Transcendental Brauer groups of products of CM elliptic curves

Article

Accepted Version

www.reading.ac.uk/centaur

CentAUR

Transcendental Brauer groups of products of CM elliptic curves

Rachel Newton

ABSTRACT

Let L be a number field and let E/L be an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K. We use class field theory and results of Skorobogatov and Zarhin to compute the transcendental part of the Brauer group of the abelian surface $E \times E$. The results for the odd order torsion also apply to the Brauer group of the K3 surface $\mathrm{Kum}(E \times E)$. We describe explicitly the elliptic curves $E/\mathbb{Q}$ with complex multiplication by $\mathcal{O}_K$ such that the Brauer group of $E \times E$ contains a transcendental element of odd order. We show that such an element gives rise to a Brauer-Manin obstruction to weak approximation on $\mathrm{Kum}(E \times E)$, while there is no obstruction coming from the algebraic part of the Brauer group.

1. Introduction

Let X be a smooth, projective, geometrically irreducible variety over a number field L. In [16], Manin showed that the Brauer group of X can obstruct the Hasse principle on X. Let $X(\mathbb{A}_L)$ denote the set of adelic points of X and let $\mathrm{Br}(X)$ denote the Brauer group of X, $\mathrm{Br}(X) = H^2_{\text{ét}}(X, \mathbb{G}_m)$. There is a pairing

$$X(\mathbb{A}_L) \times \mathrm{Br}(X) \to \mathbb{Q}/\mathbb{Z}$$

obtained by evaluating an element of $\mathrm{Br}(X)$ at an adelic point and summing the local invariants [16]. The Brauer-Manin set $X(\mathbb{A}_L)^{\mathrm{Br}(X)}$ is the set of adelic points of X which are orthogonal to $\mathrm{Br}(X)$ under this pairing. It contains the closure of the set of rational points in the adelic topology.

$$\overline{X(L)} \subset X(\mathbb{A}_L)^{\mathrm{Br}(X)} \subset X(\mathbb{A}_L).$$

If $X(\mathbb{A}_L) \neq \emptyset$ but $X(\mathbb{A}_L)^{\mathrm{Br}(X)} = \emptyset$, there is said to be a Brauer-Manin obstruction to the Hasse principle on X. If $X(\mathbb{A}_L) \neq X(\mathbb{A}_L)^{\mathrm{Br}(X)}$, there is said to be a Brauer-Manin obstruction to weak approximation on X.

Since Manin's observation, Brauer groups and the associated obstructions have been the subject of a great deal of research. Let $\overline{X}$ denote the base change of X to an algebraic closure of L. The kernel of the natural map from $\mathrm{Br}(X)$ to $\mathrm{Br}(\overline{X})$ is called the 'algebraic' part of $\mathrm{Br}(X)$ and denoted $\mathrm{Br}_1(X)$. It is usually easier to handle than the remaining 'transcendental' part and a substantial portion of the literature is devoted to its study. The quotient group $\mathrm{Br}(X)/\mathrm{Br}_1(X)$, known as the transcendental part of $\mathrm{Br}(X)$, is generally more mysterious. Nevertheless, it has arithmetic importance – transcendental elements in $\mathrm{Br}(X)$ can obstruct the Hasse principle and weak approximation, as shown by Harari in [7] and Wittenberg in [26].

Results of Skorobogatov and Zarhin in [25] allow one to compute the transcendental part of the Brauer group for a product of elliptic curves. These results were used by Ieronymou, Skorobogatov and Zarhin in [11] to give a sufficient condition for the Brauer group of a diagonal quartic surface D over $\mathbb{Q}$ to be algebraic, and to give an upper bound on the size of the quotient of $\mathrm{Br}(D)$ by the image of $\mathrm{Br}(\mathbb{Q})$. This built upon earlier work of Ieronyomou [9], who gave a

sufficient condition for the 2-primary part of the Brauer group of a diagonal quartic surface over $\mathbb{Q}$ to be algebraic. In [**10**], Ieronymou and Skorobogatov went on to use the results of [**25**] and [**11**] to compute the odd order torsion in the quotient of $\mathrm{Br}(D)$ by the image of $\mathrm{Br}(\mathbb{Q})$ for a diagonal quartic surface D over $\mathbb{Q}$.

In this paper, we use the results of [**25**] to compute the transcendental part of the Brauer group for abelian surfaces of the form $E \times E$ where E/L is an elliptic curve with complex multiplication by the ring of integers $\mathcal{O}_K$ of an imaginary quadratic field K.

Skorobogatov and Zarhin [**24**] proved that for X an abelian variety or K3 surface, $\mathrm{Br}(X)/\mathrm{Br}_1(X)$ is a finite abelian group. Therefore, computing $\mathrm{Br}(X)/\mathrm{Br}_1(X)$ is equivalent to computing its ℓ-primary part $(\mathrm{Br}(X)/\mathrm{Br}_1(X))_{\ell^\infty}$ for every prime number ℓ. To a pair (E, ℓ) consisting of an elliptic curve E defined over a number field L, with complex multiplication by $\mathcal{O}_K$, and a prime number ℓ, we associate an integer $m(\ell)$ (Definition 1) which can be calculated using class field theory (Proposition 2.2). We write Γ_L for the absolute Galois group of L. We denote the n-torsion subgroup of an abelian group A by A_n. For an elliptic curve E/L, we write E_n for the n-torsion points of E defined over an algebraic closure of L.

THEOREM 1.1.   *Let $\ell \in \mathbb{Z}_{>0}$ be an odd prime and let $m = m(\ell)$. Then*

$$\left(\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)}\right)_{\ell^\infty} = \frac{\mathrm{Br}(E \times E)_{\ell^m}}{\mathrm{Br}_1(E \times E)_{\ell^m}} = \frac{\mathrm{End}_{\Gamma_L} E_{\ell^m}}{(\mathcal{O}_K \otimes \mathbb{Z}/\ell^m)^{\Gamma_L}} \cong \begin{cases} (\mathbb{Z}/\ell^m)^2 & \text{if } K \subset L \\ \mathbb{Z}/\ell^m & \text{if } K \not\subset L. \end{cases}$$

For brevity, here we state only the result for odd primes. The results for all primes can be found in Theorems 2.5 and 2.9. In Theorems 2.6 and 2.8, we give a similar description of the ℓ-primary part of $\mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_L}$ for every prime ℓ. One can apply these results to gain information about the transcendental part of the Brauer group for a wider class of varieties. If $\pi : X \dashrightarrow Y$ is a dominant rational map of degree d between K3 or abelian surfaces over L, then by the proof of [**10**] Corollary 2.2, it induces a surjective map of Γ_L-modules

$$\pi^* : \mathrm{Br}(\overline{Y}) \to \mathrm{Br}(\overline{X})$$

whose kernel is annihilated by d. Thus, if ℓ is prime and coprime to d, then

$$\left(\frac{\mathrm{Br}(Y)}{\mathrm{Br}_1(Y)}\right)_{\ell^\infty} \hookrightarrow \mathrm{Br}(\overline{Y})_{\ell^\infty}^{\Gamma_L} = \mathrm{Br}(\overline{X})_{\ell^\infty}^{\Gamma_L}.$$

The following examples are of interest. Suppose that E/L has complex multiplication by $\mathcal{O}_K$.
   (1) $Y = E \times E'$ where E'/L is an elliptic curve which is isogenous to E over L. Take ℓ coprime to the degree of the isogeny.
   (2) $Y = E' \times E'$ where E'/L is an elliptic curve with complex multiplication by a non-maximal order $\mathcal{O} \subset \mathcal{O}_K$. Take ℓ coprime to the index $[\mathcal{O}_K : \mathcal{O}]$. This is because there is an isogeny of degree $[\mathcal{O}_K : \mathcal{O}]$, defined over L, from E' to an elliptic curve over L with complex multiplication by $\mathcal{O}_K$.
   (3) $Y = \mathrm{Kum}(E \times E)$, the K3 surface which is the minimal desingularisation of the quotient of $E \times E$ by the involution $(P, Q) \mapsto (-P, -Q)$.

More is known for a Kummer surface $X = \mathrm{Kum}(E \times E)$. By Proposition 1.3 of [**25**], there is an isomorphism of Γ_L-modules

$$\mathrm{Br}(\overline{X}) \to \mathrm{Br}(\overline{E} \times \overline{E})$$

and therefore

$$\mathrm{Br}(\overline{X})^{\Gamma_L} = \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_L}.$$

By Theorem 2.4 of [**25**], for every $n \in \mathbb{Z}_{>0}$ there is an embedding

$$\mathrm{Br}(X)_n / \mathrm{Br}_1(X)_n \hookrightarrow \mathrm{Br}(E \times E)_n / \mathrm{Br}_1(E \times E)_n \qquad (1.1)$$

which is an isomorphism if n is odd. So for ℓ an odd prime,

$$(\mathrm{Br}(X) / \mathrm{Br}_1(X))_{\ell^\infty} = (\mathrm{Br}(E \times E) / \mathrm{Br}_1(E \times E))_{\ell^\infty}. \qquad (1.2)$$

Examples involving K3 surfaces are important for applications because for abelian varieties with finite Tate-Shafarevich group, any Brauer-Manin obstruction can be explained by the algebraic part of the Brauer group, see §6.2 of [**23**]. However, for K3 surfaces the transcendental part of the Brauer group can play an essential role in the Brauer-Manin obstruction. Examples of this are given in [**9**], [**8**], [**20**] and [**10**]. We give another example in Theorem 1.3 below. We focus on elliptic curves with a transcendental element of odd order in $\mathrm{Br}(E \times E)$ because this will give rise to a transcendental element in the Brauer group of $\mathrm{Kum}(E \times E)$.

THEOREM 1.2.   *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ such that $\mathrm{Br}(E \times E)$ contains a transcendental element of odd order. Then E has affine equation $y^2 = x^3 + 2c^3$ for some $c \in \mathbb{Q}^\times$. Moreover, for $X = \mathrm{Kum}(E \times E)$ we have $\mathrm{Br}_1(X) = \mathrm{Br}(\mathbb{Q})$ and*

$$\mathrm{Br}(X) / \mathrm{Br}(\mathbb{Q}) = \mathrm{Br}(X)_3 / \mathrm{Br}(\mathbb{Q})_3 = \mathrm{Br}(E \times E)_3 / \mathrm{Br}_1(E \times E)_3 \cong \mathbb{Z}/3.$$

For $c \in \mathbb{Q}^\times$, let E^c denote the elliptic curve over $\mathbb{Q}$ with affine equation $y^2 = x^3 + 2c^3$. Let $X = \mathrm{Kum}(E^c \times E^c)$ denote the Kummer surface, which is independent of the choice of $c \in \mathbb{Q}^\times$. One consequence of Theorem 1.2 is that the algebraic elements of $\mathrm{Br}(X)$ do not produce a Brauer-Manin obstruction. The following theorem shows that a transcendental Brauer element gives rise to a Brauer-Manin obstruction to weak approximation on X.

THEOREM 1.3.   *Let $\mathcal{A} \in \mathrm{Br}(X)_3 \setminus \mathrm{Br}(\mathbb{Q})$. Let ν be a place of $\mathbb{Q}$. Then the evaluation map*

$$\mathrm{ev}_{\mathcal{A},\nu} : X(\mathbb{Q}_\nu) \to \mathrm{Br}(\mathbb{Q}_v)_3$$

is surjective for $\nu = 3$ and zero for every other place. Consequently,

$$X(\mathbb{A}_\mathbb{Q})^{\mathrm{Br}(X)} = X(\mathbb{Q}_3)_0 \times X(\mathbb{R}) \times \prod_{\ell \neq 3} X(\mathbb{Q}_\ell) \subsetneq X(\mathbb{A}_\mathbb{Q})$$

where $X(\mathbb{Q}_3)_0$ denotes the points $P \in X(\mathbb{Q}_3)$ with $\mathrm{ev}_{\mathcal{A},3}(P) = 0$, and the product runs over prime numbers $\ell \neq 3$.

The structure of the paper is as follows. Section 2 is devoted to the computation of the transcendental part of the Brauer group of $E \times E$ for a CM elliptic curve E. Section 3 contains applications of these results to special cases and explicit examples. The proof of Theorem 1.2 is carried out in Section 4. In Section 5, we compute the Brauer-Manin obstruction to weak approximation on $\mathrm{Kum}(E \times E)$ for $E/\mathbb{Q}$ (a quadratic twist of) the elliptic curve with affine equation $y^2 = x^3 + 2$, leading to a proof of Theorem 1.3.

NOTATION AND CONVENTIONS.   We fix the following notation.

K	an imaginary quadratic field
$\mathcal{O}_K$	the ring of integers of K
Δ_K	the discriminant of K
H_K	the Hilbert class field of K
$h(\mathcal{O}_K)$	the class number of $\mathcal{O}_K$, $h(\mathcal{O}_K) = [H_K : K]$

L	a number field
$\overline{L}$	an algebraic closure of L such that $H_K \subset \overline{L}$
Γ_F	the absolute Galois group of a field F
μ_n	the group of nth roots of unity
ζ_n	a primitive nth root of unity
E	an elliptic curve over L with complex multiplication by $\mathcal{O}_K$
$\overline{E}$	the base change of E to $\overline{L}$, $\overline{E} = E \times_L \overline{L}$
E_n	the n-torsion points of E defined over $\overline{L}$
$E_n(F)$	the n-torsion points of E defined over a field extension F of L
$\mathrm{Kum}(E \times E)$	the K3 surface which is the minimal desingularisation
	of the quotient of $E \times E$ by the involution $(P,Q) \mapsto (-P, -Q)$
$f_{\mathfrak{q}/\mathfrak{p}}$	the residue class degree $f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_M/\mathfrak{q} : \mathcal{O}_F/\mathfrak{p}]$ for a prime $\mathfrak{q}$ in
	a number field M lying above a prime $\mathfrak{p}$ in a subfield $F \subset M$.

