)(t, y') = 0$. This y' is consistent with equaling ${}^{\sigma}y$ with respect to the intended $\mathbb{Q}$-structure on X_K. Let $v = yy'$, which has polar divisor $4b' + 4c'$ and is hence of degree 8. We next compute a polynomial $F(T, V) \in \mathbb{Z}[T, V] \subset \mathbb{Q}[T, V]$ such that $F(t, v) = 0$, with $\deg_T F = 8$ and $\deg_V F = 23$; to carry this out, we do linear algebra modulo small primes, and reconstruct coefficients using the Chinese remainder theorem. Then $F(t, V) \in \mathbb{Q}(t)[V]$ is the desired degree 23 polynomial. This polynomial is available on the GitHub site mentioned in the footnote at the end of Section 1.1.

Remark 3.4. In principle, we could also find a function v of degree 4 instead of 8, which would reduce $\deg_T F$ to 4. To see this, let K_X be a canonical divisor on the $\mathbb{Q}$-model X.

Then $K_X - (b' + c')$ is a divisor of degree 4 defined over $\mathbb{Q}$. Since X is not hyperelliptic, $\dim L(b' + c') = 1$, so the Riemann–Roch theorem gives $\dim L(K_X - (b' + c')) = 2$. If j_1, j_2 is a $\mathbb{Q}$-basis, we can choose $v = j_1/j_2$.

In fact, degree 4 is best possible. The only nonconstant rational maps $X_{\mathbb{C}} \to \mathbb{P}^1_{\mathbb{C}}$ of degree ≤ 3 come from the rulings on the quadric $P = 0$. But the discriminant of P is not a square in K, so the rulings are not defined over K, let alone over $\mathbb{Q}$.

Let G_{geom} and G_{arith} be the geometric and arithmetic monodromy groups of $F \in \mathbb{Q}(t)[V]$. Thus $G_{\mathrm{geom}} \lhd G_{\mathrm{arith}} \le S_{23}$.

Proposition 3.5. *We have* $G_{\mathrm{geom}} = M_{23}$.

Proof. The local monodromy above each of $\pm\sqrt{-23}$ is a 23-cycle, and above 0 it has cycle type $1^7 2^8$. The classification of transitive groups of degree 23 then implies that $M_{23} \subseteq G_{\mathrm{geom}}$.

We calculate that the discriminant of $F \in \mathbb{Q}(t)[V]$ factors as $ct^8(t^2 + 23)^{88} h_{84}^2$ for some nonzero $c \in \mathbb{Z}$ and degree 84 irreducible polynomial $h_{84} \in \mathbb{Z}[t]$. (The presence of $h_{84}(t)$ reflects singularities of the plane model $F(T, V) = 0$, not actual ramification of $X \to \mathbb{P}^1_{\mathbb{Q}}$; we omit the proof since our argument does not rely on this.) Moreover, the extension defined by F is unramified above ∞. Let S' be the subscheme of $\mathbb{P}^1_{\mathbb{Z}}$ defined by $t(t^2 + 23)h_{84} = 0$. We check that $31 \nmid c$, and S' remains étale modulo 31. Also, $F \bmod 31$ defines a tame extension of $\mathbb{F}_{31}(t)$ since $31 > 23$. Let $G_{\mathrm{geom},31}$ and $G_{\mathrm{arith},31}$ be the geometric and arithmetic monodromy groups of $F \bmod 31$. The specialization map on tame fundamental groups of $\mathbb{P}^1 - S'$ is an isomorphism ([SGA71, XIII.2]; see also [OV00, Théorème 4.4]), so $G_{\mathrm{geom},31} = G_{\mathrm{geom}}$. Using Magma, we certify that $G_{\mathrm{arith},31} = M_{23}$. Thus $M_{23} \subseteq G_{\mathrm{geom}} = G_{\mathrm{geom},31} \subseteq G_{\mathrm{arith},31} = M_{23}$, so all are equal. □

Corollary 3.6. *We have* $G_{\mathrm{arith}} = M_{23}$.

