THE INVERSE GALOIS PROBLEM FOR $\mathrm{PSL}_2(\mathbb{F}_p)$

DAVID ZYWINA

Abstract. We show that the simple group $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs as the Galois group of an extension of the rationals for all primes $p \geq 5$. We obtain our Galois extensions by studying the Galois action on the second étale cohomology groups of a specific elliptic surface.

1. Introduction

1.1. **Statement.** The Inverse Galois Problem asks whether every finite group G occurs as the Galois group of an extension of $\mathbb{Q}$, i.e., whether there is a finite Galois extension $K/\mathbb{Q}$ such that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to G. This problem is still wide open; even in the case of finite non-abelian simple groups which we now restrict our attention to. Many special cases are known, including alternating groups and all but one of the sporadic simple groups. Various families of simple groups of Lie type are known to occur as Galois groups of an extension of $\mathbb{Q}$, but usually with congruences imposed on the cardinality of the fields. See [MM99] for background and many examples.

We shall study the simple groups $\mathrm{PSL}_2(\mathbb{F}_p) := \mathrm{SL}_2(\mathbb{F}_p)/\{\pm I\}$ where $p \geq 5$ is a prime; their simplicity was observed by Galois, cf. [Gal46, p. 411]. These are the "simplest" of the simple groups for which the inverse Galois problem has not been completely settled.

Shih proved that the group $\mathrm{PSL}_2(\mathbb{F}_p)$ occur as the Galois group of an extension of $\mathbb{Q}$ if 2, 3 or 7 is a quadratic non-residue modulo p, cf. [Shi74] (Serre gives a lucid exposition in §5.3 of [Ser08]). The case where 5 is a quadratic non-residue modulo p is then a consequence of a theorem of Malle [Mal93]. Clark [Cla07] showed that $\mathrm{PSL}_2(\mathbb{F}_p)$ occurs for a finite number of additional primes p (and also, assuming the Birch and Swinnerton-Dyer conjecture for elliptic curves over $\mathbb{Q}$, primes $p \equiv 1 \pmod 4$ for which 11 or 19 is a quadratic non-residue modulo p). Our main result is the following:

Theorem 1.1. *The simple group* $\mathrm{PSL}_2(\mathbb{F}_p)$ *occurs as the Galois group of an extension of* $\mathbb{Q}$ *for all primes* $p \geq 5$.

Remark 1.2. (i) The Inverse Galois Problem is easy for the (non-simple) groups $\mathrm{PSL}_2(\mathbb{F}_2)$ and $\mathrm{PSL}_2(\mathbb{F}_3)$; note that they are isomorphic to $\mathfrak{S}_3$ and $\mathfrak{A}_4$, respectively.
(ii) The simple groups $E_8(\mathbb{F}_p)$ and $G_2(\mathbb{F}_p)$ are known to occur as Galois extensions of $\mathbb{Q}$ for all sufficiently large primes p (see [Yun11] and [FF85], respectively). Theorem 1.1 is the first case where this has been proved for simple groups of a fixed *classical* Lie type.
(iii) In an upcoming paper [Zyw13], we will show that the simple groups $O_{2n+1}(p)$ and $O^+_{4n}(p)$ both occur as the Galois group of an extension of $\mathbb{Q}$ for every prime $p \geq 5$ and integer $n \geq 2$ (with group notation as in [CCN+85]). Moreover, these groups are shown to arise as the Galois group of a regular extension of the function field $\mathbb{Q}(t)$. This paper arose by trying to make progress in the excluded case $n = 1$ where we have exceptional isomorphisms $O_3(p) \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$ and $O^+_4(p) \cong \mathrm{PSL}_2(\mathbb{F}_p) \times \mathrm{PSL}_2(\mathbb{F}_p)$.

2000 *Mathematics Subject Classification.* Primary 12F12; Secondary 14J27, 11G05.
This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155.

1.2. **The representations.** Let $\mathbb{P}^1_{\mathbb{Q}}$ be the projective line; it is obtained by completing the affine line $\mathbb{A}^1_{\mathbb{Q}} := \operatorname{Spec} \mathbb{Q}[t]$ with a rational point ∞. Consider the Weierstrass equation

$$t(t-1)(t+1) \cdot y^2 = x(x+1)(x+t^2). \tag{1.1}$$

The equation (1.1) defines a relative elliptic curve $f\colon E \to U$ where $U := \mathbb{P}^1_{\mathbb{Q}} - \{0, 1, -1, \infty\}$. More precisely, E is the projective subscheme of $\mathbb{P}^2_U$ defined by the affine equation (1.1) and f is obtained by composing the inclusion $E \subseteq \mathbb{P}^1_U$ with the structure map $\mathbb{P}^1_U \to U$. The points on E off the affine model (1.1) give our distinguished section of f. For any field $K \supseteq \mathbb{Q}$ and point $s \in U(K) \subseteq K$, the fiber $f^{-1}(s)$ is the elliptic curve over K defined by specializing t by s in (1.1).

Take any odd prime ℓ. Let $E[\ell]$ be the ℓ-torsion subscheme of E. The morphism $E[\ell] \to U$ arising from f allows us to view $E[\ell]$ as a sheaf of $\mathbb{F}_\ell$-modules on U; it is free of rank 2. Define the $\mathbb{F}_\ell$-vector space

$$V_\ell := H^1_c(U_{\overline{\mathbb{Q}}}, E[\ell])$$

where we are taking étale cohomology with compact support. There is a natural action of the absolute Galois group $\operatorname{Gal}_{\mathbb{Q}} := \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on V_ℓ which we may express in terms of a representation

$$\rho_\ell\colon \operatorname{Gal}_{\mathbb{Q}} \to \operatorname{Aut}_{\mathbb{F}_\ell}(V_\ell).$$

Theorem 1.1 will be a consequence of the following.

Theorem 1.3. *For each prime $\ell \geq 11$, the group $\operatorname{PSL}_2(\mathbb{F}_\ell)$ is a quotient of $\rho_\ell(\operatorname{Gal}_{\mathbb{Q}})$.*

In §8, we shall describe the group $\rho_\ell(\operatorname{Gal}_{\mathbb{Q}})$ for all $\ell \geq 11$. Using the image of ρ_ℓ, we will use Serre's modularity theorem in §8.2 to show that our $\operatorname{PSL}_2(\mathbb{F}_\ell)$-extensions arise from modular representations.

1.3. **The surface.** We can extend $f\colon E \to U$ to a morphism $\tilde{f}\colon X \to \mathbb{P}^1_{\mathbb{Q}}$ such that X is a smooth projective surface defined over $\mathbb{Q}$ and $\tilde{f}$ is relatively minimal (so if $f'\colon X' \to \mathbb{P}^1_{\mathbb{Q}}$ was a morphism extending f with X' smooth and projective, then it would factor through $\tilde{f}$). The surface X is unique up to isomorphism.

For each prime ℓ, there is a natural Galois action on the étale cohomology group $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)$ which can be expressed in terms of a representation

$$\phi_\ell\colon \operatorname{Gal}_{\mathbb{Q}} \to \operatorname{Aut}_{\mathbb{F}_\ell}(H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)).$$

For odd ℓ, we shall see that a certain Tate twist of V_ℓ is isomorphic to a composition factor of the $\mathbb{F}_\ell[\operatorname{Gal}_{\mathbb{Q}}]$-module $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)$; this will allow us to prove the following.

Theorem 1.4. *The group $\operatorname{PSL}_2(\mathbb{F}_\ell)$ is a quotient of $\phi_\ell(\operatorname{Gal}_{\mathbb{Q}})$ for all $\ell \geq 11$.*

2. Basic properties and an overview

Take any odd prime ℓ and fix notation as in §1.2. We now describe many useful facts concerning the representation ρ_ℓ of §1.2; they are straightforward étale cohomology computations and we will supply proofs in Appendix A.

2.1. **Properties.**

Lemma 2.1.

(i) The $\mathbb{F}_\ell$-vector space V_ℓ has dimension 4.

(ii) There is a non-degenerate symmetric bilinear form $\langle\ ,\ \rangle\colon V_\ell \times V_\ell \to \mathbb{F}_\ell$ such that

$$\langle \rho_\ell(\sigma)v, \rho_\ell(\sigma)w \rangle = \langle v, w \rangle$$

for all $\sigma \in \operatorname{Gal}_{\mathbb{Q}}$ and $v, w \in V_\ell$.

Let $\mathrm{O}(V_\ell)$ be the group of automorphisms of the vector space V_ℓ which preserve the pairing $\langle\ ,\ \rangle$ of Lemma 2.1(ii). We thus have a representation

$$\rho_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{O}(V_\ell).$$

Let $\mathrm{SO}(V_\ell)$ be the kernel of the determinant map $\det\colon \mathrm{O}(V_\ell) \to \{\pm 1\}$. The image of ρ_ℓ actually lies in this smaller group.

Lemma 2.2. *We have $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathrm{SO}(V_\ell)$.*

2.2. ***L*-functions.** Fix an odd prime p and let E_p be the elliptic curve over $\mathbb{F}_p(t)$ defined by (1.1). Take any closed point x of $\mathcal{U}_p := \mathbb{P}^1_{\mathbb{F}_p} - \{0, 1, -1, \infty\} = \operatorname{Spec} \mathbb{F}_p[t, 1/(t(t-1)(t+1))]$. Let $\mathbb{F}_x$ be the residue field of x and define $\deg x := [\mathbb{F}_x : \mathbb{F}_p]$. Let $E_{p,x}$ be the elliptic curve over $\mathbb{F}_x$ obtained by reducing E_p. Let a_x be the integer that satisfies $|E_{p,x}(\mathbb{F}_x)| = |\mathbb{F}_x| - a_x + 1$. The *L*-function of the elliptic curve E_p is the power series

$$L(T, E_p) = \prod\nolimits_x (1 - a_x T^{\deg x} + p^{\deg x} T^{2 \deg x})^{-1} \in \mathbb{Z}[\![T]\!] \tag{2.1}$$

where the product is over the closed points x of $\mathcal{U}_p$ (we do not need to include factors at 0, 1, -1 and ∞ since E_p has additive reduction at these points). Define $P_p(T) := L(T/p, E_p)$.

Lemma 2.3. *For each odd prime p, $P_p(T)$ is a polynomial of degree 4 with coefficients in $\mathbb{Z}[1/p]$ that satisfies $T^4 P_p(1/T) = P_p(T)$.*

We will need to know the polynomials $P_p(T)$ for a few small primes p.

Lemma 2.4. *We have $P_3(T) = 1 - 2/9 \cdot T^2 + T^4$ and $P_5(T) = (1 - 2/5 \cdot T + T^2)^2$.*

For each integer n and odd prime p, define the polynomial $P_p^{(n)}(T) = \prod_{i=1}^4 (1 - \alpha_i^n T) \in \mathbb{Q}[T]$ where $P_p(T) = \prod_{i=1}^4 (1 - \alpha_i T)$ with $\alpha_i \in \overline{\mathbb{Q}}$. Using Lemma 2.4, it is easy to verify that

$$\begin{aligned} &P_3^{(2)}(T) = (1 - 2/9 \cdot T + T^2)^2, \\ &P_3^{(4)}(T) = (1 + 158/81 \cdot T + T^2)^2 \quad \text{and} \quad P_5^{(4)}(T) = (1 - 866/625 \cdot T + T^2)^2. \end{aligned} \tag{2.2}$$

2.3. **Compatibility.** Here, and throughout the paper, Frob_p denotes an *arithmetic* Frobenius automorphism in $\mathrm{Gal}_{\mathbb{Q}}$ corresponding to p. The following says that our representations ρ_ℓ are compatible and links them to the polynomials of §2.2.

Lemma 2.5. *For each prime $p \nmid 2\ell$, the representation ρ_ℓ is unramified at p and we have*

$$\det(I - \rho_\ell(\mathrm{Frob}_p)T) \equiv P_p(T) \pmod{\ell}.$$

As a consequence of Lemma 2.5, we find that for each integer n and prime $p \nmid 2\ell$ we have $\det(I - \rho_\ell(\mathrm{Frob}_p)^n T) \equiv P_p^{(n)}(T) \pmod{\ell}$.

2.4. **Connection with the surface X.** Let X be the surface of §1.3. We now related the $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-modules V_ℓ and $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)$. It will be convenient to work with the Tate twist $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)(1) = H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$.

Lemma 2.6. *Suppose $\ell \geq 7$. The semi-simplification of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$ as an $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-submodule is isomorphic to $V_\ell \oplus \mathbb{F}_\ell^{30}$.*

2.5. **Brief overview.** We now give some motivation for the rest of the paper; this will not be used later. Fix a prime $\ell \geq 11$. In light of Lemma 2.5, our first approach in trying to compute the image of ρ_ℓ was to compute $P_p(T)$ for many p. The following proposition describes the pattern we observed; we will prove it in Propositions 4.7 and 5.6.

Proposition 2.7. *Let p be an odd prime.*

(i) If $p \equiv 1 \pmod 4$, then $P_p(T) = (1 + bT + T^2)^2$ for a unique $b \in \mathbb{Z}[1/p]$.
(ii) If $p \equiv 3 \pmod 4$, then $P_p(T) = 1 + (b^2 - 2)T^2 + T^4$ for a unique non-negative $b \in \mathbb{Z}[1/p]$.

That the shape of $P_p(T)$ seems to depend on the value of p modulo 4 suggests that we study the action of $\mathrm{Gal}_{\mathbb{Q}(i)}$ on V_ℓ; this is done in §3. Using the automorphisms of the surface $X_{\mathbb{Q}(i)}$, we will see that all the irreducible $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-submodules of V_ℓ have dimension 1 or 2. We will eventually show that V_ℓ is isomorphic to $W \oplus W$ as an $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-module where W is irreducible of dimension 2.

Let $\Omega(V_\ell)$ be the commutator subgroup of $\mathrm{O}(V_\ell)$; it is an index 2 subgroup of $\mathrm{SO}(V_\ell)$. We will show that $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \Omega(V_\ell)$. The group $\Omega(V_\ell)$ contains $-I$ and there is an *exceptional isomorphism* $\varphi\colon \Omega(V_\ell)/\{\pm I\} \xrightarrow{\sim} \mathrm{PSL}_2(\mathbb{F}_\ell) \times \mathrm{PSL}_2(\mathbb{F}_\ell)$. We thus have a representation

$$\vartheta_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \xrightarrow{\rho_\ell} \Omega(V_\ell) \twoheadrightarrow \Omega(V_\ell)/\{\pm 1\} \xrightarrow{\varphi} \mathrm{PSL}_2(\mathbb{F}_\ell) \times \mathrm{PSL}_2(\mathbb{F}_\ell) \xrightarrow{pr} \mathrm{PSL}_2(\mathbb{F}_\ell)$$

where pr is one of the two projections. Making appropriate choices of φ and pr, for each prime $p \nmid 2\ell$ we will have $\mathrm{tr}(\vartheta_\ell(\mathrm{Frob}_p)) = \pm b$ where b is the value from Proposition 2.7 modulo ℓ.

The main task of this paper is to show that $\vartheta_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ is surjective (this will be done in §7). The proof is based on Serre's open image theorem for non-CM elliptic curves over number fields, cf. [Ser72]. We assume that the image of ϑ_ℓ is contained in one of the maximal subgroups of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ and then try to obtain a contradiction. To follow Serre's approach, we will need to understand the image under ρ_ℓ of the inertia subgroup at ℓ and 2, see §4 and §6.

One can similarly construct $\vartheta_7\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{PSL}_2(\mathbb{F}_7)$; however, it appears not to be surjective. We will thus impose the condition $\ell \geq 11$ throughout much of the paper.

3. Decomposition over $\mathbb{Q}(i)$

Fix a prime $\ell \geq 11$. We now explain how V_ℓ breaks up into irreducible representations under the $\mathrm{Gal}_{\mathbb{Q}(i)}$-action. Fix an irreducible $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-submodule W of V_ℓ and set $n := \dim_{\mathbb{F}_\ell} W$. Let $\beta\colon \mathrm{Gal}_{\mathbb{Q}(i)} \to \mathrm{Aut}_{\mathbb{F}_\ell}(W) \cong \mathrm{GL}_n(\mathbb{F}_\ell)$ be the representation describing the Galois action on W. We denote by $W^\vee$ the dual space of W with its obvious $\mathrm{Gal}_{\mathbb{Q}(i)}$-action.

Proposition 3.1. *Fix notation as above and let V_ℓ^{ss} be the semi-simplification of V_ℓ as an $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-module.*

(i) The integer n is either 1 or 2.
(ii) If $n = 1$, then $V_\ell^{\mathrm{ss}} \cong W \oplus W \oplus W^\vee \oplus W^\vee$ and $W \ncong W^\vee$ as $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-modules.
(iii) If $n = 2$, then $V_\ell \cong W \oplus W$ and $W \cong W^\vee$ as $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-modules.

The proposition will be proved by showing that the automorphisms of the surface $X_{\mathbb{Q}(i)}$ constrains the image of ρ_ℓ.

