THE GROUP $\mathrm{SL}_2(\mathbb{F}_{13})$ IS GALOIS OVER $\mathbb{Q}$

ERAY KARABIYIK

Abstract. In this paper, we prove that $\mathrm{SL}_2(\mathbb{F}_{13})$ occurs as a Galois group over $\mathbb{Q}$ and that the realizing extension can be chosen to be totally real. We start with an explicit totally real polynomial of degree 14 whose splitting field has Galois group $\mathrm{PSL}_2(\mathbb{F}_{13})$. After computing the ramification indices and residue numbers in the Galois closure, we use Böge's the central embedding problem from $\mathrm{PSL}_2(\mathbb{F}_l)$ to $\mathrm{SL}_2(\mathbb{F}_l)$.

1. Introduction

The inverse Galois problem asks whether every finite group is the Galois group of a finite Galois extension of $\mathbb{Q}$. The projective groups $\mathrm{PSL}_2(\mathbb{F}_p)$ are known to occur for every prime $p > 3$ [Zyw15]. Passing to the nonsplit central cover

$$1 \longrightarrow \{\pm I\} \longrightarrow \mathrm{SL}_2(\mathbb{F}_p) \longrightarrow \mathrm{PSL}_2(\mathbb{F}_p) \longrightarrow 1$$

is substantially subtler. For $p = 5$, Sonn realized $\mathrm{SL}_2(\mathbb{F}_5)$ over $\mathbb{Q}$ [Son80]. Mestre later gave a regular realization [Mes90] and Plans established the existence of a generic extension [Pla07]. Mestre constructed a regular realization for $p = 7$ [Mes94]. For $p = 11$, Klüners constructed a degree-24 polynomial over $\mathbb{Q}$, using class-field computations made under the generalized Riemann hypothesis, and separately proved a regular realization by an application of Mestre's theorem [Klü00]. Importantly, Uttenthal recorded the narrower absence of an explicit even irreducible representation, or equivalently an explicit totally real defining polynomial, at $p = 13$ [Utt25, Remark 20].

One obstruction to a standard explicit approach is visible in König's Hurwitz-space computation [Kön17]. For $\mathrm{PSL}_2(\mathbb{F}_{13})$, the only rational genus-zero-covering four-tuple has type $(2A, 2A, 2A, 3A)$, and its Hurwitz curve has genus one and rank zero. As mentioned by König, its rational points yield no cover with real fibres [Kön17, §7, closing Remark]. However, this does not rule out other Hurwitz-space constructions. Our family is of a different kind, in the natural degree-14 action of $\mathrm{PSL}_2(\mathbb{F}_{13})$ on $\mathbb{P}^1(\mathbb{F}_{13})$, an involution has cycle type $1^2 2^6$ and an element of order six has cycle type $1^2 6^2$, so the tuple $(2A, 2A, 2A, 6A)$ has ramification-index sum 28 and Riemann–Hurwitz gives covers of genus one, not genus zero.

Our main result is the following.

Theorem 1.1. *There is a totally real Galois extension $M/\mathbb{Q}$ such that*

$$\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{SL}_2(\mathbb{F}_{13}).$$

Theorem 1.1 initially settled the existence question but the argument did not itself give a degree 56 defining polynomial whose splitting field is M. We have continued our search and found an explicit degree 56 polynomial whose splitting field has Galois group $\mathrm{SL}_2(\mathbb{F}_{13}$. The polynomial is of 5,297,862 string length and it can be found in:

https://github.com/eekarabiyik/SL2F13.

The proof uses various computer algebra systems, mainly Sage, GAP and PARI. Starting only from the coefficients in (3.1), the main CAS certificate verifies the projective Galois group, computes the maximal order and every ramified local factorization. It then exhausts the required subgroup configurations inside $\mathrm{PSL}_2(\mathbb{F}_{13})$, and computes the trace-form invariants. A separate exact computation verifies the method we found the degree 14 polynomial. The final input is Böge's local–global criterion for the central embedding problem.