For any $c \in \mathbb{Z}_{>0}$, we use the following notation.

$\mathcal{O}_c$	the order $\mathbb{Z} + c\mathcal{O}_K$ of conductor c in $\mathcal{O}_K$
K_c	the ring class field corresponding to the order $\mathcal{O}_c$.

Specifically, let $I_K(c)$ denote the group of fractional $\mathcal{O}_K$-ideals coprime to c, and let $P_{K,\mathbb{Z}}(c)$ be the subgroup generated by the principal ideals $\alpha\mathcal{O}_K$ where $\alpha \in \mathcal{O}_c$ and α is coprime to c. Then K_c is defined to be the extension of K that corresponds under class field theory to $P_{K,\mathbb{Z}}(c)$. The Artin map gives an isomorphism $I_K(c)/P_{K,\mathbb{Z}}(c) \cong \mathrm{Gal}(K_c/K)$. In particular, we will make use of the ring class fields K_{ℓ^n} for a prime number ℓ and $n \in \mathbb{Z}_{\geq 0}$. They enjoy the following properties which will be needed later.

(i) $K_{\ell^0} = H_K$,
(ii) $K_{\ell^n} \subset K_{\ell^{n+1}}$ for $n \geq 0$,
(iii) the degree $[K_{\ell^n} : K]$ tends to infinity as n tends to infinity.

For more details on ring class fields, see [3] for example.

For an abelian group A and an integer $n \in \mathbb{Z}_{>0}$, we write A_n for the elements of order dividing n in A. For a prime number $\ell \in \mathbb{Z}_{>0}$, we write A_{ℓ^∞} for the ℓ-primary part of the abelian group A.

For $x \in \mathbb{R}$, let $\lfloor x \rfloor$, $\lceil x \rceil$ denote the floor and ceiling of x respectively.

2. Transcendental Brauer group computations

2.1. Preliminaries

Let L be a number field and let Γ_L denote its absolute Galois group. In [25], for $A = E \times E'$ a product of elliptic curves defined over L and for every $n \in \mathbb{Z}_{>0}$, Skorobogatov and Zarhin gave a canonical isomorphism of Γ_L-modules

$$\mathrm{Br}(\overline{A})_n = \mathrm{Hom}(E_n, E'_n)/(\mathrm{Hom}(\overline{E}, \overline{E'}) \otimes \mathbb{Z}/n) \qquad (2.1)$$

and a canonical isomorphism of abelian groups

$$\mathrm{Br}(A)_n / \mathrm{Br}_1(A)_n = \mathrm{Hom}_{\Gamma_L}(E_n, E'_n)/(\mathrm{Hom}(\overline{E}, \overline{E'}) \otimes \mathbb{Z}/n)^{\Gamma_L}. \qquad (2.2)$$

They used this concrete description of the transcendental part of the Brauer group to give many examples for which $\mathrm{Br}(A)/\mathrm{Br}_1(A)$ is trivial or a finite abelian 2-group.

From now on, we fix an elliptic curve E/L with complex multiplication by $\mathcal{O}_K$. We begin with a simple observation which enables us to use (2.2) to compute $(\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E))_{\ell^\infty}$.

LEMMA 2.1.   *Let X be a smooth, projective, geometrically irreducible variety over a number field. Then for any prime number ℓ, we have*

$$(\mathrm{Br}(X)/\mathrm{Br}_1(X))_{\ell^\infty} = \mathrm{Br}(X)_{\ell^\infty}/\mathrm{Br}_1(X)_{\ell^\infty}.$$

Proof.   Since X is smooth, Proposition 1.4 of [**6**] tells us that $\mathrm{Br}(X)$ is a torsion abelian group. It follows that the natural inclusion

$$\mathrm{Br}(X)_{\ell^\infty}/\mathrm{Br}_1(X)_{\ell^\infty} \hookrightarrow (\mathrm{Br}(X)/\mathrm{Br}_1(X))_{\ell^\infty}$$

is an equality.   □

To each prime number $\ell \in \mathbb{Z}_{>0}$ we associate an integer $m(\ell)$ which will appear in our description of the ℓ-primary part of the transcendental Brauer group of $E \times E$. In order to define $m(\ell)$, we use the Grössencharacter $\psi_{E/KL}$ of E considered as an elliptic curve over KL. Recall that $\psi_{E/KL}$ is unramified at the primes of KL of good reduction for E. Therefore, for such primes we write $\psi_{E/KL}(\mathfrak{q})$ for the evaluation of $\psi_{E/KL}$ at an idele $(\dots, 1, 1, \pi_\mathfrak{q}, 1, 1, \dots) \in \mathbb{A}_{KL}^\times$ where the entry $\pi_\mathfrak{q}$ at the prime $\mathfrak{q}$ is a uniformiser at $\mathfrak{q}$.

DEFINITION 1.   For a prime number $\ell \in \mathbb{Z}_{>0}$, let $m(\ell)$ be the largest integer k such that for all primes $\mathfrak{q}$ of KL which are of good reduction for E and coprime to ℓ, the Grössencharacter $\psi_{E/KL}$ satisfies

$$\psi_{E/KL}(\mathfrak{q}) \in \mathcal{O}_{\ell^k} = \mathbb{Z} + \ell^k \mathcal{O}_K.$$

We define an auxiliary integer $n(\ell)$ which aids computation of $m(\ell)$ and in most cases removes the dependence on the Grössencharacter.

DEFINITION 2.   For a prime number $\ell \in \mathbb{Z}_{>0}$, let $n(\ell)$ be the largest integer k for which the ring class field K_{ℓ^k} of the order $\mathcal{O}_{\ell^k}$ embeds into KL.

PROPOSITION 2.2.   *Let $\ell \in \mathbb{Z}_{>0}$ be prime. Then*
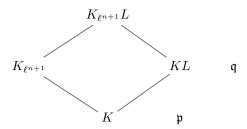
$$m(\ell) \leq n(\ell)$$

with equality if $\mathcal{O}_K^* = \{\pm 1\}$ (in other words, if $K \notin \{\mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$).

Proof.   Write $m = m(\ell)$ and $n = n(\ell)$. Let S be the set of primes $\mathfrak{r}$ of KL that satisfy at least one of the following five conditions:
   (i) $\mathfrak{r} \mid \infty$,
   (ii) $\mathfrak{r} \mid \ell$,
   (iii) E has bad reduction at $\mathfrak{r}$,
   (iv) $\mathfrak{r}$ is ramified in $K_{\ell^{n+1}}L/K$,
   (v) $\psi_{E/KL}(\mathfrak{r}) \notin \mathcal{O}_{\ell^{n+1}}$.
Suppose for contradiction that $m \geq n + 1$, and hence S is a finite set. Then, since $K_{\ell^{n+1}} \not\subseteq KL$, Exercise 6.1 of [**2**] tells us that there exists a prime $\mathfrak{q}$ of KL with $\mathfrak{q} \notin S$ which does not split completely in $K_{\ell^{n+1}}L/KL$. Let $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$. Let $f_{\mathfrak{q}/\mathfrak{p}}$ denote the residue class degree of $\mathfrak{q}$ over $\mathfrak{p}$, $f_{\mathfrak{q}/\mathfrak{p}} = [\mathcal{O}_{KL}/\mathfrak{q} : \mathcal{O}_K/\mathfrak{p}]$. By Theorems 9.1 and 9.2 of [**22**], the Grössencharacter $\psi_{E/KL}$ sends $\mathfrak{q}$ to a generator of the principal ideal $N_{KL/K}(\mathfrak{q}) = \mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}$. Consider the following diagram of

field extensions.

Recall that, given an abelian extension of number fields M/N and a prime ideal $\mathfrak{r}$ of $\mathcal{O}_N$ that is unramified in M/N, the Artin symbol $(\mathfrak{r}, M/N)$ is the unique element $\sigma \in \mathrm{Gal}(M/N)$ such that for all $\alpha \in \mathcal{O}_M$,

$$\sigma(\alpha) \equiv \alpha^{N_{F/\mathbb{Q}}(\mathfrak{r})} \pmod{\mathfrak{s}}$$

where $\mathfrak{s}$ is a prime of M above $\mathfrak{r}$. In our case, $N_{KL/\mathbb{Q}}(\mathfrak{q}) = N_{K/\mathbb{Q}}(N_{KL/K}(\mathfrak{q})) = N_{K/\mathbb{Q}}(\mathfrak{p})^{f_{\mathfrak{q}/\mathfrak{p}}}$. Therefore, the restriction of the Artin symbol $(\mathfrak{q}, K_{\ell^{n+1}}L/KL)$ to $K_{\ell^{n+1}}/K$ (in other words, its image in $\mathrm{Gal}(K_{\ell^{n+1}}/K)$) satisfies

$$\mathrm{Res}_{K_{\ell^{n+1}}/K}(\mathfrak{q}, K_{\ell^{n+1}}L/KL) = (\mathfrak{p}, K_{\ell^{n+1}}/K)^{f_{\mathfrak{q}/\mathfrak{p}}} = (\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}, K_{\ell^{n+1}}/K)$$
$$= ((\psi_{E/KL}(\mathfrak{q})), K_{\ell^{n+1}}/K).$$

Since $\mathfrak{q} \notin S$, we have $\psi_{E/KL}(\mathfrak{q}) \in \mathcal{O}_{\ell^{n+1}}$ and hence

$$((\psi_{E/KL}(\mathfrak{q})), K_{\ell^{n+1}}/K) = 1$$

by definition of the ring class field $K_{\ell^{n+1}}$. But this implies that

$$\mathrm{Res}_{K_{\ell^{n+1}}/K}(\mathfrak{q}, K_{\ell^{n+1}}L/KL) = 1$$

and therefore

$$(\mathfrak{q}, K_{\ell^{n+1}}L/KL) = 1.$$

This is a contradiction because $\mathfrak{q}$ does not split completely in $K_{\ell^{n+1}}L/KL$. Therefore, $m \le n$. It remains to show that $m = n$ when $\mathcal{O}_K^* = \{\pm 1\}$. From now on, suppose that $\mathcal{O}_K^* = \{\pm 1\}$. Let $\mathfrak{q}$ be a finite prime of KL of good reduction for E which is coprime to ℓ and unramified in KL/K. Let $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ and let $\mathfrak{s} = \mathfrak{q} \cap \mathcal{O}_{K_{\ell^n}}$. The Artin symbol $(\mathfrak{p}, K_{\ell^n}/K)$ has order $f_{\mathfrak{s}/\mathfrak{p}}$ in $\mathrm{Gal}(K_{\ell^n}/K)$. Since $K \subset K_{\ell^n} \subset KL$, we have $f_{\mathfrak{s}/\mathfrak{p}} \mid f_{\mathfrak{q}/\mathfrak{p}}$, whereby

$$1 = (\mathfrak{p}, K_{\ell^n}/K)^{f_{\mathfrak{q}/\mathfrak{p}}} = (\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}, K_{\ell^n}/K) = (N_{KL/K}(\mathfrak{q}), K_{\ell^n}/K).$$

By definition of the ring class field K_{ℓ^n}, this implies that

$$N_{KL/K}(\mathfrak{q}) = \alpha \mathcal{O}_K$$

for some $\alpha \in \mathcal{O}_{\ell^n}$. But $\psi_{E/KL}(\mathfrak{q})$ is a generator of $N_{KL/K}(\mathfrak{q})$ and $\mathcal{O}_K^* = \{\pm 1\}$ so this implies that $\psi_{E/KL}(\mathfrak{q}) \in \mathcal{O}_{\ell^n}$, as required. $\qquad \square$

REMARK 1. Class field theory gives $[K_c : K] = h(\mathcal{O}_c)$, where $h(\mathcal{O}_c)$ denotes the class number of the order $\mathcal{O}_c$. The following formula for $h(\mathcal{O}_c)$ can be found in [**3**], Theorem 7.24, for example.

$$[K_c : K] = h(\mathcal{O}_c) = \frac{h(O_K)c}{[\mathcal{O}_K^* : \mathcal{O}_c^*]} \prod_{p|c} \left(1 - \left(\frac{\Delta_K}{p}\right)\frac{1}{p}\right) \tag{2.3}$$

where the product is taken over the prime factors of c. The symbol $(\frac{\Delta_K}{p})$ denotes the Legendre symbol for odd primes. For the prime 2, the Legendre symbol is replaced by the Kronecker

symbol $(\frac{\Delta_K}{2})$, defined as

$$\left(\frac{\Delta_K}{2}\right) = \begin{cases} 0 & \text{if } 2 \mid \Delta_K \\ 1 & \text{if } \Delta_K \equiv 1 \pmod 8 \\ -1 & \text{if } \Delta_K \equiv 5 \pmod 8. \end{cases}$$

If $K_{\ell^k} \subset KL$, then $[K_{\ell^k} : K]$ divides $[KL : K]$. Thus, in any given example, (2.3) allows one to identify a finite set of primes S such that $m(\ell) = n(\ell) = 0$ for all $\ell \notin S$. For a prime ℓ in S, (2.3) gives an upper bound for $n(\ell)$, and therefore also an upper bound for $m(\ell)$. For $K \in \{\mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$, one must examine the Grössencharacter in order to compute $m(\ell)$. For explicit descriptions of Grössencharacters for elliptic curves with complex multiplication by $\mathbb{Q}(i)$ or $\mathbb{Q}(\zeta_3)$, see [21] Theorems 5.6 and 5.7 respectively.