Lemma 3.2. *Let Q be the group of quaternions $\{\pm 1, \pm i, \pm j, \pm k\}$. There is a homomorphism $\varphi\colon Q \to \mathrm{Aut}_{\mathbb{F}_\ell}(V_\ell)$ such that $\varphi(Q)$ commutes with $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ and $\varphi(-1) = -I$.*

Proof. By base extending, we may assume that the varieties U and E and the morphism $f\colon E \to U$ are all defined over $\mathbb{Q}(i)$. Let α_1 and α_2 be the automorphisms of E that are given by $(x, y, t) \mapsto (x, iy, -t)$ and $(x, y, t) \mapsto (t^{-2}x, it^{-1}y, t^{-1})$, respectively. For each $i \in \{1, 2\}$, there is a unique isomorphism $g_i\colon U \to U$ such that $f \circ \alpha_i = g_i \circ f$. Observe that the automorphisms α_i permutes

the fibers of $f\colon E \to U$; moreover, the maps between fibers are isomorphisms of elliptic curves. We find that α_i induces an automorphism of the group variety $E[\ell]$ (though not as a sheaf over U). We thus have a commutative diagram

$$\begin{array}{ccc} E[\ell] & \xrightarrow{\alpha_i}_{\sim} & E[\ell] \\ \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\ U & \xrightarrow[\sim]{g_i} & U. \end{array}$$

where the horizontal morphisms are isomorphisms. The morphisms α_i and g_i thus gives rise to a linear automorphism $\tilde{\alpha}_i$ of $V_\ell = H^1_c(U_{\overline{\mathbb{Q}}}, E[\ell])$.

Let A be the subgroup of automorphisms of E generated by α_1 and α_2. The action of the α_i on V_ℓ thus give rise to a homomorphism $\varphi\colon A \to \mathrm{Aut}_{\mathbb{F}_\ell}(V_\ell)$ satisfying $\varphi(\alpha_i) = \tilde{\alpha}_i^{-1}$. The group $\varphi(A)$ commutes with $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ since the automorphisms α_i are defined over $\mathbb{Q}(i)$. One can readily verify the relations $\alpha_1^4 = \alpha_2^4 = 1$, $\alpha_1^2 = \alpha_2^2 \neq 1$, and $\alpha_1 \circ \alpha_2 \circ \alpha_1^{-1} = \alpha_2^{-1}$, which is enough to ensure that A is isomorphic to the group $Q := \{\pm 1, \pm i, \pm j, \pm k\}$ of quaternions.

Let ι be the automorphism of E defined by $(x, y, t) \mapsto (x, -y, t)$; it is equal to α_1^2 and α_2^2. We need to show that the induced automorphism $\tilde{\iota} := \varphi(\iota)$ of V_ℓ is $-I$. We have $f \circ \iota = f$, so ι is an automorphism of the sheaf $E[\ell]$ on U. Moreover, ι acts as $-I$ on $E[\ell]$. Therefore, $\tilde{\iota}$ acts as $-I$ on V_ℓ. □

Proof of Proposition 3.1. Let Z be the $\mathbb{F}_\ell$-subalgebra of $\mathrm{End}_{\mathbb{F}_\ell}(W)$ consisting of those endomorphisms that commute with the action of $\mathrm{Gal}_{\mathbb{Q}(i)}$. Since W is irreducible, Schur's lemma implies that Z is a finite division ring and is hence a (commutative) field.

Suppose that W is stable under the action of the group Q from Lemma 3.2. Let $\tilde{\varphi}\colon Q \to \mathrm{Aut}_{\mathbb{F}_\ell}(W)$ be the corresponding representation. Since $\tilde{\varphi}(-1) = -I$ and every non-trivial normal subgroup of Q contains -1, we find that $\tilde{\varphi}(Q)$ is isomorphic to Q. Therefore, $\tilde{\varphi}(Q)$ is a non-abelian subgroup of $Z^\times$. However, this contradicts that Z is a field.

Therefore, W is not stable under the action of Q. So there is an element $\gamma \in \varphi(Q)$ such that $\gamma(W) \neq W$. The vector space $\gamma(W)$ is stable under the action of $\mathrm{Gal}_{\mathbb{Q}(i)}$ since $\varphi(Q)$ commutes with $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$. The automorphism γ gives an isomorphism of $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-modules from W to $\gamma(W)$. We have $\gamma(W) \cap W = 0$ since W is irreducible and $\gamma(W) \neq W$. Therefore, $W \oplus \gamma(W)$ is a submodule of V_ℓ with $\gamma(W)$ isomorphic to W. Since V_ℓ has dimension 4, this proves that n is 1 or 2.

If $n = 2$, then $V_\ell = W \oplus \gamma(W) \cong W \oplus W$. The $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-module W is isomorphic to its dual since V_ℓ is isomorphic to its dual by Lemma 2.1(ii).

We now suppose that $n = 1$. There is a submodule of V_ℓ isomorphic to $W \oplus W$. Since V_ℓ is self-dual by Lemma 2.1(ii), there is a submodule of V_ℓ^{ss} isomorphic to $W^\vee \oplus W^\vee$. To finish the proof of (ii), it suffices to show that $W \ncong W^\vee$. Assume to the contrary that $W \cong W^\vee$. This implies that the corresponding character $\beta\colon \mathrm{Gal}_{\mathbb{Q}(i)} \to \mathrm{Aut}_{\mathbb{F}_\ell}(W) = \mathbb{F}_\ell^\times$ and its inverse are equal. Therefore, $\beta(\mathrm{Gal}_{\mathbb{Q}(i)}) \subseteq \{\pm 1\}$, and hence $\det(I + g) = 0$ or $\det(I - g) = 0$ for every $g \in \rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$.

The prime 5 splits in $\mathbb{Q}(i)$ and $\det(I - \rho_\ell(\mathrm{Frob}_5)T) \equiv P_5(T) \pmod{\ell}$, so $P_5(1)$ or $P_5(-1)$ must be divisible by ℓ. However, by Lemma 2.4 we have $P_5(1) = (8/5)^2$ and $P_5(1) = (12/5)^2$ which are not divisible by $\ell \geq 11$. □

4. Ramification at ℓ

Throughout this section, we fix a prime $\ell \geq 11$.

4.1. **Tame inertia.** Let $\overline{\mathbb{Q}}_\ell$ be an algebraic closure of $\mathbb{Q}_\ell$. Let $\mathbb{Q}_\ell^{\mathrm{un}}$ be the maximal unramified extension of $\mathbb{Q}_\ell$ in $\overline{\mathbb{Q}}_\ell$. Let $\mathbb{Q}_\ell^t$ be the maximal tamely ramified extension of $\mathbb{Q}_\ell$ in $\overline{\mathbb{Q}}_\ell$. The subgroup

$\mathcal{I} := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell^{\mathrm{un}})$ of $\mathrm{Gal}_{\mathbb{Q}_\ell}$ is the inertia group. The wild inertia group $\mathcal{P} := \mathrm{Gal}(\overline{\mathbb{Q}}_\ell/\mathbb{Q}_\ell^t)$ is the largest pro-ℓ subgroup of $\mathcal{I}$. The tame inertia group is the quotient $\mathcal{I}_t := \mathcal{I}/\mathcal{P}$.

For each positive integer d relatively prime to ℓ, let μ_d be the d-th roots of unity in $\overline{\mathbb{Q}}_\ell$. The map $\mathcal{I} \to \mu_d$, $\sigma \mapsto \sigma(\sqrt[d]{\ell})/\sqrt[d]{\ell}$ is a surjective homomorphism which factors through $\mathcal{I}_t$. Taking the inverse limit over all d relatively prime to ℓ, we obtain an isomorphism $\mathcal{I}_t \xrightarrow{\sim} \varprojlim_d \mu_d$. The group μ_d lies in the ring of integers $\overline{\mathbb{Z}}_\ell$ of $\overline{\mathbb{Q}}_\ell$. Composing the homomorphism $\mathcal{I}_t \to \mu_d$ with reduction modulo the maximal ideal of $\overline{\mathbb{Z}}_\ell$ gives a character $\mathcal{I}_t \to \overline{\mathbb{F}}_\ell^\times$. For a positive integer m, setting $d := \ell^m - 1$ gives a surjective character $\varepsilon\colon \mathcal{I}_t \to \mathbb{F}_{\ell^m}^\times$. We obtain m characters $\mathcal{I}_t \to \mathbb{F}_{\ell^m}^\times$ by composing ε with the isomorphisms of $\mathbb{F}_{\ell^m}^\times$ arising from field automorphisms of $\mathbb{F}_{\ell^m}$; they are called the fundamental characters of level m. See §1 of [Ser72] for more details.

Let V be an irreducible $\mathbb{F}_\ell[\mathcal{I}]$-module and set $m := \dim_{\mathbb{F}_\ell} V$. The group $\mathcal{P}$ act trivially on V, cf. [Ser72, Proposition 4]. Let Z be the ring of endomomorphisms of V as an $\mathbb{F}_\ell[\mathcal{I}_t]$-module. Since V is irreducible, Z is a division algebra of finite dimension over $\mathbb{F}_\ell$. Therefore, Z is a finite field and V is a vector space of dimension 1 over Z. Choose an isomorphism $Z \cong \mathbb{F}_{\ell^m}$ of fields. The action of $\mathcal{I}_t$ on V corresponds to a character $\alpha\colon \mathcal{I}_t \to Z^\times \cong \mathbb{F}_{\ell^m}^\times$. Let $\varepsilon_1, \dots, \varepsilon_m\colon \mathcal{I}_t \to \mathbb{F}_{\ell^m}^\times$ be the fundamental characters of level m. There are unique integers $e_i \in \{0, 1, \dots, \ell-1\}$ such that $\alpha = \varepsilon_1^{e_1} \cdots \varepsilon_m^{e_m}$. These integers $e_1, \dots, e_m$ are called the tame inertia weights of V.

For an $\mathbb{F}_\ell[\mathcal{I}]$-module V of finite dimension over $\mathbb{F}_\ell$, we define its tame inertia weights to be the integers that occur as the tame inertia weight of some composition factor of V.

The following is a special case of a conjecture of Serre (cf. §1.13 of [Ser72]) and follows from a more general result of Caruso [Car08].

Theorem 4.1 (Caruso)**.** *Let $\mathcal{X}$ be a scheme that is proper and semistable over $\mathbb{Z}_\ell$. For $i < \ell - 1$, the tame inertia weights of $H^i_{\text{ét}}(\mathcal{X}_{\overline{\mathbb{Q}}_\ell}, \mathbb{F}_\ell)^\vee$ belong to the set $\{0, 1, \dots, i\}$.*

We will makes use of the following.

Proposition 4.2. *The tame inertia weights of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}_\ell}, \mathbb{F}_\ell)^\vee$ belong to the set $\{0, 1, 2\}$.*

Proof. After a change of variable in (1.1), we may start with the Weierstrass equation

$$y^2 = x^3 + (t^5 - t)x^2 + (t^8 - 2t^6 + t^4)x;$$

it has discriminant $16t^{10}(t-1)^8(t+1)^8$. Define $C := \mathbb{P}^1_{\mathbb{Z}_\ell}$ with a parameter t. The Weierstrass equation defines a closed subscheme $\mathcal{Y}$ of $\mathbb{P}^2_C$. We have a morphism $\mathcal{Y} \to C$ obtained by composing the inclusion $\mathcal{Y} \subseteq \mathbb{P}^2_C$ with the structure map $\mathbb{P}^2_C \to C$. One can check that the singular subscheme of $\mathcal{Y}$ is reduced and consists of the closure of the points $(0,0,0)$, $(0,0,1)$, $(0,0,-1)$ and a point with $t = \infty$. By resolving the singularities appropriately (more explicitly, by following Tate's algorithm), we can construct a model $\mathcal{X}/\mathbb{Z}_\ell$ of $X_{\mathbb{Q}_\ell}$ that has good reduction. The proposition then follows immediately from Theorem 4.1 (we have $2 < \ell - 1$ by our ongoing assumption $\ell \geq 11$). □

4.2. **Image of inertia.** Let $\mathcal{I}$ be an inertia subgroup of $\mathrm{Gal}_{\mathbb{Q}}$ at ℓ and let $\mathcal{P}$ be the wild inertia subgroup of $\mathcal{I}$. Since ℓ is unramified in $\mathbb{Q}(i)$, the group $\mathcal{I}$ is contained in $\mathrm{Gal}_{\mathbb{Q}(i)}$. Let $\chi_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ be the representation describing the Galois action on the group of ℓ-th roots of unity μ_ℓ, i.e., $\sigma(\zeta) = \zeta^{\chi_\ell(\sigma)}$ for $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$ and $\zeta \in \mu_\ell$.

Let W be an irreducible $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-submodule of V_ℓ. Set $n = \dim_{\mathbb{F}_\ell} W$; it is 1 or 2 by Proposition 3.1(i). Let $\beta\colon \mathrm{Gal}_{\mathbb{Q}(i)} \to \mathrm{Aut}_{\mathbb{F}_\ell}(W) \cong \mathrm{GL}_n(\mathbb{F}_\ell)$ be the representation describing the Galois action on W. The main task of this section is to prove the following proposition.

Proposition 4.3.

(i) If $n = 1$, then $\beta|_{\mathcal{I}} = \chi_\ell^e|_{\mathcal{I}}$ for some $e \in \{-1, 0, 1\}$.

(ii) If $n = 2$, then $\beta(\mathcal{I}) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$.
(iii) The group $\rho_\ell(\mathcal{I})/\rho_\ell(\mathcal{P})$ is cyclic of order 1, $\ell - 1$ or $\ell + 1$.

Lemma 4.4. *If $n = 2$, then $\det(\beta(\mathrm{Gal}_{\mathbb{Q}})) \subseteq \{\pm 1\}$.*

Proof. By Proposition 3.1(iii), W is self-dual so $\det \circ \beta = (\det \circ \beta)^{-1}$. The lemma is now immediate. □

Lemma 4.5. *Let V_ℓ^{ss} be the semi-simplification of V_ℓ as an $\mathbb{F}_\ell[\mathcal{I}]$-module. Let $\mathcal{W}$ be an irreducible $\mathbb{F}_\ell[\mathcal{I}]$-submodule of V_ℓ^{ss}. Set $m := \dim_{\mathbb{F}_\ell} \mathcal{W}$ and let $\alpha \colon \mathcal{I} \to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathcal{W}) \cong \mathrm{GL}_m(\mathbb{F}_\ell)$ be the representation corresponding to $\mathcal{W}$.*

(i) We have $m \leq n$. In particular, m is 1 or 2.
(ii) If $m = 1$, then $\alpha = \chi_\ell^e|_{\mathcal{I}}$ for some $e \in \{-1, 0, 1\}$.
(iii) If $m = 2$, then $\alpha(\mathcal{I})$ is a cyclic group of order $\ell + 1$ contained in $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Proof. We have $\mathcal{I} \subseteq \mathrm{Gal}_{\mathbb{Q}(i)}$ since ℓ is unramified in $\mathbb{Q}(i)$. Part (i) now follows immediately from Proposition 3.1.

Let $\mathcal{H}$ be the semi-simplification of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$ as an $\mathbb{F}_\ell[\mathcal{I}]$-module. By Lemma 2.6, we find that $\mathcal{W}$ is isomorphic to a submodule of $\mathcal{H}$. Therefore, $\mathcal{W}(-1)^\vee$ is isomorphic to a submodule of $\mathcal{H}(-1)^\vee$. So $\mathcal{W}(-1)^\vee$ is isomorphic to a submodule of the semi-simplification of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)^\vee$ as an $\mathbb{F}_\ell[\mathcal{I}]$-module. Proposition 4.2 implies that the possible tame inertia weights of $\mathcal{W}(-1)^\vee$ are 0, 1 and 2.

First suppose that $m = 1$. We then have $(\alpha \cdot \chi_\ell|_{\mathcal{I}}^{-1})^{-1} = \varepsilon^e$ for some $e \in \{0, 1, 2\}$ where $\varepsilon \colon \mathcal{I} \to \mathbb{F}_\ell^\times$ is the fundamental character of level 1. By Proposition 8 of [Ser72], we have $\varepsilon = \chi_\ell|_{\mathcal{I}}$. Therefore, $\alpha = \varepsilon^{-e}\chi_\ell|_{\mathcal{I}} = \chi_\ell|_{\mathcal{I}}^f$ where $f := 1 - e \in \{-1, 0, 1\}$. This proves (ii).

Now suppose that $m = 2$. The irreducible representation α corresponds to a character $\mathcal{I} \to \mathbb{F}_{\ell^2}^\times$ that we also denote by α. Let ε be a fundamental character of level 2. Using Proposition 3.1, we find that $\mathcal{W}$ is self-dual. Therefore, $\mathcal{W}(1)$ is isomorphic to $\mathcal{W}(-1)^\vee$ as an $\mathbb{F}_\ell[\mathcal{I}]$-module, and hence has possible tame inertia weights 0, 1 and 2. So $\alpha = \chi_\ell|_{\mathcal{I}}^{-1} \cdot \varepsilon^{e_1 + \ell e_2}$ with $e_1, e_2 \in \{0, 1, 2\}$. The character $\varepsilon^{1+\ell}$ is fundamental of level 1 and hence agrees with $\chi_\ell|_{\mathcal{I}}$, so $\alpha = \varepsilon^{f_1 + f_2\ell}$ with $f_i := 1 - e_i \in \{-1, 0, 1\}$.

If $f_1 + f_2\ell \in \{0, \pm(\ell + 1)\}$, then the character α is 1, $\chi_\ell|_{\mathcal{I}}$ or $\chi_\ell^{-1}|_{\mathcal{I}}$; this is impossible since $\alpha \colon \mathcal{I} \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is irreducible.