2010 *Mathematics Subject Classification.* Primary 14K15; Secondary 11F80.

1.1. **Acknowledgments.** I would like to thank Ravi Ramakrishna for introducing me to this problem many years ago. I would also like to thank David Zywina for inspiring me regarding Inverse Galois Problem. We have used ChatGPT 5.6 Sol and Claude Fable for finding the degree 14 polynomial 3.1 and especially for the generation of the computer algebra system scripts.

2. Böge's embedding criterion

As usual, we write e_q and f_q for the ramification index and residue degree at primes above q, where q is a rational prime in a finite Galois extension $L/\mathbb{Q}$.

Theorem 2.1 (Böge). *Let ℓ be a prime with $\ell \equiv 3$ or $5 \pmod 8$, and let $L/\mathbb{Q}$ be a Galois extension with group $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Then L embeds in a Galois extension $M/\mathbb{Q}$ with group $\mathrm{SL}_2(\mathbb{F}_\ell)$, compatibly with the standard central quotient, if and only if*

(1) L is totally real; and

(2) for every odd rational prime q for which e_q is even,

$$f_q \text{ is odd} \iff q \equiv 1 \pmod 4.$$

This is [Bög90, Satz 1, p. 153] in English. There is no hypothesis of tameness. The Satz 3 on in the paper treats arbitrary nondyadic Galois extensions of $\mathbb{Q}$. In particular, the criterion applies directly to the wild prime 3. Importantly, there is no separate condition at 2 after the infinite and odd local invariants vanish, Brauer–Hasse–Noether reciprocity forces the dyadic invariant to vanish.

3. The projective field

The polynomial below was found in a Hurwitz-space search by specializing the archived exact rational degree-14 family, whose branch-cycle shapes are $(2A, 2A, 2A, 6A)$ followed by PARI's exact `polredabs` reduction of the defining equation. The specialization was done at the parameter $T = 28040147150$. A seperate computation verifies the Belyi map used in the search, the rational family and its branch shapes, the specialization, and the equality of the reduced equation with the polynomial below. For the rest of the paper, this Hurwitz-space search play no role.

Consider the following monic polynomial:

$$\begin{aligned} f(x) = x^{14} &- 6x^{13} - 204840441x^{12} - 1119125930364x^{11} \\ &+ 4529702096707905x^{10} + 38159749624959546246x^{9} \\ &- 185460695747155700891 37x^{8} - 452968533089504837361085896x^{7} \\ &- 1926666991166847843513 37401333x^{6} + 2209557167547162714402116518030950x^{5} \\ &+ 14296168445224263309438957703242 25533x^{4} \\ &- 389992015243518145581296370004448 7447036x^{3} \\ &- 1769134263978452128562169254872450324635597x^{2} \\ &+ 17925481734760709327105593729555826 67141406554x \\ &+ 825828856675546377159985433494767986559465932589 \end{aligned} \tag{3.1}$$

Proposition 3.1. *The polynomial f is irreducible and has fourteen real roots. Its splitting field L has*

$$\mathrm{Gal}(L/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{F}_{13})$$

in its natural degree-14 action.

Proof. Modulo prime 5, finite-field factorization gives a squarefree product of two irreducible factors of degree 7. Modulo 23 one has the squarefree factorization

$$\begin{aligned} f(x) \equiv (x+8)(x^{13} &+ 9x^{12} + 17x^{11} + 19x^{10} + 5x^{9} + 15x^{8} \\ &+ 6x^{7} + 16x^{6} + 19x^{5} + 15x^{4} + 12x^{3} + 4x^{2} + 21x + 7). \end{aligned}$$

The factor of degree 13 is irreducible over $\mathbb{F}_{23}$. If the monic polynomial f had a proper factor over $\mathbb{Q}$, Gauss's lemma and reduction modulo 5 would force such a factor to have degree 7, whereas reduction modulo 23 would force its degree to be 1 or 13. Hence f is irreducible. We also verify that its discriminant is a nonzero square in $\mathbb{Q}$ in Sage, so its Galois group G is a transitive subgroup of A_{14}. Let $K = \mathbb{Q}(\alpha)$ with α a root of f. Since the reduction modulo 23 is squarefree, $23 \nmid \operatorname{disc}(f)$ and in particular $23 \nmid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Dedekind's theorem therefore gives us a Frobenius cycle type $(1)(13)$ in G.

