AN EXPLICIT JACOBIAN OF DIMENSION 3 WITH MAXIMAL GALOIS ACTION

DAVID ZYWINA

Abstract. We gives an explicit genus 3 curve over $\mathbb{Q}$ such that the Galois action on the torsion points of its Jacobian is a large as possible. That such curves exist is a consequence of a theorem of D. Zureick-Brown and the author; however, those methods do not produce explicit examples. We shall apply the general strategies of Hall and Serre in their open image theorems. We also make use of Serre's conjecture to show that the modulo ℓ Galois actions are irreducible. While we computationally focus on a single curve, the methods of this paper can be applied to a large family of genus 3 curves.

1. Introduction

Consider a principally polarized abelian variety A of dimension $g \geq 1$ defined over $\mathbb{Q}$. Fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and define the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. The Galois action on the torsion points of $A(\overline{\mathbb{Q}})$ can be expressed in terms of a Galois representation

$$\rho_A \colon G_{\mathbb{Q}} \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}),$$

see §2.2 for details.

In [ZBZ15], Zureick-Brown and the author prove that for each integer $g \geq 3$, there is a principally polarized abelian variety $A/\mathbb{Q}$ (in fact the Jacobian of a trigonal curve) such that $\rho_A(G_{\mathbb{Q}}) = \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. For such an abelian variety, the Galois group acts on the torsion points in the most general way possible. Unfortunately, the methods of [ZBZ15] are not useful for constructing examples.

The goal of this paper is to give the first *explicit* $A/\mathbb{Q}$ for which the representation ρ_A is surjective, i.e., the Galois group acts on the torsion points of A in the most general way possible.

When $A/\mathbb{Q}$ is an elliptic curve, the image of the representation ρ_A is an important ingredient in several deep conjectures, for example the Lang-Trotter conjectures [LT76] and the Koblitz conjecture [Zyw11]. Our explicit example should be useful in providing numerical evidence for related higher dimension conjectures.

1.1. The example.

Let C be the subscheme of $\mathbb{P}^2_{\mathbb{Q}}$ defined by the quartic equation

$$x^3y - x^2y^2 + x^2z^2 + xy^3 - xyz^2 - xz^3 - y^4 + y^3z - y^2z^2 - yz^3 = 0. \tag{1.1}$$

The curve C is smooth and hence has genus 3. Let J be the Jacobian of the curve C; it is a principally polarized abelian variety of dimension 6 defined over $\mathbb{Q}$. The Galois action on the torsion points of J is as large as possible.

Theorem 1.1. *With $J/\mathbb{Q}$ as above, we have $\rho_J(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\widehat{\mathbb{Z}})$.*

Remark 1.2. Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension $g \geq 1$. In Proposition 2.5, we will show that if $g \leq 2$ or if A is the Jacobian of a hyperelliptic curve, then ρ_A is *not* surjective. This motivates why we have first considered the Jacobian of a smooth plane quartic.

2010 *Mathematics Subject Classification.* Primary 11F80; Secondary 11G10.

Though we focus only on a specific curve, the methods will also apply to a large class of smooth plane quartics. Indeed, most of this paper can be viewed as describing how to make the criterion of C. Hall in [Hal11] effective. The largest difference from [Hal11] is that we use Serre's conjecture to prove that the modulo ℓ representations are irreducible; this is motivated by the work of Dieulefait [Die02] on abelian surfaces.

1.2. **Overview.** We now give a brief overview of the contents of this paper; none of the following will be needed later on.

For each prime ℓ, let $J[\ell]$ be the ℓ-torsion subgroup of $J(\overline{\mathbb{Q}})$. The natural $G_{\mathbb{Q}}$-action on $J[\ell]$ can be expressed by a representation

$$\rho_{J,\ell}\colon G_{\mathbb{Q}} \to \mathrm{GSp}_6(\mathbb{F}_\ell),$$

see §2.2 for details. The constraint on the image of $\rho_{J,\ell}$ arises from the Weil pairing.

We will show (Proposition 2.1) that ρ_J is surjective if and only if $\rho_{J,\ell}$ is surjective for all primes ℓ. So fix any odd prime ℓ (the prime $\ell = 2$ can be dealt with separately).

We will see in §3 that the curve C, and hence also J, has good reduction at all primes away from the set $S := \{7, 11, 83\}$. Therefore, $\rho_{J,\ell}$ is unramified at all primes $p \notin S \cup \{\ell\}$. The characteristic polynomial $\det(TI - \rho_{J,\ell}(\mathrm{Frob}_p)) \in \mathbb{F}_\ell[T]$ is the reduction modulo ℓ of a computable polynomial $P_p(T) \in \mathbb{Z}[T]$ that does not depend on ℓ.

For $p \in S$ with $p \neq \ell$, we will show in §4 that $\rho_{J,\ell}(I_p)$ is a cyclic group of order ℓ, where $I_p \subseteq G_{\mathbb{Q}}$ is an inertia subgroup for p. We will prove this by using the Picard-Lefschetz formula along with the fact that the only singularities for our model (1.1) modulo p are double ordinary points. If $p \in \{7, 11\}$, then $\rho_{J,\ell}(I_p)$ will be generated by a transvection (an element with determinant 1 that fixes a codimension 1 subspace).

In §5, we shall give constraints on the semi-simplification of the representation $\rho_{J,\ell}|_{I_\ell}$.

In §6, we will prove that the representation $\rho_{J,\ell}$ is irreducible. The most involved case is when the composition factor of $J[\ell]$ (as an $\mathbb{F}_\ell[G_{\mathbb{Q}}]$-module) with smallest $\mathbb{F}_\ell$-dimension has dimension 2; for this, we make use of Serre's conjecture.

In §7, we will prove that the representation $\rho_{J,\ell}$ is primitive. More precisely, we show that there are no non-zero subspaces $W_1, \ldots, W_r$ of $J[\ell]$ such that $J[\ell] = W_1 \oplus \cdots \oplus W_r$ and such that the $G_{\mathbb{Q}}$-action permutes the spaces $W_1, \ldots, W_r$.

Knowing that $\rho_{J,\ell}$ is irreducible and primitive, and that $\rho_{J,\ell}(G_{\mathbb{Q}})$ contains a transvection, we will be able to deduce that $\rho_{J,\ell}$ is surjective.

Remark 1.3. Instead of using Serre's conjecture for irreducibility, one could use the explicit isogeny theorem of Gaudron and Rémond as done by Lombardo in [Lom15]. This gives an explicit ℓ_0 such that $\rho_{J,\ell}$ is irreducible for all $\ell \geq \ell_0$; unfortunately, ℓ_0 will be too large to feasibly check the irreducibility for primes $\ell < \ell_0$. We finally remark that, independently, similar ideas as in this paper have been recently used to show that $\rho_{A,\ell}$ is surjective for all $\ell > 2$, where A is the Jacobian of an explicit genus 3 *hyperelliptic* curve over $\mathbb{Q}$, cf. [ALS15].

Acknowledgements. Thanks to Chris Hall and Ravi Ramakrishna for several helpful discussions. Thanks to Tetsushi Ito for pointing out a small gap in an earlier version of the paper. The computations in this paper were performed using the `Magma` computer algebra system [BCP97].

2. Background and a surjectivity criterion

Let C be a smooth projective and geometrically integral curve defined over $\mathbb{Q}$ with genus $g \geq 1$. Let J be the Jacobian of the curve C; it is a principally polarized abelian variety of dimension g defined over $\mathbb{Q}$. In later sections, we will only consider the curve $C/\mathbb{Q}$ from §1.1.

2.1. **Symplectic group background.** For a commutative ring R, let M be a finitely generated free R-module equipped with a non-degenerate alternating bilinear form $\langle\ ,\ \rangle\colon M \times M \to R$. We define $\mathrm{GSp}(M)$ to be the group of $A \in \mathrm{Aut}_R(M)$ such that for some $\mathrm{mult}(A) \in R^\times$, we have $\langle Av, Aw\rangle = \mathrm{mult}(A)\langle v, w\rangle$ for all $v, w \in M$. The element $\mathrm{mult}(A) \in R^\times$ is called the multiplier of A and gives rise to a homomorphism

$$\mathrm{mult}\colon \mathrm{GSp}(M) \to R^\times.$$

We call $\mathrm{GSp}(M)$ the group of symplectic similitudes.

The rank of M over R is an even number, say $2g$. There is an R-isomorphism between M and R^{2g} such that the pairing on M agrees with the pairing $\langle v, w\rangle = v^t \cdot J \cdot w$ on R^{2g}, where we are viewing v and w as column vectors and J is the $2g \times 2g$ matrix $\left(\begin{smallmatrix} 0 & I_g \\ -I_g & 0 \end{smallmatrix}\right)$. This gives an isomorphism between $\mathrm{GSp}(M)$ and $\mathrm{GSp}_{2g}(R) := \mathrm{GSp}(R^{2g})$. As before, we have a homomorphism $\mathrm{mult}\colon \mathrm{GSp}_{2g}(R) \to R^\times$ whose kernel, which we denote by $\mathrm{Sp}_{2g}(R)$, is called the symplectic group. Observe that $\mathrm{GSp}_{2g}(R) = \{A \in \mathrm{GL}_{2g}(R) : A^t \cdot J \cdot A = \mathrm{mult}(A)J\}$ and $\mathrm{Sp}_{2g}(R) = \{A \in \mathrm{GL}_{2g}(R) : A^t \cdot J \cdot A = J\}$.

Fix a field k and an algebraic closure $\bar{k}$. Take any $A \in \mathrm{GSp}_{2g}(k)$ and set $\gamma := \mathrm{mult}(A)$. Let $\lambda_1, \dots, \lambda_{2g} \in \bar{k}$ be the roots of $P(x) := \det(xI - A) \in k[x]$. After renumbering the λ_i, one may assume that $\lambda_{2i-1}\lambda_{2i} = \gamma$ for $1 \le i \le g$, cf. [Cha97, Lemma 3.3]. From this, one can verify that

$$x^{2g}P(\gamma/x) = \gamma^g P(x). \tag{2.1}$$

2.2. **Galois representations.** For each integer $n \ge 1$, let $J[n]$ be the n-torsion subgroup of $J(\overline{\mathbb{Q}})$; it is a $\mathbb{Z}/n\mathbb{Z}$-module of rank $2g$. There is a natural action of the Galois group $G_\mathbb{Q}$ on $J[n]$ that respects its group structure. The Weil pairing and the principal polarization of J give a non-degenerate and alternating pairing

$$e_n\colon J[n] \times J[n] \to \mu_n,$$

where μ_n is the group of n-th roots of unity in $\overline{\mathbb{Q}}$.

Let $\chi_n\colon G_\mathbb{Q} \to (\mathbb{Z}/n\mathbb{Z})^\times$ be the modulo n cyclotomic character, i.e., $\sigma(\zeta) = \zeta^{\chi_n(\sigma)}$ for all $\sigma \in G_\mathbb{Q}$ and $\zeta \in \mu_n$. The pairing e_n satisfies

$$e_n(\sigma(v), \sigma(w)) = \sigma(e_n(v, w)) = e_n(v, w)^{\chi_n(\sigma)}$$

for all $v, w \in J[n]$ and $\sigma \in G_\mathbb{Q}$. The Galois action on $J[n]$ can thus be expressed by a Galois representation

$$\rho_{J,n}\colon G_\mathbb{Q} \to \mathrm{GSp}(J[n], e_n) \cong \mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

Note that $\mathrm{mult} \circ \rho_{J,n} = \chi_n$. By combining over all n and choosing bases compatibly, we obtain a single Galois representation

$$\rho_J\colon G_\mathbb{Q} \to \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}).$$

The character $\mathrm{mult} \circ \rho_A\colon G_\mathbb{Q} \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character and is thus surjective.

