Canad. J. Math. Vol. **58** (4), 2006 pp. 796–819

Mordell–Weil Groups and the Rank of Elliptic Curves over Large Fields

Bo-Hae Im

Abstract. Let K be a number field, $\overline{K}$ an algebraic closure of K and E/K an elliptic curve defined over K. In this paper, we prove that if E/K has a K-rational point P such that $2P \neq O$ and $3P \neq O$, then for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the Mordell–Weil group $E(\overline{K}^{\sigma})$ of E over the fixed subfield of $\overline{K}$ under σ has infinite rank.

1 Introduction

In [1], G. Frey and M. Jarden showed that if K is an infinite field of finite type and A is an abelian variety of dimension $d \geq 1$ defined over K, then for any positive integer n, there is a subset of $\mathrm{Gal}(\overline{K}/K)^n$ of Haar measure 1 such that for every n-tuple $(\sigma_1, \dots, \sigma_n)$ belonging to the subset, the group of rational points $A(\overline{K}(\sigma_1, \dots, \sigma_n))$ of A over the fixed subfield of $\overline{K}$ under $(\sigma_1, \dots, \sigma_n)$ has infinite rank.

In [12], M. Larsen proved that for a number field K and an elliptic curve E/K over K, there is a nonempty open subset Σ of $\mathrm{Gal}(\overline{K}/K)$ such that for any $\sigma \in \Sigma$, the Mordell–Weil group $E(\overline{K}^{\sigma})$ of E over the fixed field under σ has infinite rank.

It is natural to ask if such an open subset can be the whole Galois group $\mathrm{Gal}(\overline{K}/K)$. We have a positive answer for elliptic curves defined over $\mathbb{Q}$. In [7], we proved that for any elliptic curve $E/\mathbb{Q}$, the rank of $E(\overline{\mathbb{Q}}^{\sigma})$ is infinite, for every $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Our approach in [7] is arithmetic: taking advantage of the modularity of elliptic curves over $\mathbb{Q}$ and the complex multiplication theory and constructing an infinite supply of rational points of E consisting of Heegner points.

This paper is motivated by [1, 7, 12], and we prove in Section 3 that if E/K has a K-rational point P such that $2P \neq O$ and $3P \neq O$, then for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the Mordell–Weil group $E(\overline{K}^{\sigma})$ over the fixed subfield of $\overline{K}$ under σ has infinite rank. Here, we approach by using Diophantine geometry which is a completely different method from the one that we use in [7].

The main strategy for constructing infinitely many linearly independent rational points of E over $\overline{K}^{\sigma}$ for $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is approximately as follows: find a finite group G, a $\mathbb{Z}$-free $\mathbb{Z}[G]$-module M of rank r and an infinite sequence $\{K_i/K\}_{i=1}^{\infty}$ of linearly disjoint finite Galois extensions of K with $\mathrm{Gal}(K_i/K) \cong G$ such that for each i, $E(K_i) \otimes \mathbb{Q}$ contains a G-submodule isomorphic to $M \otimes \mathbb{Q}$. If $M^G = 0$ but $M^g \neq 0$ for each $g \in G$, then we can find $\mathbb{Q}$-independent points of $E(K_i) \cap E(\overline{K}^{\sigma})$ for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

Then G acts on $E \otimes M$ through its action on M. Define $E \otimes M$ to be the abelian variety representing the functor $S \mapsto E(S) \otimes_{\mathbb{Z}} M$, where S is any scheme over the ground

Received by the editors February 4, 2004; revised December 21, 2004.
AMS subject classification: 11G05.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

field and $E(S)$ is the functor of points associated to E. Then, as an abelian variety, $E \otimes M$ is just E^r, since the action of G on $E \otimes M$ is only though M. Suppose we find a projective line $\mathbb{P}^1$ in $(E \otimes M)/G$ over K. If its preimage X in $E \otimes M$ under the quotient map is an irreducible curve over K, then by the Hilbert irreducibility theorem [11, Chapter 9], most points in $\mathbb{P}^1(K)$ determine points in $E^r(K_i)$ with $\mathrm{Gal}(K_i/K) = G$; the coordinates generate the desired G-submodule of $E(K_i) \otimes \mathbb{Q}$. In this paper, we take for G the alternating group A_n on $n = 2k$ letters and for the module M the irreducible $(n-1)$-dimensional quotient of the permutation representation of A_n by the trivial representation.

In Section 2, we first show that S_n admits a nontrivial action on the $(n-1)$-fold product E^{n-1} of E and that its quotient E^{n-1}/S_n by S_n is isomorphic to the $(n-1)$-dimensional projective space $\mathbb{P}^{n-1}$. We also find some properties of transitive subgroups of S_n which contain a transposition and observe properties of subgroups of A_n which occur as branched Galois coverings of a projective line.

In Section 3, if K is totally imaginary and E/K has a K-rational point P such that $2P \neq O$ and $3P \neq O$, then we show that for some even integer n, there is a projective line over K in E^{n-1}/S_n whose preimage in E^{n-1}/A_n under the double cover is a curve of genus 0, which gives infinitely many linearly independent points of E over the fixed field of each $\sigma \in \mathrm{Gal}(\overline{K}/K)$.

In Section 4, using the Hilbert irreducibility theorem [11, Chapter 9] and the density of the Hilbert sets over $\mathbb{Q}$ in $\mathbb{R}$, we prove as a special case that if K is a number field and K_{ab} is the maximal abelian extension of K, then for any complex conjugation automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$, the rank of $E((K_{\mathrm{ab}})^{\sigma})$ is infinite. Hence, the rank of $E(\overline{K}^{\sigma})$ is infinite.

Then in Section 5, we show that if $\sigma \in \mathrm{Gal}(\overline{K}/K)$ is not a complex conjugation automorphism, then there is a totally imaginary finite extension of K which is fixed under σ. So by applying this to extend the ground field to a totally imaginary extension for such automorphisms in $\mathrm{Gal}(\overline{K}/K)$, and combining the result of infinite rank of the case of totally imaginary number fields and the case of complex conjugation automorphisms, we get a more general result that if K is an arbitrary number field and E/K has a K-rational point P such that $2P \neq O$ and $3P \neq O$, then for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$ the rank of $E(\overline{K}^{\sigma})$ is infinite.

2 Action of S_n on E^{n-1} and Branched Galois Coverings of $\mathbb{P}^1$

Let $n \geq 2$ be an integer. First let S_n be the symmetric group on n letters and A_n the alternating subgroup of S_n. Denote the n-fold product of E by E^n. Naturally, S_n acts on E^n by permutation, *i.e.,* if we denote its action by "$\cdot$", for $\sigma \in S_n$ and an n-tuple $(P_1, \dots, P_n) \in E^n$, $\sigma \cdot (P_1, \dots, P_n) = (P_{\sigma(1)}, \dots, P_{\sigma(n)})$. So does A_n on E^n. Let $\Sigma\colon E^n \longrightarrow E$ be the map defined by the sum of coordinates of an n-tuple. Then identify E^{n-1} with n-tuples of elements in E which sum to O *i.e.,* $\mathrm{Ker}(\Sigma)$. S_n still acts on $E^{n-1} \cong \mathrm{Ker}(\Sigma)$ by the nontrivial induced permutation action.

Through the paper, we always consider E^{n-1} as $\mathrm{Ker}(\Sigma)$ so that a point in E^{n-1} (or its quotient E^{n-1}/S_n by S_n) is an n-tuple $(P_1, \dots, P_n) \in E^{n-1}$ whose coordinates sum to O.

The following lemma gives the structure of the quotient space E^{n-1}/S_n of E^{n-1}

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

by S_n.

Lemma 2.1 *For each $n \geq 2$, S_n admits a nontrivial action on E^{n-1}. The quotient space E^{n-1}/S_n of E^{n-1} by S_n is isomorphic to the $(n-1)$-dimensional projective space $\mathbb{P}^{n-1}$.*

Proof Identify E^{n-1} with n-tuples of elements in E which sum to O, *i.e.*, with the set $\operatorname{Ker}(\Sigma)$, where $\Sigma\colon E^n \longrightarrow E$ is the map defined by the sum of coordinates of an n-tuple. Then for each $(P_1,\dots,P_n) \in \operatorname{Ker}(\Sigma) \cong E^{n-1}$, there is a rational function f on E such that $\sum_{i=1}^n (P_i) = (f) + n(O)$ as divisors. This gives a map from E^{n-1} to the linear space of all rational functions f on E such that $(f) + n(O) \geq 0$. Denote this linear space by $|n(O)|$.

Then by the Riemann–Roch Theorem [6, Chapter IV, Theorem 1.3], the dimension of this space is n as a vector space so it gives an $(n-1)$-dimensional projective space. We choose a basis $f_0,\dots,f_{n-1}$ of the space $|n(O)|$ and define a map $\phi\colon E^{n-1} \longrightarrow \mathbb{P}^{n-1}$ in the following way.

For each $(P_1,\dots,P_n) \in \operatorname{Ker}(\Sigma) \cong E^{n-1}$, there is a rational function f on E such that $\sum_{i=1}^n (P_i) = (f) + n(O)$. Write $f = \sum_{i=0}^{n-1} a_i f_i$ with $a_0,\dots,a_{n-1} \in \mathbb{C}$. Then define $\phi(P_1,\dots,P_n) = (a_0 : a_1 : \cdots : a_{n-1}) \in \mathbb{P}^{n-1}$.

Then two n-tuples which sum to O in E^{n-1} map onto the same point in $\mathbb{P}^{n-1}$ under ϕ if and only if they are the same up to permutations of S_n. This implies that the quotient space E^{n-1}/S_n is isomorphic to the projective space $\mathbb{P}^{n-1}$. ■

Now we find some properties of subgroups of S_n which act transitively on $\{1,2,\dots,n\}$ and contain a transposition. The following lemma assumes a weaker condition than in [3, Lemma 1.4].

Lemma 2.2 *If H is a subgroup of S_n containing a transposition and H acts transitively on $\{1,2,\dots,n\}$, then there are positive integers m and k such that $mk = n$, where $m > 1$, $k \geq 1$, and there are subgroups K of H and T of S_k such that $K \lhd H$, $K \cong (S_m)^k$, $H/K \cong T$ and T acts transitively on $\{1,2,\dots,k\}$, where*

$$(S_m)^k = \underbrace{S_m \times \cdots \times S_m}_{k \text{ times}}.$$

Moreover, $K \cap A_n \trianglelefteq H \cap A_n$ and $(H \cap A_n)/(K \cap A_n) \cong T$ and $H \cap A_n$ acts transitively on $\{1,2,\dots,n\}$. In particular, if n is a prime p, then $H \cong S_p$ and $H \cap A_p \cong A_p$.

Proof Without loss of generality, we may assume that the transposition $(12) \in H$. Define a relation $\sim$ on $\{1,2,\dots,n\}$ by: for $x, y \in \{1,2,\dots,n\}$,

$$x \sim y \text{ if and only if } x = y \text{ or there is a transposition } (xy) \in H.$$

Then this relation is an equivalence relation. In fact, the transitivity of the relation holds, since if $(xy) \in H$ and $(yz) \in H$, then $(xz) = (xy)(yz)(xy) \in H$.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

Since $(12) \in H$, $1 \sim 2$, hence the equivalence class of 1 has at least two elements in $\{1, 2, \dots, n\}$. Moreover, if we suppose $x \sim y$, then $(xy) \in H$. Let $x' \in \{1, 2, \dots, n\}$. Since H acts transitively on $\{1, 2, \dots, n\}$, there is $h \in H$ such that $h(x) = x'$. Now $h(xy)h^{-1} = (h(x)\ h(y)) = (x'\ h(y))$, which is in H. Hence $h(x) = x' \sim h(y)$, *i.e.*, $x \sim y$ iff $h(x) \sim h(y)$. Therefore, each equivalence class has the same number of elements.

