OPEN CONDITIONS FOR INFINITE MULTIPLICITY EIGENVALUES ON ELLIPTIC CURVES

BO-HAE IM AND MICHAEL LARSEN

Abstract. Let $E$ be an elliptic curve defined over a number field $K$. We show that for each root of unity $\zeta$, the set $\Sigma_\zeta$ of $\sigma \in \text{Gal}(\overline{K}/K)$ such that $\zeta$ is an eigenvalue of infinite multiplicity for $\sigma$ acting on $E(\overline{K}) \otimes \mathbb{C}$ has non-empty interior.

For the eigenvalue $-1$, we can show more: for any $\sigma$ in $\text{Gal}(\overline{K}/K)$, the multiplicity of the eigenvalue $-1$ is either 0 or $\infty$. It follows that $\Sigma_{-1}$ is open.

1. Introduction

Let $K$ be a number field, $\overline{K}$ an algebraic closure of $K$, and $G_K := \text{Gal}(\overline{K}/K)$ the absolute Galois group of $\overline{K}$ over $K$. Let $E$ be an elliptic curve defined over $K$. There is a natural continuous action of $G_K$ on the countably infinite-dimensional complex vector space $V_E := E(\overline{K}) \otimes \mathbb{C}$. The resulting representation decomposes as a direct sum of finite-dimensional irreducible representations in each of which $G_K$ acts through a finite quotient group.

In particular, the action of every $\sigma \in G_K$ on $V_E$ is diagonalizable, with all eigenvalues roots of unity. In [3], the first-named author showed that for generic $\sigma$, every root of unity appears as an eigenvalue of countably infinite multiplicity. This is true both in terms of measure and of Baire category. However, there exist $\sigma$ for which the spectrum is quite different: trivially, the identity and complex conjugation elements; less trivially, examples which can be constructed for an arbitrary set $S$ of primes, such that $\zeta$ is an eigenvalue if and only if every prime factor of its order lies in $S$.

Throughout this paper, we will write $\Sigma_\zeta$ for the subset of $G_K$ consisting of elements $\sigma$ acting as $\zeta$ on an infinite-dimensional subspace of $V_E$ ($E$ and $K$ being fixed). For $\zeta = 1$, a good deal is known. In [2], it is proved that whenever 1 appears as an eigenvalue of $\sigma$ at all, we have $\sigma \in \Sigma_1$. It follows that $\Sigma_1$ is open. By [4], when $K = \mathbb{Q}$, $\Sigma_1$ is all of $G_K$, and

Date: February 8, 2022.

2000 Mathematics Subject Classification. Primary 11G05.
quite possibly this may be true without restriction on $K$. We have already observed that $\Sigma_\zeta \neq G_K$ for $\zeta \neq 1$. We can still hope for positive answers to the following progression of increasingly optimistic questions:

**Question 1.1.** Does $\Sigma_\zeta$ have non-empty interior for all $\zeta$?

**Question 1.2.** Is $\Sigma_\zeta$ open for all $\zeta$?

**Question 1.3.** Do all eigenvalues of $\sigma$ acting on $V_E$ appear with infinite multiplicity?

In this paper, we give an affirmative answer to Question 1.1 for all $\zeta$ and an affirmative answer to all three questions for $\zeta = -1$.

The difficulty in proving such theorems is that placing $\sigma$ in a basic open subset $U$ of $G_K$ amounts to specifying the action of $\sigma$ on a finite Galois extension $L$ of $K$. By the Mordell-Weil theorem, $E(L) \otimes \mathbb{C}$ cannot provide an infinite eigenspace for $\zeta$. Thus, the intersection of eigenspaces

$$\bigcap_{\sigma \in U} V_E^{\sigma-\zeta}$$

is finite-dimensional. Thus, the behavior of a finite collection of rational points must be enough to guarantee the existence of infinitely many linearly independent points on the curve with specified $\sigma$-action.

We would like to thank L. Moret-Bailly and the referee for correcting versions of Proposition 3.1 appearing in earlier drafts of this manuscript.