If $f_1 + f_2\ell \in \{\pm 1, \pm\ell\}$, then $\alpha(\mathcal{I})$ is cyclic of order $\ell^2 - 1$ since $\varepsilon(\mathcal{I}) = \mathbb{F}_{\ell^2}^\times$. We have $n = 2$ since $m = 2$. By Proposition 3.1, we deduce that α and $\beta|_{\mathcal{I}}$ are isomorphic representations (we again have $\mathcal{I} \subseteq \mathrm{Gal}_{\mathbb{Q}(i)}$ since ℓ is unramified in $\mathbb{Q}(i)$). Therefore, $\beta(\mathrm{Gal}_{\mathbb{Q}(i)})$ contains a cyclic group C of order $\ell^2 - 1$. By [Ser72, §2.6], C is a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ and satisfies $\det(C) = \mathbb{F}_\ell^\times$. So $\det(\beta(\mathrm{Gal}_{\mathbb{Q}(i)})) = \mathbb{F}_\ell^\times$ which contradicts Lemma 4.4 since $\ell \geq 11$.

Therefore, $f_1 + f_2\ell \in \{\pm(\ell - 1)\}$. This implies that $\alpha(\mathcal{I})$ is cyclic of order $\ell + 1$ and is contained in $\mathrm{SL}_2(\mathbb{F}_\ell)$. □

Proof of Proposition 4.3. We have $\mathcal{I} \subseteq \mathrm{Gal}_{\mathbb{Q}(i)}$ since ℓ is unramified in $\mathbb{Q}(i)$. Let $\mathcal{W}$ be an irreducible $\mathbb{F}_\ell[\mathcal{I}]$-submodule of W and take α and m as in Lemma 4.5.

Suppose that $n = 1$ and hence $\mathcal{W} = W$. Part (i) now follows directly from Lemma 4.5(ii). By part (i) and Proposition 3.1(ii), we deduce that the group $\rho_\ell(\mathcal{I})/\rho_\ell(\mathcal{P})$ is cyclic of order 1 or $\ell - 1$.

We are left to consider the case $n = 2$. First suppose that $\mathcal{W} = W$, and hence we may assume that $\beta|_{\mathcal{I}} = \alpha$. By Lemma 4.5(iii), $\beta(\mathcal{I}) = \alpha(\mathcal{I})$ is a cyclic group of order $\ell + 1$ in $\mathrm{SL}_2(\mathbb{F}_\ell)$. By Proposition 3.1(iii), $\rho_\ell(\mathcal{I})$ is isomorphic to $\beta(\mathcal{I})$ and hence is cyclic of order $\ell + 1$.

The final case is where $n = 2$ and $\dim_{\mathbb{F}_\ell} \mathcal{W} = 1$. Let W^{ss} be the semi-simplification of W as an $\mathbb{F}_\ell[\mathcal{I}]$-module. There is an $\mathbb{F}_\ell[\mathcal{I}]$-module $\mathcal{W}'$ such that $W^{\mathrm{ss}} \cong \mathcal{W} \oplus \mathcal{W}'$. Let $\gamma \colon \mathcal{I} \to \mathbb{F}_\ell^\times$ and $\gamma' \colon \mathcal{I} \to \mathbb{F}_\ell^\times$ be the characters describing the action of $\mathcal{I}$ on $\mathcal{W}$ and $\mathcal{W}'$, respectively. By

Lemma 4.5(ii), there are e and f in $\{-1,0,1\}$ such that $\alpha = \chi_\ell^e|_{\mathcal{I}}$ and $\alpha' = \chi_\ell^{-f}|_{\mathcal{I}}$. So for $\sigma \in \mathcal{I}$, we have

$$\det(I-\beta(\sigma)T) = (1-\alpha(\sigma)T)(1-\alpha'(\sigma)T) = 1-(\chi_\ell(\sigma)^e+\chi_\ell(\sigma)^{-f})T+\chi_\ell(\sigma)^{e-f}T^2.$$

If $e \neq f$, then we find that $\det(\beta(\mathcal{I}))$ is a cyclic group of cardinality at least $(\ell-1)/2 > 2$. However this contradicts Lemma 4.4, so $e = f$. Therefore, $\det(I-\beta(\sigma)T) = 1-(\chi_\ell(\sigma)^e+\chi_\ell(\sigma)^{-e})T+T^2$ for all $\sigma \in \mathcal{I}$. This proves that $\det(\beta(\mathcal{I})) = \{1\}$, i.e., $\beta(\mathcal{I}) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$. We have $\beta(\mathcal{I})/\beta(\mathcal{P}) \cong \alpha(\mathcal{I}) = \chi^e(\mathcal{I})$, so $\beta(\mathcal{I})/\beta(\mathcal{P})$ is a cyclic group of order 1 or $\ell-1$ if $e = 0$ or $e = \pm 1$, respectively. By Proposition 3.1(ii), we deduce that $\rho_\ell(\mathcal{I})/\rho_\ell(\mathcal{P})$ is also cyclic of order 1 or $\ell-1$. □

When $n = 2$ we have the following important constraint on the image of β.

Lemma 4.6. *If $n = 2$, then $\beta(\mathrm{Gal}_{\mathbb{Q}(i)}) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof. By Lemma 4.4, we can define a character $\varepsilon\colon \mathrm{Gal}_{\mathbb{Q}(i)} \to \{\pm 1\}$, $\sigma \mapsto \det(\beta(\sigma))$. We need to show that $\varepsilon = 1$. By Proposition 3.1(iii), we have $V_\ell \cong W \oplus W$ as $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-modules and hence

$$\det(I-\rho_\ell(\sigma)T) = \det(I-\beta(\sigma)T)^2 = (1-\mathrm{tr}(\beta(\sigma))T+\epsilon(\sigma)T^2)^2 \tag{4.1}$$

for $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$. Since 5 splits in $\mathbb{Q}(i)$, Frob_5 and Frob_3^2 belong to $\mathrm{Gal}_{\mathbb{Q}(i)}$. By (4.1) and Lemma 2.4, we have:

$$(1-\mathrm{tr}(\beta(\mathrm{Frob}_5))T+\det(\beta(\mathrm{Frob}_5))T^2)^2 \equiv P_5(T) = (1-2/5\cdot T+T^2)^2 \pmod{\ell}$$
$$(1-\mathrm{tr}(\beta(\mathrm{Frob}_3^2))T+\det(\beta(\mathrm{Frob}_3^2))T^2)^2 \equiv P_3^{(2)}(T) = (1-2/9\cdot T+T^2)^2 \pmod{\ell}.$$

From the unique factorization of $\mathbb{F}_\ell[T]$, we deduce that $\varepsilon(\mathrm{Frob}_3^2) = 1$ and $\varepsilon(\mathrm{Frob}_5) = 1$.

We claim that the character ε is unramified at all finite places v of $\mathbb{Q}(i)$ that do not lie over 2. Fix a finite place v of $\mathbb{Q}(i)$ that does not lie over 2. If v does not lie over ℓ, then ε is unramified at v since ρ_ℓ is unramified at primes $p \nmid 2\ell$. So suppose that v lies over ℓ. Let $\mathcal{I}$ be an inertia subgroup of $\mathrm{Gal}_{\mathbb{Q}(i)}$ at v. Since ℓ is unramified in $\mathbb{Q}(i)$, the group $\mathcal{I}$ is also an inertia subgroup of $\mathrm{Gal}_{\mathbb{Q}}$ at ℓ. By Proposition 4.3(ii), we have $\beta(\mathcal{I}) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$ and hence $\varepsilon(\mathcal{I}) = 1$.

Now let K be the fixed field in $\overline{\mathbb{Q}}$ of $\ker(\varepsilon)$. We have $[K:\mathbb{Q}(i)] \leq 2$ and the extension $K/\mathbb{Q}(i)$ is unramified at all finite places not lying over 2. Since $\mathbb{Z}[i]$ is a PID, K can thus be obtained by adjoining to $\mathbb{Q}(i)$ the square root of a squarefree element $a \in \mathbb{Z}[i]$ that is not divisibly by any prime of $\mathbb{Z}[i]$ except $1+i$. So a is of the form $\pm i^e(1+i)^f$ with $e, f \in \{0,1\}$. Therefore, K is the field obtained by adjoining to $\mathbb{Q}(i)$ the square-root of some $a \in \{1, i, 1+i, i(1+i)\}$.

Let $\mathfrak{p}_5$ be the prime ideal of $\mathbb{Z}[i]$ generated by $2+i$. We have $\varepsilon(\mathrm{Frob}_{\mathfrak{p}_5}) = \varepsilon(\mathrm{Frob}_5) = 1$ and hence $\mathfrak{p}_5$ splits in K. Therefore, a modulo $\mathfrak{p}_5$ is a square. We have $i \equiv -2 \pmod{\mathfrak{p}_5}$ and $i(1+i) \equiv 2 \pmod{\mathfrak{p}_5}$. Since 2 and -2 are not squares in $\mathbb{Z}[i]/\mathfrak{p}_5 \cong \mathbb{F}_5$, we deduce that $a \in \{1, 1+i\}$.

Let $\mathfrak{p}_3$ be the prime ideal of $\mathbb{Z}[i]$ generated by 3. We have $\varepsilon(\mathrm{Frob}_{\mathfrak{p}_3}) = \varepsilon(\mathrm{Frob}_3^2) = 1$ and hence $\mathfrak{p}_3$ splits in K. Therefore, a modulo $\mathfrak{p}_3$ is a square. One can check that the image of $1+i$ modulo $\mathfrak{p}_3$ generates the group $(\mathbb{Z}[i]/\mathfrak{p}_3)^\times$ which is a cyclic group of order 8; in particular, $1+i$ is not a square modulo $\mathfrak{p}_3$. Therefore, $a = 1$. So $K = \mathbb{Q}(i)$ and hence $\varepsilon = 1$. □

4.3. **L-functions with $p \equiv 1 \pmod 4$.** In this section, we show that the polynomial $P_p(T)$ with $p \equiv 1 \pmod 4$ are of a special form; we will consider the primes $p \equiv 3 \pmod 4$ in §5.3.

Proposition 4.7. *For each prime $p \equiv 1 \pmod 4$, we have $P_p(T) = (1+bT+T^2)^2$ for a unique $b \in \mathbb{Z}[1/p]$.*

In terms of our representations ρ_ℓ, we have the following:

Lemma 4.8. *For every $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$, we have $\det(I-\rho_\ell(\sigma)T) = (1+bT+T^2)^2$ for a unique $b \in \mathbb{F}_\ell$.*

Proof. Fix notation as in the beginning of §3 and take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$. If $n = 1$, then Proposition 3.1(ii) implies that

$$\det(I - \rho_\ell(\sigma)T) = (1 - \beta(\sigma)T)^2(1 - \beta(\sigma)^{-1}T)^2 = (1 - (\beta(\sigma) + \beta(\sigma)^{-1})T + T^2)^2.$$

This proves (i) in the case $n = 1$; the uniqueness follows from unique factorization.

We now assume that $n = 2$. By Proposition 3.1(iii), we have $V_\ell \cong W \oplus W$ as $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-modules. Therefore,

$$\det(I - \rho_\ell(\sigma)T) = \det(I - \beta(\sigma)T)^2 = (1 - \mathrm{tr}(\beta(\sigma))T + T^2)^2$$

where the last equality uses Lemma 4.6. □

Proof of Propositions 4.7. By Lemma 4.8, for each odd prime p and prime $\ell \geq 11$ with $\ell \neq p$, we have

$$P_p(T) \equiv \det(I - \rho_\ell(\mathrm{Frob}_p)T) = (1 + bT + T^2)^2 \pmod{\ell}$$

for some $b \in \mathbb{F}_\ell$. Since $P_p(T)$ modulo ℓ is of the form $(1+bT+T^2)^2$ for all but finitely many primes ℓ, we deduce that $P_p(T)$ is of the form $(1 + bT + T^2)^2$ for some $b \in \mathbb{Q}$. Therefore, $L(T, E_p) = P_p(pT) = (1+bpT+p^2T^2)^2$. Since $L(T, E_p)$ has integer coefficients, unique factorization shows that b is unique and that $bp \in \mathbb{Z}$. This completes the proof of Proposition 4.7. □

5. Orthogonal groups

Throughout this section, we fix a prime $\ell \geq 11$.

5.1. **The group $\Omega(V_\ell)$.** Let $\mathrm{sp}\colon \mathrm{O}(V_\ell) \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ be the spinor norm, cf. [Zas62]. If $v \in V_\ell$ satisfies $\langle v, v\rangle \neq 0$, let $r_v \in \mathrm{O}(V_\ell)$ be the reflection across v (we have $r_v(v) = -v$ and $r_v(w) = w$ for all $w \in V_\ell$ such that $\langle v, w\rangle = 0$). The spinor norm can be characterized by the property that it is the group homomorphism which satisfies $\mathrm{sp}(r_v) = \langle v, v\rangle \cdot (\mathbb{F}_\ell^\times)^2$ for all $v \in V_\ell$ for which $\langle v, v\rangle \neq 0$.

We will use the following to compute spinor norms; it follows from equation (2.1) of [Zas62, §2] and uses that V_ℓ has dimension 4.

Lemma 5.1. *If $A \in \mathrm{O}(V_\ell)$ satisfies $\det(I + A) \neq 0$, then $\mathrm{sp}(A) = \det(I + A) \cdot (\mathbb{F}_\ell^\times)^2$.* □

Let $\Omega(V_\ell)$ be the simultaneous kernel of $\det\colon \mathrm{O}(V_\ell) \to \{\pm 1\}$ and $\mathrm{sp}\colon \mathrm{O}(V_\ell) \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$. We could also define $\Omega(V_\ell)$ as the commutator subgroup of $\mathrm{O}(V_\ell)$. We now show that the image of ρ_ℓ lies in this smaller group.

Lemma 5.2. *We have $-I \in \Omega(V_\ell)$ and $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \Omega(V_\ell)$.*

Proof. We have $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}}) \subseteq \mathrm{SO}(V_\ell)$ by Lemma 2.2 and $\det(-I) = (-1)^4 = 1$. It thus remains to show that $\mathrm{sp}(-I) = (\mathbb{F}_\ell^\times)^2$ and that $\mathrm{sp}(\rho_\ell(\sigma)) = (\mathbb{F}_\ell^\times)^2$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$.

By Lemma 2.4, we have $\det(I - \rho_\ell(\mathrm{Frob}_3)T) \equiv P_3(T) = 1 - 2/9 \cdot T^2 + T^4 \pmod{\ell}$. Since $\det(I \pm \rho_\ell(\mathrm{Frob}_3)) \equiv P_3(\pm 1) = (4/3)^2 \pmod{\ell}$, Lemma 5.1 implies that $\mathrm{sp}(\rho_\ell(\mathrm{Frob}_3))$ and $\mathrm{sp}(-\rho_\ell(\mathrm{Frob}_3))$ both equal $(\mathbb{F}_\ell^\times)^2$. Therefore, $\mathrm{sp}(-I) = \mathrm{sp}(\rho_\ell(\mathrm{Frob}_3)) \cdot \mathrm{sp}(-\rho_\ell(\mathrm{Frob}_3)) = (\mathbb{F}_\ell^\times)^2$. Since 3 is inert in $\mathbb{Q}(i)$ and $\mathrm{sp}(\rho_\ell(\mathrm{Frob}_3)) = (\mathbb{F}_\ell^\times)^2$, it suffices to show that $\mathrm{sp}(\rho_\ell(\sigma)) = (\mathbb{F}_\ell^\times)^2$ for all $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$.

Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$. By Lemma 4.8, we have $\det(I - \rho_\ell(\sigma)T) = (1 + bT + T^2)^2$ for a unique $b \in \mathbb{F}_\ell$. If $b \neq 2$, then by Lemma 5.1 we have

$$\mathrm{sp}(\rho_\ell(\sigma)) = \det(I + \rho_\ell(\sigma)) \cdot (\mathbb{F}_\ell^\times)^2 = (2 - b)^2 \cdot (\mathbb{F}_\ell^\times)^2 = (\mathbb{F}_\ell^\times)^2.$$

So suppose that $b = 2$, and hence $\det(I - \rho_\ell(\sigma)T) = (1 + 2T + T^2)^2 = (1 + T)^4$. Since ℓ is odd, there is an $e \geq 0$ such that $\rho_\ell(\sigma)^{\ell^e} = -I$. Therefore, $\mathrm{sp}(\rho_\ell(\sigma)) = \mathrm{sp}(\rho_\ell(\sigma))^{\ell^e} = \mathrm{sp}(-I) = (\mathbb{F}_\ell^\times)^2$. □

5.2. **The representation ϑ_ℓ.** Define the 4-dimensional $\mathbb{F}_\ell$-vector space $\mathcal{V}_\ell := \mathbb{F}_\ell^2 \otimes_{\mathbb{F}_\ell} \mathbb{F}_\ell^2$. We have a natural action of $\mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$ on $\mathcal{V}_\ell$ with $(-I, -I)$ acting trivially; we denote the image in $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathcal{V}_\ell)$ by $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SL}_2(\mathbb{F}_\ell)$.

Lemma 5.3. *There is an isomorphism $V_\ell \cong \mathcal{V}_\ell$ of vector spaces such that the induced isomorphism $\mathrm{Aut}_{\mathbb{F}_\ell}(V_\ell) \cong \mathrm{Aut}_{\mathbb{F}_\ell}(\mathcal{V}_\ell)$ of groups gives an isomorphism $\psi_\ell \colon \Omega(V_\ell) \xrightarrow{\sim} \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof. Let $\{e, f\}$ be the standard basis of the vector space $\mathcal{W} := \mathbb{F}_\ell^2$ over $\mathbb{F}_\ell$. Let $h \colon \mathcal{W} \times \mathcal{W} \to \mathbb{F}_\ell$ be the alternating bilinear pairing that satisfies $h(e, f) = 1$. The group of automorphisms of the vector space $\mathcal{W}$ that respect the pairing h is $\mathrm{SL}(\mathcal{W}) = \mathrm{SL}_2(\mathbb{F}_\ell)$. Let b be the bilinear pairing on $\mathcal{V}_\ell = \mathcal{W} \otimes_{\mathbb{F}_\ell} \mathcal{W}$ that satisfies $b(v_1 \otimes w_1, v_2 \otimes w_2) = h(v_1, v_2)h(w_1, w_2)$. One can show that b is symmetric and non-degenerate.

