On the Irreducibility of Galois Representations Associated to Elliptic Curves

Eric Larson and Dmitry Vaintrob

Abstract

Given an elliptic curve E over a number field K, and a prime number ℓ, the ℓ-torsion points define a representation $\rho_{E,\ell} : \mathrm{Gal}(\overline{K}/K) \to \mathrm{GL}_2(\mathbb{F}_\ell)$. It is a well-known theorem of Serre that this representation is surjective — and in particular irreducible — for all but finitely many ℓ. In this paper, we prove a theorem regarding the irreducibility (over the algebraic closure of $\mathbb{F}_\ell$) of this representation. It follows from our theorem that if K does not contain the class field of an imaginary quadratic field F, then for primes ℓ more than a bound depending only on the field K, the representation $\rho_{E,\ell}$ is irreducible.

From this, we can deduce a generalization of the well-known theorem of Mazur that the degree of an isogeny $E \to E'$ of elliptic curves defined over $\mathbb{Q}$ of prime degree is bounded by an absolute constant. Namely, we prove that the degrees of prime degree isogenies of elliptic curves defined over K are bounded by a constant depending on K if and only if K does not contain the class field of an imaginary quadratic field F, i.e. if and only if there is no CM curve defined over K whose CM field is contained in K.

1 Introduction

Let E be an elliptic curve over a number field K, and for each prime number ℓ, let

$$\rho_{E,\ell} : G = \mathrm{Gal}(\overline{\mathbb{Q}}/K) \to \mathrm{GL}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$$

be the associated Galois representation on ℓ-torsion points. These representations reflect many geometric properties of E, such as its primes of bad reduction and the number of points of E over finite fields, as well as possible isogenies of E. In particular, there exists an isogeny $E \to E'$ of prime degree ℓ if and only if $\rho_{E,\ell}$ is reducible over $\mathbb{F}_\ell$. In particular, if $\rho_{E,\ell}$ is irreducible (over the algebraic closure of $\mathbb{F}_\ell$), there can be no isogenies $E \to E'$ of prime degree ℓ. In this paper, we study the reducibility of the representations $\rho_{E,\ell}$.

Definition 1. For the remainder of the paper, we say that the representation $\rho : G \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is *reducible* if it is reducible over the algebraic closure of $\mathbb{F}_\ell$.

Definition 2. The *semi-simplification* $\widetilde{\rho}$ of a representation ρ is defined to be the direct sum of the Jordan-Holder quotients of ρ.

Note that When $\rho_{E,\ell}$ is reducible, then its semi-simplification $\widetilde{\rho}_{E,\ell}$ is abelian. The purpose of this paper is to prove the following theorem.

Theorem 1. *Let K be a number field. Then, there exists an effectively computable constant C_K depending only on K such that for any prime number $\ell > C_K$ and any elliptic curve E such that the ℓ-torsion representation $\rho_{E,\ell}$ is reducible, there exists an elliptic curve E' over K with CM defined over K such that*

$$\widetilde{\rho}^{12}_{E,\ell} \simeq \rho^{12}_{E',\ell}$$

Remark 1. If we start with the assumption that E has a degree ℓ^k cyclic isogeny then the same analysis should give a bound on k, even when $p = 2$ or 3.

Remark 2. If $E = E'$ is CM curve with CM defined over K, then $\rho_{E,\ell}$ is abelian, and hence isomorphic to its own semi-simplification.

Corollary 1. *The degrees of isogenies of elliptic curves over K are bounded if and only if K does not contain the class field of an imaginary quadratic field F.*

When $\rho_{E,\ell}$ is reducible, then its semi-simplification $\widetilde{\rho}_{E,\ell}$ is abelian; in particular it is diagonalizable over $\overline{\mathbb{F}_\ell}$ as

$$\widetilde{\rho}_{E,\ell} = \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_2 \end{pmatrix}$$

where

$$\psi_i : \mathbb{I} \to G \to \overline{\mathbb{F}_\ell}^* \simeq \overline{\mathbb{Q}}/\mathfrak{p}_\ell$$

are the two "eigencharacters" of $\widetilde{\rho}_{E,\ell}$. Here, $\mathfrak{p}_\ell$ is a fixed prime ideal of $\overline{\mathbb{Q}}$ lying over ℓ, and $\mathbb{I}$ is the group if idèles of K (which surjects onto G by class field theory, since $\widetilde{\rho}_{E,\ell}$ is abelian). By the Weil pairing, the two characters satisfy $\psi_1\psi_2 = \mathrm{cyc}_\ell$, the cyclotomic character defined by the extension $K[\zeta_\ell]$.