Proof. By Proposition 3.5, $G_{\mathrm{geom}} = M_{23}$. The group G_{geom} is normal in G_{arith}, and M_{23} is not normal in any larger subgroup of S_{23}. □

By Proposition 3.5 and Corollary 3.6, since $G_{\mathrm{geom}} = G_{\mathrm{arith}}$, the splitting field of F over $\mathbb{Q}(t)$ is a regular extension with Galois group M_{23}. This proves Theorem 1.3.

Finally, we specialize t to rational numbers to obtain degree 23 polynomials over $\mathbb{Q}$ with Galois group M_{23}. Then we use the PARI/GP routines `polredabs` and `polredbest` [CDyD91, PAR25] to find lower-height monic polynomials in $\mathbb{Z}[x]$ defining the same degree 23 number field. This is how we produced the polynomial in Example 1.2.

Example 3.7. Here is another specialization, the one of lowest height we found so far:

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

Its splitting field is an M_{23}-extension of $\mathbb{Q}$ unramified outside $\{2, 7, 23\}$. We certified this with Magma as well.

Acknowledgments

We are very grateful to Michele Tarquini and Zhiyu Zhang for discussions when we were learning the theory and exploring approaches at the beginning of our project. We began this research at the May 27–30, 2026 workshop "AI and number theory" at the American Institute of Mathematics in collaboration with the Institute for Computer-Aided Reasoning in Mathematics. No text in this article was written by AI. We used Claude Fable 5, Claude Opus 4.8, and ChatGPT 5.6 Sol for searching the literature, code generation, testing hypotheses, ruling out other approaches, devising computational strategies, checking our results, and proofreading our manuscript. We thank Anthropic for providing each of us with a 3-month Claude Max subscription. Our final results were verified in Magma and PARI/GP without the use of AI.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993). MR 1484478 2

[Bel79] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*, Izv. Akad. Nauk SSSR Ser. Mat. **43** (1979), no. 2, 267–276, 479. MR 534593 2

[CDyD91] Henri Cohen and Francisco Diaz y Diaz, *A polynomial reduction algorithm*, Sém. Théor. Nombres Bordeaux (2) **3** (1991), no. 2, 351–360. MR 1149802 7

[CH85] Kevin Coombes and David Harbater, *Hurwitz families and arithmetic Galois groups*, Duke Math. J. **52** (1985), no. 4, 821–839. MR 816387 3

[DD97] Pierre Dèbes and Jean-Claude Douai, *Algebraic covers: field of moduli versus field of definition*, Ann. Sci. École Norm. Sup. (4) **30** (1997), no. 3, 303–338. MR 1443489 3

[Elk13] Noam D. Elkies, *The complex polynomials $P(x)$ with* $\mathrm{Gal}(P(x)-t) \cong M_{23}$, ANTS X—Proceedings of the Tenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 1, Math. Sci. Publ., Berkeley, CA, 2013, pp. 359–367. MR 3207422 2

[FBA99] Helaman R. P. Ferguson, David H. Bailey, and Steve Arno, *Analysis of PSLQ, an integer relation finding algorithm*, Mathematics of Computation **68** (1999), no. 225, 351–369. MR 1489971 6

[Fri77] M. Fried, *Fields of definition of function fields and Hurwitz families—groups as Galois groups*, Comm. Algebra **5** (1977), no. 1, 17–82. MR 453746 2

[FV91] Michael D. Fried and Helmut Völklein, *The inverse Galois problem and rational points on moduli spaces*, Math. Ann. **290** (1991), no. 4, 771–800. MR 1119950 2, 4

[Gra96] Louis Granboulan, *Construction d'une extension régulière de $\mathbf{Q}(T)$ de groupe de Galois M_{24}*, Experiment. Math. **5** (1996), no. 1, 3–14. MR 1412950 2

[Häf87] Frank Häfner, *Realisierung der Mathieugruppen M_{23} und M_{24} als Galoisgruppen*, Diplomarbeit, Universität Karlsruhe, Karlsruhe, 1987. 2

[Häf22] ———, *Braid orbits and the Mathieu group M_{23} as Galois group*, arXiv:2202.08222v3 [math.NT], 2022. 2

