TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY, SERIES B
Volume 10, Pages 1173–1211 (August 29, 2023)
https://doi.org/10.1090/btran/124

THE INVERSE GALOIS PROBLEM FOR ORTHOGONAL GROUPS

DAVID ZYWINA

ABSTRACT. We prove many cases of the Inverse Galois Problem for those simple groups arising from orthogonal groups over finite fields. For example, we show that the finite simple groups $\Omega_{2n+1}(p)$ and $\mathrm{P}\Omega^+_{4n}(p)$ both occur as the Galois group of a Galois extension of the rationals for all integers $n \geq 2$ and all primes $p \geq 5$. We obtain our representations by studying families of twists of elliptic curves and using some known cases of the Birch and Swinnerton-Dyer conjecture along with a big monodromy result of Hall.

1. INTRODUCTION

The Inverse Galois Problem asks whether every finite group G is isomorphic to the Galois group of some Galois extension of $\mathbb{Q}$. This problem is extremely difficult, even in the special case of 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. Several 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. Moreover, one can ask whether there is a regular Galois extension $K/\mathbb{Q}(t)$ with Galois group isomorphic to G (by regular, we mean that $\mathbb{Q}$ is algebraically closed in K). If such an extension $K/\mathbb{Q}(t)$ exists, then Hilbert's irreducibility theorem implies that there are infinitely many Galois extensions of $\mathbb{Q}$ with Galois group isomorphic to G, and likewise over every number field.

1.1. **The groups.**

We first introduce the simple groups that we are interested in realizing as Galois groups; further background can be found in [Wil09, §3.7] and [CCN+85, §2.4].

Take any prime $\ell \geq 5$. An orthogonal space over $\mathbb{F}_\ell$ is a finite dimensional $\mathbb{F}_\ell$-vector space V equipped with a non-degenerate and symmetric bilinear pairing $\langle\, ,\, \rangle \colon V \times V \to \mathbb{F}_\ell$. A homomorphism of orthogonal spaces is an $\mathbb{F}_\ell$-linear map which is compatible with the respective pairings. The orthogonal group of V, denoted by $\mathrm{O}(V)$, is the group of automorphisms of V as an orthogonal space. The special orthogonal group $\mathrm{SO}(V)$ is the index 2 subgroup of $\mathrm{O}(V)$ consisting of those elements with determinant 1. For each $v \in V$ with $\langle v, v\rangle \neq 0$, we have a reflection $r_v \in \mathrm{O}(V)$ defined by $x \mapsto x - 2\langle x, v\rangle/\langle v, v\rangle \cdot v$. The spinor norm of V is the homomorphism

$$\mathrm{sp}\colon\ \mathrm{O}(V) \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$$

Received by the editors January 13, 2022, and, in revised form, May 16, 2022.

2020 *Mathematics Subject Classification.* Primary 12F12; Secondary 14J27, 11G05, 11G40.

This material is based upon work supported by the National Science Foundation under agreement No. DMS-1128155.

characterized by the property that it satisfies $\operatorname{sp}(r_v) = \langle v, v\rangle \cdot (\mathbb{F}_\ell^\times)^2$ for every $v \in V$ with $\langle v, v\rangle \neq 0$. The discriminant of V is $\operatorname{disc}(V) := \operatorname{sp}(-I)$; it can also be defined as the coset in $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ represented by $\det(\langle e_i, e_j\rangle)$ where $\{e_1, \ldots, e_n\}$ is any basis of V.

Now fix an integer $n \geq 5$, and take any orthogonal space V over $\mathbb{F}_\ell$ of dimension n. We define $\Omega(V)$ to be the subgroup of $\operatorname{SO}(V)$ consisting of elements with trivial spinor norm. Using that $\mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ has order 2, one can show that $\Omega(V)$ is an index 2 subgroup of $\operatorname{SO}(V)$. The group $\Omega(V)$ is perfect and its center is either $\{I\}$ or $\{\pm I\}$. Denote by $\mathrm{P}\Omega(V)$ the quotient of $\Omega(V)$ by its center.

Suppose that n is odd. The group $\Omega(V)$ has trivial center and is simple. The isomorphism class of $\mathrm{O}(V)$, and hence also $\Omega(V)$, depends only on n and ℓ. Denote by $\Omega_n(\ell)$ an abstract group isomorphic to $\Omega(V)$ (other common notation for this group is $O_n(\ell)$ and $B_{(n-1)/2}(\ell)$).

Suppose that n is even. Up to isomorphism, there are two orthogonal spaces of dimension n over $\mathbb{F}_\ell$ and they are distinguishable by their discriminants. We say that V is split if $\operatorname{disc}(V) = (-1)^{n/2}(\mathbb{F}_\ell^\times)^2$ and non-split otherwise (note that V is split if and only if it is an orthogonal sum of hyperbolic planes). Denote by $\mathrm{P}\Omega_n^+(\ell)$ and $\mathrm{P}\Omega_n^-(\ell)$ an abstract group isomorphic to $\mathrm{P}\Omega(V)$ when V is split or non-split, respectively. The groups $\mathrm{P}\Omega_n^+(\ell)$ and $\mathrm{P}\Omega_n^-(\ell)$ are both simple. (Other common notation for $\mathrm{P}\Omega_n^+(\ell)$ is $O_n^+(\ell)$ and $D_{n/2}(\ell)$. Other common notation for $\mathrm{P}\Omega_n^-(\ell)$ is $O_n^-(\ell)$ and ${}^2D_{n/2}(\ell^2)$.)

1.2. **Main results.**

Theorem 1.1. *Take any integer $n \geq 5$ and prime $\ell \geq 5$.*

- (i) *If n is odd, then the simple group $\Omega_n(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.*
- (ii) *If n is even, and $n \equiv 0 \pmod 4$ or $\ell \equiv 1 \pmod 4$, then the simple group $\mathrm{P}\Omega_n^+(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.*
- (iii) *If $n \equiv 2 \pmod 4$ and $\ell \equiv 3 \pmod 4$, then the simple group $\mathrm{P}\Omega_n^-(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.*
- (iv) *If n is even and 2, 3, 5 or 7 is not a square modulo ℓ, then the groups $\mathrm{P}\Omega_n^+(\ell)$ and $\mathrm{P}\Omega_n^-(\ell)$ both occur as the Galois group of a regular extension of $\mathbb{Q}(t)$.*

The following is a restatement of Theorem 1.1(ii) and (iii).

Corollary 1.2. *Take any even integer $n \geq 6$ and prime $\ell \geq 5$. If V is an orthogonal space of dimension n over $\mathbb{F}_\ell$ with $\operatorname{disc}(V) = (\mathbb{F}_\ell^\times)^2$, then the simple group $\mathrm{P}\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.*

The following is a consequence of Theorem 1.1 and the exceptional isomorphisms $\Omega_5(\ell) \cong \mathrm{PSp}_4(\mathbb{F}_\ell)$, $\mathrm{P}\Omega_6^+(\ell) \cong \mathrm{PSL}_4(\mathbb{F}_\ell)$ and $\mathrm{P}\Omega_6^-(\ell) \cong \mathrm{PSU}_4(\mathbb{F}_\ell)$.

Corollary 1.3. *Take any prime $\ell \geq 5$.*

- (i) *The simple group $\mathrm{PSp}_4(\mathbb{F}_\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.*
- (ii) *If ℓ is not congruent to 311, 479, 551, 671, 719 and 839 modulo 840, then the simple group $\mathrm{PSL}_4(\mathbb{F}_\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.*

(iii) *If ℓ is not congruent to* 1, 121, 169, 289, 361 *and* 529 *modulo* 840, *then the simple group* $\mathrm{PSU}_4(\mathbb{F}_\ell)$ *occurs as the Galois group of a regular extension of* $\mathbb{Q}(t)$.

1.3. **Some previous work and related cases.** Reiter [Rei99] proved Theorem 1.1(i) in the special case where 2 or 3 is not a square modulo ℓ; in particular, it covers the case $\ell = 3$ which we excluded. Additional special cases of Theorem 1.1(i) for $n = 5$ and 7 were proved by Häfner [Häf92]. Theorem 1.1(iv) covers the various cases of the regular inverse Galois problem for $\mathrm{P}\Omega_n^+(\ell)$ and $\mathrm{P}\Omega_n^-(\ell)$ with $\ell \geq 5$ that are due to Reiter [Rei99] and Malle-Matzat [MM99, §10.2]. The cases of the regular inverse Galois problem in Theorem 1.1(ii) and (iii) appear to be new.

We now briefly discuss the excluded cases $n = 3$ and 4; we do not obtain nonabelian simple groups when $n \leq 2$. These cases are especially interesting because of the exceptional isomorphisms

$$\Omega_3(\ell) \cong \mathrm{PSL}_2(\mathbb{F}_\ell), \quad \mathrm{P}\Omega_4^+(\ell) \cong \mathrm{PSL}_2(\mathbb{F}_\ell)\times\mathrm{PSL}_2(\mathbb{F}_\ell) \quad \text{and} \quad \mathrm{P}\Omega_4^-(\ell) \cong \mathrm{PSL}_2(\mathbb{F}_{\ell^2}).$$

The simple group $\mathrm{PSL}_2(\mathbb{F}_\ell)$ is known to occur as the Galois group of a regular extension of $\mathbb{Q}(t)$ if 2, 3, 5 or 7 is not a square modulo ℓ; the cases 2, 3 and 7 are due to Shih [Shi74] and 5 is then due to Malle [Mal93]. The conclusion of Theorem 1.1(i) and Theorem 1.1(ii) with $n = 3$ and $n = 4$, respectively, remains open.

In [Zyw15], the author showed that $\mathrm{PSL}_2(\mathbb{F}_\ell)$ occurs as a Galois group of an extension of $\mathbb{Q}$ for all primes ℓ. The construction of such extensions in [Zyw15] is similar to those of this paper; however, regular extensions of $\mathbb{Q}(t)$ are not obtained.

The group $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ is already known to occur as the Galois group of a regular extension of $\mathbb{Q}(t)$ if 2, 3, 5 or 7 is not a square modulo ℓ; see [Shi04] and [Shi03] for 2 and 3, [Mes88] for 5, and [DW06] for 7. For many other ℓ, the group $\mathrm{PSL}_2(\mathbb{F}_{\ell^2})$ is known to occur as the Galois group of an extension of $\mathbb{Q}$; for examples, see [Rib75, §7], [RV95] and [DV00].

The simple group $G_2(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$ for all primes $\ell \geq 5$ (cf. [FF85] for $\ell > 5$ and [Tho85] for $\ell = 5$). The simple group $E_8(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$ for all primes $\ell \geq 7$, cf. [GM14]; this was first shown to be true by Yun for all ℓ sufficiently large [Yun14]. Theorem 1.1(i) and Theorem 1.1(ii) with $n \equiv 0 \pmod 4$ are the first cases where one has analogous results for finite simple groups of a fixed *classical* Lie type.

1.4. **A special case.** We now give an overview of the ideas behind the proof of Theorem 1.1 in the special case $n = 5$. In particular, for a fixed $\ell \geq 5$, we will describe a regular extension of $\mathbb{Q}(t)$ with Galois group isomorphic to $\Omega_5(\ell)$. This section can be safely skipped and will not be referred to later on.

Define $S := \{2, 3, \ell\}$ and the ring $R := \mathbb{Z}[S^{-1}]$. Define the R-scheme

$$M = \operatorname{Spec} R[u, u^{-1}, (u-1)^{-1}, (u+1)^{-1}];$$

it is an open subscheme of $\mathbb{A}^1_R = \operatorname{Spec} R[u]$.

Let k be any finite field that is an R-algebra, i.e., a finite field whose characteristic is not 2, 3 or ℓ. Denote the cardinality of k by q. Take any $m \in M(k)$, i.e., any $m \in k - \{0, 1, -1\}$. Let E_m be the elliptic curve over the function field $k(t)$ defined by the Weierstrass equation

$$(t-m)\cdot \mathsf{y}^2 = \mathsf{x}^3 + 3(t^2-1)^3\mathsf{x} - 2(t^2-1)^5.$$

Denote by $L(T, E_m)$ the L-function of the elliptic curve $E_m/k(t)$, see §2.3 for details. One can show that $L(T, E_m)$ is a polynomial in $\mathbb{Z}[T]$ of degree 5. For example, with $k = \mathbb{F}_5$ and $m = 1$, one can compute that $L(T, E_m) = 1 - 2T + T^2 - 5T^3 + 2 \cdot 5^3T^4 - 5^5T^5$.

Using the cohomological description of L-functions, we will construct an orthogonal space V_ℓ over $\mathbb{F}_\ell$ of dimension 5 and a continuous representation

$$\theta_\ell\colon \pi_1(M) \to \mathrm{O}(V_\ell)$$

such that for any k and $m \in M(k)$ as above, we have

$$\det(I - \theta_\ell(\mathrm{Frob}_m)T) \equiv L(T/q, E_m) \pmod{\ell}. \tag{1.1}$$

Here $\pi_1(M)$ is the étale fundamental group of M (with suppressed base point) and Frob_m is the geometric Frobenius conjugacy class of m in $\pi_1(M)$.

The representation θ_ℓ has big monodromy, i.e., $\theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}})) \supseteq \Omega(V_\ell)$. This will be shown following the approach of Hall in [Hal08] (we will directly use Hall's results for the cases with $n > 5$). The key step is to show that the group $\mathcal{R}$ generated by the reflections in $\theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}}))$ acts irreducibly on V_ℓ. The classification of finite irreducible linear groups generated by reflections then gives a finite number of small possibilities for $\mathcal{R}$ that need to be ruled out to ensure that $\mathcal{R} \supseteq \Omega(V_\ell)$.

The image of θ_ℓ can sometimes be the full orthogonal group $\mathrm{O}(V_\ell)$ (in fact, this happens if $\ell \equiv \pm 3 \pmod 8$).

Let W be the open subscheme $\operatorname{Spec} R[u, u^{-1}, (u^2-3)^{-1}, (u^2+3)^{-1}]$ of $\mathbb{A}^1_R$. The morphism $h\colon W \to M$ given by $w \mapsto (-w^2+3)/(w^2+3)$ is étale of degree 2, so we have a representation

$$\vartheta_\ell\colon \pi_1(W) \xrightarrow{h_*} \pi_1(M) \xrightarrow{\theta_\ell} \mathrm{O}(V_\ell).$$

We claim that there are inclusions

$$\Omega(V_\ell) \subseteq \vartheta_\ell(\pi_1(W_{\overline{\mathbb{Q}}})) \subseteq \vartheta_\ell(\pi_1(W)) \subseteq \pm\Omega(V_\ell), \tag{1.2}$$

where $\pm\Omega(V_\ell)$ is the group generated by $\Omega(V_\ell)$ and $-I$. The natural map $\Omega(V_\ell) \to (\pm\Omega(V_\ell))/\{\pm I\}$ is an isomorphism, so the claimed inclusions give a surjective homomorphism

$$\beta\colon \pi_1(W) \xrightarrow{\vartheta_\ell} \pm\Omega(V_\ell) \to (\pm\Omega(V_\ell))/\{\pm I\} \cong \Omega(V_\ell)$$

that satisfies $\beta(\pi_1(W_{\overline{\mathbb{Q}}})) = \Omega(V_\ell)$. Therefore, β gives rise to a regular extension of $\mathbb{Q}(u)$, i.e., the function field of W, that is Galois with Galois group isomorphic to $\Omega(V_\ell) \cong \Omega_5(\ell)$; this gives the desired extension for the $n = 5$ case of Theorem 1.1(i). We now explain why the inclusions of (1.2) hold.

We have the inclusion $\vartheta_\ell(\pi_1(W_{\overline{\mathbb{Q}}})) \supseteq \Omega(V_\ell)$ of (1.2) since the simple non-abelian group $\Omega(V_\ell)$ is a normal subgroup of $\theta_\ell(M_{\overline{\mathbb{Q}}})$ and the cover h is abelian.

Now let κ be any coset of $\Omega(V_\ell)$ in $\theta_\ell(\pi_1(M))$ with $\det(\kappa) = \{-1\}$. Since $\det(\kappa) = \{-1\}$, one can show that there is an element $A \in \kappa$ such that $\det(I - A) \neq 0$. From a formula of Zassenhaus, cf. Lemma 2.13, we find that $\mathrm{sp}(-A) = 2\det(I - A) \cdot (\mathbb{F}_\ell^\times)^2$. Using equidistribution, there is a prime $p \nmid 6\ell$ and an $m \in M(\mathbb{F}_p)$ such that A is conjugate to $\theta_\ell(\mathrm{Frob}_m)$ in $\mathrm{O}(V_\ell)$. We have $L(T/p, E_m) \equiv \det(I - AT) \pmod{\ell}$ and hence $L(1/p, E_m) \equiv \det(I - A) \pmod{\ell}$. Therefore,

$$\mathrm{sp}(-A) = 2 \cdot L(1/p, E_m) \cdot (\mathbb{F}_\ell^\times)^2.$$

The special value $L(1/p, E_m)$ is linked to the arithmetic of the curve $E_m/\mathbb{F}_p(t)$. We have $L(1/p, E_m) \neq 0$ (since it is non-zero modulo ℓ), so the Birch and Swinnerton-Dyer (BSD) conjecture predicts that the Mordell-Weil group $E_m(\mathbb{F}_p(t))$ is finite. For background on the Birch and Swinnerton-Dyer conjecture and related results, see §2.4. In fact, BSD is known unconditionally for E_m by work of Artin and Tate. Moreover, from Artin, Tate and Milne, the following refined version of BSD is known to hold: we have

$$L(1/p, E_m) = \frac{|\text{Ш}_{E_m}| \cdot c_{E_m}}{|E_m(\mathbb{F}_p(t))|^2 \cdot p^{-1+\chi_{E_m}}},$$

where c_{E_m} is the product of Tamagawa numbers of E_m over the places of $\mathbb{F}_p(t)$, $12\chi_{E_m}$ is the degree of the minimal discriminant of E_m, and Ш_{E_m} is the (finite!) Tate-Shafarevich group of E_m. Since Ш_{E_m} is finite, a pairing of Cassels on Ш_{E_m} shows that $|\text{Ш}_{E_m}|$ is a square. An application of Tate's algorithm shows that $\chi_{E_m} = 3$ and that c_{E_m} is a power of 2. So $2L(1/p, E_m) \in 2c_{E_m}(\mathbb{Q}^\times)^2$ and $\operatorname{sp}(-A) = 2c_{E_m} \cdot (\mathbb{F}_\ell^\times)^2$. Using Tate's algorithm, one can show that $2c_{E_m} \in \{16, 64\}$ if $-3(m^2-1) \in \mathbb{F}_p$ is a square and $2c_{E_m} = 32$ otherwise. Therefore,

$$\operatorname{sp}(-A) = \begin{cases} (\mathbb{F}_\ell^\times)^2 & \text{if } -3(m^2-1) \in \mathbb{F}_p \text{ is a square,} \\ 2(\mathbb{F}_\ell^\times)^2 & \text{if } -3(m^2-1) \in \mathbb{F}_p \text{ is not a square.} \end{cases}$$

Now suppose that κ is actually a coset of $\Omega(V_\ell)$ in $\vartheta_\ell(\pi_1(W))$. Then $m = h(w)$ for some $w \in W(\mathbb{F}_p)$. We have $-3(m^2-1) = 6^2w^2/(w^2+3)^2$ which is clearly a square (our degree 2 cover $h\colon W \to M$ was chosen to ensure this held), so $\operatorname{sp}(-A) = (\mathbb{F}_\ell^\times)^2$. We have $-A \in \Omega(V_\ell)$ since $\operatorname{sp}(-A) = (\mathbb{F}_\ell^\times)^2$ and $\det(-A) = (-1)^5\det(A) = 1$. Therefore, $\kappa = A\Omega(V_\ell) = -\Omega(V_\ell)$.

We now know that $\vartheta_\ell(\pi_1(W))$ contains $\Omega(V_\ell)$ and the only possible $\Omega(V_\ell)$-coset with determinant -1 is $-\Omega(V_\ell)$. Therefore, $\vartheta_\ell(\pi_1(W))$ is either $\pm\Omega(V_\ell)$ or is a subgroup of $\mathrm{SO}(V_\ell)$. So to explain the last inclusion of (1.2), we need only show that $\vartheta_\ell(\pi_1(W))$ contains an element with determinant -1.

For any $p \notin S$ and $m \in M(\mathbb{F}_p)$, there is a functional equation

$$T^5 L(T^{-1}/p, E_m) = \varepsilon_{E_m} L(T/p, E_m),$$

where $\varepsilon_{E_m} \in \{\pm 1\}$ is the *root number* of E_m, cf. §2.3. Since $A := \theta_\ell(\mathrm{Frob}_m)$ belongs to $\mathrm{O}(V_\ell)$, we have $T^5\det(I - T^{-1}A) \equiv \det(-A)\det(I - TA)$. From (1.1), we deduce that $\det(-A) = \varepsilon_{E_m}$ and hence $\det(\theta_\ell(\mathrm{Frob}_m)) = -\varepsilon_{E_m}$. One can express ε_{E_m} as a product of local root numbers and a computation shows that $-\varepsilon_{E_m}$ is 1 if $-3m \in \mathbb{F}_p$ is a square and -1 otherwise.

So if $\vartheta_\ell(\pi_1(W))$ is a subgroup of $\mathrm{SO}(V_\ell)$, then $-3h(w) = -3(-w^2+3)/(w^2+3)$ is a square in $\mathbb{F}_p$ for all primes $p \notin S$ and $w \in W(\mathbb{F}_p)$. This is easily seen to be false, so we deduce that $\vartheta_\ell(\pi_1(W))$ is not a subgroup of $\mathrm{SO}(V_\ell)$.