To prove theorem 1, we study these eigencharacters: When ℓ is sufficiently large (more than some constant depending only on K), we use algebraic geometry to patch together local information about these characters, and show that up to a twist by a 12th root of unity, these eigencharacters have a particularly simple form. Namely, for some imaginary quadratic subfield $F \subset K$, the characters ψ_i are equal to Nm^K_F (times a 12th root of unity) and its conjugate. In particular, the norm map $\mathrm{Cl}(K) \to \mathrm{Cl}(F)$ is zero, and hence K contains the Hilbert class field of F.

2 Action of Inertia Groups

In this section, we study the ramification of the eigencharacters ψ_1 and ψ_2, and explicitly determine ψ_i^{12} on all inertia subgroups in terms of a certain algebraic character θ^S. In the following, we will sometimes drop the subscript from ψ_i and write just $\psi : \mathbb{I} \to \mathbb{F}_\ell$ to denote either ψ_1 or ψ_2.

If $v \in \Sigma_K \setminus \Sigma_E$ is a place of good reduction for E, and π_v is a uniformizer at v, then we have a well-defined value for $\psi(\pi_v)$ (as ρ_ℓ is unramified), and this means that the $\psi_i(\pi_v)$ are roots of the frobenius polynomial, i.e.

$$P_v(\psi_i(\pi_v)) \equiv 0 \mod \ell \quad \text{where} \quad P_v(x) = x^2 - \mathrm{Tr}_E(v)x + \mathrm{Nm}_{\mathbb{Q}}^K v$$

is a polynomial with integer coefficients and nonpositive discriminant.

In fact, by slightly re-defining the frobenius polynomial and twisting $\psi(\pi_v)$ by 12^{th} roots of unity, we can make sense of this for primes v of bad reduction as well. Namely, we have the following lemma.

Lemma 1. *Let $v \in \Sigma_K \setminus \Sigma_\ell$ be any prime not dividing ℓ. Then ψ^{12} is unramified at v and there exists a polynomial with integer coefficients*

$$P_v = x^2 + a_v x + \mathrm{Nm}_{\mathbb{Q}}^K(v) \in \mathbb{Z}[x]$$

such that

1. *If v has potentially good reduction, then P_v has nonpositive discriminant.*
2. *If v has potentially multiplicative reduction, then $P_v = (x \pm 1)(x \pm \mathrm{Nm}_{\mathbb{Q}}^K(v))$.*
3. *There exists $\zeta \in \overline{\mathbb{F}_\ell}$ a $12th$ root of unity such that $P_v(\zeta\psi_i(f_v)) \equiv 0$ mod ℓ.*

Remark 3. Note that in the above, either $a_v = \pm(\mathrm{Nm}(v) + 1)$ or P_v has nonpositive discriminant and $a_v \leq 2\sqrt{\mathrm{Nm}(v)}$, so there are only finitely many possibilities for P_v as (E, ℓ) varies over all curves for which $\rho_{E,\ell}$ is reducible.

Proof. Most of this proof is done in the paper [3].

First suppose v has potentially multiplicative reduction. After possibly taking a quadratic extension L_w of K_v, we have (as a w-adic variety) E isomorphic to a Tate curve $\overline{L}_w^*/\alpha^{\mathbb{Z}}$ where α is some element of nonzero valuation. In particular, the image of the valuation $w : E[\ell] \to \mathbb{Q}/w(\alpha)\mathbb{Z}$ is isomorphic to $\mathbb{Z}/\ell\mathbb{Z}$ with trivial G_v-action. As all semisimplifications are isomorphic, either ψ_1 or ψ_2 becomes trivial after taking a quadratic extension, and hence has values in ± 1. The other character then has to evaluate on (any choice of) the uniformizer π_v to $\pm\,\mathrm{cyc}_\ell(\pi_v) = \pm\,\mathrm{Nm}_{\mathbb{Q}}(v)$ as $v \nmid \ell$. This proves the statement of the lemma in the potentially multiplicative case, with $\zeta = \pm 1$. (This implies that ψ_i^2, hence also ψ_i^{12} are unramified at v.)