The 63 conjugacy classes of transitive subgroups of S_{14} are classified in [But93]. They are also available in the GAP transitive-group library [The26, Hul23]. We check them and see that the only even transitive groups of degree 14 whose orders are divisible by 13 are

$$14T30 \cong \mathrm{PSL}_2(\mathbb{F}_{13}) \quad \text{and} \quad 14T62 = A_{14}.$$

So we are left with showing that G is not A_{14}. We do this by comparing how the two groups act on the $\binom{14}{3} = 364$ unordered triples of roots.

Let $r_1, \dots, r_{14}$ be the roots of f. To each three-element set $\{i, j, k\}$ attach the sum $r_i + r_j + r_k$, and put all these sums into one polynomial

$$R_3(y) = \prod_{1 \leqslant i < j < k \leqslant 14} \big(y - (r_i + r_j + r_k)\big).$$

i.e., the triple-sum resolvent. We compute it exactly from the coefficients of f with no numerical approximation of any of the roots.

If $s_m = \sum_i r_i^m$ and

$$P_a(z) = \sum_{m=0}^{364} \frac{a^m s_m}{m!} z^m,$$

then, modulo z^{365},

$$\sum_{i<j<k} \exp\big((r_i + r_j + r_k)z\big) = \frac{P_1(z)^3 - 3P_1(z)P_2(z) + 2P_3(z)}{6}.$$

All equalities here are taken modulo z^{365}. Newton identities compute $s_1, \dots, s_{364}$ directly from f. For the sum, $m!$ times the coefficient of z^m is

$$\sum_{i<j<k} (r_i + r_j + r_k)^m,$$

the m-th power sum of the 364 roots of R_3. Applying Newton identities a second time therefore reconstructs every coefficient of R_3.

Each coefficient of R_3 is a symmetric polynomial with integer coefficients in $r_1, \dots, r_{14}$. The fundamental theorem of symmetric polynomials expresses it as an integer polynomial in the elementary symmetric functions of the r_i and consequently $R_3 \in \mathbb{Z}[y]$.

We show, using Sage, that R_3 is squarefree and is the product of two irreducible polynomials over $\mathbb{Q}$, each of degree 182. Thus

$$\{i, j, k\} \longmapsto r_i + r_j + r_k$$

is a G-equivariant bijection from the three-subsets of the roots to the roots of R_3. Under this bijection, the irreducible factors of R_3 correspond exactly to the G-orbits. Hence G has two orbits, both of size 182, on the three-subsets.

The group A_{14} is transitive on all 364 three-subsets. In contrast, the natural degree-14 action of $\mathrm{PSL}_2(\mathbb{F}_{13})$ has precisely two orbits of size 182. As a result, we conclude that $G \cong \mathrm{PSL}_2(\mathbb{F}_{13})$ in its natural action. Finally, an exact Sturm-sequence calculation proves that all fourteen roots of f are real. $\square$

Because every root of f is real, its splitting field L is totally real. Thus the first condition of Theorem 2.1 already holds.