The following proposition, which will be proved in §2.4, will let us restrict our attention to the representations $\rho_{J,\ell}$.

Proposition 2.1. *Let $C/\mathbb{Q}$ be a smooth projective and geometrically integral curve of genus $g \ge 3$ and let J be its Jacobian. Then $\rho_J(G_\mathbb{Q}) = \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ if and only if $\rho_{J,\ell}(G_\mathbb{Q}) \supseteq \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ for all primes ℓ.*

With the above proposition in mind, we now give a criteria for showing that a subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ contains $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. First we need to introduces a few definitions.

Fix a representation $G \to \mathrm{Aut}_{\mathbb{F}_\ell}(V)$, where V is a finite dimensional $\mathbb{F}_\ell$-vector space. We say that V is reducible (and irreducible otherwise) if there is a non-trivial proper subspace of V that

is stable under the G-action. We say that V is imprimitive (and primitive otherwise) if there is an integer $r \geq 2$ and non-zero subspaces $W_1, \ldots, W_r$ of V such that $V = W_1 \oplus \cdots \oplus W_r$ and such that $\{\sigma(W_1), \ldots, \sigma(W_r)\} = \{W_1, \ldots, W_r\}$ for all $\sigma \in G$.

For $A \in \mathrm{Aut}_{\mathbb{F}_\ell}(V)$, let $V^{A=1}$ be the subspace of V consisting of the vectors that are fixed by A. We say that A is a transvection if $V^{A=1}$ has codimension 1 in V and $\det(A) = 1$.

Proposition 2.2. *Fix an integer $g \geq 2$ and an odd prime ℓ. Let G be a subgroup of $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$ with its natural action on $V = \mathbb{F}_\ell^{2g}$. Suppose that G contains a transvection and that the action of G on V is irreducible and primitive. Then $G \supseteq \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$.*

Proof. Let R be the subgroup of G generated by transvections; it is a subgroup of $G \cap \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. We have $R \neq 1$ since G contains a transvection by assumption. The group R is normal in G since the conjugate of a transvection is also a transvection.

Fix an irreducible R-submodule W of V. Using that R is normal in G, one can verify that $\sigma(W)$ is an R-module for all $\sigma \in G$. Let H be the group consisting of $\sigma \in G$ for which $\sigma(W) = W$. Using that V is an irreducible G-module, we find that that $V = \sum_{\sigma \in G/H} \sigma(W)$. Lemma 6 of [Hal11], which uses parts of [Hal08], says that we in fact have a direct sum $V = \oplus_{\sigma \in G/H} \sigma(W)$.

Therefore, V is the direct sum of the subspaces $\{\sigma(W) : \sigma \in G/H\}$ which are permuted by the natural action of G. Since G acts primitively on V by assumption, we deduce that $W = V$, i.e., V is an irreducible R-module.

The main theorem of Zalesskiĭ and Serežkin in [ZS76] shows that $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ contains no proper subgroups that act irreducibly on V and are generated by transvections. Therefore, $R = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. The lemma follows since $R \subseteq G$. □

2.3. **Compatibility.** Take any prime p for which $C/\mathbb{Q}$, and hence also $J/\mathbb{Q}$, has good reduction. Let C_p and J_p be the reduction of C and J, respectively, modulo p. The abelian variety $J_p/\mathbb{F}_p$ agrees with the Jacobian of $C_p/\mathbb{F}_p$.

Take any prime $\ell \neq p$. Let

$$\rho_{J,\ell^\infty} \colon G_{\mathbb{Q}} \to \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$$

be the Galois representation obtained by composing ρ_J with the natural projection $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}}) \to \mathrm{GSp}_{2g}(\mathbb{Z}_\ell)$; it can also be obtained by taking the inverse limit of the representations ρ_{J,ℓ^n}. The representation ρ_{J,ℓ^∞} is unramified at p and we have

$$\det(TI - \rho_{J,\ell^\infty}(\mathrm{Frob}_p)) = P_{J_p}(T),$$

for some polynomial $P_{J_p}(T) \in \mathbb{Z}[T]$ that does not depend on the choice of ℓ. Here Frob_p is an (arithmetic) Frobenius automorphism of p.

Let $\pi_p \colon J_p \to J_p$ be the Frobenius endomorphism of $J_p/\mathbb{F}_p$. We may also characterize $P_{J_p}(T)$ as the polynomial in $\mathbb{Q}[T]$ for which $P_{J_p}(n)$ is the degree of the isogeny $n - \pi_p$ for every integer n.

We can also describe the polynomial $P_{J_p}(T)$ in terms of the zeta function of C_p. Recall that the zeta function of $C_p/\mathbb{F}_p$ is the formal power series

$$Z_{C_p}(T) = \exp\Big(\sum_{m=1}^{\infty} |C_p(\mathbb{F}_{p^m})| \cdot T^m/m\Big).$$

From Weil, we know that $Z_{C_p}(T) = P_{J_p}^{\mathrm{rev}}(T)/\big((1-T)(1-pT)\big)$, where $P_{J_p}^{\mathrm{rev}}(T) := T^{2g} P_{J_p}(1/T)$.

We have $\mathrm{mult} \circ \rho_{J,\ell}(\mathrm{Frob}_p) = p$, so from (2.1) we obtain the functional equation

$$T^{2g} P(p/T) = p^g P(T). \tag{2.2}$$

2.4. **Proof of Proposition 2.1.** We first prove two group theoretic lemmas.

Lemma 2.3. *Take any integers $g \geq 3$ and $n \geq 2$.*

(i) *The group $\mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ is perfect.*
(ii) *The only simple groups that are quotients of $\mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ are the groups $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ with $\ell | N$.*

Proof. Fix $g \geq 3$. Part (i) follows by observing that $\mathrm{Sp}_{2g}(\mathbb{Z})$ is its own commutator subgroup and that the reduction modulo n map $\mathrm{Sp}_{2g}(\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ is surjective for all $n \geq 2$, cf. [BMS67, §12]. Here we need $g \geq 3$ since $\mathrm{Sp}_{2g}(\mathbb{Z})$ is not its own commutator subgroup when g is 1 or 2.

We now prove (ii). Using part (i), it suffices to show that $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ is the only non-abelian simple group occurring as a Jordan-Hölder factor of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^e\mathbb{Z})$ for a fixed prime ℓ and integer $e \geq 1$. Note that the kernel of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^e\mathbb{Z}) \to \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is an ℓ-group and hence solvable, so one may assume that $e = 1$. The group $\{\pm I\}$ is abelian and $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\}$ is simple and non-abelian. Here we need $g \geq 3$ again, since $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ is solvable if $(g, \ell) \in \{(1,2), (1,3), (2,2)\})$. □

Lemma 2.4. *Fix an integer $g \geq 3$ and let H be a closed subgroup of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$. Suppose that the reduction modulo ℓ map $H \to \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is surjective for all primes ℓ. Then $H = \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$.*

Proof. For each integer $n \geq 2$, let $H(n) \subseteq \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ be the image of H under the reduction modulo n map. We claim that $H(n) = \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ for all $n \geq 2$. The lemma will follow directly from the claim since H is closed.

First suppose that n is a prime power, say $n = \ell^e$ for some prime ℓ and integer $e \geq 1$. One can show that there are no proper subgroups of $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell^e\mathbb{Z})$ whose image modulo ℓ is the full group $\mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ (this for example follows from [Vas04, Theorem 2.2.5] with $G = \mathrm{Sp}_{2g}$ and $k = \mathbb{F}_\ell$). Since $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell\mathbb{Z})$ by hypothesis, we deduce that $H(\ell^e) = \mathrm{Sp}_{2g}(\mathbb{Z}/\ell^e\mathbb{Z})$. So the claim holds when n is a prime power.

Now suppose that $n \geq 2$ is not a prime power. By induction, we may assume that $n = m_1 m_2$ with $m_1, m_2 \geq 2$ relatively prime such that $H(m_1) = \mathrm{Sp}_{2g}(\mathbb{Z}/m_1\mathbb{Z})$ and $H(m_2) = \mathrm{Sp}_{2g}(\mathbb{Z}/m_2\mathbb{Z})$. We can thus view $H(m)$ as a subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/m_1\mathbb{Z}) \times \mathrm{Sp}_{2g}(\mathbb{Z}/m_1\mathbb{Z})$ that projects surjectively on each of the two factors. If $H(m) \neq \mathrm{Sp}_{2g}(\mathbb{Z}/m\mathbb{Z})$, then Goursat's lemma (cf. [Rib75, Lemma 3.2]) implies that $\mathrm{Sp}_{2g}(\mathbb{Z}/m_1\mathbb{Z})$ and $\mathrm{Sp}_{2g}(\mathbb{Z}/m_2\mathbb{Z})$ have a common simple group as a quotient; this is impossible by Lemma 2.3(ii). Therefore, $H(n) = \mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$. This completes our proof of the claim. □

We now prove Proposition 2.1. First suppose that $\rho_{J,\ell}(G_\mathbb{Q}) \supseteq \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ for all primes ℓ. Let H be the the commutator subgroup of $\rho_J(G_\mathbb{Q})$, i.e., the maximal closed normal subgroup of $\rho_J(G_\mathbb{Q})$ with abelian quotient. Observe that H is a closed subgroup of $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$.

Take any prime ℓ. The image $H(\ell) \subseteq \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ of H under the reduction modulo ℓ map is equal to the commutator subgroup of $\rho_{J,\ell}(G_\mathbb{Q})$. We thus have $H(\ell) = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ since $\rho_{J,\ell}(G_\mathbb{Q}) \supseteq \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ by assumption and since $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is perfect by Lemma 2.3. Lemma 2.4 now implies that $H = \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$.

Since $\rho_{J,\ell}(G_\mathbb{Q})$ contains $H = \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$ and $\mathrm{mult}(\rho_J(G_\mathbb{Q})) = \widehat{\mathbb{Z}}^\times$ (see §2.2), we deduce that $\rho_{J,\ell}(G_\mathbb{Q}) = \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ as desired. Finally, the other direction of Proposition 2.1 is easy.

2.5. **Further remarks.** We now explain the claims from Remark 1.2; we will not use this later on.

Proposition 2.5. *Let $A/\mathbb{Q}$ be a principally polarized abelian variety of dimension $g \geq 1$. Suppose that $g \in \{1, 2\}$ or that A is the Jacobian of a hyperelliptic curve. Then $\rho_A(G_\mathbb{Q}) \neq \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$.*

Proof. Suppose that $\rho_A(G_{\mathbb{Q}}) = \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$. Since $\mathrm{mult} \circ \rho_A \colon G_{\mathbb{Q}} \to \widehat{\mathbb{Z}}^\times$ is the cyclotomic character, we have $\rho_A(G_{\mathbb{Q}^{\mathrm{cyc}}}) = \rho_A(G_{\mathbb{Q}}) \cap \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}}) = \mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$, where $\mathbb{Q}^{\mathrm{cyc}}$ is the cyclotomic extension of $\mathbb{Q}$. The group $\rho_A(G_{\mathbb{Q}^{\mathrm{ab}}})$ is the commutator subgroup of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$, where $\mathbb{Q}^{\mathrm{ab}}$ is the maximal abelian extension of $\mathbb{Q}$. By the Kronecker-Weber theorem, we have $\mathbb{Q}^{\mathrm{ab}} = \mathbb{Q}^{\mathrm{cyc}}$ and hence the commutator subgroup of $\mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ is equal to $\mathrm{Sp}_{2g}(\widehat{\mathbb{Z}})$. In particular, the commutator subgroup of $\mathrm{GSp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ is $\mathrm{Sp}_{2g}(\mathbb{Z}/n\mathbb{Z})$ for all $n \geq 2$. However, when $g \in \{1, 2\}$, the group $\mathrm{GSp}_{2g}(\mathbb{Z}/2\mathbb{Z}) = \mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$ is solvable and hence its commutator is a proper subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z}/2\mathbb{Z})$.