1.5. **Overview.** In §2, we give background on elliptic curves defined over global function fields. We will mainly be interested in non-isotrivial elliptic curves E defined over a function field $k(t)$, where k is a finite field of order q with $(q, 6) = 1$. We will recall the definition of the *L-function* $L(T, E)$ of E; it is a polynomial with integer coefficients. For almost all primes ℓ, we will construct an orthogonal space $V_{E,\ell}$ over $\mathbb{F}_\ell$ and a representation

$$\theta_{E,\ell}\colon \operatorname{Gal}(\bar{k}/k) \to \mathrm{O}(V_{E,\ell})$$

such that $\det(I-\theta_{E,\ell}(\mathrm{Frob}_q)T) \equiv L(T/q, E) \pmod{\ell}$, where Frob_q is the geometric Frobenius (i.e., the inverse of $x \mapsto x^q$). The determinant of $\theta_{E,\ell}(\mathrm{Frob}_q)$ is related to the *root number* of E. In many case, we can compute the spinor norm of $\theta_{E,\ell}(\mathrm{Frob}_q)$ by using the special value of $L(T, E)$ arising in the *Birch and Swinnerton-Dyer conjecture*. We will discuss the Birch and Swinnerton-Dyer conjecture in §2.4. We shall use known cases to give a simple description of the square class $L(1/q, E) \cdot (\mathbb{Q}^\times)^2$ when $L(1/q, E)$ is non-zero.

In §3, we follow Hall and consider families of quadratic twists. We shall construct a representation that encodes the representations $\theta_{E,\ell}$ as E varies in our family. In §3.3, we state an explicit version of a *big monodromy* result of Hall.

In §4, we state a criterion to ensure that the representation of §3 will produce a group $\Omega(V)$ as the Galois group of a regular extension of $\mathbb{Q}(t)$. For any given example, the conditions are straightforward to verify using some basic algebra and Tate's algorithm.

In §§5, 6 and 7, we give many examples and use our criterion to prove Theorem 1.1 for all $n > 5$. We shall not explain how the equations in these sections were found; they were discovered through many numerical experiments (though the paper [Her91] served as a useful starting point since it gives many elliptic surfaces with only four singular fibers).

Finally, in §8 we complete the proof of Theorem 1.1 for $n = 5$. The big monodromy criterion of Hall does not apply for our example, so we need to prove it directly.

Notation. Throughout the paper, we will freely use Tate's algorithm, see [Sil94, IV §9] or [Tat75]. All fundamental groups, cohomology and sheaves in the paper are with respect to the étale topology. We will often suppress base points for our fundamental groups, so many groups and representations will only be determined up to conjugacy. We will indicate base change of schemes by subscripts, for example given a scheme X over $\mathbb{Q}$, we denote by $X_{\overline{\mathbb{Q}}}$ the corresponding scheme base changed to $\overline{\mathbb{Q}}$.

2. L-functions of elliptic curves over global function fields

In this section, we give some background on the arithmetic of elliptic curves defined over global function fields. For a gentle introduction to elliptic curve over global function fields and the Birch and Swinnerton–Dyer conjecture, see [Ulm11] and [Gro11].

Fix a finite field k whose cardinality q is relatively prime to 2 and 3. Let C be a smooth, proper and geometrically irreducible curve of genus g over k and denote its function field by K. Let $|C|$ be the set of closed points of C. For each $x \in |C|$, let $\mathbb{F}_x$ be the residue field at x and let $\deg x$ be the degree of $\mathbb{F}_x$ over k. Each closed point $x \in |C|$ gives a discrete valuation $v_x\colon K \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$ and we denote by K_x the corresponding local field.

Fix an elliptic curve E defined over K whose j-invariant j_E is non-constant (i.e., $j_E \in K - k$). Let $\pi\colon \mathcal{E} \to C$ be the Néron model of E/K, cf. [BLR90, §1.4]. Let $U \subseteq C$ be the dense open subset complementary to the finite number of points of bad reduction for E. By abuse of notation, we let $E \to U$ be the (relative) elliptic curve $\pi^{-1}(U) \xrightarrow{\pi} U$; the fiber over the generic point of U is E/K.

2.1. **Kodaira symbols.** For each closed point x of C, we can assign a Kodaira symbol to the elliptic curve E after base extending by the local field K_x; it can be quickly computed using Tate's algorithm, cf. [Sil94, IV §9] or [Tat75]. The possible Kodaira symbols are the following: I_n $(n \geq 0)$, I_n^* $(n \geq 0)$, II, III, IV, IV*, III*, II*.

Let $\operatorname{Kod}(E)$ be the multiset consisting of the Kodaira symbols of E at the points $x \in C$ for which E has bad reduction; we count a Kodaira symbol at x with multiplicity $\deg x$. Note that the multiset $\operatorname{Kod}(E)$ does not change if we replace E by its base extension to the function field of $C_{k'}$ for any finite extension k'/k.

2.2. **Some invariants.** We now define some numerical invariants of the curve E. For each $x \in |C|$, we define integers $f_x(E)$, $e_x(E)$, $\gamma_x(E)$, $\lambda_x(E)$, $r_x(E)$ and $b_x(E)$ as in the following table:

Kodaira	I_0	I_0^*	I_n	II	III	IV	I_n^*	IV*	III*	II*
symbol at x			$(n \geq 1)$				$(n \geq 1)$			
f_x	0	2	1	2	2	2	2	2	2	2
e_x	0	6	n	2	3	4	$6+n$	8	9	10
γ_x	1	1	$\frac{n}{\gcd(2,n)}$	1	1	3	$\frac{2}{\gcd(2,n)}$	3	1	1
λ_x	1	1	n	1	1	1	n	1	1	1
r_x	1	1	1	1	2	3	1	3	2	1
b_x	0	0	0	1	1	1	1	1	1	1

Define

$$N_E = -4 + 4g + \sum_{x \in |C|} f_x(E) \deg(x), \quad \chi_E = \frac{1}{12} \sum_{x \in |C|} e_x(E) \deg x,$$

$$\text{and } \gamma_E = \prod_{x \in |C|} \gamma_x(E)^{\deg x}.$$

Define $\mathcal{L}_E$ to be the product of the primes $\ell \geq 5$ that divide $\lambda_x(E)$ for some $x \in |C|$; it is also the product of primes $\ell \geq 5$ that divide $\max\{1, -v_x(j_E)\}$ for some $x \in |C|$.

Remark 2.1.

(i) The integers N_E, χ_E, γ_E and $\mathcal{L}_E$ can all be determined directly from the multiset $\operatorname{Kod}(E)$.

(ii) One way to prove that χ_E is an integer is to show that it agrees with the Euler characteristic of the sheaf $\mathcal{O}_X$, where $X \to C$ is a relatively minimal elliptic surface that extends $E \to U$ with X smooth and projective.

Let $\mathcal{E}_x/\mathbb{F}_x$ be the fiber of the Néron model $\mathcal{E} \to C$ of E/K at x. We define $c_x(E)$ to be the order of the group $\mathcal{E}_x(\mathbb{F}_x)/\mathcal{E}_x^\circ(\mathbb{F}_x)$, where $\mathcal{E}_x^\circ$ is the identity component of the group scheme $\mathcal{E}_x$. Define the integer

$$c_E = \prod_{x \in |C|} c_x(E);$$

it is well-defined since $c_x(E) = 1$ whenever E has good reduction at x. The integer c_E serves as a "fudge factor" in the Birch and Swinnerton-Dyer conjecture, cf. §2.4, and can be quickly computed using Tate's algorithm.

Let A_E be the set of closed points x of C for which E has bad reduction of additive type. For each $x \in A_E$, let $\chi_x \colon \mathbb{F}_x^\times \to \{\pm 1\}$ be the non-trivial quadratic character (recall that q is odd). Let m_+ be the number of closed points x of C for which E has split multiplicative reduction. Define

$$\varepsilon_E := (-1)^{m_+} \prod\nolimits_{x \in A_E} \chi_x(-r_x(E)) \in \{\pm 1\};$$

it is the root number of E, cf. Theorem 2.2.

2.3. **L-functions.** Take any closed point x of C. If E has good reduction at x, define the polynomial $L_x(T) := 1 - a_x(E) T^{\deg x} + q^{\deg x} T^{2 \deg x}$, where $E_x/\mathbb{F}_x$ is the fiber of E over x and $a_x(E) := q^{\deg x} + 1 - |E_x(\mathbb{F}_x)|$. If E has bad reduction at x, define $a_x(E)$ to be 1, -1 or 0 when E has split multiplicative, non-split multiplicative or additive reduction, respectively, at x; define the polynomial $L_x(T) = 1 - a_x(E) T^{\deg x}$.

The L-function of E is the formal power series

$$L(T, E) := \prod\nolimits_{x \in |C|} L_x(T)^{-1} \in \mathbb{Z}[\![T]\!].$$

The following gives some fundamental properties of $L(T,E)$; we will give a sketch in §2.7.

Theorem 2.2. *The L-function $L(T,E)$ is a polynomial of degree N_E with integer coefficients and satisfies the functional equation*

$$T^{N_E} L(T^{-1}/q, E) = \varepsilon_E \cdot L(T/q, E).$$

If q is a power of 2 or 3, then Theorem 2.2 will hold except the numerical recipes for N_E and ε_E need to be refined. One can also consider the case where E has constant j-invariant; $L(T,E)$ is still a rational function but is no longer a polynomial.

Another important property of $L(T,E)$, which we will not require, is that all its complex roots have absolute value q^{-1}. This will follow from the cohomological interpretation and the work of Deligne.

2.4. **The Birch and Swinnerton-Dyer conjecture.** The Mordell-Weil theorem for E says that the abelian group $E(K)$ is finitely generated. It is straightforward to compute the torsion subgroup of $E(K)$ but computing its rank is more difficult. Before stating the conjecture, we mention several invariants of E:

- Let $Ш_E$ be the Tate-Shafarevich group of E/K.
- Let $\mathcal{D}_E$ be the minimal discriminant of E/K; we may view it as a divisor of C. Using Tate's algorithm (and our ongoing assumption that q is not a power of 2 or 3), we find that the degree of $\mathcal{D}_E$ is $12\chi_E$.
- The integer c_E from §2.2.
- Let $E(K)_{\text{tors}}$ be the torsion subgroup of $E(K)$.
- The regulator of E is the real number $R_E := \det(\langle P_i, P_j \rangle)$, where $\langle\, ,\, \rangle \colon E(K) \times E(K) \to \mathbb{R}$ is the canonical height pairing and $P_1, \ldots, P_r \in E(K)$ are points that give a basis for the free abelian group $E(K)/E(K)_{\text{tors}}$.

The following is a conjectural relation between the rank of the Mordell-Weil group $E(K)$ and its L-function.

Conjecture 2.3 (Birch and Swinnerton-Dyer)**.** Let r be the rank of $E(K)$.

(a) The rank r agrees with multiplicity of $1/q$ as a root of $L(T,E)$.
(b) For some prime ℓ, the ℓ-primary component of $Ш_E$ is finite.

(c) The group $Ш_E$ is finite and

$$L(q^{-s}, E) \sim \frac{|Ш_E|\, R_E\, c_E}{|E(K)_{\mathrm{tors}}|^2 \cdot q^{g-1+\chi_E}} \cdot (s-1)^r$$

as $s \to 1$.

A nice exposition of the conjecture, with the explicit constant α, is given by Gross in [Gro11]; he also gives similar details for the more familiar number field analogue. Note that the regulator in [Gro11] is equal to $R_E/|E(K)_{\mathrm{tors}}|^2$.

Conjecture 2.3(c) clearly implies the other two parts; they are in fact equivalent.

Theorem 2.4 (Artin-Tate, Milne). *Statements* (a), (b) *and* (c) *of Conjecture* 2.3 *are equivalent.*

Proof. This follows from Theorem 8.1 of [Mil75]; it builds on the work of Artin and Tate presented in Tate's 1966 Bourbaki seminar [Tat66]. It should be noted that the L-functions in [Tat66] do not include the now familiar factors at the bad places; those were later worked out by Tate in [Tat75, §5]. □

The following gives an a priori inequality between the two quantities in Conjecture 2.3(a); it follows from the injectivity of the homomorphism h of Theorem 5.2 of [Tat66].

Proposition 2.5. *The rank of $E(K)$ is always less than or equal to the multiplicity of $1/q$ as a root of $L(T, E)$.*

In this paper, we will use only the following special consequence of the above results.

Corollary 2.6. *Suppose that $L(1/q, E) \neq 0$. Then*

$$L(1/q, E) \in q^{g-1+\chi_E} c_E \cdot (\mathbb{Q}^\times)^2.$$

Proof. Let r be the rank of $E(K)$. Proposition 2.5 and our assumption $L(1/q, E) \neq 0$ implies that $r \leq 0$. Therefore, $r = 0$, i.e., $E(K)$ is finite. Thus Conjecture 2.3(a) holds in this situation; hence Theorem 2.4 implies that the group $Ш_E$ is finite and that

$$L(1/q, E) = \frac{|Ш_E| \cdot c_E}{|E(K)_{\mathrm{tors}}|^2 \cdot q^{g-1+\chi_E}}$$

(we have $R_E = 1$ since $r = 0$). Therefore,

$$L(1/q, E) \in |Ш_E| \cdot q^{g-1+\chi_E} \cdot c_E \cdot (\mathbb{Q}^\times)^2.$$

Cassels constructed an alternating and non-degenerate pairing $Ш_E \times Ш_E \to \mathbb{Q}/\mathbb{Z}$, cf. [Mil06, Theorem 6.13], from which one can deduce that $Ш_E$ has square cardinality (we are using of course that $Ш_E$ is finite in our case). The result is then immediate. □

2.5. **L-functions modulo ℓ.** Take any prime $\ell \nmid 6q\mathcal{L}_E$ with $\mathcal{L}_E$ defined as in §2.2. Let $E[\ell]$ be the ℓ-torsion subscheme of E; it is a sheaf of $\mathbb{F}_\ell$-modules on U that is free of rank 2. The lisse sheaf $E[\ell]$ corresponds to a representation

$$\rho_{E,\ell}\colon \pi_1(U, \overline{\eta}) \to \mathrm{Aut}_{\mathbb{F}_\ell}(E[\ell]_{\overline{\eta}}) \cong \mathrm{GL}_2(\mathbb{F}_\ell),$$

where $\overline{\eta}$ is a geometric generic point of U. The Weil pairing $E[\ell] \times E[\ell] \to \mathbb{F}_\ell(1)$ is non-degenerate and alternating, so $\rho_{E,\ell}(\pi_1(U_{\overline{k}})) \subseteq \mathrm{SL}_2(\mathbb{F}_\ell)$. The following "big monodromy" result will be proved in §2.6.

Proposition 2.7. *We have* $\rho_{E,\ell}(\pi_1(U_{\bar{k}})) = \mathrm{SL}_2(\mathbb{F}_\ell)$.

Pushing forward, we obtain a sheaf $j_*(E[\ell])$ of $\mathbb{F}_\ell$-modules on C, where $j\colon U \to C$ is the inclusion morphism. Define the $\mathbb{F}_\ell$-vector space

$$V_{E,\ell} := H^1(C_{\bar{k}}, j_*(E[\ell])).$$

The Weil pairing $E[\ell] \times E[\ell] \to \mathbb{F}_\ell(1)$ is non-degenerate and alternating, and gives rise to an isomorphism $E[\ell]^\vee(1) \cong E[\ell]$ of sheaves. Using this isomorphism and Poincaré duality (for example, as in [Mil80, V Proposition 2.2(b)]), we obtain a non-degenerate and symmetric pairing

$$\langle\ ,\ \rangle\colon V_{E,\ell} \times V_{E,\ell} \to H^2(C_{\bar{k}}, \mathbb{F}_\ell(1)) \cong \mathbb{F}_\ell.$$

Therefore, $V_{E,\ell}$ with the pairing $\langle\ ,\ \rangle$ is an orthogonal space over $\mathbb{F}_\ell$.

There is a natural action of $\mathrm{Gal}(\bar{k}/k)$ on the vector space $V_{E,\ell}$. The Galois action on $V_{E,\ell}$ respects the pairing and hence gives rise to a representation

$$\theta_{E,\ell}\colon \mathrm{Gal}(\bar{k}/k) \to \mathrm{O}(V_{E,\ell}).$$

Let $\mathrm{Frob}_q \in \mathrm{Gal}(\bar{k}/k)$ be the *geometric* Frobenius (i.e., the inverse of $x \mapsto x^q$). The following says that we can recover $L(T,E)$ modulo ℓ from the characteristic polynomial of $\theta_{E,\ell}(\mathrm{Frob}_q)$.

Proposition 2.8. *The vector space* $V_{E,\ell}$ *has dimension* N_E *over* $\mathbb{F}_\ell$ *and*

$$\det(I - \theta_{E,\ell}(\mathrm{Frob}_q)T) \equiv L(T/q, E) \pmod{\ell}.$$

In many cases, Proposition 2.9 gives a way to compute the determinant and the spinor norm of $\theta_{E,\ell}(\mathrm{Frob}_q)$ in terms of some of the invariants of E. Our assumption $\ell \nmid 6q\mathcal{L}_E$ ensures that ℓ does not divide the integer $2^{N_E} q^{g-1+\chi_E} c_E \gamma_E$ (if $c_x(E)$ is divisible by a prime $p \geq 5$ for some $x \in |C|$, then Tate's algorithm shows that E must have Kodaira symbol I_n at x where $n = c_x(E)$, and hence p divides $\mathcal{L}_E$).

Proposition 2.9.

(i) *We have* $\det(\theta_{E,\ell}(\mathrm{Frob}_q)) = (-1)^{N_E} \cdot \varepsilon_E$.

(ii) *If* $\det(I - \theta_{E,\ell}(\mathrm{Frob}_q)) \neq 0$, *then* $\mathrm{sp}(-\theta_{E,\ell}(\mathrm{Frob}_q)) = 2^{N_E} q^{g-1+\chi_E} c_E \cdot (\mathbb{F}_\ell^\times)^2$.

(iii) *If* $\det(I + \theta_{E,\ell}(\mathrm{Frob}_q)) \neq 0$, *then* $\mathrm{sp}(\theta_{E,\ell}(\mathrm{Frob}_q)) = 2^{N_E} q^{g-1+\chi_E} c_E \cdot \gamma_E \cdot (\mathbb{F}_\ell^\times)^2$.

(iv) *If* $\det(I \pm \theta_{E,\ell}(\mathrm{Frob}_q)) \neq 0$, *then* $\mathrm{disc}(V_{E,\ell}) = \gamma_E \cdot (\mathbb{F}_\ell^\times)^2$.

The proofs of Propositions 2.8 and 2.9 will be given in §2.7 and §2.8, respectively. Recall that $\mathrm{sp}\colon \mathrm{O}(V_{E,\ell}) \to \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2$ is the spinor norm that we defined in §1.1.

Remark 2.10. Let $\mathcal{E}[\ell]$ be the ℓ-torsion subscheme of the Néron model $\mathcal{E} \to C$; it is a sheaf of $\mathbb{F}_\ell$-modules on C. For any non-empty open subvariety U' of C, one can show that $\mathcal{E}[\ell]$ is canonically isomorphic to $j'_*j'^*(\mathcal{E}[\ell])$, where $j'\colon U' \hookrightarrow C$ is the inclusion morphism. In particular with $U' = U$, we find that $V_{E,\ell} = H^1(C_{\bar{k}}, \mathcal{E}[\ell])$. If $U' \subseteq U$, then we have $V_{E,\ell} = H^1(C_{\bar{k}}, j'_*(E[\ell]|_{U'}))$.

Remark 2.11. Let $X \to C$ be a relatively minimal morphism extending $E \to U$, where X is a smooth and projective surface over k. One can give a filtration of $H^2(X, \mathbb{F}_\ell(1))$ as an $\mathbb{F}_\ell[\mathrm{Gal}(\bar{k}/k)]$-module such that one of the quotients is $V_{E,\ell}$ (and the cup pairing on H^2 induces our pairing on $V_{E,\ell}$). Similar remarks hold for the more general constructions of §3.

2.6. **Proof of Proposition 2.7.** Take any proper subgroup H of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. For a fixed algebraically closed field F whose characteristic is not ℓ, let $X(\ell)$ be the modular curve over F parametrizing elliptic curves with level ℓ-structure; it is smooth and projective. There is a natural action of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ on $X(\ell)$. Define the curve $X_H = X(\ell)/H$ and let $\pi_H\colon X_H \to X(\ell)/\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z}) \cong \mathbb{P}^1_F$ be the morphism down to the j-line. Let m be the least common multiple of the order of the poles of π_H.

We claim that $m = \ell$. There is a model of the modular curve X_H over $\operatorname{Spec}\mathbb{Z}[1/\ell]$ such that the the divisor consisting of cusps is étale over $\operatorname{Spec}\mathbb{Z}[1/\ell]$, for background see §3 in part IV of [DR73]. The integer m is thus independent of F, so we may take $F = \mathbb{C}$. Let Γ be the congruence subgroup consisting of matrices $A \in \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ such that A modulo ℓ belongs to H. The map $\pi_H\colon X_H(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ of compact Riemann surfaces comes from compactifying the natural quotient map $\mathfrak{h}/\Gamma \to \mathfrak{h}/\mathrm{SL}_2(\mathbb{Z})$, where $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper-half plane $\mathfrak{h}$ via linear fractional transformations. Therefore, m is equal to the least common multiple of the width of the cusps of Γ. Since Γ has level ℓ, we have $m = \ell$ (in [Woh64], the quantity m is called the "general level" of Γ and it is shown to agree with the usual level).

