mathematics

MDPI

Article

Seven Small Simple Groups Not Previously Known to Be Galois Over $\mathbb{Q}$

Luis Dieulefait *, Enric Florit and Núria Vila

Departament de Matemàtiques i Informàtica, University of Barcelona, 08007 Barcelona, Spain; enricflorit@ub.edu (E.F.); nuriavila@ub.edu (N.V.)
* Correspondence: ldieulefait@ub.edu

Abstract: In this note we realize seven small simple groups as Galois groups over $\mathbb{Q}$. The technique that we employ is the determination of the images of Galois representations attached to modular and automorphic forms, relying in two cases on recent results of Scholze on the existence of Galois representations attached to non-selfdual automorphic forms.

Keywords: Galois representations; modular forms; inverse Galois theory; automorphic forms; finite simple groups

MSC: 11F11; 11F12; 11F80; 12F12

Citation: Dieulefait, L.; Florit, E.; Vila, N. Seven Small Simple Groups Not Previously Known to Be Galois Over $\mathbb{Q}$. *Mathematics* **2022**, *10*, 2048. https://doi.org/10.3390/math10122048

Academic Editor: Yucai Su

Received: 6 April 2022
Accepted: 10 June 2022
Published: 13 June 2022

1. Preliminaries

In his note [1], David Zywina compiled a list of all simple groups up to a hundred million that are not yet known to be Galois groups over $\mathbb{Q}$. The list contains only 14 groups. Most of them are classical groups, and we noticed that the technique of determining the images of the Galois representations attached to modular and automorphic forms, a technique that we employed several years ago in the first named author's thesis (with the third named author as advisor) could be applied to prove that some of these groups are in fact Galois over $\mathbb{Q}$. We succeed in doing so for seven of the simple groups in Zywina's list. In this note we present the details of these computations.

Two-Dimensional Representations

We denote by $G_{\mathbb{Q}}$ the absolute Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Given a prime ℓ, we will write χ_ℓ for the mod ℓ cyclotomic character $G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$, sending each Frobenius element Frob_p to $p \pmod{\ell}$ for $p \neq \ell$.

For any ring R, we denote by $\mathrm{PSL}_2(R)$ and $\mathrm{PGL}_2(R)$ the respective quotients of $\mathrm{SL}_2(R)$ and $\mathrm{GL}_2(R)$ by their subgroup of scalar matrices. The determinant yields a short exact sequence

$$0 \to \mathrm{PSL}_2(R) \to \mathrm{PGL}_2(R) \overset{\det}{\to} R^\times/(R^\times)^2 \to 0,$$

so that an element of $\mathrm{PGL}_2(R)$ is in $\mathrm{PSL}_2(R)$ if and only if its determinant is a square.

Let $k > 1$ and $N \geq 1$ be positive integers, and let ψ be a primitive Dirichlet character. We consider newforms $f \in S_k(N, \psi)$ of weight k, level N, and nebentypus ψ. If the q-expansion of f is $f(\tau) = \sum_{n\geq 1} a_n q^n$, the extension $\mathbb{Q}_f$ of $\mathbb{Q}$ generated by all a_n is a number field, called the field of coefficients of f. Let $\mathcal{O}$ be its ring of integers.

For any prime ℓ, Deligne [2] constructs a continuous representation associated with f,

$$\rho_\ell : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O} \otimes \mathbb{Z}_\ell),$$

which is unramified at all primes $p \nmid \ell N$. Moreover, for any prime Λ in $\mathcal{O}$ above ℓ, we have a representation

$$\rho_\Lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}_\Lambda),$$

where $\mathcal{O}_\Lambda$ is the Λ-adic completion of $\mathcal{O}$, such that for all $p \nmid \ell N$,

$$\operatorname{trace}(\rho_\Lambda(\operatorname{Frob}_p)) = a_p \qquad \text{and} \qquad \det(\rho_\Lambda(\operatorname{Frob}_p)) = \psi(p)\chi_\ell^{k-1}(p).$$

We can compose ρ_Λ with the reduction modulo Λ to obtain a mod Λ representation $\bar{\rho}_\Lambda : G_\mathbb{Q} \to \operatorname{GL}_2(\mathcal{O}/\Lambda)$. Furthermore, we may projectivize $\bar{\rho}_\Lambda$ by quotienting out scalar matrices, yielding

$$\mathbb{P}(\bar{\rho}_\Lambda) : G_\mathbb{Q} \to \operatorname{PGL}_2(\mathcal{O}/\Lambda).$$

Our goal will be to determine the image of $\mathbb{P}(\bar{\rho}_\Lambda)$ for specific forms f and for certain primes Λ.

In our discussion, we shall need to look at the ramification of $\bar{\rho}_\Lambda$ at ℓ, that is, its restriction to an inertia group $I_\ell \subset G_\mathbb{Q}$, defined uniquely up to conjugacy. This is described by Theorem 2.5 in [3].

Theorem 1. *Fix a prime $\ell \geq k-1$ for which $\ell \nmid 2N$. Let Λ be a prime ideal of $\mathcal{O}$ dividing ℓ. Suppose $a_\ell \not\equiv 0 \pmod{\Lambda}$. After conjugating $\bar{\rho}_\Lambda$ by a matrix in $\operatorname{GL}_2(\mathcal{O}/\Lambda)$, we have*

$$\bar{\rho}_\Lambda|_{\mathcal{I}_\ell} = \begin{pmatrix} \chi_\ell^{k-1} & * \\ 0 & 1 \end{pmatrix}.$$

2. Realization of Groups $\mathbf{PSL_2}(\mathbb{F}_q)$ with $q = p^{2m+1}$

Let $k > 1$ be an odd positive integer, ψ a quadratic Dirichlet character, N a positive integer. We focus on newforms $f \in S_k(N, \psi)$ without CM having any nontrivial inner twists besides ψ. Ribet [4] proves that for every p not dividing the level N,

$$a_p(f) = a_p(f)^c \psi(p),$$

where c denotes complex conjugation. This implies that $f \otimes \psi^{-1} = f^c$. We denote by $\mathbb{Q}_f$ the field of coefficients of f. We shall also consider the subfield F_f of $\mathbb{Q}_f$ generated by $\{a_p^2/\psi(p)\}_p$.