Now suppose that A is the Jacobian of a hyperelliptic curve $X/\mathbb{Q}$ (of genus $g \geq 3$). We have $\rho_A(G_{\mathbb{Q}}) = \mathrm{GSp}_{2g}(\widehat{\mathbb{Z}})$ and hence $\rho_{A,2}(G_{\mathbb{Q}}) = \mathrm{GSp}_{2g}(\mathbb{F}_2) = \mathrm{Sp}_{2g}(\mathbb{F}_2)$. Let $P_1, \dots, P_{2g+2} \in X(\overline{\mathbb{Q}})$ be the Weierstrass points of X; they are the points fixed by the hyperelliptic involution. Let K be the smallest extension of $\mathbb{Q}$ for which all the points $P_1, \dots, P_{2g+2}$ lie in $X(K)$. The extension $K/\mathbb{Q}$ is Galois and the group $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to a subgroup of $\mathfrak{S}_{2g+2}$. One can show that the 2-torsion subgroup of $A(\overline{\mathbb{Q}})$ is generated by the points represented by the divisors $P_i - P_j$. Therefore, $\rho_{A,2}(\mathrm{Gal}(\overline{\mathbb{Q}}/K)) = \{I\}$ and hence

$$\prod_{i=1}^{g} \left(2^{2i-1}(2^{2i} - 1)\right) = |\mathrm{Sp}_{2g}(\mathbb{F}_2)| = |\rho_{A,2}(G_{\mathbb{Q}})| \leq [K : \mathbb{Q}] \leq (2g+2)!.$$

Proceeding by induction on g, one can check that this inequality fails for all $g \geq 3$. Therefore, ρ_A is not surjective. □

The case $g = 1$ of Proposition 2.5 was first observed by Serre [Ser72, Prop. 22].

Proposition 2.5 need not hold over a general number field when $g \in \{1, 2\}$. For example, Grecius [Gre10] found an explicit elliptic curve E/k, with k a cubic extension of $\mathbb{Q}$, such that $\rho_E(\mathrm{Gal}(\overline{k}/k)) = \mathrm{GL}_2(\widehat{\mathbb{Z}})$.

3. Good primes

Define the set of primes

$$S := \{7, 11, 83\};$$

these are the primes for which $C/\mathbb{Q}$, and hence J, has bad reduction, cf. Lemma 3.1.

3.1. **Singularities.** Let $\mathcal{C}$ be the subscheme of $\mathbb{P}^2_{\mathbb{Z}}$ defined by the equation (1.1). For each ring R, let $\mathcal{C}_R$ be the scheme over $\mathrm{Spec}\, R$ obtained by base extending $\mathcal{C}$ to R. The curve $C/\mathbb{Q}$ is of course $\mathcal{C}_{\mathbb{Q}}$. Let $\mathbb{Q}_p^{\mathrm{un}}$ be the maximal unramified extension of $\mathbb{Q}_p$ in $\overline{\mathbb{Q}}_p$ and let $\mathbb{Z}_p^{\mathrm{un}}$ be its local ring. The residue field of $\mathbb{Z}_p^{\mathrm{un}}$ is an algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$.

Lemma 3.1.

(i) *For any prime $p \notin S$, the curve $C/\mathbb{Q}$ has good reduction at p. Moreover, $\mathcal{C}_{\mathbb{Z}_p} \to \mathrm{Spec}\, \mathbb{Z}_p$ is smooth and proper.*

(ii) *Take any prime $p \in S$. The morphism*

$$\mathcal{C}_{\mathbb{Z}_p^{\mathrm{un}}} \to \mathrm{Spec}\, \mathbb{Z}_p^{\mathrm{un}}$$

is smooth away from a finite set Σ of points that lie in the special fiber $\mathcal{C}_{\overline{\mathbb{F}}_p}$. The points in Σ are all ordinary double points of $\mathcal{C}_{\overline{\mathbb{F}}_p}$. We have $|\Sigma| = 1$ if $p \in \{7, 11\}$ and $|\Sigma| = 2$ otherwise.

For each $P \in \Sigma$, the completion of the local ring of $\mathcal{C}_{\mathbb{Z}_p^{\mathrm{un}}}$ at P is isomorphic as a $\mathbb{Z}_p^{\mathrm{un}}$-algebra to $\mathbb{Z}_p^{\mathrm{un}}[[x, y]]/(xy + p)$.

Proof. Let $f(x, y, z)$ be the polynomial on the left hand side of (1.1). Define the polynomial $g(x, y, z) := f(x - 69y - 1389z, y - 64z, z)$. Since $f(x, y, z) = g(x + 69y + 5805z, y + 64, z)$, there is no harm in assuming instead that $\mathcal{C}$ is the subscheme of $\mathbb{P}^2_{\mathbb{Z}}$ defined by $g(x, y, z) = 0$.

Let I be the the ideal of $\mathbb{Z}[x,y,z]$ generated by g and the partial derivatives g_x, g_y and g_z. Let I' be the saturation of I (with respect to the irrelevant ideal of $\mathbb{Z}[x,y,z]$). One can show, as in the following `Magma` code, that

$$I' = \big(6391,\ x,\ 83y,\ y^2 + 11yz + 616z^2\big).$$

```
R<x,y,z>:=PolynomialRing(Integers(),3);
f:=x^3*y-x^2*y^2+x^2*z^2+x*y^3-x*y*z^2-x*z^3-y^4+y^3*z-y^2*z^2-y*z^3;
g:=Evaluate(f,[x-69*y-1389*z,y-64*z,z]);
I:=ideal<R|[g,Derivative(g,x),Derivative(g,y),Derivative(g,z)]>;
Saturation(I) eq ideal<R|[6391,x,83*y,y^2+11*y*z+616*z^2]>;
```

That the primes divisors of 6391 are the elements of S is enough to show that $\mathcal{C}$ is smooth away from the fibers over the primes $p \in S$. Part (i) is an immediate consequence.

From our description of I', we find that the only singular points of $\mathcal{C}$ are:

- the point $(0:0:1)$ in the fiber $\mathcal{C}_{\mathbb{F}_7}$,
- the point $(0:0:1)$ in the fiber $\mathcal{C}_{\mathbb{F}_{11}}$,
- the points $(0:32:1)$ and $(0:40:1)$ in the fiber $\mathcal{C}_{\mathbb{F}_{83}}$.

Take any singular point P of $\mathcal{C}$. Take a prime $p \in S$ and integer $y_0 \in \{0, 32, 40\}$ such that P is the image of $(0:y_0:1)$ modulo p. Define the polynomial

$$F(x,y) := g(x, y + y_0, 1) \in \mathbb{Z}[x,y].$$

The completion of the local ring of $\mathcal{C}_{\mathbb{Z}_p^{\mathrm{un}}}$ at P is thus isomorphic to $\mathbb{Z}_p^{\mathrm{un}}[[x,y]]/(F(x,y))$.

It is straightforward to check that in $\mathbb{Z}[x,y]$, we have

$$F(x,y) \equiv a + a_1 x + a_2 y + Q(x,y) \pmod{(x,y)^3}$$

where is $Q(x,y) \in \mathbb{Z}[x,y]$ is a quadratic form whose image in $\mathbb{F}_p[x,y]$ is also non-degenerate, and $a \equiv a_1 \equiv a_2 \equiv 0 \pmod{p}$ with $a \not\equiv 0 \pmod{p^2}$.

Proposition 2.4 of [FK88, III] shows that we have an isomorphism of $\mathbb{Z}_p$-algebras

$$\mathbb{Z}_p[[x,y]]/(F(x,y)) \cong \mathbb{Z}_p[[x,y]]/(Q'(x,y) + b),$$

where $Q'(x,y) \in \mathbb{Z}_p[x,y]$ is a quadratic form whose image in $\mathbb{F}_p[x,y]$ is non-degenerate and $b \in \mathbb{Z}_p$. More precisely, the proof of Proposition 2.4 of [FK88, III] shows that there are $\alpha_1, \alpha_2 \in p\mathbb{Z}_p$ and $h_1, h_2 \in (x,y)^3 \subseteq \mathbb{Z}_p[[x,y]]$ such that $F(x + \alpha_1 + h_1, y + \alpha_2 + h_2)$ is of the desired form $Q'(x,y) + b$; hence b has p-adic valuation 1 since a has p-adic valuation 1 and $a_1, a_2, \alpha_2, \alpha_2 \in p\mathbb{Z}_p$.

Since $\mathbb{Z}_p^{\mathrm{un}}$ is strictly Henselian, there is a matrix $A \in \mathrm{GL}_2(\mathbb{Z}_p^{\mathrm{un}})$ such that $Q'(A_{1,1}x + A_{1,2}y, A_{2,1}x + A_{2,2}y) = xy$, cf. Proposition 2.2 of [FK88, III]. We deduce that the completion of the local ring of $\mathcal{C}_{\mathbb{Z}_p^{\mathrm{un}}}$ is isomorphic as a $\mathbb{Z}_p^{\mathrm{un}}$-algebra to $\mathbb{Z}_p^{\mathrm{un}}[[x,y]]/(xy + b)$. After replacing x by itself times an appropriate unit of $\mathbb{Z}_p^{\mathrm{un}}$, we may further assume that $b = p$. □

3.2. **Frobenius polynomials.** Now take any prime $p \notin S$. Let C_p be the curve in $\mathbb{P}^2_{\mathbb{F}_p}$ defined by (1.1). By Lemma 3.1, we find that $C_p/\mathbb{F}_p$ is a smooth projective curve of genus 3. The abelian variety J thus has good reduction modulo p and its reduction $J_p/\mathbb{F}_p$ is equal to the Jacobian of C_p.

We take $P_p(T)$ to be the polynomial $P_{J_p}(T)$ from §2.3; it is monic with integer coefficients and has degree 6. From §2.3, we find that for each prime $\ell \neq p$, we have

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

Using (2.2), we find that

$$P_p(T) = T^6 + a_p T^5 + b_p T^4 + c_p T^3 + p b_p T^2 + p^2 a_p T + p^3$$

for unique integers a_p, b_p and c_p.