We now focus on the case $F = \bar{k}$. Suppose that $H = \rho_{E,\ell}(\pi_1(U_{\bar{k}}))$ is a proper subgroup of $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. Let $J\colon U_{\bar{k}} \to \mathbb{A}^1_{\bar{k}}$ be the morphism given by the j-invariant of E; it is dominant since E is non-isotrivial. Since $\rho_{E,\ell}(\pi_1(U_{\bar{k}})) \subseteq H$, the morphism J factors as

$$U_{\bar{k}} \to X_H \xrightarrow{\pi_H} \mathbb{A}^1_{\bar{k}}.$$

Let m' be the least common multiple of the order of the poles of the morphism $C_{\bar{k}} \to \mathbb{P}^1_{\bar{k}}$ extending J. The integer m' is divisible by m; the least common multiple of the order of the poles of π_H. By our claim, m' is divisible by ℓ. However, ℓ dividing m' implies that there is a closed point x of C such that $v_x(j_E)$ is negative and divisible by our prime $\ell \geq 5$; this in turn implies that ℓ divides $\mathcal{L}_E$. This contradicts our ongoing assumption that $\ell \nmid \mathcal{L}_E$, so $H = \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$ as desired.

2.7. **Proof of Proposition 2.8 and Theorem 2.2.** We first recall a cohomological description of $L(T, E)$. For each integer $n \geq 1$, let $E[\ell^n]$ be the ℓ^n-torsion subscheme of E; it is a lisse sheaf of $\mathbb{Z}/\ell^n\mathbb{Z}$-modules on U that is free of rank 2. The sheaves $\{E[\ell^n]\}_{n\geq 1}$ with the multiplication by ℓ morphism $E[\ell^{n+1}] \to E[\ell^n]$ form a lisse sheaf of $\mathbb{Z}_\ell$-modules on U which we denote by $T_\ell(E)$. Define the $\mathbb{Q}_\ell$-sheaf $\mathcal{F} := j_*(T_\ell(E)) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$, where $j\colon U \hookrightarrow C$ is the inclusion morphism, and let $\mathcal{F}^\vee$ be its dual.

Take any closed point x of C and let $\bar{x}$ be a geometric point of C mapping to x arising from a choice of algebraic closure $\overline{\mathbb{F}}_x$ of $\mathbb{F}_x$. The geometric Frobenius $\mathrm{Frob}_x \in \mathrm{Gal}(\overline{\mathbb{F}}_x/\mathbb{F}_x)$ acts on the fibers $\mathcal{F}_{\bar{x}}$ and $\mathcal{F}^\vee_{\bar{x}}$. One can show that

$$\det(I - \mathrm{Frob}_x T^{\deg x} \,|\, \mathcal{F}^\vee_{\bar{x}}) = L_x(T).$$

The Weil pairings give an isomorphism $\mathcal{F}^\vee \cong \mathcal{F}(-1)$, and hence the polynomials $\det(I - \mathrm{Frob}_x T^{\deg x} \,|\, \mathcal{F}_{\bar{x}})$ and $L_x(T/q)$ agree. Therefore,

$$L(T/q, E) = \prod_{x \in |C|} \det(I - \mathrm{Frob}_x T^{\deg x} \,|\, \mathcal{F}_{\bar{x}})^{-1}.$$

By the Grothendieck-Lefschetz trace formula, we have

$$L(T/q, E) = \prod\nolimits_i \det\left(I - \mathrm{Frob}_q T \,|\, H^i(C_{\bar{k}}, \mathcal{F})\right)^{(-1)^{i+1}}.$$

Lemma 2.12(ii) then shows that $L(T/q, E)$ is equal to the polynomial

$$\det(I - \mathrm{Frob}_q T \,|\, M \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell),$$

where M is the $\mathbb{Z}_\ell$-module $H^1(C_{\bar{k}}, j_*(T_\ell(E)))$. That the polynomial $L(T, E)$ has integer coefficients is clear from its power series definition.

Lemma 2.12. *Take any integer $i \neq 1$.*

(i) *We have $H^i(C_{\bar{k}}, j_*(E[\ell^n])) = 0$ for all $n \geq 1$.*

(ii) *We have $H^i(C_{\bar{k}}, j_*(T_\ell(E))) = 0$ and $H^i(C_{\bar{k}}, \mathcal{F}) = 0$.*

Proof. The lisse sheaf $E[\ell^n]$ corresponds to a representation

$$\rho_{E,\ell^n} \colon \pi_1(U, \bar{\eta}) \to \mathrm{Aut}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n]_{\bar{\eta}}) \cong \mathrm{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z}),$$

where $\bar{\eta}$ is a geometric generic point of U. The Weil pairing on $E[\ell^n]$ is non-degenerate and alternating, so $H := \rho_{E,\ell^n}(\pi_1(U_{\bar{k}})) \subseteq \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. Proposition 2.7 implies that the image of H modulo ℓ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$. We thus have $H = \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ since $\mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$ has no proper subgroups whose image modulo ℓ is $\mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})$, cf. Lemma 2 on page IV-23 of [Ser68].

We now prove (i). Since C has dimension 1, we need only consider $i \in \{0, 2\}$. The Weil pairing on $E[\ell^n]$ gives rise to an isomorphism $E[\ell^n]^\vee(1) \cong E[\ell^n]$ of sheaves on U. Using this isomorphism and Poincaré duality (for example, as in [Mil80, V Proposition 2.2(b)]), we obtain a non-degenerate pairing $H^0(C_{\bar{k}}, j_*(E[\ell^n])) \times H^2(C_{\bar{k}}, j_*(E[\ell^n]))) \to \mathbb{Z}/\ell^n\mathbb{Z}$. So we may assume that $i = 0$. We have

$$H^0(C_{\bar{k}}, j_*(E[\ell^n])) = H^0(U_{\overline{\mathbb{F}}_q}, E[\ell^n]) = (E[\ell^n]_{\bar{\eta}})^{\pi_1(U_{\bar{k}}, \bar{\eta})} = 0,$$

where the last equality uses that $\rho_{E,\ell^n}(\pi_1(U_{\bar{k}})) = \mathrm{SL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$. □

We have a short exact sequence $0 \to T_\ell(E) \xrightarrow{\times \ell} T_\ell(E) \to E[\ell] \to 0$ of sheaves on U. Pushing forward, we have a short exact sequence

$$0 \to j_*(T_\ell(E)) \xrightarrow{\times \ell} j_*(T_\ell(E)) \to j_*(E[\ell]) \to 0$$

of sheaves on C which gives an exact sequence

$$0 = H^0(C_{\bar{k}}, j_*(E[\ell])) \to M \xrightarrow{\times \ell} M \to V_{E,\ell} \to H^2(C_{\bar{k}}, j_*(T_\ell(E))) = 0, \tag{2.1}$$

where we have used Lemma 2.12 for the H^0 and H^2 terms. From (2.1), the finitely generated $\mathbb{Z}_\ell$-module M has trivial ℓ-torsion and is thus a free $\mathbb{Z}_\ell$-module of finite rank. From (2.1), we have an isomorphism of $M/\ell M$ and $V_{E,\ell}$ that respects the action of Frob_q. Therefore, $L(T/q, E) = \det(I - \mathrm{Frob}_q T | M \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell)$ is congruent modulo ℓ to $\det(I - \mathrm{Frob}_q T | V_{E,\ell})$.

To complete the proof of Proposition 2.8, it remains to show that $V_{E,\ell}$ has dimension N_E over $\mathbb{F}_\ell$. Define $\chi_\ell = \sum_i (-1)^i \dim_{\mathbb{F}_\ell} H^i(C_{\bar{k}}, j_*(E[\ell]))$. By [Mil80, V Theorem 2.12], we have

$$\chi_\ell = (2 - 2g) \dim_{\mathbb{F}_\ell} j_*(E[\ell])_{\bar{\eta}} - \sum\nolimits_x \mathfrak{f}_x = 4 - 4g - \sum\nolimits_x \mathfrak{f}_x,$$

where the sums are over the closed points of $C_{\bar{k}}$ and $\mathfrak{f}_x$ is the (exponent of the) conductor of the sheaf $j_*(E[\ell])$ at x. Since the sheaf $j_*(E[\ell])$ is tamely ramified (q is not a power of 2 or 3), we have $\mathfrak{f}_x = \dim_{\mathbb{F}_\ell} j_*(E[\ell])_{\bar{\eta}} - \dim_{\mathbb{F}_\ell} j_*(E[\ell])_{\bar{x}} = 2 - \dim_{\mathbb{F}} j_*(E[\ell])_{\bar{x}}$. In particular, $\mathfrak{f}_x$ is 0, 1, or 2 if E has good, multiplicative or additive reduction, respectively, at x. The sum of the $\mathfrak{f}_x$ over the closed points x of $C_{\bar{k}}$ is equal to $\sum_{x \in |C|} f_x(E) \deg x$. Therefore, $-\chi_\ell$ equals N_E. Using Lemma 2.12(i), we deduce that $V_{E,\ell} = H^1(C_{\bar{k}}, j_*(E[\ell]))$ has dimension $-\chi_\ell = N_E$ over $\mathbb{F}_\ell$. This completes the proof of Proposition 2.8.

It remains to prove Theorem 2.2. Let us prove the functional equation for $L(T,E)$ using what we have already proved. Take any prime $\ell \nmid 6q\mathcal{L}_E$. We have shown that $L(T/q,E) \equiv \det(I - AT) \pmod{\ell}$ for some $A \in \mathrm{O}(V_{E,\ell})$. We have $T^{N_E}\det(I - AT^{-1}) = \pm\det(I - AT)$ for every $A \in \mathrm{O}(V_{E,\ell})$, so $T^{N_E}L(T^{-1}/q,E) \equiv \pm L(T,E) \pmod{\ell}$. Since this holds for all but finitely many primes ℓ, we must have $T^{N_E}L(T^{-1}/q,E) = \varepsilon L(T/q,E)$ for a unique $\varepsilon \in \{\pm 1\}$. Observe that $L(T,E)$ has degree N_E since we know its reduction modulo ℓ has degree N_E for all primes $\ell \nmid 6q\mathcal{L}_E$.

It remains to show that $\varepsilon = \varepsilon_E$. We can express ε as a product of local root numbers $\varepsilon_x(E)$ over the closed points x of C; note that $\varepsilon_x(E) = 1$ if E has good reduction at x. Fix a closed point x of C for which E has bad reduction and let κ be the Kodaira symbol of E at x. If κ is not of the form I_n or I_n^* with $n > 0$, then $\varepsilon_x(E) = \chi_x(-r_x(E))$ by Theorem 3.1 of [CCH05]; this uses the ongoing assumption that $\gcd(q,6) = 1$ and also that the e of loc. cit. is $12/\gcd(e_x(E),12)$. If κ is of the form I_n^* for some $n \geq 0$, then $\varepsilon_x(E) = \chi_x(-r_x(E))$ by Theorem 3.1(2) of [CCH05]. If κ is of the form I_n for some $n > 0$, then $\varepsilon_x(E)$ is -1 or 1 when E has split or nonsplit multiplicative reduction, respectively, at x; cf. Theorem 3.1(2) and Lemma 2.2 of [CCH05]. This shows that ε agrees with our value ε_E. This completes the proof of Theorem 2.2.

2.8. **Proof of Proposition 2.9.**

To compute spinor norms, we will use the following result of Zassenhaus.

Lemma 2.13. *Let V be an orthogonal space of dimension N defined over a finite field $\mathbb{F}$ of odd characteristic. If $B \in \mathrm{O}(V)$ satisfies $\det(I + B) \neq 0$, then $\mathrm{sp}(B) = 2^N \det(I + B) \cdot (\mathbb{F}^\times)^2$.*

Proof. This is a special case of Zassenhaus' formula for the spinor norm in §2 of [Zas62]; see Theorem C.5.7 of [Con14] for a modern proof. □

Set $A := \theta_{E,\ell}(\mathrm{Frob}_q)$. By Proposition 2.8, the vector space $V_{E,\ell}$ has dimension N_E and we have

$$\det(I - AT) \equiv L(T/q,E) \pmod{\ell}. \tag{2.2}$$

Since A belongs to $\mathrm{O}(V_\ell)$, we find that $T^{N_E}\det(I - AT^{-1}) = \det(-A)\det(I - AT)$. By (2.2) and the functional equation in Theorem 2.2, we also have $T^{N_E}\det(I - AT^{-1}) = \varepsilon_E \det(I - AT)$. Comparing these two equations, we deduce that $\det(-A) = (-1)^{N_E}\det(A)$ agrees with ε_E. This proves part (i).

Now suppose that $\det(I - A) \neq 0$. Since $\det(I + (-A)) \neq 0$, Lemma 2.13 and (2.2) give us

$$\mathrm{sp}(-A) = 2^{N_E}\det(I - A) \cdot (\mathbb{F}_\ell^\times)^2 = 2^{N_E} L(1/q,E) \cdot (\mathbb{F}_\ell^\times)^2.$$

Therefore, $\mathrm{sp}(-A) = 2^{N_E} q^{g-1+\chi_E} c_E \cdot (\mathbb{F}_\ell^\times)^2$ by Corollary 2.6 (as noted in §2.5, $\ell \nmid q^{g-1+\chi_E} c_E$). This proves (ii). Before proving parts (iii) and (iv), we need Lemma 2.14.

Lemma 2.14. *Let E'/K be the quadratic twist of E/K by a non-square β in $k^\times$. Take any closed point x of C.*

(i) *The curves E' and E have the same Kodaira symbol at x.*

(ii) *We have* $a_x(E') = (-1)^{\deg x} a_x(E)$.
(iii) *The integer* $c_x(E)c_x(E')\gamma_x(E)^{\deg x}$ *is a square.*

Proof. First suppose that $\deg x$ is even. Since β is a square in $\mathbb{F}_x$, we find that E and E' are isomorphic over K_x. All the parts of the lemma are now immediate.

Now suppose that $\deg x$ is odd. Let $\mathcal{O}_x$ be the valuation ring of K_x and let π be a uniformizer. Tate's algorithm, as presented in [Sil94, IV §9] or [Tat75], starts with a Weierstrass equation

$$\mathsf{y}^2 + a_1\mathsf{x}\mathsf{y} + a_3 y = \mathsf{x}^3 + a_2\mathsf{x}^2 + a_4\mathsf{x} + a_6 \tag{2.3}$$

for E over the local field K_x with $a_i \in \mathcal{O}_x$. The algorithm then changes coordinates several times which imposes various conditions on the powers of π dividing the coefficients a_i; these conditions in loc. cit. are boxed (similar remarks hold for Subprocedure 7). By completing the square in (2.3), we find that this elliptic curve is isomorphic to the one defined by the equation

$$\mathsf{y}^2 = \mathsf{x}^3 + a_2'\mathsf{x}^2 + a_4'\mathsf{x} + a_6', \tag{2.4}$$

with $a_2' = a_2 + a_1^2/4$, $a_4' = a_4 + a_1a_3/2$ and $a_6' = a_6 + a_3^2/4$. Using that q is odd, we find that a_2', a_4' and a_6' belong to $\mathcal{O}_x$ and that the conditions in Tate's algorithm are preserved. So, we may thus always assume in any application of Tate's algorithm that we have a Weierstrass equation of the form (2.4).

If E over K_x is given by (2.4), then E' over K_x has a Weierstrass equation $\mathsf{y}^2 = \mathsf{x}^3 + a_2'\beta\mathsf{x}^2 + a_4'\beta^2\mathsf{x} + \beta^3 a_6'$. Applying Tate's algorithm, it is now easy to see that E and E' have the same Kodaira symbol and to determine the possibilities for $c_x(E)c_x(E')$. Let κ be the Kodaira symbol of E and E' at x. If $\kappa \in \{\mathrm{I}_0, \mathrm{II}, \mathrm{II}^*\}$, then $c_x(E)c_x(E') = 1$. If $\kappa = \mathrm{I}_n$ with $n > 0$, then $c_x(E)c_x(E') = \gcd(2n) \cdot n$ (precisely one of curves E and E' has split reduction at x; this uses that β is a non-square in $\mathbb{F}_x$ since $\deg x$ is odd). If $\kappa \in \{\mathrm{III}, \mathrm{III}^*\}$, then $c_x(E)c_x(E') = 2^2$. If $\kappa \in \{\mathrm{IV}, \mathrm{IV}^*\}$, then $c_x(E)c_x(E') = 1 \cdot 3 = 3$. If $\kappa = \mathrm{I}_n^*$ with n odd, then $c_x(E)c_x(E') = 2 \cdot 4 = 8$. If $\kappa = \mathrm{I}_n^*$ with $n > 0$ even, then $c_x(E)c_x(E') \in \{2^2, 4^2\}$. Finally, if $\kappa = \mathrm{I}_0^*$, then $c_x(E)c_x(E') \in \{1^2, 2^2, 4^2\}$. In all these cases, we find that integer $c_x(E)c_x(E')\gamma_x(E)$ is a square. Since $\deg x$ is odd, we conclude that $c_x(E)c_x(E')\gamma_x(E)^{\deg x} = c_x(E)c_x(E')\gamma_x(E) \cdot (\gamma_x(E)^{(\deg x - 1)/2})^2$ is a square.

It remains to verify that $a_x(E') = -a_x(E)$. This is immediate if E, and hence E', has additive reduction at x since $a_x(E') = a_x(E) = 0$. If E, and hence E', has multiplicative reduction at x, then one has split reduction and the other non-split reduction (since β is not a square in $\mathbb{F}_x$), so $a_x(E') = -a_x(E)$.

Finally suppose that E, and hence E', has good reduction at x. Fix a Weierstrass model $\mathsf{y}^2 = f(\mathsf{x})$ for $E_x/\mathbb{F}_x$ with a cubic $f \in \mathbb{F}_x[\mathsf{x}]$; the equation $\beta\mathsf{y}^2 = f(\mathsf{x})$ is a model of $E_x'/\mathbb{F}_x$. Take any $a \in \mathbb{F}_x$. If $f(a)$ is a non-zero square in $\mathbb{F}_x$, then there are two point in $E_x(\mathbb{F}_x)$ with x-coordinate a. If $f(a)$ is a non-square in $\mathbb{F}_x$, then there are two point on $E_x'(\mathbb{F}_x)$ with x-coordinate a. If $f(a) = 0$, then $E_x(\mathbb{F}_x)$ and $E_x'(\mathbb{F}_x)$ both have one point with x-coordinate a. Remembering the points at infinite, we find that $|E_x(\mathbb{F}_x)| + |E_x'(\mathbb{F}_x)| = 2q^{\deg x} + 2$ and hence $a_x(E') = -a_x(E)$. □

Now suppose that $\det(I + A) \neq 0$. By Lemma 2.13 and (2.2), we have

$$\mathrm{sp}(A) = 2^{N_E} \det(I + A) \cdot (\mathbb{F}_\ell^\times)^2 = 2^{N_E} L(-1/q, E) \cdot (\mathbb{F}_\ell^\times)^2.$$

Let E' be an elliptic curve over K that is a quadratic twist of E by a non-square in $k^\times$. Lemma 2.14(ii) implies that $L(T, E') = L(-T, E)$ and hence $L(1/q, E') =$

$L(-1/q,E)$. By Corollary 2.6, we deduce that $L(-1/q,E) \in q^{g-1+\chi_{E'}} c_{E'} (\mathbb{Q}^\times)^2$. We have $\chi_{E'} = \chi_E$ since E and E' have the same Kodaira symbols by Lemma 2.14(i). By Lemma 2.14(iii), the integer $c_E c_{E'} \gamma_E = \prod_{x \in |C|} c_x(E) c_x(E') \gamma_x(E)^{\deg x}$ is a square. Therefore, $L(-1/q,E) \in q^{g-1+\chi_E} c_E \gamma_E (\mathbb{Q}^\times)^2$. Since $\ell \nmid q^{g-1+\chi_E} c_E \gamma_E$, we conclude that

$$\mathrm{sp}(A) = 2^{N_E} q^{g-1+\chi_E} c_E \gamma_E \cdot (\mathbb{F}_\ell^\times)^2.$$

This completes the proof of (iii). Finally, suppose that $\det(I \pm A) \neq 0$. By (ii) and (iii), we have

$$\mathrm{sp}(-I) = \mathrm{sp}(-A)\,\mathrm{sp}(A) = (2^{N_E} q^{g-1+\chi_E} c_E) \cdot (2^{N_E} q^{g-1+\chi_E} c_E \gamma_E) \cdot (\mathbb{F}_\ell^\times)^2 = \gamma_E \cdot (\mathbb{F}_\ell^\times)^2.$$

This proves part (iv) since $\mathrm{disc}(V_{E,\ell}) = \mathrm{sp}(-I)$.

3. Families of quadratic twists

3.1. **Setup.** Let R be either a finite field whose characteristic is greater than 3 or a ring of the form $\mathbb{Z}[S^{-1}]$ with S a finite set of primes containing 2 and 3. Fix a Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}^3 + a_2(t)\mathsf{x}^2 + a_4(t)\mathsf{x} + a_6(t) \tag{3.1}$$

with $a_i \in R[t]$ such that its discriminant $\Delta \in R[t]$ is non-zero. Assume that the j-invariant $J(t)$ of the elliptic curve over $F(t)$ defined by (3.1), where F is the quotient field of R, has non-constant j-invariant. When $R = \mathbb{Z}[S^{-1}]$, we will allow ourselves to repeatedly enlarge the finite set S so that various properties hold. For example if R has characteristic 0, we shall assume that $\Delta(t) \not\equiv 0 \pmod p$ for all primes $p \notin S$.