Now suppose v has potentially good reduction. Then by [3] the image of inertia $I_v \subset G$ under ρ_ℓ is either a cyclic group Φ of order 2, 3, 4, or 6, or a nonabelian group of order 8, 12 or 24 (and indeed the image under ρ_ℓ must be isomorphic for all primes $\ell \geq 5, \ell \neq p_v$.) The last three cases are impossible when $\ell \geq 5$ since any nonabelian subgroup of the borel group $B \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ contains a copy of $\mathbb{Z}/\ell\mathbb{Z}$ (the unipotent matrices). Hence the image Φ must be abelian and a subgroup of $\mathbb{Z}/12\mathbb{Z}$. Thus, there exists a (non-unique) totally ramified local extension L_w of K_v whose galois group is Φ and over which ρ_1 is unramified (this is true by local class field theory, since $\mathrm{Gal}^{\mathrm{ab}}(\overline{K_v}/K_v) = K_v^* \cong \mathcal{O}_v^* \oplus \mathbb{Z}$ noncanonically, and so we can extend a subgroup of $\mathcal{O}_v^*$ to a subgroup of K^* with the same quotient.) The prime w has good reduction for E and $\mathrm{Nm}_{K_v}^{L_w}(w) = v$. Since L_w/K_v has degree dividing 12, we see that ψ_i^{12} is unramified outside of ℓ. □

Definition 3. Define $P_{v^{12}}$ to be the quadratic polynomial whose roots are the 12th powers of the roots of P_v.

Remark 4. Note that $P_{v^{12}}$ is equal mod ℓ to the characteristic polynomial of $\psi(v)^{12}$ (the root of unity gets absorbed in the twelfth power).

The above lemma characterized the actions of the ψ_i on the inertia groups G_v for $v \nmid \ell$. We now deal with the case $v \mid \ell$. Let $U \subset \mathbb{I}$ be the group of units. Suppose $v \in \Sigma_\ell$. Let Γ be the set of embeddings $\sigma : K \to \overline{\mathbb{Q}}$, and for a subset $S \subset \Gamma$ define

$$\theta^S = \prod_{\sigma \in S} \sigma : K^* \to \overline{\mathbb{Q}}^*,$$

a map of algebraic groups over $\mathbb{Q}$. We will often abuse notation, speaking of θ^S both as a map of group schemes and as the corresponding map on their $\mathbb{Q}$-points, and it should be clear from context which is meant. Note that θ (both as a scheme and on points) factors through the galois closure $(K^{\mathrm{gal}})^* \subset \overline{\mathbb{Q}}^*$.

For the remainder of the paper, we fix an ideal $\mathfrak{p}_\ell \subset \mathcal{O}_{\overline{\mathbb{Q}}}$ extending $(\ell) \subset \mathbb{Z}$. We identify $\overline{\mathbb{F}_\ell}$ with $\mathcal{O}_{\overline{\mathbb{Q}}}/\mathfrak{p}_\ell$ and $\overline{\mathbb{Q}_\ell}$ with the completion of $\overline{\mathbb{Q}}$ at $\mathfrak{p}_\ell$. Now given a map over $\mathbb{Q}$ of algebraic groups $\theta : K^* \to \overline{\mathbb{Q}}^*$, we can give a map

$$\theta_\ell : \prod_{v \mid \ell} K_v \to \overline{\mathbb{Q}_\ell}.$$

defined by the composition

$$\prod_{v|\ell} K_v^* \xrightarrow{\simeq} (K \otimes \mathbb{Q}_\ell)^* \xrightarrow{\theta \otimes \mathrm{id}} (\overline{\mathbb{Q}} \otimes \mathbb{Q}_\ell)^* \xrightarrow{\simeq} \prod_{\mathfrak{p}|\ell} (\overline{\mathbb{Q}})_{\mathfrak{p}}^* \longrightarrow (\overline{\mathbb{Q}})_{\mathfrak{p}_\ell}^* \xrightarrow{\simeq} \overline{\mathbb{Q}_\ell}^*$$