In Sections 2.2 and 2.3, we will use the isomorphisms (2.1) and (2.2) to compute the ℓ-primary part of the transcendental Brauer group of $E \times E$ in terms of endomorphisms of the ℓ-power torsion of E. For this, we will need two auxiliary lemmas. Before stating the first lemma, we note that since $\text{End}\,\overline{E} = \mathcal{O}_K$, there is a natural map $\mathcal{O}_K \otimes \mathbb{Z}/\ell^k \to \text{End}\,E_{\ell^k}$. The injectivity of this map follows from the fact that the ℓ-adic Tate module $T_\ell(E)$ is a free $\mathcal{O}_K \otimes \mathbb{Z}_\ell$-module of rank 1. (For a more general fact about abelian varieties, see Proposition 2.2.1 of [19].) Thus, we may view $\mathcal{O}_K \otimes \mathbb{Z}/\ell^k$ as a subring of $\text{End}\,E_{\ell^k}$.

LEMMA 2.3.   Let $\ell \in \mathbb{Z}_{>0}$ be prime, let $k \in \mathbb{Z}_{\geq 0}$ and let
$$(\text{End}\,E_{\ell^k})^+ = \{\psi \in \text{End}\,E_{\ell^k} \mid \psi x = x\psi \; \forall x \in \mathcal{O}_K\}.$$
Then, viewing $\mathcal{O}_K \otimes \mathbb{Z}/\ell^k$ as a subring of $\text{End}\,E_{\ell^k}$, we have
$$(\text{End}\,E_{\ell^k})^+ = \mathcal{O}_K \otimes \mathbb{Z}/\ell^k.$$

Proof.   As an abelian group, $E_{\ell^k} \cong (\mathbb{Z}/\ell^k)^2$, and therefore $\text{End}\,E_{\ell^k} \cong M_2(\mathbb{Z}/\ell^k)$. The proof comes down to an easy calculation with two-by-two matrices with entries in $\mathbb{Z}/\ell^k$.   □

LEMMA 2.4.   Let $\ell \in \mathbb{Z}_{>0}$ be prime and let $m = m(\ell)$. Let $k \in \mathbb{Z}_{\geq 0}$ and let $\varphi \in \text{End}\,E_{\ell^k}$. Then
  (i) The class of φ in $\text{End}\,E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by Γ_{KL} if and only if for all $x \in \mathcal{O}_K$,
$$\ell^m(x\varphi - \varphi x) \in (\text{End}\,E_{\ell^k})^+ = \mathcal{O}_K \otimes \mathbb{Z}/\ell^k.$$
  (ii) The endomorphism φ is fixed by Γ_{KL} if and only if
$$\ell^m \varphi \in (\text{End}\,E_{\ell^k})^+ = \mathcal{O}_K \otimes \mathbb{Z}/\ell^k.$$

Proof.   The action of Γ_{KL} on $\text{End}\,E_{\ell^k}$ factors through the abelian Galois group $\text{Gal}(KL(E_{\ell^k})/KL)$. Let $\mathfrak{q}$ be a finite prime of KL which is coprime to ℓ and of good reduction for E. The Néron-Ogg-Shafarevich criterion tells us that $\mathfrak{q}$ is unramified in $KL(E_{\ell^k})/KL$. Since E has complex multiplication by $\mathcal{O}_K$, the Artin symbol $(\mathfrak{q}, KL(E_{\ell^k})/KL)$ acts on E_{ℓ^k} as multiplication by $\psi_{E/KL}(\mathfrak{q})$. For a proof of this fact, see [13], Ch. 4, Corollary 1.3 (iii), for example. Therefore, the action of $(\mathfrak{q}, KL(E_{\ell^k})/KL)$ on $\text{End}(E_{\ell^k})$ is conjugation by $\psi_{E/KL}(\mathfrak{q})$. The Artin symbols for the unramified primes generate $\text{Gal}(KL(E_{\ell^k})/KL)$.

Let $\alpha = (\Delta_K + \sqrt{\Delta_K})/2$, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$. Let $a, b \in \mathbb{Z}$ be such that $a + b\alpha$ is invertible in $\mathcal{O}_K \otimes \mathbb{Z}/\ell^k$. Let $\varphi \in \text{End}\,E_{\ell^k}$. We have
$$(a + b\alpha)\varphi - \varphi(a + b\alpha) = b(\alpha\varphi - \varphi\alpha).$$

Hence, the class of φ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by conjugation by $a + b\alpha$ if and only if

$$b(\alpha\varphi - \varphi\alpha) \in \mathcal{O}_K \otimes \mathbb{Z}/\ell^k \tag{2.4}$$

and φ is fixed by conjugation by $a + b\alpha$ if and only if

$$b(\alpha\varphi - \varphi\alpha) = 0. \tag{2.5}$$

Recall that $m = m(\ell)$ is the largest integer t such that for all finite primes $\mathfrak{q}$ of KL which are of good reduction for E and coprime to ℓ,

$$\psi_{E/KL}(\mathfrak{q}) \in \mathcal{O}_{\ell^t} = \mathbb{Z} + \ell^t \mathcal{O}_K.$$

In other words, for a prime $\mathfrak{q}$ which is unramified in $KL(E_{\ell^k})/KL$, we can write $\psi_{E/KL}(\mathfrak{q}) = a + b\alpha$ for some $a, b \in \mathbb{Z}$ with $\operatorname{ord}_\ell(b) = m$. Hence, by (2.4), the class of φ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by Γ_{KL} if and only if

$$\ell^m(\alpha\varphi - \varphi\alpha) \in \mathcal{O}_K \otimes \mathbb{Z}/\ell^k.$$

By (2.5), the endomorphism φ is fixed by Γ_{KL} if and only if

$$\ell^m(\alpha\varphi - \varphi\alpha) = 0.$$

An application of Lemma 2.3 completes the proof. $\qquad\square$

2.2. *Case I: Complex multiplication defined over the base field.*

In this subsection, we compute the transcendental Brauer group of $E \times E$ in the case where the complex multiplication field K is a subfield of L, the field of definition of E.

THEOREM 2.5. *Suppose that $K \subseteq L$. Let $\ell \in \mathbb{Z}_{>0}$ be prime and let $m = m(\ell)$. Then*

$$\left(\frac{\operatorname{Br}(E \times E)}{\operatorname{Br}_1(E \times E)}\right)_{\ell^\infty} = \frac{\operatorname{Br}(E \times E)_{\ell^m}}{\operatorname{Br}_1(E \times E)_{\ell^m}} = \frac{\operatorname{End} E_{\ell^m}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^m} \cong (\mathbb{Z}/\ell^m)^2.$$

Proof. By (2.2), for all primes ℓ and all $k \in \mathbb{Z}_{\geq 0}$, we have

$$\frac{\operatorname{Br}(E \times E)_{\ell^k}}{\operatorname{Br}_1(E \times E)_{\ell^k}} = \frac{\operatorname{End}_{\Gamma_L} E_{\ell^k}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^k}.$$

Also,

$$\frac{\operatorname{End} E_{\ell^k}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^k} \cong (\mathbb{Z}/\ell^k)^2.$$

The result now follows from Lemma 2.4, part (ii). $\qquad\square$

THEOREM 2.6. *Suppose that $K \subseteq L$. Let $\ell \in \mathbb{Z}_{>0}$ be prime and let $m = m(\ell)$. Then*

$$\operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_L} = \left(\frac{\operatorname{End} E_{\ell^{m+\lceil \operatorname{ord}_\ell(\Delta_K)/2 \rceil}}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^{m+\lceil \operatorname{ord}_\ell(\Delta_K)/2 \rceil}}\right)^{\Gamma_L}$$
$$\cong \mathbb{Z}/\ell^{m+\lfloor \operatorname{ord}_\ell(\Delta_K)/2 \rfloor} \times \mathbb{Z}/\ell^{m+\lceil \operatorname{ord}_\ell(\Delta_K)/2 \rceil}.$$

In particular, if $\ell \nmid \Delta_K$ then

$$\operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_L} = \frac{\operatorname{End} E_{\ell^m}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^m} \cong (\mathbb{Z}/\ell^m)^2.$$

Proof. Fix a prime number $\ell \in \mathbb{Z}_{>0}$ and let $k \in \mathbb{Z}_{\geq 0}$. By (2.1), we have

$$\mathrm{Br}(\overline{E} \times \overline{E})_{\ell^k}^{\Gamma_L} = \left(\frac{\mathrm{End}\, E_{\ell^k}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^k} \right)^{\Gamma_L}.$$

Write $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where $\alpha = (\Delta_K + \sqrt{\Delta_K})/2$ and let $\varphi \in \mathrm{End}\, E_{\ell^k}$. By part (i) of Lemma 2.4, the class of φ in $\mathrm{End}\, E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by Γ_L if and only if

$$\ell^m(\alpha\varphi - \varphi\alpha) \in \mathcal{O}_K \otimes \mathbb{Z}/\ell^k. \tag{2.6}$$

Let $P, \alpha P$ be a $\mathbb{Z}/\ell^k$-basis for E_{ℓ^k}. With respect to this basis, multiplication by α is given by the following matrix:

$$\begin{pmatrix} 0 & \frac{\Delta_K(1-\Delta_K)}{4} \\ 1 & \Delta_K \end{pmatrix}.$$

Subtracting an element of $\mathcal{O}_K \otimes \mathbb{Z}/\ell^k$ if necessary, we may assume that φ is of the form

$$\begin{pmatrix} 0 & t \\ 0 & u \end{pmatrix}$$

for some $t, u \in \mathbb{Z}/\ell^k$. In terms of matrices, equation (2.6) becomes

$$\begin{pmatrix} -\ell^m t & -\ell^m t \Delta_K + \ell^m u \frac{\Delta_K(1-\Delta_K)}{4} \\ -\ell^m u & \ell^m t \end{pmatrix} = \begin{pmatrix} a & b\frac{\Delta_K(1-\Delta_K)}{4} \\ b & a + b\Delta_K \end{pmatrix}$$

for some $a, b \in \mathbb{Z}/\ell^k$. The resulting equations reduce to

$$2\ell^m t \equiv \ell^m \Delta_K t \equiv \ell^m \Delta_K u \equiv \ell^m \frac{\Delta_K(1 - \Delta_K)}{2} u \equiv 0 \pmod{\ell^k}. \tag{2.7}$$

We have $\mathrm{ord}_2(\Delta_K) \in \{0, 2, 3\}$ and for an odd prime ℓ, $\mathrm{ord}_\ell(\Delta_K) \in \{0, 1\}$. Thus, (2.7) can be summarised as

$$\ell^{m+\lfloor \mathrm{ord}_\ell(\Delta_K)/2 \rfloor} t \equiv \ell^{m+\lceil \mathrm{ord}_\ell(\Delta_K)/2 \rceil} u \equiv 0 \pmod{\ell^k}.$$

Therefore,

$$\begin{aligned}
\mathrm{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_L} &= \mathrm{Br}(\overline{E} \times \overline{E})_{\ell^{m+\lceil \mathrm{ord}_\ell(\Delta_K)/2 \rceil}}^{\Gamma_L} \\
&= \left(\frac{\mathrm{End}\, E_{\ell^{m+\lceil \mathrm{ord}_\ell(\Delta_K)/2 \rceil}}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^{m+\lceil \mathrm{ord}_\ell(\Delta_K)/2 \rceil}} \right)^{\Gamma_L} \\
&\cong \mathbb{Z}/\ell^{m+\lfloor \mathrm{ord}_\ell(\Delta_K)/2 \rfloor} \times \mathbb{Z}/\ell^{m+\lceil \mathrm{ord}_\ell(\Delta_K)/2 \rceil}.
\end{aligned}$$

$\square$

REMARK 2. The fact that $(\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E))_{\ell^\infty} = \mathrm{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_L}$ for $\ell \nmid \Delta_K$ also follows from Proposition 5.2 of [**5**]. A computation of the relevant intersection pairing shows that the cokernel of the map $\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E) \hookrightarrow \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_L}$ is annihilated by the discriminant of K.

2.3. *Case II: Complex multiplication not defined over the base field.*

Throughout this subsection, we make the assumption that $K \not\subseteq L$. We write τ for an element of $\Gamma_L \setminus \Gamma_{KL}$. We set $\alpha = (\Delta_K + \sqrt{\Delta_K})/2$, so $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

LEMMA 2.7. *Suppose that $K \not\subseteq L$. Let $\ell \in \mathbb{Z}_{>0}$ be prime and let $k \in \mathbb{Z}_{\geq 0}$. Let $a, b \in \mathbb{Z}$ and consider $(a + b\alpha)\tau$ as an element of $\mathrm{End}\, E_{\ell^k}$. Then*

(i) *The class of $(a + b\alpha)\tau$ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by Γ_{KL} if and only if*

$$\operatorname{ord}_\ell(a),\ \operatorname{ord}_\ell(b) \geq k - m(\ell) - \operatorname{ord}_\ell(\Delta_K).$$

(ii) *The class of $(a + b\alpha)\tau$ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by τ if and only if*

$$\operatorname{ord}_\ell(b) \geq k - \operatorname{ord}_\ell(\Delta_K).$$

(iii) *We have $(a + b\alpha)\tau \in (\operatorname{End} E_{\ell^k})^+ = \mathcal{O}_K \otimes \mathbb{Z}/\ell^k$ if and only if*

$$\operatorname{ord}_\ell(a) \geq k - \lfloor \operatorname{ord}_\ell(\Delta_K)/2 \rfloor$$
$$\text{and}\quad \operatorname{ord}_\ell(b) \geq k - \lceil \operatorname{ord}_\ell(\Delta_K)/2 \rceil.$$

(iv) *We have $(a + b\alpha)\tau \in \operatorname{End}_{\Gamma_{KL}} E_{\ell^k}$ if and only if*

$$\operatorname{ord}_\ell(a) \geq k - m(\ell) - \lfloor \operatorname{ord}_\ell(\Delta_K)/2 \rfloor$$
$$\text{and}\quad \operatorname{ord}_\ell(b) \geq k - m(\ell) - \lceil \operatorname{ord}_\ell(\Delta_K)/2 \rceil.$$

(v) *The endomorphism $(a + b\alpha)\tau$ is fixed by the action of τ if and only if*

$$\operatorname{ord}_\ell(b) \geq k - \lfloor \operatorname{ord}_\ell(\Delta_K)/2 \rfloor.$$

Proof. Write $m = m(\ell)$.