2. **Multiplicity of the eigenvalue -1**

In this section, we answer Questions 1.2 and 1.3 for $\zeta = -1$.

**Proposition 2.1.** Let $E/K$ be an elliptic curve over $K$. Suppose $-1$ is an eigenvalue of the action of $\sigma \in G_K$ on $V_E$. Then the $-1$-eigenspace of $\sigma$ is infinite-dimensional.

**Proof.** As $-1$ is an eigenvalue of $\sigma$ acting on $V_E$, it is an eigenvalue of $\sigma$ acting on $E(K) \otimes \mathbb{Q}$. Clearing denominators, there exists a non-torsion $P \in E(K)$ such that $\sigma(P) + P \in E(K)_{\text{tor}}$. Replacing $P$ by a suitable positive integral multiple, $\sigma(P) = -P$.

Let $y^2 = f(x)$ be a fixed Weierstrass equation of $E/K$. Let $P = (\alpha, \sqrt{f(\alpha)})$. As $\sigma(P) = -P$, we have $\alpha \in K'$ but $\sigma(\sqrt{f(\alpha)}) = -\sqrt{f(\alpha)}$ so $\sqrt{f(\alpha)} \notin K'$. Then, $\sqrt{f(\alpha)} \notin K(\alpha)$, since $K(\alpha) \subseteq K'$. 

Note that $f(\alpha) \in K(\alpha) \subseteq \overline{K'}$. Let $c = f(\alpha) \in K(\alpha)$. We still have $\sigma \in \text{Gal}(\overline{K}/K(\alpha))$ and $\sigma(\sqrt{c}) = -\sqrt{c}$.

Let $E'/K(\alpha)$ denote the twist $y^2 = cf(x)$. Then, $E'$ has a rational point $P' = (\alpha, f(\alpha))$ over $K(\alpha)$. The $\overline{K}$-isomorphism $\phi: E \rightarrow E'$ mapping $(x,y) \mapsto (x, \sqrt{f(x)y})$ sends $P$ to $P'$, so $P'$ is of infinite order on $E'$. By (2, Theorem 5.3), $E'(\overline{K'})$ has infinite rank.

Let $\{P'_i = (x_i, \sqrt{cf(x_i)})\}_{i=1}^{\infty}$ be an infinite sequence of linearly independent points of $E'$ generating the infinite dimensional eigenspace of $1$ of $\sigma$ in $E'(\overline{K}) \otimes \C$. Then, $\sigma(x_i) = x_i$ and $\sigma(\sqrt{f(x_i)}) = -\sqrt{f(x_i)}$ for all $i$, since $\sigma(\sqrt{c}) = -\sqrt{c}$.

Let $P_i = \phi^{-1}(P'_i) = (x_i, \sqrt{f(x_i)})$. These are points of the given elliptic curve $E$ such that $\sigma(P_i) = -P_i$ for all $i$, since $\sigma(x_i) = x_i$ and $\sigma(\sqrt{f(x_i)}) = -\sqrt{f(x_i)}$.

The points $P_i$ are linearly independent because the $P'_i$ are so. Therefore, $\{P_i \otimes 1\}_{i=1}^{\infty}$ generates an infinite dimensional subspace of the $-1$-eigenspace of $\sigma$ on $V_E$. This completes the proof. \hfill $\square$

**Theorem 2.2.** Let $E/K$ be an elliptic curve over $K$. Then, $\Sigma_{-1}$ is open.

**Proof.** We have already seen that if $\sigma \in \Sigma_{-1}$, we can choose a point $P \in E(\overline{K})$ of infinite order such that $\sigma(P) = -P$. By Proposition 2.1, $\tau(P) = -P$ implies $\tau \in \Sigma_{-1}$. It follows that $\Sigma_{-1}$ contains the open neighborhood $\{\tau \in G_K \mid \tau(P) = \sigma(P)\}$ of $\sigma$. \hfill $\square$

**Remark 2.3.** The same argument shows that Questions 1.2 and 1.3 have an affirmative answer for $\zeta = \omega$ (resp. $\zeta = i$) when $E$ has complex multiplication by $\Z[\omega]$ (resp. $\Z[i]$).