4. Ramification and the local obstruction

Let $\mathsf{K} = \mathbb{Q}(\alpha)$ for a root α of f. Put

$$p_1 = 1854089821344611, \qquad p_2 = 2086114950053051.$$

Computing the maximal order using Sage and PARI, we have

$$\operatorname{disc}(\mathsf{K}) = 2^{22}3^{22}13^6 5119^6 p_1^6 p_2^6. \tag{4.1}$$

For a ramified rational prime q, let

$$S_q = [(e_i, f_i)]_i$$

be the prime-ideal factorization signature in K, and let d_i be the corresponding exponents of the local different. The complete calculation is shown in Table 1. The inertia group and the decomposition group data can be seen as well.

q	S_q	$(d_i)_i$	(I, D)	(e_q, f_q)
2	$(1,2),(6,1)^2$	$0,11,11$	—	not needed
3	$(2,1),(3,2),(6,1)$	$1,5,11$	(S_3, D_{12})	$(6,2)$
13	$(1,1)^2,(2,3)^2$	$0,0,1,1$	(C_2, C_6)	$(2,3)$
$5119, p_1, p_2$	$(1,2),(2,1)^2,(2,2)^2$	$0,1,1,1,1$	$(C_2, C_2 \times C_2)$	$(2,2)$

Table 1. Maximal-order data in K and the recovered inertia and decomposition data in L. Here D_{12} is the dihedral group of order 12.

We justify both the completeness of the table and the passage from the degree-14 stem to the Galois closure.

Lemma 4.1. *The rational primes in (4.1) are exactly the primes ramified in* L. *At every odd ramified prime, the full pair* (e_q, f_q) *is the one shown in Table 1.*

Proof. Let B be a point stabilizer in the natural degree-14 action of $G = \mathrm{PSL}_2(\mathbb{F}_{13})$ which means that $\mathsf{K} = \mathsf{L}^B$. Using Sage, we compute the maximal order of K, its discriminant, and the factorizations of the ramified primes. This gives precisely the signatures displayed in Table 1.

Now fix a prime of L above q, with inertia and decomposition groups $I \triangleleft D$. The primes of K above q are described by the D-orbits on the fourteen points, while the I-orbits inside them record the ramification indices and residue degrees. A GAP computation enumerates all pairs $I \triangleleft D \leqslant G$ and compares their orbit data with the computed signatures. The only matches give

$$(e_q, f_q) = (6,2), \quad (2,3), \quad (2,2)$$

for $q = 3$, $q = 13$, and $q = 5119, p_1, p_2$, respectively, with the group structures shown in the table.

Finally, a prime ramified in K is certainly ramified in L. Conversely, if q ramified in L but not in K, its nontrivial inertia group would fix all fourteen points. This is impossible because the degree-14 action of G is faithful. Hence the table is complete. □

We now check Böge's condition. At every odd ramified prime the full inertia index is even, and Table 1 gives

q	3	13	5119	p_1	p_2
f_q	2	3	2	2	2
$q \bmod 4$	3	1	3	3	3.

Thus

$$f_q \text{ is odd} \iff q \equiv 1 \pmod 4$$

at every required prime.

Proof of Theorem 1.1. The extension $L/\mathbb{Q}$ of Proposition 3.1 is totally real and has group $\mathrm{PSL}_2(\mathbb{F}_{13})$. Lemma 4.1 verifies the finite local condition in Theorem 2.1, and $13 \equiv 5 \pmod 8$. Böge's theorem therefore gives a Galois extension $M/\mathbb{Q}$ containing L and compatible with

$$1 \longrightarrow \{\pm I\} \longrightarrow \mathrm{SL}_2(\mathbb{F}_{13}) \longrightarrow \mathrm{PSL}_2(\mathbb{F}_{13}) \longrightarrow 1.$$

Consequently $\mathrm{Gal}(M/\mathbb{Q}) \cong \mathrm{SL}_2(\mathbb{F}_{13})$.

It remains to show that M is totally real. Let $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, and let $\rho\colon G_{\mathbb{Q}} \twoheadrightarrow \mathrm{SL}_2(\mathbb{F}_{13})$ be the map just obtained. Since L is totally real, complex conjugation c has $\rho(c) \in \{\pm I\}$. If $\rho(c) = I$, let χ be the trivial character and if $\rho(c) = -I$, choose any imaginary quadratic character $\chi\colon G_{\mathbb{Q}} \to \{\pm I\}$. In either case put $\rho^{\chi} = \chi\rho$. Its projectivization is unchanged and $\rho^{\chi}(c) = I$.