Let k be the number of equivalence classes and let $C_1, \dots, C_k$ be the equivalence classes of $\{1, 2, \dots, n\}$. And let $m = \frac{n}{k}$. Each class C_i has m elements. Note that $m \geq 2$, since $(12) \in H$.

For each $h \in H$, on each class C_i, $h(C_i) = C_{h_i}$, for some $h_i \in \{1, 2, \dots, k\}$, since we have showed in the above that $x \sim y$ iff $h(x) \sim h(y)$. And h gives a bijection of C_i and C_{h_i}. Hence we have a natural map $\phi_h \colon \{C_i\}_{1 \leq i \leq k} \to \{C_i\}_{1 \leq i \leq k}$ defined by $\phi_h(C_i) = C_{h_i}$ where $i, h_i = 1, 2, \dots, k$. This shows that ϕ_h permutes equivalence classes $C_1, \dots, C_k$. Hence we get a permutation $\sigma_h \in S_k$ such that $\sigma_h(i) = h_i$, where i_k is given by $h(C_i) = C_{h_i}$.

So we can define a map $\pi \colon H \to S_k$ given by $\pi(h) = \sigma_h$ defined as above. Then π is a group homomorphism, since $hh'(x) = h(h'(x))$, for $h, h' \in H$ and $x \in \{1, 2, \dots, n\}$.

Let $T = \text{Image}(\pi)$ and $K = \ker(\pi)$. Then $K \trianglelefteq H$ and $T \leq S_k$. Moreover, T acts transitively on $\{1, 2, \dots, k\}$, since $C_1 \sqcup C_2 \sqcup \cdots \sqcup C_k = \{1, 2, \dots, n\}$ and H acts on $\{1, 2, \dots, n\}$ transitively.

Now we show that

$$K \cong \underbrace{S_m \times \cdots \times S_m}_{k \text{ times}} := (S_m)^k.$$

Let $S(C_i)$ be the group of all permutations on elements of C_i. For any $h \in K$, h has a decomposition, $h = h_1 h_2 \dots h_k$, where each permutation h_i is a product of disjoint cycles in $S(C_i)$, since h is stable on each class. If $h, g \in K$, let $h = h_1 h_2 \cdots h_k$ and $g = g_1 g_2 \cdots g_k$, where $h_i, g_i \in S(C_i)$, then $hg = h_1 g_1 h_2 g_2 \cdots h_k g_k$, since h_i and g_j are disjoint for $i \neq j$. Hence we get an injective homomorphism $f \colon K \to S(C_1) \times \cdots \times S(C_k)$ defined by $f(h) = (h_1, \cdots, h_k)$, where $h = h_1 h_2 \cdots h_k$ and $h_i \in S(C_i)$. Since $S(C_i) \cong S_m$ is generated by transpositions and for any $x_i, y_i \in C_i$, there is a transposition $(x_i y_i) \in H$, $f((x_1 y_1) \cdots (x_k y_k)) = ((x_1 y_1), \dots, (x_k y_k))$. Hence f is surjective. Therefore, $K \cong S(C_1) \times \cdots \times S(C_k) \cong (S_m)^k$. By the first isomorphism theorem, $H/K \cong T$.

Hereafter we identify the subgroup K of H with $(S_m)^k$ under the isomorphism in the above. Then we get a short exact sequence of groups,

$$1 \longrightarrow (S_m)^k \xrightarrow{f} H \xrightarrow{\pi} T \longrightarrow 1.$$

Next we show that the following sequence is exact:

$$1 \longrightarrow (S_m)^k \cap A_n \xrightarrow{f'} H \cap A_n \xrightarrow{\pi'} T \longrightarrow 1,$$

where f' is the restriction of the inclusion f to $(S_m)^k \cap A_n$.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

First, it is obvious that f' is injective, since f is injective. Moreover, since $\ker(\pi) = \mathrm{Image}(f)$, we have $\ker(\pi') = \ker(\pi) \cap A_n = \mathrm{Image}(f) \cap A_n = \mathrm{Image}(f')$. So this implies the exactness of the middle one. Now we need to show π' is surjective. For any $\sigma \in T$, there is $h \in H$ such that $\pi(h) = \sigma$, since π is surjective. If h is an even permutation, then $h \in H \cap A_n$ and $\pi'(h) = \pi(h) = \sigma$. If h is not even, then consider σ as a permutation of $\{C_1, \dots, C_k\}$ as in the above. Then there are two distinct integers i and $j \in \{1, 2, \dots, k\}$ such that $\sigma(C_i) = C_j$. Since C_i has at least two elements, there are two elements $a, b \in C_i$, *i.e.*, $a \sim b \in C_i$. Hence $(ab) \in H$. Moreover, $(ab) \in \mathrm{Ker}(\pi)$ from the construction. Hence $(ab) \circ h$ is an even permutation and $\pi'((ab) \circ h) = \pi((ab) \circ h) = \pi(h) = \sigma$. Hence π' is surjective. Therefore, $K \cap A_n \cong (S_m)^k \cap A_n = \ker(f') \trianglelefteq H \cap A_n$ and $(H \cap A_n)/((S_m)^k \cap A_n) \cong T$.

Now we show that $H \cap A_n$ acts transitively on $\{1, 2, \dots, n\}$. If $k = 1$, then $m = n$, hence $H \cong S_n$. Therefore, $H \cap A_n = A_n$, which acts transitively on $\{1, 2, \dots, n\}$. Assume that $k \geq 2$. Let $a, b \in \{1, 2, \dots, n\}$. We need to find an even permutation $\sigma \in H$ such that $\sigma(a) = b$. If both a and b are in the same class C_i for some $i \in \{1, 2, \dots, k\}$, then there is $(ab) \in H$. Since $k \geq 2$, we choose two distinct elements c and $d \in C_j$ for some $j \neq i$. Then if let $\sigma = (ab)(cd)$, then $\sigma \in H \cap A_n$ and $\sigma(a) = b$.

If a and b are in distinct classes, say $a \in C_i$ and $b \in C_j$ for $i \neq j$, then there is $\tau \in T$ such that $\tau(i) = j$. Since τ is a bijection between C_i and C_j, there are $b' \in C_j$ and $a' \in C_i$ such that $\tau(a) = b'$ and $\tau(a') = b$. If τ is an even permutation, then let $\sigma = (aa')(bb') \circ \tau$. Then $\sigma(a) = b$ and $\sigma \in H \cap A_n$. If τ is odd, then let $\sigma = (bb') \circ \tau$. Then $\sigma(a) = b$ and $\sigma \in H \cap A_n$. This completes the proof. ■

Lemma 2.3 *If H is a transitive subgroup of S_n and (V, ρ) is the permutation representation of S_n, then the restriction of (V, ρ) to H has one 1-dimensional invariant subspace.*

Proof Let $e_1, \dots, e_n$ be a basis for the restriction (V, ρ') of the permutation representation of S_n to H. Let $H_1 = \{h \in H \mid h(1) = 1\}$ be the stabilizer of 1 in H. Let W be the subspace of V generated by e_1. Then W is invariant under H_1. Moreover, since H acts transitively on $\{1, 2, \dots, n\}$, we have exactly n left cosets of H_1 in H. Hence we can identify the permutation representation (V, ρ') with the induced representation $\bigl(\bigoplus_{i=1}^{n} \rho'_{g_i}(W),\ \mathrm{Ind}_{H_1}^{H}(1)\bigr)$ of H by the trivial representation $(W, 1)$ of H_1, where g_i are representatives of left cosets of H_1 in H.

If we denote by 1 the trivial representation of H, then by Frobenius reciprocity,

$$\langle 1, \mathrm{Ind}_{H_1}^{H}(1) \rangle_H = \langle \mathrm{Res}_{H_1}^{H}(1), 1 \rangle_{H_1} = \langle 1, 1 \rangle_{H_1} = 1.$$

Therefore, the restriction (V, ρ) of the permutation representation to H has one 1-dimensional invariant subspace. ■

Corollary 2.4 *If H is a transitive subgroup of S_n and H contains a transposition, then the restriction of the permutation representation of S_n to $H \cap A_n$ has one 1-dimensional invariant subspace.*

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

Proof This follows from Lemma 2.3, since $H \cap A_n$ acts transitively on $\{1, 2, \dots, n\}$ by Lemma 2.2. ■

Lemma 2.5 *Let $n \geq 1$ be an integer. Let $\sigma \in A_n$ have k disjoint cycles for some positive integer $k \leq n$. Then there are k fixed vectors under σ in the permutation representation of A_n.*

Proof Let $e_1, \dots, e_n$ be a basis of the permutation representation of A_n. Let $\sigma \in A_n$ have k disjoint cycles. Then they form k partitions $C_1, \dots, C_k$ of $\{1, 2, \dots, n\}$.

For $1 \leq i \leq k$, let

$$v_i = \sum_{j \in C_i} e_j.$$

Then, these k vectors are fixed under σ. ■

Lemma 2.6 *For any even integer n, every element in A_n has more than one cycle.*

Proof Let $\sigma \in A_n$ have the cycle decomposition

$$\sigma = (a_{11} \cdots a_{1m_1})(a_{21} \cdots a_{2m_2}) \cdots (a_{k1} \cdots a_{km_k}),$$

where $a_{ij} \in \{1, 2, \dots, n\}$ are distinct and $m_1 + m_2 + \cdots + m_k = n$ for some positive integer m_i. If $k = 1$, then $m_1 = n$ and $\sigma = (a_{11}a_{12} \cdots a_{1n})$ has one cycle of length of the even integer n which is an odd permutation, hence it is not in A_n. Thus, we must have that $k \geq 2$. This implies that $\sigma \in A_n$ has at least two cycles. ■

The following two lemmas show that subgroups of S_n which occur as Galois coverings of a projective line (which is isomorphic to a projective closure of a base-point free linear system of E) act transitively on $\{1, 2, \dots, n\}$ and contain a transposition.

Lemma 2.7 *Let K be a number field and E/K an elliptic curve over K. Suppose that there is a projective line L in $E^{n-1}/S_n \cong \mathbb{P}^{n-1}$ which is a projective closure of a base point-free linear system of E. Let C be the preimage of L in E^{n-1}/A_n under the double cover from E^{n-1}/A_n to E^{n-1}/S_n and let the preimage in E^{n-1} of C under the quotient map of E^{n-1} by A_n have a decomposition $X_1 \cup X_2 \cup \cdots \cup X_k$ into irreducible components X_i.*

Then for each $i = 1, \dots, k$, the morphisms $\psi_i \colon X_i \to C$ and $\phi_i \colon X_i \to L$ are Galois coverings with $K_i = \mathrm{Gal}(X_i/C)$ and $H_i = \mathrm{Gal}(X_i/L)$, respectively, such that $K_i \leq A_n$, $H_i \leq S_n$ and $H_i \cap A_n = K_i$. Moreover, the H_i are conjugate to each other, and each H_i acts transitively on $\{1, 2, \dots, n\}$.