### 3. Interior Points

In this section, we show that for every root of unity $\zeta$, the set $\Sigma_{\zeta}$ contains a non-empty open subset. We assume that the order of $\zeta$ is $n \geq 3$, the case $n = 1$ having been treated in [2], and the case $n = 2$ in Theorem 2.2.

Our strategy will be to find points $Q_i \in E(\overline{K})$ such that the $\sigma$-orbit of $Q_i$ has length $n$. For each such point $Q_i$, we set

$$R_i := \sum_{j=0}^{n-1} \sigma^j(Q_i) \otimes \zeta^{-j}$$

and observe that $R_i$ is a $\zeta$-eigenvector of $\sigma$ provided that it is non-zero.
We therefore begin with the following proposition:

**Proposition 3.1.** Let $X$ be a Riemann surface of genus $g \geq 3$ with an automorphism $\sigma$ of order $n \geq 3$. Then $X$ contains a non-empty open set $U$ such that $x \in U$ implies that

$$\sum_{i=0}^{n-1} [\sigma^i x] \otimes \zeta^{-i} \neq 0$$

in $\text{Pic} X \otimes \mathbb{C}$.

**Proof.** We can regard $X$ as the group of complex points of a non-singular projective curve whose Picard scheme has complex locus $\text{Pic} X$. Then $\text{Pic} X \otimes \mathbb{Z}[\zeta]$ is the group of complex points of a group scheme whose identity component $\text{Pic}^0 X \otimes \mathbb{Z}[\zeta]$ is isomorphic to the $\phi(n)$th power of the Jacobian variety of this curve. The action of $\sigma$ on $X$ defines an action on $\text{Pic} X$, and the map $\psi: \text{Pic} X \to \text{Pic} X \otimes \mathbb{Z}[\zeta]$ given by

$$\psi(y) = \sum_{i=0}^{n-1} \sigma^i y \otimes \zeta^{-i}$$

then comes from a morphism of group schemes. The image of $\psi$ actually lies in $\text{Pic}^0 X \otimes \mathbb{Z}[\zeta]$, and its kernel $P^0_{\zeta}$ is Zariski-closed in $\text{Pic} X$.

The set $P_{\zeta}$ of $y$ such that $\psi(y)$ maps to 0 in $\text{Pic} X \otimes \mathbb{C}$ is the union of all translates of $P^0_{\zeta}$ by torsion points of $\text{Pic} X$. Applying Raynaud’s theorem \[7\] (i.e., the proof of the Manin-Mumford conjecture) to the image of $X$ in $\text{Pic} X / P^0_{\zeta}$, the intersection $X \cap P_{\zeta}$ is finite whenever dim $\text{Pic} X / P^0_{\zeta} \geq 2$. It therefore suffices to prove that the Lie algebra of $P^0_{\zeta}$ is a subspace of the Lie algebra of $\text{Pic} X$ of codimension $\geq 2$ or, equivalently, that the rank of the map $\psi_*$ of Lie algebras is at least 2. We identify the Lie algebra of $\text{Pic} X$ in the usual way \[1\] Ch. 2, §6] with $H^1(X, \mathcal{O}_X) = H^{0,1}(X)$. Likewise, the Lie algebra of $\text{Pic} X \otimes \mathbb{Z}[\zeta]$ is isomorphic to $H^{0,1}(X) \otimes \mathbb{Z}[\zeta]$. For every $k$ prime to $n$, there exists a morphism

$$\phi_k: H^{0,1}(X) \otimes \mathbb{Z}[\zeta] \to H^{0,1}(X)$$

obtained from the embedding of $\mathbb{Z}[\zeta]$ into $\mathbb{C}$ mapping $\zeta$ to $\zeta^k$:

$$\phi_k(v \otimes \zeta^i) = \zeta^{ik} v.$$

The composition of this map with $\psi_*$ is $\sum_{i=0}^{n-1} \zeta^{-ik} \sigma^i$. 