We are going to use Theorem 3.1 from [5]. Let $\rho_\ell : G_\mathbb{Q} \to \operatorname{GL}_2(\mathcal{O}_\ell)$ be the ℓ-adic representation associated with f, where $\mathcal{O}_\ell = \mathcal{O} \otimes_\mathbb{Z} \mathbb{Z}_\ell$ and $\mathcal{O}$ is the ring of integers of $\mathbb{Q}_f$. Let

$$A_\ell = \{x \in \operatorname{GL}_2(R_\ell) \mid \det(x) = (\mathbb{Z}_\ell^\times)^{(k-1)}\}$$

where $R_\ell = R \otimes \mathbb{Z}_\ell$ and R is the ring of integers of F_f. Considering ψ as a character of $G_\mathbb{Q}$, we can consider its kernel H, and K the corresponding fixed field, which is a quadratic extension of $\mathbb{Q}$ in our case. If we set $H_\ell = \rho_\ell(H)$, Theorem 3.1 of Ribet [4] is as follows:

Theorem 2. *For all ℓ, we have the inclusion $H_\ell \subseteq A_\ell$, which is an equality for almost every prime ℓ.*

For each $g \in G_\mathbb{Q}$, there is some element $\alpha(g) \in \mathbb{Q}_f^\times$ such that $\alpha(g)^c = \psi(g)\alpha(g)$. We can choose the different $\alpha(g)$ independently of ℓ and only depending on the coset gH. The full image of the representation is then given by Theorem 4.1 in [5].

Theorem 3. *The image of ρ_ℓ is contained in the subgroup of $\operatorname{GL}_2(\mathcal{O}_\ell)$ generated by A_ℓ and the finite set of matrices*

$$\begin{pmatrix} \alpha(g) & 0 \\ 0 & \psi(g)/\alpha(g) \end{pmatrix}, \tag{1}$$

with $g \in G/H$. Moreover, the inclusion is an equality for all but finitely many primes ℓ.

Since ψ is quadratic and H has index 2, we can choose $g = \operatorname{Frob}_p$ for a prime p such that $\psi(p) = -1$ and $\alpha(\operatorname{Frob}_p) = a_p \neq 0$, so that $\alpha(g)$ generates $\mathbb{Q}_f$ and $\alpha(g)^2$ is in F_f.

Let Λ be a prime in $\mathbb{Q}_f$ lying over ℓ, and let $r = [\mathcal{O}/\Lambda : \mathbb{F}_\ell]$ be its inertia degree. We also let $\lambda = \Lambda \cap R$ and $r' = [R/\lambda : \mathbb{F}_\ell]$. We look at one of the induced representations associated with ρ_ℓ,

$$\bar{\rho}_\Lambda : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_{\ell^r}).$$

Recall that we are assuming f has odd weight k. Considering that for any $\Lambda \mid \ell$, the determinant of $\bar{\rho}_\Lambda|_H$ is χ_ℓ^{k-1} (a square in $\mathbb{F}_\ell$), and that $\bar{\rho}_\Lambda|_H$ is defined over $\mathbb{F}_{\ell^{r'}}$ by Theorem 2, we conclude that

$$\mathbb{P}(\bar{\rho}_\Lambda(H)) \subseteq \mathrm{PSL}_2(\mathbb{F}_{\ell^{r'}}).$$

We now have to impose conditions so that we also have $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q})) \subseteq \mathrm{PSL}_2(\mathbb{F}_{\ell^{r'}})$. By Theorem 3, the image $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q}))$ is generated by $\mathbb{P}(\bar{\rho}_\Lambda(H))$ and the class of a single matrix of the form in (1), which modulo scalars takes the form

$$\begin{pmatrix} \alpha(g)^2 & 0 \\ 0 & \psi(g) \end{pmatrix} = \begin{pmatrix} \alpha(g)^2 & 0 \\ 0 & -1 \end{pmatrix} =: M_g.$$

The matrix M_g is now in $\mathrm{PGL}_2(\mathbb{F}_{\ell^{r'}})$ by the choice of $\alpha(g)$. For it to be in $\mathrm{PSL}_2(\mathbb{F}_{\ell^{r'}})$, we only need

$$\det(M_g) = -\alpha(g)^2 \pmod{\lambda}$$

to be a square in $\mathbb{F}_{\ell^{r'}}$. We assume from now on that r' is odd and $\ell \neq 2$.

Theorem 4. *If ℓ and λ satisfy one of the following conditions:*

1. $\ell \equiv 1 \pmod 4$ *and λ is split in $\mathbb{Q}_f/F_f$;*
2. $\ell \equiv 3 \pmod 4$ *and λ is inert in $\mathbb{Q}_f/F_f$, and $\overline{a_p} \notin \mathbb{F}_{\ell^{r'}}$ where p is a prime with $\psi(p) = -1$;*

then we have $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q})) \subseteq \mathrm{PSL}_2(\mathbb{F}_{\ell^{r'}})$.

Proof. Case 1: $\ell \equiv 1 \pmod 4$. In this case -1 is a square in $\mathbb{F}_{\ell^{r'}}$, and we need a_p^2 to be a square in $\mathbb{F}_{\ell^{r'}}$. That is, it is enough that $\overline{a_p}$ is in $\mathbb{F}_{\ell^{r'}}$. We recall that a_p is a generator of $\mathbb{Q}_f$, and thus we see that $\overline{a_p} \in \mathbb{F}_{\ell^{r'}}$ if λ is a split prime in $\mathbb{Q}_f/F_f$.