We now consider quadratic twists by degree 1 polynomials. Define the R-scheme

$$M = \operatorname{Spec} R[u, \Delta(u)^{-1}].$$

Let k be any finite field that is an R-algebra (i.e., a finite extension of the field R or a finite field whose characteristic does not lie in S). Take any $m \in M(k)$, i.e., an element $m \in k$ with $\Delta(m) \neq 0$, and let E_m be the elliptic curve over $k(t)$ defined by the Weierstrass equation

$$(t-m)\mathsf{y}^2 = \mathsf{x}^3 + a_2(t)\mathsf{x}^2 + a_4(t)\mathsf{x} + a_6(t). \tag{3.2}$$

We will prove the following in §3.5.

Lemma 3.1. *After possibly increasing the finite set S when $R = \mathbb{Z}[S^{-1}]$, the multiset* $\mathrm{Kod}(E_m)$ *and the Kodaira symbol of E_m at ∞ are independent of the choice of k and m.*

After possibly increasing the set S when R has characteristic 0, we shall assume that the conclusions of Lemma 3.1 hold. Let Φ be the common multiset of Kodaira symbols from Lemma 3.1; the assumption that $J(t)$ is non-constant ensures that Φ is non-empty. Let κ_∞ be the common Kodaira symbol at ∞ of Lemma 3.1.

With notation as in §2.2, the integers N_{E_m}, χ_{E_m}, $\mathcal{L}_{E_m}$ and γ_{E_m} can be determined directly from $\mathrm{Kod}(E_m) = \Phi$. So the integers N_{E_m}, χ_{E_m}, $\mathcal{L}_{E_m}$ and γ_{E_m} are independent of k and m; denote their common values by N, χ, $\mathcal{L}$ and γ, respectively.

Define the integer $B_{E_m} := \sum_{x \neq \infty} b_x(E_m) \deg x$, where the sum is over the closed points of $\mathbb{A}^1_k = \operatorname{Spec} k[t]$ and the $b_x(E_m)$ are defined in §2.2. Since B_{E_m} can be determined directly from Φ and κ_∞, we find that it is independent of k and m; denote this common integer by B.

Finally, take any prime $\ell \nmid 6\mathcal{L}$ that is not the characteristic of R. If R has characteristic 0, we replace S by $S \cup \{\ell\}$.

3.2. **Main representation.** Fix notation and assumptions as in §3.1. The goal of this section is to prove Proposition 3.2 which gives a representation of the étale fundamental group of M that encodes the L-functions of the various quadratic twists E_m.

Proposition 3.2. *After possibly replacing S by a larger finite set of primes when R has characteristic* 0*, there is an N-dimensional orthogonal space V_ℓ over $\mathbb{F}_\ell$ and a continuous representation*

$$\theta_\ell \colon \pi_1(M) \to \mathrm{O}(V_\ell)$$

such that for any R-algebra k that is a finite field of order q and any $m \in M(k)$, the following hold:

(a) $\det(I - \theta_\ell(\mathrm{Frob}_m)T) \equiv L(T/q, E_m) \pmod{\ell}$,
(b) $\det(\theta_\ell(\mathrm{Frob}_m)) = (-1)^N \varepsilon_{E_m}$,
(c) *if* $\det(I - \theta_\ell(\mathrm{Frob}_m)) \neq 0$*, then* $\mathrm{sp}(-\theta_\ell(\mathrm{Frob}_m)) = 2^N q^{-1+\chi} c_{E_m} \cdot (\mathbb{F}_\ell^\times)^2$,
(d) *if* $\det(I + \theta_\ell(\mathrm{Frob}_m)) \neq 0$*, then* $\mathrm{sp}(\theta_\ell(\mathrm{Frob}_m)) = 2^N q^{-1+\chi} c_{E_m}\gamma \cdot (\mathbb{F}_\ell^\times)^2$,
(e) *if* $\det(I \pm \theta_\ell(\mathrm{Frob}_m)) \neq 0$*, then* $\mathrm{disc}(V_\ell) = \gamma \cdot (\mathbb{F}_\ell^\times)^2$.

We now construct a lisse sheaf of $\mathbb{F}_\ell$-modules that will give rise to the representation θ_ℓ of Proposition 3.2. We have already defined the R-scheme $M = \operatorname{Spec} A$, where $A := R[u, \Delta(u)^{-1}]$. Set $C = \mathbb{P}^1_M$; it is a smooth proper curve of genus 0 over M that can be obtained by extending $\mathbb{A}^1_M = \operatorname{Spec} A[t]$. Define $U = \operatorname{Spec} A[t, (t-u)^{-1}, \Delta(t)^{-1}]$; it is an open M-subscheme of C. After possibly enlarging the set S, we may assume that the closed subscheme $D := C - U$ of C is étale over M.

The Weierstrass equation

$$(t-u)\mathsf{y}^2 = \mathsf{x}^3 + a_2(t)\mathsf{x}^2 + a_4(t)\mathsf{x} + a_6(t)$$

defines an elliptic curve $E \to U$. Let $\mathcal{F} := E[\ell]$ be the ℓ-torsion subscheme of E. The morphism $\mathcal{F} \hookrightarrow E \to U$ allows us to view $\mathcal{F}$ as a lisse $\mathbb{F}_\ell$-sheaf on U.

Define the sheaf

$$\mathcal{G} := R^1\pi_*(j_*(\mathcal{F}))$$

of $\mathbb{F}_\ell$-modules on M, where $j \colon U \to C$ is the inclusion morphism and $\pi \colon C \to M$ is the structure morphism. The Weil pairing gives an alternating pairing $\mathcal{F} \times \mathcal{F} \to \mathbb{F}_\ell(1)$. The cup product and this pairing on $\mathcal{F}$ gives a symmetric pairing

$$\mathcal{G} \times \mathcal{G} \to R^2\pi_*(j_*(\mathcal{F}) \otimes j_*(\mathcal{F})) \to R^2\pi_*(j_*(\mathbb{F}_\ell(1))) = \mathbb{F}_\ell$$

of sheaves on M.

Lemma 3.3. *The sheaf $\mathcal{G}$ is lisse.*

Proof. Define $\overline{\pi} = \pi \circ j$; it is the structure morphism $U \to M$. We can identify $\mathcal{G}$ with a subsheaf of $R^1\overline{\pi}_*(\mathcal{F})$; for example by using the low degree terms of the Leray spectral sequence. The homomorphism $R^1\overline{\pi}_!(\mathcal{F}) := R^1\pi_*(j_!(\mathcal{F})) \to \mathcal{G}$ induced by the inclusion $j_!(\mathcal{F}) \subseteq j_*(\mathcal{F})$ is surjective (this uses that $D \to M$ has relative dimension 0). Therefore, $\mathcal{G}$ is the image of a homomorphism $R^1\overline{\pi}_!(\mathcal{F}) \to R^1\overline{\pi}_*(\mathcal{F})$. It thus suffices to prove that the sheaves $R^1\overline{\pi}_!(\mathcal{F})$ and $R^1\overline{\pi}_*(\mathcal{F})$ are lisse. Using Poincaré duality, it suffices to prove that $R^1\overline{\pi}_!(\mathcal{F})$ and $R^1\overline{\pi}_!(\mathcal{F}^\vee)$ are lisse.

The sheaves $R^1\pi_!(\mathcal{F})$ and $R^1\pi_!(\mathcal{F}^\vee)$ of $\mathbb{F}_\ell$-modules are lisse by Corollaire 2.1.1 of [Lau81]; the function φ of loc. cit. is constant since $D \to M$ is étale and the sheaves $\mathcal{F}$ and $\mathcal{F}^\vee$ are tamely ramified (since 2 and 3 are invertible in A). □

Now take any $m \in M(k)$, where k is a finite field of order q that is an R-algebra. Base changing by m, we obtain from $E \to U \to M$ an open subvariety U_m of $C_m = \mathbb{P}^1_k$ and an elliptic curve $E_m \to U_m$. The generic fiber of $E_m \to U_m$ is an elliptic curve defined over $k(t)$ given by the equation (3.2) with u substituted by m which, by abuse of notation, we have already denoted by E_m.

Let $\overline{m}$ be a geometric point of M lying over m obtained from an algebraic closure $\bar{k}$ of k. Let $\mathcal{G}_{\overline{m}}$ be the fiber of $\mathcal{G}$ at $\overline{m}$; it is an $\mathbb{F}_\ell$-vector space that comes with a symmetric pairing $\langle\, ,\, \rangle$ from specializing the pairing on $\mathcal{G}$. The geometric Frobenius Frob_m acts on $\mathcal{G}_{\overline{m}}$. By proper base change, we have

$$\mathcal{G}_{\overline{m}} = H^1(C_{\overline{m}}, j'_*(E_m[\ell])) = H^1(C_{\bar{k}}, j'_*(E_m[\ell])) = V_{E_m,\ell}, \tag{3.3}$$

where $j' \colon U_m \hookrightarrow C_m$ is the inclusion morphism; the last equality uses Remark 2.10. The induced pairing on $\mathcal{G}_{\overline{m}}$ agrees with the pairing on $V_{E_m,\ell}$ from §2.5. With respect to (3.3), the action of Frob_m on $\mathcal{G}_{\overline{m}}$ corresponds to the action of Frob_q on $V_{E,\ell}$.

Let $\bar{\xi}$ be a geometric generic point of M. Our pairing on $\mathcal{G}$ is non-degenerate since $\mathcal{G}$ is lisse and it is non-degenerate on the fiber $\mathcal{G}_{\overline{m}}$. Denote by V_ℓ the fiber of $\mathcal{G}$ at $\bar{\xi}$ with its pairing; it is an orthogonal space over $\mathbb{F}_\ell$. The lisse sheaf $\mathcal{G}$ thus gives rise to a continuous representation

$$\theta_\ell \colon \pi_1(M, \bar{\xi}) \to \mathrm{O}(V_\ell).$$

With $m \in M(k)$ above, we find that there is an isomorphism $\varphi \colon V_\ell \xrightarrow{\sim} V_{E,\ell}$ of orthogonal spaces such that $\varphi^{-1} \circ \theta_{E,\ell}(\mathrm{Frob}_q) \circ \varphi$ lies in the same conjugacy class of $\mathrm{O}(V_\ell)$ as $\theta_\ell(\mathrm{Frob}_m)$. All the properties of θ_ℓ given in Proposition 3.2 are now direct consequences of Propositions 2.8 and 2.9. This concludes the proof of Proposition 3.2.

3.3. **Big monodromy.** Fix notation and assumptions as in §3.1. After possibly increasing S when R has characteristic 0, let

$$\theta_\ell \colon \pi_1(M) \to \mathrm{O}(V_\ell)$$

be the representation of Proposition 3.2.

Let Φ' be the multiset consisting of Φ with one symbol κ_∞ removed. Assume further that the following conditions hold:

- Φ' contains I_n for some $n \geq 1$,
- Φ' contains more than one I_0^*,
- $6B \leq N$.

The following explicit version of a theorem of Hall [Hal08] says that the image under θ_ℓ of the geometric fundamental group is big.

Theorem 3.4 (Hall). *With assumptions as above, the group $\theta_\ell(\pi_1(M_{\overline{F}}))$ contains $\Omega(V_\ell)$ and is not a subgroup of $\mathrm{SO}(V_\ell)$, where $\overline{F}$ is an algebraic closure of the quotient field F of R.*

In §3.4, we will sketch some of the steps in Hall proof of Theorem 3.4. The main reason for doing this is to ensure that all the conditions are explicit (in [Hal08], one is allowed to replace the original curve by a suitably high degree twist so that the last two conditions before the statement of the theorem hold). We will also need to refer to some of the details when handling the $n = 5$ case of Theorem 1.1.

3.4. **Sketch of Theorem 3.4.** First suppose that $R = \mathbb{Z}[S^{-1}]$ and let $\mathcal{G}$ be the lisse sheaf on M from §3.2. Take any $p \notin S$ and let $\theta_{p,\ell}\colon \pi_1(M_{\mathbb{F}_p}) \to \mathrm{O}(V_\ell)$ be the representation obtained by specializing θ_ℓ, equivalently $\mathcal{G}$, at the fiber of M above p. Since the formation of $\mathcal{G}$ commutes with arbitrary base change, the representation $\theta_{p,\ell}$ agrees with the representation arising from the setup with §3.1 by starting with the same Weierstrass equation except replacing R by $\mathbb{F}_p$. For $p \notin S$ sufficiently large, all the conditions of Theorem 3.4 hold. Since $\theta_{p,\ell}(\pi_1(M_{\overline{\mathbb{F}}_p}))$ agrees with $\theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}}))$ for all sufficiently large p, it thus suffices to prove the theorem in the case where R is a finite field.

Now assume that R is a finite field k whose characteristic is at least 5. We now describe the setup and key results of Hall from §6 of [Hal08].

Set $C = \mathbb{P}^1_k$ and denote its function field by $K := k(t)$. Let E_1 be the elliptic curve over K defined by (3.1). For each non-zero polynomial $f \in k[t]$, let E_f be the elliptic curve over K obtained by taking the quadratic twist of E_1 by f. *Warning:* we are following Hall's notation throughout §3.4; the curve E_{t-m} is denoted elsewhere in the paper by E_m.

We have $\ell \geq 5$ and ℓ is invertible in k. The j-invariant $j_{E_1} \in K$ of E_1 is the same as the j-invariant of each E_f. Therefore, $\mathcal{L}_{E_f}$ is independent of f and hence agrees with $\mathcal{L}$. In particular, our assumption $\ell \nmid 6\mathcal{L}$ implies that ℓ does not divide $\max\{1, -v_x(j_{E_1})\}$ for all $x \in |C|$. In [Hal08, §6], it is also assumed that ℓ is chosen so that the Galois group of the extension $K(E_1[\ell])/K$ contains a subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell)$; however, this is a consequence of $\ell \nmid 6q\mathcal{L}$ and Proposition 2.7.

Let $\mathcal{E}_f \to C$ be the Néron model of E_f/K and let $\mathcal{E}_f[\ell]$ be its ℓ-torsion subscheme. We have $V_{E_f,\ell} = H^1(C_{\bar{k}}, \mathcal{E}_f[\ell])$ by Remark 2.10.

For each integer $d \geq 0$, we let F_d be the open subvariety of $\mathbb{A}^{d+1}_k$ consisting of tuples $(a_0, \ldots, a_d)$ for which the polynomial $\sum_{i=0}^d a_i t^i$ is separable of degree d and relatively prime to $\Delta(t) \in k[t]$. For each extension k'/k, we will identify each point $f \in F_d(k')$ with the corresponding degree d polynomial in $k'[t]$.

Now assume that $d \geq 1$. As noted in [Hal08], there is an orthogonally self-dual lisse sheaf $\mathcal{T}_{d,\ell} \to F_d$ of $\mathbb{F}_\ell$-modules such that for any finite extension $k' \subseteq \bar{k}$ of k and any $f \in F_d(k')$, the (geometric) fiber of $\mathcal{T}_{d,\ell}$ above f is $H^1(C_{\bar{k}}, \mathcal{E}_f[\ell]) = V_{E_f,\ell}$. Moreover, the pairing on $\mathcal{T}_{d,\ell}$ agrees with the pairing from §2.5 on the fibers $V_{E_f,\ell}$.

Fix a polynomial $g \in F_{d-1}(k)$. Let U_g be the open subvariety of $\mathbb{A}^1_k$ consisting of c for which $\Delta(c)g(c) \neq 0$. We view U_g as a closed subvariety of F_d via the closed embedding $\varphi\colon U_g \hookrightarrow F_d$, $c \mapsto (c-t)g(t)$. We then have an orthogonally self-dual lisse sheaf $\varphi^*(\mathcal{T}_{d,\ell})$ of $\mathbb{F}_\ell$-modules on U_g.

In §6.3 of [Hal08], it is noted that $\varphi^*(\mathcal{T}_{d,\ell})$ over $U_{g,\bar{k}}$ agrees with the middle convolution sheaf $\mathrm{MC}_{-1}(\mathcal{E}_g[\ell])$; this has the consequence that the sheaf $\varphi^*(\mathcal{T}_{d,\ell})$ is geometrically irreducible and tame.

We now focus on the case with $d = 1$ and $g = -1$. The variety U_g in $\mathbb{A}^1_k = \operatorname{Spec} k[u]$ is equal to $M = \operatorname{Spec} k[u, \Delta(u)^{-1}]$. For each finite extension k'/k and $m \in M(k')$, the (geometric) fiber of $\varphi^*(\mathcal{T}_{d,\ell})$ above m is $H^1(C_{\bar{k}}, \mathcal{E}_{t-m}[\ell]) = V_{E_{t-m},\ell}$ (which is $V_{E_m,\ell}$ in the notation of §3.1).

We find that the sheaf $\varphi^*(\mathcal{T}_{d,\ell})$ over $M = U_g$ is precisely our sheaf $\mathcal{G}$ from §3.2 and they have the same pairing. We record the follow consequence for θ_ℓ.

Lemma 3.5. *The representation $\theta_\ell \colon \pi_1(M) \to \mathrm{O}(V_\ell)$ is geometrically irreducible and tame.* □

Since θ_ℓ is tamely ramified, its restriction to $\pi_1(M_{\bar{k}})$ factors through the maximal tame quotient $\pi_1^t(M_{\bar{k}})$ of $\pi_1(M_{\bar{k}})$. Let Z be the set of $\bar{k}$-points of $\mathbb{A}^1_k - M$; it consists of the $c \in \bar{k}$ for which $\Delta(c) = 0$. For each point $c \in Z \cup \{\infty\}$, let σ_c be a generator of an inertia subgroup $\pi_1^t(M_{\bar{k}})$ at c. Choosing an ordering of the points $Z \cup \{\infty\}$, we may assume that the σ_c are taken so that the product of the σ_c, with respect to the ordering, is trivial.

The group $\pi_1^t(M_{\bar{k}})$ is (topologically) generated by $\{\sigma_c : c \in Z\}$; we do not need σ_∞ since the product of the σ_c is trivial. In particular, $\{\theta_\ell(\sigma_c) : c \in Z\}$ generates the group $\theta_\ell(\pi_1(M_{\bar{k}}))$.

We need two quick group theory definitions. For each $A \in \mathrm{O}(V_\ell)$, we define $\mathrm{drop}(A)$ to be the codimension in V_ℓ of the subspace fixed by A. We say that an element $A \in \mathrm{O}(V_\ell)$ is an isotropic shear if it is non-trivial, unipotent and satisfies $(A - I)^2 = 0$.

Lemma 3.6. *Fix a point $c \in Z$ and let κ be the Kodaira symbol of E_1/K at $t = c$.*

(i) *If $\kappa = \mathrm{I}_0$, then $\theta_\ell(\sigma_c) = I$.*
(ii) *If $\kappa = \mathrm{I}_n$ for some $n \geq 1$, then $\theta_\ell(\sigma_c)$ is a reflection.*
(iii) *If $\kappa = \mathrm{I}_0^*$, then $\theta_\ell(\sigma_c)$ is an isotropic shear.*
(iv) *We have* $\mathrm{drop}(\theta_\ell(\sigma_c)) \leq 2$.

Proof. The is a consequence of Lemma 6.5 of [Hal08] and also its proof for part (iv). It is actually stated for $E_g = E_{-1}$ in loc. cit., but E_1 and E_{-1} have the same Kodaira symbols). □

Remark 3.7. For later, we note that up to this point we have not made use of the three additional assumptions from §3.3.

The following group theoretic result is a special case of Theorem 3.1 of [Hal08] with $r = 2$.

Proposition 3.8. *Let G be an irreducible subgroup of $\mathrm{O}(V_\ell)$ generated by a set $\mathcal{S}$. Assume that G contains a reflection and an isotropic shear. Suppose that there is a subset $\mathcal{S}_0 \subseteq \mathcal{S}$ satisfying the following properties:*

(a) $\mathrm{drop}(A) \leq 2$ *for every $A \in \mathcal{S}$,*
(b) *every $A \in \mathcal{S} - \mathcal{S}_0$ has order relative prime to 6 or is a reflection,*
(c) $6|\mathcal{S}_0| \leq \dim_{\mathbb{F}_\ell} V_\ell$.

Then G contains $\Omega(V_\ell)$ and is not a subgroup of $\mathrm{SO}(V_\ell)$.

We can now finish our sketch of Theorem 3.4. Define the group $G := \theta_\ell(\pi_1(M_{\bar{k}}))$; it is irreducible since θ_ℓ is geometrically irreducible. The group G is generated by the set $\mathcal{S} := \{\theta_\ell(\sigma_c) : c \in Z\}$. Let $\mathcal{S}_0$ be the set of $\theta_\ell(\sigma_c)$ with $c \in Z$ for which E_1 has additive reduction at $t = c$ and the Kodaira symbol at $t = c$ is not I_0^*.

We may assume that $M(k)$ is non-empty (we may always replace k by a finite extension at the beginning). Fix any $m \in M(k)$. The curve E_{t-m}/K is a quadratic twist of E_1/K by $t - m$. Hence E_{t-m} and E_1 have the same Kodaira symbol at each closed point x of $\mathbb{A}^1_k$ except for one (correspond to the point $t = m$) for which E_{t-m} has Kodaira symbol I_0^* and E_1 has good reduction.