We have computed $P_p(T)$ for a few small primes $p \notin S$.

$$\begin{aligned}
P_2(T) &= T^6 + 3T^5 + 6T^4 + 9T^3 + 12T^2 + 12T + 8\\
P_3(T) &= T^6 + T^5 + 2T^4 + 3T^3 + 6T^2 + 9T + 27\\
P_5(T) &= T^6 + 4T^5 + 10T^4 + 17T^3 + 50T^2 + 100T + 125\\
P_{17}(T) &= T^6 + 2T^5 + 9T^4 + 120T^3 + 153T^2 + 578T + 4913\\
P_{19}(T) &= T^6 + 4T^5 + 18T^4 + 91T^3 + 342T^2 + 1444T + 6859\\
P_{23}(T) &= T^6 + 5T^5 + 19T^4 + 53T^3 + 437T^2 + 2645T + 12167\\
P_{41}(T) &= T^6 + 42T^4 - 212T^3 + 1722T^2 + 68921\\
P_{43}(T) &= T^6 + 3T^5 - T^4 - 43T^3 - 43T^2 + 5547T + 79507\\
P_{73}(T) &= T^6 - 4T^5 - 43T^4 + 581T^3 - 3139T^2 - 21316T + 389017
\end{aligned}$$

One way to compute $P_p(T)$ is by using the zeta function interpretation in §2.3. After computing $|C_p(\mathbb{F})|$, $|C_p(\mathbb{F}_{p^2})|$ and $|C_p(\mathbb{F}_{p^3})|$, one can determine a_p, b_p and c_p (and hence $P_p(T)$) from the congruence

$$1 + a_pT + b_pT^2 + c_pT^3 \equiv (1-T)(1-pT)\exp\Big(\sum_{m=1}^{3} |C_p(\mathbb{F}_{p^m})| \cdot T^m/m\Big) \mod T^3.$$

The above explicit polynomials $P_p(T)$ have been computed using the follow `Magma` code:

```
Pol<T>:=PolynomialRing(Rationals());
for p in [2,3,5,17,19,23,41,43,73] do
    P2<x,y,z>:=ProjectiveSpace(GF(p),2);
    f:=x^3*y-x^2*y^2+x^2*z^2+x*y^3-x*y*z^2-x*z^3-y^4+y^3*z-y^2*z^2-y*z^3;
    Cp:=Curve(P2,f);
    P:=Pol!LPolynomial(Cp);
    print T^6*Evaluate(P,1/T);
end for;
```

3.3. **Maximal image modulo 2.** We now show that $\rho_{J,2}$ is surjective.

Lemma 3.2. *We have $\rho_{J,2}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_2)$.*

Proof. Define $G := \rho_{J,2}(G_{\mathbb{Q}})$; it is a subgroup of $\mathrm{GSp}_6(\mathbb{F}_2) = \mathrm{Sp}_6(\mathbb{F}_2)$. Consider an odd prime $p \notin S$ and let $f_p(x) \in \mathbb{F}_2[x]$ be the reduction of $P_p(x)$ modulo 2. Assume that $f_p(x)$ is separable and hence it is also the minimal polynomial of $g_p := \rho_{J,2}(\mathrm{Frob}_p)$. Therefore, the order of g_p is the smallest integer $n_p \geq 1$ for which $f_p(x)$ divides $x^{n_p} - 1 \in \mathbb{F}_2[x]$. From §3, we find that $f_5(x) = x^6 + x^3 + 1$, $f_{23}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ and $f_{73}(x) = (x^2 + x + 1)(x^4 + x^3 + x^2 + x + 1)$. One can then check that $n_5 = 9$, $n_{23} = 7$ and $n_{73} = 15$, and thus G contains elements of order 7, 9 and 15.

A computation shows that $\mathrm{Sp}_6(\mathbb{F}_2)$ has no maximal subgroups containing elements of order 7, 9 and 15; therefore, $G = \mathrm{Sp}_6(\mathbb{F}_2)$. Moreover, any maximal subgroup of G that has order divisible by $7 \cdot 15$ is isomorphic to $\mathfrak{S}_8$ and hence has no element of order 9 (this can be easily deduced from the description of maximal subgroups of $\mathrm{Sp}_6(\mathbb{F}_2)$ in [CCN+85, p.46]). □

4. Inertia at bad primes

For a prime $p \in S$, let I_p be an inertia subgroup of $G_{\mathbb{Q}}$ at the prime p. The goal of this section is to prove the following using the Picard-Lefschetz formula.

Proposition 4.1. *For primes $p \in S$ and $\ell \neq p$, the group $\rho_{J,\ell}(I_p)$ is cyclic of order ℓ. If $p \in \{7, 11\}$, then $\rho_{J,\ell}(I_p)$ is generated by a transvection.*

Fix a prime $p \in S$. Set $R = \mathbb{Z}_p^{\mathrm{un}}$ and let $K = \mathbb{Q}_p^{\mathrm{un}}$ be its quotient field. Fix an algebraic closure $\overline{K}$ of K. With a choice of embedding $\overline{\mathbb{Q}} \hookrightarrow \overline{K}$, the restriction map gives an injective homomorphism $G_K := \mathrm{Gal}(\overline{K}/K) \hookrightarrow G_{\mathbb{Q}}$ that we can view as an inclusion. The group G_K is then conjugate to I_p in $G_{\mathbb{Q}}$.

Fix a prime $\ell \neq p$. So to prove Proposition 4.1, we need only consider the action of G_K on $J[\ell] \subseteq J(\overline{K})$. Define the $\mathbb{F}_\ell$-vector space $V := H^1(C_{\overline{K}}, \mathbb{F}_\ell)$; for background on étale cohomology, see [Mil80], [FK88] or [Del77]. There is a natural action of G_K on V that we can express in terms of a representation

$$\rho\colon G_K \to \mathrm{Aut}(V).$$

Let $\mathbb{F}_\ell(1)$ be the group of ℓ-th roots of unity in $\overline{K}$ and let $\mathbb{F}_\ell(-1)$ be the $\mathbb{F}_\ell$-dual of $\mathbb{F}_\ell(1)$. Evaluation gives a natural isomorphism $\mathbb{F}_\ell(1) \otimes_{\mathbb{F}_\ell} \mathbb{F}_\ell(-1) = \mathbb{F}_\ell$.

One knows that $J[\ell]$ is isomorphic to the étale cohomology group $H^1(C_{\overline{K}}, \mathbb{F}_\ell(1))$ as an $\mathbb{F}_\ell[G_K]$-module. The group G_K acts trivially on $\mathbb{F}_\ell(1)$ since $\ell \neq p$, so $J[\ell]$ and V are isomorphism $\mathbb{F}_\ell[G_K]$-modules. Therefore, ρ and $\rho_{J,\ell}|_{G_K}$ are isomorphic representations. It thus suffices to prove that $\rho(G_K)$ is a group of order ℓ and that it is generated by a transvection when $p \in \{7, 11\}$.

We have an alternating pairing

$$\langle\,,\,\rangle\colon V \times V \xrightarrow{\cup} H^2(C_{\overline{K}}, \mathbb{F}_\ell \otimes_{\mathbb{F}_\ell} \mathbb{F}_\ell) = H^2(C_{\overline{K}}, \mathbb{F}_\ell) \xrightarrow{\sim} \mathbb{F}_\ell(-1),$$

where we are composing the cup product and trace map. The G_K-action on V respects the pairing $\langle\,,\,\rangle$, i.e., $\langle \sigma(v), \sigma(w)\rangle = \sigma(\langle v, w\rangle) = \langle v, w\rangle$ for all $\sigma \in G_K$ and $v, w \in V$. The pairing $\langle\,,\,\rangle$ is non-degenerate (after taking Tate twists, we can identify this pairing with the Weil pairing on $J[\ell]$).

The morphism $\mathcal{C}_R \to \operatorname{Spec} R$ is a proper and flat morphism of relative dimension 1. From Lemma 3.1(ii), we know that $\mathcal{C}_K$ is smooth and that $\mathcal{C}_{\overline{\mathbb{F}}_p}$ is smooth away from a finite set Σ of ordinary double points.

The Picard-Lefschetz formula (see [SGA7-II, XV Théorème 3.4]) shows that there are non-zero and pairwise orthogonal *vanishing cycles* $\{\delta_x\}_{x\in\Sigma}$ in V such that for $v \in V$ and $\sigma \in G_K$, we have

$$\sigma(v) = v - \sum_{x\in\Sigma} \varepsilon_x(\sigma)\langle v, \delta_x\rangle \cdot \delta_x,$$

where $\varepsilon_x\colon G_K \to \mathbb{F}_\ell(1)$ is a certain homomorphism and where we view $\varepsilon_x(\sigma)\langle v, \delta_x\rangle$ as an element of $\mathbb{F}_\ell(1) \otimes_{\mathbb{F}_\ell} \mathbb{F}_\ell(-1) = \mathbb{F}_\ell$.

Let $\varepsilon\colon G_K \to \mathbb{F}_\ell(1)$ be the surjective homomorphism that satisfies $\sigma(\sqrt[\ell]{p}) = \varepsilon(\sigma)\sqrt[\ell]{p}$ for all $\sigma \in G_K$. From Lemma 3.1(ii), we find that the completion of the local ring of $\mathcal{C}_R$ at a point $x \in \Sigma$ is isomorphic as an R-algebra to $R[[x, y]]/(xy + p)$. From [SGA7-II, XV §3.3], we find that $\varepsilon_x = \varepsilon$ (in general, you would need to raise ε to some power). Therefore,

$$\sigma(v) = v - \sum_{x\in\Sigma} \varepsilon(\sigma)\langle v, \delta_x\rangle \cdot \delta_x \tag{4.1}$$

for $v \in V$ and $\sigma \in G_K$. The representation ρ thus factors through the order ℓ group $\mathrm{Gal}(K(\sqrt[\ell]{p})/K)$. Therefore, $\rho(G_K)$ is a group of order 1 or ℓ. Since $\varepsilon \neq 1$ and $v \mapsto \langle v, \delta_x\rangle$ is non-trivial, we deduce from (4.1) that $\rho(G_K)$ is a non-trivial group and hence is a cyclic of order ℓ.

Now suppose that $p \in \{7, 11\}$. Fix any $\sigma_0 \in G_K$ with $\rho(\sigma_0) \neq 1$. It remains to prove that $\rho(\sigma_0)$ is a transvection. Since $\rho(\sigma_0) \neq 1$ has order ℓ, it suffices to prove that σ_0 fixes an $\mathbb{F}_\ell$-subspace of V of dimension $\dim_{\mathbb{F}_\ell} V - 1$. Since $p \in \{7, 11\}$, we have $|\Sigma| = 1$ by Lemma 3.1(ii). We thus have

$$\sigma_0(v) = v - \varepsilon(\sigma_0)\langle v, \delta_x\rangle \cdot \delta_x, \tag{4.2}$$

where x is the unique element of Σ. Let W be the subspace of V consisting of $v \in V$ for which $\langle v, \delta_x \rangle$ is trivial; it has $\mathbb{F}_\ell$-dimension $\dim_{\mathbb{F}_\ell} V - 1$ since the pairing is non-degenerate and $\delta_x \neq 0$. By (4.2), we deduce that $\sigma_0(v) = v$ for all $v \in W$. This completes the proof of Proposition 4.1.

5. Inertia at ℓ

Fix an odd prime $\ell \notin S$ and let I_ℓ be any inertia subgroup of $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ at the prime ℓ. In this section, we give some information on how I_ℓ acts on $J[\ell]$.