Case 2: $\ell \equiv 3 \pmod 4$. In this case -1 is not a square in $\mathbb{F}_{\ell^{r'}}$, and we need $\overline{a_p} \notin \mathbb{F}_{\ell^{r'}}$. This is satisfied as long as λ is an inert prime not dividing the conductor of the order of $\mathcal{O}$ generated by a_p. □

2.1. Discarding Possible Images

We have already proven how to achieve $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q})) \subseteq \mathrm{PSL}_2(\mathbb{F}_{\ell^{r'}})$ in cases where r' is odd using modular forms of odd weight. However, the image might be smaller in some cases which we now list.

Lemma 1. *From Dickson's work [6], the maximal subgroups of $\mathrm{PSL}_2(\mathbb{F}_q)$ with $q = p^r \geq 5$ are:*

- *Borel subgroups (i.e., conjugate to the subgroup of upper triangular matrices), corresponding to the case where $\bar{\rho}_\Lambda$ is reducible;*
- *Dihedral subgroups;*
- *S_4, when $q = p \equiv \pm 1 \pmod 8$;*
- *A_4, when $q = p \equiv 3, 5, 13, 27, 37 \pmod{40}$;*
- *A_5, when $q \equiv 1 \pmod{10}$, $\mathbb{F}_q = \mathbb{F}_p(\sqrt{5})$.*
- *$\mathrm{PSL}_2(\mathbb{F}_{p^s})$ and $\mathrm{PGL}_2(\mathbb{F}_{p^s})$, with $s \mid r$.*

The dihedral case corresponds to a subgroup which is the normalizer of a Cartan subgroup. Given a Cartan subgroup C and its normalizer N, we have that $[N : C] = 2$, and $\mathrm{trace}(g) = 0$ for all $g \in N \setminus C$.

To show the image of some representation $\mathbb{P}(\bar{\rho}_\Lambda)$ is equal to $\mathrm{PSL}_2(\mathbb{F}_{\ell^{r'}})$, we discard that the image is contained in one of the maximal subgroups as follows.

1. For the reducible case, we will usually be able to choose $k = \ell$, so that $\ell \geq k - 1$. This means χ_ℓ^{k-1} is the trivial character, and all our residual representations have diagonal entries equal to one when restricted to inertia by Theorem 1, as long as $a_\ell \not\equiv 0 \pmod{\Lambda}$. Hence the characters ψ_1, ψ_2 in the diagonal of $\bar{\rho}_\Lambda$ are unramified outside N. Whenever N is prime, and because the prime-to-ℓ part of the conductor of $\bar{\rho}_\Lambda$ divides N, one of these characters must be trivial and the other one has to be the nebentypus. Therefore, we have proved the following:

   Lemma 2. *Let f be a newform of prime level N, weight k, quadratic nebentypus ψ which is the single inner twist, and a prime ℓ for which Theorem 4 says $\bar{\rho}_\Lambda(G) \subseteq \mathrm{PSL}_2(\mathbb{F}_\lambda)$. If $\ell = k$ and $\ell \nmid 2N$, then $\bar{\rho}_\Lambda^{ss} \sim 1 \oplus \psi$.*

   This yields a contradiction once we find a prime p with $\psi(p) = -1$ and $a_p \not\equiv 0 \pmod{\Lambda}$. Alternatively, this gives a representation whose trace is defined over $\mathbb{F}_\ell$, while we may have examples of traces not in $\mathbb{F}_\ell$ as long as $\overline{a_p} \notin \mathbb{F}_\ell$.
2. After proving non-reducibility, we continue with the dihedral case (i.e., normalizer of Cartan). We can assume that the image is not inside a Cartan subgroup C because we have already dealt with the reducible case. To discard the image being in its normalizer N, one takes the nontrivial character

   $$G_{\mathbb{Q}} \to N \to N/C \cong \{\pm 1\},$$

   which is unramified outside ℓN because so is $\bar{\rho}_\Lambda$. Taking a Dirichlet character ε to concord with this character on Frobenius, there are finitely many primitive possible Dirichlet characters, with conductors dividing ℓN. It is a matter of finding some p with $\varepsilon(p) = -1$ and $a_p \not\equiv 0 \pmod{\ell}$. If $\varepsilon(p) = -1$, $g = \bar{\rho}_\ell(\mathrm{Frob}_p)$ is in $N \setminus C$, but for such matrices $\mathrm{trace}(g) = 0$, which does not happen.
3. The groups $\mathrm{PSL}_2(\mathbb{F}_{p^s})$, $\mathrm{PGL}_2(\mathbb{F}_{p^s})$, A_4, A_5 and S_4 are discarded by finding some element of large order. We can actually avoid considering the last three when R/λ is a nontrivial odd extension of $\mathbb{F}_\ell$ because of Dickson's congruences.

With these steps, we are able to show the following.

Theorem 5. *The groups $\mathrm{PSL}_2(\mathbb{F}_{5^3})$, $\mathrm{PSL}_2(\mathbb{F}_{3^3})$, $\mathrm{PSL}_2(\mathbb{F}_{7^3})$ and $\mathrm{PSL}_2(\mathbb{F}_{3^5})$ are Galois groups over $\mathbb{Q}$.*

Remark 1. *At the same period of time that this project was completed, the groups $\mathrm{PSL}_2(\mathbb{F}_{3^3})$ and $\mathrm{PSL}_2(\mathbb{F}_{7^3})$ have been independently realized as Galois groups over $\mathbb{Q}$ by similar methods by D. Zywina, cf. [7].*

2.2. $\mathrm{PSL}_2(\mathbb{F}_{5^3})$

We consider a newform f in the orbit denoted as Newform orbit 31.5.b.b in [8], of level $N = 31$, weight $k = 5$, and nebentypus ψ the quadratic character associated to the field $\mathbb{Q}(\sqrt{-31})$. The coefficient field $\mathbb{Q}_f$ is the degree-6 field with defining polynomial $x^6 + 398x^4 + 49236x^2 + 1934136$. Let ν be a root of this polynomial.