As before, we can define $\mathrm{O}(\mathcal{V}_\ell)$ to be the group of automorphisms of $\mathcal{V}_\ell$ that preserve the pairing b, and we define $\Omega(\mathcal{V}_\ell)$ to be the simultaneous kernels of the determinant $\det \colon \mathrm{O}(\mathcal{V}_\ell) \to \{\pm 1\}$ and the spinor norm $\mathrm{sp}_{\mathcal{V}_\ell} \colon \mathrm{O}(\mathcal{V}_\ell) \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$. By [Zas62, (2.3)], $\mathrm{sp}_{\mathcal{V}_\ell}(-I)$ agrees with the discriminant of the pairing b on $\mathcal{V}_\ell$. One can then check that $\mathrm{sp}_{\mathcal{V}_\ell}(-I) = (\mathbb{F}_\ell^\times)^2$.

Up to isomorphism, there are two 4-dimensional vector spaces over $\mathbb{F}_\ell$ equipped with a bilinear, symmetric and non-degenerate pairing. They can be distinguished by the spinor norm of $-I$ (see [Ser73, IV §1.7] where it is stated in terms of quadratic forms; the discriminant of the corresponding quadratic form agrees with the spinor norm of $-I$). We have $\dim_{\mathbb{F}_\ell} \mathcal{V}_\ell = 4 = \dim_{\mathbb{F}_\ell} V_\ell$ and $\mathrm{sp}_{\mathcal{V}_\ell}(-I) = (\mathbb{F}_\ell^\times)^2 = \mathrm{sp}(-I)$ where the last equality uses Lemma 5.2. There is thus an isomorphism $\varphi \colon \mathcal{V}_\ell \to V_\ell$ of $\mathbb{F}_\ell$-vector spaces such that $\langle \varphi(v), \varphi(w) \rangle = b(v, w)$ for all $v, w \in \mathcal{V}_\ell$. It now suffices to prove the lemma for $\Omega(\mathcal{V}_\ell)$ instead of $\Omega(V_\ell)$.

Since $\mathrm{sp}_{\mathcal{V}_\ell}(-I) = (\mathbb{F}_\ell^\times)^2$, $\Omega(\mathcal{V}_\ell)$ is isomorphic to the group denoted by $\Omega_4^+(\ell)$ in [CCN+85, §2]. There is an exceptional isomorphism $\Omega_4^+(\ell)/\{\pm I\} \cong \mathrm{PSL}_2(\mathbb{F}_\ell) \times \mathrm{PSL}_2(\mathbb{F}_\ell)$, so $\Omega(\mathcal{V}_\ell)/\{\pm I\}$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_\ell) \times \mathrm{PSL}_2(\mathbb{F}_\ell)$. We have a natural action of $\mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$ on $\mathcal{V}_\ell$ with $(-I, -I)$ acting trivially. This action respects the pairing b and gives rise to an injective homomorphism

$$\xi \colon \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SL}_2(\mathbb{F}_\ell) = (\mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell))/\{\pm(I, I)\} \hookrightarrow \Omega(\mathcal{V}_\ell). \tag{5.1}$$

Quotienting out by the subgroup generated by $(I, -I)$, ξ gives rise to an injective homomorphism $\bar{\xi} \colon \mathrm{PSL}_2(\mathbb{F}_\ell) \times \mathrm{PSL}_2(\mathbb{F}_\ell) \hookrightarrow \Omega(\mathcal{V}_\ell)/\{\pm I\}$ that must be an isomorphism by cardinality considerations. That $\bar{\xi}$ is an isomorphism implies that ξ is also an isomorphism. □

Let $\widetilde{\rho}_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SL}_2(\mathbb{F}_\ell)$ be the representation obtained by composing ρ_ℓ with the isomorphism ψ_ℓ of Lemma 5.3 (this of course uses Lemma 5.2). Let

$$\vartheta_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{PSL}_2(\mathbb{F}_\ell)$$

be the homomorphism obtained by composing $\widetilde{\rho}_\ell$ with the homomorphism $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SL}_2(\mathbb{F}_\ell) \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ which maps $A \otimes B$ to the image of A in $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Similarly, we define $\vartheta'_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ except projecting on the second factor.

Lemma 5.4. *After possibly switching ϑ_ℓ and ϑ'_ℓ, we may assume that the group $\vartheta'_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ has cardinality 1 or ℓ. For $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$, we have $\mathrm{tr}(\vartheta_\ell(\sigma)) = \pm b$ where $\det(I - \rho_\ell(\sigma)T) = (1 + bT + T^2)^2$.*

Proof. Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$. Choose $A, B \in \mathrm{SL}_2(\mathbb{F}_\ell)$ such that $\psi_\ell(\rho_\ell(\sigma)) = \widetilde{\rho}_\ell(\sigma)$ equals $A \otimes B$. Take $\lambda_1, \lambda_2 \in \overline{\mathbb{F}}_\ell^\times$ such that the eigenvalues of A and B are $\{\lambda_1, \lambda_1^{-1}\}$ and $\{\lambda_2, \lambda_2^{-1}\}$, respectively. The roots of $\det(I - \rho_\ell(\sigma)T) = \det(I - \widetilde{\rho}_\ell(\sigma)T)$ in $\overline{\mathbb{F}}_\ell$ are thus $\lambda_1\lambda_2$, $\lambda_1\lambda_2^{-1}$, $\lambda_1^{-1}\lambda_2$ and $\lambda_1^{-1}\lambda_2^{-1}$.

We claim that the image of A or B in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ has order belonging to $\{1, \ell\}$. It suffices to prove that $\lambda_1 = \pm 1$ or $\lambda_2 = \pm 1$. Since $\det(I - \rho_\ell(\sigma)T)$ is a square by Lemma 4.8, $\lambda_1\lambda_2^{-1}$ equals $\lambda_1\lambda_2$, $\lambda_1^{-1}\lambda_2^{-1}$ or $\lambda_1^{-1}\lambda_2$. If $\lambda_1\lambda_2^{-1} = \lambda_1\lambda_2$, then $\lambda_2 = \pm 1$. If $\lambda_1\lambda_2^{-1} = \lambda_1^{-1}\lambda_2^{-1}$, then $\lambda_1 = \pm 1$. Finally, suppose that $\lambda_1\lambda_2^{-1}$ equals $\lambda_1^{-1}\lambda_2 = (\lambda_1\lambda_2^{-1})^{-1}$ and hence $\lambda_1 = \varepsilon\lambda_2$ for some $\varepsilon \in \{\pm 1\}$. The roots of

$\det(I-gT)$ are thus $\varepsilon\lambda_2^2$, ε, ε and $\varepsilon\lambda_2^{-2}$. Since $\det(I-\rho_\ell(\sigma)T)$ is a square, we have $\varepsilon\lambda_2^2=\varepsilon\lambda_2^{-2}$ and hence $\lambda_2^4=1$. So if $\lambda_2\neq\pm1$, then $\lambda_2^2=-1$ and hence $\det(I-gT)=(1-T)^2(1+T)^2=(1-T^2)^2$; however, this is impossible by Lemma 4.8. This proves the claim.

If the image of B in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ has order 1 or ℓ, then λ_2 equals some $\varepsilon\in\{\pm1\}$ and hence $\det(I-\rho_\ell(\sigma)T)=(1-\varepsilon\lambda_1T)^2(1-\varepsilon\lambda_1^{-1}T)^2=(1-\varepsilon(\lambda_1+\lambda_1^{-1})T+T^2)^2=(1-\varepsilon\,\mathrm{tr}(A)T+T^2)^2$.

To complete the proof of the lemma, it remains to show, after possibly swapping ϑ_ℓ and ϑ'_ℓ, that $\vartheta'_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ has cardinality 1 or ℓ. If this is not true, then there are elements σ_1 and σ_2 of $\mathrm{Gal}_{\mathbb{Q}(i)}$ such that $\vartheta_\ell(\sigma_1)^\ell\neq1$ and $\vartheta'_\ell(\sigma_2)^\ell\neq1$. The order of $\vartheta'_\ell(\sigma_1)$ and $\vartheta_\ell(\sigma_2)$ are 1 or ℓ by our claim. After replacing σ_1 and σ_2 by an ℓ-th power, we may assume that $\vartheta_\ell(\sigma_2)=1$ and $\vartheta'_\ell(\sigma_1)=1$. So with $\sigma:=\sigma_1\sigma_2$ we have $\vartheta_\ell(\sigma)^\ell\neq1$ and $\vartheta'_\ell(\sigma)^\ell\neq1$. This is a contradiction since $\vartheta_\ell(\sigma)^\ell=1$ or $\vartheta'_\ell(\sigma)^\ell=1$ by our claim. □

From now on, we take $\vartheta_\ell\colon\mathrm{Gal}_{\mathbb{Q}}\to\mathrm{PSL}_2(\mathbb{F}_\ell)$ and $\vartheta'_\ell\colon\mathrm{Gal}_{\mathbb{Q}}\to\mathrm{PSL}_2(\mathbb{F}_\ell)$ as in Lemma 5.4.

Lemma 5.5. *For $\sigma\in\mathrm{Gal}_{\mathbb{Q}}-\mathrm{Gal}_{\mathbb{Q}(i)}$, we have $\mathrm{tr}(\vartheta_\ell(\sigma))=\pm b$ for some $b\in\mathbb{F}_\ell$ which satisfies $\det(I-\rho_\ell(\sigma)T)=1+(b^2-2)T^2+T^4$.*

Proof. Fix $\sigma\in\mathrm{Gal}_{\mathbb{Q}}-\mathrm{Gal}_{\mathbb{Q}(i)}$. Choose $A,B\in\mathrm{SL}_2(\mathbb{F}_\ell)$ such that $\psi_\ell(\rho_\ell(\sigma))=\widetilde{\rho}_\ell(\sigma)$ equals $A\otimes B$. The image of A and B in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is $\vartheta_\ell(\sigma)$ and $\vartheta'_\ell(\sigma)$, respectively. Take $\lambda_1,\lambda_2\in\overline{\mathbb{F}}_\ell^\times$ such that the eigenvalues of A and B are $\{\lambda_1,\lambda_1^{-1}\}$ and $\{\lambda_2,\lambda_2^{-1}\}$, respectively. The roots of $\det(I-\rho_\ell(\sigma)T)$ in $\overline{\mathbb{F}}_\ell$ are thus $\lambda_1\lambda_2$, $\lambda_1\lambda_2^{-1}$, $\lambda_1^{-1}\lambda_2$ and $\lambda_1^{-1}\lambda_2^{-1}$.

By Lemma 5.4 and our choice of ϑ'_ℓ, the coset of B^2 in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ has order 1 or ℓ. Therefore, $\lambda_2^4=1$. Since the group $\vartheta'_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ has order 1 or ℓ by Lemma 5.4, we find that λ_2, up to a sign, does not depend on the initial choice of $\sigma\in\mathrm{Gal}_{\mathbb{Q}}-\mathrm{Gal}_{\mathbb{Q}(i)}$.

Suppose that $\lambda_2=\pm1$, and hence $\det(I-\rho_\ell(\sigma)T)$ equals $\det(I-AT)^2$ or $\det(I+AT)^2$ for each $\sigma\in\mathrm{Gal}_{\mathbb{Q}}-\mathrm{Gal}_{\mathbb{Q}(i)}$. Since 3 is inert in $\mathbb{Q}(i)$, the polynomial $P_3(T)\equiv\det(I-\rho_\ell(\mathrm{Frob}_3)T)\pmod{\ell}$ must be a square. The discriminant of $P_3(T)$, by Lemma 2.4, is $2^{16}5^2/3^8$. Since $\ell\geq11$, we find that $P_3(T)\pmod{\ell}$ is separable which contradicts that it is a square.

Therefore, λ_2 is a primitive 4-th root of unity and hence

$$\begin{aligned}\det(I-(A\otimes B)T)&=(1-\lambda_1\lambda_2T)(1-\lambda_1\lambda_2^{-1}T)(1-\lambda_1^{-1}\lambda_2T)(1-\lambda_1^{-1}\lambda_2^{-1}T)\\&=(1-\lambda_1(\lambda_2+\lambda_2^{-1})T+\lambda_1^2T^2)(1-\lambda_1^{-1}(\lambda_2+\lambda_2^{-1})T+\lambda_1^{-2}T^2)\\&=(1+\lambda_1^2T^2)(1+\lambda_1^{-2}T^2)\\&=1+(\lambda_1^2+\lambda_1^{-2})T^2+T^4=1+((\mathrm{tr}\,A)^2-2)T^2+T^4.\end{aligned}$$

The lemma is now immediate. □

5.3. **L-functions with $p\equiv3\pmod4$.** We now show that the polynomial $P_p(T)$ with $p\equiv3\pmod4$ are of a special form; we considered the primes $p\equiv1\pmod4$ in §4.3.

Proposition 5.6. *For each prime $p\equiv3\pmod4$, we have $P_p(T)=1+(b^2-2)T^2+T^4$ for a unique non-negative $b\in\mathbb{Z}[1/p]$.*

Proof. Fix a prime $p\equiv3\pmod4$. By Lemma 5.5, for each prime $\ell\geq11$ with $\ell\neq p$ we have

$$P_p(T)\equiv\det(I-\rho_\ell(\mathrm{Frob}_p)T)=1+(b^2-2)T^2+T^4\pmod{\ell}$$

for some $b\in\mathbb{F}_\ell$. Since $P_p(T)$ modulo ℓ is of the form $1+(b^2-2)T^2+T^4$ modulo ℓ for all but finitely many primes ℓ, we deduce that $P_p(T)$ is of the form $1+(b^2-2)T^2+T^4$ for some $b\in\mathbb{Q}$. Therefore, $L(T,E_p)=P_p(pT)=1+(p^2b^2-2p^2)T^2+p^4T^4$. Since $L(T,E_p)$ has integer coefficients, unique factorization shows that b^2 is uniquely determined and that $bp\in\mathbb{Z}$. Uniqueness for b is obtained by imposing the condition $b\geq0$. □

6. Ramification at 2

Fix an inertia subgroup $\mathcal{I}_2$ of $\mathrm{Gal}_{\mathbb{Q}}$ at the prime 2. The goal of this section is to prove the following.

Proposition 6.1. *For any prime $\ell \geq 11$ and $g \in \mathcal{I}_2$, $\rho_\ell(g)^{12}$ is unipotent.*

Take any $\ell \geq 11$. Let

$$\varphi_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Q}_\ell}(H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell))$$

be the representation describing the Galois action on $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$. Grothendieck proved that there is an open subgroup $\mathcal{I}'$ of $\mathcal{I}_2$ such that $\varphi_\ell(g)$ is unipotent for all $g \in \mathcal{I}'$; see the appendix of [ST68]. Thus for each $g \in \mathcal{I}_2$, some positive power of $\varphi_\ell(g)$ is unipotent. For each $g \in \mathcal{I}_2$, let m_g be the smallest positive integer for which $\varphi_\ell(g)^{m_g}$ is unipotent.

Lemma 6.2. *The integer m_g does not depend on ℓ.*

Proof. Take any $g \in \mathcal{I}_2$. It suffices to show that $\varphi_\ell(g)$ is unipotent for one prime ℓ if and only if it is unipotent for all ℓ. Let d be the dimension of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell)$ over $\mathbb{Q}_\ell$; it does not depend on ℓ.

Define $t_g := \mathrm{tr}(\varphi_\ell(g))$. Since some power of $\varphi_\ell(g)$ is unipotent, we find that the eigenvalues of $\varphi_\ell(g)$ are roots of unity. Therefore, $\varphi_\ell(g)$ is unipotent if and only if $t_g = d$. It thus suffices to show that t_g is an integer that does not depend on ℓ. This follows from Corollary 2.5 of [Och99] and uses that X is a smooth proper surface. □

Let ϕ_ℓ be the Galois representation of §1.3. For a prime ℓ and $g \in \mathcal{I}_2$, let $n_{g,\ell}$ be the smallest positive integer for which $\phi_\ell(g)^{n_{g,\ell}}$ is unipotent.

Lemma 6.3. *Take any prime $\ell \geq 11$ and $g \in \mathcal{I}_2$.*

(i) The integer $n_{g,\ell}$ divides m_g.
(ii) If $\ell \nmid m_g$, then $m_g = n_{g,\ell}$.

Proof. By Lemma A.10, we can identify φ_ℓ with the representation $\mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(\Lambda)$ describing the Galois action on $\Lambda := H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}_\ell)$. Again by Lemma A.10, the quotient $\Lambda/\ell\Lambda$ is isomorphic to $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell)$ and the action of $\mathrm{Gal}_{\mathbb{Q}}$ on the quotient gives rise to ϕ_ℓ. Since $\varphi_\ell(g)^{m_g}$ is unipotent, we deduce that $\phi_\ell(g)^{m_g}$ is unipotent. Therefore, $n_{g,\ell}$ divides m_g and $m_g/n_{g,\ell}$ is a power of ℓ. This proves (i) and we have $m_g = n_{g,\ell}$ when $\ell \nmid m_g$. □

Proof of Proposition 6.1. Fix $g \in \mathcal{I}_2$. Take any prime $\ell \geq 11$. By Lemma 2.6, $n_{g,\ell}$ is also the smallest positive integer for which $\rho_\ell(g)^{n_{g,\ell}}$ is unipotent. By Lemma 6.3(i), it suffices to prove that m_g divides 12.

