INVERSE GALOIS PROBLEM FOR SMALL SIMPLE GROUPS

DAVID ZYWINA

ABSTRACT. In this short note, we list all simple groups with cardinality at most a hundred million that are not known to occur as the Galois group of an extension of $\mathbb{Q}$.

Recall that the Inverse Galois Problem (IGP) asks whether every finite group G occurs as the Galois group of some Galois extension of $\mathbb{Q}$. We will focus on the fundamental case where G is simple.

Let G be a non-abelian simple group with cardinality at most 10^8 (note that the IGP is known for abelian groups).

The following is a list of possibilities for those G of the form $\mathrm{PSL}_2(\mathbb{F}_q)$:

- $\mathrm{PSL}_2(\mathbb{F}_p)$ where $2 \le p \le 577$ is a prime [Zyw12] (earlier results of Shih and Malle cover the cases $p \notin \{311, 479\}$)
- $\mathrm{PSL}_2(\mathbb{F}_{p^2})$ where p is a prime such $2 \le p \le 23$ [Shi04, DV00]
- $\mathrm{PSL}_3(\mathbb{F}_{2^3})$ [Mat87]
- $\mathrm{PSL}_2(\mathbb{F}_{2^n})$ with $4 \le n \le 8$ [Wie05]
- $\mathrm{PSL}_2(\mathbb{F}_{3^3})$, $\mathrm{PSL}_2(\mathbb{F}_{3^4})$, $\mathrm{PSL}_2(\mathbb{F}_{3^5})$
- $\mathrm{PSL}_2(\mathbb{F}_{5^3})$
- $\mathrm{PSL}_2(\mathbb{F}_{7^3})$

Those groups for which the inverse Galois problem is known, we have given a reference. Those groups without a reference, and in blue, have not been realized as a Galois extension of $\mathbb{Q}$ (at least as far as the author is aware[1]).

Disclaimer: I have only given the most convenient reference, and have not tried to find the first occurrence in the literature or assign credit. The goal of this note is not to summarize what has been done, but to determine which small cases of the IGP still remain open.

We now list those G that are not of the form $\mathrm{PSL}_2(\mathbb{F}_q)$. For a statement of the classification of finite simple groups, see [CCN+85].

- $\mathfrak{A}_7$ [Ser08, §4.4]
- $\mathrm{PSL}_3(\mathbb{F}_3)$ [Rei99]
- $\mathrm{PSU}_3(\mathbb{F}_3)$ [Rei99]
- Mathieu group M_{11} [MM99, II §9]
- $\mathfrak{A}_8$ [Ser08, §4.4]
- $\mathrm{PSL}_3(\mathbb{F}_4)$ (cf. §1 below)
- $\mathrm{PSU}_4(\mathbb{F}_2) \cong \mathrm{PSp}_4(\mathbb{F}_3)$ [Rei99]
- Suzuki group ${}^2B_2(8)$
- $\mathrm{PSU}_3(\mathbb{F}_4)$
- Mathieu group M_{12} [MM99, II §9]
- $\mathrm{PSU}_3(\mathbb{F}_5)$
- Janko group J_1 [MM99, II §9]
- $\mathfrak{A}_9$ [Ser08, §4.4]
- $\mathrm{PSL}_3(\mathbb{F}_5)$ [Rei99]

[1]Any additional information would be greatly appreciated.