---

\[4\] BO-HAE IM AND MICHAEL LARSEN

---

\[7\] Raynaud’s theorem

---

\[1\] Ch. 2, §6

---

\[7\] Manin-Mumford conjecture

---

\[1\] Ch. 2, §6

---

\[7\] The Lie algebra

---

\[1\] A morphism
Let $H_{\text{prim}}^{0,1}$ (resp. $H_{\text{prim}}^{1}(X(\mathbb{C}),\mathbb{C})$) denote the subspace of $H^{0,1}$ (resp. $H^{1}(X(\mathbb{C}),\mathbb{C})$) spanned by eigenvectors of $\sigma$ whose eigenvalues are primitive $n$th roots of unity. If $v$ is an eigenvector of $\sigma$ in $H^{0,1}$ whose eigenvalue is a primitive $n$th root of unity $\zeta^k$, then $\phi_k(\psi_*(v)) = nv \neq 0$, while $\phi_j(\phi_*(v)) = 0$ for all $j \neq k$. It follows that $\ker \psi_* \cap H_{\text{prim}}^{0,1} = \{0\}$, so the rank of $\psi_*$ is at least $\dim H_{\text{prim}}^{0,1}$. The Hodge decomposition $H^{1}(X(\mathbb{C}),\mathbb{C}) = H^{0,1} \oplus \overline{H^{0,1}}$ implies

$$\dim H_{\text{prim}}^{1}(X(\mathbb{C}),\mathbb{C}) = 2 \dim H_{\text{prim}}^{0,1}.$$  

It suffices, therefore, to prove $\dim H_{\text{prim}}^{1}(X(\mathbb{C}),\mathbb{C}) \geq 4$.

Let $R_{G}(G)$ denote the ring of complex (virtual) representations of $G$. For any subgroup $H$ of $G := \langle \sigma \rangle$, let $R_{G/H}$ denote the regular representation of $G/H$ regarded as an element of $R_{G}(G)$, and let $I_{H} := R_{G} - R_{G/H}$. In particular, $I_{\{1\}} = 0$. Regarded as an element of $R_{G}(G)$, the $G$-representation $H^{1}(X(\mathbb{C}),\mathbb{C})$ is

$$2g + (2h - 2)I_{G} + \sum_{[x] \in X/G} I_{\text{Stab}_{G}(x)},$$

where $h$ is the genus of $X/G$, and $\text{Stab}_{G}(x)$ is the stabilizer of any element of $X$ representing the $G$-orbit $[x]$. This is worked out in the case that $h = 0$ in [6, Prop. 2.2], but the method (in which the character of $H^{1}(X(\mathbb{C}),\mathbb{C})$ as a representation of $G$ is deduced from the Hurwitz formula and the Lefschetz trace formula) works in general.

The dimension of $H_{\text{prim}}^{1}(X(\mathbb{C}),\mathbb{C})$ is therefore $(2h - 2 + r)\phi(n)$, where $r$ is the number of ramification points of the cover $X \to X/G$. This is positive except in two cases: the cyclic cover $\mathbb{P}^{1} \to \mathbb{P}^{1}$ of degree $n$ (necessarily ramified over two points) and a degree $n$ isogeny of elliptic curves; these have genus 0 and 1 respectively. Otherwise, it is at least 4 unless $2h - 2 + r = 1$ and $\phi(n) = 2$. The triples $(h, r, n)$ for which this happens are $(0, 3, 3)$, $(0, 3, 4)$, $(1, 1, 3)$, and $(1, 1, 4)$. None of these is consistent with the condition $g \geq 3$.

\[\square\]