Now take any prime $\ell \geq 11$ which does not divide m_g. By Lemma 6.3(ii), m_g is the smallest positive integer for which $\rho_\ell(g)^{m_g}$ is unipotent.

The order of $\vartheta'_\ell(g)$ divides 2. The order of any element of $\mathrm{PSL}_2(\mathbb{F}_\ell)$, and in particular $\vartheta_\ell(g)$, divides ℓ, $(\ell-1)/2$ or $(\ell+1)/2$. Therefore, the order of the image of $\rho_\ell(g)$ in $\Omega(V_\ell)/\{\pm I\}$ divides 2ℓ, $\mathrm{lcm}(2, (\ell-1)/2)$ or $\mathrm{lcm}(2, (\ell+1)/2)$. The order $e_{g,\ell}$ of $\rho_\ell(g)$ thus divides 4ℓ, $\mathrm{lcm}(4, \ell-1)$ or $\mathrm{lcm}(4, \ell+1)$.

Since m_g divides $e_{g,\ell}$ and is not divisible by ℓ, we deduce that m_g divides $\mathrm{lcm}(4, \ell-1)$ or $\mathrm{lcm}(4, \ell+1)$ for all sufficiently large primes ℓ. Using Dirichlet's theorem on arithmetic progressions, we can then deduce from this that m_g divides 12. □

7. Proof of Theorems 1.1, 1.3 and 1.4

Fix a prime $\ell \geq 11$. Let $\mathcal{I}$ and $\mathcal{I}_2$ be inertia subgroups of $\mathrm{Gal}_{\mathbb{Q}}$ corresponding to the primes ℓ and 2, respectively.

Let $\rho_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{O}(V_\ell)$ be the representation of §1.2; its image is contained in $\Omega(V_\ell)$ by Lemma 5.2. Let ϑ_ℓ and ϑ'_ℓ be the homomorphisms $\mathrm{Gal}_{\mathbb{Q}} \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ from §5.2 chosen so that they satisfy the conclusion of Lemma 5.4.

We shall prove that ϑ_ℓ is surjective. To do this, we first describe the maximal subgroups of $\mathrm{PSL}_2(\mathbb{F}_\ell)$. The description of subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ from §2.4 and §2.6 of [Ser72] shows that if M is a maximal subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$, then one of the following holds:

- M is a Borel subgroup,
- M is the normalizer of a Cartan subgroup,
- M is isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$.

A Borel subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is a group whose inverse image in $\mathrm{SL}_2(\mathbb{F}_\ell)$ is conjugate to the subgroup of upper triangular matrices.

A Cartan subgroup C of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is a maximal cyclic subgroup whose order is relatively prime to ℓ. The group C is cyclic of order $(\ell-1)/2$ or $(\ell+1)/2$; we say that C is split or non-split, respectively. Let N be the normalizer of C in $\mathrm{PSL}_2(\mathbb{F}_\ell)$. The group C has index 2 in N and one can show that $\mathrm{tr}(A) = 0$ for all $A \in N - C$.

7.1. **Borel case.** Assume that $\vartheta_\ell(\mathrm{Gal}_{\mathbb{Q}})$ is contained in a Borel subgroup $\overline{B}$ of $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Let B be the inverse image of $\overline{B}$ under the quotient homomorphism $\mathrm{SL}_2(\mathbb{F}_\ell) \to \mathrm{PSL}_2(\mathbb{F}_\ell)$. There is a non-zero vector $v \in \mathbb{F}_\ell^2$ such that the subspace $\mathbb{F}_\ell \cdot v$ is stable under the action of B. Let $\varphi\colon B \to \mathbb{F}_\ell^\times$ be the homomorphism such that $Av = \varphi(A)v$ for all $A \in B$; it gives rise to a character $\overline{\varphi}\colon \overline{B} \to \mathbb{F}_\ell^\times/\{\pm 1\}$. Let $\alpha\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_\ell^\times/\{\pm 1\}$ be the character $\overline{\varphi} \circ \vartheta_\ell$.

Lemma 7.1. *For each $\sigma \in \mathrm{Gal}_{\mathbb{Q}(i)}$, there is a root $a \in \mathbb{F}_\ell^\times$ of $\det(I - \rho_\ell(\sigma)T)$ whose image in $\mathbb{F}_\ell^\times/\{\pm 1\}$ is $\alpha(\sigma)$.*

Proof. Choose a matrix $A \in \mathrm{SL}_2(\mathbb{F}_\ell)$ whose image in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is $\vartheta_\ell(\sigma)$. By Lemma 5.4, after possibly replacing A by $-A$, we have $\det(I - \rho_\ell(\sigma)T) = (1 - \mathrm{tr}(A)T + T^2)^2$. Since A belong to B, $\varphi(A)$ is a root of $\det(I - \rho_\ell(\sigma)T) = (1 - \mathrm{tr}(A)T + T^2)^2$. So $\varphi(A) \in \mathbb{F}_\ell^\times$ is a representative of $\overline{\varphi}(\vartheta_\ell(\sigma)) = \alpha(\sigma)$ and a root of $\det(I - \rho_\ell(\sigma)T)$. □

Lemma 7.2. *There is an integer $e \in \{-1, 0, 1\}$ such that the character $\gamma\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_\ell^\times/\{\pm 1\}$ given by $\sigma \mapsto \alpha(\sigma) \cdot \chi_\ell(\sigma)^{-e}$ is unramified at all odd primes.*

Proof. Fix a $\tau \in \mathcal{I}$ whose image topologically generates $\mathcal{I}_t$. By Lemma 7.1, there is a representative $a \in \mathbb{F}_\ell^\times$ of $\alpha(\tau)$ which is a root of $\det(I - \rho_\ell(\tau)T)$. So there is a one-dimensional subspace $\mathcal{W}$ of V_ℓ which is stable under the action of $\mathcal{I}$, and τ acts on $\mathcal{W}$ as multiplication by a. By Lemma 4.5(ii), $a = \chi_\ell(\tau)^e$ for some $e \in \{-1, 0, 1\}$. Define the character $\gamma\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathbb{F}_\ell^\times/\{\pm 1\}$ by $\sigma \mapsto \alpha(\sigma)\chi_\ell(\sigma)^{-e}$. We have $\gamma(\tau) = 1$, so $\gamma(\mathcal{I}) = \gamma(\mathcal{I}_t) = 1$. Therefore, γ is unramified at ℓ. The character γ is unramified at the primes $p \nmid 2\ell$ since ρ_ℓ and χ_ℓ are unramified at such primes. □

Lemma 7.3. *For each prime $p \nmid 2\ell$, we have $P_p^{(4)}(\epsilon p^{4e}) \equiv 0 \pmod{\ell}$ for some $\epsilon \in \{\pm 1\}$ and $e \in \{0, 1\}$.*

Proof. Take e and γ as in Lemma 7.2. Since the image of γ lies in an abelian group, we find that $\gamma(\mathcal{I}_2)$ does not depend on the choice of $\mathcal{I}_2$. We claim that $\gamma(\mathcal{I}_2) = \gamma(\mathrm{Gal}_{\mathbb{Q}})$. If $\gamma(\mathcal{I}_2)$ is a proper subgroup of $\gamma(\mathrm{Gal}_{\mathbb{Q}})$, then it gives rise to a non-trivial extension of $\mathbb{Q}$ that is unramified at all primes. The claim follows since $\mathbb{Q}$ has no such extension.

The group $(\mathbb{F}_\ell^\times)^2/\{\pm 1\}$ is cyclic, so $\gamma(\mathrm{Gal}_{\mathbb{Q}}) = \gamma(\mathcal{I}_2)$ is cyclic of some order m. Proposition 6.1 implies that m divides 12. We claim that the cardinality of $\gamma(\mathrm{Gal}_{\mathbb{Q}})$ divides 4. If 3 divides $|\gamma(\mathrm{Gal}_{\mathbb{Q}})|$, then γ gives rise to a cubic abelian extension of $\mathbb{Q}$ that is unramified outside of 2. However, by class field theory no such cubic extensions exist, so the claim follows.

Take any $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. We have $\gamma^4 = 1$, so $\chi_\ell(\sigma)^{4e}$ is a representative of $\alpha(\sigma)^4 = \alpha(\sigma^4)$. By Lemma 7.1, $\epsilon\chi_\ell(\sigma)^{4e}$ is a root of $\det(I - \rho_\ell(\sigma)^4 T)$ for some $\epsilon \in \{\pm 1\}$. Since $\rho_\ell(\sigma) \in \mathrm{SO}(V_\ell)$ by Lemma 2.2, we find that $\chi_\ell(\sigma)^{-4e}$ is also a root of $\det(I - \rho_\ell(\sigma)^4 T)$.

Now take any prime $p \nmid 2\ell$. We have $\chi_\ell(\mathrm{Frob}_p) \equiv p \pmod{\ell}$ and $\det(I - \rho_\ell(\mathrm{Frob}_p)^4 T) \equiv P_p^{(4)}(T) \pmod{\ell}$. Therefore, $P_p^{(4)}(\epsilon p^{4e'}) \equiv 0 \pmod{\ell}$ where $e' = |e|$. □

Using (2.2), we find that $P_3^{(4)}(1) = 2^{12}5^2/3^8$, $P_3^{(4)}(-1) = 2^4/3^8$, $P_3^{(4)}(3^4) = 2^{12}3^25^27^2$, $P_3^{(4)}(-3^4) = 2^41601^2$, $P_5^{(4)}(1) = 2^{14}3^2/5^8$, $P_5^{(4)}(-1) = 2^423^4/5^8$, $P_5^{(4)}(5^4) = 2^{14}3^25^27^229^2$ and $P_5^{(4)}(-5^4) = 2^497^21009^2$. By Lemma 7.3 with $p \in \{3, 5\}$ and our ongoing assumption $\ell \geq 11$, we obtain a contradiction.

Therefore, $\vartheta_\ell(\mathrm{Gal}_{\mathbb{Q}})$ is not contained in a Borel subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$.

7.2. **Cartan case.** We now suppose that $\vartheta_\ell(\mathrm{Gal}_{\mathbb{Q}})$ is contained in the normalizer of a Cartan subgroup C of $\mathrm{PSL}_2(\mathbb{F}_\ell)$.

Lemma 7.4. *We have $\vartheta_\ell(\mathrm{Gal}_{\mathbb{Q}}) \subseteq C$ and the group $\vartheta_\ell(\mathcal{I})$ is either 1 or C.*

Proof. Let N be the normalizer of C in $\mathrm{PSL}_2(\mathbb{F}_\ell)$. By Proposition 4.3(iii), the group $\rho_\ell(\mathcal{I})/\rho_\ell(\mathcal{P})$ is cyclic of order 1, $\ell - 1$ or $\ell + 1$. If $\rho_\ell(\mathcal{I})/\rho_\ell(\mathcal{P}) = 1$, then $\vartheta_\ell(\mathcal{I}) = 1$ since $\ell \nmid |N|$.

Now assume that $\rho_\ell(\mathcal{I})/\rho_\ell(\mathcal{P})$ is cyclic of order $\ell - 1$ or $\ell + 1$. The image of $\rho_\ell(\mathcal{I})$ in $\Omega(V_\ell)/\{\pm I\}$ thus contains a cyclic group of order $(\ell - 1)/2$ or $(\ell + 1)/2$. The group $\vartheta'_\ell(\mathcal{I})$ is of order 1 or ℓ by Lemma 5.4 since $\mathcal{I} \subseteq \mathrm{Gal}_{\mathbb{Q}(i)}$. Since $\ell \nmid |N|$, we deduce that $\vartheta_\ell(\mathcal{I})$ is a cyclic group containing a subgroup of order $(\ell - 1)/2$ or $(\ell + 1)/2$. This implies that $\vartheta_\ell(\mathcal{I})$ is a Cartan subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$. The group N contains a unique Cartan subgroup, so $\vartheta_\ell(\mathcal{I}) = C$.

It remains to show that $\vartheta_\ell(\mathrm{Gal}_{\mathbb{Q}}) \subseteq C$. Let $\varepsilon\colon \mathrm{Gal}_{\mathbb{Q}} \to \{\pm 1\}$ be the character obtained by composing $\vartheta_\ell\colon \mathrm{Gal}_{\mathbb{Q}} \to N$ with the quotient map $N \to N/C \cong \{\pm 1\}$. It thus suffices to show that $\varepsilon = 1$.

Suppose $p \nmid 2\ell$ is a prime that satisfies $\varepsilon(\mathrm{Frob}_p) = -1$ and hence $\vartheta_\ell(\mathrm{Frob}_p) \in N - C$. Recall that every $g \in N - C$ satisfies $\mathrm{tr}(g) = 0$. By Lemmas 5.4 and 5.5, the polynomial $\det(I - \rho_\ell(\mathrm{Frob}_p)T) \equiv P_p(T) \pmod{\ell}$ is either $(1+T^2)^2$ or $1 - 2T^2 + T^4 = (1 - T^2)^2$. Using the values of $P_3(T)$ and $P_5(T)$ from Lemma 2.4, this shows that $\varepsilon(\mathrm{Frob}_3) = 1$ and $\varepsilon(\mathrm{Frob}_5) = 1$.

The character ε is unramified at $p \nmid 2\ell$ since ρ_ℓ is unramified at such primes. The character ε is also unramified at ℓ since $\vartheta_\ell(\mathcal{I}) \subseteq C$. Let K be the fixed field in $\overline{\mathbb{Q}}$ of $\ker(\varepsilon)$. The extension $K/\mathbb{Q}$ is unramified at all odd primes and has degree at most 2, so K is $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. The primes 3 and 5 split in K, which rules out $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. Therefore, $K = \mathbb{Q}$ and hence $\varepsilon = 1$. □

A split Cartan subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ lies in a Borel subgroup. So by the case considered in §7.1 and Lemma 7.4, we deduce that C is non-split.

Lemma 7.5. *The representation ϑ_ℓ is unramified at ℓ.*

Proof. Suppose that ϑ_ℓ is ramified at ℓ. By Lemma 7.4, we have $\vartheta_\ell(\mathrm{Gal}_{\mathbb{Q}}) = \vartheta_\ell(\mathcal{I}) = C$. So ϑ_ℓ gives rise to an abelian extension $K/\mathbb{Q}$ of degree $(\ell + 1)/2$ that is totally ramified at ℓ. There is thus a totally ramified abelian extension $K'/\mathbb{Q}_\ell$ of degree $(\ell+1)/2$. By local class field theory, $\mathrm{Gal}(K'/\mathbb{Q}_\ell)$ must be a quotient of $\mathbb{Z}_\ell^\times \cong \mathbb{F}_\ell^\times \times \mathbb{Z}_\ell$. However, this is impossible since $(\ell + 1)/2 > 1$ is relatively to the integers $(\ell - 1)\ell^e$. □

Lemma 7.6. *For each prime $p \nmid 2\ell$, the polynomial $P_p^{(4)}(T)$ is congruent modulo ℓ to $(1 - T)^4$ or $(1 + T)^4$.*

Proof. Since the image of ϑ_ℓ lies in the cyclic group C, we find that $\vartheta_\ell(\mathcal{I}_2)$ does not depend on the choice of $\mathcal{I}_2$. We claim that $\vartheta_\ell(\mathcal{I}_2) = \vartheta_\ell(\mathrm{Gal}_\mathbb{Q})$. If $\vartheta_\ell(\mathcal{I}_2)$ is a proper subgroup of $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q})$, then it gives rise to a non-trivial extension of $\mathbb{Q}$ that is unramified at all primes (this uses Lemma 7.5). The claim follows since $\mathbb{Q}$ has no such extension.

The group C is cyclic, so $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q}) = \vartheta_\ell(\mathcal{I}_2)$ is cyclic of some order m. Proposition 6.1 implies that m divides 12. We claim that the cardinality of $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q})$ divides 4. If 3 divides $|\vartheta_\ell(\mathrm{Gal}_\mathbb{Q})|$, then ϑ_ℓ gives rise to a cubic abelian extension of $\mathbb{Q}$ that is unramified outside of 2. However, by class field theory no such cubic extension exist, so the claim follows.

Take any $\sigma \in \mathrm{Gal}_\mathbb{Q}$. We have $\vartheta_\ell(\sigma^4) = \vartheta_\ell(\sigma)^4 = I$, so $\det(I - \rho_\ell(\sigma)^4 T)$ is $(1+2T+T^2)^2 = (1+T)^4$ or $(1-2T+T^2)^2 = (1-T)^4$ by Lemma 5.4. The lemma follows since $P_p^{(4)}(T) \equiv \det(I - \rho_\ell(\mathrm{Frob}_p)^4 T) \pmod{\ell}$ for every prime $p \nmid 2\ell$. □

From (2.2), we have $P_3^{(4)}(1) = 2^{12}5^2/3^8$ and $P_3^{(4)}(-1) = 2^4/3^8$. Since $\ell \geq 11$, we have $P_3^{(4)}(1) \not\equiv 0 \pmod{\ell}$ and $P_3^{(4)}(-1) \not\equiv 0 \pmod{\ell}$. However, this contradicts Lemma 7.6 with $p = 3$. Therefore, $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q})$ is not contained in the normalizer of a Cartan subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$.

