ELSEVIER

Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Algebra 299 (2006) 707–713

JOURNAL OF Algebra

www.elsevier.com/locate/jalgebra

Open conditions for infinite multiplicity eigenvalues on elliptic curves

Bo-Hae Im [a], Michael Larsen [b,*]

[a] *Department of Mathematics, University of Utah, Salt Lake City, UT 84112, USA*
[b] *Department of Mathematics, Indiana University, Bloomington, IN 47405, USA*

Received 4 April 2005

Available online 20 March 2006

Communicated by Laurent Moret-Bailly

Abstract

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

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

1. Introduction

Let K be a number field, $\overline{K}$ an algebraic closure of K, and $G_K := \mathrm{Gal}(\overline{K}/K)$ 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* σ, 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 σ for which the spectrum is quite different: trivially, the

* Corresponding author.
E-mail addresses: im@math.utah.edu (B.-H. Im), larsen@math.indiana.edu (M. Larsen).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.02.011

identity and complex conjugation elements; less trivially, examples which can be constructed for an arbitrary set S of primes, such that ζ is an eigenvalue if and only if every prime factor of its order lies in S.

Throughout this paper, we will write Σ_ζ for the subset of G_K consisting of elements σ acting as ζ 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 σ at all, we have $\sigma \in \Sigma_1$. It follows that Σ_1 is open. By [4], when $K = \mathbb{Q}$, Σ_1 is all of G_K, and 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 Σ_ζ have non-empty interior for all ζ?*

Question 1.2. *Is Σ_ζ open for all ζ?*

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

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

The difficulty in proving such theorems is that placing σ in a basic open subset U of G_K amounts to specifying the action of σ on a finite Galois extension L of K. By the Mordell–Weil theorem, $E(L) \otimes \mathbb{C}$ is finite-dimensional. The surprising thing is that knowing the action of σ on this finite-dimensional subspace of V_E can be enough to guarantee the existence of an infinite-dimensional ζ-eigenspace for σ.

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 σ is infinite-dimensional.*

Proof. As -1 is an eigenvalue of σ acting on V_E, it is an eigenvalue of σ acting on $E(\overline{K}) \otimes \mathbb{Q}$. Clearing denominators, there exists a non-torsion $P \in E(\overline{K})$ such that $\sigma(P) + P \in E(\overline{K})_{\mathrm{tor}}$. 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 $\alpha \in \overline{K}^\sigma$ but $\sigma(\sqrt{f(\alpha)}) = -\sqrt{f(\alpha)}$ so $\sqrt{f(\alpha)} \notin \overline{K}^\sigma$. Then, $\sqrt{f(\alpha)} \notin K(\alpha)$, since $K(\alpha) \subseteq \overline{K}^\sigma$.

Let $c = f(\alpha) \in K(\alpha)$. We still have $\sigma \in \mathrm{Gal}(\overline{K}/K(\alpha))$ 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 $\phi : E \to E'$ mapping $(x, y) \mapsto (x, \sqrt{f(\alpha)}y)$ sends P to P', so P' is of infinite order on E'. By [2, Theorem 5.3], $E'(\overline{K}^\sigma)$ 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 σ in $E'(\overline{K}) \otimes \mathbb{C}$. 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 σ on V_E. This completes the proof. □

Theorem 2.2. *Let E/K be an elliptic curve over K. Then, Σ_{-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 Σ_{-1} contains the open neighborhood $\{\tau \in G_K \mid \tau(P) = \sigma(P)\}$ of σ. □

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

3. Interior points

In this section, we show that for every root of unity ζ, the set Σ_ζ contains a non-empty open subset. We assume that the order of ζ is $n \geqslant 3$, 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 σ-orbit of Q_i has length n. For each such point Q_i, we set

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

and observe that R_i is a ζ-eigenvector of σ provided that it is non-zero.

We therefore begin with the following proposition.

Proposition 3.1. *Let X be a Riemann surface of genus $g \geqslant 3$ with an automorphism σ of order $n \geqslant 3$. 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 $\operatorname{Pic} X \otimes \mathbb{C}$.

To prove the proposition, we need the following lemma, which is essentially due to Weil (see [7, VI, Proposition 7] for a formulation more general than ours, in the setting of ℓ-adic homology).

Lemma 3.2. *Let $R_{\mathbb{C}}(G)$ denote the ring of virtual complex representations of a finite group G, and for every subgroup $H \subset G$, let $I_H = \operatorname{Ind}_H^G 1$, where 1 is the trivial representation. For any compact Riemann surface X on which G acts faithfully, we have the following identity in $R_{\mathbb{C}}(G) \otimes \mathbb{Q}$:*

$$\left[H^1(X, \mathbb{C})\right] = 2 + (2h-2)[I_{\{1\}}] + \sum_{x \in X} \frac{[I_{\{1\}}] - [I_{\mathrm{Stab}_G(x)}]}{[G : \mathrm{Stab}_G(x)]}, \tag{2}$$

where h is the genus of X/G, and $[V]$ denotes the class in $R_{\mathbb{C}}(G)\otimes\mathbb{Q}$ associated to the representation V. Note that the summand on the right-hand side of (2) *is zero for every x with* $\mathrm{Stab}_G(x)=\{1\}$, *and therefore the sum is finite.*