We first need to recall some background on tame inertia groups and tame inertia weights, see §1 of [Ser72] for more details. Let $\mathcal{P} \subseteq I_\ell$ be the wild inertia subgroup of I_ℓ; it is the largest pro-ℓ subgroup of I_ℓ. The quotient $I_\ell^t := I_\ell/\mathcal{P}$ is the tame inertia group for the prime ℓ. For an integer $d \geq 1$ relatively prime to ℓ, let μ_d be the d-th roots of unity in $\overline{\mathbb{Q}}$. The map

$$\theta_d \colon I_\ell \to \mu_d, \quad \sigma \mapsto \sigma(\sqrt[d]{\ell})/\sqrt[d]{\ell}$$

is a surjective homomorphism which factors through I_ℓ^t. Taking the inverse limit over all d relatively prime to ℓ (ordered by divisibility), we obtain an isomorphism

$$I_\ell^t \xrightarrow{\sim} \varprojlim_d \mu_d.$$

By composing the homomorphism θ_d with reduction modulo a place of $\overline{\mathbb{Q}}$ lying over ℓ, we obtain a character $I_\ell^t \to \overline{\mathbb{F}}_\ell^\times$. For an integer $m \geq 1$, setting $d := \ell^m - 1$ gives a surjective character

$$\phi \colon I_\ell^t \to \mathbb{F}_{\ell^m}^\times.$$

The fundamental characters of level m are the m characters $I_\ell^t \to \mathbb{F}_{\ell^m}^\times$ obtained by composing ϕ with the isomorphisms of $\mathbb{F}_{\ell^m}^\times$ arising from field automorphisms of $\mathbb{F}_{\ell^m}$; they are $\phi, \phi^\ell, \dots, \phi^{\ell^{m-1}}$.

Let V be an irreducible $\mathbb{F}_\ell[I_\ell]$-module and set $m := \dim_{\mathbb{F}_\ell}(V)$. There is then an isomorphism $V \cong \mathbb{F}_{\ell^m}$ of $\mathbb{F}_\ell$-vector spaces such that the induced character

$$I_\ell \to \mathrm{Aut}_{\mathbb{F}_\ell}(V) \cong \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^m})$$

has image in $\mathbb{F}_{\ell^m}^\times$, where the first map gives the action of I_ℓ on V (here we use scalar multiplication to identify $\mathbb{F}_{\ell^m}^\times$ with a subgroup of $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^m})$). This representation arising from V thus factors through a character $\alpha \colon I_\ell^t \to \mathbb{F}_{\ell^m}^\times$. Given a fundamental character $\phi \colon I_\ell^t \to \mathbb{F}_{\ell^m}^\times$ of level m, there are unique integers $0 \leq e_1, \dots, e_m \leq \ell - 1$ such that

$$\alpha = \phi^{e_1 + e_2\ell + \cdots + e_m\ell^{m-1}}. \tag{5.1}$$

The integers $e_1, \dots, e_m$ are called the tame inertia weights of V.

Let V be an $\mathbb{F}_\ell[I_\ell]$-module with V a finite dimensional $\mathbb{F}_\ell$-vector space. Let $V_1, \dots, V_r$ be the composition factors of V as an $\mathbb{F}_\ell[I_\ell]$-module. An integer is a tame inertia weight for V if it is a tame inertia weight for at least one of the V_i.

We now consider the representations occurring in this paper.

Proposition 5.1. *Fix an odd prime $\ell \notin S$. The only possible tame inertia weights for the $\mathbb{F}_\ell[I_\ell]$-module $J[\ell]$ are 0 and 1.*

Proof. This follows from work of Raynaud, cf. [Ray74, Corollaire 3.4.4]. One could also deduce this from [Car08]. □

The following lemma gives some consequences of Proposition 5.1 that we will use later. Recall that $\chi_\ell \colon G_{\mathbb{Q}} \to \mathbb{F}_\ell^\times$ was defined in §2.2.

Lemma 5.2. *Fix an odd prime $\ell \notin S$ and let V be any composition factor of the $\mathbb{F}_\ell[I_\ell]$-module $J[\ell]$. Set $m := \dim_{\mathbb{F}_\ell} V$ and let $\rho\colon I_\ell \to \mathrm{Aut}_{\mathbb{F}_\ell}(V)$ be the representation describing the I_ℓ-action.*

(i) *We have $\det\circ\rho = \chi_\ell^e|_{I_\ell}$ for some integer $0 \le e \le m$.*
(ii) *If H is a closed subgroup of I_ℓ satisfying $[I_\ell : H] < \ell - 1$, then $\rho|_H$ is irreducible.*

Proof. We first prove (i). As noted above, ρ gives rise to a character $\alpha\colon I_\ell^t \to \mathbb{F}_{\ell^m}^\times$ of the form (5.1) with ϕ a fundamental character of level m and $0 \le e_1, \dots, e_m \le \ell - 1$. By Proposition 5.1, we have $e_1, \dots, e_m \in \{0, 1\}$.

The character $\det\circ\rho\colon I_\ell \to \mathbb{F}_\ell^\times$ factors through $N\circ\alpha\colon I_\ell^t \to \mathbb{F}_\ell^\times$, where $N := N_{\mathbb{F}_{\ell^m}/\mathbb{F}_\ell}\colon \mathbb{F}_{\ell^m}^\times \to \mathbb{F}_\ell^\times$ is the norm map. Therefore,

$$N\circ\alpha = (N\circ\phi)^{e_1+e_2\ell+\cdots+e_m\ell^{m-1}} = (N\circ\phi)^{e_1+\ldots+e_m},$$

where we have used that $N^\ell = N$. We have $0 \le e_1 + \ldots + e_m \le m$, so it suffices to prove that $N\circ\phi = \chi_\ell|_{I_\ell}$. We have $N\circ\phi = \phi^{1+\ell+\ldots+\ell^{m-1}}$ which one can check is the (unique) fundamental character of level 1. Part (i) follows by noting that the fundamental character of level 1 is $\chi_\ell|_{I_\ell}$, cf. [Ser72, Prop. 8].

We now prove (ii). Set $T := \mathbb{F}_{\ell^m}^\times$ and define the representation

$$\beta\colon T \to \mathbb{F}_{\ell^m}^\times \subseteq \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^m}), \quad x \mapsto x^{e_1+e_2\ell+\cdots+e_m\ell^{m-1}}.$$

The representation ρ is isomorphic to the one obtained by composing the surjective character $I_\ell \to I_\ell^t \xrightarrow{\phi} T$ with β. The representation β is irreducible since V is an irreducible $\mathbb{F}_\ell[I_\ell]$-module.

Let H be any closed subgroup of I_ℓ satisfying $[I_\ell : H] < \ell - 1$. The subgroup $S := \phi(H)$ of T then satisfies $[T : S] < \ell - 1$.

We can now use the rigidity of tori as described by Hall in [Hal11]. In the language of [Hal11, §2], the amplitude of β is $\max\{e_i\}$ which in our case is 0 or 1. Lemma 3 of [Hal11] and our condition $[T : S] < \ell - 1$ implies that $\beta(T)$ and $\beta(S)$ have the same centralizer in $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^m})$.

Suppose that $\beta|_S\colon S \to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^m})$ is reducible. Since $\ell \nmid |S|$, we have $\mathbb{F}_{\ell^m} = W_1 \oplus W_2$, where W_1 and W_2 are non-zero $\mathbb{F}_\ell$-subspaces fixed under the action of S. Take $A \in \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^m})$ such that $A(w) = w$ for $w \in W_1$ and $A(w) = -w$ for $w \in W_2$. Since A commutes with $\beta(S)$, we deduce that it also commutes with $\beta(T)$. For any $B \in \beta(T)$ and $w \in W_1$, we have $A(Bw) = B(Aw) = Bw$. Therefore, $B(W_1) \subseteq W_1$ for all $B \in \beta(T)$ which contradicts that β is irreducible.

Therefore, the representation $\beta|_S$, and hence also $\rho|_H$, is irreducible. □

6. Irreducibility

For a prime ℓ, the $\mathbb{F}_\ell$-vector space $J[\ell]$ has dimension 6 and comes with a natural $G_\mathbb{Q}$-action. The goal of this section is to prove the following:

Proposition 6.1. *For every odd prime ℓ, the $\mathbb{F}_\ell[G_\mathbb{Q}]$-module $J[\ell]$ is irreducible.*

Suppose that there is an odd prime ℓ such that $J[\ell]$ is a reducible $\mathbb{F}_\ell[G_\mathbb{Q}]$-module; we will try to obtain a contradiction. We first exclude a few possibilities for ℓ.

Lemma 6.2. *We have $\ell \notin \{3, 5, 7, 11, 41, 83\}$.*

Proof. For one of the given primes $\ell \in \{3, 5, 7, 11, 41, 83\}$, it suffices to show that there is a prime $p \notin S \cup \{\ell\}$ such that $P_p(T)$ is irreducible modulo ℓ.

We have computed $P_p(T)$ for several small p, cf. §3. The polynomial $P_{17}(x)$ is irreducible modulo 3. The polynomial $P_{41}(x)$ is irreducible modulo 5. The polynomial $P_2(x)$ is irreducible modulo 7, 11 and 41. The polynomial $P_{19}(x)$ is irreducible modulo 83. □

For the rest of this section, we may thus assume that ℓ is odd and $\ell \notin \{3, 5, 7, 11, 41, 83\}$. In particular, $\ell \notin S$.

Let $V_1, \dots, V_r$ be the composition factors of $J[\ell]$ as an $\mathbb{F}_\ell[G_\mathbb{Q}]$-module; the semisimplification of $J[\ell]$ as an $\mathbb{F}_\ell[G_\mathbb{Q}]$-module is then isomorphic to $V_1 \oplus \cdots \oplus V_r$. We have $r \geq 2$ since $J[\ell]$ is a reducible $\mathbb{F}_\ell[G_\mathbb{Q}]$-module by assumption.

Let

$$\rho_i \colon G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{F}_\ell}(V_i)$$

be the Galois representation corresponding to V_i. Define $d_i = \dim_{\mathbb{F}_\ell} V_i$. We may assume that the V_i have been numbered so that $d_1 \leq \cdots \leq d_r$. We have $\sum_i d_i = 6$, so $d_1 \in \{1, 2, 3, 6\}$. We have $r \geq 2$, so $d_1 \in \{1, 2, 3\}$.

We will rule out the three cases $d_1 \in \{1, 2, 3\}$ separately in §§6.2–6.4. This contradiction will imply that $J[\ell] = V_1$ is an irreducible $\mathbb{F}_\ell[G_\mathbb{Q}]$-module.

6.1. **Determinants.** Fix a finite dimensional $\mathbb{F}_\ell$-vector space W with an action of $G_\mathbb{Q}$ given by a representation $\rho \colon G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{F}_\ell}(W)$. Let $W^\vee$ to be the dual vector space of W and let $\rho^* \colon G_\mathbb{Q} \to \mathrm{Aut}_{\mathbb{F}_\ell}(W^\vee)$ be the contragredient representation, i.e., $\rho^*(\sigma)$ is the transpose of $\rho(\sigma^{-1})$. Let $W^\vee(1)$ be the vector space $W^\vee$ where $G_\mathbb{Q}$ acts via the representation $\chi_\ell \cdot \rho^*$.

Since the pairing $J[\ell] \times J[\ell] \to \mu_\ell$ coming from the Weil pairing and the natural principal polarization of J is non-degenerate, we find that $J[\ell]$ and $J[\ell]^\vee(1)$ are isomorphic $\mathbb{F}_\ell[G_\mathbb{Q}]$-modules. Therefore, the $\mathbb{F}_\ell[G_\mathbb{Q}]$-modules $V_1, \dots, V_r$ are isomorphic to $V_1^\vee(1), \dots, V_r^\vee(1)$, though possibly in a different order.

The following lemma constrains the possibilities for the characters $\det \circ \rho_i \colon G_\mathbb{Q} \to \mathbb{F}_\ell^\times$.