For primes $v \mid \ell$, we define $\theta_v : K_v^* \to \overline{\mathbb{Q}_\ell}^*$ to be the composition of θ_ℓ with $K_v^* \hookrightarrow \prod_{v|\ell} K_v^*$.

Lemma 2. *There is a subset $S \subset \Gamma$ such that the restriction $\psi|_U = (\theta_\ell^S \cdot \epsilon)^{-1}$ where ϵ takes values in μ_{12}.*

Proof. The case where E is semistable is done in [2], lemma 4 of section 4.2 (in which case we can take ϵ to be the trivial character). Here, we essentially reduce to this case.

Since we have fixed a prime ideal $\mathfrak{p}_\ell$ of $\overline{\mathbb{Q}}$ extending $(\ell) \subset \mathbb{Z}$, we have that S is canonically identified with $\bigcup_{v|\ell} \Gamma_v$, where Γ_v is the set of embeddings $K_v \hookrightarrow \overline{\mathbb{Q}_\ell}$. Thus, it suffices to show that for all $v \mid \ell$, there is some subset $S_v \subset \Gamma_v$ and some character $\epsilon : \mathcal{O}_{K_v}^* \to \mu_{12}$ such that

$$\psi(u) = (\theta_v^{S_v}(u) \cdot \epsilon(u))^{-1} \qquad \text{for } u \in \mathcal{O}_{K_v}^*.$$

To do this, let $p \neq \ell$ be an odd prime number, and let L_w be the extension of local fields obtained by adjoining the p-torsion points of E to K_v. Then, from [3], we know that E is semistable over L_w. Therefore, using the result for the case where E is semistable and taking norms, we have that for some subset $S_w \subset \Gamma_w$,

$$\psi(u) = (\theta_w^{S_w})^{-1}(u) \qquad \text{for } u \in \mathcal{O}_{L_w}^*.$$

Now, we claim that the character $\theta_w^{S_w}$ factors through taking norm down to K_v. To see this, it suffices to examine the construction given in [2] of the the set S_w in the case where E is semistable: Whether we take $f \in S_w$ is determined by the reduction type of E at w, and if the reduction type is supersingular, by how $f : L_w \hookrightarrow \overline{\mathbb{Q}_\ell}$ embedds the unique degree 2 subfield (i.e. the unique subfield isomorphic to $\mathbb{F}_{\ell^2}$) of the residue field of L_w into the residue field of $\overline{\mathbb{Q}_\ell}$. By [2], proposition 12d of section 1.11, if E has supersingular reduction, then the residue field of K_v must be of even degree, since $\widetilde{\rho}_{E,\ell}$ is abelian. Therefore, whether we take $f \in S_w$ depends only the restriction of f to K_v. Thus, the character θ^{S_w} factors through taking norm down to K_v. In other words, for some subset $S_v \subset \Gamma_v$, we have

$$\psi(u) = (\theta_v^{S_v})^{-1}(u) \qquad \text{for } u \in \mathrm{Nm}_{K_v}^{L_w} \mathcal{O}_{L_w}^*.$$