Proof. Let $\pi : X \to X/G$ denote the quotient map. There is a natural injective trace map from $R_{\mathbb{C}}(G)\otimes\mathbb{Q}$ to the space of complex-valued functions on G. To prove the lemma, it suffices to take traces of both sides and check equality for all elements of $g \in G$. When $g=1$, the equality of traces in (2) is just the Riemann–Hurwitz formula. For $g \neq 1$, the Lefschetz trace formula asserts

$$2-\mathrm{tr}\bigl(g \mid H^1(X,\mathbb{C})\bigr)=\mathrm{Fix}(g)=\sum_{y\in X/G}\ \sum_{\{x\in\pi^{-1}y \mid g(x)=x\}} 1.$$

The contribution of the G-orbit of $x_0 \in X$ to this sum is

$$\frac{1}{[G:\mathrm{Stab}_G(x_0)]}\sum_{\{k\in G \mid g(k(x_0))=k(x_0)\}} 1=\frac{|\{k\in G \mid g\in k\,\mathrm{Stab}_G(x_0)k^{-1}\}|}{[G:\mathrm{Stab}_G(x_0)]}.$$

On the other hand, any non-zero g has trace 2 on $2+(2h-2)[I_{\{1\}}]$. To compute the trace of g on the remaining terms on the right-hand side of (2), we note that for any subgroup H of G, g fixes a coset kH if and only if $g\in kHk^{-1}$, so the trace of g on I_H equals

$$\frac{|\{k\in G \mid g\in kHk^{-1}\}|}{|H|}.$$

Thus, the trace of g on

$$\sum_{x\in\pi^{-1}(\pi(x_0))}\frac{[I_{\{1\}}]-[I_{\mathrm{Stab}_G(x)}]}{[G:\mathrm{Stab}_G(x)]}$$

is

$$\mathrm{tr}\bigl(g \mid [I_{\{1\}}]-[I_{\mathrm{Stab}_G(x_0)}]\bigr)=-\frac{|\{k\in G \mid g\in k\,\mathrm{Stab}_G(x_0)k^{-1}\}|}{|\mathrm{Stab}_G(x_0)|}.$$

The lemma follows. □

We can now prove Proposition 3.1.

Proof. We can regard X as the set of complex points of a non-singular projective curve whose Picard scheme has complex locus $\mathrm{Pic}\,X$. Then $\mathrm{Pic}\,X\otimes\mathbb{Z}[\zeta]$ is the group of complex points of a group scheme whose identity component $\mathrm{Pic}^0X\otimes\mathbb{Z}[\zeta]$ is isomorphic to the $\phi(n)$th power of the Jacobian variety of this curve. The action of σ on X defines an action on $\mathrm{Pic}\,X$, and the map $\psi:\mathrm{Pic}\,X\to\mathrm{Pic}\,X\otimes\mathbb{Z}[\zeta]$ 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 ψ actually lies in $\operatorname{Pic}^0 X \otimes \mathbb{Z}[\zeta]$, and its kernel P_ζ^0 is Zariski-closed in $\operatorname{Pic} X$.

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

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

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

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

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

Let $H_{\mathrm{prim}}^{0,1}$ (respectively $H_{\mathrm{prim}}^1(X, \mathbb{C})$) denote the subspace of $H^{0,1}$ (respectively $H^1(X, \mathbb{C})$) spanned by eigenvectors of σ whose eigenvalues are primitive nth roots of unity. If v is an eigenvector of σ in $H^{0,1}$ whose eigenvalue is a primitive nth root of unity ζ^k, then $\phi_k(\psi_*(v)) = nv \neq 0$, while $\phi_j(\phi_*(v)) = 0$ for all $j \neq k$. It follows that $\ker \psi_* \cap H_{\mathrm{prim}}^{0,1} = \{0\}$, so the rank of ψ_* is at least $\dim H_{\mathrm{prim}}^{0,1}$. The Hodge decomposition

$$H^1(X, \mathbb{C}) = H^{0,1} \oplus \overline{H^{0,1}}$$

implies

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

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

We apply Lemma 3.2 in the case $G = \langle \sigma \rangle$. In this case, the primitive part of I_H is trivial if $H \subset \langle \sigma \rangle$ is non-trivial, and it has dimension $\phi(n)$ for $H = \{1\}$. Thus, the dimension of $H_{\mathrm{prim}}^1(X, \mathbb{C})$ is $(2h - 2 + r)\phi(n)$, 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 $g \geqslant 3$. □

Theorem 3.3. *Let E/K be an elliptic curve over a number field K. For each root of unity ζ, there exists a non-empty open subset Σ_ζ of* $\operatorname{Gal}(\overline{K}/K)$ *such that the multiplicity of the eigenvalue ζ for $\sigma \in \Sigma_\zeta$ acting on $E(\overline{K}) \otimes \mathbb{C}$ is infinite.*