The two assumptions of §3.3 on Φ' imply that E_1 has multiplicative reduction at some $c \in Z$ and Kodaira symbol I_0^* at some $c \in Z$. From Propositions 3.6(ii) and (iii), we deduce that G contains a reflection and an isotropic shear.

Proposition 3.6(iv) implies that $\operatorname{drop}(A) \leq 2$ for all $A \in \mathcal{S}$. For every $A \in \mathcal{S} - \mathcal{S}_0$, Proposition 3.6 implies that either A is a reflection or that the order of A is a power of ℓ (which is relatively prime to 6 since $\ell \geq 5$).

We have $|\mathcal{S}_0| \leq \sum_{x \neq \infty} b_x(E_1) \deg x$, where the sum is over the closed points x of $\mathbb{A}^1_k$. By our comparison of the Kodaira symbols of E_1 and E_{t-m}, we deduce that $|\mathcal{S}_0| \leq B_{E_m} = B$. Our assumption $6B \leq N$ then implies that $6|\mathcal{S}_0| \leq 6B \leq N = \dim_{\mathbb{F}_\ell} V_\ell$.

The conditions of Proposition 3.8 have all been verified and thus $G = \theta_\ell(\pi_1(M_{\bar{k}}))$ contains $\Omega(V_\ell)$ and is not a subgroup of $\mathrm{SO}(V_\ell)$. This completes the proof of Theorem 3.4.

3.5. **Proof of Lemma 3.1.** Let E' be the elliptic curve over $k(t)$ given by (3.1); denote its Kodaira symbol at ∞ by κ'_∞.

Take any closed point x of $\mathbb{P}^1_k$. Let κ and κ' be the Kodaira symbols of E_m and E', respectively, at x. If t^{-1} and $t-m$ are not uniformizers for the local field K_x, then we will have $\kappa = \kappa'$. If $t-m$ is a uniformizer for K_x, then E' has good reduction at x (since $\Delta(m) \neq 0$) and hence $\kappa = \mathrm{I}_0^*$. Finally, if t^{-1} (and hence also $(t-m)^{-1}$) is a uniformer for K_x, then the pair $\{\kappa, \kappa'\}$ is one of the following: $\{\mathrm{I}_n, \mathrm{I}_n^*\}$, $\{\mathrm{II}, \mathrm{IV}^*\}$, $\{\mathrm{IV}, \mathrm{II}^*\}$, $\{\mathrm{III}, \mathrm{III}^*\}$; in particular, κ is determined by $\kappa' = \kappa'_\infty$. Therefore, $\operatorname{Kod}(E_m)$ and the Kodaira symbol of E_m at ∞ are determined by $\operatorname{Kod}(E')$ and κ'_∞. Observe that the quantities $\operatorname{Kod}(E')$ and κ'_∞ do not change if we replace E' by its base extension to $k'(t)$ where k' is any finite extension of k. The lemma is now immediate when R is a finite field.

When $R = \mathbb{Z}[S^{-1}]$, it suffices to show that for the elliptic curve E' over $\mathbb{F}_p(t)$ given by (3.1), the multiset $\operatorname{Kod}(E')$ and the Kodaira symbol of E' at ∞ is independent of p for all sufficiently large $p \notin S$. The equation (3.1) defines an elliptic surface $\pi\colon X \to \mathbb{P}^1_{\mathbb{Q}}$, where $\mathbb{P}^1_{\mathbb{Q}} = \operatorname{Spec} \mathbb{Q}[t] \cup \{\infty\}$. We may assume that X is geometrically smooth and projective, and that π is relatively minimal. The singular fibers of π are, geometrically, projectively lines and the pattern in which they intersect determines the Kodaira symbol of the fiber. Choosing models and increasing S, we obtain a morphism $\mathcal{X} \to \mathbb{P}^1_R$ of R-scheme. For all primes $p \notin S$, after possibly increasing S, we find that the number of singular fibers of $\mathcal{X}_{\overline{\mathbb{F}}_p} \to \mathbb{P}^1_{\overline{\mathbb{F}}_p}$, their Kodaira symbols (counted with multiplicity), and the Kodaira symbol above ∞ agree with those of $X_{\overline{\mathbb{Q}}} = \mathcal{X}_{\overline{\mathbb{Q}}} \to \mathbb{P}^1_{\overline{\mathbb{Q}}}$. This gives the desired independence.

4. A criterion

In this section, we give a criterion for various simple groups $\mathrm{P}\Omega(V)$ to occur as the Galois group of a regular extension of $\mathbb{Q}(t)$. The goal is not to give the most general formulation possible, but simply one that covers almost all of our cases.

Consider a Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}^3 + a_2(t)\mathsf{x}^2 + a_4(t)\mathsf{x} + a_6(t) \tag{4.1}$$

with $a_2, a_4, a_6 \in \mathbb{Z}[t]$. Let $\Delta \in \mathbb{Z}[t]$ be the discriminant of (4.1) and assume that it is non-zero. Assume that the j-invariant $J(t) \in \mathbb{Q}(t)$ of the elliptic curve over $\mathbb{Q}(t)$ defined by (3.1) is non-constant.

For each prime $p \geq 5$, let $M(\mathbb{F}_p)$ be the set of $m \in \mathbb{F}_p$ for which $\Delta(m) \neq 0$. Let E_m be the elliptic curve over $\mathbb{F}_p(t)$ defined by the Weierstrass equation

$$(t-m) \cdot \mathsf{y}^2 = \mathsf{x}^3 + a_2(t)\mathsf{x}^2 + a_4(t)\mathsf{x} + a_6(t).$$

Let $\mathbb{P}^1_{\mathbb{F}_p}$ be the smooth proper curve over $\mathbb{F}_p$ obtained by adjoining to $\mathbb{A}^1_{\mathbb{F}_p} := \operatorname{Spec} \mathbb{F}_p[t]$ a point ∞; it has function field $\mathbb{F}_p(t)$.

From §3.1, we find that there are integers N, χ, $\mathcal{L}$ and γ such $N = N_{E_m}$, $\chi = \chi_{E_m}$, $\mathcal{L} = \mathcal{L}_{E_m}$ and $\gamma = \gamma_{E_m}$ for all sufficiently large primes p and all $m \in M(\mathbb{F}_p)$. From §3.1, there is an integer B that equals $B_{E_m} := \sum_{x \neq \infty} b_x(E_m) \deg x$ for all sufficiently large primes p and all $m \in M(\mathbb{F}_p)$, where the sum is over the closed points of $\mathbb{A}^1_{\mathbb{F}_p}$.

Fix a non-constant $h \in \mathbb{Q}(t)$ whose numerator and denominator have degree at most 4. There are unique relatively prime $\alpha, \beta \in \mathbb{Z}[t]$ such that the leading coefficient of β is positive and $h = \alpha/\beta$. For each prime $p \geq 5$, let $W(\mathbb{F}_p)$ be the set of $w \in \mathbb{F}_p$ that satisfy $\beta(w) \neq 0$ and $\Delta(h(w)) \neq 0$. We have a map $W(\mathbb{F}_p) \to M(\mathbb{F}_p)$, $w \mapsto h(w) = \alpha(w)/\beta(w)$.

Assume that the following hold for all for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$:

- $E_{h(w)}$ has multiplicative reduction at some closed point of $\mathbb{A}^1_{\mathbb{F}_p}$,
- $E_{h(w)}$ has Kodaira symbol I_0^* at more that one closed point of $\mathbb{A}^1_{\mathbb{F}_p}$.

Assume also that $6B \leq N$.

Fix a prime $\ell \geq 5$ that does not divide $\mathcal{L}$. Assume that one of the following three conditions holds:

(A) The integers N and χ are odd, and γ is a square modulo ℓ. For all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$, the integer $2 \cdot c_{E_{h(w)}}$ is a square modulo ℓ.

(B) The integer N is even and γ is a non-square modulo ℓ. For all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$, we have $\varepsilon_{E_{h(w)}} = 1$.

(C) The integer N is even, χ is odd, and γ is a square modulo ℓ. For all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$, we have $\varepsilon_{E_{h(w)}} = 1$ and the integer $c_{E_{h(w)}}$ is a square modulo ℓ.

Theorem 4.1. *Fix notation and assumptions as above. Let V be an orthogonal space of dimension N over $\mathbb{F}_\ell$. If N is even, suppose further that* $\operatorname{disc}(V) = \gamma \cdot (\mathbb{F}_\ell^\times)^2$. *Then the group $\Omega(V)$, and hence also* $\mathrm{P}\Omega(V)$*, occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.*

Proof. For a finite set of primes S, define the ring $R = \mathbb{Z}[S^{-1}]$. We will allow ourselves to increase the finite set S to ensure various conditions hold; for example, we will assume that S contains 2, 3, ℓ and the primes p for which $\Delta(t) \equiv 0 \pmod{p}$. We may also assume that all the conditions that are assumed to hold for sufficiently large primes p actually hold for all $p \notin S$.

Define the R-scheme $M = \operatorname{Spec} R[u, \Delta(u)^{-1}]$. For each prime $p \notin S$, $M(\mathbb{F}_p)$ is indeed the set of $m \in \mathbb{F}_p$ for which $\Delta(m) \neq 0$. After possibly increasing S, there is an orthogonal space V_ℓ over $\mathbb{F}_\ell$ of dimension N and a representation

$$\theta_\ell \colon \pi_1(M) \to \mathrm{O}(V_\ell)$$

satisfying the conclusions of Proposition 3.2.

Let Φ' be the multiset of Kodaira symbols as in §3.3. Our assumption that E_m has multiplicative reduction at some closed point $\mathbb{A}^1_{\mathbb{F}_p}$ implies that Φ' contains a symbol I_n for some $n \geq 1$. Our assumption that E_m has at least Kodaira symbol I_0^* at more than one closed point $\mathbb{A}^1_{\mathbb{F}_p}$ implies that Φ' contains the symbol I_0^* at least twice. We have $6B \leq N$ by assumption. Theorem 3.4 now applies and thus $\theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}})) \supseteq \Omega(V_\ell)$.

Define the R-scheme $W = \operatorname{Spec} R[v, \beta(v)^{-1}, \Delta(h(v))^{-1}]$. For each prime $p \notin S$, $W(\mathbb{F}_p)$ is indeed the set of $w \in \mathbb{F}_p$ for which $\beta(w) \neq 0$ and $\Delta(h(w)) \neq 0$. Define the morphism

$$\varphi\colon W \to M,\ w \mapsto h(w).$$

We can replace $a_i(t)$ by $a_i(t)f(t)^i$ for a fixed non-zero separable polynomial $f(t) \in \mathbb{Z}[t]$ that is relatively prime to $\Delta(t)$; the new discriminant equals $f(t)^6\Delta(t)$ and all the assumptions of the theorem still hold. We may choose f so that the morphism $W_{\mathbb{Q}} \to M_{\mathbb{Q}}$ is finite étale. After possibly increasing the set S, we may thus assume that φ is also finite étale.

The morphism φ thus gives rise to an injective homomorphism $\varphi_*\colon \pi_1(W) \hookrightarrow \pi_1(M)$; uniquely determined up to conjugacy. Let

$$\vartheta_\ell\colon \pi_1(W) \to \mathrm{O}(V_\ell)$$

be the representation obtained by composing φ_* and θ_ℓ. For each prime $p \notin S$ and $w \in W(\mathbb{F}_p)$, we have an equality

$$\vartheta_\ell(\mathrm{Frob}_w) = \theta_\ell(\mathrm{Frob}_{h(w)})$$

of conjugacy classes in $\mathrm{O}(V_\ell)$. Define the groups

$$G := \vartheta_\ell(\pi_1(W)) \quad \text{and} \quad G^g := \vartheta_\ell(\pi_1(W_{\overline{\mathbb{Q}}})).$$

We claim that $G^g \supseteq \Omega(V_\ell)$. The étale morphism φ has degree at most 4 by our assumption on the degree of the numerator and denominator of $h(t)$. Since $\mathfrak{S}_4$ is solvable, there is a normal open subgroup H of $\pi_1(M_{\overline{\mathbb{Q}}})$ such that $H \subseteq \varphi_*(\pi_1(W_{\overline{\mathbb{Q}}}))$ and such that $\pi_1(M_{\overline{\mathbb{Q}}})/H$ is solvable. The group $\Omega(V_\ell)$ is perfect and non-abelian and we have seen that it is a normal subgroup of $\theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}}))$. Therefore, $\theta_\ell(H)$ contains $\Omega(V_\ell)$ since the quotient $\pi_1(M_{\overline{\mathbb{Q}}})/H$ is solvable. This proves the claim since $G^g \supseteq \theta_\ell(H)$.

We will now show that G is a subgroup of $\pm\Omega(V_\ell)$.

Let us first assume that N is odd and hence assumption (A) holds. Let κ be any coset of $\Omega(V_\ell)$ in G. Take $e \in \{0,1\}$ such that $\det(\kappa) = \{(-1)^e\}$. There exists an element $A \in \kappa$ such that $\det(I + (-1)^e A) \neq 0$. We have $\det((-I)^e A) = (-1)^e(-1)^e = 1$ since N is odd. Using equidistribution, there is a prime $p \notin S$ and an element $w \in W(\mathbb{F}_p)$ such that the conjugacy class $\vartheta_\ell(\mathrm{Frob}_w) = \theta_\ell(\mathrm{Frob}_{h(w)})$ of $\mathrm{O}(V_\ell)$ contains A.

By assumption (A), γ is a square modulo ℓ (it is non-zero modulo ℓ since $\ell \nmid 6\mathcal{L}$). Therefore, $\mathrm{sp}((-1)^e A) = \mathrm{sp}((-1)^e\theta_\ell(\mathrm{Frob}_{h(w)}))$ equals

$$2^N q^{-1+\chi} c_{E_{h(w)}} (\mathbb{F}_\ell^\times)^2 = 2q^{-1+\chi} c_{E_{h(w)}} (\mathbb{F}_\ell^\times)^2$$

by parts (c) and (d) of Proposition 3.2. By assumption (A), χ is odd and $2 \cdot c_{E_{h(w)}}$ is a square modulo ℓ. Therefore, $\mathrm{sp}((-1)^e A) = (\mathbb{F}_\ell^\times)^2$.

Since $(-1)^e A$ has trivial determinant and spinor norm, it belongs to $\Omega(V_\ell)$. The coset $\kappa = A\Omega(V_\ell)$ is thus either $\Omega(V_\ell)$ or $-\Omega(V_\ell)$. Therefore, $G \subseteq \pm\Omega(V_\ell)$ since κ was an arbitrary coset of $\Omega(V_\ell)$ in G.

Now suppose that N is even and hence assumption (B) or (C) holds. Since $G \supseteq \Omega(V_\ell)$ and N is even, there is an element $A \in G$ such that $\det(I \pm A) \neq 0$. Using equidistribution, there is a prime $p \notin S$ and an element $w \in W(\mathbb{F}_p)$ such that the conjugacy class $\vartheta_\ell(\mathrm{Frob}_w) = \theta_\ell(\mathrm{Frob}_{h(w)})$ of $\mathrm{O}(V_\ell)$ contains A. By part (e) of Proposition 3.2, we have $\mathrm{disc}(V_\ell) = \gamma(\mathbb{F}_\ell^\times)^2$.

By Proposition 3.2(b), we find that

$$\det(\vartheta_\ell(\mathrm{Frob}_w)) = \det(\theta_\ell(\mathrm{Frob}_{h(w)})) = (-1)^N \varepsilon_{E_{h(w)}} = \varepsilon_{E_{h(w)}}$$

for all sufficiently large primes $p \notin S$ and all $w \in W(\mathbb{F}_p)$. Assumption (B) or (C) then implies that $\det(\vartheta_\ell(\mathrm{Frob}_w)) = 1$ for all large p and all $w \in W(\mathbb{F}_p)$. Using equidistribution, we deduce that G is a subgroup of $\mathrm{SO}(V_\ell)$.

Suppose that γ is not a square modulo ℓ. Then $-I \notin \Omega(V_\ell)$ since $\mathrm{sp}(-I) = \mathrm{disc}(V_\ell) = \gamma(\mathbb{F}_\ell^\times)^2$. Therefore, G is a subgroup of $\mathrm{SO}(V_\ell)$ and $\mathrm{SO}(V_\ell) = \pm\Omega(V_\ell)$.

Now assume that γ is a square modulo ℓ and hence that assumption (C) holds. Let κ be any coset of $\Omega(V_\ell)$ in G. Since $G \subseteq \mathrm{SO}(V_\ell)$, there is an element $A \in \kappa$ such that $\det(I + A) \neq 0$. Using equidistribution, there is a prime $p \notin S$ and an element $w \in W(\mathbb{F}_p)$ such that the conjugacy class $\vartheta_\ell(\mathrm{Frob}_w) = \theta_\ell(\mathrm{Frob}_{h(w)})$ of $\mathrm{O}(V_\ell)$ contains A. By part (d) of Proposition 3.2, $\mathrm{sp}(A)$ equals $2^N q^{-1+\chi} c_{E_{h(w)}} (\mathbb{F}_\ell^\times)^2 = q^{-1+\chi} c_{E_{h(w)}} (\mathbb{F}_\ell^\times)^2$. By assumption (C), χ is odd and $c_{E_{h(w)}}$ is a square modulo ℓ. Therefore, $\mathrm{sp}(A) = (\mathbb{F}_\ell^\times)^2$. So $\kappa = A\Omega(V_\ell)$ is $\Omega(V_\ell)$ and hence $G = \Omega(V_\ell)$ since κ was an arbitrary coset.

We have proved the inclusions $\Omega(V_\ell) \subseteq G^g \subseteq G \subseteq \pm\Omega(V_\ell)$. Let Z be the group $\{I\}$ if $-I \in \Omega(V_\ell)$ and the group $\{\pm I\}$ if $-I \notin \Omega(V_\ell)$. The natural map $\Omega(V_\ell) \to (\pm\Omega(V_\ell))/Z$ is thus an isomorphism. Since $G \subseteq \pm\Omega(V_\ell)$, we can define the homomorphism

$$\psi\colon \pi_1(W) \xrightarrow{\vartheta_\ell} \pm\Omega(V_\ell) \twoheadrightarrow (\pm\Omega(V_\ell))/Z \cong \Omega(V_\ell).$$

We have $\psi(\pi_1(W)) = \psi(\pi_1(W_{\overline{\mathbb{Q}}})) = \Omega(V_\ell)$ since $G^g \supseteq \Omega(V_\ell)$. Therefore, ψ gives rise to a regular extension of $\mathbb{Q}(v)$, the function field of W, that is Galois with Galois group isomorphic to $\Omega(V_\ell)$.

To complete the proof of the theorem, it suffices to show that $\Omega(V_\ell) \cong \Omega(V)$ with V as in the statement of the theorem. The orthogonal spaces V and V_ℓ over $\mathbb{F}_\ell$ have the same dimension N. When N is odd, we indeed have $\Omega(V_\ell) \cong \Omega(V)$; as noted in §1.1, the isomorphism class of these groups depend only on N and ℓ. Now suppose that N is even. We have shown that $\mathrm{disc}(V_\ell) = \gamma \cdot (\mathbb{F}_\ell^\times)^2$. So V and V_ℓ are isomorphic orthogonal spaces over $\mathbb{F}_\ell$ since they have the same dimension and discriminant. Therefore, $\Omega(V_\ell) \cong \Omega(V)$. This completes the proof of the theorem. □

5. Proof of Theorem 1.1(*i*) for $n > 5$

Take any odd integer $N > 5$ and prime $\ell \geq 5$. Note that to match the notation of §4, and much of the paper, we are using N to denote the integer n in the statement of the theorem.

In this section, we use the criterion of §4 with assumption (A) to show that $\Omega_N(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$. The case $N = 5$

requires extra attention and will be discussed in §8. The proof is broken up into four cases depending on the value of N modulo 8.

5.1. $N \equiv 1 \pmod 8$**.** We have $N = 8n+1$ for a unique integer $n \geq 1$. Define the rational function $h(u) = u$ and the polynomial $f(t) = \prod_{i=1}^{4n}(t-(i+1))$. Consider the Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}\cdot(\mathsf{x}-f(t))\cdot(\mathsf{x}-tf(t)) = \mathsf{x}^3-(t+1)f(t)\mathsf{x}^2+tf(t)^2\mathsf{x}; \tag{5.1}$$

it has discriminant $\Delta(t) = 16f(t)^6t^2(t-1)^2$ and the j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $2^8(t^2-t+1)^3t^{-2}(t-1)^{-2}$.

Now take notation as in §4. Take any prime $p \nmid 6\ell$ such that $f(t)$ modulo p is separable and $f(0)f(1) \not\equiv 0 \pmod p$. Take any $w \in W(\mathbb{F}_p)$ with W defined as in §4, i.e., any $w \in \mathbb{F}_p$ for which $\Delta(w) \neq 0$. Let x be any closed point of $\mathbb{P}^1_{\mathbb{F}_p} = \operatorname{Spec}\mathbb{F}_p[t]\cup\{\infty\}$ for which $E_{h(w)}/\mathbb{F}_p(t)$ has bad reduction and let κ_x be the Kodaira symbol of $E_{h(w)}/\mathbb{F}_p(t)$ at x.

- Suppose $x = 0$, 1 or ∞. We have $\kappa_x = \mathrm{I}_2$, so $c_x(E_{h(w)}) = 2$.
- Suppose $x = a$ is a root of $(t-h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. Using that the degree 3 polynomial of x in the Weierstrass equation (5.1) factors into linear terms, Tate's algorithm shows that $c_x(E_{h(w)}) = 4$.