Now, we can finish the proof of this lemma using local class field theory. By the norm limitation theorem, we have

$$\mathrm{Nm}_{K_v}^{L_w} \mathcal{O}_{L_w}^* = \mathrm{Nm}_{K_v}^{L_w^{\mathrm{ab}}} \mathcal{O}_{L_w^{\mathrm{ab}}}^*$$

where L_w^{ab} is the abelianization of L_w, viewed as an extension of K_v. This gives

$$\left[\mathcal{O}_{K_v}^* : \mathrm{Nm}_{K_v}^{L_w} \mathcal{O}_{K_w}^*\right] = \left[\mathcal{O}_{K_v}^* : \mathrm{Nm}_{K_v}^{L_w^{\mathrm{ab}}} \mathcal{O}_{L_w^{\mathrm{ab}}}^*\right] = e\left(L_w^{\mathrm{ab}}/K_v\right) \leq \left|I_v^{\mathrm{ab}}\right|$$

where I_v^{ab} is the abelianization of the inertia subgroup $I_v \subset \mathrm{Gal}(L_w/K_v)$ at v. By the explicit description of the possible inertia subgroups I_v of p-division fields, it follows that $|I_v^{\mathrm{ab}}|$ divides 12, and hence that $\psi(u)$ equals $(\theta_v^{S_v})^{-1}(u)$ on an index 12 subgroup of $\mathcal{O}_{K_v}^*$. Therefore, taking their quotient gives a character $\epsilon : \mathcal{O}_{K_v}^* \to \mu_{12}$, completing the proof. □

Remark 1. When the image of ρ_{E,ℓ^k} is contained in a Borel subgroup, it follows from arguments in [2] that all primes $v \mid \ell$ have either potentially multiplicative or potentially good and non-supersingular reduction. Using this, when ρ_{E,ℓ^k} is contained in a Borel subgroup, we can extend the congruence of characters in the above lemma to hold modulo ℓ^k as opposed to just modulo ℓ.

Definition 4. We will say that the set $S \subset \Gamma$ (and the corresponding algebraic character $\theta : K^* \to \overline{\mathbb{Q}}$) are *associated* to the prime ℓ and the elliptic curve E.

Definition 5. For an idèle x, we define x_ℓ and $x_{\widehat{\ell}}$ to be the idèles whose components at v are given by

$$(x_\ell)_v = \begin{cases} x_v & \text{if } v \mid \ell \\ 1 & \text{if } v \nmid \ell \end{cases} \qquad \text{and} \qquad (x_{\widehat{\ell}})_v = \begin{cases} 1 & \text{if } v \mid \ell \\ x_v & \text{if } v \nmid \ell \end{cases}$$

We also use this notation when $x \in K^*$ (consider x as a principal idèle).

Corollary 1. *Let $x \in K^*$ be relatively prime to ℓ. Then, for some character ϵ which takes values in μ_{12}, we have*

$$\psi(x_{\widehat{\ell}}) \equiv \theta^S(x) \cdot \epsilon(x) \mod \mathfrak{p}_\ell$$

We will show now that for ℓ suffiently large, we must have in fact

$$\theta^S \in \left\{1, \mathrm{Nm}^K_{\mathbb{Q}}, \mathrm{Nm}^K_F, \overline{\mathrm{Nm}^K_F}\right\}$$

where F is some imaginary quadratic subfield whose class field is contained in K.

3 Proof of Theorem 1

For the rest of this section, we fix K and one of the 2^n possible subsets $S \subset \Gamma(K)$. Here we will give ineffective bounds; we will make these arguments effective in an upcoming version of this paper.

Definition 6. We adopt the notation "ℓ sufficiently large" to mean "ℓ bounded by a constant depending only on K."

Lemma 3. *For ℓ sufficiently large, the image $\theta^S(K)^{12} \subset \overline{\mathbb{Q}}$ is contained in a quadratic subfield $F \subset K$.*

Proof. Define $\Theta = (\theta^S)^{12}$. Suppose the image of Θ is not contained in a single quadratic field. Then since K^* is an irreducible variety, there must be an element $x \in K^*$ such that $\Theta(x)$ is not contained in any imaginary quadratic field.