Proof. Let ζ be an nth 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 λ 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 λ is not 1 or ∞, we have $b, \zeta b \notin \{a, \zeta a\}$. Thus the elliptic curves

$$X_i : y^2 = \bigl(x - \zeta^{i-1}a\bigr)\bigl(x - \zeta^{i-1}b\bigr)\bigl(x - \zeta^i a\bigr)\bigl(x - \zeta^i b\bigr), \quad \text{for } i = 1, \ldots, n$$

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 Σ_ζ contains the open set

$$U_\zeta := \bigl\{\sigma \in \operatorname{Gal}(\overline{K}/L) \mid \sigma\bigl(\sqrt[n]{q}\bigr) = \zeta \sqrt[n]{q}\bigr\}.$$

Let $M = L(\sqrt[n]{q})$. For N any number field containing M, let C_N denote the affine curve over N

$$\operatorname{Spec} N[x, y_1, \ldots, y_n]/\bigl(P_1(x, y_1), \ldots, P_n(x, y_n), y_1 \cdots y_n - \bigl(x^n - a^n\bigr)\bigl(x^n - b^n\bigr)\bigr),$$

where

$$P_i(x, y) = y^2 - \bigl(x - \zeta^{i-1}a\bigr)\bigl(x - \zeta^i a\bigr)\bigl(x - \zeta^{i-1}b\bigr)\bigl(x - \zeta^i b\bigr).$$

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 $\geqslant 3$ since $n \geqslant 3$. For any n-tuple $(k_1, \ldots, k_n) \in \{0, 1\}^n$ with even sum, the map

$$(x, y_1, \ldots, y_n) \mapsto \bigl(\zeta x, (-1)^{k_1}\zeta^2 y_n, (-1)^{k_2}\zeta^2 y_1, (-1)^{k_3}\zeta^2 y_2, \ldots, (-1)^{k_n}\zeta^2 y_{n-1}\bigr) \qquad (3)$$

defines an automorphism σ of C_N and therefore of X. As the k_i have even sum, σ 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 σ acts on $Q := (x, y_1, \ldots, y_n)$ by (3). 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 σ with eigenvalue ζ.

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 $(x, y_1, \dots, y_n) \mapsto x$. This is a branched Galois cover with Galois group $\mathrm{Gal}(N/M) \times (\mathbb{Z}/2\mathbb{Z})^{n-1}$. There exists a Hilbert set of values $t \in M$ such that the geometric points lying over $x = \sqrt[n]{q}t$ in C_M consists of a single $\mathrm{Gal}(\overline{K}/M)$-orbit or, equivalently, $\mathrm{Gal}(M(y_1, \dots, y_n)/M) \cong (\mathbb{Z}/2\mathbb{Z})^{n-1}$ and $M(y_1, \dots, y_n)$ 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, Chapter 9, Proposition 3.3], it follows that there exists $t \in L$ such that setting $x = \sqrt[n]{q}t$, relative to M, the extension $M(y_1, \dots, y_n)$ is linearly disjoint from N and has Galois group $(\mathbb{Z}/2\mathbb{Z})^{n-1}$.

We can therefore iteratively construct a sequence $t_1, t_2, \dots \in L^*$ such that the extensions

$$M_i := M\Big(\sqrt{\big(\sqrt[n]{q}t_i - a\big)\big(\sqrt[n]{q}t_i - b\big)\big(\sqrt[n]{q}t_i - \zeta a\big)\big(\sqrt[n]{q}t_i - \zeta b\big)}, \dots, \\ \sqrt{\big(\sqrt[n]{q}t_i - \zeta^{n-1}a\big)\big(\sqrt[n]{q}t_i - \zeta^{n-1}b\big)\big(\sqrt[n]{q}t_i - a\big)\big(\sqrt[n]{q}t_i - b\big)}\Big)$$

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

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

Question 3.4. *Does the set $\bigcap_{\zeta \in \mathbb{C}^*_{\mathrm{tor}}} \Sigma_\zeta$ of elements of G_K having generic spectrum on V_E always have an interior point?*

Acknowledgments

The authors thank L. Moret-Bailly and the referee for correcting versions of Proposition 3.1 appearing in earlier drafts of this manuscript and for suggesting many other improvements.

References

[1] P. Griffiths, J. Harris, Principles of Algebraic Geometry, Wiley, New York, 1978.
[2] B. Im, Mordell–Weil groups and the rank over large fields of elliptic curves over large fields, math.NT/0411533, Canad. J. Math., in press.
[3] B. Im, Infinite multiplicity of roots of unity of the Galois group in the representation on elliptic curves, J. Number Theory 114 (2) (2005) 312–323.
[4] B. Im, Heegner points and Mordell–Weil groups of elliptic curves over large fields, preprint, math.NT/0411534.
[5] S. Lang, Fundamentals of Diophantine Geometry, Springer-Verlag, New York, 1983.
[6] M. Raynaud, Courbes sur une variété abélienne et points de torsion, Invent. Math. 71 (1) (1983) 207–233.
[7] J.-P. Serre, Local Fields, Springer-Verlag, New York, 1979.