- Mathieu group M_{22} [MM99, II §9]
- Janko group J_2 [MM99, II §9]
- $\mathrm{PSp}_4(\mathbb{F}_4)$ [Shi03]
- $\mathrm{Sp}_6(\mathbb{F}_2)$ [Rei99]
- $\mathfrak{A}_{10}$ [Ser08, §4.4]
- $\mathrm{PSL}_3(\mathbb{F}_7)$
- $\mathrm{PSU}_4(\mathbb{F}_3)$ [Shi03]
- $G_2(\mathbb{F}_3)$ [MM99, II §8.1]
- $\mathrm{PSp}_4(\mathbb{F}_5)$ [Rei99]
- $\mathrm{PSU}_3(\mathbb{F}_8)$
- $\mathrm{PSU}_3(\mathbb{F}_7)$ [Rei99]
- $\mathrm{PSL}_4(\mathbb{F}_3)$ [Rei99]
- $\mathrm{PSL}_5(\mathbb{F}_2)$ [Kön13]
- Mathieu group M_{23}
- $\mathrm{PSU}_5(\mathbb{F}_2)$ [Shi03]
- $\mathrm{PSL}_3(\mathbb{F}_8)$
- Tits group ${}^2F_4(2)'$ [Shi03]
- $\mathfrak{A}_{11}$ [Ser08, §4.4]
- Suzuki group ${}^2B_2(32)$
- $\mathrm{PSL}_3(\mathbb{F}_9)$ [Shi03]
- $\mathrm{PSU}_3(\mathbb{F}_9)$
- Higman–Sims group HS [MM99, II §9]
- Janko group J_3 [MM99, II §9]
- $\mathrm{PSU}_3(\mathbb{F}_{11})$ [Mal90]

Finally, we summarize the open cases. The following is the list of simple groups G with cardinality at most 10^8 for which it is currently unknown if there is a Galois extension of $\mathbb{Q}$ with Galois group G. (For each group, we also give its cardinality.)

- $\mathrm{PSL}_2(\mathbb{F}_{3^3})$, 9828
- ${}^2B_2(8)$, 29120
- $\mathrm{PSU}_3(\mathbb{F}_4)$, 62400
- $\mathrm{PSU}_3(\mathbb{F}_5)$, 126000
- $\mathrm{PSL}_2(\mathbb{F}_{3^4})$, 265680
- $\mathrm{PSL}_2(\mathbb{F}_{5^3})$, 976500
- $\mathrm{PSL}_3(\mathbb{F}_7)$, 1876896
- $\mathrm{PSU}_3(\mathbb{F}_8)$, 5515776
- $\mathrm{PSL}_2(\mathbb{F}_{3^5})$, 7174332
- M_{23}, 10200960
- $\mathrm{PSL}_3(\mathbb{F}_8)$, 16482816
- $\mathrm{PSL}_2(\mathbb{F}_{7^3})$, 20176632
- ${}^2B_2(32)$, 32537600
- $\mathrm{PSU}_3(\mathbb{F}_9)$, 42573600

1. Realization of $\mathrm{PSL}_3(\mathbb{F}_4)$ as a Galois group

In this section, using the work of G. Malle, we give a polynomial in $\mathbb{Q}[x]$ whose splitting field over $\mathbb{Q}$ has Galois group $\mathrm{PSL}_3(\mathbb{F}_4)$. The group $\mathrm{PSL}_3(\mathbb{F}_4)$ is simple with cardinality 20160.

Define the polynomials $q(x) := 11(39x^8+280x^7+4092x^6-4136x^5+110594x^4-146168x^3+984940x^2-734712x+2668655)$ and $p(x) := 29x^7-165x^6-539x^5+363x^4-12705x^3+3993x^2-35937x-49247$ in $\mathbb{Q}[x]$, and the polynomial

$$h(x,t) := \big(p(x)^2q(x)(t^2+11)^{11} - p(t)^2q(t)(x^2+11)^{11}\big)/(x-t) \in \mathbb{Q}(t)[x].$$

Malle proved that the Galois group of $h(x,t)$ over $\mathbb{Q}(t)$ is isomorphic to $H := \mathrm{PSL}_3(\mathbb{F}_4)\cdot 2_2$ [Mal88, Theorem 3] (the notation for H is described in [CCN+85]). The group H has $\mathrm{PSL}_3(\mathbb{F}_4)$ as a normal subgroup of index 2.