(i) By part (i) of Lemma 2.4, the class of $(a + b\alpha)\tau$ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by Γ_{KL} if and only if

$$\ell^m(a + b\alpha)(\alpha\tau - \tau\alpha) = \ell^m \sqrt{\Delta_K}(a + b\alpha)\tau \in (\operatorname{End} E_{\ell^k})^+. \tag{2.8}$$

By the definition of $(\operatorname{End} E_{\ell^k})^+$, (2.8) shows that the class of $(a + b\alpha)\tau$ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by Γ_{KL} if and only if

$$\ell^m \sqrt{\Delta_K}(a + b\alpha)(\alpha\tau - \tau\alpha) = \ell^m \Delta_K(a + b\alpha)\tau \equiv 0 \pmod{\ell^k}.$$

(ii) The class of $(a + b\alpha)\tau$ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by τ if and only if

$$(a + b\alpha)\tau - \tau(a + b\alpha)\tau\tau^{-1} = b\sqrt{\Delta_K}\tau \in \mathcal{O}_K \otimes \mathbb{Z}/\ell^k. \tag{2.9}$$

By Lemma 2.3, $\mathcal{O}_K \otimes \mathbb{Z}/\ell^k = (\operatorname{End} E_{\ell^k})^+$. So, by (2.9) and the definition of $(\operatorname{End} E_{\ell^k})^+$, the class of $(a + b\alpha)\tau$ in $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$ is fixed by τ if and only if

$$\alpha b\sqrt{\Delta_K}\tau - b\sqrt{\Delta_K}\tau\alpha = b\Delta_K\tau \equiv 0 \pmod{\ell^k}.$$

(iii) By definition of $(\operatorname{End} E_{\ell^k})^+$, we have

$$(a + b\alpha)\tau \in (\operatorname{End} E_{\ell^k})^+ \iff (a + b\alpha)(\alpha\tau - \tau\alpha) \equiv 0 \pmod{\ell^k}.$$

Expanding $(a + b\alpha)(\alpha\tau - \tau\alpha)$ gives

$$(a + b\alpha)(\alpha\tau - \tau\alpha) = \Big(b\frac{\Delta_K(1 - \Delta_K)}{2} - \Delta_K a + (2a + b\Delta_K)\alpha\Big)\tau.$$

The conditions of part (iii) are precisely those arising from

$$b\frac{\Delta_K(1 - \Delta_K)}{2} - \Delta_K a \equiv 2a + b\Delta_K \equiv 0 \pmod{\ell^k}.$$

(iv) By part (ii) of Lemma 2.4,

$$(a + b\alpha)\tau \in \operatorname{End}_{\Gamma_{KL}} E_{\ell^k} \iff \ell^m(a + b\alpha)\tau \in (\operatorname{End} E_{\ell^k})^+.$$

Now apply part (iii) of Lemma 2.7.

(v) The endomorphism $(a + b\alpha)\tau$ is fixed by the action of τ if and only if

$$(a + b\alpha)\tau - \tau(a + b\alpha)\tau\tau^{-1} = b\sqrt{\Delta_K}\tau \equiv 0 \pmod{\ell^k}. \tag{2.10}$$

It is easily seen that $b\sqrt{\Delta_K} \equiv 0 \pmod{\ell^k}$ if and only if

$$\operatorname{ord}_\ell(b) \geq k - \lfloor \operatorname{ord}_\ell(\Delta_K)/2 \rfloor.$$

$\square$

THEOREM 2.8.   *Suppose that $K \nsubseteq L$ and let $\ell \in \mathbb{Z}_{>0}$ be prime. Let $m = m(\ell)$ and let $k = m + \operatorname{ord}_\ell(\Delta_K)$. Let θ denote the image of τ in the quotient group $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$. Then*

$$\operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_{KL}} = \mathcal{O}_K \theta$$

and

$$\operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_L} = \mathcal{O}_{\ell^m}\theta \cong \begin{cases} \mathbb{Z}/\ell^k & \text{if } \ell \text{ is odd or } \ell \nmid \Delta_K \\ \mathbb{Z}/2^{k-1} \times \mathbb{Z}/2 & \text{if } \ell = 2 \text{ and } 2 \mid \Delta_K. \end{cases}$$

Proof.   Since $\operatorname{ord}_\ell(\Delta_K) \geq \lceil \operatorname{ord}_\ell(\Delta_K)/2 \rceil$, applying Theorem 2.6 to KL gives

$$\operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_{KL}} = \operatorname{Br}(\overline{E} \times \overline{E})_{\ell^k}^{\Gamma_{KL}} = (\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k))^{\Gamma_{KL}} \tag{2.11}$$

$$\cong \mathbb{Z}/\ell^{m+\lfloor \operatorname{ord}_\ell(\Delta_K)/2 \rfloor} \times \mathbb{Z}/\ell^{m+\lceil \operatorname{ord}_\ell(\Delta_K)/2 \rceil}. \tag{2.12}$$

By part (i) of Lemma 2.7,

$$\mathcal{O}_K \theta \subset (\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k))^{\Gamma_{KL}}.$$

Using part (iii) of Lemma 2.7 to count the number of elements in $\mathcal{O}_K \theta$ and comparing to (2.12) gives

$$\mathcal{O}_K \theta = (\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k))^{\Gamma_{KL}}.$$

Now part (ii) of Lemma 2.7 shows that

$$\mathcal{O}_{\ell^m}\theta = (\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k))^{\Gamma_L}.$$

Moreover, since $\operatorname{ord}_\ell(\Delta_K) \leq 1$ for an odd prime ℓ, part (iii) of Lemma 2.7 gives $\mathcal{O}_{\ell^m}\theta \cong \mathbb{Z}/\ell^k$ if ℓ is odd or $\ell \nmid \Delta_K$. If $\ell = 2$ and $2 \mid \Delta_K$, then part (iii) of Lemma 2.7 gives $\mathcal{O}_{2^m}\theta \cong \mathbb{Z}/2^{k-1} \times \mathbb{Z}/2$.
$\square$

THEOREM 2.9.   *Suppose that $K \nsubseteq L$ and let $\ell \in \mathbb{Z}_{>0}$ be prime. Let $m = m(\ell)$. Let η denote the image of τ in the quotient group $\operatorname{End} E_{\ell^m}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^m)$. Then*

$$\left(\frac{\operatorname{Br}(E \times E)}{\operatorname{Br}_1(E \times E)}\right)_{\ell^\infty} = \frac{\operatorname{Br}(E \times E)_{\ell^m}}{\operatorname{Br}_1(E \times E)_{\ell^m}} = \frac{\operatorname{End}_{\Gamma_L} E_{\ell^m}}{(\mathcal{O}_K \otimes \mathbb{Z}/\ell^m)^{\Gamma_L}} = (\mathbb{Z}/\ell^m)\eta \cong \mathbb{Z}/\ell^m$$

unless $\ell = 2$, $2 \mid \Delta_K$, $m \geq 1$ and $E_2 = E_2(L)$, in which case

$$\left(\frac{\operatorname{Br}(E \times E)}{\operatorname{Br}_1(E \times E)}\right)_{2^\infty} = \frac{\operatorname{Br}(E \times E)_{2^{m+1}}}{\operatorname{Br}_1(E \times E)_{2^{m+1}}} = \frac{\operatorname{End}_{\Gamma_L} E_{2^{m+1}}}{(\mathcal{O}_K \otimes \mathbb{Z}/2^{m+1})^{\Gamma_L}}$$

$$\cong \mathbb{Z}/2^m \times \mathbb{Z}/2$$

where the copy of $\mathbb{Z}/2^m$ is generated by the image of τ.

Proof.   Let $k = m + \operatorname{ord}_\ell(\Delta_K)$ and let θ denote the image of τ in the quotient group $\operatorname{End} E_{\ell^k}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^k)$. Then

$$\frac{\operatorname{Br}(E \times E)_{\ell^\infty}}{\operatorname{Br}_1(E \times E)_{\ell^\infty}} \hookrightarrow \operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_L} = \mathcal{O}_{\ell^m}\theta, \tag{2.13}$$

by Theorem 2.8. For all $t \in \mathbb{Z}_{\geq 0}$,

$$\frac{\mathrm{Br}(E \times E)_{\ell^t}}{\mathrm{Br}_1(E \times E)_{\ell^t}} = \frac{\mathrm{End}_{\Gamma_L} E_{\ell^t}}{(\mathcal{O}_K \otimes \mathbb{Z}/\ell^t)^{\Gamma_L}} \hookrightarrow \frac{\mathrm{End}_{\Gamma_{KL}} E_{\ell^t}}{\mathcal{O}_K \otimes \mathbb{Z}/\ell^t}. \tag{2.14}$$

First suppose that ℓ is odd or $\ell \nmid \Delta_K$. Then (2.13) and (2.14) combined with Theorems 2.5 and 2.8 show that

$$\left(\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \right)_{\ell^\infty} \hookrightarrow \mathbb{Z}/\ell^m. \tag{2.15}$$

Consider τ as an element of $\mathrm{End}\, E_{\ell^m}$. By parts (iv) and (v) of Lemma 2.7, $\tau \in \mathrm{End}_{\Gamma_L} E_{\ell^m}$. By part (iii) of Lemma 2.7, η has order ℓ^m in

$$\mathrm{End}_{\Gamma_L} E_{\ell^m}/(\mathcal{O}_K \otimes \mathbb{Z}/\ell^m)^{\Gamma_L} = \mathrm{Br}(E \times E)_{\ell^m}/\mathrm{Br}_1(E \times E)_{\ell^m}.$$

Hence, by (2.15),

$$(\mathbb{Z}/\ell^m)\eta = \frac{\mathrm{End}_{\Gamma_L} E_{\ell^m}}{(\mathcal{O}_K \otimes \mathbb{Z}/\ell^m)^{\Gamma_L}} = \left(\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \right)_{\ell^\infty}.$$

Now suppose that $\ell = 2$ and $2 \mid \Delta_K$. If $m(2) = 0$, then $(\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E))_{2^\infty} = 0$, by (2.14) and Theorem 2.5 applied to KL. So we assume from now on that $m = m(2) \geq 1$. Theorems 2.5 and 2.8 combined with (2.13) and (2.14) show that

$$\left(\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \right)_{2^\infty} \hookrightarrow \mathbb{Z}/2^m \times \mathbb{Z}/2. \tag{2.16}$$

By parts (iii), (iv) and (v) of Lemma 2.7, the image of τ generates a copy of $\mathbb{Z}/2^m$ inside $\mathrm{End}_{\Gamma_L} E_{2^{m+1}}/(\mathcal{O}_K \otimes \mathbb{Z}/2^{m+1})^{\Gamma_L} = \mathrm{Br}(E \times E)_{2^{m+1}}/\mathrm{Br}_1(E \times E)_{2^{m+1}}$. Therefore, (2.16) shows that $(\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E))_{2^\infty}$ is isomorphic to either $\mathbb{Z}/2^m$ or $\mathbb{Z}/2^m \times \mathbb{Z}/2$.