Note that the curve $E_{h(w)}$ has multiplicative reduction at a closed point $x \neq \infty$ and Kodaira symbol I_0^* at more than one closed point $x \neq \infty$.

From the computations above, we find that $N_{E_{h(w)}} = -4+3\cdot 1+(4n+1)\cdot 2 = 8n+1 = N$, $\chi_{E_{h(w)}} = (2+2+2+6(4n+1))/12 = 2n+1$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 1$ and $B_{E_{h(w)}} = 0$. Since this holds for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$, we have $\chi = 2n+1$, $\mathcal{L} = 1$, $\gamma = 1$ and $B = 0$. Observe that N is odd, χ is odd and γ is a square modulo ℓ. We have $6B = 0 \leq 8n+1 = N$.

We have verified all the conditions of §4 and in particular showed that assumption (A) holds. From Theorem 4.1, we deduce that $\Omega(V) \cong \Omega_N(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$ where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N.

5.2. $N \equiv 3 \pmod 8$**.** We have $N = 8n+3$ for a unique integer $n \geq 1$. Now take $h(u) = 3u^2/(3u^2+1)$ and $f(t) = \prod_{i=1}^{4n}(t-h(i))$, together with the Weierstrass equation $\mathsf{y}^2 = \mathsf{x}^3-3tf(t)^2\mathsf{x}+2t^2f(t)^3$ having discriminant $\Delta(t) = -2^63^3f(t)^6t^3(t-1)$. The j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $-1728(t-1)^{-1}$. With notation as before, there are the following cases:

- Suppose $x = \infty$. We have $\kappa_x = \mathrm{II}$, so $c_x(E_{h(w)}) = 1$.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{III}$, so $c_x(E_{h(w)}) = 2$.
- Suppose $x = 1$. We have $\kappa_x = \mathrm{I}_1$, so $c_x(E_{h(w)}) = 1$.
- Suppose $x = a$ is a root of $(t-h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. Tate's algorithm shows that $c_x(E_{h(w)}) = 1+m$ where m is the number of roots of
$$P(\mathsf{x}) := \mathsf{x}^3-3a\mathsf{x}+2a^2$$
in $\mathbb{F}_p$. Using that $a = h(b)$ for some $b \in \mathbb{F}_p$, we find that the discriminant of $P(\mathsf{x})$ is a non-zero square (moreover, it equals $54b^3/(3b^2+1)^2$ squared), so m equals 0 or 3. Therefore, $c_x(E_{h(w)})$ equals 1 or 4.

Proceeding as before, we find that $N_{E_{h(w)}} = -4+2+2+1+(4n+1)\cdot 2 = 8n+3 = N$, $\chi_{E_{h(w)}} = (2+3+1+6(4n+1))/12 = 2n+1$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 1$

and $B_{E_{h(w)}} = 1$, for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$. Again, the conditions of §4 hold, including assumption (A), so Theorem 4.1 implies that $\Omega_N(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.

5.3. $N \equiv 5 \pmod 8$. We have $N = 8n+5$ for a unique integer $n \geq 1$ (recall $N > 5$). Now take $h(u) = (-u^2+3)/(u^2+3)$ and $f(t) = \prod_{i=1}^{4n}(t - h(i))$, together with the Weierstrass equation $\mathsf{y}^2 = \mathsf{x}^3 + 3(t^2-1)^3 f(t)^2\mathsf{x} - 2(t^2-1)^5 f(t)^3$ having discriminant $\Delta(t) = -1728 f(t)^6 t^2 (t-1)^9 (t+1)^9$. The j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $1728t^{-2}$. With notation as before, there are the following cases:

- Suppose $x = \infty$. We have $\kappa_x = \mathrm{II}^*$, so $c_x(E_{h(w)}) = 1$.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_2$, so $c_x(E_{h(w)}) = 2$.
- Suppose $x = 1$ or -1. We have $\kappa_x = \mathrm{III}^*$, so $c_x(E_{h(w)}) = 2$.
- Suppose $x = a$ is a root of $(t - h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. Tate's algorithm shows that $c_x(E_{h(w)}) = 1 + m$ where m is the number of roots of
$$P(\mathsf{x}) := \mathsf{x}^3 + 3(a^2-1)^3\mathsf{x} - 2(a^2-1)^5$$
in $\mathbb{F}_p$. Using that $a = h(b)$ for some $b \in \mathbb{F}_p$, we find that the discriminant of $P(\mathsf{x})$ is a non-zero square (moreover, it equals $2^{10}3^6b^9(b^2-3)/(b^2+3)^{10}$ squared), so m equals 0 or 3. Therefore, $c_x(E_{h(w)})$ equals 1 or 4.

Proceeding as before, we have $N_{E_{h(w)}} = -4+2+1+2+2+(4n+1)\cdot 2 = 8n+5 = N$, $\chi_{E_{h(w)}} = (10+2+9+9+6(4n+1))/12 = 2n+3$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 1$ and $B_{E_{h(w)}} = 2$, for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$. Again, the conditions of §4 hold, including assumption (A), so Theorem 4.1 implies that $\Omega_N(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.

Remark 5.1. Consider the excluded case $N = 5$. For later, note that the conditions of §4 with assumption (A) hold except for two things: The first is that each $E_{h(w)}$ has Kodaira symbol I_0^* at only one closed point $x \neq \infty$ of $\mathbb{P}^1_{\mathbb{F}_p}$. The second is that $6B = 12$ is now greater than $N = 5$.

5.4. $N \equiv 7 \pmod 8$. We have $N = 8n+7$ for a unique integer $n \geq 0$. Now take $h(u) = u$ and $f(t) = \prod_{i=1}^{4n+2}(t - (i+1))$, together with the Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}\cdot(\mathsf{x} + tf(t))\cdot(\mathsf{x} + t^2 f(t)) = \mathsf{x}^3 + t(t+1)f(t)\mathsf{x}^2 + t^3 f(t)^2\mathsf{x} \tag{5.2}$$

having discriminant $\Delta(t) = 16 f(t)^6 t^8 (t-1)^2$. The j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $2^8(t^2-t+1)^3t^{-2}(t-1)^{-2}$. With notation as before, there are the following cases:

- Suppose $x = \infty$. Over $\mathbb{F}_p(t)_x = \mathbb{F}_p(\!(t^{-1})\!)$, the elliptic curve $E_{h(w)}$ is isomorphic to the curve defined by the Weierstrass equation
$$\mathsf{y}^2 = \mathsf{x}(\mathsf{x} + t^{-2})(\mathsf{x} + t^{-1}) = \mathsf{x}^3 + (1 + t^{-1})\cdot t^{-1}\mathsf{x}^2 + t^{-3}\mathsf{x}.$$
We have $\kappa_x = \mathrm{I}_2^*$. Using Tate's algorithm, we find that $c_x(E_{h(w)}) = 4$ (since the quadratic equation arising has vanishing constant term).
- Suppose $x = 0$. Over $\mathbb{F}_p(t)_x$, the elliptic curve $E_{h(w)}$ is isomorphic to the curve defined by the Weierstrass equation
$$\mathsf{y}^2 = \mathsf{x}^3 - h(w)f(0)(t+1)\cdot t\,\mathsf{x}^2 + h(w)^2 f(0)^2\cdot t^3\mathsf{x}.$$
We have $\kappa_x = \mathrm{I}_2^*$. Using Tate's algorithm, we find that $c_x(E_{h(w)}) = 4$ (since the quadratic equation arising has vanishing constant term).

- Suppose $x = 1$. We have $\kappa_x = \mathrm{I}_2$, so $c_x(E_{h(w)}) = 2$.
- Suppose $x = a$ is a root of $(t - h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. We have $c_x(E_{h(w)}) = 4$ since the polynomial of x in (5.2) splits into linear factors.

Proceeding as before, we find that $N_{E_{h(w)}} = -4+2+2+1+(4n+3)\cdot 2 = 8n+7$, $\chi_{E_{h(w)}} = (8+8+2+6(4n+3))/12 = 2n+3$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 1$ and $B_{E_{h(w)}} = 1$, for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$. Again, the conditions of §4 hold, including assumption (A), so Theorem 4.1 implies that $\Omega_N(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$.

6. Proof of Theorem 1.1(ii) and (iii)

Take any even integer $N \geq 6$ and prime $\ell \geq 5$. Note that to match the notation of §4, and much of the paper, we are using N to denote the integer n in the statement of the theorem.

Let V be an orthogonal space of dimension N over $\mathbb{F}_\ell$ satisfying $\operatorname{disc}(V) = (\mathbb{F}_\ell^\times)^2$. We use the criterion of §4 with assumption (C) to show that $\Omega(V)$, and hence $\mathrm{P}\Omega(V)$, occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$. Note that $\mathrm{P}\Omega(V)$ is isomorphic to $\mathrm{P}\Omega_N^+(\ell)$ if $N \equiv 0 \pmod 4$ or $\ell \equiv 1 \pmod 4$ and isomorphic to $\mathrm{P}\Omega_N^-(\ell)$ if $N \equiv 2 \pmod 4$ and $\ell \equiv 3 \pmod 4$.

The proof is broken up into four cases depending on the value of N modulo 8.

6.1. $N \equiv 0 \pmod 8$**.** We have $N = 8n$ for a unique integer $n \geq 1$. Define the rational function $h(u) = 4u^2/(u^2+1)^2$ and the polynomial $f(t) = \prod_{i=1}^{4n-1}(t - h(i+1))$. Consider the Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}^3 - 3(t-1)^3(t-4)f(t)^2\mathsf{x} - 2(t-1)^5(t+8)f(t)^3; \tag{6.1}$$

it has discriminant $\Delta(t) = -2^6 3^6 f(t)^6 t^2 (t-1)^9$ and the j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $-64(t-4)^3 t^{-2}$.

Now take notation as in §4. Take any prime $p \nmid 6\ell$ such that $f(t)$ modulo p is well-defined and separable, and $f(0)f(1) \not\equiv 0 \pmod p$. Take any $w \in W(\mathbb{F}_p)$ with W defined as in §4, i.e., any $w \in \mathbb{F}_p$ for which $w^2 + 1 \neq 0$ and $\Delta(h(w)) \neq 0$. Let x be any closed point of $\mathbb{P}^1_{\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[t] \cup \{\infty\}$ for which $E_{h(w)}/\mathbb{F}_p(t)$ has bad reduction and let κ_x be the Kodaira symbol of $E_{h(w)}/\mathbb{F}_p(t)$ at x.

- Suppose $x = \infty$. We have $\kappa_x = \mathrm{I}_1$ and hence $c_x(E_{h(w)}) = 1$. Over $\mathbb{F}_p(t)_x = \mathbb{F}_p(\!(t^{-1})\!)$, the elliptic curve $E_{h(w)}$ is isomorphic to the curve defined by (6.1) and hence also by $\mathsf{y}^2 = \mathsf{x}^3 - 3(1-t^{-1})(1-4t^{-1})\mathsf{x} - 2(1-t^{-1})^2(1+8t^{-1})$. Reducing to $\mathbb{F}_x$, we have the equation
$$\mathsf{y}^2 = \mathsf{x}^3 - 3\mathsf{x} - 2 = -3(\mathsf{x}+1)^2 + (\mathsf{x}+1)^3.$$
Therefore, the curve $E_{h(w)}$ has split multiplicative reduction at x if and only if -3 is a square in $\mathbb{F}_p$.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_2$ and hence $c_x(E_{h(w)}) = 2$. Reducing the Weierstrass equation for $E_{h(w)}$ over $\mathbb{F}_x$, we have
$$-h(w)\mathsf{y}^2 = \mathsf{x}^3 - 12f(0)^2\mathsf{x} + 16f(0)^3 = 6f(0)(\mathsf{x} - 2f(0))^2 + (\mathsf{x} - 2f(0))^3.$$
So $E_{h(w)}$ has split multiplicative reduction at x if and only if $-6h(w)f(0)$ is a square in $\mathbb{F}_p$. Since $h(u) = (2u/(u^2+1))^2$, we find that $-h(w)f(0) =$

$h(w)\prod_{i=1}^{4n-1} h(i+1)$ is a non-zero square in $\mathbb{F}_p$. So $E_{h(w)}$ has split multiplicative reduction at x if and only if 6 is a square in $\mathbb{F}_p$.

- Suppose $x = 1$. We have $\kappa_x = \mathrm{III}^*$ and hence $c_x(E_{h(w)}) = 2$.
- Suppose $x = a$ is a root of $(t - h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. Tate's algorithm shows that $c_x(E_{h(w)}) = 1 + m$ where m is the number of roots of
$$P(\mathsf{x}) := \mathsf{x}^3 - 3(a-1)^3(a-4)\mathsf{x} - 2(a-1)^5(a+8)$$
in $\mathbb{F}_p$. The polynomial $P(\mathsf{x})$ has root $2(a-1)^2$, and $P(\mathsf{x})/(\mathsf{x} - 2(a-1)^2)$ equals
$$Q(\mathsf{x}) := \mathsf{x}^2 + 2(a-1)^2\mathsf{x} + (a-1)^3(a+8).$$
Using that $a = h(b)$ for some $b \in \mathbb{F}_p$, we find that the discriminant of $Q(\mathsf{x})$ is a square (moreover, it equals $6^2(b-1)^6(b+1)^6/(b^2+1)^6$), so $m = 3$. Therefore, $c_x(E_{h(w)}) = 4$.

Note that the curve $E_{h(w)}$ has multiplicative reduction at a closed point $x \neq \infty$ and Kodaira symbol I_0^* at more than one closed point $x \neq \infty$.

From the computations above, we find that $N_{E_{h(w)}} = -4 + 1 + 2 + 1 + (4n)\cdot 2 = 8n = N$, $\chi_{E_{h(w)}} = (2 + 9 + 1 + 6(4n))/12 = 2n + 1$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 1$ and $B_{E_{h(w)}} = 1$. Since this holds for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$, we thus have $\chi = 2n + 1$, $\mathcal{L} = 1$, $\gamma = 1$ and $B = 1$. Observe that N is even, χ is odd and γ is a square modulo ℓ. We have $6B = 6 \leq 8n = N$.

The above computations show that $c_{E_{h(w)}}$ is a power of 4, and hence a square modulo ℓ, and that
$$\varepsilon_{E_{h(w)}} = \left(\frac{6}{p}\right)\left(\frac{-3}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{-1}{p}\right)^{4n} = 1.$$

We have verified all the conditions of §4 and in particular assumption (C) holds. From Theorem 4.1, we deduce that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$, where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N with $\operatorname{disc}(V) = (\mathbb{F}_\ell^\times)^2$.

6.2. $N \equiv 2 \pmod 8$**.** We have $N = 8n + 2$ for a unique integer $n \geq 1$. Now take $h(u) = -(u^2-1)^2/(4u^2)$ and $f(t) = \prod_{i=1}^{4n}(t - h(i+1))$, together with the Weierstrass equation
$$\mathsf{y}^2 = \mathsf{x}^3 - 3(t-1)(t-4)f(t)^2\mathsf{x} - 2(t-1)^2(t+8)f(t)^3$$
having discriminant $\Delta(t) = -2^6 3^6 f(t)^6 t^2 (t-1)^3$. The j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $-2^6(t-4)^3 t^{-2}$. With notation as before, there are the following cases:

- Suppose $x = \infty$. We have $\kappa_x = \mathrm{I}_1$, so $c_x(E_{h(w)}) = 1$. Over $\mathbb{F}_p(t)_x = \mathbb{F}_p(\!(t^{-1})\!)$, the elliptic curve $E_{h(w)}$ is isomorphic to the curve defined by the Weierstrass equation $\mathsf{y}^2 = \mathsf{x}^3 - 3(1-t^{-1})(1-4t^{-1})\mathsf{x} - 2(1-t^{-1})^2(1+8t^{-1})$. Reducing, we have the equation
$$\mathsf{y}^2 = \mathsf{x}^3 - 3\mathsf{x} - 2 = -3(\mathsf{x}+1)^2 + (\mathsf{x}+1)^3$$
over $\mathbb{F}_x$. The curve $E_{h(w)}$ has split multiplicative reduction at x if and only if -3 is a square in $\mathbb{F}_p$.

- Suppose $x=0$. We have $\kappa_x = \mathrm{I}_2$, so $c_x(E_{h(w)})=2$. Reducing the Weierstrass equation for $E_{h(w)}$ over $\mathbb{F}_x$, we have

$$-h(w)\mathsf{y}^2 = \mathsf{x}^3 - 12f(0)^2\mathsf{x} - 16f(0)^3 = -6f(0)(\mathsf{x}+2f(0))^2 + (\mathsf{x}+2f(0))^3.$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $6h(w)f(0)$ is a square in $\mathbb{F}_p$. Since $-h(u) = ((u^2-1)/(2u))^2$ and $-h(w)f(0) = -h(w)\prod_{i=1}^{4n}(-h(i+1))$, we deduce that $E_{h(w)}$ has split multiplicative reduction at x if and only if -6 is a square in $\mathbb{F}_p$.
- Suppose $x=1$. We have $\kappa_x = \mathrm{III}$, so $c_x(E_{h(w)})=2$.
- Suppose $x=a$ is a root of $(t-h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. Tate's algorithm shows that $c_x(E_{h(w)}) = 1+m$ where m is the number of roots of

$$P(\mathsf{x}) := \mathsf{x}^3 - 3(a-1)(a-4)\mathsf{x} - 2(a-1)^2(a+8)$$

  in $\mathbb{F}_p$. The polynomial $P(\mathsf{x})$ has root $2(a-1)$, and $P(\mathsf{x})/(\mathsf{x}-2(a-1))$ equals

$$Q(\mathsf{x}) := \mathsf{x}^2 + 2(a-1)\mathsf{x} + (a-1)(a+8).$$

  Using that $a=h(b)$ for some $b\in\mathbb{F}_p$, we find that the discriminant of $Q(\mathsf{x})$ is a square (moreover, it equals $3^2(b^2+1)^2/b^2$), so $m=3$. Therefore, $c_x(E_{h(w)})=4$.

Proceeding as before, the following hold for all sufficiently large primes p and all $w\in W(\mathbb{F}_p)$: $N_{E_{h(w)}} = -4+1+2+1+(4n+1)\cdot 2 = 8n+2 = N$, $\chi_{E_{h(w)}} = (2+3+1+6(4n+1))/12 = 2n+1$, $\mathcal{L}_{E_{h(w)}}=1$, $\gamma_{E_{h(w)}}=1$, $B_{E_{h(w)}}=1$, $c_{E_{h(w)}}$ is a power of 4, and

$$\varepsilon_{E_{h(w)}} = \left(\frac{-3}{p}\right)\left(\frac{-6}{p}\right)\left(\frac{-2}{p}\right)\left(\frac{-1}{p}\right)^{4n+1} = 1.$$

Again, the conditions of §4 hold, including assumption (C), so Theorem 4.1 implies that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$, where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N with $\operatorname{disc}(V) = (\mathbb{F}_\ell^\times)^2$.

6.3. $N\equiv 4 \pmod 8$.

We have $N=8n+4$ for a unique integer $n\geq 1$. Now take $h(u)=-3u^2$ and $f(t)=\prod_{i=1}^{4n}(t-h(i))$, together with the Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}^3 - 3(t-1)(t-9)f(t)^2\mathsf{x} - 2(t-1)(t-3)(t-9)f(t)^3$$

having discriminant $\Delta(t) = -2^8 3^3 f(t)^6 t(t-1)^2(t-9)^2$. The j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $-2^4 3^3(t-1)(t-9)t^{-1}$. With notation as before, there are the following cases:

- Suppose $x=\infty$. We have $\kappa_x = \mathrm{I}_1$, so $c_x(E_{h(w)})=1$. Over $\mathbb{F}_p(t)_x = \mathbb{F}_p(\!(t^{-1})\!)$, the elliptic curve $E_{h(w)}$ is isomorphic to the curve defined by the Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}^3 - 3(1-t^{-1})(1-9t^{-1})\mathsf{x} - 2(1-t^{-1})(1-3t^{-1})(1-9t^{-1}).$$

  Reducing, we have the equation $\mathsf{y}^2 = \mathsf{x}^3 - 3\mathsf{x} - 2 = -3(\mathsf{x}+1)^2 + (\mathsf{x}+1)^3$ over $\mathbb{F}_x$. The curve $E_{h(w)}$ has split multiplicative reduction at x if and only if -3 is a square in $\mathbb{F}_p$.

- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_1$, so $c_x(E_{h(w)}) = 1$. Reducing the Weierstrass equation for $E_{h(w)}$ over $\mathbb{F}_x$, we have

$$-h(w)\mathsf{y}^2 = \mathsf{x}^3 - 27f(0)^2\mathsf{x} + 54f(0)^3 = 9f(0)(\mathsf{x} - 3f(0))^2 + (\mathsf{x} - 3f(0))^3.$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $-h(w)f(0)$ is a square in $\mathbb{F}_p$. Since $-h(w)f(0) = 3w^2\prod_{i=1}^{4n}(-3i^2) = 3(3^{2n}w\prod_{i=1}^{4n} i)^2$, we deduce that $E_{h(w)}$ has split multiplicative reduction at x if and only if 3 is a square in $\mathbb{F}_p$.
- Suppose $x = 1$ or 9. We have $\kappa_x = \mathrm{II}$, so $c_x(E_{h(w)}) = 1$.
- Suppose $x = a$ is a root of $(t - h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. Tate's algorithm shows that $c_x(E_{h(w)}) = 1 + m$ where m is the number of roots of

$$P(\mathsf{x}) := \mathsf{x}^3 - 3(a-1)(a-9)\mathsf{x} - 2(a-1)(a-3)(a-9)$$

  in $\mathbb{F}_p$. Using that $a = h(b)$ for some $b \in \mathbb{F}_p$, we find that the discriminant of $P(\mathsf{x})$ is a square (moreover, it equals $2^2 3^4 b(b^2+3)(3b^2+1)$ squared), so m equals 0 or 3. Therefore, $c_x(E_{h(w)})$ equals 1 or 4.