This twist is still surjective. Any subgroup of $\mathrm{SL}_2(\mathbb{F}_{13})$ mapping onto $\mathrm{PSL}_2(\mathbb{F}_{13})$ is either the whole group or a complement to the center, and the latter would have index 2 which would contradict the perfectness of $\mathrm{SL}_2(\mathbb{F}_{13})$ [Zyw24, Lemma 7.7(i)]. Let M_{χ} be the fixed field of $\ker(\rho^{\chi})$. All complex conjugations in $G_{\mathbb{Q}}$ are conjugate, and this kernel is normal; hence every complex conjugation acts trivially on M_{χ}. Thus $M_{\chi}/\mathbb{Q}$ is a totally real $\mathrm{SL}_2(\mathbb{F}_{13})$-extension.

□

5. Reproducibility

Every script and related data can be found in

https://github.com/eekarabiyik/SL2F13.

References

[Bög90] Sigrid Böge, *Witt-Invariante und ein gewisses Einbettungsproblem*, Journal für die reine und angewandte Mathematik **410** (1990), 153–159. ↑2

[But93] Gregory Butler, *The transitive groups of degree fourteen and fifteen*, Journal of Symbolic Computation **16** (1993), no. 5, 413–422. ↑3

[Hul23] Alexander Hulpke, *TransGrp: Transitive groups library*, 2023. Version 3.6.5. ↑3

[Klü00] Jürgen Klüners, *A polynomial with Galois group* $\mathrm{SL}_2(11)$, Journal of Symbolic Computation **30** (2000), no. 6, 733–737. ↑1

[Kön17] Joachim König, *Computation of Hurwitz spaces and new explicit polynomials for almost simple Galois groups*, Mathematics of Computation **86** (2017), no. 305, 1473–1498, available at 1512.05533. ↑1

[Mes90] Jean-François Mestre, *Extensions régulières de* $\mathbf{Q}(T)$ *de groupe de Galois* $\widetilde{A}_n$, Journal of Algebra **131** (1990), no. 2, 483–495. ↑1

[Mes94] ______, *Construction d'extensions régulières de* $\mathbf{Q}(T)$ *à groupes de Galois* $\mathrm{SL}_2(\mathbf{F}_7)$ *et* $\widetilde{M}_{12}$, Comptes rendus de l'Académie des sciences. Série I, Mathématique **319** (1994), no. 8, 781–782. ↑1

[Pla07] Bernat Plans, *Generic Galois extensions for* $\mathrm{SL}_2(\mathbf{F}_5)$ *over* $\mathbf{Q}$, Mathematical Research Letters **14** (2007), no. 3, 443–452. ↑1

[Son80] Jack Sonn, $\mathrm{SL}(2,5)$ *and Frobenius Galois groups over* $\mathbf{Q}$, Canadian Journal of Mathematics **32** (1980), no. 2, 281–293. ↑1

[The26] The GAP Group, *GAP—groups, algorithms, and programming*, 2026. Official release 4.16.0; the certificate transcript records and checks the runtime version and the loaded TransGrp version. ↑3

[Utt25] Peter Vang Uttenthal, *Level-raising of even representations of tetrahedral type and equidistribution of lines in the projective plane*, 2025. arXiv:2310.14352, version 2, 22 December 2025. ↑1

[Zyw15] David Zywina, *The inverse Galois problem for* $\mathrm{PSL}_2(\mathbf{F}_p)$, Duke Mathematical Journal **164** (2015), no. 12, 2253–2292, available at 1303.3646. ↑1

[Zyw24] ______, *Explicit open images for elliptic curves over* $\mathbf{Q}$, 2024. Version 2, 22 March 2024. ↑5

Hetao Institute of Mathematics and Interdisciplinary Sciences, Shenzhen, China

Email address: ek693@cornell.edu