Since the level is prime, we see that f has no CM, as $\psi(3) = \left(\frac{-31}{3}\right) = -1$ and $a_3 = \nu \neq 0$. The element $a_3^2 = \nu^2$ generates the field F_f, which is a cubic extension of $\mathbb{Q}$. In particular, this implies that ψ is the only inner twist of f.

Let $\ell = 5$. It is inert in F_f, so that $\ell R = \lambda = (5)$. In turn, λ splits in $\mathbb{Q}_f$ as the product of two prime ideals, we fix Λ one of them. We have $\mathcal{O}/\Lambda = \mathbb{F}_{5^3}$ and $R/\lambda = \mathbb{F}_{5^3}$, so that $r = r' = 3$. Since $\ell \equiv 1 \pmod{4}$ and λ splits completely in $\mathbb{Q}_f$, Theorem 4 implies that

$$\mathbb{P}(\bar{\rho}_\Lambda(G_{\mathbb{Q}})) \subseteq \mathrm{PSL}_2(\mathbb{F}_{5^3}).$$

We now start discarding possible small images. Assume first that $\bar{\rho}_\Lambda$ is reducible. We have $\ell = k \geq k-1$ and $\ell \neq N$. Since $a_5 \not\equiv 0 \pmod{\Lambda}$, we may apply Lemma 2 to show that $\bar{\rho}_\Lambda^{ss} \sim 1 \oplus \psi$. However, this means the trace of $\bar{\rho}_\Lambda$ would be zero for primes p such that $\psi(p) = -1$, and we have $a_3 \not\equiv 0 \pmod{\Lambda}$. Hence, $\bar{\rho}_\Lambda$ is irreducible.

To show the image is not contained in the normalizer of a Cartan subgroup, we only need to consider the quadratic primitive Dirichlet characters of conductor dividing $5 \cdot 31$, which are those associated to the quadratic fields

$$\mathbb{Q}(\sqrt{5}), \mathbb{Q}(\sqrt{-31}) \text{ and } \mathbb{Q}(\sqrt{-155}).$$

The first two have value -1 at 3, while $a_3 \not\equiv 0 \pmod{\Lambda}$. The third character gives -1 at 2, and we also have $a_2 \not\equiv 0 \pmod{\Lambda}$. These facts are incompatible with $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q}))$ being in the normalizer of a Cartan subgroup.

The other maximal subgroup of $\mathrm{PSL}_2(\mathbb{F}_{5^3})$, according to the congruences in Lemma 1 and point (3) in the discussion following Lemma 2, is $\mathrm{PGL}_2(\mathbb{F}_5)$. Let Frob_3 be a Frobenius element for 3 in $G_\mathbb{Q}$. Modulo conjugation, we have

$$\bar{\rho}_\Lambda(\mathrm{Frob}_3) = \begin{pmatrix} 1 & 1 \\ a_3 & a_3 - 1 \end{pmatrix}.$$

This matrix has order 124 in $\mathrm{GL}_2(\mathbb{F}_{5^3})$, and actually $\bar{\rho}_5(\mathrm{Frob}_3)^{31} = 2\,\mathrm{Id}$, so the element has order 31 in $\mathrm{PSL}_2(\mathbb{F}_{5^3})$. Hence $\mathbb{P}(\bar{\rho}_5(G_\mathbb{Q}))$ cannot be inside $\mathrm{PGL}_2(\mathbb{F}_5)$. We conclude that the projective image is the whole $\mathrm{PSL}_2(\mathbb{F}_{5^3})$, which is a Galois group over $\mathbb{Q}$.

2.3. $\mathrm{PSL}_2(\mathbb{F}_{3^3})$

We consider a newform f in the orbit denoted as Newform orbit 43.5.b.b in [8] of level $N = 43$, weight $k = 5$, and nebentypus ψ the quadratic character associated to the field $\mathbb{Q}(\sqrt{-43})$. The field $\mathbb{Q}_f$ is defined by the polynomial $x^{12} + 142x^{10} + 7173x^8 + 157368x^6 + 1510016x^4 + 5098688x^2 + 90352$, it has degree 12 over $\mathbb{Q}$. We let ν be a root of this polynomial. The q-expansion of f begins with

$$q + \nu q^2 + O(q^3).$$

We have $\psi(2) = -1$ and $a_2 \neq 0$, therefore, f has no CM. The coefficient $a_2^2 = \nu^2$ generates a field F_f with $[F_f : \mathbb{Q}] = 6$, which confirms that ψ is the only inner twist of f.

We let $\ell = 3$. It splits as the product of two primes λ and λ' in F_f. Furthermore, λ remains inert in $\mathbb{Q}_f$, we write $\Lambda = \lambda\mathcal{O}$. We check that $\mathcal{O}/\Lambda = \mathbb{F}_{3^6}$ and $R/\lambda = \mathbb{F}_{3^3}$, $r = 6$, $r' = 3$. Because $\ell \equiv 3 \pmod{4}$, and $a_2 \pmod{\Lambda} \notin \mathbb{F}_{3^3}$, Theorem 4 implies that

$$\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q})) \subseteq \mathrm{PSL}_2(\mathbb{F}_{3^3}).$$