**Theorem 3.2.** Let $E/K$ be an elliptic curve over a number field $K$. For each root of unity $\zeta$, there exists a nonempty open subset $\Sigma_{\zeta}$ of $\text{Gal}(\overline{K}/K)$ such that the multiplicity of the eigenvalue $\zeta$ for $\sigma \in \Sigma_{\zeta}$ acting on $E(\overline{K}) \otimes \mathbb{C}$ is infinite.
Proof. Let $\zeta$ be an $n$th root of unity. Let $\lambda_1, \lambda_2, \lambda_3, \infty$ be the ramification points of a double cover $E \to \mathbb{P}^1$, and let $\lambda$ denote the cross-ratio of $(\lambda_1, \lambda_2, \lambda_3, \infty)$. Choose $a, b \in \overline{K}$ such that the ordered quadruple $(a, b, \zeta a, \zeta b)$ satisfies
\[
\frac{(\zeta a - a)(\zeta b - b)}{(\zeta b - a)(\zeta a - b)} = \lambda
\]
This is always possible; for instance, setting $a = 1$, we get a non-trivial quadratic equation for $b$, and since $\lambda$ is not 1 or $\infty$, we have $b, \zeta b \not\in \{a, \zeta a\}$. Thus the elliptic curves
\[
X_i : y^2 = (x - \zeta^{i-1}a)(x - \zeta^{i-1}b)(x - \zeta a)(x - \zeta b), \quad \text{for } i = 1, \ldots, n.
\]
all have the same $j$-invariant as $E$.

Let $L = K(a, b, \zeta)$. Fix $q \in K$ such that $L(\sqrt[n]{q})$ is a Galois $\mathbb{Z}/n\mathbb{Z}$-extension of $L$. We claim that $\Sigma_\zeta$ contains the open set $U_\zeta := \{\sigma \in \text{Gal}(\overline{K}/L) \mid \sigma(\sqrt[n]{q}) = \zeta^{n}\sqrt[n]{q}\}$.

Let $M = L(\sqrt[n]{q})$. For $N$ any number field containing $M$, let $C_N$ denote the affine curve over $N$
\[
\text{Spec } N[x, y_1, \ldots, y_n]/(P_1(x, y_1), \ldots, P_n(x, y_n), y_1 \cdots y_n - (x^n - a^n)(x^n - b^n))
\]
where
\[
P_i(x, y) = y^2 - (x - \zeta^{i-1}a)(x - \zeta a)(x - \zeta^{i-1}b)(x - \zeta b).
\]
Note that the equation $y_1 \cdots y_n - (x^n - a^n)(x^n - b^n) = 0$ merely selects one of the two irreducible components of the 1-dimensional affine scheme cut out by the other equations.

Let $X$ denote the compact Riemann surface which is the compactification of $C_N(\mathbb{C})$. By the Hurwitz genus formula, the genus of $X$ is $(n - 2)2^{n-2} + 1$, which is $\geq 3$ since $n \geq 3$. For any $n$-tuple $(k_1, \ldots, k_n) \in \{0, 1\}^n$ with even sum, the map
\[
(2) \quad (x, y_1, \ldots, y_n) \mapsto (\zeta x, (-1)^{k_1}\zeta^2 y_n, (-1)^{k_2}\zeta^2 y_1, (-1)^{k_3}\zeta^2 y_2, \ldots, (-1)^{k_n}\zeta^2 y_{n-1})
\]
defines an automorphism $\sigma$ of $C_N$ and therefore of $X$. As the $k_i$ have even sum, $\sigma$ is of order $n$. If $x \in \sqrt[n]{q}L^*$ and $\sigma \in U_\zeta$, then $\sigma(x) = \zeta x$, so
\[
\sigma(y_i)^2 = \zeta^4 y_{i-1}^2,
\]
and so there exists an \( n \)-tuple \((k_1, \ldots, k_n)\) with even coordinate sum such that \( \sigma \) acts on \( Q := (x, y_1, \ldots, y_n) \) by \((\mathbb{I})\). By Proposition 3.1 for all but finitely many values of \( x \),

\[
R := \sum_{i=0}^{n-1} \sigma^i(Q) \otimes \zeta^{-i}
\]

is a non-zero eigenvector of \( \sigma \) with eigenvalue \( \zeta \).