Lemma 6.3.

(i) *For each $1 \leq i \leq r$, there is a unique integer $0 \leq e_i \leq d_i$ such that $\det \circ \rho_i = \chi_\ell^{e_i}$.*
(ii) *We have $\sum_{i=1}^r e_i = 3$.*
(iii) *We have $\{e_1, \dots, e_r\} = \{d_1 - e_1, \dots, d_r - e_r\}$.*
(iv) *If $V_i^\vee(1) \cong V_i$, then d_i is even and $e_i = d_i/2$.*

Proof. Fix an integer $1 \leq i \leq r$. The semi-simplification of V_i as an $\mathbb{F}_\ell[I_\ell]$-module is of the form $W_{i,1} \oplus \cdots \oplus W_{i,s}$, where $W_{i,j}$ is an irreducible $\mathbb{F}_\ell[I_\ell]$-module. By Lemma 5.2(i), the determinant of the action of I_ℓ on $W_{i,j}$ is a character $I_\ell \to \mathbb{F}_\ell^\times$ equal to $\chi_\ell^{e_{i,j}}|_{I_\ell}$ for some integer $0 \leq e_{i,j} \leq \dim_{\mathbb{F}_\ell} W_{i,j}$. Therefore,

$$(\det \circ \rho_i)|_{I_\ell} = \prod_{j=1}^{s} \chi_\ell^{e_{i,j}}|_{I_\ell} = \chi_\ell^{e_i}|_{I_\ell}, \tag{6.1}$$

where $e_i := \sum_{j=1}^s e_{i,j}$. We have $0 \leq e_i \leq \sum_{j=1}^s \dim_{\mathbb{F}_\ell} W_{i,j} = \dim_{\mathbb{F}_\ell} V_i = d_i$. Define the character

$$\alpha_i := (\det \circ \rho_i) \cdot \chi_\ell^{-e_i} \colon G_\mathbb{Q} \to \mathbb{F}_\ell^\times.$$

The representation $\rho_{J,\ell}$, and hence also α_i, is unramified at all primes $p \notin S \cup \{\ell\}$. Since the order of $\mathbb{F}_\ell^\times$ is relatively prime to ℓ, Proposition 4.1 implies that α_i is also unramified at the primes $p \in S$. The character α_i is unramified at the prime ℓ by (6.1). We thus have $\alpha_i = 1$ since $\alpha_i \colon G_\mathbb{Q} \to \mathbb{F}_\ell^\times$ is unramified at all primes and $\mathbb{Q}$ has no non-trivial extensions unramified at all primes. Therefore, $\det \circ \rho_i = \chi_\ell^{e_i}$.

This proves the existence of e_i in (i); it remains to prove the uniqueness. Take any integer $0 \leq f \leq d_i$ such that $\det \circ \rho_i = \chi_\ell^f$. We thus have $\chi_\ell^{f - e_i} = 1$ and hence $f - e_i \equiv 0 \pmod{\ell - 1}$ since χ_ℓ has order $\ell - 1$. We have $d_i \leq 3$ since $r \geq 2$, so $|f - e_i| \leq 3$. Since $|f - e_i| \leq 3 < \ell - 1$ and $f - e_i \equiv 0 \pmod{\ell - 1}$, we must have $f = e_i$.

We now prove part (ii). Since $\det(\rho_{J,\ell}(\mathrm{Frob}_p)) \equiv P_p(0) = p^3 \pmod{\ell}$ for all $p \notin S \cup \{\ell\}$, we have $\det \circ \rho_{J,\ell} = \chi_\ell^3$. Therefore, $\chi_\ell^3 = \prod_{i=1}^r \det \circ \rho_i = \chi_\ell^e$, where $e := \sum_{i=1}^r e_i$. We have $3 - e \equiv 0$

$(\mathrm{mod}\ \ell-1)$ since $\chi_\ell^{3-e}=1$ and χ_ℓ has order $\ell-1$. We have $|3-e|\le 3$ since $0\le e\le\sum_i d_i=6$. Since $3-e\equiv 0\ (\mathrm{mod}\ \ell-1)$ and $|3-e|\le 3<\ell-1$, we conclude that $e=3$ which proves (ii).

We now prove part (iii). Fix an integer $1\le i\le r$. The representation $G_{\mathbb{Q}}\to \mathrm{Aut}_{\mathbb{F}_\ell}(V_i^\vee)$, $\sigma\mapsto\chi_\ell(\sigma)\cdot\rho_i^*(\sigma)$ is isomorphic to $V_i^\vee(1)$ and its determinant is given by

$$G_{\mathbb{Q}}\to\mathbb{F}_\ell^\times,\quad \sigma\mapsto \det(\chi_\ell(\sigma)\rho_i^*(\sigma))=\chi_\ell(\sigma)^{d_i}\det(\rho_i(\sigma^{-1}))=\chi_\ell(\sigma)^{d_i-e_i}.$$

We noted above that the $\mathbb{F}_\ell[G_{\mathbb{Q}}]$-modules $V_1,\dots,V_r$ are isomorphic to $V_1^\vee(1),\dots,V_r^\vee(1)$ though possibly in a different order. Therefore, $\{\chi_\ell^{e_1},\dots,\chi_\ell^{e_r}\}=\{\chi_\ell^{d_1-e_1},\dots,\chi_\ell^{d_r-e_r}\}$. The uniqueness in part (i) implies that $\{e_1,\dots,e_r\}=\{d_1-e_1,\dots,d_r-e_r\}$.

It remains to prove part (iv). If $V_i\cong V_i^\vee(1)$, then the computation above shows that $\det\circ\rho_i$ is equal to both $\chi_\ell^{e_i}$ and $\chi_\ell^{d_i-e_i}$. Therefore, $e_i=d_i-e_i$ by the uniqueness in part (i) and hence $d_i=2e_i$. □

6.2. **One-dimensional case.** Suppose that $d_1=1$. The Galois action on V_1 is described by the character $\rho_1\colon G_{\mathbb{Q}}\to\mathrm{Aut}_{\mathbb{F}_\ell}(V_1)=\mathbb{F}_\ell^\times$. So for any prime $p\notin S\cup\{\ell\}$, $\rho_1(\mathrm{Frob}_p)$ is a root of $P_p(T)\equiv\det(TI-\rho_{J,\ell}(\mathrm{Frob}_p))\ (\mathrm{mod}\ \ell)$. The character ρ_1 is 1 or χ_ℓ by Lemma 6.3(i), so $P_p(1)\equiv 0\ (\mathrm{mod}\ \ell)$ or $P_p(p)\equiv 0\ (\mathrm{mod}\ \ell)$.

With $p=2$ and using the polynomial $P_2(T)$ from §3, we find that $P_2(1)=3\cdot 17$ and $P_2(2)=2^3\cdot 3\cdot 17$. Therefore, $\ell\in\{3,17\}$. However, this contradicts Lemma 6.2.

This completes our proof that the case $d_1=1$ does not occur.

6.3. **Two-dimensional case.** Suppose that $d_1=2$.

Lemma 6.4. *We have $d_i=2$ and $\det\circ\rho_i=\chi_\ell$ for some $1\le i\le r$.*

Proof. Since $d_1=2$, we either have $r=3$ with $d_1=d_2=d_3=2$ or $r=2$ with $d_1=2$ and $d_2=4$. If $r=3$, then Lemma 6.3(i) and (ii) imply that $e_i=1$ for some $1\le i\le 3$ and hence $d_i=2$ and $\det\circ\rho_i=\chi_\ell$. So suppose that $r=2$ and hence $(d_1,d_2)=(2,4)$. Lemma 6.3(iii) implies that $\{e_1,e_2\}=\{2-e_1,4-e_2\}$ and this can only hold if $e_1=1$ and $e_2=2$. Therefore, $d_1=2$ and $\det\circ\rho_1=\chi_\ell$. □

After possibly renumbering the V_i, we may assume by Lemma 6.4 that

$$\rho_1\colon G_{\mathbb{Q}}\to\mathrm{Aut}_{\mathbb{F}_\ell}(V_1)\cong\mathrm{GL}_2(\mathbb{F}_\ell)$$

has determinant χ_ℓ. The following lemma uses Serre's conjecture to relate ρ_1 to a newform of weight 2 and bounded level.

Lemma 6.5. *There exists a newform $f=q+\sum_{n\ge 2}a_n(f)q^n\in S_2(\Gamma_0(N))$ with N dividing $7\cdot 11\cdot 83=6391$ and a maximal ideal λ of the ring of integers of the number field $\mathbb{Q}(a_n(f))$ such that*

$$\mathrm{tr}(\rho_1(\mathrm{Frob}_p))\equiv a_p(f)\pmod{\lambda}$$

for all primes $p\notin S\cup\ell$.

Proof. The 2-dimensional representation ρ_1 is irreducible and is also odd since $\det\rho_1=\chi_\ell$. Serre's conjecture [Ser87], proved by Khare and Wintenberger [KW09a, KW09b], implies that the representation ρ_1 is isomorphic to one arising from some newform f. Moreover, the newform $f=q+\sum_{n\ge 2}a_n(f)q^n$ can be found in $S_k(\Gamma_1(N))$ with prescribed weight k and level N. Let K be the subfield of $\mathbb{C}$ generated by the Fourier coefficients of f; it is a number field. Let $\varepsilon\colon(\mathbb{Z}/N\mathbb{Z})^\times\to K^\times$ be the nebentypus of f. There is thus a maximal ideal λ of the ring of integers of K such that

$$\det(xI-\rho_1(\mathrm{Frob}_p))\equiv x^2-a_p(f)x+\varepsilon(p)p^{k-1}\pmod{\lambda}$$

for all primes $p\nmid N\ell$.

Let us compute the weight k. Suppose that $\rho_1|_{I_\ell}$ is reducible. The semisimplification of $\rho_1|_{I_\ell}$ is then given by two characters $\varphi_1, \varphi_2 \colon I_\ell^t \to \mathbb{F}_\ell^\times$. By Proposition 5.1, each φ_i is either 1 or the fundamental character of level 1. Since the fundamental character of level 1 is $\chi_\ell|_{I_\ell}$, cf. [Ser72, Prop. 8] and $\det \circ \rho_1 = \chi_\ell$, we deduce that $\{\varphi_1, \varphi_2\} = \{1, \chi_\ell|_{I_\ell}\}$. In the notation of §2.3 of [Ser87], we have $a = 0$ and $b = 1$, and hence $k = 1 + \ell a + b = 2$.

Now suppose that $\rho_1|_{I_\ell}$ is irreducible. As explained in §5 (and using Proposition 5.1), $\rho_1|_{I_\ell}$ factor through I_ℓ^t and is then isomorphic to a representation of the form

$$I_\ell^t \xrightarrow{\phi^{e_1+e_2\ell}} \mathbb{F}_{\ell^2}^\times \subseteq \mathrm{Aut}_{\mathbb{F}_\ell}(\mathbb{F}_{\ell^2}),$$

where $\phi \colon I_\ell^t \to \mathbb{F}_{\ell^2}^\times$ is a fundamental character of level 2 and $0 \leq e_1, e_2 \leq 1$. We have $\{e_1, e_2\} = \{0, 1\}$ since otherwise $\phi^{e_1+e_2\ell}$ would have image in $\mathbb{F}_\ell^\times$ which would contradict the irreducibility of $\rho_1|_{I_\ell}$. Therefore, the I_ℓ^t-action on $V_1 \otimes_{\mathbb{F}_\ell} \mathbb{F}_{\ell^2}$ is diagonalizable and is given by the characters $\phi, \phi^\ell \colon I_\ell^t \to \mathbb{F}_{\ell^2}^\times$. In the notation of §2.2 of [Ser87], we may take $a = 0$ and $b = 1$, and hence $k = 1 + \ell a + b = 2$.