First suppose that $E_2 = E_2(L)$. Then Γ_L acts trivially on E_2 and hence

$$\frac{\mathrm{Br}(E \times E)_2}{\mathrm{Br}_1(E \times E)_2} = \frac{\mathrm{End}_{\Gamma_L} E_2}{(\mathcal{O}_K \otimes \mathbb{Z}/2)^{\Gamma_L}} = \frac{\mathrm{End}\, E_2}{\mathcal{O}_K \otimes \mathbb{Z}/2} \cong \mathbb{Z}/2 \times \mathbb{Z}/2.$$

Therefore,

$$\left(\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \right)_{2^\infty} = \frac{\mathrm{Br}(E \times E)_{2^{m+1}}}{\mathrm{Br}_1(E \times E)_{2^{m+1}}} \cong \mathbb{Z}/2^m \times \mathbb{Z}/2.$$

Now suppose that $E_2 \neq E_2(L)$. By Theorem 2.8,

$$\mathrm{Br}(\overline{E} \times \overline{E})_{2^\infty}^{\Gamma_L} = \left(\frac{\mathrm{End}\, E_{2^k}}{\mathcal{O}_K \otimes \mathbb{Z}/2^k} \right)^{\Gamma_L} = \mathcal{O}_{2^m}\theta$$

and, in particular, for any $t \in \mathbb{Z}_{\geq 0}$ the natural injection

$$\mathcal{O}_{2^m}\theta = \left(\frac{\mathrm{End}\, E_{2^k}}{\mathcal{O}_K \otimes \mathbb{Z}/2^k} \right)^{\Gamma_L} \hookrightarrow \left(\frac{\mathrm{End}\, E_{2^{k+t}}}{\mathcal{O}_K \otimes \mathbb{Z}/2^{k+t}} \right)^{\Gamma_L} \tag{2.17}$$

induced by multiplication by 2^t on $E_{2^{k+t}}$ is an isomorphism. Let $\varphi \in \mathrm{End}_{\Gamma_L} E_{2^{k+t}}$ for some $t \in \mathbb{Z}_{\geq 0}$. We have

$$\frac{\mathrm{End}_{\Gamma_L} E_{2^{k+t}}}{(\mathcal{O}_K \otimes \mathbb{Z}/2^{k+t})^{\Gamma_L}} \hookrightarrow \left(\frac{\mathrm{End}\, E_{2^{k+t}}}{\mathcal{O}_K \otimes \mathbb{Z}/2^{k+t}} \right)^{\Gamma_L}. \tag{2.18}$$

Since $2 \mid \Delta_K$, we can write $\mathcal{O}_K = \mathbb{Z}[\sqrt{-d}]$ where $\Delta_K = -4d$. Since the injection in (2.17) is an isomorphism, we can use (2.18) to write

$$\varphi = 2^t(x + 2^m y\sqrt{-d})\tau + z + w\sqrt{-d} \tag{2.19}$$

for some $x, y, z, w \in \mathbb{Z}/2^{k+t}$. Here we abuse notation slightly by using τ to denote the image of τ in $\mathrm{End}_{\Gamma_L} E_{2^{k+t}}$. Since φ is fixed by τ, we have

$$2\sqrt{-d}(2^{m+t}y\tau + w) \equiv 0 \pmod{2^{k+t}}.$$

Multiplying by $\sqrt{-d}$ and recalling that $k = m + \mathrm{ord}_2(\Delta_K) = m + \mathrm{ord}_2(d) + 2$, we see that

$$2^{m+t} y\tau + w \equiv 0 \pmod{2^{m+t+1}}.$$

Therefore, $w = 2^{m+t} u$ for some $u \in \mathbb{Z}/2^{k+t}$ and we have

$$y\tau + u \equiv 0 \pmod 2.$$

Suppose for contradiction that $y \not\equiv 0 \pmod 2$. Then τ acts as multiplication by a scalar on E_2. Furthermore, since τ is invertible, this scalar cannot be zero and therefore must be 1. In other words, τ acts as the identity on E_2. Furthermore, since $m(2) \geq 1$, Γ_{KL} acts trivially on E_2 and hence $E_2 = E_2(L)$, giving the required contradiction. Therefore, $y \equiv 0 \pmod 2$ and we can write $y = 2v$ for some $v \in \mathbb{Z}/2^{k+t}$ and substituting into (2.19) gives

$$\varphi = 2^t(x + 2^{m+1} v\sqrt{-d})\tau + z + w\sqrt{-d}. \tag{2.20}$$

Now part (iii) of Lemma 2.7 shows that $2^{t+m+1}\sqrt{-d}\tau \in \mathcal{O}_K \otimes \mathbb{Z}/2^{k+t}$. Thus, (2.20) shows that the class of φ in $(\mathrm{End}\, E_{2^{k+t}}/(\mathcal{O}_K \otimes \mathbb{Z}/2^{k+t}))^{\Gamma_L}$ is represented by $2^t x\tau$. But φ was arbitrary and (2.18) is injective, hence $\mathrm{End}_{\Gamma_L} E_{2^{k+t}}/(\mathcal{O}_K \otimes \mathbb{Z}/2^{k+t})^{\Gamma_L}$ is a cyclic group. Therefore,

$$\left(\frac{\mathrm{Br}(E \times E)}{\mathrm{Br}_1(E \times E)} \right)_{2^\infty} = \frac{\mathrm{Br}(E \times E)_{2^{m+1}}}{\mathrm{Br}_1(E \times E)_{2^{m+1}}} \cong \mathbb{Z}/2^m.$$

$\square$

3. Special cases and examples

We retain the notation and conventions of Section 2. In particular, L is a number field and E/L is an elliptic curve with complex multiplication by $\mathcal{O}_K$.

THEOREM 3.1.   Suppose that $L \subset H_K$, where H_K denotes the Hilbert class field of K. Let $\ell \in \mathbb{Z}_{>0}$ be prime. Then $m(\ell) = n(\ell) = 0$, except in the following special cases where $n(\ell) = 1$:
  (i) $K = \mathbb{Q}(\zeta_3)$ and $\ell \leq 3$,
  (ii) $K = \mathbb{Q}(i)$ and $\ell = 2$,
  (iii) $\Delta_K \equiv 1 \pmod 8$ and $\ell = 2$.
Consequently, if $\mathcal{O}_K^* = \{\pm 1\}$ and $\Delta_K \not\equiv 1 \pmod 8$, then

$$\mathrm{Br}(E \times E) = \mathrm{Br}_1(E \times E).$$

Proof.   Let $j(E)$ denote the j-invariant of the elliptic curve E. Since E is defined over L, we have $\mathbb{Q}(j(E)) \subset L$. The theory of complex multiplication tells us that $K(j(E)) = H_K$. Therefore, $[KL : K] = [H_K : K] = h(\mathcal{O}_K)$. Using the formula for the degree of a ring class field, as given in (2.3), we see that in every case, $[K_{\ell^2} : K] > h(\mathcal{O}_K)$ so $n(\ell) \leq 1$. Furthermore, $[K_\ell : K] > h(\mathcal{O}_K)$ except in the special cases (i), (ii) and (iii) of the theorem. The rest follows immediately from Proposition 2.2 and Theorems 2.5 and 2.9. $\square$

REMARK 3.   Since $K(j(E)) = H_K$, the hypothesis $L \subset H_K$ holds precisely when $L = H_K$ or $L = \mathbb{Q}(j(E))$.

If $\mathcal{O}_K^* = \{\pm 1\}$, then Proposition 2.2 allows us to calculate $m(\ell)$ for all primes $\ell \in \mathbb{Z}_{>0}$, and hence compute the transcendental part of $\mathrm{Br}(E \times E)$. On the other hand, if $K \in \{\mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$, then Proposition 2.2 only tells us that $m(\ell) \leq n(\ell)$ for all primes $\ell \in \mathbb{Z}_{>0}$. The following two

propositions deal with $K = \mathbb{Q}(i)$ and $K = \mathbb{Q}(\zeta_3)$, and in each case give sufficient conditions which allow us to conclude that $m(\ell) = 0$.

PROPOSITION 3.2.   Let $\ell \in \mathbb{Z}_{>0}$ be an odd prime. Let $K = \mathbb{Q}(i)$. Suppose that there exists a finite prime $\mathfrak{q}$ of KL satisfying all of the following conditions.
   (i) $\mathfrak{q}$ is coprime to 2ℓ,
   (ii) E has good reduction at $\mathfrak{q}$,
   (iii) $f_{\mathfrak{s}/\mathfrak{p}} \mid f_{\mathfrak{q}/\mathfrak{p}}$, where $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ and $\mathfrak{s}$ is a prime of $K_{2\ell}$ above $\mathfrak{p}$,
   (iv) $\psi_{E/KL}(\mathfrak{q}) \notin \mathcal{O}_2$.
Then $m(\ell) = 0$, and hence
$$(\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E))_{\ell^\infty} = \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_L}_{\ell^\infty} = \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_{KL}}_{\ell^\infty} = 0.$$

Note that condition (iii) is trivially satisfied if $K_{2\ell} \subseteq KL$.

Proof.   Let $\mathfrak{q}$ be a finite prime of KL satisfying conditions (1)–(4). Let $\mathfrak{p}$ and $\mathfrak{s}$ be primes as described in condition (iii). The Artin symbol $(\mathfrak{p}, K_{2\ell}/K)$ has order $f_{\mathfrak{s}/\mathfrak{p}}$ in $\mathrm{Gal}(K_{2\ell}/K)$. Since $f_{\mathfrak{s}/\mathfrak{p}}$ divides $f_{\mathfrak{q}/\mathfrak{p}}$, we have
$$1 = (\mathfrak{p}, K_{2\ell}/K)^{f_{\mathfrak{q}/\mathfrak{p}}} = (\mathfrak{p}^{f_{\mathfrak{q}/\mathfrak{p}}}, K_{2\ell}/K) = (N_{KL/K}(\mathfrak{q}), K_{2\ell}/K).$$
By the definition of the ring class field $K_{2\ell}$, this implies that
$$N_{KL/K}(\mathfrak{q}) = (\alpha)$$
for some $\alpha \in \mathcal{O}_{2\ell}$. Now $\psi_{E/KL}(\mathfrak{q})$ is a generator of $N_{KL/K}(\mathfrak{q})$ but $\psi_{E/KL}(\mathfrak{q}) \notin \mathcal{O}_2$ by the hypothesis, so $\psi_{E/KL}(\mathfrak{q}) = \pm i\alpha$. Therefore, $\psi_{E/KL}(\mathfrak{q}) \notin \mathcal{O}_\ell$, and hence $m(\ell) = 0$.   □

PROPOSITION 3.3.   Let $K = \mathbb{Q}(\zeta_3)$ and let $\ell \in \mathbb{Z}_{>0}$ be prime with $\ell \neq 3$. Suppose that there exists a finite prime $\mathfrak{q}$ of KL satisfying all of the following conditions.
   (i) $\mathfrak{q}$ is coprime to 3ℓ
   (ii) E has good reduction at $\mathfrak{q}$,
   (iii) $f_{\mathfrak{s}/\mathfrak{p}} \mid f_{\mathfrak{q}/\mathfrak{p}}$, where $\mathfrak{p} = \mathfrak{q} \cap \mathcal{O}_K$ and $\mathfrak{s}$ is a prime of $K_{3\ell}$ above $\mathfrak{p}$,
   (iv) $\psi_{E/KL}(\mathfrak{q}) \notin \mathcal{O}_3$.
Then $m(\ell) = 0$ and hence
$$(\mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E))_{\ell^\infty} = \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_L}_{\ell^\infty} = \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_{KL}}_{\ell^\infty} = 0.$$

As before, condition (iii) is trivially satisfied if $K_{3\ell} \subseteq KL$.

Proof.   The strategy is the same as for Proposition 3.2.   □

EXAMPLE 1.   Let E be the elliptic curve over $\mathbb{Q}$ with affine equation
$$y^2 + y = x^3 - x^2 - 7x + 10.$$
By [14], E has complex multiplication by the ring of integers of $K = \mathbb{Q}(\sqrt{-11})$. Theorem 3.1 tells us that $m(\ell) = n(\ell) = 0$ for every prime $\ell \in \mathbb{Z}_{>0}$ and therefore
$$\mathrm{Br}(E \times E) = \mathrm{Br}_1(E \times E).$$
Let θ denote the image of complex conjugation in $\mathrm{End}\, E_{11}/(\mathcal{O}_K \otimes \mathbb{Z}/11)$. Then Theorem 2.8 gives
$$\mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_{\mathbb{Q}(\sqrt{-11})}} = \mathrm{Br}(\overline{E} \times \overline{E})^{\Gamma_{\mathbb{Q}}} = \mathcal{O}_K\theta \cong \mathbb{Z}/11.$$

EXAMPLE 2.   Let E be the elliptic curve over $\mathbb{Q}$ with affine equation

$$y^2 = x^3 - Dx$$

where $D \in \mathbb{Z} \setminus \{0\}$. Then $\operatorname{End} E = \mathbb{Z}[i]$. Let $K = \mathbb{Q}(i)$. For any odd prime $\ell \in \mathbb{Z}_{>0}$, Theorem 3.1 gives

$$(\operatorname{Br}(E \times E) / \operatorname{Br}_1(E \times E))_{\ell^\infty} = \operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_\mathbb{Q}} = \operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_K} = 0.$$

Theorem 3.1 tells us that $n(2) = 1$. We must compute $m(2)$. By Proposition 2.2, $m(2) \leq n(2)$. Let $\mathfrak{q}$ be a finite prime of $\mathbb{Z}[i]$ that is coprime to $2D$. Let $\pi_\mathfrak{q} \in \mathbb{Z}[i]$ be the unique generator of $\mathfrak{q}$ such that $\pi_\mathfrak{q} \equiv 1 \pmod{(2 + 2i)}$. Exercise 2.34 in [**22**] shows that

$$\psi_{E/K}(\mathfrak{q}) = \left(\frac{D}{\pi_\mathfrak{q}}\right)_4^{-1} \pi_\mathfrak{q}$$

where $(\frac{\cdot}{\cdot})_4$ denotes the quartic residue symbol on $\mathbb{Z}[i]$.