Let us discard possible small images. If $\bar{\rho}_\Lambda$ is reducible, and because its determinant is $\det(\bar{\rho}_\Lambda) = \chi_3^4\psi = \psi$, it has to be conjugate to

$$\begin{pmatrix} \chi_3^a\varepsilon_1 & * \\ 0 & \chi_3^a\varepsilon_2 \end{pmatrix},$$

where $a = 0$ or 1, and $\varepsilon_1, \varepsilon_2$ are characters ramified at most at $N = 43$. If both ε_1 and ε_2 were ramified at N, which is prime, then 43^2 would divide the conductor of $\bar{\rho}_\Lambda$, which is not the case. Hence, one of them (say ε_1) must be unramified at N and trivial, and the other one must be ramified at N and quadratic, that is, $\varepsilon_2 = \psi$. Hence we find that $\bar{\rho}_\Lambda^{ss} \sim \chi_3^a \oplus \chi_3^a\psi$ and the trace of $\bar{\rho}_\Lambda$ is defined over $\mathbb{F}_3$. However, $\overline{a_2} = \mathrm{trace}(\bar{\rho}_\Lambda(\mathrm{Frob}_2) \notin \mathbb{F}_3$, so $\bar{\rho}_\Lambda$ has to be irreducible.

Now we look at the case when the image is inside the normalizer of a Cartan subgroup. We need to consider the quadratic primitive Dirichlet characters ε with conductor dividing $3 \cdot 43$, which are the ones associated to the fields

$$\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-43}) \text{ and } \mathbb{Q}(\sqrt{129}).$$

In the first two cases $\varepsilon(2) = -1$, but $a_2 \not\equiv 0 \pmod{\Lambda}$. In the third case, we have $\varepsilon(7) = \left(\frac{129}{7}\right) = -1$, and it is easy to check that $a_7 \not\equiv 0 \pmod{\Lambda}$. Hence, the image is not contained in a normalizer of Cartan subgroup.

By the congruences of Lemma 1 and the subsequent discussion, we still need to discard the image of $\mathbb{P}(\bar{\rho}_\Lambda)$ being contained in $\mathrm{PSL}_2(\mathbb{F}_3)$ and $\mathrm{PGL}_2(\mathbb{F}_3)$. To that effect, we consider the image of Frob_2, which up to conjugation is

$$\bar{\rho}_\Lambda(\mathrm{Frob}_2) = \begin{pmatrix} 1 & 1 \\ \overline{a_2} & \overline{a_2} - 1 \end{pmatrix}.$$

This matrix has order 13 in $\mathrm{PSL}_2(\mathbb{F}_{3^3})$, so the image cannot be in such smaller subgroups. Therefore, $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q})) = \mathrm{PSL}_2(\mathbb{F}_{3^3})$.

2.4. $\mathrm{PSL}_2(\mathbb{F}_{7^3})$

Let f be a newform in the orbit denoted as Newform orbit 31.7.b.c in [8], of level $N = 31$, weight $k = 7$, and nebentypus ψ the quadratic character associated to the field $\mathbb{Q}(\sqrt{-31})$. The degree-12 field of coefficients $\mathbb{Q}_f$ is given by the polynomial $x^{12} + 7208x^{10} + 19859688x^8 + 26566749360x^6 + 17884354852944x^4 + 5570285336959680x^2 + 590986232936064000$. As usual we let ν be a root of this polynomial.

The form f does not have CM, since $\psi(3) = \left(\frac{-31}{3}\right) = -1$ and $a_3 = -\nu \neq 0$. The field F_f is generated over $\mathbb{Q}$ by $a_3^2 = \nu^2$ and $[F_f : \mathbb{Q}] = 6$, so that ψ is the unique inner twist of f.

The rational prime $\ell = 7$ splits in F_f as the product of three primes λ_1, λ_2 and λ_3, with inertia degrees $1, 2$ and 3, respectively. The prime λ_3 is inert in $\mathbb{Q}_f$, so that $\Lambda = \lambda_3\mathcal{O}$ satisfies $\mathcal{O}/\Lambda = \mathbb{F}_{7^6}$ and $R/\lambda_3 = \mathbb{F}_{7^3}$. We have $a_3 \pmod{\Lambda} \notin \mathbb{F}_{7^3}$, in fact, $\overline{a_3}$ generates $\mathbb{F}_{7^6}$. Since $7 \equiv 3 \pmod{4}$, Theorem 4 gives the inclusion $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q})) \subseteq \mathrm{PSL}_2(\mathbb{F}_{7^3})$.

In this example, we have again $\ell = k \geq k - 1$ and $\ell \neq N$. Since $a_7 \not\equiv 0 \pmod{\Lambda}$, if the representation were irreducible, by Lemma 2 we would have $\bar{\rho}_\Lambda^{ss} \sim 1 \oplus \psi$, but this cannot happen since $\psi(3) = -1$ and $a_3 \not\equiv 0 \pmod{\Lambda}$, so $\bar{\rho}_\Lambda$ is irreducible. To rule out the normalizer of Cartan case, we look at the primitive Dirichlet characters ε with conductor dividing $7 \cdot 31$, namely the ones corresponding to the fields

$$\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-31}) \text{ and } \mathbb{Q}(\sqrt{217}).$$

We need to find some prime p with $\varepsilon(p) = -1$ and $a_p \not\equiv 0 \pmod{\Lambda}$. For the first two characters this is satisfied by $p = 3$, while for the third we may look at $p = 5$. Hence $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q}))$ is not contained in a normalizer of a Cartan subgroup.

By Lemma 1, it remains to check that the projective image is not contained in $\mathrm{PGL}_2(\mathbb{F}_7)$ or $\mathrm{PSL}_2(\mathbb{F}_7)$. To that effect, we note that $\bar{\rho}_\Lambda(\mathrm{Frob}_3)$ is conjugate in $\mathrm{GL}_2(\mathbb{F}_{\ell^6})$ to the matrix

$$\begin{pmatrix} 1 & 1 \\ \overline{a_3} & \overline{a_3} - 1 \end{pmatrix}.$$

This matrix has order $2^4 \cdot 43$ in $\mathrm{GL}_2(\mathbb{F}_{\ell^6})$, and even in $\mathrm{PGL}_2(\mathbb{F}_{\ell^6})$. Therefore, $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q}))$ is not contained in such a smaller subgroup, and the image is all of $\mathrm{PSL}_2(\mathbb{F}_{7^3})$.