7.3. **Exceptional case.** Assume that $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q})$ is contained in a subgroup M of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ that is isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$. As observed in [Ser72, §2.6], for every $g \in M$, $u := \mathrm{tr}(g)^2 \in \mathbb{F}_\ell^\times$ is an element of $\{0, 1, 2, 4\}$ or satisfies $u^2 - 3u + 1 = 0$. For each prime $p \nmid 2\ell$, define $u_p := \mathrm{tr}(\vartheta_\ell(\mathrm{Frob}_p))^2 \in \mathbb{F}_\ell$. We thus have $u_p \in \{0, 1, 2, 4\}$ or $u_p^2 - 3u_p + 1 = 0$.

By Lemmas 2.4 and 5.4, we have $u_3 = 16/9$. So $u_3 = 2^4/3^2$, $u_3 - 1 = 7/3^2$, $u_3 - 2 = -2/3^2$, $u_3 - 4 = -2^2 5/3^2$ and $u_3^2 - 3u_3 + 1 = -5 \cdot 19/3^4$. Since $\ell \geq 11$, the prime ℓ must be 19.

By Lemmas 2.4 and 5.5, we have $u_5 = 4/25$. So $u_5 = 2^2/5^2$, $u_5 - 1 = -3 \cdot 7/5^2$, $u_5 - 2 = -2 \cdot 23/5^2$, $u_5 - 4 = -2^5 3/5^2$ and $u_5^2 - 3u_5 + 1 = 11 \cdot 31/5^4$. However, since $\ell = 19$, this contradicts that $u_5 \in \{0, 1, 2, 4\}$ or $u_5^2 - 3u_5 + 1 = 0$.

Therefore, $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q})$ is not contained in a subgroup of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ which is isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$ or $\mathfrak{A}_5$.

7.4. **Proof of Theorem 1.3.** Fix a prime $\ell \geq 11$. Since $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q})$ is a quotient of $\rho_\ell(\mathrm{Gal}_\mathbb{Q})$, it thus suffices to prove that $\vartheta_\ell(\mathrm{Gal}_\mathbb{Q}) = \mathrm{PSL}_2(\mathbb{F}_\ell)$.

Lemma 7.7. *The representation $\vartheta_\ell \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ is surjective.*

Proof. If ϑ_ℓ is not surjective, then its image lies in a maximal subgroup M of $\mathrm{PSL}_2(\mathbb{F}_\ell)$. From §§7.1–7.3, we find that M is not a Borel subgroup, not the normalizer of a Cartan subgroup, and not isomorphic to $\mathfrak{A}_4$, $\mathfrak{S}_4$ and $\mathfrak{A}_5$. This contradicts the classification of maximal subgroups of $\mathrm{PSL}_2(\mathbb{F}_\ell)$ described at the beginning of §7. Therefore, ϑ_ℓ is surjective. □

7.5. **Proof of Theorem 1.1.** The theorem is an immediate consequence of Theorem 1.3 for primes $p \geq 11$. The groups $\mathrm{PSL}_2(\mathbb{F}_5)$ and $\mathrm{PSL}_2(\mathbb{F}_7)$ are both known to occur as the Galois group of an extension of $\mathbb{Q}$; for example, this follows from the results of Shih mentioned in the introduction (or more concretely one can just write down polynomials with these Galois groups).

Remark 7.8. We can actually show that for each prime $\ell \geq 5$, there is a Galois extension $K/\mathbb{Q}$ which is unramified away from 2 and ℓ such that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$. For $\ell \geq 11$, this is clear from Theorem 1.3 since ρ_ℓ is unramified away from 2 and ℓ. One can show that the polynomial $x^5 + 20x - 16$ has discriminant $2^{16}5^6$ and has Galois group isomorphic to $\mathrm{PSL}_2(\mathbb{F}_5)$. One can show that the polynomial $x^7 - 7x^5 - 14x^4 - 7x^3 - 7x + 2$ has discriminant $2^{20}7^8$ and has Galois group isomorphic to $\mathrm{PSL}_2(\mathbb{F}_7)$.

7.6. **Proof of Theorem 1.4.** Theorem 1.4 is an easy consequence of Theorem 1.3 and Lemma 2.6.

8. The image of ρ_ℓ

Let $\mathcal{H}_\ell$ be the subgroup of $\mathrm{SL}_4(\mathbb{F}_\ell)$ consisting of the matrices $\left(\begin{smallmatrix} A & 0 \\ 0 & A \end{smallmatrix}\right)$ with $A \in \mathrm{SL}_2(\mathbb{F}_\ell)$. Let $\mathcal{G}_\ell$ be the subgroup of $\mathrm{SL}_4(\mathbb{F}_\ell)$ generated by $\mathcal{H}_\ell$ and the matrix $\gamma := \left(\begin{smallmatrix} 0 & -I \\ I & 0 \end{smallmatrix}\right)$. We have $\gamma^2 = -I$ and $\mathcal{H}_\ell$ commutes with γ, so $\mathcal{H}_\ell$ is a normal subgroup of $\mathcal{G}_\ell$ with index 2.

The following describes the groups $\rho_\ell(\mathrm{Gal}_\mathbb{Q})$ and $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ up to conjugation in $\mathrm{Aut}_{\mathbb{F}_\ell}(V_\ell)$.

Theorem 8.1. *Take any prime $\ell \geq 11$. There is a representation $\varrho_\ell \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{GL}_4(\mathbb{F}_\ell)$ isomorphic to ρ_ℓ such that $\varrho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathcal{H}_\ell$ and $\varrho_\ell(\mathrm{Gal}_\mathbb{Q}) = \mathcal{G}_\ell$.*

Theorem 8.1 is of course a generalization of Theorem 1.3; note that $\mathcal{G}_\ell/\langle\gamma\rangle \cong \mathrm{PSL}_2(\mathbb{F}_\ell)$.

8.1. **Proof of Theorem 8.1.** Fix a prime $\ell \geq 11$ and define $\mathcal{V}_\ell := \mathbb{F}_\ell^2 \otimes_{\mathbb{F}_\ell} \mathbb{F}_\ell^2$. Let

$$\widetilde{\rho}_\ell \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \mathrm{SL}_2(\mathbb{F}_\ell) \subseteq \mathrm{Aut}_{\mathbb{F}_\ell}(\mathcal{V}_\ell)$$

and $\vartheta_\ell, \vartheta'_\ell \colon \mathrm{Gal}_\mathbb{Q} \to \mathrm{PSL}_2(\mathbb{F}_\ell)$ be the representations of §5.2. We choose ϑ_ℓ and ϑ'_ℓ so that they satisfy the conditions of Lemma 5.4.

Lemma 8.2. *The group $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$, and hence also $\widetilde{\rho}_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$, is isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Proof. Let W be an irreducible $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-submodule of V_ℓ. If W has dimension 1 over $\mathbb{F}_\ell$, then Proposition 3.1(ii) tells us that $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ is a solvable group. This is impossible since the non-abelian simple group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is a quotient of $\rho_\ell(\mathrm{Gal}_\mathbb{Q})$, and hence also of $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$, by Theorem 1.3. By Proposition 3.1, we deduce that W has dimension 2 over $\mathbb{F}_\ell$ and that V_ℓ and $W \oplus W$ are isomorphic $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}(i)}]$-modules. Let $\beta \colon \mathrm{Gal}_{\mathbb{Q}(i)} \to \mathrm{Aut}_{\mathbb{F}_\ell}(W) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ be the representation describing the Galois action on W. It thus suffices to show that $\beta(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathrm{SL}_2(\mathbb{F}_\ell)$ since $\beta_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) \cong \rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ and since ρ_ℓ and $\widetilde{\rho}_\ell$ are isomorphic.

We have $\beta_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$ by Lemma 4.6. The group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is a quotient of $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ and hence is also a quotient of $\beta(\mathrm{Gal}_{\mathbb{Q}(i)})$. So $\beta(\mathrm{Gal}_{\mathbb{Q}(i)})$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell)$ that has a quotient isomorphic $\mathrm{PSL}_2(\mathbb{F}_\ell)$. Since $\mathrm{SL}_2(\mathbb{F}_\ell)$ is perfect (and in particular has no subgroups of index 2), we deduce that $\beta(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathrm{SL}_2(\mathbb{F}_\ell)$. □

Lemma 8.3. *We have $\vartheta'_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) = 1$.*

Proof. By Lemma 5.4 and our choice of ϑ_ℓ, the group $\vartheta'_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ has order 1 or ℓ. Since $\vartheta'_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ is a quotient of the perfect group $\rho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) \cong \mathrm{SL}_2(\mathbb{F}_\ell)$ by Lemma 8.2, we deduce that has $\vartheta'_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) = 1$. □

Lemma 8.3 implies that $\widetilde{\rho}_\ell(\mathrm{Gal}_{\mathbb{Q}(i)})$ is a subgroup of $\mathrm{SL}_2(\mathbb{F}_\ell) \otimes \langle \pm I \rangle = \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \langle I \rangle$. So from Lemma 8.2, we deduce that

$$\widetilde{\rho}_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \langle I \rangle. \tag{8.1}$$

Lemma 8.4. *There is a matrix $B \in \mathrm{SL}_2(\mathbb{F}_\ell)$ such that $B^2 = -I$ and $\vartheta'_\ell(\mathrm{Gal}_\mathbb{Q})$ is generated by the image of B in $\mathrm{PSL}_2(\mathbb{F}_\ell)$.*

Proof. By Lemma 8.3, there is a matrix $B \in \mathrm{SL}_2(\mathbb{F}_\ell)$ such that the image $\overline{B}$ of B in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ generates $\vartheta'_\ell(\mathrm{Gal}_\mathbb{Q})$ and $\overline{B}^2 = -I$. We have $\vartheta'_\ell(\sigma) = \overline{B}$ for all $\sigma \in \mathrm{Gal}_\mathbb{Q} - \mathrm{Gal}_{\mathbb{Q}(i)}$. The proof of Lemma 5.5 shows that the eigenvalues of B are primitive 4-th roots of unity, so $B^2 = -I$. □

By Lemma 8.4, the group $\vartheta'_\ell(\mathrm{Gal}_\mathbb{Q})$ is generated by the image in $\mathrm{PSL}_2(\mathbb{F}_\ell)$ of some matrix $B \in \mathrm{SL}_2(\mathbb{F}_\ell)$ that satisfies $B^2 = -I$. So there is an inclusion $\widetilde{\rho}_\ell(\mathrm{Gal}_\mathbb{Q}) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \langle B \rangle$. This inclusion with (8.1) proves that

$$\widetilde{\rho}_\ell(\mathrm{Gal}_\mathbb{Q}) = \mathrm{SL}_2(\mathbb{F}_\ell) \otimes \langle B \rangle. \tag{8.2}$$

After conjugating $\widetilde{\rho}_\ell$ by an element of $\langle I\rangle \otimes \mathrm{GL}_2(\mathbb{F}_\ell)$, we may assume that $B = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$.

Let e_1 and e_2 be the standard basis of $\mathbb{F}_\ell^2$. Define

$$\varrho_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{F}_\ell)$$

to be the representation obtained from $\widetilde{\rho}_\ell$ by using the basis $\beta := \{e_1 \otimes e_1, e_2 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_2\}$ of $\mathcal{V}_\ell$. Using (8.1), we find that $\varrho_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathcal{H}_\ell$. With respect to the basis β, $I \otimes B$ acts on $\mathcal{V}_\ell$ via the matrix γ. So $\varrho_\ell(\mathrm{Gal}_{\mathbb{Q}})$ is generated by $\mathcal{H}_\ell$ and γ, and hence equals $\mathcal{G}_\ell$.

8.2. **Modularity.** Knowing the image of our representations, we can now show that they also arise from modular forms. Fix a prime $\ell \geq 11$ and take ϱ_ℓ as in Theorem 8.1.

Define the ring $\mathcal{O} := \mathbb{Z}[i]$. We view $\mathbb{F}_\ell^4$ as an $\mathcal{O}$-module by letting i act as γ (note that $\gamma^2 = -I$). This action turns $\mathbb{F}_\ell^4$ into an $\mathcal{O}/\ell\mathcal{O}$-module that is free of rank 2. Let $\{e_1, e_2, e_3, e_4\}$ be the standard basis of $\mathbb{F}_\ell^4$. One can verify that $\beta := \{e_1, e_2\}$ is a basis of $\mathbb{F}_\ell^4$ as an $\mathcal{O}/\ell\mathcal{O}$-module. Using the basis β, we can write ϱ_ℓ as a representation $\varphi_\ell \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O}/\ell\mathcal{O})$. By Theorem 8.1, we find that $\varphi_\ell(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathrm{SL}_2(\mathbb{F}_\ell)$ and that $\varphi_\ell(\mathrm{Gal}_{\mathbb{Q}})$ is generated by $\mathrm{SL}_2(\mathbb{F}_\ell)$ and the scalar matrix $\bar{i}I$ where $\bar{i}$ is the image of i in $\mathcal{O}/\ell\mathcal{O}$.

Let λ be a prime ideal of $\mathcal{O}$ lying over ℓ and set $\mathbb{F}_\lambda = \mathcal{O}/\lambda$. Composing φ_ℓ with the reduction modulo λ map gives a representation $\varphi_\lambda \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda)$. We have $\varphi_\lambda(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathrm{SL}_2(\mathbb{F}_\ell)$ and the group $\varphi_\lambda(\mathrm{Gal}_{\mathbb{Q}})$ is generated by $\mathrm{SL}_2(\mathbb{F}_\ell)$ and the scalar matrix $\bar{i}I$ where $\bar{i}$ is the image of i in $\mathbb{F}_\lambda$. Note that the group $\varphi_\lambda(\mathrm{Gal}_{\mathbb{Q}})/\langle \bar{i}I\rangle$ is isomorphic to $\mathrm{PSL}_2(\mathbb{F}_\ell)$.

The representation φ_λ is absolutely irreducible since $\varphi_\lambda(\mathrm{Gal}_{\mathbb{Q}(i)}) = \mathrm{SL}_2(\mathbb{F}_\ell)$. For all $\sigma \in \mathrm{Gal}_{\mathbb{Q}} - \mathrm{Gal}_{\mathbb{Q}(i)}$, we have $\det(\varphi_\lambda(\sigma)) = \bar{i}^2 = -1$. In particular, $\det(\varphi_\lambda(c)) = -1$ for any $c \in \mathrm{Gal}_{\mathbb{Q}}$ that arises from complex conjugation under some embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$. By Serre's modularity theorem [Ser87], which was proved by Khare and Wintenberger [KW09], we find that the representation φ_λ arises from a cuspidal eigenform f.

We shall not describe f here (it can be chosen to have weight 3 and independent of λ). Motivated by this paper, we will discuss in future work how to obtain $\mathrm{PSL}_2(\mathbb{F}_\ell)$-extensions of $\mathbb{Q}$ using suitable eigenforms. The ideas in this paper have the advantage that they might lead to a construction of a regular extension of the function field $\mathbb{Q}(s)$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ (by considering a *family* of surfaces with a free parameter s). A regular extension of $\mathbb{Q}(s)$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ would then, by Hilbert's irreducibility theorem, show that there are infinitely many extension of $\mathbb{Q}$ with Galois group $\mathrm{PSL}_2(\mathbb{F}_\ell)$.

Appendix A. Proof of Lemmas from §2

Fix an odd prime ℓ. For background on étale cohomology, see [Mil80].

A.1. **Galois representations.** For each positive integer n, let $E[\ell^n]$ be the ℓ^n-torsion subscheme of E; it is a sheaf of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules on U which is free of rank 2. The sheaves $\{E[\ell^n]\}_{n\geq 1}$ with the multiplication by ℓ morphisms $E[\ell^{n+1}] \to E[\ell^n]$ form a sheaf of $\mathbb{Z}_\ell$-modules on U which we denote by $T_\ell(E)$.

Let η be the generic point of U. Set $K = \overline{\mathbb{Q}}(t)$. Fix an algebraic closure $\overline{K}$ of $\mathbb{Q}(t)$ containing K and let $\overline{\eta}$ be the corresponding geometric generic point of U. The sheaf $E[\ell^n]$ on U corresponds to a representation

$$\beta_{\ell^n} : \pi_1(U, \overline{\eta}) \to \mathrm{Aut}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n]_{\overline{\eta}}) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}).$$

Let E_η be fiber of $E \to U$ above η; it is the elliptic curve over $\mathbb{Q}(t)$ defined by (1.1). We can identify the stalk $E[\ell^n]_{\overline{\eta}}$ with the group of ℓ^n-torsion points in $E_\eta(\overline{K})$. The representation $\beta_{\ell^n}|_{\pi_1(U_{\overline{\mathbb{Q}}}, \overline{\eta})}$ extends to a representation $\tilde{\beta}_{\ell^n} \colon \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.