Proof For each $i = 1, \dots, k$, the morphism $\psi_i \colon X_i \to C$ is the quotient map by the stabilizer K_i of X_i in A_n, that is, $K_i = \{\sigma \in A_n \mid \sigma \cdot X_i = X_i\}$. Since X_i is an irreducible component of the preimage of C under the action of A_n, for any $\sigma \neq 1 \in K_i$, X_i is not contained in the kernel of $1 - \sigma$ acting on E^n. So ψ_i is a regular Galois covering map with Galois group $\mathrm{Gal}(X_i/C) = K_i$ a subgroup of A_n. Similarly, each map

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

$\phi_i \colon X_i \to L$ is also a Galois covering with Galois group $\mathrm{Gal}(X_i/L) = H_i$ which is the stabilizer of X_i in S_n and ϕ_i is the composite of the Galois covering from X_i to C with $K_i = \mathrm{Gal}(X_i/C)$ and the double cover from C to L. Hence $H_i \leq S_n$ and $H_i \cap A_n = K_i$.

First, we show that the H_i are conjugate to each other. Note that S_n acts transitively on $\{X_1, X_2, \dots, X_k\}$, since $X_1 \cup X_2 \cup \dots \cup X_k$ is the preimage of the irreducible curve L. Hence for each i, there is $\tau_i \in S_n$ such that $\tau_i \cdot X_i = X_1$. Let $\sigma \in H_1$. Then $\tau_i \cdot X_i = X_1 = \sigma \cdot X_1 = \sigma\tau_i \cdot X_i$. Hence $\tau_i^{-1}\sigma\tau_i \cdot X_i = X_i$. Hence $\tau_i^{-1}\sigma\tau_i \in H_i$. This proves that $\tau_i^{-1} H_1 \tau_i = H_i$ for each i.

Next, we show that each H_i acts transitively on $\{1, 2, \dots, n\}$. It is enough to show that H_1 acts transitively on $\{1, 2, \dots, n\}$, since H_i are conjugate to each other. Note that E^{n-1}/S_n is isomorphic to the projective closure of the linear space $|n(O)|$ of all rational functions f such that $(f) + n(O) \geq 0$ by Lemma 2.1. Since the curve $L \subset E^{n-1}/S_n$ is a projective closure of a base point-free linear system of E, there exists an elliptic function f in $H^0(E, \mathcal{L}(n(O)))$ which has n zeros which sum to O of E such that the base-point free linear system is generated by f and the constant function 1.

Parameterize an open dense subset of the projective line L in $\mathbb{P}^{n-1} \cong E^{n-1}/S_n$ by the parameter λ such that $f - \lambda$ represents a point of the open subset. Let $g \colon E^{n-1} \to E$ be defined by $g(z_1, \dots, z_n) = z_1$ where $(z_1, \dots, z_n)$ is a point of E^{n-1} so that the sum of coordinates equals O. Then, the curve $X_1 \subseteq E^{n-1}$ maps to E through g as well as to the projective line $L \in E^{n-1}/S_n$ through the quotient map by S_n. So X_1 maps to $E \times L$ and projects onto L.

Choose a fundamental domain so that the distinct zeros $z_1, \dots, z_n$ of $f - \lambda$ are in the interior of the domain. Let $i \in \{2, 3, \dots, n\}$ be fixed. We can take a path $\alpha \colon [0, 1] \to E$ such that $\alpha(0) = z_1$ and $\alpha(1) = z_i$ so that the path does not pass through the other zeros of $f - \lambda$. By composing α with f, we get a closed path in E^{n-1}/S_n starting and ending at λ, that is $f - \lambda$, since $f(z_1) = \lambda = f(z_i)$.

Since X_1 is a connected component which maps to $E \times L$ through g and ϕ_1 and the morphism ϕ_1 is a Galois covering, by the unique path homotopy lifting property of a covering space, there exist P and $Q \in X_1$ such that $\phi_1(P) = \lambda = \phi_1(Q)$, and $g(P) = z_1$ and $g(Q) = z_i$. This implies that there is an element $\sigma \in H_1$ such that $\sigma(1) = i$. This shows H_1 acts transitively on $\{1, 2, \dots, n\}$. ■

The following lemma has a similar setting as in [3, Lemma 1.5]. But here we assume that there is a divisor in a given projective line which decomposes into the sum of one ramified divisor of degree 2 and other divisors of odd degree or unramified divisors under a Galois covering, while the lemma in [3, Lemma 1.5] assumes every divisor decomposes into one ramified divisor of degree 2 and other unramified divisors.

Lemma 2.8 *Suppose there is a curve $L \subset E^{n-1}/S_n \cong \mathbb{P}^{n-1}$ which is isomorphic to a projective closure of a base-point free linear system on E and the normalization of its preimage in E^{n-1} under the quotient map is $X_1 \cup X_2 \cup \dots \cup X_k$ such that for each $m \in \{1, 2, \dots, k\}$, the Galois covering $H_m := \mathrm{Gal}(X_m/L)$ is a subgroup of S_n. Then if L contains a divisor $D = 2(P_1) + \sum_{i=2}^{\ell} k_i(P_i) - n(O)$, where P_i are points of E such that*

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

$P_i \neq P_j$, $2P_1 + \sum_{i=2}^{\ell} k_iP_i = O$ and k_i are odd integers ≥ 1 with $\sum_{i=2}^{\ell} k_i = n-2$, then each H_m contains a transposition.

Proof Note that if $k_i = 1$, for all $i = 2, \dots, \ell$, then we apply the proof in [3, Lemma 1.5] with the given divisor D to get a transposition. Now we assume the general case when k_i are odd integers.

Let $k_1 = 2$. For each $m = 1, \dots, k$, let $\phi_m \colon X_m \to L$ be the restriction of the quotient map of E^{n-1} by S_n with $H_m = \mathrm{Gal}(X_m/L)$. Let H_m act by permutation of coordinates of each point: for $\sigma \in H_m$, $\sigma \cdot (P_1, P_2, \dots, P_n) = (P_{\sigma(1)}, P_{\sigma(2)}, \dots, P_{\sigma(n)})$, where $P_n = -(P_1 + P_2 + \cdots + P_{n-1})$.

Suppose L contains a divisor $D = \sum_{i=1}^{\ell} k_i(P_i) - n(O) = 2(P_1) + \sum_{i=2}^{\ell} k_i(P_i) - n(O)$, where $P_1, \dots, P_\ell$ are distinct points of E and k_i are odd integers such that $\sum_{i=2}^{\ell} k_i = n-2$. Let f be the function whose divisor is equivalent to D and let z_i be the zeros of f corresponding to P_i for each $i = 1, \dots, \ell$, *i.e.*, $f(z) = (z - z_i)^{k_i}(a_{i0} + a_{i1}(z - z_i) + \cdots +)$ with $a_{i0} \neq 0$. Then by Hensel's Lemma [19, Chapter IV, Lemma 1.2], for a number λ with small $|\lambda|$, $f - \lambda = (z - z_i)^{k_i}(a_{i0} + a_{i1}(z - z_i) + \cdots) - \lambda$ has zeros at

$$Q_{i,j} = z_i + \left(\frac{\lambda}{a_{i0}}\right)^{\frac{1}{k_i}} \zeta_{k_i}^{j-1} + A_{i,j}, \text{ for each } i = 1, \dots, \ell, \text{ and } j = 1, \dots, k_i,$$

where $A_{i,j}$ are convergent Puiseux series in λ such that each term of $A_{i,j}$ is of higher degree than λ^{1/k_i}, and ζ_{k_i} is a primitive k_i-th root of unity.

Note that each quotient map ϕ_m by H_m is surjective. Choose a small enough number λ such that for each $i = 1, \dots, \ell$ and $j = 1, \dots, k_i$, the circles centered at z_i with radius $\left(\frac{\lambda}{a_{i0}}\right)^{1/k_i}$ do not intersect each other and the k_i points $Q_{i,j}$ lie in the circle centered at z_i.

Since these circles are closed paths and $Q_{i,j}$ are zeros of one fixed function $f - \lambda$, their preimages in E^{n-1} still lie in one irreducible component X_m for some m. Therefore, for each $i = 1, \dots, \ell$, there exists a cycle τ_i in S_n of length k_i which permutes $Q_{i,j}$ for $j = 1, \dots, k_i$ and the product of all τ_i is in H_m. In particular, τ_i are disjoint cycles and τ_1 is a transposition permuting $Q_{1,1}$ and $Q_{1,2}$.

Let $r = \mathrm{lcm}(k_2, \dots, k_\ell)$. Then r is odd, since all k_i for $i = 2, \dots, \ell$ are odd. Since τ_1 is of order 2, $(\tau_1\tau_2 \cdots \tau_\ell)^r = \tau_1 \in H_m$. Hence, H_m contains a transposition τ_1. Since M_m are conjugate to each other by Lemma 2.7, every H_m has a transposition. ∎

3 E/K for K a Totally Imaginary Number Field with a Rational Point P Such That $2P \neq O$ and $3P \neq O$

First, we show that if K is a totally imaginary number field and E/K has a K-rational point P such that $6P \neq O$, then for some even integer n there is a projective line over K in $E^{n-1}/S_n \cong \mathbb{P}^{n-1}$ whose preimage under the quotient map of E^{n-1} by A_n is a curve of genus 0 in E^{n-1} over K. We will need the following lemma to show the existence of such a projective line. We start with the definition of *rank* of quadratic forms that we use in this paper.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

Definition 3.1 The rank of a quadratic form Φ on the space V is the codimension of the orthogonal complement of V with respect to Φ in the sense of [16, Chapter IV, Section 1.2, p. 28].

Lemma 3.2 *Suppose Φ_1 and Φ_2 are two quadratic forms defined over $\overline{K}$ such that for all $r, s \in \overline{K}$, not both zero, the form $r\Phi_1 + s\Phi_2$ is of rank ≥ 5. Then the intersection of the zero loci of Φ_1 and Φ_2 is not entirely contained in a finite union of hyperplanes.*

Proof By the abuse of the notation, we denote the intersection of two hypersurfaces defined by f and g by $f \cap g$ and the union of them by $f \cup g$.

Suppose $\operatorname{codim}(\Phi_1 \cap \Phi_2 \cap L) = 2$ for some hyperplane by L. If both intersections $\Phi_1 \cap L$ and $\Phi_2 \cap L$ are irreducible, then $\Phi_1 \cap L = \Phi_2 \cap L$. Thus $\Phi_1 \equiv c\Phi_2 \pmod{L}$ for some $c \in \overline{K}$, that is, $\Phi_1 - c\Phi_2 = LL'$ for some linear form L'. Hence, the pencil of Φ_1 and Φ_2 contains some form which has rank ≤ 2, which leads to a contradiction of the hypothesis.

So we assume that a quadratic form, say Φ_1, intersected with L is reducible into two hyperplanes defined by linear forms L_2 and L_3 on the original space. Then $\Phi_1 \equiv L_2L_3 \pmod{L}$. Therefore, for some linear form L_4, $\Phi_1 = LL_4 + L_2L_3$, so it has rank ≤ 4, which is a contradiction to the hypothesis. Hence, we have shown that for every hyperplane by L,

$$\operatorname{codim}(\Phi_1 \cap \Phi_2 \cap L) < 2.$$

Now, suppose the intersection of Φ_1 and Φ_2 is entirely contained in the union of hyperplanes by $L_1, \dots, L_n$. Then

$$\min_{1 \leq i \leq n} \operatorname{codim}(\Phi_1 \cap \Phi_2 \cap L_i) = \operatorname{codim}(\Phi_1 \cap \Phi_2) = 2,$$

which is impossible. This completes the proof. ■

We will need the following weak approximation of quadrics.