First suppose that D is a square in $\mathbb{Z}[i]$. Then for all finite primes $\mathfrak{q}$ which are coprime to $2D$, $\psi_{E/K}(\mathfrak{q}) = \pm \pi_\mathfrak{q} \in \mathcal{O}_2$ and therefore $m(2) = 1$. Let θ denote the image of complex conjugation in $\operatorname{End} E_8/(\mathbb{Z}[i] \otimes \mathbb{Z}/8)$. Applying Theorems 2.8 and 2.6, we see that

$$\operatorname{Br}(\overline{E} \times \overline{E})^{\Gamma_K} = \operatorname{Br}(\overline{E} \times \overline{E})_{2^\infty}^{\Gamma_K} = \mathbb{Z}[i]\theta \cong \mathbb{Z}/4 \times \mathbb{Z}/4$$

$$\text{and} \quad \operatorname{Br}(\overline{E} \times \overline{E})^{\Gamma_\mathbb{Q}} = \operatorname{Br}(\overline{E} \times \overline{E})_{2^\infty}^{\Gamma_\mathbb{Q}} = \mathcal{O}_2\theta \cong \mathbb{Z}/4 \times \mathbb{Z}/2.$$

Applying Theorem 2.9, we see that

$$\frac{\operatorname{Br}(E \times E)}{\operatorname{Br}_1(E \times E)} = \frac{\operatorname{Br}(E \times E)_4}{\operatorname{Br}_1(E \times E)_4} = \frac{\operatorname{End}_{\Gamma_\mathbb{Q}} E_4}{(\mathbb{Z}[i] \otimes \mathbb{Z}/4)^{\Gamma_\mathbb{Q}}}$$

$$\cong \begin{cases} \mathbb{Z}/2 \times \mathbb{Z}/2 & \text{if } D \text{ is a square in } \mathbb{Z} \\ \mathbb{Z}/2 & \text{if } D \text{ is not a square in } \mathbb{Z}. \end{cases}$$

Now suppose that D is not a square in $\mathbb{Z}[i]$. By [**2**], Exercise 6.1, there exist infinitely many finite primes $\mathfrak{q}$ of K coprime to $2D$ such that D is not a square modulo $\mathfrak{q}$. For such $\mathfrak{q}$, we have $\psi_{E/K}(\mathfrak{q}) = \pm i\pi_\mathfrak{q}$ and therefore $\psi_{E/K}(\mathfrak{q}) \notin \mathcal{O}_2$. Consequently, $m(2) = 0$. Let η denote the image of complex conjugation in $\operatorname{End} E_4/(\mathbb{Z}[i] \otimes \mathbb{Z}/4)$. Then Theorem 2.8 gives

$$\operatorname{Br}(\overline{E} \times \overline{E})^{\Gamma_K} = \operatorname{Br}(\overline{E} \times \overline{E})^{\Gamma_\mathbb{Q}} = \mathbb{Z}[i]\eta \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

and Theorem 2.9 gives $\operatorname{Br}(E \times E) = \operatorname{Br}_1(E \times E)$.

EXAMPLE 3.   Let E be the elliptic curve over $\mathbb{Q}$ with affine equation

$$y^2 = x^3 + D$$

where $D \in \mathbb{Z} \setminus \{0\}$. Then $\operatorname{End} E = \mathbb{Z}[\zeta_3]$, where ζ_3 denotes a primitive 3rd root of unity. Let $K = \mathbb{Q}(\zeta_3)$. For any prime $\ell > 3$, Theorem 3.1 tells us that $m(\ell) = 0$ and therefore

$$(\operatorname{Br}(E \times E) / \operatorname{Br}_1(E \times E))_{\ell^\infty} = \operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_\mathbb{Q}} = \operatorname{Br}(\overline{E} \times \overline{E})_{\ell^\infty}^{\Gamma_K} = 0.$$

It remains to compute $m(\ell)$ for $\ell \leq 3$. For $\ell \leq 3$, Theorem 3.1 gives $m(\ell) \leq 1$. Let $\mathfrak{q}$ be a finite prime of K that is coprime to $6D$. Let $\pi_\mathfrak{q} \in \mathbb{Z}[\zeta_3]$ be the unique generator of $\mathfrak{q}$ which satisfies $\pi_\mathfrak{q} \equiv 1 \pmod 3$. By [**22**], Ch. II, Example 10.6, the Grössencharacter attached to E/K is given by

$$\psi_{E/K}(\mathfrak{q}) = \left(\frac{4D}{\pi_\mathfrak{q}}\right)_6^{-1} \pi_\mathfrak{q} \tag{3.1}$$

where $(\frac{\cdot}{\cdot})_6$ denotes the sextic residue symbol on $\mathbb{Z}[\zeta_3]$.

Computing $m(2)$ By the cubic reciprocity law (see Theorem 7.8 of [**12**], for example),

$$\left(\frac{4}{\pi_{\mathfrak{q}}}\right)_6 = \left(\frac{2}{\pi_{\mathfrak{q}}}\right)_3 = \left(\frac{\pi_{\mathfrak{q}}}{2}\right)_3 \equiv \pi_{\mathfrak{q}} \pmod{2} \tag{3.2}$$

where $(\frac{\cdot}{\cdot})_3$ denotes the cubic residue symbol on $\mathbb{Z}[\zeta_3]$. Substituting (3.2) into (3.1) gives

$$\psi_{E/K}(\mathfrak{q}) = \left(\frac{4}{\pi_{\mathfrak{q}}}\right)_6^{-1} \left(\frac{D}{\pi_{\mathfrak{q}}}\right)_6^{-1} \pi_{\mathfrak{q}} \equiv \left(\frac{D}{\pi_{\mathfrak{q}}}\right)_6^{-1} \pmod{2}. \tag{3.3}$$

First, suppose that D is a cube in $\mathbb{Z}$ (equivalently, D is a cube in $\mathbb{Z}[\zeta_3]$). Then $\left(\frac{D}{\pi_{\mathfrak{q}}}\right)_6 = \pm 1$ and (3.3) shows that $\psi_{E/K}(\mathfrak{q}) \in \mathcal{O}_2$ for all finite primes $\mathfrak{q}$ that are coprime to $6D$. Therefore, $m(2) = 1$.

Now suppose that D is not a cube in $\mathbb{Z}$. By [**2**], Exercise 6.1, there exists a finite prime $\mathfrak{q}$ of K coprime to $6D$ such that D is not a cube modulo $\mathfrak{q}$. For such $\mathfrak{q}$, $\left(\frac{D}{\pi_{\mathfrak{q}}}\right)_6 \neq \pm 1$, and (3.3) shows that $\psi_{E/K}(\mathfrak{q}) \notin \mathcal{O}_2$. Therefore, $m(2) = 0$.

Computing $m(3)$ First suppose that $4D$ is a cube in $\mathbb{Z}$. Then (3.1) shows that for all finite primes $\mathfrak{q}$ which are coprime to $6D$, $\psi_{E/K}(\mathfrak{q}) = \pm \pi_{\mathfrak{q}} \in \mathcal{O}_3$. Hence, $m(3) = 1$.

Now suppose that $4D$ is not a cube in $\mathbb{Z}$. By [**2**], Exercise 6.1, there exists a finite prime $\mathfrak{q}$ of K coprime to $6D$ such that $4D$ is not a cube modulo $\mathfrak{q}$. For such $\mathfrak{q}$, $\left(\frac{4D}{\mathfrak{q}}\right)_6 \neq \pm 1$, whereby $\psi_{E/K}(\mathfrak{q}) \notin \mathcal{O}_3$. Therefore, $m(3) = 0$.

4.   The Brauer group of $\mathrm{Kum}(E \times E)$

Let L be a number field and let E/L be an elliptic curve with complex multiplication by an order $\mathcal{O}$ of an imaginary quadratic field K. Let $X = \mathrm{Kum}(E \times E)$ be the K3 surface which is the minimal desingularisation of the quotient of $E \times E$ by the involution $(P, Q) \mapsto (-P, -Q)$.

PROPOSITION 4.1.   *If $\Delta_K \equiv 1 \pmod 4$ and $2 \nmid [\mathcal{O}_K : \mathcal{O}]$ then*

$$\mathrm{Br}_1(X) = \mathrm{Br}(L)$$

and therefore there is no algebraic Brauer-Manin obstruction to weak approximation on X.

Proof.   By Proposition 1.4 of [**25**], it suffices to show that $H^1(L, \mathcal{O}) = 0$. Inflation-restriction gives

$$0 \to H^1(\mathrm{Gal}(KL/L), \mathcal{O}) \to H^1(L, \mathcal{O}) \to H^1(KL, \mathcal{O}) = \mathrm{Hom}_{cts}(\Gamma_{KL}, \mathbb{Z}^2) = 0.$$

Therefore, $H^1(L, \mathcal{O}) \cong H^1(\mathrm{Gal}(KL/L), \mathcal{O})$. If $K \subset L$ then $H^1(\mathrm{Gal}(KL/L), \mathcal{O}) = 0$, so suppose that

$$\mathrm{Gal}(KL/L) = \langle \tau \rangle \cong \mathbb{Z}/2.$$

Then

$$H^1(\mathrm{Gal}(KL/L), \mathcal{O}) = \frac{\{x \in \mathcal{O} \mid x + \tau(x) = 0\}}{\{\tau(x) - x \mid x \in \mathcal{O}\}}.$$

Writing $\mathcal{O} = \mathbb{Z}[f\alpha]$, where $f = [\mathcal{O}_K : \mathcal{O}]$ and $\alpha = (1 + \sqrt{\Delta_K})/2$, gives

$$\{x \in \mathcal{O} \mid x + \tau(x) = 0\} = \{\tau(x) - x \mid x \in \mathcal{O}\} = f\sqrt{\Delta_K} \cdot \mathbb{Z}.$$

$\square$

By (1.1), the existence of a transcendental element of odd order in $\mathrm{Br}(E \times E)$ implies that $\mathrm{Br}(X)$ contains a transcendental element. The same cannot be said for transcendental elements of even order. For this reason, we concentrate on elliptic curves E for which $\mathrm{Br}(E \times E)$ contains a transcendental element of odd order.

THEOREM 4.2.   *Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_K$ such that $\mathrm{Br}(E \times E)$ contains a transcendental element of odd order. Then $K = \mathbb{Q}(\zeta_3)$ and E has affine equation $y^2 = x^3 + 2c^3$ for some squarefree $c \in \mathbb{Z}$. Furthermore,*

$$\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q}) = \mathrm{Br}(E \times E)/\mathrm{Br}_1(E \times E) = \mathrm{Br}(E \times E)_3/\mathrm{Br}_1(E \times E)_3 = (\mathbb{Z}/3)\eta \cong \mathbb{Z}/3$$

where η denotes the image of complex conjugation in $\mathrm{End}\, E_3/(\mathbb{Z}[\zeta_3] \otimes \mathbb{Z}/3)$.

Proof.   Setting $L = \mathbb{Q} = \mathbb{Q}(j(E))$ in Theorem 3.1 shows that $K = \mathbb{Q}(\zeta_3)$. Since $\mathbb{Z}[\zeta_3]$ has class number 1, E is isomorphic over $\overline{\mathbb{Q}}$ to the elliptic curve E' with affine equation $y^2 = x^3 + 1$. Therefore, E is the sextic twist of E' by a class in $H^1(\mathbb{Q}, \mu_6) = \mathbb{Q}^\times/(\mathbb{Q}^\times)^6$. Consequently, E has an affine equation of the form $y^2 = x^3 + D$ for some sixth-power-free $D \in \mathbb{Z}$. Example 3 shows that $m(\ell) = 0$ for every odd prime ℓ with $\ell \neq 3$. Since $\mathrm{Br}(E \times E)$ contains a transcendental element of odd order, we have $m(3) \neq 0$. The computation of $m(3)$ in Example 3 shows that $m(3) = 1$ and $4D$ is a cube in $\mathbb{Z}$. Now the computation of $m(2)$ in Example 3 gives $m(2) = 0$. Thus, the statement on the transcendental Brauer group of $E \times E$ follows from Theorem 2.9. The statement for $X = \mathrm{Kum}(E \times E)$ follows from (1.1) and Proposition 4.1. $\square$

5.   *A transcendental Brauer-Manin obstruction to weak approximation*

Henceforth, for each $c \in \mathbb{Q}^\times$, let E^c be the elliptic curve over $\mathbb{Q}$ with affine equation

$$y^2 = x^3 + 2c^3.$$

Let $X = \mathrm{Kum}(E^c \times E^c)$. An affine model for X is

$$u^2 = (x^3 + 2c^3)(t^3 + 2c^3) \tag{5.1}$$

Note that X is independent of $c \in \mathbb{Q}^\times$, since $(x, t, u) \mapsto (x/c, t/c, u/c^3)$ gives the following alternative affine model for X

$$u^2 = (x^3 + 2)(t^3 + 2). \tag{5.2}$$

By Proposition 4.1, $\mathrm{Br}_1(X) = \mathrm{Br}(\mathbb{Q})$ and therefore there is no algebraic Brauer-Manin obstruction to weak approximation on X. By (1.1),

$$\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q}) = \mathrm{Br}(X)_3/\mathrm{Br}_1(X)_3 = \mathrm{Br}(E^c \times E^c)_3/\mathrm{Br}_1(E^c \times E^c)_3.$$

Let $\tau \in \Gamma_\mathbb{Q} \setminus \Gamma_{\mathbb{Q}(\zeta_3)}$ and let θ denote the image of τ in $\mathrm{End}\, E_3^c$. The image of τ generates $\mathrm{End}_{\Gamma_\mathbb{Q}}(E_3^c)/(\mathbb{Z}/3) \cong \mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q}) \cong \mathbb{Z}/3$. Let $\mathcal{A} \in \mathrm{Br}(X) \setminus \mathrm{Br}(\mathbb{Q})$ be a corresponding generator of $\mathrm{Br}(X)/\mathrm{Br}(\mathbb{Q})$.