By the Chebotarev density theorem, we know that generators of prime ideals are Zariski dense in K^*. Since Θ is algebraic, we can assume that x generates a prime ideal v. But by the Hasse bound, $\psi(x_{\widehat{\ell}})^{12} = \psi(v)^{12}$ can assume only finitely many possible values as E ranges over all elliptic curves, and all of these values lie in some imaginary quadratic field. Also, by corollary 1, it follows that $\Theta(x)$ is congruent modulo $\mathfrak{p}_\ell$ to $\psi(x_{\widehat{\ell}})^{12}$. Thus, ℓ must divide the norm of their difference, which is nonzero. For ℓ sufficiently large this is impossible, which concludes the proof. ∎

Corollary 2. *For ℓ as above, we must either have $\theta^S = 1$, $\theta^S = \mathrm{Nm}_{\mathbb{Q}}^K$, or $\theta^S = \mathrm{Nm}_F^K$ or its conjugate for some imaginary quadratic subfield $F \subset K$.*

Proof. Since that the $\sigma \in \Gamma$ are algebraically independent over $\mathbb{Q}$, any element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ which fixes $(\theta^S)^{12}$ must fix the set S (under the evident action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on Γ). Thus, the set S must be fixed by the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/F)$, implying the corollary. □

In particular, if K has no imaginary quadratic subfields and ℓ is sufficiently large, we must have $\theta^S \in \{\mathrm{Nm}_{\mathbb{Q}}^K, 1\}$. We will show that this is also the case if K does not contain the class field of any imaginary quadratic subfield.

Lemma 4. *Suppose $F \subset K$ is an imaginary quadratic subfield. Then for sufficiently large ℓ, we can have $\theta^S = \mathrm{Nm}_F^K$ only if the Hilbert class field $H_F \subset K$.*

Proof. Assume to the contrary that H_F is not contained in K. Then the composite $H_F \cdot K$ is a nontrivial extension of K. Therefore, by the Chebotarev density theorem, we can find a prime ideal $v \in K$ which does not split totally in the composite $H_F \cdot K$. Moreover, we can take this prime to be of degree 1, not lie over ℓ, and unramified in $K/\mathbb{Q}$. (Since the set of primes which do not have degree 1, which lie over ℓ, or which are ramified in $K/\mathbb{Q}$ has density zero.)

Now, the ideal $v^{h_K} = (x)$ is principal. Therefore, for any choice of Frobenius element f_v at v, corollary 1 implies

$$\psi(f_v^{h_K})^{12} \equiv (\mathrm{Nm}_F^K x)^{12} \mod \mathfrak{p}_\ell$$

Hence ℓ divides the norm of their difference. By the Hasse bound and lemma 1, there are only finitely many possibilities for the left-hand side as E ranges over all elliptic curves. So if ℓ is sufficiently large, we have

$$\psi(f_v)^{12h_K} = \psi(f_v^{h_K})^{12} = (\mathrm{Nm}_F^K x)^{12}$$

By lemma 1, we can choose the Frobenius element f_v so that $\psi(f_v)$ belongs to some quadratic field F'. Since v was an unramified prime of degree 1, no power of its norm down to F can be generated by an element of $\mathbb{Q}$. Thus, we conclude that the right-hand side lies in F but not in $\mathbb{Q}$. Since the left-hand side lies in the quadratic field F', it follows that $F = F'$. Therefore, we have an equality of ideals of F:

$$(\psi(f_v))^{12h_K} = (\mathrm{Nm}_F^K x)^{12} = (\mathrm{Nm}_F^K v)^{12h_K}$$

Because the group of fractional ideals is torsion-free, this implies

$$(\psi(f_v)) = \mathrm{Nm}_F^K v$$

By assumption, v did not totally split in the composite $H_F \cdot K$ and is of degree 1; hence, $\mathrm{Nm}_F^K v$ does not totally split in H_F, and is therefore a non-principal ideal of F. However, the left-hand side is a principal ideal, which is a contradiction. □

Thus unless K contains the Hilbert class field of an imaginary quadratic subfield, the map θ^S must be either 1 or $\mathrm{Nm}_{\mathbb{Q}}^K$. Suppose $\theta^S \in \{1, \mathrm{Nm}_{\mathbb{Q}}^K\}$. Recall that we've chosen $\psi = \psi_i$ for $i = 1$ or 2. Thus in fact we have two algebraic maps, $\theta^{S_1}, \theta^{S_2} : K^* \to \overline{\mathbb{Q}}^*$. By the Weil pairing, we have

$$\psi_1\psi_2|_U = \mathrm{cyc}_\ell = (\mathrm{Nm}_{\mathbb{Q}}^K)_\ell \quad \Rightarrow \quad \{\theta^{S_1}, \theta^{S_2}\} = \{1, \mathrm{Nm}_{\mathbb{Q}}^K\}$$

for ℓ sufficiently large. Now we prove the following lemma, as a straightforward application of the result of Merel, [1].