Lemma A.1. *For all $n \geq 1$, we have $\beta_{\ell^n}(\pi_1(U_{\overline{\mathbb{Q}}}, \overline{\eta})) = \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$.*

Proof. It suffices to show that $\tilde{\beta}_{\ell^n}(\mathrm{Gal}(\overline{K}/K)) = \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. This follows from Proposition 2.1 of [CP84] and requires that ℓ is odd; note that the j-invariant of $E_\eta/\mathbb{Q}(t)$ is $256(t^4 - t^2 + 1)^3 t^{-4}(t - 1)^{-2}(t + 1)^{-2}$ and hence the least common multiple of the order of its poles is 4. □

Lemma A.2. *For all $n \geq 1$ and $i \neq 1$, we have $H^i_c(U_{\overline{\mathbb{Q}}}, E[\ell^n]) = 0$.*

Proof. The lemma holds for $i \geq 3$ since U has dimension 1. The lemma holds for $i = 0$ since U is an affine curve. We may now assume that $i = 2$. By Poincaré duality, it suffices to show that $H^0_{\text{ét}}(U_{\overline{\mathbb{Q}}}, E[\ell^n]^\vee(1)) = 0$. The Weil pairing shows that $E[\ell^n]^\vee(1)$ and $E[\ell^n]$ are isomorphic, so we need only show that $H^0_{\text{ét}}(U_{\overline{\mathbb{Q}}}, E[\ell^n]) = 0$. We have $H^0_{\text{ét}}(U_{\overline{\mathbb{Q}}}, E[\ell^n]) = E[\ell^n]_{\overline{\eta}}^{\pi_1(U,\overline{\eta})}$ which is 0 by Lemma A.1. □

Let $j\colon U \hookrightarrow \mathbb{P}^1_{\mathbb{Q}}$ be the inclusion morphism.

Lemma A.3.

(i) For $n \geq 1$, we have $j_!(E[\ell^n]) = j_*(E[\ell^n])$. We have $j_!(T_\ell(E)) = j_*(T_\ell(E))$.
(ii) The $\mathbb{F}_\ell$-vector space V_ℓ has dimension 4.

Proof. Take any closed point x of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ and let I_x be a corresponding inertia subgroup of $\mathrm{Gal}(\overline{K}/K)$. The stalk $j_*(E[\ell^n])_x$ is isomorphic to $E[\ell^n]_{\overline{\eta}}^{I_x}$. If E_η has good, multiplicative or additive reduction at x, then the $\mathbb{Z}/\ell^n\mathbb{Z}$-module $j_*(\mathcal{F})_x$ is free of rank 2, 1 or 0, respectively. The elliptic curve E_η has good reduction at the points of $U_{\overline{\mathbb{Q}}}$ and additive reduction at the closed points of $\mathbb{P}^1_{\overline{\mathbb{Q}}} - U_{\overline{\mathbb{Q}}}$ (moreover, it has reduction of Kodaira type I_2^* or I_4^* at 0, 1, -1 and ∞). So $j_*(E[\ell^n])$ vanishes on $\mathbb{P}^1_{\overline{\mathbb{Q}}} - U_{\overline{\mathbb{Q}}}$ and thus $j_!(E[\ell^n]) = j_*(E[\ell^n])$. This implies that $j_!(T_\ell(E)) = j_*(T_\ell(E))$ which completes the proof of (i).

Now restrict to the case $n = 1$. Define $\chi := \sum_i (-1)^i \dim_{\mathbb{F}_\ell} H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(E[\ell]))$. By [Mil80, V Theorem 2.12], we have

$$\chi = (2 - 2 \cdot 0) \cdot 2 - \sum_x c_x$$

where the sum is over the closed points x of $\mathbb{P}^1_{\overline{\mathbb{Q}}}$ and c_x is the exponent of the conductor of $j_*(E[\ell])$ at x. The integer c_x can be computed using Tate's algorithm [Tat75]. Since our fields have characteristic 0, we have $c_x = 2 - d_x$ where d_x is the dimension over $\mathbb{F}_\ell$ of the stalk of $j_*(E[\ell])$ at x. Therefore, $c_x = 0$ if x belongs to $U_{\overline{\mathbb{Q}}}$ and $c_x = 2$ otherwise. Therefore, $\chi = 4 - 4 \cdot 2 = -4$.

By part (i) and Lemma A.2, we have

$$\chi = \sum_i (-1)^i \dim_{\mathbb{F}_\ell} H^i_c(U_{\overline{\mathbb{Q}}}, E[\ell]) = -\dim_{\mathbb{F}_\ell} H^1_c(U_{\overline{\mathbb{Q}}}, E[\ell]) = -\dim_{\mathbb{F}_\ell} V_\ell.$$

Therefore, $\dim_{\mathbb{F}_\ell} V_\ell = -\chi = 4$, which proves (ii). □

Define the $\mathbb{Z}_\ell$-module $M_\ell := H^1_c(U_{\overline{\mathbb{Q}}}, T_\ell(E))$ and let

$$\rho_{\ell^\infty}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{Aut}_{\mathbb{Z}_\ell}(M_\ell)$$

be the representation describing the natural Galois action on M_ℓ.

Lemma A.4.

(i) The $\mathbb{Z}_\ell$-module M_ℓ is free of rank 4.
(ii) The homomorphism $M_\ell \to V_\ell$ induced by the morphism $T_\ell(E) \to E[\ell]$ gives an isomorphism between $M_\ell/\ell M_\ell$ and V_ℓ that respects the $\mathrm{Gal}_{\mathbb{Q}}$-actions.

Proof. The short exact sequence $0 \to T_\ell(E) \xrightarrow{\times \ell} T_\ell(E) \to E[\ell] \to 0$ of sheaves on U gives rise to an exact sequence

$$H^0_c(U_{\overline{\mathbb{Q}}}, E[\ell]) \to M_\ell \xrightarrow{\times \ell} M_\ell \to V_\ell \to H^2_c(U_{\overline{\mathbb{Q}}}, T_\ell(E)).$$

We have $H^0_c(U_{\overline{\mathbb{Q}}}, E[\ell]) = 0$ and $H^2_c(U_{\overline{\mathbb{Q}}}, T_\ell(E)) = \varprojlim_n H^2_c(U_{\overline{\mathbb{Q}}}, E[\ell^n]) = 0$ by Lemma A.2. The short exact sequence $0 \to M_\ell \xrightarrow{\times \ell} M_\ell \to V_\ell \to 0$ then gives the desired isomorphism of part (ii). Since multiplication by ℓ on M_ℓ is injective, we deduce that the $\mathbb{Z}_\ell$-module M_ℓ is free. The rank of M_ℓ is then equal to the dimension of $M_\ell/\ell M_\ell = V_\ell$, which is 4 by Lemma A.3. □

Define the ring $R = \mathbb{Z}[1/2, 1/\ell]$ and the R-scheme

$$\mathcal{U} := \mathbb{A}^1_R - \{0, 1, -1\} = \operatorname{Spec} R[t, (t(t-1)(t+1))^{-1}].$$

The equation (1.1) defines a relative elliptic curve $\mathcal{E} \to \mathcal{U}$. For each positive integer n, let $\mathcal{E}[\ell^n]$ be the ℓ^n-torsion subscheme of $\mathcal{E}$; it is a sheaf of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules on $\mathcal{U}$ which is free of rank 2. The sheaves $\{\mathcal{E}[\ell^n]\}_{n\geq 1}$ with the multiplication by ℓ morphisms $\mathcal{E}[\ell^{n+1}] \to \mathcal{E}[\ell^n]$ form a sheaf of $\mathbb{Z}_\ell$-modules on $\mathcal{U}$ which we denote by $T_\ell(\mathcal{E})$.

Let $j\colon \mathcal{U} \hookrightarrow \mathbb{P}^1_R$ be the inclusion morphism and let $\pi\colon \mathbb{P}^1_R \to \operatorname{Spec} R$ be the structure map. Define the sheaf $\mathcal{F} := R^1\pi_*(j_*(T_\ell(\mathcal{E})))$ on $\operatorname{Spec} R$ of $\mathbb{Z}_\ell$-modules. Using [73, XVI Corollaire 2.2], we find that the sheaf $\mathcal{F}$ on $\operatorname{Spec} R$ is a lisse sheaf of $\mathbb{Z}_\ell$-modules. The sheaf $\mathcal{F}$ thus corresponds to a representation $\varrho_{\ell^\infty}\colon \pi_1(\operatorname{Spec} R, \bar{\xi}) \to \operatorname{Aut}_{\mathbb{Z}_\ell}(\mathcal{F}_{\bar{\xi}})$ where $\bar{\xi}$ is the geometric point of $\operatorname{Spec} R$ corresponding to a fixed algebraic closure $\overline{\mathbb{Q}}$.

Base extension gives a morphism $\mathcal{E}_{\mathbb{Q}} \to \mathcal{U}_{\mathbb{Q}}$ that agrees with our earlier morphism $f\colon E \to U$. The restriction of $T_\ell(\mathcal{E})$ to $U = \mathcal{U}_{\mathbb{Q}}$ is our sheaf $T_\ell(E)$. Therefore, $\mathcal{F}_{\bar{\xi}} = H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(T_\ell(\mathcal{E}))) = H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(T_\ell(E)))$ which is $H^1_c(U_{\overline{\mathbb{Q}}}, T_\ell(E)) = M_\ell$ by Lemma A.3(i). So we can view ϱ_{ℓ^∞} as a morphism

$$\varrho_{\ell^\infty}\colon \pi_1(\operatorname{Spec} R, \bar{\xi}) \to \operatorname{Aut}_{\mathbb{Z}_\ell}(M_\ell);$$

it gives rise to a representation $\operatorname{Gal}_{\mathbb{Q}} \to \operatorname{Aut}_{\mathbb{Z}_\ell}(M_\ell)$ that agrees with ρ_{ℓ^∞} up to conjugacy. In particular, ρ_{ℓ^∞} is unramified at every prime $p \nmid 2\ell$.

We now fix a prime $p \nmid 2\ell$. Let s be the closed point of $\operatorname{Spec} R$ corresponding to the prime p and let $\bar{s}$ be the geometric point arising from a fixed algebraic closure $\overline{\mathbb{F}}_p$.

Base extending by s, we obtain a relative elliptic curve $\mathcal{E}_{\mathbb{F}_p} \to \mathcal{U}_{\mathbb{F}_p} =: \mathcal{U}_p$. The fiber of $\mathcal{E}_{\mathbb{F}_p} \to \mathcal{U}_p$ over the generic point of $\mathcal{U}_p$ is the elliptic curve $E_p/\mathbb{F}_p(t)$ of §2.3. For each integer $n \geq 1$, let $\mathcal{E}_{\mathbb{F}_p}[\ell^n]$ be the ℓ^n-torsion subscheme of $\mathcal{E}_{\mathbb{F}_p}$; it is a sheaf of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules on $\mathcal{U}_p$ which is free of rank 2. The sheaves $\{\mathcal{E}_{\mathbb{F}_p}[\ell^n]\}_{n\geq 1}$ with the multiplication by ℓ morphisms $\mathcal{E}_{\mathbb{F}_p}[\ell^{n+1}] \to \mathcal{E}_{\mathbb{F}_p}[\ell]$ form a sheaf of $\mathbb{Z}_\ell$-modules on $\mathcal{U}_p$ which we denote by $T_\ell(\mathcal{E}_{\mathbb{F}_p})$. The sheaf $T_\ell(\mathcal{E}_{\mathbb{F}_p})$ is of course the restriction of $T_\ell(\mathcal{E})$ to $\mathcal{U}_p$.

Take any closed point x of $\mathcal{U}_p$ and let $\bar{x}$ be a geometric point extending x. Denote the stalk of $T_\ell(\mathcal{E}_{\mathbb{F}_p})$ at $\bar{x}$ by $T_\ell(\mathcal{E}_{\mathbb{F}_p})_{\bar{x}}$; it is a free $\mathbb{Z}_\ell$-module of rank 2. The *geometric* Frobenius F_x acts $\mathbb{Z}_\ell$-linearly on the fiber $T_\ell(\mathcal{E}_{\mathbb{F}_p})_{\bar{x}}$. Let $\operatorname{Frob}_x := F_x^{-1}$ be the arithmetic Frobenius. One can show that $\det(I - \operatorname{Frob}_x T^{\deg x} | T_\ell(\mathcal{E}_{\mathbb{F}_p})_{\bar{x}})$ equals $L_x(T) := 1 - a_x T^{\deg x} + p^{\deg x} T^{2\deg x}$ with notation as in §2.3. Therefore, $\det(I - F_x T^{\deg x} | T_\ell(\mathcal{E}_{\mathbb{F}_p})_{\bar{x}})$ equals

$$\det(F_x) T^{2\deg x} \det(I - \operatorname{Frob}_x T^{-\deg x} | T_\ell(\mathcal{E}_{\mathbb{F}_p})_{\bar{x}}) = p^{-\deg x} T^{2\deg x} L_x(T^{-1}) = L_x(T/p).$$

Therefore, $L(T/p, E_p) = \prod_x L_x(T/p) = \prod_x \det(I - F_x T^{\deg x} | T_\ell(\mathcal{E}_{\mathbb{F}_p})_{\bar{x}})^{-1}$ where the product is over the closed points of $\mathcal{U}_p$. By the Grothendieck-Lefschetz trace formula, we have

$$L(T/p, E_p) = \prod\nolimits_i \det(I - \operatorname{Frob}_p^{-1} T | H^i_c(\mathcal{U}_{p,\overline{\mathbb{F}}_p}, T_\ell(\mathcal{E}_{\mathbb{F}_p})) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^{(-1)^{i+1}}.$$

The morphism j gives an inclusion morphism $\mathcal{U}_p \hookrightarrow \mathbb{P}^1_{\mathbb{F}_p}$ that we also denote by j. Since $E_p/\mathbb{F}_p(t)$ has additive reduction at 0, 1, -1 and ∞, we have $j_!(T_\ell(\mathcal{E}_{\mathbb{F}_p})) = j_*(T_\ell(\mathcal{E}_{\mathbb{F}_p}))$. Therefore,

$$L(T/p, E_p) = \prod\nolimits_i \det(I - \mathrm{Frob}_p^{-1}\, T |\, H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_p}, j_*(T_\ell(\mathcal{E}_{\mathbb{F}_p}))) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)^{(-1)^{i+1}}.$$

Lemma A.5. *We have* $L(T/p, E_p) = \det(I - \rho_{\ell\infty}(\mathrm{Frob}_p^{-1})T)$.

Proof. Take any integer i and define the sheaf $\mathcal{G} = R^i\pi_*(j_*(T_\ell(\mathcal{E}))$ on $\operatorname{Spec} R$ (we have $\mathcal{F} = \mathcal{G}$ when $i = 1$). Using [73, XVI Corollaire 2.2], we find that the sheaf $\mathcal{G}$ on $\operatorname{Spec} R$ is a lisse sheaf of $\mathbb{Z}_\ell$-modules (and so is constructible and locally constant). The stalk of $\mathcal{G}$ at $\bar{s}$ is $H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_p}, j_*(T_\ell(\mathcal{E})) = H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_p}, j_*(T_\ell(\mathcal{E}_{\mathbb{F}_p}))$. The stalk of $\mathcal{G}$ at $\bar{\xi}$ is $H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(T_\ell(\mathcal{E}))) = H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(T_\ell(E)))$.

If $i \neq 1$, then we have $\mathcal{G}_{\bar{\xi}} = 0$ by Lemma A.2, and hence $H^i_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_p}, j_*(T_\ell(\mathcal{E}_{\mathbb{F}_p})) = 0$ since $\mathcal{G}$ is locally constant. Therefore,

$$L(T/p, E_p) = \det(I - \mathrm{Frob}_p^{-1}\, T |\, H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{F}}_p}, j_*(T_\ell(\mathcal{E}_{\mathbb{F}_p}))) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) = \det(I - \mathrm{Frob}_p^{-1}\, T |\, \mathcal{F}_{\bar{s}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$$

Since $\mathcal{F}$ is locally compatible and constructible, each cospecialization map $\mathcal{F}_{\bar{s}} \to \mathcal{F}_{\bar{\xi}}$ is an isomorphism of $\mathbb{Z}_\ell$-modules. The isomorphism coming from the cospecialization map has a compatible Galois action, i.e., there is a Frobenius automorphism $\mathrm{Frob}_p \in \mathrm{Gal}_{\mathbb{Q}}$ such that the action of Frob_p on $\mathcal{F}_{\bar{\xi}}$ corresponds with the action of $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ on $\mathcal{F}_{\bar{s}}$. In particular, $\det(I - \mathrm{Frob}_p^{-1}\, T | \mathcal{F}_{\bar{\xi}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) = \det(I - \mathrm{Frob}_p^{-1}\, T | \mathcal{F}_{\bar{s}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$. Therefore, $L(T/p)$ agrees with $\det(I - \mathrm{Frob}_p^{-1}\, T | \mathcal{F}_{\bar{\xi}} \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) = \det(I - \rho_{\ell\infty}(\mathrm{Frob}_p^{-1})T)$. □

Since M_ℓ is a free $\mathbb{Z}_\ell$-module of rank 4 by Lemma A.4(i), Lemma A.5 implies that $L(T, E_p)$ is a polynomial of degree 4; that it is has integer coefficients and is independent of ℓ is clear from the series definition of $L(T, E_p)$. Define $P_p(T) := L(T/p, E_p)$.

Lemma A.6. *The series* $P_p(T)$ *is a polynomial of degree* 4 *with coefficients in* $\mathbb{Z}[1/p]$. □

Lemma A.7. *For each prime* $p \nmid 2\ell$*, the representation* ρ_ℓ *is unramified at* p *and satisfies* $\det(I - \rho_\ell(\mathrm{Frob}_p^{-1})T) \equiv P_p(T) \pmod{\ell}$.