Proposition 3.3 *There exists a function $F \colon \mathbb{N} \to \mathbb{N}$ with the following property: Given a non-negative integer n, a number field K, a K-vector space V, an n-dimensional K-vector space of quadratic forms $W \subset \operatorname{Sym}^2 V$ on V, and a finite set of places S of K, if for every non-zero $w \in W$ there exists an $F(n)$-dimensional subspace $V_w \subset V$ on which w is non-degenerate, then the intersection of all quadrics in W, $X_W(K)$, is dense in $\prod_{v \in S} X_W(K_v)$.*

Proof See [8, Theorem 2] for the complete proof, where we use induction on the dimension n of W to find points in $X_W(K)$. Note that we show in [8] that such a function $F(n)$ can be given explicitly by $F(n) = 2n^2 + 2n - 1$. ■

Proposition 3.4 *Let K be a totally imaginary number field. If E/K has a K-rational point P such that $2P \neq O$ and $3P \neq O$, then for some even integer n, there is a projective line over K in $E^{n-1}/S_n \cong \mathbb{P}^{n-1}$ as a projective closure of a base-point free linear system of E such that the normalization of its preimage under the double cover is a curve of*

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

genus 0 *over* K *in* E^{n-1}/A_n *which contains a divisor of a rational function on* E *of degree* n *which has one double zero and all other zeros of odd order (including simple zeros).*

Proof By Lemma 2.1, $E^{n-1}/S_n \cong \mathbb{P}^{n-1}$, which is isomorphic to the $(n-1)$-dimensional projective space $\mathbb{P}(H^0(E, \mathcal{L}(n(O))))$.

If f is an elliptic function of degree n, holomorphic except at a unique pole O, the vector space spanned by f and 1 defines a pencil of all divisors $(a+bf)+n(O)$ with $a, b \in \mathbb{C}$ on E linearly equivalent to $n(O)$, or equivalently, a line on $E^{n-1}/S_n \cong \mathbb{P}^{n-1}$. Note that since P is neither 2-torsion nor 3-torsion, we have that $-2P \notin \{P, O\}$. Now we find an elliptic function f of degree $n = 2k$ for some integer k, whose derivative is of the form $f' = lh^2$, where l has the divisor $2(P) + (-2P) - 3(O)$ and h is in the vector space of elliptic functions defined over K with divisors $\geq (1-k)(O)$. Let $y + ax + b = 0$ be the affine tangent line at a K-rational point P and let $l := y + ax + b$. Let f and f' be as follows:

Case 1 Suppose $n \equiv 0 (\mathrm{mod} 4)$. Let $n = 4m$ for some integer m. For parameters $a_0, \dots, a_{m-1}, b_0, \dots, b_{m-3}, d_0, \dots, d_{2m-2}, c_1, \dots, c_{2m}$ to be determined and the given tangent line $l = 0$, let

$$f(z) = y(d_{2m-2}x^{2m-2} + \cdots + d_1x + d_0) + c_{2m}x^{2m} + \cdots + c_1x$$

and

$$f'(z) = l(h(z))^2,$$

where $h(z) = a_{m-1}x^{m-1} + \cdots + a_1x + a_0 + y(x^{m-2} + \cdots + b_1x + b_0)$.

Case 2 Suppose $n \equiv 2 (\mathrm{mod}\, 4)$. Let $n = 4m+2$ for some integer m. For parameters $a_0, \dots, a_{m-1}$, $b_0, \dots, b_{m-2}$, $d_0, \dots, d_{2m-1}$, $c_1, \dots, c_{2m+1}$ to be determined and the given tangent line $l = 0$, let

$$f(z) = y(d_{2m-1}x^{2m-1} + \cdots + d_1x + d_0) + c_{2m+1}x^{2m+1} + \cdots + c_1x$$

and

$$f'(z) = l(h(z))^2,$$

where $h(z) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0 + y(b_{m-2}x^{m-2} + \cdots + b_1x + b_0)$.

From the equations obtained by equating the coefficient of each x^iy^j-term of $f'(z)$ with that of the derivative of $f(z)$ given in the above form (equivalently, by equating f with the integral of f' along two periods of E), we get two quadratic equations over K in $\frac{n-4}{2}$ variables, namely $a_0, \dots, a_{m-1}, b_0, \dots, b_{m-4}$ and b_{m-3} if $n = 4m$, and $a_0, \dots, a_{m-1}, b_0, \dots, b_{m-3}$ and b_{m-2} if $n = 4m+2$. Homogenize these two quadratic equations to get two quadratic forms in $\frac{n-4}{2} + 1$ variables with a new variable. We need to find a common isotropic vector over K of two quadratic forms which defines a common solution of two original quadratic equations, (that is, which is outside the hyperplane at ∞) and defines $f' = lh^2$ such that $h(-2P) \neq 0$ in the above notation of cases 1 and 2.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

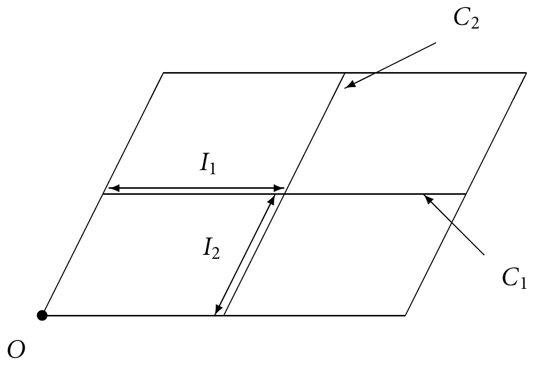

Figure 1: A fundamental domain D of E with two periods C_1 and C_2

Let D be a fundamental domain of E and C_1 and C_2 be two line segments dividing the fundamental domain of E into four congruent parallelograms and I_1 and I_2 the first half line segments of C_1 and C_2 respectively, as shown in Figure 1.

Let $M = \max\{F(2), 5\}$, where F is the function given in Proposition 3.3. We can choose $2M$ holomorphic functions $f_1, \dots, f_{2M}$ on $I_1 \cup I_2$ such that

$$\int_{I_1} lf_i f_j\,dz = \int_{I_2} lf_i f_j\,dz = 0, \text{ for } i \neq j,$$

$$\int_{I_1 \cup I_2} lf_i^2\,dz = \int_{I_1} lf_i^2\,dz \neq 0, \text{ for } i = 1, 2, \dots, M,$$

$$\int_{I_1 \cup I_2} lf_i^2\,dz = \int_{I_2} lf_i^2\,dz \neq 0, \text{ for } i = M+1, , \dots, 2M.$$

Since the Weierstrass $\wp$-function $x = \wp(z)\colon I_1 \cup I_2 \to \mathbb{C}$ is injective, its inverse $\wp^{-1}$ is well defined on the image $\wp(I_1 \cup I_2)$ and the image is a compact contractible set in $\mathbb{C}$. Hence the complement of $\wp(I_1 \cup I_2)$ is connected. So by Mergelyan's Theorem [15, p. 390], each holomorphic function $f_i \circ \wp^{-1}\colon \wp(I_1 \cup I_2) \to \mathbb{C}$ can be approximated by some polynomial $p_i(z)$, for each $i = 1, \dots, 2M$. Moreover, since K is a totally imaginary number field, K is dense in $\left(\prod_{v \in S_\infty} \mathbb{C}\right)$ with respect to the usual topology for any embeddings of K in $\mathbb{C}$, where S_∞ is the set of all infinite places. Hence we may assume that coefficients of $p_i(z)$ are in K. So each f_i can be approximated by the polynomial $p_i(x)$ in terms of $x = \wp(z)$ with coefficients in K.

Let W be a space of dimension $\geq 2M$ generated by elliptic functions including all of $p_i(x)$ for $i = 1, \dots, 2M$. Integrating functions in W defines quadratic polynomials and by homogenizing them, we get quadratic forms. Then any two quadratic forms Φ_1 and Φ_2 over K obtained from this homogenization of the integration on W satisfy the property:

for any $r, s \in \overline{K}$ not both zero, any form in the pencil $r\Phi_1 + s\Phi_2$ is of rank $\geq M$.

For example, if $r = 0$, then the M functions $p_i(x)$ for $i = M+1, \dots, 2M$ generate an M-dimensional non-degenerate subspace of W for the form $r\Phi_1 + s\Phi_2$. If $s = 0$,

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

then $p_i(x)$ for $i = 1, \dots, M$ generates an M-dimensional non-degenerate subspace for $r\Phi_1 + s\Phi_2$. And if neither r nor s is zero, either the M functions $p_i(x)$ for $i = M+1, \dots, 2M$ or for $i = 1, \dots, M$ generate an M-dimensional non-degenerate subspace.

Hence, any pencil of Φ_1 and Φ_2 has rank $\geq F(2)$, since $M \geq F(2)$. Then since K is totally imaginary, the previous argument implies that the hypothesis of Proposition 3.3 is satisfied. So by Proposition 3.3 it has the weak approximation. Therefore, the set of K-rational points in the intersection of Φ_1 and Φ_2 on a non-degenerate subspace of dimension $\geq M$ is Zariski-dense in the variety defined by Φ_1 and Φ_2.

Let L be the hyperplane at ∞ and L' the hyperplane defined by $h(-2P)$ in the above notation of $f' = lh^2$ in case 1 or 2. By Lemma 3.2 the intersection of two forms Φ_1 and Φ_2 is not contained in the union of two hyperplanes defined by L and L'. Hence, by the density of K-rational points, we can get a nontrivial common zero over K which is a common zero of two original quadratic equations which defines an elliptic function f such that $f' = lh^2$ for some elliptic function h such that $h(-2P) \neq 0$.

Now we take the projective closure V over K of the linear subspace of

$$\mathbb{P}(H^0(E, \mathcal{L}(n(O))))$$

generated by f and the constant function 1 over K. Note that the linear space generated by f and 1 is a base-point free linear system on E from the construction. Then V is isomorphic to the projective line $\mathbb{P}^1(K)$. And the normalization $X \subseteq E^{n-1}/A_n$ of its preimage under the 2-1 map from E^{n-1}/A_n to E^{n-1}/S_n meets the ramification divisor wherever the divisor $f - \lambda$ for some λ has a zero or a pole of even multiplicity ≥ 2, that is, wherever its derivative $(f - \lambda)' = f'$ has a zero or a pole of odd order. And by Lemma 3.5 X has only two points which meet the ramification locus at $-2P$ and O to odd contact order. Hence by the Hurwitz formula, the normalization of X in E^{n-1}/A_n is a curve of genus 0 defined over K. By subtracting the constant $\lambda_p = f(-2P)$ from f, the function $f - \lambda_p$ has one double zero at $-2P$ and other zeros of odd order, since f' has only one simple zero at $-2P$ and other zeros of even order. ■

Lemma 3.5 *Under the same notation as in the proof of Proposition* 3.4*, if an elliptic function f has a zero (or a pole) at a point P of order m, the contact order of f with the ramification locus of the double cover from E^{n-1}/A_n onto E^{n-1}/S_n at P is $m-1$.*

Proof Suppose f has a zero α corresponding to the zero P of order m. Let $f(z) = (z-\alpha)^m(a_0 + a_1(z-\alpha) + \cdots +$ higher terms in $(z-\alpha))$, where $a_0 \neq 0$.