2.5. $\mathrm{PSL}_2(\mathbb{F}_{3^5})$

Let us consider a newform f of level $N = 67$, weight $k = 3$, and quadratic nebentypus ψ associated with the field $\mathbb{Q}(\sqrt{-67})$, in the orbit denoted as Newform orbit 67.3.b.b in [8].

Its coefficient field $\mathbb{Q}_f$ is given by the degree-10 polynomial $x^{10} + 32x^8 + 357x^6 + 1725x^4 + 3366x^2 + 1519$, let ν be one of its roots in $\mathbb{Q}_f$. The q-expansion of f begins with

$$q + \nu q^2 + O(q^3).$$

We see f has neither CM nor inner twists besides ψ, since the field F_f is generated over $\mathbb{Q}$ by ν^2, $\mathbb{Q}_f$ has degree 2 over F_f, and $\psi(2) = -1$, while $a_2 \neq 0$. The prime $\ell = 3$ is inert in F_f, while $\lambda = \ell R$ is inert in $\mathbb{Q}_f$. Setting $\Lambda = \lambda\mathcal{O}$, this means $\mathcal{O}/\Lambda = \mathbb{F}_{3^{10}}$ and $R/\lambda = \mathbb{F}_{3^5}$. We have $a_2 \pmod{\Lambda} \notin \mathbb{F}_{3^5}$, hence Theorem 4 says that $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q})) \subseteq \mathrm{PSL}_2(\mathbb{F}_{3^5})$.

We have $\ell = k \geq k - 1$ and $\ell \neq N$. Furthermore, $a_3 \not\equiv 0 \pmod{\Lambda}$, so we can apply Theorem 1 and Lemma 2 to show $\bar{\rho}_\Lambda$ is irreducible. Indeed, if $\bar{\rho}_\Lambda$ were reducible, we would have as usual $\bar{\rho}_\Lambda^{ss} \sim 1 \oplus \psi$, but $\psi(2) = -1$ and $a_2 \not\equiv 0 \pmod{\Lambda}$.

Next, we look at the possibility of $\mathbb{P}(\bar{\rho}_\Lambda(G_\mathbb{Q}))$ being inside the normalizer of a Cartan subgroup of $\mathrm{PSL}_2(\mathbb{F}_{3^5})$. Because the representation is unramified outside $3 \cdot 67$, we just need to find some p with $\varepsilon(p) = -1$ and $a_p \not\equiv 0 \pmod{\Lambda}$ for any of the primitive quadratic Dirichlet characters ε associated with the fields

$$\mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-67}), \text{ and } \mathbb{Q}(\sqrt{201}).$$

For the first two characters, this is the case for $p = 2$, for the third, we may use $p = 7$.

If we look at Lemma 1 and the discussion after, we need to check that the projective image is not contained in some maximal subgroup of $\mathrm{PSL}_2(\mathbb{F}_{3^5})$, namely $\mathrm{PSL}_2(\mathbb{F}_3)$ and $\mathrm{PGL}_2(\mathbb{F}_3)$. For instance, we can look at the image of Frob_2, which up to conjugation is

$$\bar{\rho}_\Lambda(\mathrm{Frob}_2) = \begin{pmatrix} 1 & 1 \\ \overline{a_2} & \overline{a_2} - 1 \end{pmatrix}.$$

This matrix has order $2 \cdot 61$ both in $\mathrm{GL}_2(\mathbb{F}_{3^5})$ and in $\mathrm{PSL}_2(\mathbb{F}_{3^5})$. It follows that the projective image of $\bar{\rho}_\Lambda$ is not contained in any smaller subgroup, and it is the full $\mathrm{PSL}_2(\mathbb{F}_{3^5})$, as desired.

3. $\mathbf{PSL_2(\mathbb{F}_{3^4})}$

Theorem 6. *The group* $\mathrm{PSL}_2(\mathbb{F}_{3^4})$ *is a Galois group over* $\mathbb{Q}$*.*

Proof. We consider a newform f of level $N = 226$, weight 2, and trivial nebentypus in the orbit denoted as Newform orbit 67.3.b.b in [8]. We know f has no inner twists nor CM, since the form is Steinberg at the primes dividing the level. The coefficient field $\mathbb{Q}_f$ is the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{20})$ containing all 20th roots of unity. We have $[\mathbb{Q}_f : \mathbb{Q}] = 4$, and $\mathbb{Q}_f$ is generated by $a_5(f)$, whose irreducible polynomial is

$$x^4 - 4x^3 - 4x^2 + 16x - 4.$$

This polynomial is also irreducible mod 3, so 3 is inert in $\mathbb{Q}_f$ and we may consider the representation

$$\bar{\rho}_3 : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{F}_{3^4}).$$

The determinant of $\bar{\rho}_3$ is the mod 3 cyclotomic character χ_3. Hence, the projective image of $\bar{\rho}_3$ is contained in $\mathrm{PSL}_2(\mathbb{F}_{3^4})$. We will determine its image using the classification by Dickson in Lemma 1.

If $\bar{\rho}_3$ was reducible we would have $\bar{\rho}_3^{ss} \sim 1 \oplus \chi_3$, since the level is squarefree (and thus the conductor of $\bar{\rho}_f$ is squarefree with determinant χ_3). Therefore, $\bar{\rho}_3^{ss}$ will have trace in $\mathbb{F}_3$, but $\bar{\rho}_3(\mathrm{Frob}_5)$ has trace $\overline{a_5}$, which is a generator of $\mathbb{F}_{3^4}$. Hence, $\bar{\rho}_3$ is irreducible.