In the splitting field of $h(x,t)$ over $\mathbb{Q}(t)$, the degree 2 extension of $\mathbb{Q}(t)$ corresponding to the subgroup $\mathrm{PSL}_3(\mathbb{F}_4)$ equals $\mathbb{Q}(t,T)$ where T satisfies $T^2 = q(t)$, cf. [Mal88, Prop. 2]. The (projective) curve defined by $T^2 = q(t)$ has genus 3 and hence has only a finite number of rational points. We found the rational points $(t,T) = (1,\pm 5632)$ for the equation $T^2 = q(t)$ which were overlooked in [Mal88]. Thus the Galois group G of the (separable) polynomial $f(x) := h(x,1) \in \mathbb{Q}[x]$ can be identified with a subgroup of $\mathrm{PSL}_3(\mathbb{F}_4)$.

The polynomial $f(x)$ has degree 21 and its leading coefficient is divisible only by the primes 2, 11, 6011 and 48481. The discriminant of $f(x)$ equals $2^{1700}\cdot 3^{200}\cdot 11^{230}\cdot 23^{12}\cdot 67^{28}$. One can check that $f(x)$ mod 5 factors into four irreducible polynomials of degree 5 and

one linear term, and that $f(x)$ mod 31 factors into three irreducible polynomials of degree 7. Therefore, G contains elements of order 5 and of order 7. However, no maximal subgroup of $\mathrm{PSL}_3(\mathbb{F}_4)$ has cardinality divisible by $5 \cdot 7 = 35$. Therefore, $G \cong \mathrm{PSL}_3(\mathbb{F}_4)$.

Acknowledgments. Thanks to Joachim König for informing me about his paper [Kön13].

References

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray. MR827219 (88g:20025) ↑1, 2

[DV00] Luis Dieulefait and Núria Vila, *Projective linear groups as Galois groups over* **Q** *via modular representations*, J. Symbolic Comput. **30** (2000), no. 6, 799–810. Algorithmic methods in Galois theory. MR1800679 (2001k:11093) ↑1

[Kön13] Joachim König, *A family of polynomials with Galois group* $PSL_5(2)$ *over* $\mathbb{Q}(t)$ (2013), available at arXiv:1308.1566. ↑2, 3

[Mal88] Gunter Malle, *Polynomials with Galois groups* $\mathrm{Aut}(M_{22})$, M_{22}, *and* $\mathrm{PSL}_3(\mathbf{F}_4) \cdot 2_2$ *over* **Q**, Math. Comp. **51** (1988), no. 184, 761–768. MR958642 (90h:12008) ↑2

[Mal90] ———, *Some unitary groups as Galois groups over* **Q**, J. Algebra **131** (1990), no. 2, 476–482. MR1058559 (91i:12004) ↑2

[Mat87] B. Heinrich Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Mathematics, vol. 1284, Springer-Verlag, Berlin, 1987. MR1004467 (91a:12007) ↑1

[MM99] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999. MR1711577 (2000k:12004) ↑1, 2

[Rei99] Stefan Reiter, *Galoisrealisierungen klassischer Gruppen*, J. Reine Angew. Math. **511** (1999), 193–236. MR1695795 (2000f:12003) ↑1, 2

[Ser08] Jean-Pierre Serre, *Topics in Galois theory*, Second, Research Notes in Mathematics, vol. 1, A K Peters Ltd., Wellesley, MA, 2008. With notes by Henri Darmon. MR2363329 (2008i:12010) ↑1, 2

[Shi03] Takehito Shiina, *Rigid braid orbits related to* $\mathrm{PSL}_2(p^2)$ *and some simple groups*, Tohoku Math. J. (2) **55** (2003), no. 2, 271–282. MR1979499 (2004d:12009) ↑2

[Shi04] ———, *Regular Galois realizations of* $\mathrm{PSL}_2(p^2)$ *over* $\mathbb{Q}(T)$, Galois theory and modular forms, 2004, pp. 125–142. MR2059760 (2005b:12011) ↑1

[Wie05] Gabor Wiese, *Modular forms of weight one over finite fields*, Ph.D. Thesis, 2005. http://math.uni.lu/~wiese/thesis/. ↑1

[Zyw12] David Zywina, *The inverse Galois problem for* $\mathrm{PSL}_2(\mathbb{F}_p)$, 2012. preprint. ↑1

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
E-mail address: zywina@math.cornell.edu
URL: http://www.math.cornell.edu/~zywina