For a prime ℓ, let

$$\cup : H^1(\mathbb{Q}_\ell, E_3^c) \times H^1(\mathbb{Q}_\ell, E_3^c) \longrightarrow \mathrm{Br}(\mathbb{Q}_\ell)_3 \xrightarrow{\mathrm{inv}_\ell} \tfrac{1}{3}\mathbb{Z}/\mathbb{Z}$$

be the non-degenerate pairing given by the composition of the cup product, the Weil pairing and the local invariant. Let θ^* denote the map induced by θ on $H^1(\mathbb{Q}_\ell, E_3^c)$. For $P \in E(\mathbb{Q}_\ell)$, let χ_P denote the image of P under the homomorphism

$$\chi : E^c(\mathbb{Q}_\ell) \to H^1(\mathbb{Q}_\ell, E_3^c).$$

PROPOSITION 5.1. *Let $P, Q \in E^c(\mathbb{Q}_\ell) \setminus E_2^c$. The $\mathbb{Q}_\ell$-point (P, Q) on $E^c \times E^c$ gives rise to a point $R \in X(\mathbb{Q}_\ell)$. We have*

$$\mathrm{ev}_{\mathcal{A},\ell}(R) = \chi_P \cup \theta^*(\chi_Q) \in \frac{1}{3}\mathbb{Z}/\mathbb{Z}. \tag{5.3}$$

Proof. The statement follows from the results of [**25**], Section 3. The details are explained in Section 5.1 of [**10**]. □

THEOREM 5.2. *Let $\mathcal{A} \in \mathrm{Br}(X)_3 \setminus \mathrm{Br}(\mathbb{Q})$. Let $\nu \neq 3$ be a rational place. Then the evaluation map $\mathrm{ev}_{\mathcal{A},\nu} : X(\mathbb{Q}_\nu) \to \mathrm{Br}(\mathbb{Q}_\nu)_3$ is zero.*

Proof. The statement for the infinite place is clear, since $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2$ has trivial 3-torsion. By [**4**], finite primes of good reduction do not appear in the description of the Brauer-Manin set. Lemma 4.2 of [**17**] shows that odd primes of good reduction for an abelian surface are primes of good reduction for the corresponding Kummer surface. Thus, by (5.2), $\mathrm{ev}_{\mathcal{A},\ell}$ is zero for every finite prime $\ell \nmid 6$. From now on, let $\ell = 2$, and let $R \in X(\mathbb{Q}_2)$. We will show that $\mathrm{ev}_{\mathcal{A},2}(R) = 0$. We can represent R by (x_0, t_0, u_0) satisfying (5.2). Let $d_R = t_0^3 + 2$. Since the evaluation map $\mathrm{ev}_{\mathcal{A},2} : X(\mathbb{Q}_2) \to \mathrm{Br}(\mathbb{Q}_2)_3$ is locally constant, we are free to use the implicit function theorem to replace R by a point $R' = (x_1, t_1, u_1) \in X(\mathbb{Q}_2)$, sufficiently close to R, such that $d = d_{R'} \in \mathbb{Q}^\times$ and $u_1 \neq 0$. Now R' gives rise to $P = (dx_1, du_1) \in E^d(\mathbb{Q}_2)$ and $Q = (dt_1, d^2) \in E^d(\mathbb{Q}_2)$. Recalling that $X = \mathrm{Kum}(E^d \times E^d)$, we apply Proposition 5.1 to see that

$$\mathrm{ev}_{\mathcal{A},2}(R') = \chi_P \cup \theta^*(\chi_Q) \in \frac{1}{3}\mathbb{Z}/\mathbb{Z}. \tag{5.4}$$

We will study $E^d(\mathbb{Q}_2)$. Denote by $E_0^d(\mathbb{Q}_2)$ the $\mathbb{Q}_2$-points of E^d that reduce to smooth points on the reduction of E^d at 2. Rescaling the coordinates x, y of E^d if necessary, we may assume that the 2-adic valuation of d satisfies $\mathrm{ord}_2(d) \in \{0, 1\}$.

First suppose that $\mathrm{ord}_2(d) = 0$. Then the equation $y^2 = x^3 + 2d^3$ is a minimal Weierstrass equation, and $E^d/\mathbb{Q}_2$ has additive reduction. Since $2 \nmid d$, Tate's algorithm (as described in [**22**], Ch. IV, §9) terminates at Step 3 and $E^d(\mathbb{Q}_2) = E_0^d(\mathbb{Q}_2)$. Alternatively, considering the 2-adic valuations of the coordinates of points in $E^d(\mathbb{Q}_2)$ allows one to verify directly that $E^d(\mathbb{Q}_2) = E_0^d(\mathbb{Q}_2)$.

Now suppose that $d = 2e$ for some $e \in \mathbb{Z}_2^*$. Then the equation $y^2 = x^3 + 2d^3$ is no longer minimal. The transformation $y = y' + 2^2$ gives the equation

$$y'^2 + 2^3 y' = x^3 + 2^4(e^3 - 1). \tag{5.5}$$

Note that $e \in \mathbb{Z}_2^*$, so $e^3 \equiv e \equiv \pm 1 \pmod 4$. Suppose that $e \in -1 + 4\mathbb{Z}_2$. Then we have $\mathrm{ord}_2(2^4(e^3 - 1)) < 6$, which implies that (5.5) is minimal and $E^d/\mathbb{Q}_2$ has additive reduction. Applying Tate's algorithm, or considering the 2-adic valuations of the coordinates of points in $E^d(\mathbb{Q}_2)$, we see that $E^d(\mathbb{Q}_2) = E_0^d(\mathbb{Q}_2)$.

In both the case $\mathrm{ord}_2(d) = 0$ and the case $d \in -2 + 8\mathbb{Z}_2$, we may apply Theorem 1 of [**18**] to see that $E^d(\mathbb{Q}_2) = E_0^d(\mathbb{Q}_2)$ is topologically isomorphic to $\mathbb{Z}_2$, which is 3-divisible. Therefore, if $\mathrm{ord}_2(d) = 0$ or $d \in -2 + 8\mathbb{Z}_2$ then $\chi = 0$.

Finally, suppose that $d = 2e$ with $e \in 1 + 4\mathbb{Z}_2$. Then (5.5) is no longer minimal and the transformation $(x, y') = (2^2 x'', 2^3 y'')$ gives $y''^2 + y'' = x''^3 + \frac{e^3 - 1}{4}$, which is a minimal Weierstrass equation for E^d. In particular, $E^d/\mathbb{Q}_2$ has good reduction. Therefore,

$$E^d(\mathbb{Q}_2)/E_1^d(\mathbb{Q}_2) \cong \tilde{E}^d(\mathbb{F}_2) \cong \mathbb{Z}/3,$$

where $E_1^d(\mathbb{Q}_2)$ denotes the kernel of the reduction map and $\tilde{E}^d$ denotes the reduced elliptic curve. Thus, $3E^d(\mathbb{Q}_2) \subset E_1^d(\mathbb{Q}_2)$. We will show that this inclusion is an equality. The standard

filtration on the $\mathbb{Q}_2$-points of E^d gives

$$E^d(\mathbb{Q}_2) \supset E_1^d(\mathbb{Q}_2) \supset E_2^d(\mathbb{Q}_2) \supset \ldots$$

The theory of formal groups shows that $E_2^d(\mathbb{Q}_2) \cong 4\mathbb{Z}_2$. Hence, $E_2^d(\mathbb{Q}_2)$ is 3-divisible. Since $E_1^d(\mathbb{Q}_2)/E_2^d(\mathbb{Q}_2) \cong \mathbb{Z}/2$, it follows that $E_1^d(\mathbb{Q}_2)$ is 3-divisible. Therefore,

$$E_1^d(\mathbb{Q}_2) = 3E_1^d(\mathbb{Q}_2) = 3E^d(\mathbb{Q}_2).$$

Thus, χ factors through $E^d(\mathbb{Q}_2)/3E^d(\mathbb{Q}_2) = E^d(\mathbb{Q}_2)/E_1^d(\mathbb{Q}_2) \cong \mathbb{Z}/3$ and it is enough to show that

$$\chi_P \cup \theta^*(\chi_P) = 0$$

for any $P \in E^d(\mathbb{Q}_2) \setminus E_1^d(\mathbb{Q}_2)$ with $2P \neq 0$. The diagonal embedding $E^d \to E^d \times E^d$ induces a map $E^d \to X$ whose image is a copy of $\mathbb{P}_{\mathbb{Q}}^1$. The restriction of $\mathcal{A}$ to $\mathbb{P}_{\mathbb{Q}}^1$ is in $\mathrm{Br}(\mathbb{P}_{\mathbb{Q}}^1) = \mathrm{Br}(\mathbb{Q})$. In other words, $\mathcal{A}$ restricts to a constant algebra on the image of E^d in X. Thus, the evaluation of $\mathcal{A}$ at a point on X corresponding to (P, P) on $E^d(\mathbb{Q}_2) \times E^d(\mathbb{Q}_2)$ is independent of the point P. Hence, it suffices to show that $\chi_P \cup \theta^*(\chi_P) = 0$ for a single $P \in E^d(\mathbb{Q}_2)$. Taking $P \in 3E^d(\mathbb{Q}_2)$ completes the proof. □

The main result of this section is the following theorem.

THEOREM 5.3.   *The evaluation map*

$$\mathrm{ev}_{\mathcal{A},3} : X(\mathbb{Q}_3) \to \frac{1}{3}\mathbb{Z}/\mathbb{Z}$$

is surjective. Consequently,

$$X(\mathbb{A}_{\mathbb{Q}})^{\mathrm{Br}(X)} = X(\mathbb{Q}_3)_0 \times X(\mathbb{R}) \times \prod_{\ell \neq 3} X(\mathbb{Q}_\ell) \subsetneq X(\mathbb{A}_{\mathbb{Q}})$$

where $X(\mathbb{Q}_3)_0$ denotes the points $P \in X(\mathbb{Q}_3)$ with $\mathrm{ev}_{\mathcal{A},3}(P) = 0$, and the product runs over prime numbers $\ell \neq 3$.

Theorem 5.3 will be proved via several auxiliary results.

LEMMA 5.4.   *In order to show that $\mathrm{ev}_{\mathcal{A},3} : X(\mathbb{Q}_3) \to \frac{1}{3}\mathbb{Z}/\mathbb{Z}$ is surjective, it is enough to exhibit $c \in \mathbb{Q}^\times$ and $P \in E^c(\mathbb{Q}_3)$ such that $\theta^*(\chi_P)$ is not in the image of $E^c(\mathbb{Q}_3)$ inside $H^1(\mathbb{Q}_3, E_3^c)$.*

Proof.   Suppose that $P \in E^c(\mathbb{Q}_3)$ is such that $\theta^*(\chi_P)$ is not in the image of $E^c(\mathbb{Q}_3)$ inside $H^1(\mathbb{Q}_3, E_3^c)$. Since the image of $E^c(\mathbb{Q}_3)$ is a maximal isotropic subspace inside $H^1(\mathbb{Q}_3, E_3^c)$, there exists $Q \in E^c(\mathbb{Q}_3)$ such that $\chi_Q \cup \theta^*(\chi_P) \neq 0$. Note that $P, Q \notin E_2^c$ because if, for example, $2P = 0$ then $\chi_P = \chi_{3P} = 0$. Now by Proposition 5.1, the point $R \in X(\mathbb{Q}_3)$ coming from $(Q, P) \in E^c(\mathbb{Q}_3) \times E^c(\mathbb{Q}_3)$ satisfies

$$\mathrm{ev}_{\mathcal{A},3}(R) = \chi_Q \cup \theta^*(\chi_P) \neq 0.$$

Surjectivity follows since for every $n \in \mathbb{Z}$, $\chi_{nQ} \cup \theta^*(\chi_P) = n(\chi_Q \cup \theta^*(\chi_P))$. □

In Proposition 5.6, we will show that we can take $c = 3$ and $P = (3, 9)$ in Lemma 5.4. From now on, let $E = E^{(3)}$ be the elliptic curve with affine equation $y^2 = x^3 + 2 \cdot 3^3$. First, we determine the group $E(\mathbb{Q}_3)/3$ and give explicit generators.

LEMMA 5.5.   *We have $E(\mathbb{Q}_3)/3 \cong (\mathbb{Z}/3)^2$, with generators $P = (3, 9)$ and $Q = (4, \sqrt{2 \cdot 59})$.*

Proof.   Denote by $E_0(\mathbb{Q}_3)$ the $\mathbb{Q}_3$-points of E that reduce to smooth points on the reduction of E modulo 3. Denote by $E_1(\mathbb{Q}_3)$ the kernel of reduction. The elliptic curve $E/\mathbb{Q}_3$ has additive reduction and hence

$$E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3) \cong \mathbb{F}_3. \tag{5.6}$$

Applying Tate's algorithm (or see the Tamagawa number for 3 given in [**15**]), we find that

$$E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3) \cong \mathbb{Z}/3. \tag{5.7}$$

By Theorem 1 of [**18**], $E_0(\mathbb{Q}_3) \cong \mathbb{Z}_3$. The following sequence is exact.

$$0 \longrightarrow \frac{E_0(\mathbb{Q}_3)}{3E(\mathbb{Q}_3)} \longrightarrow \frac{E(\mathbb{Q}_3)}{3E(\mathbb{Q}_3)} \longrightarrow \frac{E(\mathbb{Q}_3)}{E_0(\mathbb{Q}_3)} \longrightarrow 0.$$

Since $E_0(\mathbb{Q}_3) \cong \mathbb{Z}_3$ and $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3) \cong \mathbb{F}_3$, we have $3E_0(\mathbb{Q}_3) = E_1(\mathbb{Q}_3)$. By (5.7), $E(\mathbb{Q}_3)/E_0(\mathbb{Q}_3) \cong \mathbb{Z}/3$. A suitable generator is $P = (3, 9)$. A calculation shows that $3P = (3^{-2} \cdot 19, -3^{-3} \cdot 5 \cdot 43) \in E_1(\mathbb{Q}_3)$. Therefore, $3E(\mathbb{Q}_3) = E_1(\mathbb{Q}_3)$. The point Q generates $E_0(\mathbb{Q}_3)/E_1(\mathbb{Q}_3)$. $\square$