We next consider the case where the projective image of $\bar{\rho}_3$ is contained in the normalizer N of a Cartan subgroup C. As in Section 2.1, we only need to look at primitive quadratic Dirichlet characters ε with conductor dividing $\ell \cdot N = 2 \cdot 3 \cdot 113$. What is more, 2 and 113 are primes where $\bar{\rho}_3$ is Steinberg, so that for $p \in \{2, 113\}$,

$$\bar{\rho}_3|_{I_p} \cong \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

This means ε cannot be ramified at 2 or 113, since it is a nontrivial quadratic character and $\bar{\rho}_3|_{I_p}$ has odd order. Therefore ε is the character associated with the quadratic field $\mathbb{Q}(\sqrt{-3})$. However, we then have $\varepsilon(2) = -1$, while $a_2 = 1 \not\equiv 0 \pmod 3$. We have thus discarded the dihedral case.

Lastly, we will see the projective image of $\bar{\rho}_3$ is not contained in $\mathrm{PGL}_2(\mathbb{F}_9)$. The field of definition of the projective representation $\mathbb{P}(\bar{\rho}_3)$ is that generated by the different $a_p^2/\psi(p) \pmod 3$ (here ψ is the nebentypus, which is trivial in this case). We have already shown that $a_5^2 \pmod 3$ generates $\mathbb{F}_{3^4}$, therefore, the image cannot be contained in $\mathrm{PGL}_2(\mathbb{F}_9)$. We have no further maximal subgroups of $\mathrm{PSL}_2(\mathbb{F}_{3^4})$ because of Lemma 1 and the fact that $\mathbb{F}_{3^4}$ is an extension of $\mathbb{F}_3$ of degree larger than two.

Therefore, the image $\mathbb{P}(\bar{\rho}_3(G_{\mathbb{Q}}))$ is maximal. $\square$

4. $\mathrm{PSU}_3(\mathbb{F}_5)$ and $\mathrm{PSL}_3(\mathbb{F}_7)$ as Galois groups over $\mathbb{Q}$

The images of modular and geometric three-dimensional Galois representation have been studied in our previous paper [9]. As a consequence of the recent results of P. Scholze [10], we know the existence of Galois representations associated with the mod p cohomology of the locally symmetric spaces for GL_n over F a totally real or CM field. Moreover, we have for characteristic 0 cohomology classes the existence of p-adic Galois representations by the recent result of Harris–Lan–Taylor–Thorne [11] (also proved by Scholze). We state the result that we will use to obtain the Galois realization over $\mathbb{Q}$ of the group $\mathrm{PSU}_3(\mathbb{F}_5)$ (cf. [10], V.4.2; V.4.6).

Theorem 7. *Let F be an imaginary quadratic field. Let S be the pullback from finite set of primes of $\mathbb{Q}$, which contains p and all places at which $F/\mathbb{Q}$ is ramified. Let π be a cuspidal automorphic representation of $\mathrm{GL}_n(\mathbb{A}_F)$ such that π_∞ is regular algebraic, and such that π_v is unramified at all finite places $v \notin S$. Then there exists a unique continuous semisimple representation*

$$\sigma_\pi : G_{F,S} \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$$

such that for all finite places $v \notin S$, the Satake parameters of π_v agree with the eigenvalues of $\sigma_\pi(\mathrm{Frob}_v)$.

Lemma 3. *Let $f \in H^3(\Gamma_0(88), \mathbb{C})$ be the eigenform for the action of the Hecke algebra $\mathcal{T}(N)$ computed in [12] Table 2 such that $\mathbb{Q}_f = \mathbb{Q}(\sqrt{-7})$. The eigenform f is cuspidal.*

Proof. If f is not cuspidal, there is a unique decomposition

$$f = \omega \boxplus g$$

where ω is an automorphic form on $\mathrm{GL}(1)/\mathbb{Q}$ and g is an automorphic form on $\mathrm{GL}(2)/\mathbb{Q}$. We remark that ω is algebraic, as a consequence it is a Hecke character of type A_0 and the finite part only ramifies at two and 11. According with the eigenvalues computed in [12] we can determine the attached Satake polynomials which are of the form

$$\mathrm{Pol}_p(X) = X^3 - a_p X^2 + \bar{a}_p p X - p^3, \;\; p \nmid 88.$$

In particular, if f is not cuspidal they will have as a factor the Satake character attached to ω, that is $X - p^t \epsilon(p)$, where $\epsilon(p)$ is a root of the unit with order coprime to 3, since the conductor of the character ϵ is $2^\alpha 11^\beta$ and $3 \nmid \varphi(2^\alpha 11^\beta)$. Let $p = 3$, the polynomial $\mathrm{Pol}_3(\mathrm{X})$ is irreducible since we compute that it is irreducible modulo 5. Let γ be a root of it, the degree of $\mathbb{Q}(\gamma, \sqrt{-7})$ over $\mathbb{Q}$ is therefore equal to 6. If $\gamma = 3^t\epsilon(3)$ then $\mathbb{Q}(\gamma, \sqrt{-7}) = \mathbb{Q}(\epsilon(3), \sqrt{-7})$, so $\epsilon(3)$ must be a root of unity of order 3 or 6, which is a contradiction.