Note that the ramification locus under the quotient map from E^{n-1} to E^{n-1}/S_n is the zero locus of $\prod_{i<j}(z_i - z_j)$, where z_i are zeros of $f - \lambda$ for a parameter λ, that is, the quotient map is ramified whenever $f - \lambda$ has a double zero. By considering the ramification index, since the degree of the map from E^{n-1}/A_n onto E^{n-1}/S_n is 2, the ramification locus under the double cover from E^{n-1}/A_n onto E^{n-1}/S_n is the

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

zero locus of the discriminant of $f - \lambda$, that is,

$$\prod_{i<j} (z_i - z_j)^2,$$

where z_i are zeros of $f - \lambda$. If we write the discriminant of $f - \lambda$ in terms of λ with small $|\lambda|$, then its degree with respect to λ is the contact order of f at P. We may assume that $\alpha = 0$ by translation. Hence we have

$$f - \lambda = 0 \Leftrightarrow z^m(a_0 + a_1 z + a_2 z + \cdots + \text{ higher terms in } z) - \lambda = 0.$$

By Hensel's Lemma [19, Chapter IV, Lemma 1.2] on $\mathbb{C}[[\lambda^{\frac{1}{m}}]]$, all zeros of $z^m(a_0 + a_1 z + a_2 z + \cdots + \text{ higher terms in } z) - \lambda$ are

$$z_i = \left(\frac{\lambda}{a}\right)^{\frac{1}{m}} \zeta_m^i + A_i(\lambda), \text{for } 0 \le i \le m - 1,$$

where ζ_m is a primitive m-th root of unity, and $A_i(\lambda)$ is a convergent Puiseux series in λ, that is, a convergent power series in $\lambda^{\frac{1}{m}}$. Hence the degree of the discriminant of $f - \lambda$ with respect to λ is $\frac{1}{m} \cdot \binom{m}{2} \cdot 2 = m - 1$, which is the contact order at α with the ramification locus. For a pole, we proceed similarly, replacing f by $1/f$. ■

Next, we examine the Galois theory of the fixed fields $\overline{K}^{\sigma}$ under automorphisms $\sigma \in \mathrm{Gal}(\overline{K}/K)$. We give some definitions.

Definition 3.6 A field F is (*formally*) real, if -1 is not a sum of squares in F. A real field F is real closed if no algebraic extension of F is real.

Lemma 3.7 *Let K be a number field. Then for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$,*

$$\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma}) \cong \prod_{p\in S} \mathbb{Z}_p \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z},$$

where S is a set of prime integers. In particular, if K is totally imaginary, $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ has no torsion element, hence, the Brauer group $\mathrm{Br}(\overline{K}^{\sigma})$ of the fixed field under σ is trivial.

Proof Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ is isomorphic to the closure of the subgroup generated by σ in the sense of the Krull topology by [13, Theorem 17.7]. Hence,

$$\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma}) \cong \prod_{p\in S} \mathbb{Z}_p \times \prod_{p\in T} \mathbb{Z}/p^{m_p}\mathbb{Z} \cong \prod_{p\in S} \langle \sigma_p \rangle \times \prod {}_{\text{-}}p \in T \langle \tau_p \rangle,$$

where S and T are disjoint sets of primes, m_p are positive integers, and τ_p has a finite order p^{m_p}. But since any element in $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ has the order $1, 2$ or ∞ by Artin–Schreier theorem [9, Theorem 25.1], the torsion part of $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ is trivial or $\mathbb{Z}/2\mathbb{Z}$. Moreover, if there are $q \in T$ and $p \in S \cup (T - \{q\})$, then, τ_q is an involution and

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

its fixed field $\overline{K}^{\tau_q}$ is a real closed field by [9, Theorem 25.13]. Also $\sigma_p^{-1}\tau_q\sigma_p = \tau_q$, so σ_p induces a nontrivial automorphism of $\overline{K}^{\tau_q}$. This contradicts the uniqueness of an isomorphism between two real closed fields [10, XI, §2, Theorem 2.9, p. 455]. Therefore,

$$\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma}) \cong \prod_{p\in S}\mathbb{Z}_p \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z}.$$

On the other hand, if $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ generated by τ, then $[\overline{K}:\overline{K}^{\tau}] = 2$, so $\overline{K}^{\tau}$ is real-closed by [9, Theorem 25.13], so it has a real embedding by [9, Theorem 25.18]. Hence if $K \subseteq \overline{K}^{\tau}$ is totally imaginary, then $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ is isomorphic to $\prod_{p\in S}\mathbb{Z}_p$. Then since $\overline{K}^{*}$ is a divisible topological $\prod_{p\in S}\mathbb{Z}_p$-group, $H^2(\prod_{p\in S}\mathbb{Z}_p, \overline{K}^{*})$ is trivial by [14, Proposition 1.6.13.(ii)]. Therefore, $Br(\overline{K}^{\sigma}) = 0$. ■

Lemma 3.8 *Let K be a totally imaginary number field. Then for any $\sigma \in \mathrm{Gal}(\overline{K}/K)$, a conic curve X defined over K has a $\overline{K}^{\sigma}$-rational point.*

Proof Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Since a conic can be identified with an element of $\mathrm{Br}(\overline{K}^{\sigma})$ as a Severi–Brauer variety of dimension 1, and $\mathrm{Br}(\overline{K}^{\sigma}) = 0$ by Lemma 3.7, a conic is isomorphic to $\mathbb{P}^1$ over $\overline{K}^{\sigma}$. Equivalently, it has a $\overline{K}^{\sigma}$-rational point. ■

Let $f \in K(t_1,\dots,t_m)[X_1,\dots,X_n]$ be a polynomial with coefficients in the quotient field $K(t_1,\dots,t_m)$ of $K[t_1,\dots,t_m]$ which is irreducible over $K(t_1,\dots,t_m)$. We define

$$H_K(f) = \{(a_1,\dots,a_m) \in K^m \mid f(a_1,\dots,a_m,X_1,\dots,X_n) \text{ is irreducible over } K\}$$

to be the Hilbert set of f over K. We need the following lemma.

Lemma 3.9 *Let L be a finite separable extension of K and let $f \in L(t_1,\dots,t_m)[X_1,\dots,X_n]$ is an irreducible polynomial over the quotient field $L(t_1,\dots,t_m)$. Then there exists a polynomial $p \in K[t_1,\dots,t_m,X_1,\dots,X_n]$ such that p is irreducible over $K(t_1,\dots,t_m)$ and $H_K(p) \subseteq H_L(f)$.*

Proof For a given irreducible polynomial $f \in L(t_1,\dots,t_m)[X_1,\dots,X_n]$, by [2, Lemma 11.6], there is an irreducible polynomial $q \in K(t_1,\dots,t_m)[X_1,\dots,X_n]$ such that $H_K(q) \subseteq H_L(f)$. By [2, Lemma 11.1], there is an irreducible polynomial $p \in K[t_1,\dots,t_m,X_1,\dots,X_n]$ which is irreducible over $K(t_1,\dots,t_m)$ such that $H_K(p) \subseteq H_K(q)$. Hence the Hilbert set $H_L(f)$ of f over L contains the Hilbert set $H_K(p)$ of p over K. ■

Let G be a finite group and Λ an n-dimensional G-representation. Then G acts on $E \otimes \Lambda$ through its action on Λ. Define $E \otimes \Lambda$ to be the abelian variety representing the functor $S \mapsto E(S) \otimes_{\mathbb{Z}} \Lambda$, where S is any scheme over the ground field and $E(S)$ is the functor of points associated to E. Then as an abelian variety $E \otimes \Lambda$ is just E^n, since the action of G on $E \otimes \Lambda$ is only though Λ. With this background, we prove the following proposition.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

Proposition 3.10 *Let K be a totally imaginary number field and $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Let G be a nontrivial finite group and Λ an n-dimensional integral G-representation for a positive integer n and G act on $E^n \cong E \otimes \Lambda$ through Λ. Suppose that there is a curve X of genus 0 in E^n/G over K. Suppose the preimage of X under the quotient map by G is decomposed into k irreducible curves $C_1, \dots, C_k$ such that each $C_j \to X$ is a Galois covering with $\mathrm{Gal}(C_j/X) \leq G$. Then*

(i) *X cannot be decomposed completely,* i.e., *$k < |G|$;*
(ii) *$\mathrm{Gal}(C_j/X)$ are conjugate to each other in G, for $j = 1, \dots, k$;*
(iii) *for an irreducible component $C \subseteq E^n$ in the preimage of X, there exist a finite extension F of K and an infinite sequence $\{L_i/F\}_{i=1}^{\infty}$ of linearly disjoint finite Galois extensions of F such that $F \subseteq \overline{K}^{\sigma}$ and for each i,*
    (1) *$\mathrm{Gal}(L_i/F)$ is naturally isomorphic to $\mathrm{Gal}(C/X)$ as a subgroup of G, and*
    (2) *there exists a submodule M_i of $E(L_i) \otimes \mathbb{Q}$ isomorphic to $\Lambda \otimes \mathbb{Q}$ as a $\mathrm{Gal}(L_i/F)$-module via the inclusion $\mathrm{Gal}(L_i/F) \hookrightarrow G$.*

In particular, if K is an arbitrary number field and X is isomorphic to $\mathbb{P}^1$ over K, then this holds with $F = K$. And if the preimage of X in E^n is irreducible, then each $\mathrm{Gal}(L_i/F)$ is isomorphic to G itself.

Proof Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. If the curve X of genus 0 has a K-rational point, then $X \cong \mathbb{P}^1$ over K. If not, it is isomorphic to a conic curve. Then since K is totally imaginary, by Lemma 3.8, for every $\sigma \in \mathrm{Gal}(\overline{K}/K)$, X has a $\overline{K}^{\sigma}$-rational point. Choose a point of X over $\overline{K}^{\sigma}$ and let F be the field of definition of this point. Then $F \subseteq \overline{K}^{\sigma}$, F is a finite extension of K, and X is isomorphic to $\mathbb{P}^1$ over F. Now we consider $X \subseteq E^n/G$ as $\mathbb{P}^1$ over F. Note that if $X \cong \mathbb{P}^1$ over K, then we can take $F = K$.

First, suppose that the preimage of the curve X in E^n under the quotient map by G is an irreducible curve C with the function field $F(C)$, that is, $k = 1$. Then the restricted quotient map $\phi\colon C \to X$ by G realizes $F(C)$ as a Galois extension of the function field $F(x)$ of $X(F) \cong \mathbb{P}^1_F$ with the Galois group isomorphic to G. By the theorem of the primitive element, there exists $t \in F(C)$ such that $F(C) = F(x, t)$ and

$$g_m t^m + g_{m-1} t^{m-1} + \cdots + g_1 t + g_0 = 0,$$

where g_i are polynomials in $F[x]$. Choose a minimal polynomial of t over $F(x)$ and clear its denominators so that we let $f(x, y)$ be a minimal polynomial of t in $F[x, y]$. Then f is absolutely irreducible over F, so it is irreducible over $F(x)$.

By [18, Lemma], the set $\bigcup_{[L:F] \leq k} E(L)_{\mathrm{tor}}$ is a finite set, where the union runs over all finite extensions L of F whose degree over F is $\leq k$, where $k = |G|$. Let L' be a finite field extension of F over which all points of $\bigcup_{[L:F] \leq k} E(L)_{\mathrm{tor}}$ are defined. Applying Lemma 3.9 and [2, Lemma 12.12] to f over L', we can choose $x_1 \in H_F(f) \cap K$ such that the specialization $x \mapsto x_1$ preserves the Galois group G and there is a point Q_1 of $C \subseteq E^n \cong E \otimes \Lambda$ in the preimage $\phi^{-1}((1\!:\!x_1))$ of $(1\!:\!x_1) \in \mathbb{P}^1(F) \cong X$ under ϕ which is defined over a finite Galois extension L_1 of F with $\mathrm{Gal}(L_1/F) \cong G$. That is, the preimage of $(1\!:\!x_1)$ under ϕ consists of a single point, $\mathrm{Spec}\, L_1$. Let Λ^* be the dual of Λ with the action of G. Then the morphism from $\mathrm{Spec}\, L_1$ to $E \otimes \Lambda$ induces a $\mathbb{Z}[G]$-linear map $g\colon \Lambda^* \to E(L_1)$ given by $\lambda^* \mapsto \sum_j \lambda^*(\lambda_j) P_j$, where $Q_1 = \sum_j P_j \otimes \lambda_j \in E \otimes \Lambda$.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

Since $f(x_1, y)$ is irreducible over L', two extensions L_1 and L' are linearly disjoint over F. So for $\lambda^* \in \Lambda^*$, $g(\lambda^*) \in E(L_1)$ is a non-torsion point. Then if we let $M_1 \subseteq E(L_1) \otimes \mathbb{C}$ be the submodule generated by the points of $E(L_1)$ in the image of Λ^* under the given map g in the above, it is a submodule of $E(L_1) \otimes \mathbb{Q}$ isomorphic to $\Lambda^* \otimes \mathbb{Q}$ as a $\mathrm{Gal}(L_1/F)$-module via the natural isomorphism $\mathrm{Gal}(L_1/F) \cong G$. Since Λ is a finite dimensional integral representation, it is isomorphic to its dual Λ^* as G-representations. So M_1 is isomorphic to $\Lambda \otimes \mathbb{Q}$ as a $\mathrm{Gal}(L_1/F)$-module.