Proceeding as before, the following hold for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$: $N_{E_{h(w)}} = -4 + 1 + 1 + 2 + 2 + (4n+1)\cdot 2 = 8n + 4 = N$, $\chi_{E_{h(w)}} = (1 + 1 + 2 + 2 + 6(4n+1))/12 = 2n + 1$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 1$, $B_{E_{h(w)}} = 2$, $c_{E_{h(w)}}$ is a power of 4, and

$$\varepsilon_{E_{h(w)}} = \Big(\frac{3}{p}\Big)\Big(\frac{-3}{p}\Big)\Big(\frac{-1}{p}\Big)^2\Big(\frac{-1}{p}\Big)^{4n+1} = 1.$$

Again, the conditions of §4 hold, including assumption (C), so Theorem 4.1 implies that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$, where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N with $\operatorname{disc}(V) = (\mathbb{F}_\ell^\times)^2$.

6.4. $N \equiv 6 \pmod 8$**.** We have $N = 8n + 6$ for a unique integer $n \geq 0$. Now take $h(u) = 2u/(u^2+1)$ and $f(t) = \prod_{i=1}^{4n+1}(t - \psi(i+1))$, where $\psi(u) = (u^2+1)/(2u)$, together with the Weierstrass equation

$$\begin{aligned} \mathsf{y}^2 &= (\mathsf{x} - t(t^2-2)f(t))\cdot(\mathsf{x} - t(t^2+1)f(t))\cdot(\mathsf{x} + t(2t^2-1)f(t)) \\ &= \mathsf{x}^3 - 3t^2(t^4 - t^2 + 1)f(t)^2\mathsf{x} + t^3(2t^6 - 3t^4 - 3t^2 + 2)f(t)^3 \end{aligned} \tag{6.2}$$

having discriminant $\Delta(t) = 2^4 3^6 f(t)^6 t^{10}(t-1)^2(t+1)^2$. The j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $2^8(t^4 - t^2 + 1)^3 t^{-4}(t-1)^{-2}(t+1)^{-2}$. With notation as before, there are the following cases:

- Suppose $x = 1$. We have $\kappa_x = \mathrm{I}_2$, so $c_x(E_{h(w)}) = 2$. Reducing the equation to $\mathbb{F}_x$, we have

$$\begin{aligned} (1 - h(w))\mathsf{y}^2 &= (\mathsf{x} + f(1))^2(\mathsf{x} - 2f(1)) \\ &= -3f(1)(\mathsf{x} + f(1))^2 + (\mathsf{x} + f(1))^3. \end{aligned}$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $-3(1 - h(w))f(1)$ is a square in $\mathbb{F}_p^\times$.

- Suppose $x = -1$. We have $\kappa_x = \mathrm{I}_2$, so $c_x(E_{h(w)}) = 2$. Reducing the equation to $\mathbb{F}_x$, we have
$$\begin{aligned}(-1 - h(w))\mathsf{y}^2 &= (\mathsf{x} - f(-1))^2(\mathsf{x} + 2f(-1))\\ &= 3f(-1)(\mathsf{x} - f(-1))^2 + (\mathsf{x} - f(-1))^3.\end{aligned}$$
So $E_{h(w)}$ has split multiplicative reduction at x if and only if $-3(h(w) + 1)f(-1)$ is a square in $\mathbb{F}_p^\times$.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_4^*$. Using that p is odd and $f(0) \neq 0$, we find that $(t - h(w))f(t)$ belongs to $-h(w)f(0) \cdot (\mathbb{F}_p(\!(t)\!)^\times)^2$. Using Tate's algorithm, one can then show that $c_x(E_{h(w)})$ is a power of 2 and equals the Tamagawa number of the elliptic curve
$$\mathsf{y}^2 = \mathsf{x}^3 - 3(t^2 - 1 + t^{-2})\mathsf{x} + (2t^3 - 3t - 3t^{-1} + 2t^{-3})$$
over $\mathbb{F}_p(\!(t)\!)$.
- Suppose $x = \infty$. We have $\kappa_x = \mathrm{I}_4^*$. Using that p is odd and $f(t)$ is monic of odd degree, we find that $(t - h(w))f(t)$ belongs to $(\mathbb{F}_p(\!(t^{-1})\!)^\times)^2$. So $c_x(E_{h(w)})$ equals the Tamagawa number of the elliptic curve
$$\mathsf{y}^2 = \mathsf{x}^3 - 3(t^2 - 1 + t^{-2})\mathsf{x} + (2t^3 - 3t - 3t^{-1} + 2t^{-3})$$
over $\mathbb{F}_p(\!(t^{-1})\!)$.
- Suppose $x = a$ is a root of $(t - h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$. We have $c_x(E_{h(w)}) = 4$ since the polynomial of x in (6.2) splits into linear factors.

Proceeding as before, the following holds for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$: $N_{E_{h(w)}} = -4 + 2 + 2 + 1 + 1 + (4n + 2) \cdot 2 = 8n + 6 = N$, $\chi_{E_{h(w)}} = (10 + 10 + 2 + 2 + 6(4n + 2))/12 = 2n + 3$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 1$ and $B_{E_{h(w)}} = 1$.

Note that the Tamagawa numbers described in the cases $x = 0$ and $x = \infty$ are equal, since the given curves are isomorphic with respect to the isomorphism $\mathbb{F}_p(\!(t)\!) \xrightarrow{\sim} \mathbb{F}_p(\!(t^{-1})\!)$, $\alpha(t) \mapsto \alpha(t^{-1})$ of base fields. Therefore, the product $\prod_x c_x(E_{h(w)})$ is a power of 4 and is thus a square modulo ℓ. We also have
$$\begin{aligned}\varepsilon_{E_{h(w)}} &= \Big(\frac{-3(1 - h(w))f(1)}{p}\Big)\Big(\frac{-3(1 + h(w))f(-1)}{p}\Big)\Big(\frac{-1}{p}\Big)^2\Big(\frac{-1}{p}\Big)^{4n+2}\\ &= \Big(\frac{1 - h(w)^2}{p}\Big)\prod_{i=1}^{4n+1}\Big(\frac{(1 - \psi(i + 1))(-1 - \psi(i + 1))}{p}\Big) = 1,\end{aligned}$$
where the last equality uses that $1 - h(u)^2 = (u^2 - 1)^2/(u^2 + 1)^2$ and $(1 - \psi(u))(-1 - \psi(u)) = (u^2 - 1)^2/(2u)^2$.

Again, the conditions of §4 hold, including assumption (C), so Theorem 4.1 implies that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$, where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N with $\operatorname{disc}(V) = (\mathbb{F}_\ell^\times)^2$.

7. Proof of Theorem 1.1(iv)

Take any even integer $N \geq 6$. Note that to match the notation of §4, and much of the paper, we are using N to denote the integer n from the statement of the theorem. Instead, we will let $n \geq 2$ be the unique integer for which $N = 2n + 2$.

Take any prime $\ell \geq 5$ such that 2, 3, 5 or 7 is a non-square modulo ℓ. Let V be an orthogonal space of dimension N over $\mathbb{F}_\ell$ satisfying $\operatorname{disc}(V) \neq (\mathbb{F}_\ell^\times)^2$. We will use the criterion of §4 with assumption (B) to show that $\Omega(V)$, and hence $\mathrm{P}\Omega(V)$, occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$. The proof is broken up into four cases.

7.1. **Case 1.** *Suppose that* 2 *is not a square modulo* ℓ.

Define the rational function $h(u) = 1/(2u^2+1)$ and the polynomial $f(t) = \prod_{i=1}^{n-1}(t-g(i))$ where $g(u) = 1/(u^2+1)$. Consider the Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}^3 + 3(t-1)(t-4)(3t-4)f(t)^2\mathsf{x} - 4(t-1)^2(9t^2-32t+32)f(t)^3$$

it has discriminant $\Delta(t) = -2^6 3^6 f(t)^6 t^4 (t-1)^3 (t-2)^2$ and the j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $1728(t-4)^3(t-4/3)^3(t-2)^{-2}t^{-4}$.

Now take notation as in §4. Take any prime $p \nmid 6\ell$ such that $f(t)$ modulo p is well-defined and separable, and $f(0)f(1)f(2) \not\equiv 0 \pmod{p}$. Take any $w \in W(\mathbb{F}_p)$ with with W defined as in §4, i.e., any $w \in \mathbb{F}_p$ for which $2w^2+1 \neq 0$ and $\Delta(h(w)) \neq 0$. Let x be any closed point of $\mathbb{P}^1_{\mathbb{F}_p} = \operatorname{Spec} \mathbb{F}_p[t] \cup \{\infty\}$ for which $E_{h(w)}/\mathbb{F}_p(t)$ has bad reduction and let κ_x be the Kodaira symbol of $E_{h(w)}/\mathbb{F}_p(t)$ at x.

- Suppose $x = \infty$. The symbol κ_x is either III or III*.
- Suppose $x = 1$. We have $\kappa_x = \mathrm{III}$.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_4$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have

$$-h(w)\mathsf{y}^2 = \mathsf{x}^3 - 48f(0)^2\mathsf{x} - 128f(0)^3 = -12f(0)(\mathsf{x}+4f(0))^2 + (\mathsf{x}+4f(0))^3.$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $3h(w)f(0)$ is a square in $\mathbb{F}_p$.
- Suppose $x = 2$. We have $\kappa_x = \mathrm{I}_2$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have

$$(1-h(w))\mathsf{y}^2 = \mathsf{x}^3 - 12f(1)^2\mathsf{x} - 16f(1)^3 = -6f(1)(\mathsf{x}+2f(1))^2 + (\mathsf{x}+2f(1))^3.$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $-6(1-h(w))f(1)$ is a square in $\mathbb{F}_p$.
- Suppose $x = a$ is an irreducible factor of $(t-h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$.

Note that the curve $E_{h(w)}$ has multiplicative reduction at a closed point $x \neq \infty$ and Kodaira symbol I_0^* at more than one closed point $x \neq \infty$.

From the computations above, we find that $N_{E_{h(w)}} = -4+2+2+1+1+n\cdot 2 = N$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 2$ and $B_{E_{h(w)}} = 1$. Since this holds for all large primes p and all $w \in W(\mathbb{F}_p)$, we thus have $\mathcal{L} = 1$, $\gamma = 2$ and $B = 1$. By our assumption on ℓ, $\gamma = 2$ is a non-square modulo ℓ. We have $6B = 6 \leq 2n+2 = N$.

From our computations, we have

$$\begin{aligned}\varepsilon(E_{h(w)}) &= \Big(\frac{-2}{p}\Big)^2\Big(\frac{3h(w)f(0)}{p}\Big)\Big(\frac{-6(1-h(w))f(1)}{p}\Big)\Big(\frac{-1}{p}\Big)^n \\ &= \Big(\frac{2h(w)(1-h(w))}{p}\Big)\prod_{i=1}^{n-1}\Big(\frac{g(i)(1-g(i))}{p}\Big) = 1,\end{aligned}$$

where the last equality uses that $2h(u)(1-h(u)) = (2u)^2/(2u^2+1)^2$ and $g(u)(1-g(u)) = u^2/(u^2+1)^2$.

We have verified all the conditions of §4 and in particular that assumption (B) holds. From Theorem 4.1, we deduce that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$ where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N and $\operatorname{disc}(V) \neq (\mathbb{F}_\ell^\times)^2$.

7.2. **Case 2.** *Suppose that* 3 *is not a square modulo* ℓ *and that* 2 *is a square modulo* ℓ.

Now take $h(u) = 1/(2u^2+1)$ and $f(t) = \prod_{i=1}^{n-1}(t-g(i))$ where $g(u) = 1/(u^2+1)$. Consider the Weierstrass equation

$$\begin{aligned}\mathsf{y}^2 = \mathsf{x}^3 &- 3(28t-1)(147t^2+112t-16)f(t)^2\mathsf{x}\\ &-2(28t-1)(21609t^3-3430t^2+1568t-64)f(t)^3;\end{aligned}$$

it has discriminant $\Delta(t) = 2^{12}3^6 7^9 f(t)^6 t^4 (t-1)^3 (t-1/28)^2$ and the j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $2^6 7^{-6}(t-1/28)(147t^2+112t-16)^3 t^{-4}(t-1)^{-3}$.

With notation as before, there are the following cases:

- Suppose $x = \infty$. The symbol κ_x is III or III*.
- Suppose $x = 1/28$. We have $\kappa_x = \mathrm{II}$.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_4$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have

$$-h(w)\mathsf{y}^2 = \mathsf{x}^3 - 48f(0)^2\mathsf{x} - 128f(0)^3 = -12f(0)(\mathsf{x}+4f(0))^2 + (\mathsf{x}+4f(0))^3.$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $3h(w)f(0)$ is a square in $\mathbb{F}_p$.
- Suppose $x = 1$. We have $\kappa_x = \mathrm{I}_3$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have

$$\begin{aligned}(1-h(w))\mathsf{y}^2 &= \mathsf{x}^3 - 19683f(1)^2\mathsf{x} - 1062882f(1)^3\\ &= -243f(1)(\mathsf{x}+81f(1))^2 + (\mathsf{x}+81f(1))^3.\end{aligned}$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $-3(1-h(w))f(1)$ is a square in $\mathbb{F}_p$.
- Suppose $x = a$ is a root of $(t-h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$.

Proceeding as before, the following holds for all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$: $N_{E_{h(w)}} = -4+2+2+1+1+n\cdot 2 = N$, $\mathcal{L}_{E_{h(w)}} = 1$, $\gamma_{E_{h(w)}} = 6$ and $B_{E_{h(w)}} = 1$. We also have

$$\begin{aligned}\varepsilon_{E_{h(w)}} &= \Big(\frac{-1}{p}\Big)\Big(\frac{-2}{p}\Big)\Big(\frac{3h(w)f(0)}{p}\Big)\Big(\frac{-3(1-h(w))f(1)}{p}\Big)\Big(\frac{-1}{p}\Big)^n\\ &= \Big(\frac{2h(w)(1-h(w))}{p}\Big)\prod_{i=1}^{n-1}\Big(\frac{g(i)(1-g(i))}{p}\Big) = 1,\end{aligned}$$

where the last equality uses that $2h(u)(1-h(u)) = (2u)^2/(2u^2+1)^2$ and $g(u)(1-g(u)) = u^2/(u^2+1)^2$.

We can verify that all the conditions of §4, and in particular assumption (B), hold. By our assumptions on ℓ, the integer $\gamma = 6$ is a non-square modulo ℓ. From Theorem 4.1, we deduce that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$ where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N and $\operatorname{disc}(V) \neq (\mathbb{F}_\ell^\times)^2$.

7.3. **Case 3.** *Suppose that* 5 *is not a square modulo* ℓ *and that* 2 *and* 3 *are squares modulo* ℓ.

Now take $h(u) = 15/(-u^2+15)$ if n is even and $h(u) = 5/(-u^2+5)$ if n is odd. Define the polynomial $f(t) = \prod_{i=1}^{n-1}(t - g(i))$ where $g(u) = 1/(u^2+1)$. Consider the Weierstrass equation

$$\begin{aligned}\mathsf{y}^2 = \mathsf{x}^3 &+ 3(135t^2 + 96t - 256)f(t)^2\mathsf{x}\\ &-2(486t^4 + 621t^3 - 3024t^2 - 2304t + 4096)f(t)^3;\end{aligned}$$

it has discriminant $\Delta(t) = -2^8 3^{13} f(t)^6 t^5 (t-1)(t+16/9)^2$ and the j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $2^4 3^2 5^3 (t+16/9)(t-16/15)^3 t^{-5}(t-1)^{-1}$.

With notation as before, there are the following cases:

- Suppose $x = \infty$. The symbol κ_x is IV or II* when n is even or odd, respectively.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_5$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have
$$-h(w)\mathsf{y}^2 = \mathsf{x}^3 - 768f(0)^2\mathsf{x} - 8192f(0)^3 = -48f(0)(\mathsf{x}+16f(0))^2 + (\mathsf{x}+16f(0))^3.$$
So $E_{h(w)}$ has split multiplicative reduction at x if and only if $3h(w)f(0)$ is a square in $\mathbb{F}_p$.
- Suppose $x = 1$. We have $\kappa_x = \mathrm{I}_1$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have
$$(1-h(w))\mathsf{y}^2 = \mathsf{x}^3 - 75f(1)^2\mathsf{x} + 250f(1)^3 = 15f(1)(\mathsf{x}-5f(1))^2 + (\mathsf{x}-5f(1))^3.$$
So $E_{h(w)}$ has split multiplicative reduction at x if and only if $15(1-h(w))f(1)$ is a square in $\mathbb{F}_p$.
- Suppose $x = -16/9$. We have $\kappa_x = \mathrm{II}$.
- Suppose $x = a$ is a root of $(t - h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$.

Proceeding as before, the following hold for all sufficiently large primes p and $w \in W(\mathbb{F}_p)$: $N_{E_{h(w)}} = -4+2+2+1+1+n\cdot 2 = N$, $\mathcal{L}_{E_{h(w)}} = 5$ and $B_{E_{h(w)}} = 1$. Also $\gamma_{E_{h(w)}}$ is equal to 15 or 5 if n is even or odd, respectively. If n is even, then

$$\begin{aligned}\varepsilon_{E_{h(w)}} &= \Big(\frac{-3}{p}\Big)\Big(\frac{3h(w)f(0)}{p}\Big)\Big(\frac{15(1-h(w))f(1)}{p}\Big)\Big(\frac{-1}{p}\Big)\Big(\frac{-1}{p}\Big)^n\\ &= \Big(\frac{-15h(w)(1-h(w))}{p}\Big)\prod_{i=1}^{n-1}\Big(\frac{g(i)(1-g(i))}{p}\Big) = 1,\end{aligned}$$

where the last equality uses that $-15h(u)(1-h(u)) = 15^2u^2/(u^2-15)^2$ and $g(u)(1-g(u)) = u^2/(u^2+1)^2$. If n is odd, then

$$\begin{aligned}\varepsilon_{E_{h(w)}} &= \Big(\frac{-1}{p}\Big)\Big(\frac{3h(w)f(0)}{p}\Big)\Big(\frac{15(1-h(w))f(1)}{p}\Big)\Big(\frac{-1}{p}\Big)\Big(\frac{-1}{p}\Big)^n\\ &= \Big(\frac{-5h(w)(1-h(w))}{p}\Big)\prod_{i=1}^{n-1}\Big(\frac{g(i)(1-g(i))}{p}\Big) = 1,\end{aligned}$$

where the last equality uses that $-5h(u)(1-h(u)) = 5^2u^2/(u^2-5)^2$ and $g(u)(1-g(u)) = u^2/(u^2+1)^2$.

We can verify that all the conditions of §4, and in particular assumption (B), hold. By our assumptions on ℓ, the integer $\gamma \in \{5, 15\}$ is a non-square modulo ℓ. From Theorem 4.1, we deduce that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$ where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N and $\operatorname{disc}(V) \neq (\mathbb{F}_\ell^\times)^2$.

7.4. **Case 4.** *Suppose that* 7 *is not a square modulo* ℓ *and that* 2, 3 *and* 5 *are squares modulo* ℓ.

Now take $h(u) = 63/4 \cdot (u^2-14)^{-1}$ if n is even and $h(u) = 189/4 \cdot (u^2-42)^{-1}$ if n is odd. Define the polynomial $f(t) = \prod_{i=1}^{n-1}(t-g(i))$ where $g(u) = -9/8 \cdot (u^2+1)^{-1}$. Consider the Weierstrass equation

$$\begin{aligned}\mathsf{y}^2 = \mathsf{x}^3 &- 12(9t+4)^2(14t^3+42t^2+36t+9)f(t)^2\mathsf{x}\\ &-24(9t+4)^3(8t^5+87t^4+222t^3+234t^2+108t+18)f(t)^3;\end{aligned}$$

it has discriminant $\Delta(t) = -2^{10}3^3t^7(8t+9)^2(9t+4)^7$ and the j-invariant of the corresponding elliptic curve over $\mathbb{Q}(t)$ is $-2^83^3(14t^3+42t^2+36t+9)^3t^{-7}(8t+9)^{-2}(9t+4)^{-1}$.

With notation as before, there are the following cases:

- Suppose $x = \infty$. The symbol κ_x is II or IV* when n is even or odd, respectively.
- Suppose $x = -4/9$. We have $\kappa = \mathrm{I}_1^*$.
- Suppose $x = 0$. We have $\kappa_x = \mathrm{I}_7$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have

$$-h(w)\mathsf{y}^2 = \mathsf{x}^3 - 1728f(0)^2\mathsf{x} - 27648f(0)^3 = -72f(0)(\mathsf{x}+24f(0))^2 + (\mathsf{x}+24f(0))^3.$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $2h(w)f(0)$ is a square in $\mathbb{F}_p$.
- Suppose $x = -9/8$. We have $\kappa = \mathrm{I}_2$. Reducing the Weierstrass equation for $E_{h(w)}$ to an equation over $\mathbb{F}_x$, we have

$$\begin{aligned}&(-9/8-h(w))\mathsf{y}^2\\ &= \mathsf{x}^3 - 3176523/4096 \cdot f(-9/8)^2\mathsf{x} + 1089547389/131072 \cdot f(-9/8)^3\\ &= 3087/64 f(-9/8)(\mathsf{x} - 1029/64 \cdot f(-9/8))^2 + (\mathsf{x} - 1029/64 \cdot f(-9/8))^3.\end{aligned}$$

  So $E_{h(w)}$ has split multiplicative reduction at x if and only if $7(-9/8 - h(w))f(-9/8)$ is a square in $\mathbb{F}_p$.
- Suppose $x = a$ is a root of $(t-h(w))f(t) \bmod p \in \mathbb{F}_p[t]$. We have $\kappa_x = \mathrm{I}_0^*$.