In light of Lemma 5.4, we will study the action of θ on the image of $E(\mathbb{Q}_3)$ in $H^1(\mathbb{Q}_3, E_3)$. We have

$$E_3 = \{O_E, (0, 3\sqrt{6}), (0, -3\sqrt{6})\} \cup \bigcup_{0 \le k \le 2} \{(-6\zeta_3^k, 9\sqrt{-2}), (-6\zeta_3^k, -9\sqrt{-2})\}$$

and therefore

$$\mathbb{Q}_3(E_3) = \mathbb{Q}_3(\zeta_3, \sqrt{6}, \sqrt{-2}) = \mathbb{Q}_3(\zeta_3).$$

Let $F = \mathbb{Q}_3(E_3) = \mathbb{Q}_3(\zeta_3)$. The inflation-restriction exact sequence gives

$$H^1(\mathrm{Gal}(F/\mathbb{Q}_3), E_3) \to H^1(\mathbb{Q}_3, E_3) \to H^1(F, E_3)^{\mathrm{Gal}(F/\mathbb{Q}_3)} \to H^2(\mathrm{Gal}(F/\mathbb{Q}_3), E_3).$$

Since $[F : \mathbb{Q}_3] = 2$, we have $H^1(\mathrm{Gal}(F/\mathbb{Q}_3), E_3) = H^2(\mathrm{Gal}(F/\mathbb{Q}_3), E_3) = 0$. Therefore, the restriction map gives an isomorphism

$$H^1(\mathbb{Q}_3, E_3) \to H^1(F, E_3)^{\mathrm{Gal}(F/\mathbb{Q}_3)}.$$

Let $T \in E(\mathbb{Q}_3)$. In a slight abuse of notation, we continue to write χ_T for the image of T in $H^1(F, E_3) = \mathrm{Hom}_{\mathrm{cts}}(\Gamma_F, E_3)$. In order to study the action of θ on $\chi_T(\Gamma_F) \subset E_3$, we will use the following polynomials. Let $f_T \in \mathbb{Q}_3[t]$ be the degree 9 polynomial satisfied by the x-coordinates of the points $R \in E(\overline{\mathbb{Q}_3})$ such that $3R = T$. By Exercise III.3.7 of [**22**],

$$f_T(t) = 3^2 t^2 (t - x(T))(t^3 + 2^3 \cdot 3^3)^2 - 2^3 (t^3 + 2 \cdot 3^3)(t^6 + 2^3 \cdot 3^3 \cdot 5t^3 - 2^5 \cdot 3^6). \tag{5.8}$$

Let $g_T \in \mathbb{Q}_3(\zeta_3)[t]$ be the cubic polynomial satisfied by the x-coordinates of the points $S \in E(\overline{\mathbb{Q}_3})$ such that $(1 - \zeta_3)S = T$. The addition formula shows that

$$g_T(t) = t^3 + 3\zeta_3 x(T)t^2 + 2^3 \cdot 3^3. \tag{5.9}$$

Combining Lemma 5.4 with Proposition 5.6 below completes the proof of Theorem 5.3.

PROPOSITION 5.6.   *Let $P = (3, 9) \in E(\mathbb{Q}_3)$. Then $\theta^*(\chi_P)$ is not in the image of $E(\mathbb{Q}_3)$ inside $H^1(\mathbb{Q}_3, E_3)$.*

Proof.   We have $\mathbb{Q}_3(E_3) = \mathbb{Q}_3(\zeta_3)$. By Lemma 5.5, $E(\mathbb{Q}_3)/3$ is generated by $P = (3, 9)$ and $Q = (4, \sqrt{2 \cdot 59})$. A calculation using MAGMA [**1**] shows that the degree 9 polynomial f_P given

by (5.8) is irreducible over $\mathbb{Q}_3$ and therefore also irreducible over $\mathbb{Q}_3(\zeta_3)$. By (5.9), we have

$$g_P(t) = t^3 + 3^2\zeta_3 t^2 + 2^3 \cdot 3^3 \quad \text{and} \quad g_Q(t) = t^3 + 2^2 3\zeta_3 t^2 + 2^3 \cdot 3^3.$$

Making a change of variables $t = 3u$, we see that $g_Q(t)$ defines the same extension of $\mathbb{Q}(\zeta_3)$ as $h_Q(u) = u^3 + 2^2\zeta_3 u^2 + 2^3$. Now $h_Q(u) \equiv u^3 + u^2 - 1 \pmod{(1 - \zeta_3)}$, which is irreducible over the residue field $\mathbb{F}_3$ of $\mathbb{Q}_3(\zeta_3)$. Thus, $g_Q(t)$ defines an unramified extension of $\mathbb{Q}_3(\zeta_3)$. On the other hand, we claim that $g_P(t)$ defines a ramified extension of $\mathbb{Q}_3(\zeta_3)$. Making a change of variables $t = 3(u + 1)$, we see that $g_P(t)$ defines the same extension of $\mathbb{Q}(\zeta_3)$ as $h_P(u) = u^3 + 3(1 + \zeta_3)u^2 + 3(1 + 2\zeta_3)u + 3\zeta_3 + 3^2$. Let $\pi = (1 - \zeta_3)$. Examining the π-adic valuation of the terms in $h_P(u)$, we see that any root of $h_P(u)$ has π-adic valuation $2/3$. Therefore, $g_P(t)$ defines a ramified extension of $\mathbb{Q}_3(\zeta_3)$, as claimed.

Let $R_P, R_Q \in E(\overline{\mathbb{Q}_3})$ be such that $3R_P = P$ and $3R_Q = Q$. Let $S_P = (1 - \zeta_3^2)R_P$ and let $S_Q = (1 - \zeta_3^2)R_Q$. Recall that $\mathbb{Q}_3(\zeta_3, x(R_P))$ is the degree 9 extension of $\mathbb{Q}_3(\zeta_3)$ defined by f_P. Since P is not a 2-torsion point, $\mathbb{Q}_3(\zeta_3, x(R_P)) = \mathbb{Q}_3(\zeta_3, R_P)$. Likewise, g_P defines the ramified cubic extension $\mathbb{Q}_3(\zeta_3, S_P)/\mathbb{Q}_3(\zeta_3)$ and g_Q defines the unramified cubic extension $\mathbb{Q}_3(\zeta_3, S_Q)/\mathbb{Q}_3(\zeta_3)$. Therefore, there exists $\sigma \in \Gamma_{\mathbb{Q}_3(\zeta_3)}$ such that $\sigma(S_Q) \neq S_Q$, $\sigma(S_P) = S_P$ and $\sigma(R_P) \neq R_P$. We have

$$(1 - \zeta_3^2)\chi_P(\sigma) = (1 - \zeta_3^2)(\sigma(R_P) - R_P) = \sigma(S_P) - S_P = 0$$

and

$$(1 - \zeta_3^2)\chi_Q(\sigma) = (1 - \zeta_3^2)(\sigma(R_Q) - R_Q) = \sigma(S_Q) - S_Q \neq 0.$$

Thus, $\chi_Q(\sigma) \notin E_{(1-\zeta_3)}$ and $\chi_P(\sigma) \in E_{(1-\zeta_3)} \setminus \{O_E\}$. Suppose for contradiction that $\theta^*(\chi_P)$ is in the image of $E(\mathbb{Q}_3)$ inside $H^1(\mathbb{Q}_3, E_3)$, so that

$$\theta^*(\chi_P) = \chi_{(aP+bQ)} = a\chi_P + b\chi_Q \tag{5.10}$$

for $a, b \in \mathbb{F}_3$. Note that θ acts as multiplication by -1 on $E_{(1-\zeta_3)} = \{O_E, (0, 3\sqrt{6}), (0, -3\sqrt{6})\}$, so

$$-\chi_P(\sigma) = \theta^*(\chi_P)(\sigma) = a\chi_P(\sigma) + b\chi_Q(\sigma) \tag{5.11}$$

which implies that $b\chi_Q(\sigma) \in E_{(1-\zeta_3)}$ and hence $b = 0$ and $a = -1$. Since g_P is irreducible over $\mathbb{Q}_3(\zeta_3)$, there exists $\rho \in \Gamma_{\mathbb{Q}(\zeta_3)}$ such that $\rho(S_P) \neq S_P$. For such ρ we have

$$(1 - \zeta_3^2)\chi_P(\rho) = (1 - \zeta_3^2)(\rho(R_P) - R_P) = \rho(S_P) - S_P \neq 0$$

and hence $\chi_P(\rho) \notin E_{(1-\zeta_3)}$. Therefore, $\chi_P(\Gamma_{\mathbb{Q}(\zeta_3)}) = E_3$. In particular, $T = (-6\zeta_3, 9\sqrt{-2})$ is in the image of χ_P. But $\theta(T) \neq -T$, which contradicts $\theta^*(\chi_P) = -\chi_P$. $\qquad\square$

References

1. W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language.* J. Symbolic Comput. **24** (1997), 235–265.

2. J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory.* Second Edition. London Mathematical Society. 2010.

3. D.A. Cox. *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory, and Complex Multiplication.* A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

4. J.-L. Colliot-Thélène and A.N. Skorobogatov. *Good reduction of the Brauer–Manin obstruction.* Trans. Amer. Math. Soc. **365** (2013), 579–590.

5. J.-L. Colliot-Thélène and A.N. Skorobogatov. *Descente galoisienne sur le groupe de Brauer.* J. reine angew. Math. **682** (2013), 141–165.

6. A. Grothendieck. *Le groupe de Brauer II.* In: Dix exposés sur la cohomologie des schémas (A. Grothendieck, N.H. Kuiper, eds.), North-Holland, 1968, 67–87.

7. D. Harari. *Obstructions de Manin transcendantes.* In: Number theory (Paris, 1993-1994), LMS Lecture Note Ser. 235 Cambridge Univ. Press, 1996, 75–87.

8. B. Hassett, P. Varilly and A. Várilly-Alvarado. *Transcendental obstructions to weak approximation on general K3 surfaces.* Advances in Mathematics **228** (2011), no. 3, 1377–1404.

9. E. Ieronymou. *Diagonal quartic surfaces and transcendental elements of the Brauer group.* J. Inst. Math. Jussieu (4) **9** (2010), 769–798.

10. E. Ieronymou and A.N. Skorobogatov. *Odd order Brauer-Manin obstruction on diagonal quartic surfaces.* Adv. Math. **270** (2015), 181–205. Corrigendum: `http://wwwf.imperial.ac.uk/~anskor/diag_corrigendum.pdf`

11. E. Ieronymou, A.N. Skorobogatov and Yu.G. Zarhin, *On the Brauer group of diagonal quartic surfaces.* (with an appendix by Sir Peter Swinnerton-Dyer). J. London Math. Soc. (2) **83** (2011), no. 3, 659–672.

12. F. Lemmermeyer. *Reciprocity Laws: from Euler to Eisenstein.* Springer Monographs in Mathematics, 2000.

13. S. Lang. *Complex multiplication.* Grundlehren Math. Wiss. 255, Springer-Verlag, 1983.

14. The LMFDB Collaboration, *The L-functions and Modular Forms Database, Home page of the Elliptic Curve 1728.o4 (Cremona label 1728v3),* `http://www.lmfdb.org/EllipticCurve/Q/1728/o/4`, 2015, [Online; accessed 29 September 2015].

15. The LMFDB Collaboration, *The L-functions and Modular Forms Database, Home page of the Elliptic Curve 121.b2 (Cremona label 121b1),* `http://www.lmfdb.org/EllipticCurve/Q/121/b/2`, 2015, [Online; accessed 29 September 2015].

16. Yu.I. Manin. *Le groupe de Brauer-Grothendieck en géométrie diophantienne.* In: Actes Congrès Internat. Math. Nice I (Gauthier-Villars, 1971), 401–411.

17. Y. Matsumoto. *On good reduction of some K3 surfaces related to abelian surfaces.* Tohoku Math J. **67** (2015), 83–104.

18. R. Pannekoek. *On p-torsion of p-adic elliptic curves with additive reduction.* arXiv:1211.5833v2

19. K.A. Ribet, *Galois action on division points of abelian varieties with real multiplications.* Amer. J. Math. Vol. 98, No. 3, pp. 751–804.

20. Th. Preu. *Example of a transcendental 3-torsion Brauer-Manin obstruction on a diagonal quartic surface.* In: Torsors, étale homotopy and applications to rational points. LMS Lecture Note series **405**, Cambridge University Press, 2013, 449–461.

21. K. Rubin and A. Silverberg. *Point counting on reductions of CM elliptic curves.* J. Number Theory **129** (2009) 2903–2923.

22. J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Graduate Texts in Mathematics **151**, Springer-Verlag, 1994.

23. A. Skorobogatov. *Torsors and rational points.* Cambridge Tracts in Mathematics **144**, Cambridge University Press, Cambridge, 2001.

24. A.N. Skorobogatov and Yu.G. Zarhin. *A finiteness theorem for the Brauer group of abelian varieties and K3 surfaces.* J. Alg. Geom. **17** (2008) 481–502.

25. A.N Skorobogatov and Yu.G. Zarhin. *The Brauer group of Kummer surfaces and torsion of elliptic curves.* J. reine angew. Math. **666** (2012) 115–140.

26. O. Wittenberg. *Transcendental Brauer-Manin obstruction on a pencil of elliptic curves.* In: Arithmetic of higher dimensional algebraic varieties (Palo Alto, 2002), B. Poonen, Yu. Tschinkel, eds. Progr. Math. **226** Birkhäuser, 2004, 259–267.

R. Newton,
Institut des Hautes Études Scientifiques,
35 Route de Chartres,
91440 Bures-sur-Yvette,
France

newton@ihes.fr
racheldominicanewton@gmail.com