By Theorem 0 we can consider the 5-adic Galois representation attached to f

$$\rho_f : G_{\mathbb{Q}} \to \mathrm{GL}_3(\mathbb{Z}(\sqrt{-7})_5).$$

Let $\overline{\rho}_f$ the reduced Galois representation modulo 5. Because 5 is inert in $\mathbb{Q}(\sqrt{-7})$, we have

$$\overline{\rho}_f : G_{\mathbb{Q}} \to \mathrm{GL}_3(\mathbb{F}_{5^2}).$$

As we have observed in [9], the form of the characteristic polynomial of the Frobenius, implies that $\overline{\rho}_f^v \cong \overline{\rho}_f^c \otimes \psi$, where $< c >= \mathrm{Gal}(\mathbb{F}_{25}/\mathbb{F}_5)$. So we have that the image is unitary. Moreover, since the determinant of ρ_f is χ^3 (cf. [9]), we have that

$$\overline{\rho}_f \otimes \overline{\chi}^{-1}(G_{\mathbb{Q}}) \subset \mathrm{SU}_3(\mathbb{F}_5).$$

Theorem 8.

$$\mathbb{P}(\overline{\rho}_f)(G_{\mathbb{Q}}) = \mathrm{PSU}_3(\mathbb{F}_5)$$

Proof. We know that $\mathbb{P}(\overline{\rho}_f)(G_{\mathbb{Q}}) \subset \mathrm{PSU}_3(\mathbb{F}_5)$. From the classification of the maximal subgroups of $\mathrm{PSL}_3(\mathbb{F}_p)$ in our case $p = 5$, we know that the maximal proper subgroups are of type C_1 reducible (two cases over $\mathbb{F}_{25}$) or of type S, that is, $M_{10} = A_6.2$ or A_7 (cf. Liebeck's Ph.D. thesis). The polynomial $\mathrm{Pol}_3(X) \in \mathbb{F}_{25}[X]$ is irreducible modulo 5, as a consequence, the cases C_1 are not possible. On the other hand, $\mathrm{Pol}_7(X)$ modulo 5 is reducible and splits into a linear factor and a quadratic factor. The roots of the quadratic factor have order divisible by 13. That means that in the image of $\overline{\rho}_f$, there is an element M of order divisible by 13. Since 13 is relatively prime with $24 = \sharp Z(\mathrm{SU}_3(\mathbb{F}_{25}))$, the order of $\mathbb{P}(M)$ is also divisible by 13. This exclude that the image is of the type S in the classification. □

As a consequence, we have that the group $\mathrm{PSU}_3(\mathbb{F}_5)$ occurs as a Galois group over $\mathbb{Q}$.

In the case of the group $\mathrm{PSL}_3(\mathbb{F}_7)$, we obtain that it is a Galois group over $\mathbb{Q}$ since conjecture 1′ of [13] has been proved as a consequence of P. Scholze results modulo p (cf. [10], cor. V.4.3). That means that to a Hecke eigenclass in the mod p cohomology of the congruence subgroup of $\mathrm{SL}(3, \mathbb{Z})$ we can attach a three-dimensional mod p semisimple Galois representation of $G_{\mathbb{Q}}$. We consider a Hecke eigenclass over the field $\mathbb{F}_7$ of level 167 for which several eigenvalues and the image of the mod 7 corresponding Galois representation have been computed in [13], p. 222, and we conclude that thanks to Scholze's result the realization of this group, already obtained as a result of these computations in [13], now holds unconditionally.

Theorem 9 (Ash-McConnell; Scholze)**.** *The group* $\mathrm{PSL}_3(\mathbb{F}_7)$ *is a Galois group over* $\mathbb{Q}$.

Author Contributions: Conceptualization, L.D., E.F. and N.V.; Investigation, L.D., E.F. and N.V.; Methodology, L.D., E.F. and N.V. All authors have read and agreed to the published version of the manuscript.

Funding: The first author is partially supported by the PID2019-107297GB-I00 grant of the MICINN (Spain). The second author is partially supported by the Spanish Ministry of Universities (FPU20/05059).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Zywina, D. Inverse Galois Problem for Small Simple Groups. 2013 preprint. Available online: http://pi.math.cornell.edu/~zywina/papers/smallGalois.pdf (accessed on 5 April 2022).
2. Deligne, P. *Formes Modulaires et Représentations l-adiques*; Lecture Notes in Mathematics; Springer: Berlin/Heidelberg, Germany, 1971; Volume 175.

3. Edixhoven, B. The weight in Serre's conjectures on modular forms. *Invent. Math.* **1992**, *109*, 563–594.
4. Ribet, K. *Galois Representations Attached to Eigenforms with Nebentypus*; Modular Functions of one Variable V; Lecture Notes in Mathematics; Springer: Berlin/Heidelberg, Germany, 1977.
5. Ribet, K. On l-adic representations attached to modular forms II. *Glasg. Math. J.* **1985**, *27*, 185–194.
6. Dickson, L.E. *Linear Groups with an Exposition of the Galois Field Theory*; Dover Publications: Mignola, NY, USA, 1958.
7. Zywina, D. Modular forms and some cases of the inverse Galois problem. *arXiv* **2015**, arXiv:1508.07916.
8. The LMFDB Collaboration. The L-Functions and Modular Forms Database. Available online: http://www.lmfdb.org (accessed on 5 April 2022).
9. Dieulefait, L.; Vila, N. On the images of modular and geometric three-dimensional Galois representations. *Am. J. Math.* **2004**, *126*, 335–361.
10. Scholze, P. On torsion in the cohomology of locally symmetric varieties. *Annals Math.* **2015**, *182*, 945–1066.
11. Harris, M.; Lan, K.-W.; Taylor, R.; Thorne, J. On the rigid cohomology of certain Shimura varieties. *Res. Math. Sci.* **2016**, *3*, 37.
12. van Geemen, B.; van der Kallen, W.; Top, J.; Verberkmoes, A. Hecke Eigenforms in the Cohomology of Congruences Subgroups of $SL(3,\mathbb{Z})$. *Experiment. Math.* **1997**, *6*, 163–174.
13. Ash, A.; McConnell, M. Experimental indications of three-dimensional Galois representations from the cohomology of $SL(3,\mathbb{Z})$. *Experimental Math.* **1992**, *1*, 209–223.