Now suppose the preimage of X is decomposed into a union of irreducible curves $C_1 \cup C_2 \cup \cdots \cup C_k$, where $k \geq 2$. Then G acts transitively on the set of k curves and each $\mathrm{Gal}(C_j/K)$ can be identified with the stabilizer of C_j in G, so $\mathrm{Gal}(C_j/K)$ are conjugate to each other. If $k = |G|$, then this implies that $C_j \cong \mathbb{P}^1$ in E^n, which is impossible, because no abelian variety contains $\mathbb{P}^1$ as a subvariety. So $k < |G|$.

Let C be one of irreducible components C_j. Applying the same argument with the quotient map from the fixed component C to X, we get a Galois extension L_1 of F with the Galois group $\mathrm{Gal}(L_1/F)$ which is isomorphic to the stabilizer $\mathrm{Gal}(C/X) \leq G$ of C in G, and a $\mathrm{Gal}(L_1/F)$-submodule M_1 of $E(L) \otimes \mathbb{Q}$ generated by n non-torsion points of $E(L_1)$ which is isomorphic to $\Lambda \otimes \mathbb{Q}$ as a $\mathrm{Gal}(L_1/F)$-module via the natural inclusion $\mathrm{Gal}(L_1/F) \hookrightarrow G$.

Inductively, suppose we have found linearly disjoint finite Galois extensions $L_1, L_2, \ldots, L_k$ of F and for each $i = 1, 2, \ldots, k$, there is a submodule M_i of $E(L_i) \otimes \mathbb{Q}$ isomorphic to $\Lambda \otimes \mathbb{Q}$ as a $\mathrm{Gal}(L_i/F)$-module via the natural inclusion $\mathrm{Gal}(L_1/F) \hookrightarrow G$. By applying Lemma 3.9 and [2, Lemma 12.12] to f over the composite field $L'L_1L_2 \cdots L_k$, there is a point $x_{k+1} \in X(F)$ such that the specialization $x \mapsto x_{k+1}$ preserves the Galois group G, and a point in the preimage of x_{k+1} in C is defined over a Galois extension L_{k+1} of F which is linearly disjoint from $L'L_1L_2 \cdots L_k$ and has the Galois group isomorphic to a subgroup of G. Then, similarly, we get a $\mathrm{Gal}(L_{k+1}/F)$-submodule M_{k+1} generated by n non-torsion points of $E(L_{k+1})$ isomorphic to $\Lambda \otimes \mathbb{Q}$ via $\mathrm{Gal}(L_{k+1}/F) \hookrightarrow G$. This completes the proof. ■

Corollary 3.11 *Let K be a totally imaginary number field and E/K an elliptic curve over K with a K-rational point such that $2P \neq O$ and $3P \neq O$. Let Λ be the $(n-1)$-dimensional irreducible quotient representation space of the natural permutation representation of the alternating group A_n by the trivial representation. Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. Then for some even integer n, there exists a finite extension $F \subseteq \overline{K}^{\sigma}$ over K and an infinite sequence $\{L_i/F\}_{i=1}^{\infty}$ of linearly disjoint finite Galois extensions of F such that for each i,*

(i) *$\mathrm{Gal}(L_i/F)$ acts transitively on $\{1, 2, \ldots, n\}$ as a subgroup of A_n, and*

(ii) *there exists a submodule M_i of $E(L_i) \otimes \mathbb{Q}$ isomorphic to the $(n-1)$-dimensional irreducible quotient representation space $\Lambda \otimes \mathbb{Q}$ as a $\mathrm{Gal}(L_i/F)$-module via the natural inclusion $\mathrm{Gal}(L_i/F) \hookrightarrow A_n$.*

Proof By Proposition 3.4, there is a curve X of genus 0 defined over K in E^{n-1}/A_n, for some even integer n. So by Proposition 3.10, there exist such an infinite sequence of Galois extensions L_i and submodules M_i of $E(L_i) \otimes \mathbb{Q}$ isomorphic to the $(n-1)$-dimensional irreducible quotient representation space $\Lambda \otimes \mathbb{Q}$ of A_n as

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

a $\mathrm{Gal}(L_i/F)$-module via the natural inclusion $\mathrm{Gal}(L_i/F) \hookrightarrow A_n$. And by Proposition 3.4, Proposition 3.10, and Lemma 2.7, for each $\mathrm{Gal}(L_i/F)$ as a subgroup of A_n, there is a subgroup $H_i \leq S_n$ such that $H_i \cap A_n \cong \mathrm{Gal}(L_i/F)$ and which acts transitively on $\{1, 2, \ldots, n\}$. Moreover, the image of X given by Proposition 3.4 under the 2-to-1 map from E^{n-1}/A_n onto E^{n-1}/S_n has a divisor which decomposes into one divisor of ramification degree 2 and other divisors of odd degree. So by Lemma 2.8, H_i contains a transposition. Therefore, by Lemma 2.2, $\mathrm{Gal}(L_i/F)$ also acts transitively on $\{1, 2, \ldots, n\}$. ■

Lemma 3.12 *Let E/K be an elliptic curve over a number field K. Let d be a positive integer ≥ 2. Suppose $\{L_i/K\}_{i=1}^{\infty}$ is an infinite sequence of linearly disjoint finite Galois extensions of K whose degrees $[L_i\!:\!K]$ are $\leq d$ and $\{P_i\}_{i=1}^{\infty}$ is an infinite sequence of points in $E(\overline{K})$ such that for each i, $P_i \in E(L_i)$ but $P_i \notin E(K)$. Then there is an integer N such that $\{P_i\}_{i \geq N}$ is a sequence of linearly independent non-torsion points of E.*

Proof By [18, Lemma], the set $S = \bigcup_{[L:K] \leq d} E(L)_{\mathrm{tor}}$ is a finite set, where the union runs all over finite extensions L of K whose degree over K is $\leq d$. So there is a finite extension F of K over which all points of S are defined and there is an integer n such that $nP = O$, for all $P \in S$. Let n be such a fixed integer and let T be the set of all points P of $E(\overline{K})$ such that $nP \in E(K)$. Then since $E(K)$ is finitely generated by the Mordell–Weil theorem [19, Chapter VIII], there is a finite extension F' of K over which all points of T are defined. Then all but finitely many fields L_i in the given sequence $\{L_i/K\}_{i=1}^{\infty}$ are linearly disjoint from F and F' over K. This implies that there is an integer N such that points P_i for all $i \geq N$ are non-torsion points in $E(L_i)$. And by linear disjointness of fields L_i, F and F' over K, we have that for all $i \geq N$,

$$E(L_i) \cap S \subseteq E(K)_{\mathrm{tor}} \quad \text{and} \quad E(L_i) \cap T \subseteq E(K).$$

Note that since each $P_i \notin E(K)$, we have that for any integer $m \geq N$ and for each i such that $N \leq i \leq m$, there is an automorphism $\tau_i \in \mathrm{Gal}(\overline{K}/K)$ such that $\tau_i|_{L_j} = \mathrm{id}_{L_j}$ for all $N \leq j \neq i \leq m$, but $\tau_i(P_i) \neq P_i$. Moreover, we may choose such a τ_i that $\tau_i(P_i) - P_i$ is not a torsion point. In fact, otherwise, for every restriction $\tau_i|_{L_i} \in \mathrm{Gal}(L_i/K)$ of τ_i, $\tau_i|_{L_i}(P_i) - P_i$ is a torsion point in $E(L_i)$. Hence, $\tau_i|_{L_i}(P_i) - P_i \in E(L_i) \cap S \subseteq E(K)_{\mathrm{tor}}$. Then $n(\tau_i|_{L_i}(P_i) - P_i) = O$ so $\tau_i|_{L_i}(nP_i) = nP_i$ for all $\tau_i|_{L_i} \in \mathrm{Gal}(L_i/K)$. This implies $nP_i \in E(K)$ so $P_i \in T \cap E(L_i) \subseteq E(K)$ which contradicts the assumption that $P_i \notin E(K)$. Hence, we conclude that for each i such that $N \leq i \leq m$, there is an automorphism $\tau_i \in \mathrm{Gal}(\overline{K}/K)$ such that $\tau_i|_{L_j} = \mathrm{id}_{L_j}$ for all $N \leq j \neq i \leq m$, but $\tau_i(P_i) - P_i$ is a non-trivial and non-torsion point of E.

Let $m \geq N$ be a given positive integer. Suppose that for some integers a_i,

$$a_N P_N + a_{N+1} P_{N+1} + \cdots + a_m P_m = 0.$$

By the claim above, for each $i = N, N+1, \ldots, m$, there is an automorphism $\tau_i \in \mathrm{Gal}(\overline{K}/K)$ such that $\tau_i|_{L_j} = \mathrm{id}_{L_j}$ for all $1 \leq j \neq i \leq m$ but $\tau_i(P_i) - P_i$ is a non-trivial and non-torsion point of E. Now we apply such τ_i to get

$$a_N P_N + a_{N+1} P_{N+1} + \cdots + a_{i-1} P_{i-1} + a_i \tau_i(P_i) + a_{i+1} P_{i+1} + \cdots + a_m P_{i_m} = 0.$$

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

So by subtracting, we get $a_i(P_i - \tau_i(P_i)) = 0$, which implies $a_i = 0$. Hence any non-torsion points in $\{P_i\}_{i \geq N}$ are linearly independent. ■

Theorem 3.13 *Let K be a totally imaginary number field. Suppose E/K has a K-rational point P such that $2P \neq O$ and $3P \neq O$. Then for each $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $E(\overline{K}^{\sigma})$ has infinite rank.*

Proof Let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. By Proposition 3.4 and Corollary 3.11, there are a finite extension $F \subseteq \overline{K}^{\sigma}$ over K and an infinite sequence $\{L_i/F\}_{i=1}^{\infty}$ of linearly disjoint finite Galois extensions of F such that the Galois group $\mathrm{Gal}(L_i/F)$ acts transitively on $\{1, 2, \dots, n\}$ as a subgroup of A_n for some even integer n. And for each i, there is a $\mathrm{Gal}(L_i/F)$-submodule of $E(L_i) \otimes \mathbb{Q}$ which is isomorphic to the restriction of the natural $(n-1)$-dimensional quotient of the permutation representation of A_n to $\mathrm{Gal}(L_i/F)$.