Proof. This follows immediately from Lemmas A.5 and A.4. □

A.2. **Proof of Lemma 2.1.** Part (i) is Lemma A.3(ii). We now prove (ii). The Weil pairing gives an alternating non-degenerate pairing $E[\ell] \times E[\ell] \to \mathbb{F}_\ell(1)$ of sheaves on U. It extends to an alternating non-degenerate pairing

$$j_*(E[\ell]) \times j_*(E[\ell]) \to j_*(\mathbb{F}_\ell(1)) \cong \mathbb{F}_\ell(1). \tag{A.1}$$

Composing the cup product

$$H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(E[\ell])) \times H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(E[\ell])) \xrightarrow{\cup} H^2_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(E[\ell]) \otimes j_*(E[\ell]))$$

with the homomorphism $H^2_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(E[\ell]) \otimes j_*(E[\ell])) \to H^2_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1)) \cong \mathbb{F}_\ell$ arising from (A.1), we obtain a pairing

$$\langle\, ,\, \rangle \colon V_\ell \times V_\ell \to \mathbb{F}_\ell;$$

note that $V_\ell = H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, j_*(E[\ell])$ by Lemma A.3. We have $\langle \sigma(v), \sigma(w)\rangle = \sigma(\langle v, w\rangle) = \langle v, w\rangle$ for all $v, w \in V_\ell$ and $\sigma \in \mathrm{Gal}_{\mathbb{Q}}$. The pairing $\langle\, ,\, \rangle$ is symmetric; observe that the cup-product and (A.1) are both alternating. The pairing $\langle\, ,\, \rangle$ is also non-degenerate; this follows from Poincaré duality, cf. [Mil80, V Proposition 2.2(b)].

A.3. **Proof of Lemmas 2.2, 2.3 and 2.4.**

Lemma A.8.

(i) For each odd prime p, we have $T^4 P_p(1/T) = \varepsilon_p \cdot P_p(T)$ for a unique $\varepsilon_p \in \{\pm 1\}$.
(ii) For each odd prime ℓ and prime $p \nmid 2\ell$, we have $\det(\rho_\ell(\mathrm{Frob}_p)) = \varepsilon_p$.

Proof. Recall that $\rho_\ell(\mathrm{Gal}_\mathbb{Q}) \subseteq \mathrm{O}(V_\ell)$ by Lemma 2.1(ii) and $\dim_{\mathbb{F}_\ell} V_\ell = 4$. So for each $A \in \mathrm{O}(V_\ell)$, we have $T^4 \det(I - AT^{-1}) = \det(A) \cdot \det(I - AT)$ where $\det(A) \in \{\pm 1\}$. In particular, for each prime $p \nmid 2\ell$, we have $T^4 \det(I - \rho_\ell(\mathrm{Frob}_p^{-1})T^{-1}) = \det(\rho_\ell(\mathrm{Frob}_p^{-1})) \cdot \det(I - \rho_\ell(\mathrm{Frob}_p^{-1})T)$. By Lemma A.7, we have $T^4 P_p(T^{-1}) \equiv \det(\rho_\ell(\mathrm{Frob}_p)^{-1}) \cdot P_p(T) \pmod{\ell}$.

Since $T^4 P_p(T^{-1})$ is congruent to $P_p(T)$ or $-P_p(T)$ for infinitely many primes ℓ, we have $T^4 P_p(T) = \varepsilon_p P_p(T)$ for a unique $\varepsilon_p \in \{\pm 1\}$. Reducing modulo ℓ, we find that $\det(\rho_\ell(\mathrm{Frob}_p)) = \varepsilon_p^{-1} = \varepsilon_p$. □

For each odd prime ℓ, define the character $\alpha_\ell \colon \mathrm{Gal}_\mathbb{Q} \to \{\pm 1\}$, $\sigma \mapsto \det(\rho_\ell(\sigma^{-1}))$. By Lemma A.8, we have $\alpha_\ell(\mathrm{Frob}_p) = \varepsilon_p$ for all $p \nmid 2\ell$. By the Chebotarev density theorem, we find that α_ℓ is a character $\alpha \colon \mathrm{Gal}_\mathbb{Q} \to \{\pm 1\}$ that does not depend on ℓ. Since $\alpha = \alpha_\ell$ is unramified at $p \nmid 2\ell$ for all odd ℓ, we deduce that α is unramified at all odd p. Let K be the fixed field of $\ker(\alpha)$ in $\overline{\mathbb{Q}}$; it is unramified at odd primes and satisfies $[K : \mathbb{Q}] \leq 2$. So K is $\mathbb{Q}$, $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$.

By Lemma A.6, $P_p(T)$ is a polynomial of degree 4. So to prove Lemma 2.2 and 2.3, it suffices to show that $\alpha = 1$. If $\alpha \neq 1$, then $K \neq \mathbb{Q}$ and hence 3 or 5 is inert in $K \in \{\mathbb{Q}(i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{-2})\}$. So if $\alpha \neq 1$, then $\varepsilon_3 = \alpha(\mathrm{Frob}_3)$ or $\varepsilon_5 = \alpha(\mathrm{Frob}_5)$ is -1. Therefore, Lemmas 2.2 and 2.3 will follow from Lemma 2.4.

We now sketch Lemma 2.4. Computing the product (2.1) with the closed points x with $\deg x \leq 2$, we find that $L(T, E_3) = 1 - 2T^2 + O(T^3)$ and $L(T, E_5) = 1 - 4T + 54T^2 + O(T^3)$. Therefore, $P_3(T) = 1 - 2/9 \cdot T^2 + O(T^3)$ and $P_5(T) = 1 - 4/5 \cdot T + 54/25 \cdot T^2 + O(T^3)$. Since the coefficients of T^2 in $P_3(T)$ and $P_5(T)$ are non-zero, we have $\varepsilon_3 = \varepsilon_5 = 1$ and hence the polynomials $P_3(T)$ and $P_5(T)$ are reciprocal of degree 4. Therefore, $P_3(T) = 1 - 2/9 \cdot T^2 + T^4$ and $P_5(T) = 1 - 4/5 \cdot T + 54/25 \cdot T^2 - 4/5 \cdot T^3 + T^4 = (1 - 2/5 \cdot T + T^2)^2$. We have also verified these examples with `Magma`'s function `LFunction` [BCP97].

A.4. **Proof of Lemma 2.5.** Take any prime $p \nmid 2\ell$. By Lemma A.7, ρ_ℓ is unramified at p and $\det(I - \rho_\ell(\mathrm{Frob}_p^{-1})T) \equiv P_p(T) \pmod{\ell}$. We have $\det(I - A^{-1}T) = \det(I - A)$ for all $A \in \mathrm{SO}(V_\ell)$. So by Lemma 2.2, we have $\det(I - \rho_\ell(\mathrm{Frob}_p)T) \equiv \det(I - \rho_\ell(\mathrm{Frob}_p^{-1})T) \equiv P_p(T) \pmod{\ell}$.

A.5. **Proof of Lemma 2.6.** Let $\mathrm{NS}(X)$ be the Néron-Severi group of $X_{\overline{\mathbb{Q}}}$. Let $\mathcal{T}$ be the subgroup of $\mathrm{NS}(X)$ generated by a section of $\tilde{f}$, a non-singular fiber of $\tilde{f}$ over a rational point of $\mathbb{P}^1_\mathbb{Q}$, and the irreducible components of the singular fibers of $\tilde{f}$. There is a natural $\mathrm{Gal}_\mathbb{Q}$-action on $\mathrm{NS}(X)$ that preserves $\mathcal{T}$.

Lemma A.9.

(i) The group $\mathcal{T}$ is free abelian of rank 30.
(ii) The group $\mathrm{Gal}_\mathbb{Q}$ acts trivially on $\mathcal{T}$.

Proof. The singular fibers of $\tilde{f} \colon X \to \mathbb{P}^1_\mathbb{Q}$ are at 0, 1, -1 and ∞. Fix $s \in \{0, 1, -1, \infty\}$, and let $\mathcal{I}_s$ be the set of irreducible components (defined over $\overline{\mathbb{Q}}$) of the fiber $\tilde{f}^{-1}(s)$ of $\tilde{f}$ over s. There is a natural action of $\mathrm{Gal}_\mathbb{Q}$ on $\mathcal{I}_s$; to prove (ii) it suffices to show that this action is trivial.

By Tate's algorithm, the fiber $\tilde{f}^{-1}(s)$ of $\tilde{f}$ at s is of Kodaira type I_4^* if $s \in \{0, \infty\}$ and of Kodaira type I_2^* if $s \in \{1, -1\}$. The Dykin diagram corresponding to the intersection matrix of $\mathcal{I}_s$ is of type D_6 or D_8. We find that $\mathrm{Gal}_\mathbb{Q}$ acts trivially on $\mathcal{I}_s$ if and only if $\mathrm{Gal}_\mathbb{Q}$ acts trivially on the 4 elements

of $\mathcal{I}_s$ that occur with multiplicity 1 in $\tilde{f}^{-1}(s)$. Using Tate's algorithm, one can show that the four irreducible components of $\tilde{f}^{-1}(s)$ with multiplicity 1 are all defined over $\mathbb{Q}$.

Part (i) follows from equation (1.3) of [Shi92]. □

Let $\gamma\colon \mathrm{NS}(X) \to H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell(1))$ be the cycle map; it is a homomorphism that respects the natural $\mathrm{Gal}_{\mathbb{Q}}$-actions. As explained in §1 of [Shi92], there is a $\mathbb{Q}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-submodule $\mathcal{V}_\ell$ such that

$$H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Q}_\ell(1)) = \mathcal{V}_\ell \oplus (\gamma(\mathcal{T}) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell) \cong \mathcal{V}_\ell \oplus \mathbb{Q}_\ell^{30}; \tag{A.2}$$

the last isomorphism uses Lemma A.9. By Proposition 1 of [Shi92], the vector space $\mathcal{V}_\ell$ has dimension 4 over $\mathbb{Q}_\ell$.

Lemma A.10. *The $\mathbb{Z}_\ell$-module $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}_\ell)$ is free.*

Proof. By choosing an embedding $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and using the comparison isomorphism, we need only show that $H^2(X(\mathbb{C}), \mathbb{Z}_\ell) = H^2(X(\mathbb{C}), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$ is a free $\mathbb{Z}_\ell$-module. By applying Corollary 1.48 of [CZ79] to the elliptic fibration $X(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ arising from $\tilde{f}$, we find that $H^2(X(\mathbb{C}), \mathbb{Z})$ is a free abelian group. □

By Lemma A.10, the $\mathbb{Z}_\ell$-module $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{Z}_\ell(1))$ is free. So from (A.2), we deduce that the semi-simplification of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$ as an $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$ is isomorphic to $\overline{\mathcal{V}}_\ell \oplus \mathbb{F}_\ell^{30}$ where $\overline{\mathcal{V}}_\ell$ has dimension 4 over $\mathbb{F}_\ell$. The lemma is then a consequence of the following.

Lemma A.11. *The $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-modules V_ℓ and $\overline{\mathcal{V}}_\ell$ are isomorphic.*

Proof. Using Lemma 2.4, we have $\det(I - \rho_\ell(\mathrm{Frob}_3)) \equiv 1 - 2/9 \cdot T^2 + T^4 \pmod{\ell}$. The discriminant of $1 - 2/9 \cdot T^2 + T^4$ is $2^{16}5^2/3^8$. Since $\ell \geq 7$, the polynomial $1 - 2/9 \cdot T^2 + T^4 \in \mathbb{F}_\ell[T]$ is separable and 1 is not a root. Therefore, V_ℓ is a semi-simple $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-module and $V_\ell^{\mathrm{Gal}_{\mathbb{Q}}} = 0$. Since also $\dim_{\mathbb{F}_\ell} V_\ell = 4$, to prove the lemma we need only show that V_ℓ is the quotient of some $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-submodule of $H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$.

Consider the Leray spectral sequence with E_2-terms $E_2^{p,q} = H^p_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, R^q\tilde{f}_*\mathbb{F}_\ell(1))$ which converges to $L^n = H^n_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$. Let $E_\infty^{p,q}$ be the limiting value of the $\{E_r^{p,q}\}_r$. There is thus a filtration $0 \subseteq W_1 \subseteq W_2 \subseteq L^2 = H^2_{\text{ét}}(X_{\overline{\mathbb{Q}}}, \mathbb{F}_\ell(1))$ of $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-modules such that W_2/W_1 is isomorphic to $E_\infty^{1,1}$. Using that $E_2^{p,q} = 0$ for $p > 2$, we find that $E_\infty^{1,1}$ equals $E_2^{1,1} = H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, R^1\tilde{f}_*\mathbb{F}_\ell(1))$. So we need only show that the $\mathbb{F}_\ell[\mathrm{Gal}_{\mathbb{Q}}]$-modules V_ℓ and $H^1_{\text{ét}}(\mathbb{P}^1_{\overline{\mathbb{Q}}}, R^1\tilde{f}_*\mathbb{F}_\ell(1))$ are isomorphic. In particular, it suffices to show that the sheaves $j_!(E[\ell])$ and $R^1\tilde{f}_*\mathbb{F}_\ell(1)$ of $\mathbb{F}_\ell$-modules on $\mathbb{P}^1_{\mathbb{Q}}$ are isomorphic.

Take any geometric point s of $\mathbb{P}^1_{\mathbb{Q}} - U$. The stalk of $R^1\tilde{f}_*\mathbb{F}_\ell(1)$ at s is $H^1_{\text{ét}}(X_s, \mathbb{F}_\ell(1))$ where X_s is the fiber of $\tilde{f}$ above s. The fiber X_s is simply connected (it has Kodaira type I_2^* or I_4^*) and hence the stalk of $R^1\tilde{f}_*\mathbb{F}_\ell(1)$ at s vanishes.

It thus suffices to show that $E[\ell]$ and $R^1f_*\mathbb{F}_\ell(1) = R^1\tilde{f}_*\mathbb{F}_\ell(1)|_U$ are isomorphic sheaves of $\mathbb{F}_\ell$-modules on U. Since these sheaves are both locally constant and constructible, it suffices to prove that $E[\ell]_{\bar{\eta}}$ and $(R^1f_*\mathbb{F}_\ell(1))_{\bar{\eta}} = H^1_{\text{ét}}(E_{\bar{\eta}}, \mathbb{F}_\ell(1))$ are isomorphic $\mathbb{F}_\ell[\mathrm{Gal}(\overline{\mathbb{Q}(t)}/\mathbb{Q}(t))]$-modules. Indeed, if $\mathcal{E}$ is an elliptic curve over *any* field k of characteristic 0, then the group of ℓ-torsion points in $\mathcal{E}(\bar{k})$ is isomorphic as an $\mathbb{F}_\ell[\mathrm{Gal}(\bar{k}/k)]$-modules with $H^1_{\text{ét}}(\mathcal{E}_{\bar{k}}, \mathbb{F}_\ell(1))$. □

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). ↑A.3

[Car08] Xavier Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), no. 3, 629–699. ↑4.1

[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. ↑1.2, 5.2

[Cla07] Pete L. Clark, *Galois groups via Atkin-Lehner twists*, Proc. Amer. Math. Soc. **135** (2007), no. 3, 617–624. ↑1.1

[CP84] David A. Cox and Walter R. Parry, *Representations associated with elliptic surfaces*, Pacific J. Math. **114** (1984), no. 2, 309–323. ↑A.1

[CZ79] David A. Cox and Steven Zucker, *Intersection numbers of sections of elliptic surfaces*, Invent. Math. **53** (1979), no. 1, 1–44. ↑A.5

[FF85] W. Feit and P. Fong, *Rational rigidity of $G_2(p)$ for any prime $p > 5$*, Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, N.J., 1983–1984), 1985, pp. 323–326. ↑1.2

[Gal46] Évariste Galois, *Œuvres mathématiques d'Évariste Galois*, Journal des mathématiques pures et appliquées **XI** (1846), 381–444. ↑1.1

[KW09] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. ↑8.2

[Mal93] Gunter Malle, *Polynome mit Galoisgruppen* $\mathrm{PGL}_2(p)$ *und* $\mathrm{PSL}_2(p)$ *über* $\mathbf{Q}(t)$, Comm. Algebra **21** (1993), no. 2, 511–526. ↑1.1

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. ↑A, A.1, A.2

[MM99] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999. ↑1.1

[73] *Théorie des topos et cohomologie étale des schémas. Tome 3*, Lecture Notes in Mathematics, Vol. 305, Springer-Verlag, Berlin, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1963–1964 (SGA 4), Dirigé par M. Artin, A. Grothendieck et J. L. Verdier. Avec la collaboration de P. Deligne et B. Saint-Donat. ↑A.1, A.1

[Och99] Tadashi Ochiai, *l-independence of the trace of monodromy*, Math. Ann. **315** (1999), no. 2, 321–340. ↑6

[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. ↑1.1

[Ser87] ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230. ↑8.2

[Ser72] ———, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. ↑2.5, 4.1, 4.2, 7, 7.3

[Ser73] ———, *A course in arithmetic*, Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7. ↑5.2

[Shi74] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120. ↑1.1

[Shi92] Tetsuji Shioda, *Some remarks on elliptic curves over function fields*, Astérisque **209** (1992), 12, 99–114. Journées Arithmétiques, 1991 (Geneva). ↑A.5, A.5

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. ↑6

[Tat75] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), 1975, pp. 33–52. Lecture Notes in Math., Vol. 476. ↑A.1

[Yun11] Zhiwei Yun, *Motives with exceptional galois groups and the inverse galois problem*, arXiv preprint arXiv:1112.2434 (2011). ↑1.2

[Zas62] Hans Zassenhaus, *On the spinor norm*, Arch. Math. **13** (1962), 434–451. ↑5.1, 5.2

[Zyw13] David Zywina, *The inverse Galois problem for orthogonal groups*, 2013. preprint. ↑1.2

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