Assume now that \( N \) is a finite Galois extension of \( M \). Consider the morphism from \( C_N \) to the affine line over \( M \) given by \((x, y_1, \ldots, y_n) \mapsto x\). This is a branched Galois cover with Galois group \( \text{Gal}(N/M) \times (\mathbb{Z}/2\mathbb{Z})^{n-1} \). There exists a Hilbert set of values \( t \in M \) such that the geometric points lying over \( x = \sqrt[1]{q}t \) in \( C_M \) consists of a single \( \text{Gal}(\overline{K}/M) \)-orbit or, equivalently, \( \text{Gal}(M(y_1, \ldots, y_n)/M) \cong (\mathbb{Z}/2\mathbb{Z})^{n-1} \) and \( M(y_1, \ldots, y_n) \) is linearly disjoint from \( N \) over \( M \). As a Hilbert set of a finite extension of \( L \) always contains some Hilbert set of \( L \) \([5, \text{Ch. 9, Prop. 3.3}]\), it follows that there exists \( t \in L \) such that setting \( x = \sqrt[1]{q}t \), relative to \( M \), the extension \( M(y_1, \ldots, y_n) \) is linearly disjoint from \( N \) and has Galois group \( (\mathbb{Z}/2\mathbb{Z})^{n-1} \).

We can therefore iteratively construct a sequence \( t_1, t_2, \ldots \in L^* \) such that the extensions

\[
M_i := M\left(\sqrt{\left(\sqrt[1]{q}t_i - a\right)\left(\sqrt[1]{q}t_i - b\right)\left(\sqrt[1]{q}t_i - \zeta a\right)\left(\sqrt[1]{q}t_i - \zeta b\right)}\cdots, \right.
\]

are all linearly disjoint over \( M \). Let \( Q_i \) be a point with \( x \)-coordinate \( \sqrt[1]{q}t_i \), and \( R_i \) the corresponding \( \zeta \)-eigenvector of \( \sigma \) given by \((\mathbb{I})\). We claim that the \( R_i \) span a space of infinite dimension. The \( Q_i \) do so by \([2, \text{Lemma 3.12}]\), and as the \( \zeta^{-j} \) are linearly independent over \( \mathbb{Q} \), it follows that the \( R_i \) do so as well.

\[\square\]

We conclude with a question that does not seem to be directly amenable to the methods of this paper:

**Question 3.3.** Does the set \( \bigcap_{\zeta \in C^*_{\text{tor}}} \sum_{\zeta} \) of elements of \( G_K \) having generic spectrum on \( V_E \) always have an interior point?
References

[1] P. Griffiths and J. Harris: *Principles of Algebraic Geometry*, John Wiley & Sons, New York, 1978.

[2] B. Im: Mordell-Weil groups and the rank over large fields of elliptic curves over large fields, arXiv: math.NT/0411533 to appear in *Canadian J. Math.*

[3] B. Im: Infinite multiplicity of roots of unity of the Galois group in the representation on elliptic curves, preprint, 2003.

[4] B. Im: Heegner points and Mordell-Weil groups of elliptic curves over large fields, preprint, arXiv: math.NT/0411534

[5] S. Lang: *Fundamentals of Diophantine Geometry*, Springer-Verlag, New York, 1983.

[6] M. Larsen: *Rigid lattices are Mordell-Weil*, preprint, arXiv: math.NT/0401209

[7] M. Raynaud: Courbes sur une variété abélienne et points de torsion. *Invent. Math.* 71 (1983), no. 1, 207–233.

Department of Mathematics, University of Utah, Salt Lake City, Utah 84112, USA
E-mail address: im@math.utah.edu

Department of Mathematics, Indiana University, Bloomington, Indiana 47405, USA
E-mail address: larsen@math.indiana.edu