Let $\sigma_i = \sigma|_{L_i}$ be the restriction of σ to L_i. Then since $F \subseteq \overline{K}^{\sigma}$, $\sigma_i|_F = \mathrm{id}_F$. Therefore, $\sigma_i \in \mathrm{Gal}(L_i/F) \leq A_n$. Let $E(L_i^{\sigma_i})$ be the group of fixed points of $E(L_i)$ under σ_i. Then obviously, $E(L_i^{\sigma_i}) \subseteq E(\overline{K}^{\sigma})$. Since n is even, each M_i of $E(L_i) \otimes \mathbb{Q}$ has a fixed element v_i under σ_i by Lemma 2.6 and Lemma 2.5.

Note that each v_i is not a torsion point and not defined over F. In fact, if v_i is defined over F, then v_i is fixed under every element in $\mathrm{Gal}(L_i/F)$. But since $\mathrm{Gal}(L_i/F)$ acts transitively on $\{1, 2, \dots, n\}$, by Lemma 2.3 there is no fixed vector of the restriction to $\mathrm{Gal}(L_i/F)$ of the $(n-1)$-dimensional quotient of the permutation representation of $A_n \leq S_n$. Then by Lemma 3.12 there is an integer N such that $\{v_i\}_{i \geq N}$ are linearly independent.

Since $v_i \in E(L_i^{\sigma_i}) \otimes \mathbb{Q}$ for each i, the module generated by $\{v_i\}_{i=1}^{\infty}$ over $\mathbb{Q}$ is a submodule of $E\big(\prod_{i=1}^{\infty} L_i^{\sigma_i}\big) \otimes \mathbb{Q}$. Hence

$$E(\overline{K}^{\sigma}) \otimes \mathbb{Q} \supseteq E\Big(\prod_{i=1}^{\infty} L_i^{\sigma_i}\Big) \otimes \mathbb{Q} \supseteq \{v_i\}_{i=1}^{\infty} \supseteq \{v_i\}_{i \geq N}$$

is infinite dimensional. ■

4 Infinite Rank over the Fixed Fields under Complex Conjugation Automorphisms

As we have seen in the proof of Proposition 3.4 and Lemma 3.8, if K has no real embeddings, then the fixed field $\overline{K}^{\sigma}$ under an element $\sigma \in \mathrm{Gal}(\overline{K}/K)$ has no real embeddings and there exists a rational curve over $\overline{K}^{\sigma}$ in the quotient space E^{n-1}/A_n for some n. So if $\overline{K}^{\sigma}$ has a real embedding, there may be a potential obstruction to find a rational curve over $\overline{K}^{\sigma}$ in E^{n-1}/A_n. So this is the only difficulty in proving the rank of $E(\overline{K}^{\sigma})$ is infinite.

In this section, we consider complex conjugation automorphisms of $\overline{K}$ and prove that without hypothesis on rational points of elliptic curves and the ground field, the rank of an elliptic curve over the fixed field under every complex conjugation automorphism is infinite.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

Definition 4.1 A field F is called an ordered field with the positive set P, if $F = P \sqcup \{0\} \sqcup -P$, a disjoint union, where P is a subset of F closed under addition and multiplication.

Now we prove the following two lemmas by using the relation between real fields (see Definition 3.6) and ordered fields.

Lemma 4.2 *If a field F is ordered (or real) and algebraic over $\mathbb{Q}$, then F has a real embedding θ, that is, $\theta(F) \subseteq \mathbb{R} \cap \overline{F}$, where $\overline{F}$ is an algebraic closure in $\mathbb{C}$.*

Proof By [9, Corollary 25.22, p. 411], a field F is ordered if and only if it is real. Hence, F is real. And since F is real and algebraic over $\mathbb{Q}$, by [9, Theorem 25.18, p. 410] there exists an isomorphism from F into $\mathbb{R} \cap \overline{F}$. ■

We give some equivalent statements of complex conjugation automorphisms.

Lemma 4.3 *For an automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$ the following statements are equivalent.*

(i) *$\overline{K}^{\sigma}$ has a real embedding θ, that is, $\theta(\overline{K}^{\sigma}) \subseteq \mathbb{R} \cap \overline{K}$.*
(ii) *σ is a complex conjugation automorphism, that is, the order of σ in $\mathrm{Gal}(\overline{K}/K)$ is 2.*
(iii) *$\overline{K}^{\sigma} \cong \mathbb{R} \cap \overline{K}$.*

Proof Suppose (i). Then

$$\langle\sigma\rangle \cong \mathrm{Gal}(\overline{K}/\overline{K}^{\sigma}) \cong \mathrm{Gal}(\overline{K}/\theta(\overline{K}^{\sigma})) \trianglerighteq \mathrm{Gal}(\overline{K}/\mathbb{R} \cap \overline{K}) \cong \mathbb{Z}/2\mathbb{Z},$$

since $[\overline{K} : \mathbb{R} \cap \overline{K}] = 2$. Hence, $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ has a torsion subgroup of order 2. Then by Lemma 3.7 $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma})$ itself is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Since σ is not trivial, we have $\mathrm{Gal}(\overline{K}/\overline{K}^{\sigma}) \cong \mathrm{Gal}(\overline{K}/\mathbb{R} \cap \overline{K})$, hence, the order of σ is 2, which implies (ii). And $\overline{K}^{\sigma} \cong \mathbb{R} \cap \overline{K}$, which implies (iii).

Now we suppose (iii). Then the order of σ equals the degree $[\overline{K} : \overline{K}^{\sigma}]$ which is equal to $[\overline{K} : \mathbb{R} \cap \overline{K})] = 2$, and this implies (ii).

Suppose (ii). Then $[\overline{K} : \overline{K}^{\sigma}] = 2$. By [9, Theorem 25.13], $\overline{K}^{\sigma}$ is real closed. Then it is real and algebraic over $\mathbb{Q}$. So by Lemma 4.2, it has a real embedding. This implies (i). ■

The following lemma gives the density of the Hilbert sets over a number field K with respect to any real embeddings of K into $\mathbb{R}$.

Lemma 4.4 *Let K be a number field and $\tau_1, \dots, \tau_m$ be a family of real embeddings of K. For $i = 1, 2, \dots, k$, let $f_i(x, y) \in K[x, y]$ be irreducible polynomials over $K(x)$. Let $H_K(f_i)$ be the Hilbert set of f_i over K. Then*

$$\Big(\bigcap_{i=1}^{k} H_K(f_i)\Big) \cap \Big(\bigcap_{j=1}^{m} \tau_j^{-1}(I)\Big) \neq \varnothing,$$

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

for any open interval I in $\mathbb{R}$.

Proof This is a special case of [4, Lemma 3.4]. ■

Theorem 4.5 *Let K be a number field, K_{ab} the maximal abelian extension of K, and E/K an elliptic curve over K. Then for any complex conjugation automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$, $E((K_{\mathrm{ab}})^{\sigma})$ has infinite rank. Hence, $E(\overline{K}^{\sigma})$ has infinite rank.*

Proof For a complex conjugation automorphism $\sigma \in \mathrm{Gal}(\overline{K}/K)$, there exists a real embedding θ such that $\theta(\overline{K}^{\sigma}) \subseteq \mathbb{R} \cap \overline{K}$, by Lemma 4.3. Note that $\sigma(\sqrt{-1}) = -\sqrt{-1}$, since otherwise $\sigma(\sqrt{-1}) = \sqrt{-1}$ and then $\sqrt{-1} \in \overline{K}^{\sigma}$ and $0 < (\theta(\sqrt{-1}))^2 = \theta(-1) = -1$ which is a contradiction. And for any element $\alpha \in K$ such that $\theta(\alpha) > 0$, $\sigma(\sqrt{\alpha}) = \sqrt{\alpha}$, since otherwise, $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$, hence $\sigma(\sqrt{-\alpha}) = \sqrt{-\alpha}$, then $\sqrt{-\alpha} \in \overline{K}^{\sigma}$ and $0 < (\theta(\sqrt{-\alpha}))^2 = -\theta(\alpha) < 0$ which is a contradiction.

Let us fix a Weierstrass equation of E/K, $y^2 = x^3 + ax + b$, for $a, b \in K$. Then there exists $\alpha \in \mathbb{R}$ such that $x^3 + \theta(a)x + \theta(b) > 0$ for all $x > \alpha$. Let $I = (\alpha, \infty)$ be the open interval of all real numbers $> \alpha$. Let $f(x, y) = y^2 - (x^3 + ax + b)$. Then f is an absolutely irreducible polynomial in $K[x, y]$, hence irreducible over $K(x)$. Let $H_K(f)$ be the Hilbert set of f over K. Note that the restriction $\theta|_K$ of θ to K is a real embedding of K.

By Lemma 4.4 there is an element $x_1 \in H_K(f) \cap \theta|_K^{-1}(I)$. Then $x_1^3 + ax_1 + b \in K$ and since $\theta(x_1) > \alpha$, $\theta(x_1^3 + ax_1 + b)$ is positive, hence $\sigma(\sqrt{x_1^3 + ax_1 + b}) = \sqrt{x_1^3 + ax_1 + b}$. Hence σ fixes $\sqrt{x_1^3 + ax_1 + b}$. Let $K_1 = K(\sqrt{x_1^3 + ax_1 + b})$. Then since $f(x_1, y)$ is irreducible in $K[y]$, K_1 is a quadratic extension of K and $K_1 \subseteq \overline{K}(\sigma)$.

Inductively, suppose we have constructed linearly disjoint quadratic extensions $K_1, \dots, K_{n-1}$ of K such that $K_i = K(\sqrt{x_i^3 + ax_i + b})$ for $x_i \in H_K(f) \cap \theta|_K^{-1}(I)$. Let $L_{n-1} = K_1 \cdots K_{n-1}$ be the composite field extension over K. By Lemma 4.4 again, there is $x_n \in H_{L_{n-1}}(f) \cap \theta|_K^{-1}(I)$. Let $K_n = K(\sqrt{x_n^3 + ax_n + b})$. Then, similarly, we can show that K_n is a quadratic extension of K and $K_n \subseteq \overline{K}(\sigma)$. Moreover, K_n is linearly disjoint from all $K_1, K_2, \dots, K_{n-1}$, since $x_n \in H_{L_{n-1}}(f)$.

Hence we have obtained $\{x_i\}_{i=1}^{\infty} \subseteq K$ and an infinite sequence $\{K_i/K\}_{i=1}^{\infty}$ of linearly disjoint quadratic extensions of K such that $K_i = K(\sqrt{x_i^3 + ax_i + b})$. For each i, let P_i be a point of $E(K_i)$ whose x-coordinate is x_i. Note that $P_i \notin E(K)$, for each i. Hence, by Lemma 3.12 for some N, $\{P_i\}_{i \geq N}$ consists of linearly independent non-torsion points of $E(\overline{K})$. In particular, since K_i are abelian extensions of K and are fixed under σ, P_i are points of $E((K_{\mathrm{ab}})^{\sigma})$. Hence

$$E((K_{\mathrm{ab}})^{\sigma}) \otimes \mathbb{Q} \supseteq E\Bigl(\prod_{i=N}^{\infty} K_i\Bigr) \otimes \mathbb{Q} \supseteq \{P_i \otimes 1\}_{i \geq N}$$

is infinite dimensional. And $E(\overline{K}^{\sigma})$ has infinite rank as well. ■

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

5 More General Result: E over Arbitrary Number Fields with a Rational Point Which Is Neither 2-Torsion Nor 3-Torsion

In this section, we prove a more general result than the result of Theorem 3.13 for E/K with a rational point P such that $2P \neq O$ and $3P \neq O$ without hypothesis on the ground field K. To do so, we need the following lemma and proposition.