Proceeding as before, the following hold for all sufficiently large primes p and $w \in W(\mathbb{F}_p)$: $N_{E_{h(w)}} = -4+2+2+1+1+n\cdot 2 = N$, $\mathcal{L}_{E_{h(w)}} = 7$ and $B_{E_{h(w)}} = 1$. Also $\gamma_{E_{h(w)}}$ is equal to $2\cdot 7$ or $6 \cdot 7$ if n is even or odd, respectively. If n is even, then

$$\begin{aligned}\varepsilon_{E_{h(w)}} &= \Big(\frac{-1}{p}\Big)^2\Big(\frac{2h(w)f(0)}{p}\Big)\Big(\frac{7(-9/8-h(w))f(-9/8)}{p}\Big)\Big(\frac{-1}{p}\Big)^n\\ &= \Big(\frac{14h(w)(9/8+h(w))}{p}\Big)\prod_{i=1}^{n-1}\Big(\frac{g(i)(-9/8-g(i))}{p}\Big) = 1,\end{aligned}$$

where the last equality uses that $14h(u)(9/8+h(u)) = 3^47^24^{-2}u^2(u^2-14)^{-2}$ and $g(u)(-9/8-g(u)) = 9^28^{-2}u^2(u^2+1)^{-2}$.

We can verify that all the conditions of §4, and in particular assumption (B), hold. By our assumptions on ℓ, the integer $\gamma \in \{2\cdot 7, 6\cdot 7\}$ is a non-square modulo ℓ. From Theorem 4.1, we deduce that $\Omega(V)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$ where V is an orthogonal space over $\mathbb{F}_\ell$ of dimension N and $\operatorname{disc}(V) \neq (\mathbb{F}_\ell^\times)^2$.

8. Proof of Theorem 1.1 for $n = 5$

We now prove Theorem 1.1(i) in the special case $n = 5$. This will conclude our proof of Theorem 1.1 since the other cases have already been proved in §5–7.

Fix a prime $\ell \geq 5$. Define the set $S = \{2, 3, \ell\}$ and the ring $R = \mathbb{Z}[S^{-1}]$. We use the construction of §3 with the Weierstrass equation

$$\mathsf{y}^2 = \mathsf{x}^3 + 3(t^2-1)^3\mathsf{x} - 2(t^2-1)^5$$

being used for (3.1); its discriminant is $\Delta(t) = -2^6 3^3 t^2 (t-1)^9 (t+1)^9$. Define the R-scheme $M = \operatorname{Spec} R[u, \Delta(u)^{-1}]$.

Take any $m \in M(k)$, where k is a finite field whose characteristic is not in S. Let E_m be the elliptic curve over $k(t)$ defined by the Weierstrass equation

$$(t-m)\mathsf{y}^2 = \mathsf{x}^3 + 3(t^2-1)^3\mathsf{x} - 2(t^2-1)^5.$$

The Kodaira symbol of E_m at $t = 0$, 1, -1 and m is I_2, III^*, III^* and I_0^*, respectively. The Kodaira symbol of E_m at ∞ is II^*. Therefore, Lemma 3.1 holds (without increasing S) and we have $\Phi = \{\mathrm{I}_2, \mathrm{III}^*, \mathrm{III}^*, \mathrm{I}_0^*, \mathrm{II}^*\}$, $N = 5$, $\chi = 3$, $\mathcal{L} = 1$, $\gamma = 1$ and $B = 2$. In particular, $\ell \nmid 6\mathcal{L}$.

By Proposition 3.2 (an examination of the proof shows that one does not need to increase S), there is an orthogonal space V_ℓ of dimension 5 over $\mathbb{F}_\ell$ and a continuous representation

$$\theta_\ell \colon \pi_1(M) \to \mathrm{O}(V_\ell)$$

such that $\det(I - \theta_\ell(\mathrm{Frob}_m)T) \equiv L(T/q, E_m) \pmod{\ell}$ for any $m \in M(k)$, where k is any finite field of order q whose characteristic is not in S.

Take $h(u) = (-u^2+3)/(u^2+3)$. As noted in Remark 5.1, all the conditions of the criterion of §4 hold *except* for the following two:

- For all sufficiently large primes p and all $w \in W(\mathbb{F}_p)$, $E_{h(w)}$ has Kodaira symbol I_0^* at more that one closed point of $\mathbb{A}^1_{\mathbb{F}_p}$.
- $6B \leq N$.

In the proof of Theorem 4.1, these two conditions are only used to prove that $\theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}})) \supseteq \Omega(V_\ell)$. So to prove that $\Omega_5(\ell)$ occurs as the Galois group of a regular extension of $\mathbb{Q}(t)$, and therefore to complete the proof of Theorem 1.1(i) for $n = 5$, it suffices to prove Lemma 8.1.

Lemma 8.1. *The group $\theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}}))$ contains $\Omega(V_\ell)$ and is not a subgroup of $\mathrm{SO}(V_\ell)$.*

We will give a proof of Lemma 8.1 in §8.1. To rule out some of the possible small images of θ_ℓ, we will use the following computational result.

Lemma 8.2. *There is an element $g \in \theta_\ell(\pi_1(M))$ such $g^e \neq I$ holds for all $e \in \{16, 20, 24, 28, 36\}$.*

Proof. First suppose that $\ell \neq 5$. Take $m := 2$ in $M(\mathbb{F}_5)$; we have an elliptic curve E_2 defined over $\mathbb{F}_5(t)$. One can compute that

$$L(T/5, E_2) = -T^5 + 2/5 \cdot T^4 - 1/25 \cdot T^3 + 1/25 \cdot T^2 - 2/5 \cdot T + 1.$$

One approach is to use the power series definition to compute the terms up to degree 5 (less terms are required if you use the functional equation); we have verified this L-function with Magma's function LFunction [BCP97]. Since $5 \notin S$, we have $\det(I - \theta_\ell(\mathrm{Frob}_m)T) \equiv L(T/5, E_2) \pmod{\ell}$. Let $A \in \mathrm{GL}_5(\mathbb{Z}[5^{-1}])$ be the companion matrix for the monic polynomial $-L(T/5, E_2)$. The matrix A modulo ℓ in $\mathrm{GL}_2(\mathbb{F}_\ell)$ has the same characteristic polynomial as $-\theta_\ell(\mathrm{Frob}_m)$.

Take any $e \in \{16, 20, 24, 28, 36\}$ and suppose that $\theta_\ell(\mathrm{Frob}_m)^e = I$. Then the characteristic polynomial of A^e modulo ℓ is $(T-1)^5$. In particular, all the coefficients of the polynomial $\det(TI - A^e) - (T-1)^5 \in \mathbb{Z}[1/5]$ are divisible by ℓ. An easy computer computation shows that this only happens when $\ell = 17$ and $e = 36$ (we are using that $\ell > 5$). This shows that the lemma holds with $g = \theta_\ell(\mathrm{Frob}_m)$ when $\ell \notin \{5, 17\}$.

A similar computation starting with $m = 3$ in $M(\mathbb{F}_7)$ can be used to prove the lemma for the excluded primes $\ell \in \{5, 17\}$. Similarly, we take $A \in \mathrm{GL}_5(\mathbb{Z}[7^{-1}])$ to be the companion matrix of

$$L(T/7, E_3) = 1 - 33/49 \cdot T^3 - 33/49 \cdot T^2 + T^5;$$

you do not need to change the sign since the polynomial is monic. □

8.1. **Proof of Lemma 8.1.** Define the group $G := \theta_\ell(\pi_1(M))$ and the subgroup $G^g := \theta_\ell(\pi_1(M_{\overline{\mathbb{Q}}}))$.

Using the work of Hall, as outlined in §3.4, we find that the group G^g contains acts irreducibly on V_ℓ (by Lemma 3.5) and contains a reflection (by Lemma 3.6(ii)); see Remark 3.7.

Let $\mathcal{R}$ be the group generated by all the reflections in G^g; it is a normal subgroup of both G^g and G. The group $\mathcal{R}$ is non-trivial since G^g contains a reflection.

Lemma 8.3. *Let W be an irreducible $\mathcal{R}$-submodule of V_ℓ and let H be the subgroup of G that stabilizes W. The subspaces $\{gW\}_{g \in G/H}$ are pairwise orthogonal and we have $V_\ell = \oplus_{g \in G/H}\, gW$.*

Proof. The proof of Lemma 3.2 of [Hal08] carries over verbatim (in the lemma of loc. cit. the role of G is played by G^g). Note that the subspace gW is a $\mathcal{R}$-module for all $g \in G$ since $\mathcal{R}$ is a normal subgroup of G. □

Lemma 8.4. *The group $\mathcal{R}$ acts irreducibly on V_ℓ.*

Proof. Suppose that V_ℓ is not an irreducible $\mathcal{R}$-module and hence there is a proper irreducible $\mathcal{R}$-submodule W of V_ℓ. By Lemma 8.3, we have $V_\ell = \oplus_{g \in G/H}\, gW$, where H is the subgroup of G that stabilizes W. The vector space V_ℓ has dimension $N = 5$, so $5 = [G : H] \dim_{\mathbb{F}_\ell} W$. Since W is a proper subspace of V_ℓ, we deduce that W, and hence all the gW, have dimension 1 over $\mathbb{F}_\ell$. We thus have an orthogonal sum $V_\ell = \oplus_{i=1}^5 W_i$ with the group G permuting the subspaces W_i.

Take any $g \in G$. Since g permutes the spaces $W_1, \ldots, W_5$, there is an integer $e \in \{4, 5, 6\}$ such that g^e stabilizes each W_i. The automorphism $g^e \in \mathrm{O}(V_\ell)$ acts on W_i and preserves the induced pairing on it. We have $\mathrm{O}(W_i) = \{\pm 1\}$ since W_i has dimension 1, so g^{2e} acts trivially on each W_i. Therefore, for any $g \in G$ we have $g^e = I$ for some $e \in \{8, 10, 12\}$. However, this contradicts Lemma 8.2. Therefore, V_ℓ is an irreducible $\mathcal{R}$-module. □

Since $\mathcal{R}$ is generated by reflections and since V_ℓ is an irreducible $\mathcal{R}$-module by Lemma 8.4, we may use the classification of irreducible reflection groups as described by Zalesskiĭ and Serežkin in [ZS80].

Assume that $\Omega(V_\ell)$ is not a subgroup of $\mathcal{R}$. The classification in [ZS80] shows that $\mathcal{R}$ can be obtained by the reduction modulo ℓ of a finite irreducible reflection group of degree 5 in characteristic 0 and that the action of $\mathcal{R}$ on V_ℓ is absolutely irreducible.

From Lemma 3.7 of [Hal08] and the classification in [ZS80], we find that $\mathcal{R}$ is conjugate in $\mathrm{GL}(V_\ell) \cong \mathrm{GL}_5(\mathbb{F}_\ell)$ to one of the groups denoted in [ZS80] by $G_\ell(2,2,5)$, $G_\ell(2,1,5)$, $W_\ell(A_5)$ or $W_\ell(K_5)$.

- The group $G_\ell(2,2,5)$ is the subgroup of $\mathrm{GL}_5(\mathbb{F}_\ell)$ generated by the permutation matrices and the diagonal matrix whose diagonal is $(-1,-1,1,1,1)$; it is isomorphic to the Weyl group of $W(D_5)$.
- The group $G_\ell(2,1,5)$ is the subgroup of $\mathrm{GL}_5(\mathbb{F}_\ell)$ generated by $G_\ell(2,2,5)$ and the matrix $-I$; it is isomorphic to the Weyl group of $W(C_5)$.
- The group $W_\ell(A_5)$ is isomorphic to the symmetric group $\mathfrak{S}_6$ when $\ell \neq 7$.
- The group $W_\ell(A_5)$ is isomorphic to the symmetric group $\mathfrak{S}_7$ when $\ell = 7$.
- The group $W_\ell(K_5)$ is isomorphic to $\{\pm 1\} \times \Omega_5(3)$.

A group theory computation shows that for any of the possibilities for $\mathcal{R}$ given above, the outer automorphism group $\mathrm{Out}(G)$ of $\mathcal{R}$ has cardinality at most 2. One can also verify that for any $r \in \mathcal{R}$, there is an integer $e \in \{8,10,12,14,18\}$ such $r^e = I$.

Let $\mathcal{N}$ be the normalizer of $\mathcal{R}$ in $\mathrm{O}(V_\ell)$. Take any $g \in \mathcal{N}$; conjugation by g defines an automorphism of $\mathcal{R}$. Since $\#\,\mathrm{Out}(\mathcal{R}) \leq 2$, there is an $r \in \mathcal{R}$ such that $g^2 r^{-1}$ commutes with $\mathcal{R}$. Since V_ℓ is an absolutely irreducible $\mathcal{R}$-module, $g^2 r^{-1}$ must be a scalar matrix. Therefore, $g^2 = \pm r$ since the only scalar matrices in $\mathrm{O}(V_\ell)$ are I and $-I$. So $g^{2e} = I$ for some $e \in \{8,10,12,14,18\}$. We have $G \subseteq \mathcal{N}$ since $\mathcal{R}$ is a normal subgroup of G. So for each $g \in G$, we have $g^e = I$ for some $e \in \{16,20,24,28,36\}$. However, this contradicts Lemma 8.2.

Therefore, $\mathcal{R}$ contains $\Omega(V_\ell)$. We have $\mathcal{R} \not\subseteq \mathrm{SO}(V_\ell)$ since reflections have determinant -1. Lemma 8.1 follows since $G^g \supseteq \mathcal{R}$ (and this also concludes the proof of Theorem 1.1 in the case $n = 5$).

Acknowledgments

Numerical experiments and computations were done using `Magma` [BCP97]. Thanks to Brian Conrad and Stefan Patrikis for comments and corrections.

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, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 21, Springer-Verlag, Berlin, 1990, DOI 10.1007/978-3-642-51438-8. MR1045822

[CCH05] B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), no. 2, 684–731, DOI 10.1016/j.aim.2005.06.013. MR2183392

[CCN$^+$85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, $\mathbb{ATLAS}$ *of finite groups*, Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups; With computational assistance from J. G. Thackray. MR827219

[Con14] Brian Conrad, *Reductive group schemes* (English, with English and French summaries), Autour des schémas en groupes. Vol. I, Panor. Synthèses, vol. 42/43, Soc. Math. France, Paris, 2014, pp. 93–444. MR3362641

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques* (French), Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Lecture Notes in Math., Vol. 349, Springer, Berlin, 1973, pp. 143–316. MR0337993

[DV00] Luis Dieulefait and Núria Vila, *Projective linear groups as Galois groups over* $\mathbf{Q}$ *via modular representations*, J. Symbolic Comput. **30** (2000), no. 6, 799–810, DOI 10.1006/jsco.1999.0383. Algorithmic methods in Galois theory. MR1800679

[DW06] Michael Dettweiler and Stefan Wewers, *Variation of local systems and parabolic cohomology*, Israel J. Math. **156** (2006), 157–185, DOI 10.1007/BF02773830. MR2282374

[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), Cambridge Univ. Press, Cambridge, 1985, pp. 323–326. MR817266

[GM14] Robert Guralnick and Gunter Malle, *Rational rigidity for* $E_8(p)$, Compos. Math. **150** (2014), no. 10, 1679–1702, DOI 10.1112/S0010437X14007271. MR3269463

[Gro11] Benedict H. Gross, *Lectures on the conjecture of Birch and Swinnerton-Dyer*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 169–209, DOI 10.1090/pcms/018/08. MR2882691

[Häf92] Frank Häfner, *Einige orthogonale und symplektische Gruppen als Galoisgruppen über* $\mathbf{Q}$ (German), Math. Ann. **292** (1992), no. 4, 587–618, DOI 10.1007/BF01444638. MR1157316

[Hal08] Chris Hall, *Big symplectic or orthogonal monodromy modulo* l, Duke Math. J. **141** (2008), no. 1, 179–203, DOI 10.1215/S0012-7094-08-14115-8. MR2372151

[Her91] Stephan Herfurtner, *Elliptic surfaces with four singular fibres*, Math. Ann. **291** (1991), no. 2, 319–342, DOI 10.1007/BF01445211. MR1129371

[Lau81] G. Laumon, *Semi-continuité du conducteur de Swan (d'après P. Deligne)* (French), The Euler-Poincaré characteristic (French), Astérisque, vol. 83, Soc. Math. France, Paris, 1981, pp. 173–219. MR629128

[Mal93] Gunter Malle, *Polynome mit Galoisgruppen* $\mathrm{PGL}_2(p)$ *und* $\mathrm{PSL}_2(p)$ *über* $\mathbf{Q}(t)$ (German), Comm. Algebra **21** (1993), no. 2, 511–526, DOI 10.1080/00927879308824575. MR1199685

[Mes88] Jean-François Mestre, *Courbes hyperelliptiques à multiplications réelles* (French, with English summary), C. R. Acad. Sci. Paris Sér. I Math. **307** (1988), no. 13, 721–724. MR972820

[Mil06] J. S. Milne, *Arithmetic duality theorems*, 2nd ed., BookSurge, LLC, Charleston, SC, 2006. MR2261462

[Mil75] J. S. Milne, *On a conjecture of Artin and Tate*, Ann. of Math. (2) **102** (1975), no. 3, 517–533, DOI 10.2307/1971042. MR414558

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, No. 33, Princeton University Press, Princeton, N.J., 1980. MR559531

[MM99] Gunter Malle and B. Heinrich Matzat, *Inverse Galois theory*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 1999, DOI 10.1007/978-3-662-12123-8. MR1711577

[Rei99] Stefan Reiter, *Galoisrealisierungen klassischer Gruppen* (German), J. Reine Angew. Math. **511** (1999), 193–236, DOI 10.1515/crll.1999.511.193. MR1695795

[Rib75] Kenneth A. Ribet, *On* l*-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275, DOI 10.1007/BF01425561. MR419358

[RV95] Amadeu Reverter and Núria Vila, *Some projective linear groups over finite fields as Galois groups over* $\mathbf{Q}$, Recent developments in the inverse Galois problem (Seattle, WA, 1993), Contemp. Math., vol. 186, Amer. Math. Soc., Providence, RI, 1995, pp. 51–63, DOI 10.1090/conm/186/02175. MR1352266

[Ser68] Jean-Pierre Serre, *Abelian* l*-adic representations and elliptic curves*, W. A. Benjamin, Inc., New York-Amsterdam, 1968. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. MR0263823

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

[Shi04] Takehito Shiina, *Regular Galois realizations of* $\mathrm{PSL}_2(p^2)$ *over* $\mathbb{Q}(T)$, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 125–142, DOI 10.1007/978-1-4613-0249-0_6. MR2059760

[Shi74] Kuang-yen Shih, *On the construction of Galois extensions of function fields and number fields*, Math. Ann. **207** (1974), 99–120, DOI 10.1007/BF01362150. MR332725

[Sil94] Joseph H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994, DOI 10.1007/978-1-4612-0851-8. MR1312368

[Tat66] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, 1966, pp. 415–440.

[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), Lecture Notes in Math., Vol. 476, Springer, Berlin, 1975, pp. 33–52. MR0393039

[Tho85] J. G. Thompson, *Rational rigidity of* $G_2(5)$, Proceedings of the Rutgers group theory year, 1983–1984 (New Brunswick, N.J., 1983), Cambridge Univ. Press, Cambridge, 1985, pp. 321–322. MR817265

[Ulm11] Douglas Ulmer, *Elliptic curves over function fields*, Arithmetic of L-functions, IAS/Park City Math. Ser., vol. 18, Amer. Math. Soc., Providence, RI, 2011, pp. 211–280, DOI 10.1090/pcms/018/09. MR2882692

[Wil09] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009, DOI 10.1007/978-1-84800-988-2. MR2562037

[Woh64] Klaus Wohlfahrt, *An extension of F. Klein's level concept*, Illinois J. Math. **8** (1964), 529–535. MR167533

[Yun14] Zhiwei Yun, *Motives with exceptional Galois groups and the inverse Galois problem*, Invent. Math. **196** (2014), no. 2, 267–337, DOI 10.1007/s00222-013-0469-9. MR3193750

[Zas62] Hans Zassenhaus, *On the spinor norm*, Arch. Math. **13** (1962), 434–451, DOI 10.1007/BF01650092. MR148760

[ZS80] A. E. Zalesskiĭ and V. N. Serežkin, *Finite linear groups generated by reflections* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **44** (1980), no. 6, 1279–1307, 38. MR603578

[Zyw15] David Zywina, *The inverse Galois problem for* $\mathrm{PSL}_2(\mathbb{F}_p)$, Duke Math. J. **164** (2015), no. 12, 2253–2292, DOI 10.1215/00127094-3129271. MR3397386

Department of Mathematics, Cornell University, Ithaca, New York 14853
Email address: zywina@math.cornell.edu
URL: http://www.math.cornell.edu/~zywina