We now consider the level N. The representation $\rho_{J,\ell}$, and hence also ρ_1, is unramified at all primes $p \notin S \cup \{\ell\}$. Take any $p \in S$; we have $p \neq \ell$ by Lemma 6.2. Let $V_1^{I_p}$ be the subspace of V_1 fixed by I_p. From [Ser87, §1.2], the Artin conductor of ρ_1 is $N := \prod_{p \in S} p^{n_p}$ where $n_p = \dim_{\mathbb{F}_\ell} V_1/V_1^{I_p}$; there is no wild ramification since the cardinality of $\rho_{J,\ell}(I_p)$ is not divisible by p by Lemma 4.1. Since $\rho_{J,\ell}(I_p)$ is a group of order ℓ by Lemma 4.1, the group $\rho_1(I_p)$ has order 1 or ℓ. If $\rho_1(I_p)$ has order 1, then $n_p = 0$. If $\rho_1(I_p)$ has order ℓ, then it is conjugate in $\mathrm{Aut}_{\mathbb{F}_\ell}(V_1) \cong \mathrm{GL}_2(\mathbb{F}_\ell)$ to the group generated by $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. In this last case, we have $n_p = 1$. This completes the proof that N divides $7 \cdot 11 \cdot 83 = 6391$.

Finally, it remains to show that $f \in S_2(\Gamma_1(N))$ actually lies in $S_2(\Gamma_0(N))$; equivalently, that the nebentypus ε is trivial. Let μ be the image of ε; it is a finite group of roots of unity in K.

With $\mathcal{O}$ the ring of integers of K, the kernel of the reduction modulo λ homomorphism $\mu \to (\mathcal{O}/\lambda)^\times$ is an ℓ-group. For any $p \notin S \cup \{\ell\}$, the equality $\det \circ \rho_1 = \chi_\ell$ implies that $\varepsilon(p)p \equiv \chi_\ell(p) = p \pmod{\lambda}$ and hence $\varepsilon(p) \equiv 1 \pmod{\lambda}$. Therefore, μ is an ℓ-group. Since $|\mu|$ divides the cardinality of $(\mathbb{Z}/N\mathbb{Z})^\times \cong (\mathbb{Z}/7\mathbb{Z})^\times \times (\mathbb{Z}/11\mathbb{Z})^\times \times (\mathbb{Z}/83\mathbb{Z})^\times$, we deduce that $\mu = 1$ or $\ell \in \{3, 5, 41\}$. We have $\ell \notin \{3, 5, 41\}$ by Lemma 6.2, so $\mu = 1$ and hence $\varepsilon = 1$. □

Take any prime $p \notin S \cup \{\ell\}$.

Let $H_p(x)$ be the characteristic polynomial of the Hecke operator T_p acting on $S_2(\Gamma_0(6391))$; it is monic with integer coefficients. Take f and λ as in Lemma 6.5. Since $p \nmid 6391$, there is a cusp form $f' \in S_2(\Gamma_0(6391))$ such that $T_p(f') = a_p(f)f'$; we can take f' to be an oldform if N properly divides 6391. Therefore, $H_p(a_p(f)) = 0$ and in particular $H_p(a_p(f)) \equiv 0 \pmod{\lambda}$. Lemma 6.5 then implies that $\mathrm{tr}(\rho_1(\mathrm{Frob}_p)) \in \mathbb{F}_\ell$ is a root of $H_p(x)$.

Let $P_p(T)$ be the polynomial from §3. Define the polynomial $Q_p(x) := \prod_\alpha (x - \alpha)$, where α runs over the values $\lambda + p/\lambda$ with $\lambda \in \overline{\mathbb{Q}}$ being a root of $P_p(x)$. The polynomial $Q_p(x)$ is monic with integer coefficients. Since $\det(\rho_1(\mathrm{Frob}_p)) = \chi_\ell(\mathrm{Frob}_p) \equiv p \pmod{\ell}$, we have $\mathrm{tr}(\rho_1(\mathrm{Frob}_p)) = \lambda + p/\lambda$ for some root $\lambda \in \overline{\mathbb{F}}_\ell$ of $P_p(T)$. Therefore, $\mathrm{tr}(\rho_1(\mathrm{Frob}_p)) \in \mathbb{F}_\ell$ is a root of $Q_p(x)$ modulo ℓ.

A computation show that $Q_2(x) = x^3 + 3x^2 - 3$ for $Q_5(x) = x^3 + 4x^2 - 5x - 23$. For example, the following code gives $Q_2(x)$; one could also compute $Q_2(x)$ using approximations for the roots of $P_2(T)$ in $\mathbb{C}$ and use that $Q_2(x)$ has integer coefficients.

```
_<T>:=PolynomialRing(Rationals());
p:=2;  P:=T^6+3*T^5+6*T^4+9*T^3+12*T^2+12*T+8;
K:=SplittingField(P); Pol<x>:=PolynomialRing(K);
```

```
&*[x-a : a in {r[1]+p/r[1]: r in Roots(Pol!P)}];
```

Let r_p be the resultant of $H_p(x)$ and $Q_p(x)$; it is an integer. Since $\mathrm{tr}(\rho_1(\mathrm{Frob}_p)) \in \mathbb{F}_\ell$ is a common root of $H_p(x)$ and $Q_p(x)$, we deduce that ℓ divides r_p.

The `Magma` code below shows that the greatest common divisor of r_2 and r_5 is 3^{16}.

```
Pol<x>:=PolynomialRing(Rationals());
S:=CuspForms(Gamma0(7*11*83),2);
H2:=Pol!HeckePolynomial(S,2);
H5:=Pol!HeckePolynomial(S,5);
r2:=Integers()!Resultant(H2,x^3+3*x^2-3);
r5:=Integers()!Resultant(H5,x^3+4*x^2-5*x-23);
GCD([r2,r5]) eq 3^16;
```

Since ℓ divides r_2 and r_5, we must have $\ell = 3$. However, this is impossible by Lemma 6.2. This shows that the case $d_1 = 2$ does not occur.

Remark 6.6. To compute the Hecke polynomials, one could also use modular symbols (in our case, `Magma` does this approach much faster). For example, one can compute $H_2(x)$ by the code:

```
M:=CuspidalSubspace(ModularSymbols(7*11*83,2,1));
CharacteristicPolynomial(HeckeOperator(M,2));
```

We are not using $p = 3$ in the above computations because $r_3 = 0$.

6.4. **Three-dimensional case.** Suppose that $d_1 = 3$, and hence $r = 2$ with $d_1 = d_2 = 3$. After possibly swapping V_1 and V_2, we may assume by Lemma 6.3 that there is an integer $e \in \{0, 1\}$ such that $\det \circ \rho_1 = \chi_\ell^e$.

Lemma 6.7. *Take any prime $p \notin S \cup \{\ell\}$. If $\alpha, \beta, \gamma \in \overline{\mathbb{F}}_\ell$ are the roots of $\det(xI - \rho_1(\mathrm{Frob}_p)) \in \mathbb{F}_\ell[x]$, then $p/\alpha, p/\beta, p/\gamma \in \overline{\mathbb{F}}_\ell$ are the roots of $\det(xI - \rho_2(\mathrm{Frob}_p))$.*

Proof. With notation as in the beginning of §6.1, the roots of the characteristic polynomial of $\rho_1^*(\mathrm{Frob}_p)$ in $\mathbb{F}_\ell[x]$ are $1/\alpha$, $1/\beta$ and $1/\gamma$. Therefore, the roots of the characteristic polynomial of $\chi_\ell(\mathrm{Frob}_p)\rho_1^*(\mathrm{Frob}_p) = p\rho_1^*(\mathrm{Frob}_p)$ are p/α, p/β and p/γ. It thus suffices to show that V_2 and $V_1^\vee(1)$ are isomorphic $\mathbb{F}_\ell[G_\mathbb{Q}]$-modules. The $\mathbb{F}_\ell[G]$-modules $V_1^\vee(1)$ is isomorphic to V_1 or V_2. By Lemma 6.3(iv), we must have $V_2 \cong V_1^\vee(1)$. □

Take any prime $p \notin S \cup \{\ell\}$ and let $\alpha, \beta, \gamma \in \overline{\mathbb{F}}_\ell$ be the roots of $\det(xI - \rho_1(\mathrm{Frob}_p)) \in \mathbb{F}_\ell[x]$. Define the values $u := \alpha + \beta + \gamma$ and $v := \alpha\beta + \alpha\gamma + \beta\gamma$; they belong to $\mathbb{F}_\ell$. We have $\alpha\beta\gamma = \det(\rho_1(\mathrm{Frob}_p)) = \chi_\ell(\mathrm{Frob}_p)^e \equiv p^e \pmod{\ell}$.

Using Lemma 6.7 and $\alpha\beta\gamma = p^e$, we find that the polynomial $P_p(T)$ modulo ℓ is equal to

$$\begin{aligned}
&(T-\alpha)(T-\beta)(T-\gamma)(T-p/\alpha)(T-p/\beta)(T-p/\gamma)\\
=&(T^3 - uT^2 + vT - p^e)(T^3 - p^{1-e}vT^2 + p^{2-e}uT - p^{3-e})\\
=&T^6 - (p^{1-e}v + u)T^5 + (p^{2-e}u + p^{1-e}uv + v)T^4 - (p^{3-e} + p^{2-e}u^2 + p^{1-e}v^2 + p^e)T^3 + \dots.
\end{aligned}$$

With $p = 2$ and using the coefficients of $P_2(T)$ given in §3, we find that for some $e \in \{0, 1\}$, there are $u, v \in \mathbb{F}_\ell$ such that

$$2^{1-e}v + u = -3, \quad 2^{2-e}u + 2^{1-e}uv + v = 6, \quad 2^{3-e} + 2^{2-e}u^2 + 2^{1-e}v^2 + 2^e = -9. \tag{6.2}$$

First consider the case $e = 1$. The equations (6.2) become

$$v + u + 3 = 0, \quad 2u + uv + v - 6 = 0, \quad 2u^2 + v^2 + 15 = 0.$$

Substituting $v = -3 - u$ into the last two equations and using $\ell \neq 3$, we obtain $u^2 + 2u + 9 = 0$ and $u^2 + 2u + 8 = 0$. Therefore, $1 = (u^2 + 2u + 9) - (u^2 + 2u + 8) = 0 - 0 = 0$ which gives a contradiction.

We thus have $e = 0$. The equations (6.2) become

$$2v + u + 3 = 0, \quad 4u + 2uv + v - 6 = 0, \quad 4u^2 + 2v^2 + 18 = 0.$$

Substituting $u = -2v - 3$ into the last two equations and using $\ell > 3$, we obtain $4v^2 + 13v + 18 = 0$ and $3v^2 + 8v + 9 = 0$. Therefore,

$$0 = 3(4v^2 + 13v + 18) - 4(3v^2 + 8v + 9) = 7v + 18.$$

Since $\ell \neq 7$, we have $v = -18/7$. So $0 = 3v^2 + 8v + 9 = 3^4 5/7^2$ in $\mathbb{F}_\ell$, which is a contradiction since $\ell > 7$.