Lemma 5. *If ℓ is sufficiently large, we cannot have $\{\theta^{S_1}, \theta^{S_2}\} = \{1, \mathrm{Nm}_{\mathbb{Q}}^K\}$.*

Proof. Assume $\{\theta^{S_1}, \theta^{S_2}\} = \{1, \mathrm{Nm}_{\mathbb{Q}}^K\}$. Fix $i \in \{1, 2\}$ so that $\theta^{S_i} = 1$. This means that $\psi_i|_U = \epsilon$, for some character $\epsilon : U \to \mu_{12}$. The kernel $\ker \epsilon \subset U \subset \mathbb{I}/K^*$ defines an extension M of K of degree dividing $12h_K$. By construction, the galois group $\mathrm{Gal}(K^{\mathrm{ab}}/M)$ is killed by ϵ, so when we consider E as a curve over M, the character ψ_i is trivial. Thus, we have a galois-invariant subspace $V \subset E[\ell]$ such that either V is pointwise fixed by $G_M = \mathrm{Gal}(\overline{K}/M)$, or the quotient $E[\ell]/V$ is pointwise fixed by G_M. In the first case, E has an ℓ-torsion point defined over M, and in the second case, the isogenous curve E/V has an ℓ-torsion point defined over M. Thus, by Merel's theorem [1], we have

$$\ell \leq n_M^{3n_M^2} \leq (12n_K h_K)^{432n_K^2 h_K^2}$$

where $n_M \leq 12n_K h_K$ is the degree of M. This completes the proof of this lemma. □

Theorem 1. *Let K be a number field. Then, there exists an effectively computable constant C_K depending only on K such that for any prime number $\ell > C_K$ and any elliptic curve E such that the ℓ-torsion representation $\rho_{E,\ell}$ is reducible, there exists an elliptic curve E' over K with CM defined over K such that*

$$\tilde{\rho}_{E,\ell}^{12} \simeq \rho_{E',\ell}^{12}$$

Proof. By corollary 2, lemma 4, and lemma 5, for ℓ sufficiently large, we have

$$\left\{\theta^{S_1}, \theta^{S_2}\right\} = \left\{\mathrm{Nm}_F^K, \overline{\mathrm{Nm}_F^K}\right\}$$

for some imaginary quadratic field F such that K contains the Hilbert class field of F. We let E' be the CM curve defined by $\mathbb{C}/\mathcal{O}_F$. By corollary 1, the 12th powers of the eigencharacters of E and E' agree on frobenius elements for prime ideals which are principal, and hence by Chebotarev density agree on $\mathrm{Gal}(\overline{K}/H_K)$. Now, suppose that their 12th powers do not agree on the frobenius element for a prime ideal w. Then, since they agree on $\mathrm{Gal}(\overline{K}/H_K)$, it follows that they do not agree for the frobenius element at any other prime ideal v in the same ideal class as w. Choosing v to be the smallest prime ideal not lying over ℓ which represents the given ideal class, they do not agree for the frobenius element of a prime v of degree 1 not lying over ℓ and not ramified in $K/\mathbb{Q}$, whose norm is bounded independent of E. Then, the same argument as in lemma 4 implies that $(\psi(f_v)) = \mathrm{Nm}_F^K v$, which is a contradiction. □

References

[1] Merel. Bournes pour la Torsion des Courbes Elliptiques sur les Corps de Nombres. *Inventionnes Mathematicae* Volume 124, pp. 437–449.

[2] Serre. Propriétés Galoisiennes des Points d'Ordre Fini des Courbes Elliptiques. *Inventionnes Mathematicae* Volume 15, pp. 259–331.

[3] Serre and Tate. Good Reduction of Abelian Varieties. *The Annals of Mathematics* Volume 88, pp. 492–517.