[Hej99] Dennis A. Hejhal, *On eigenfunctions of the Laplacian for Hecke triangle groups*, Emerging applications of number theory (Minneapolis, MN, 1996), IMA Vol. Math. Appl., vol. 109, Springer, New York, 1999, pp. 291–315. MR 1691537 5

[HS85] Gudrun Hoyden-Siedersleben, *Realisierung der Jankogruppen J_1 und J_2 als Galoisgruppen über* $\mathbf{Q}$, J. Algebra **97** (1985), no. 1, 17–22. MR 812166 2

[HSM86] Gudrun Hoyden-Siedersleben and B. Heinrich Matzat, *Realisierung sporadischer einfacher Gruppen als Galoisgruppen über Kreisteilungskörpern*, J. Algebra **101** (1986), no. 1, 273–286. MR 843705 2

[Hun86] David C. Hunt, *Rational rigidity and the sporadic groups*, J. Algebra **99** (1986), no. 2, 577–592. MR 837564 1, 2

[KMSV14] Michael Klug, Michael Musty, Sam Schiavone, and John Voight, *Numerical calculation of three-point branched covers of the projective line*, LMS J. Comput. Math. **17** (2014), no. 1, 379–430. MR 3356040 5

[Kön14] Joachim König, *The inverse Galois problem and explicit computation of families of covers of* $\mathbb{P}^1\mathbb{C}$ *with prescribed ramification*, Ph.D. thesis, 2014, `https://opus.bibliothek.uni-wuerzburg.de/opus4-wuerzburg/frontdoor/deliver/index/docId/10014/file/Koenig_Joachim_Dissertation.pdf`. 2

[Mal88] Gunter Malle, *Polynomials with Galois groups* $\mathrm{Aut}(M_{22})$*,* M_{22}*, and* $\mathrm{PSL}_3(\mathbf{F}_4)\cdot 2_2$ *over* $\mathbf{Q}$, Math. Comp. **51** (1988), no. 184, 761–768. MR 958642 2

[Mat79] B. Heinrich Matzat, *Konstruktion von Zahlkörpern mit der Galoisgruppe* M_{11} *über* $\mathbf{Q}(\sqrt{-11})$, Manuscripta Math. **27** (1979), no. 1, 103–111. MR 524980 2

[Mat84] ———, *Konstruktion von Zahl- und Funktionenkörpern mit vorgegebener Galoisgruppe*, J. Reine Angew. Math. **349** (1984), 179–220. MR 743971 2

[Mat85] ———, *Zwei Aspekte konstruktiver Galoistheorie*, J. Algebra **96** (1985), no. 2, 499–531. MR 810543 2

[Mat89] ———, *Rationality criteria for Galois extensions*, Galois groups over **Q** (Berkeley, CA, 1987), Math. Sci. Res. Inst. Publ., vol. 16, Springer, New York, 1989, pp. 361–383. MR 1012171 2

[Mat91] ———, *Zöpfe und Galoissche Gruppen*, J. Reine Angew. Math. **420** (1991), 99–159. MR 1124568 2

[MM18] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, second ed., Springer Monographs in Mathematics, Springer, Berlin, 2018. MR 3822366 1, 2

[MSSV19] Michael Musty, Sam Schiavone, Jeroen Sijsling, and John Voight, *A database of Belyi maps*, Proceedings of the Thirteenth Algorithmic Number Theory Symposium, Open Book Ser., vol. 2, Math. Sci. Publ., Berkeley, CA, 2019, pp. 375–392. MR 3952023 2, 5

[MZM86] B. Heinrich Matzat and Andreas Zeh-Marschke, *Realisierung der Mathieugruppen* M_{11} *und* M_{12} *als Galoisgruppen über* **Q**, J. Number Theory **23** (1986), no. 2, 195–202. MR 845901 2

[MZM87] ———, *Polynome mit der Galoisgruppe* M_{11} *über* **Q**, J. Symbolic Comput. **4** (1987), no. 1, 93–97. MR 908416 2