This shows that the case $d_1 = 3$ does not occur.

7. Primitivity

In this section, we prove the following:

Proposition 7.1. *The action of $G_\mathbb{Q}$ on $J[\ell]$ is primitive for all odd primes ℓ.*

Suppose that there is an odd prime ℓ for which the action of $G_\mathbb{Q}$ on $J[\ell]$ is imprimitive. Hence there is an integer $r \geq 2$ and non-zero $\mathbb{F}_\ell$-subspaces $W_1, \ldots, W_r$ of $J[\ell]$ such that $J[\ell] = W_1 \oplus \cdots \oplus W_r$ and such that

$$\{\sigma(W_1), \ldots, \sigma(W_r)\} = \{W_1, \ldots, W_r\}$$

for all $\sigma \in G_\mathbb{Q}$. The $G_\mathbb{Q}$-action on the set $\{W_1, \ldots, W_r\}$ must be transitive since $G_\mathbb{Q}$ acts irreducibly on $J[\ell]$ by Proposition 6.1. In particular, $\dim_{\mathbb{F}_\ell} W_i$ is independent of i and hence equals $6/r$. Therefore, $r \in \{2, 3, 6\}$.

Lemma 7.2. *We have $\ell \notin \{3, 5, 7, 11, 83\}$.*

Proof. Suppose $\ell \in \{3, 5, 7, 11, 83\}$. We claim that there is a prime $p \notin S \cup \{\ell\}$ such that the polynomial $P_p(x) = x^6 + a_p x^5 + b_p x^4 + c_p x^3 + p b_p x^2 + p^2 a_p x + p^3$ is irreducible in $\mathbb{F}_\ell[x]$ and such that $\ell \nmid a_p$. From the polynomials given in §3, the claim is true with $p = 2$ if $\ell \in \{7, 11\}$, $p = 17$ if $\ell \in \{3\}$, $p = 19$ if $\ell \in \{83\}$ and $p = 43$ if $\ell \in \{5\}$.

We have $\operatorname{tr}(\rho_{J,\ell}(\mathrm{Frob}_p)) \equiv -a_p \not\equiv 0 \pmod{\ell}$. The matrix $\rho_{J,\ell}(\mathrm{Frob}_p)$ permutes the spaces $W_1, \ldots, W_r$. The matrix $\rho_{J,\ell}(\mathrm{Frob}_p)$ thus stabilizes some W_j since otherwise $\operatorname{tr}(\rho_{J,\ell}(\mathrm{Frob}_p)) = 0$. However, this is impossible since $\det(xI - \rho_{J,\ell}(\mathrm{Frob}_p)) \equiv P_p(x) \pmod{\ell}$ is irreducible. Therefore, $\ell \notin \{3, 5, 7, 11, 83\}$. □

The action of $G_\mathbb{Q}$ on the set $\{W_1, \ldots, W_r\}$ can be expressed as a representation

$$\varphi \colon G_\mathbb{Q} \to \mathfrak{S}_r,$$

i.e., $\sigma(W_i) = W_{\varphi(\sigma)i}$ for $1 \leq i \leq r$ and $\sigma \in G_\mathbb{Q}$.

Lemma 7.3. *The representation φ is unramified at all primes p.*

Proof. The representation φ factors through $\rho_{J,\ell}$. Therefore, φ is unramified at all primes $p \in S \cup \{\ell\}$. Suppose that $p \in S$. Since $\ell \notin S$ by Lemma 7.2, we have $p \neq \ell$ and hence $\rho_{J,\ell}(I_p)$ has order ℓ by Proposition 4.1. Therefore, $\varphi(I_p)$ has order 1 or ℓ. We have $r \leq 6$, so ℓ does not divide $|\mathfrak{S}_r| = r!$ by Lemma 7.2. Therefore, $\varphi(I_p) = 1$.

Finally suppose that $p = \ell$ and $p \notin S$. We have $\ell \nmid |\varphi(I_\ell)|$ since $\ell \nmid |\mathfrak{S}_r|$. Therefore, $\varphi(I_\ell) \subseteq \mathfrak{S}_r$ is cyclic of order at most $r \leq 6$ (as noted in §5, the tame inertia group at ℓ is pro-cyclic). Let H be the kernel of $\varphi|_{I_\ell}$; we have $[I_\ell : H] = |\varphi(I_\ell)| \leq 6 < \ell - 1$.

Take any $i \in \{1, \ldots, r\}$. The group H acts on W_i so there is an irreducible H-submodule $\mathcal{W}_i$ of W_i. Define $\mathcal{V}_i := \sum_{\sigma \in I_\ell} \sigma(\mathcal{W}_i)$; it is an irreducible I_ℓ-module. Lemma 5.2(ii) and $[I_\ell : H] < \ell - 1$ implies that $\mathcal{V}_i = \mathcal{W}_i$. For any $\sigma \in I_\ell$, we have $\sigma(\mathcal{W}_i) = \mathcal{W}_i \subseteq W_i$. Since I_ℓ permutes the spaces $W_1, \ldots, W_r$, we deduce that $\sigma(W_i) = W_i$ for all $\sigma \in I_\ell$. Since i was arbitrary, we find that I_ℓ acts on all the spaces W_i and hence $\varphi(I_\ell) = 1$. □

Since $\mathbb{Q}$ has no non-trivial extensions unramified at all primes, Lemma 7.3 implies that $\varphi = 1$. Therefore, $\sigma(W_i) = W_i$ for all $\sigma \in G_{\mathbb{Q}}$ and $1 \leq i \leq r$. However, this implies that the action of $G_{\mathbb{Q}}$ on $J[\ell]$ is reducible which contradicts Proposition 6.1. Therefore, the action of $G_{\mathbb{Q}}$ on $J[\ell]$ is in fact primitive and this completes the proof of Proposition 7.1.

8. Proof of Theorem 1.1

Take any odd prime ℓ. The group $\rho_{J,\ell}(G_{\mathbb{Q}}) \subseteq \mathrm{GSp}_6(\mathbb{F}_\ell)$ contains a transvection by Proposition 4.1. By Propositions 6.1 and 7.1, the representation $\rho_{J,\ell}$ is irreducible and primitive. By Proposition 2.2, we deduce that $\rho_{J,\ell}(G_{\mathbb{Q}}) \supseteq \mathrm{Sp}_6(\mathbb{F}_\ell)$. We also have $\rho_{J,2}(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\mathbb{F}_2)$ by Lemma 3.2.

From Proposition 2.1, we can now conclude that $\rho_J(G_{\mathbb{Q}}) = \mathrm{GSp}_6(\widehat{\mathbb{Z}})$.

References

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265. Computational algebra and number theory (London, 1993). ↑1.2

[BMS67] H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for* SL_n $(n \geq 3)$ *and* Sp_{2n} $(n \geq 2)$, Inst. Hautes Études Sci. Publ. Math. **33** (1967), 59–137. MR0244257 (39 #5574) ↑2.4

[Car08] Xavier Caruso, *Conjecture de l'inertie modérée de Serre*, Invent. Math. **171** (2008), no. 3, 629–699. MR2372809 (2008j:14034) ↑5

[CCN+85] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, and R. A. Wilson, *Atlas of finite groups*, Oxford University Press, Eynsham, 1985. Maximal subgroups and ordinary characters for simple groups, With computational assistance from J. G. Thackray. MR827219 (88g:20025) ↑3.3

[Cha97] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180. MR1440067 (99d:11071) ↑2.1

[Del77] P. Deligne, *Cohomologie étale*, Lecture Notes in Mathematics, Vol. 569, Springer-Verlag, Berlin, 1977. Séminaire de Géométrie Algébrique du Bois-Marie SGA 4 1/2, Avec la collaboration de J. F. Boutot, A. Grothendieck, L. Illusie et J. L. Verdier. MR0463174 (57 #3132) ↑4

[Die02] Luis V. Dieulefait, *Explicit determination of the images of the Galois representations attached to abelian surfaces with* $\mathrm{End}(A) = \mathbb{Z}$, Experiment. Math. **11** (2002), no. 4, 503–512 (2003). MR1969642 (2004b:11069) ↑1.1

[FK88] Eberhard Freitag and Reinhardt Kiehl, *Étale cohomology and the Weil conjecture*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 13, Springer-Verlag, Berlin, 1988. Translated from the German by Betty S. Waterhouse and William C. Waterhouse, With an historical introduction by J. A. Dieudonné. MR926276 (89f:14017) ↑3.1, 4

[Gre10] Aaron Greicius, *Elliptic curves with surjective adelic Galois representations*, Experiment. Math. **19** (2010), no. 4, 495–507. MR2778661 ↑2.5

[Hal08] Chris Hall, *Big symplectic or orthogonal monodromy modulo* ℓ, Duke Math. J. **141** (2008), no. 1, 179–203. MR2372151 (2008m:11112) ↑2.2

[Hal11] ———, *An open-image theorem for a general class of abelian varieties*, Bull. Lond. Math. Soc. **43** (2011), no. 4, 703–711. With an appendix by Emmanuel Kowalski. MR2820155 (2012f:11115) ↑1.1, 2.2, 5

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504. MR2551763 (2010k:11087) ↑6.3

[KW09b] ———, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586. MR2551764 (2010k:11088) ↑6.3

[LT76] Serge Lang and Hale Trotter, *Frobenius distributions in* GL_2*-extensions*, Lecture Notes in Mathematics, Vol. 504, Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers. MR0568299 (58 #27900) ↑1

[Lom15] Davide Lombardo, *Explicit open image theorems for some abelian varieties with trivial endomorphism ring*, 2015. arXiv:1508.01293 [math.NT]. ↑1.3

[ALS15] Samuele Anni Anni, Pedro Lemos, and Samir Siksek, *Residual representations of semistable principally polarized abelian varieties*, 2015. arXiv:1508.00211 [math.NT]. ↑1.3

[Mil80] James S. Milne, *Étale cohomology*, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980. MR559531 (81j:14002) ↑4

[Ray74] Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280. MR0419467 (54 #7488) ↑5

[Rib75] Kenneth A. Ribet, *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275. MR0419358 (54 #7379) ↑2.4

[Ser72] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331. MR0387283 (52 #8126) ↑2.5, 5, 5, 6.3

[Ser87] ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230. MR885783 (88g:11022) ↑6.3

[SGA7-II] *Groupes de monodromie en géométrie algébrique. II*, Lecture Notes in Mathematics, Vol. 340, Springer-Verlag, Berlin-New York, 1973. Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 II), Dirigé par P. Deligne et N. Katz. MR0354657 (50 #7135) ↑4

[Vas04] Adrian Vasiu, *Surjectivity criteria for p-adic representations. II*, Manuscripta Math. **114** (2004), no. 4, 399–422. MR2081941 (2005g:11235) ↑2.4

[ZS76] A. E. Zalesskiĭ and V. N. Serežkin, *Linear groups generated by transvections*, Izv. Akad. Nauk SSSR Ser. Mat. **40** (1976), no. 1, 26–49, 221. MR0412295 (54 #421) ↑2.2

[ZBZ15] David Zureick-Brown and David Zywina, *Abelian varieties with maximal monodromy*, 2015. preprint. ↑1

[Zyw11] David Zywina, *A refinement of Koblitz's conjecture*, Int. J. Number Theory **7** (2011), no. 3, 739–769. MR2805578 (2012e:11107) ↑1

Department of Mathematics, Cornell University, Ithaca, NY 14853
E-mail address: zywina@math.cornell.edu