Lemma 5.1 *For a number field K let $\sigma \in \operatorname{Gal}(\overline{K}/K)$. If σ does not fix any totally imaginary finite extensions of K, then σ is a complex conjugation automorphism.*

Proof Since $\overline{K}^{\sigma}$ is algebraic over $\mathbb{Q}$, by Lemma 4.2 and Lemma 4.3 it is enough to show that $\overline{K}^{\sigma}$ is ordered.

If L is a finite extension of K such that $L \subseteq \overline{K}^{\sigma}$, then L is not totally imaginary by the assumption. Let $\tau_1, \dots, \tau_r$ be all real embeddings of L.

For $\alpha \in L^*$ $(= L - \{0\})$, if $\tau_i(\alpha) < 0$ for all $i = 1, \dots, r$, then $L(\sqrt{\alpha})$ is totally imaginary (otherwise, $L(\sqrt{\alpha})$ has a real embedding ρ and $\rho|_L = \tau_i$ for some i. But we have $0 < (\rho(\sqrt{\alpha}))^2 = \rho(\alpha) = \tau_i(\alpha)$, which contradicts $\tau_i(\alpha) < 0$ for all i). Hence, σ does not fix $\sqrt{\alpha}$ by the assumption, so $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$. This implies that for $\beta \in L^*$, if $\tau_i(\beta) > 0$ for all $i = 1, \dots, r$, then $\sigma(\sqrt{-\beta}) = -\sqrt{-\beta}$, and since $\tau_i(-1) = -1 < 0$ for all i, $\sigma(\sqrt{-1}) = -\sqrt{-1}$; hence $\sigma(\sqrt{\beta}) = \sqrt{\beta}$.

Therefore, there is a homomorphism $h\colon \prod_{i=1}^r \{\pm 1\} \to \{\pm 1\}$ such that the action of σ on $\sqrt{\alpha}$ for $\alpha \in L^*$ depends only on the image of the vector of signs of α under h. In other words, for $\alpha \in L^*$ we let $f\colon L^* \to \prod_{i=1}^r \{\pm 1\}$ be a homomorphism defined by

$$f(\alpha) = (\operatorname{sign}(\tau_1(\alpha)), \dots, \operatorname{sign}(\tau_r(\alpha))),$$

and $g\colon L^* \to \{\pm 1\}$ defined by

$$g(\alpha) = \operatorname{sign}\left(\frac{\sigma(\sqrt{\alpha})}{\sqrt{\alpha}}\right),$$

so $\sigma(\sqrt{\alpha}) = g(\alpha)\sqrt{\alpha}$, then there exists a homomorphism $h\colon \prod_{i=1}^r \{\pm 1\} \to \{\pm 1\}$ such that $h \circ f = g$.

Note that from the above explanation on totally positive or totally negative elements of L^*, we get

$$(*) \qquad h(-1, \dots, -1) = -1 \quad \text{and} \quad h(1, \dots, 1) = 1.$$

In particular, there is always a vector consisting of -1 in all but one coordinate and 1 in the remaining coordinate which lies in the kernel of h. In fact, there are r vectors consisting of -1 in all but one coordinate and 1 in the remaining coordinate:

$$v_1 = (1, -1, \dots, -1), v_2 = (-1, 1, -1, \dots, -1), \dots, v_r = (-1, \dots, -1, 1).$$

If all r vectors map to -1 under h, then

$$(-1)^r = \prod_{i=1}^r h(v_i) = h\Bigl(\prod_{i=1}^r v_i\Bigr) = h((-1)^{r-1}, \dots, (-1)^{r-1}).$$

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

But this contradicts $(*)$ by taking an even and odd integer r. Therefore, at least one of v_i must map to 1, so it lies in the kernel of h. Without loss of generality, we may assume that v_1 maps to 1 under h.

Hence, we can choose $\alpha \in L^*$ such that $\sigma(\sqrt{\alpha}) = \sqrt{\alpha}$ and $\tau_1(\alpha) > 0$ but $\tau_i(\alpha) < 0$ for all $i = 2, \dots, r$, and let $L' = L(\sqrt{\alpha})$. Then L' is fixed under σ, so L' is not totally imaginary. Let ρ be a real embedding of L'. Then since α is positive only with respect to τ_1,

$$0 < (\rho(\sqrt{\alpha}))^2 = \rho(\alpha) = \rho|_L(\alpha) = \tau_1(\alpha).$$

Hence,

$$\rho(\sqrt{\alpha}) = \pm\sqrt{\tau_1(\alpha)}.$$

This shows that L' has exactly two real embeddings ρ_1 and ρ_2 such that

$$\rho_1(\sqrt{\alpha}) = \sqrt{\tau_1(\alpha)}, \quad \rho_2(\sqrt{\alpha}) = -\sqrt{\tau_1(\alpha)}, \quad \text{and} \quad \rho_i|_L = \tau_1, \text{ for } i = 1, 2.$$

We proceed using the same argument on L' with two real embeddings ρ_i as before and get a homomorphism $h'\colon \{\pm 1\} \times \{\pm 1\} \to \{\pm 1\}$ and $f'\colon L'^* \to \{\pm 1\} \times \{\pm 1\}$ given by $f(\beta) = (\operatorname{sign}\rho_1(\beta), \operatorname{sign}\rho_2(\beta))$, $g'\colon L'^* \to \{\pm 1\}$ given by $g'(\beta) = \operatorname{sign}(\sigma(\sqrt{\beta})/\sqrt{\beta})$, such that $h' \circ f' = g'$ on L'^*. Again, we have that

$$(**) \qquad h'(-1,-1) = -1 \quad \text{and} \quad h'(1,1) = 1.$$

This implies that h' cannot send both $(-1,-1)$ and $(1,1)$ to the same value 1 or -1. So either $h'(-1,1) = -1$ and $h'(1,-1) = 1$ or $h'(-1,1) = 1$ and $h'(1,-1) = -1$. Therefore, h' is the projection onto either the first factor or the second factor. Without loss of generality, we assume that h' is the projection onto the first factor, that is, g' is defined by the sign of the first real embedding ρ_1. Then if $\beta, \gamma \in L'^*$ such that $\sqrt{\beta}$, $\sqrt{\gamma}$ are fixed under σ, then $\rho_1(\beta) > 0$ and $\rho_1(\gamma) > 0$ so $\rho_1(\beta+\gamma) > 0$. Hence,

$$g'(\beta+\gamma) = h'(f'(\beta+\gamma)) = h'(1,a) = 1, \qquad \text{where } a = 1 \text{ or } -1.$$

So $\sigma(\sqrt{\beta+\gamma}) = \sqrt{\beta+\gamma}$. And obviously, $\sigma(\sqrt{\beta\gamma}) = \sqrt{\beta\gamma}$.

We have shown that the set of $\beta \in L'^*$ with $\sigma(\sqrt{\beta}) = \sqrt{\beta}$ is closed under addition and multiplication. Therefore, for any two elements a and $b \in \overline{K}^{\sigma} - \{0\}$, by applying the preceding argument and taking L as a finite extension of K generated by a^2 and b^2, the set of squares in $\overline{K}^{\sigma} - \{0\}$ is closed under addition and multiplication. Hence, if we let S be the set of squares in $\overline{K}^{\sigma} - \{0\}$ and denote the the set of non-squares in $\overline{K}^{\sigma} - \{0\}$ by $-S$, then $\overline{K}^{\sigma} = S \sqcup \{0\} \sqcup -S$, a disjoint union. Hence, $\overline{K}^{\sigma}$ is ordered with the positive set S. This completes the proof. ■

Proposition 5.2 *For a number field K, let $\sigma \in \mathrm{Gal}(\overline{K}/K)$. If σ is not a complex conjugation automorphism, then there is a totally imaginary finite extension L over K such that $L \subseteq \overline{K}^{\sigma}$.*

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

Proof It follows from Lemma 5.1. ■

The following is our more general theorem without hypothesis on the ground field or the given automorphisms.

Theorem 5.3 *Let K be a number field and E/K an elliptic curve over K with a K-rational point P such that $2P \neq O$ and $3P \neq O$. Then for each $\sigma \in \operatorname{Gal}(\overline{K}/K)$, the rank of $E(\overline{K}^{\sigma})$ is infinite.*

Proof Let $\sigma \in \operatorname{Gal}(\overline{K}/K)$. If σ is a complex conjugation automorphism, then $E(\overline{K}^{\sigma})$ has infinite rank by Theorem 4.5. If σ is not a complex conjugation automorphism, then by Proposition 5.2 there is a totally imaginary finite extension L of K such that $L \subseteq \overline{K}^{\sigma}$. Hence $\sigma \in \operatorname{Gal}(\overline{K}/L)$. Now consider E/L defined over L by replacing the ground field K by L. Then since the given K-rational point P is also defined over L, we apply Theorem 3.13 to complete the proof. ■

Acknowledgements The work in this paper is a part of my Ph.D. thesis at Indiana University, Bloomington. I wish to thank my thesis advisor, Michael Larsen for suggesting this problem, his guidance, valuable discussions and helpful comments on this paper. I would also like to thank the referee for helpful comments and remarks.

References

[1] G. Frey and M. Jarden, *Approximation theory and the rank of abelian varieties over large algebraic fields.* Proc. London Math. Soc. **28**(1974), 112–128.

[2] M. Fried and M. Jarden, *Field Arithmetic.* Ergebnisse der Mathematik und ihrer Grenzgebiete 11, Springer-Verlag, Berlin, 1986.

[3] ———, *Diophantine properties of subfields of* $\tilde{\mathbb{Q}}$. Amer. J. Math. **100**(1978), no. 1, 653–666.

[4] W.-D. Geyer, *Galois groups of intersections of local fields.* Israel J. Math. **30**(1978), no. 4, 382–396.

[5] P. Griffiths and J. Harris, *Principles of Algebraic Geometry.* Wiley-Interscience Publication, New York, 1978.

[6] R. Hartshorne, *Algebraic Geometry.* Graduate Texts in Mathematics 52, Springer-Verlag, New York, 1977.

[7] B. Im, *Heegner points and Mordell–Weil groups of elliptic curves over large fields.* Submitted for publication, 2003.

[8] B. Im and M. Larsen, *Weak approximation for linear systems of quadrics.* To appear in J. Number Theory.

[9] I. M. Isaacs, *Algebra: A Graduate Course.* Brooks/Cole, Pacific Grove, CA, 1994.

[10] S. Lang, *Algebra.* Third edition. Addison-Wesley, 1993.

[11] ———, *Fundamentals of Diophantine Geometry.* Springer-Verlag, New York, 1983.

[12] M. Larsen, *Rank of elliptic curves over almost algebraically closed fields.* Bull. London Math. Soc. **35**(2003), no. 6, 817–820.

[13] P. Morandi, *Field and Galois Theory.* Graduate Texts in Mathematics 167, Springer-Verlag, New York, 1996.

[14] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of Number Fields.* Grundlehren der Mathematischen Wissenschaften 323, Springer, Berlin, 2000.

[15] W. Rudin, *Real and complex analysis.* Third edition. McGraw-Hill, New York, 1987.

[16] J. P. Serre, *A Course in Arithmetic.* Graduate Texts in Mathematics 7, Springer-Verlag, New York, 1973.

[17] ———, *Local Fields.* Graduate Texts in Mathematics 67, Springer-Verlag, New York, 1979.

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press

[18] J. H. Silverman, *Integer points on curves of genus* 1. J. London Math. Soc. **28**(1983), no. 1, 1–7.

[19] ———, *The Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

Department of Mathematics
University of Utah
Salt Lake City, UT 84112
e-mail: im@math.utah.edu

https://doi.org/10.4153/CJM-2006-032-4 Published online by Cambridge University Press