[OV00] Fabrice Orgogozo and Isabelle Vidal, *Le théorème de spécialisation du groupe fondamental*, Courbes semi-stables et groupe fondamental en géométrie algébrique (Luminy, 1998), Progr. Math., vol. 187, Birkhäuser, Basel, 2000, pp. 169–184. MR 1768100 7

[Pah88] H. Pahlings, *Some sporadic groups as Galois groups*, Rend. Sem. Mat. Univ. Padova **79** (1988), 97–107. MR 964023 2

[Pah89] ———, *Some sporadic groups as Galois groups. II*, Rend. Sem. Mat. Univ. Padova **82** (1989), 163–171, Errata corrige: Rend. Sem. Mat. Univ. Padova **85** (1991), 309–310, MR1142546, `http://www.numdam.org/item?id=RSMUP_1991__85__309_0`. MR 1049591 2

[PAR25] The PARI Group, Univ. Bordeaux, *PARI/GP version* `2.17.3`, 2025, available from `http://pari.math.u-bordeaux.fr/`. 7

[Seg] Béranger Seguin, *Fields of definition of components of Hurwitz spaces*, Annali della Scuola Normale Superiore - Classe di Scienze, to appear, `https://doi.org/10.2422/2036-2145.202310_013`. 2

[Ser92] Jean-Pierre Serre, *Topics in Galois theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, Boston, MA, 1992, Lecture notes prepared by Henri Damon [Henri Darmon], With a foreword by Darmon and the author. MR 1162313 3, 4

[Ser97] ———, *Lectures on the Mordell-Weil theorem*, third ed., Aspects of Mathematics, Friedr. Vieweg & Sohn, Braunschweig, 1997, With a foreword by Brown and Serre. MR 1757192 3

[SGA71] *Revêtements étales et groupe fondamental*, Lecture Notes in Mathematics, vol. Vol. 224, Springer-Verlag, Berlin-New York, 1971, Séminaire de Géométrie Algébrique du Bois Marie 1960–1961 (SGA 1), Dirigé par Alexandre Grothendieck. Augmenté de deux exposés de M. Raynaud. MR 354651 7

[Shi74] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120. MR 332725 2

[Sta84] H. M. Stark, *Fourier coefficients of Maass waveforms*, Modular forms (Durham, 1983), Ellis Horwood Ser. Math. Appl.: Statist. Oper. Res., Horwood, Chichester, 1984, pp. 263–269. MR 803370 5

[Tho84] John G. Thompson, *Some finite groups which appear as* $\mathrm{Gal}(L/K)$*, where* $K \subseteq \mathbf{Q}(\mu_n)$, J. Algebra **89** (1984), no. 2, 437–499. MR 751155 2

[vBCPS26] Raymond van Bommel, Edgar Costa, Bjorn Poonen, and Padmavathi Srinivasan, *Curve equations from expansions of 1-forms at a nonrational point*, LuCaNT: databases, algorithms, and computational number theory, Contemp. Math., vol. 840, Amer. Math. Soc., [Providence], RI, 2026, pp. 345–354. MR 5070733 6

Department of Mathematics, Temple University, Philadelphia, PA 19122, USA
Email address: xiaoyu.huang@temple.edu
URL: https://sites.google.com/view/xiaoyuhuang/home

Institute for Computer-Aided Reasoning in Mathematics, Carnegie Mellon University, Pittsburgh, PA 15213, USA
Email address: jackson@icarm.io
URL: https://www.blakejacksonmath.com/

Department of Mathematics, University of Connecticut, Storrs, CT 06269, USA
Korea Institute for Advanced Study, Seoul 02455, Republic of Korea
Email address: khlee@math.uconn.edu
URL: https://khlee-math.github.io/

Department of Mathematics, Massachusetts Institute of Technology, Cambridge, MA 02139-4307, USA
Email address: poonen@math.mit.edu
URL: http://math.mit.edu/~poonen/

Department of Mathematics, Colorado State University, Fort Collins, CO 80523, USA
Email address: pries@colostate.edu
URL: http://math.colostate.edu/~pries/

Department of Mathematics, California Institute of Technology, Pasadena, CA 91125, USA
Email address: szhang7@caltech.edu
URL: https://www.shaowuzhang.com/