ENDOMORPHISM ALGEBRAS OF GEOMETRICALLY SPLIT ABELIAN SURFACES OVER $\mathbb{Q}$

FRANCESC FITÉ AND XAVIER GUITART

Abstract. We determine the set of geometric endomorphism algebras of geometrically split abelian surfaces defined over $\mathbb{Q}$. In particular we find that this set has cardinality 92. The essential part of the classification consists in determining the set of quadratic imaginary fields M with class group $\mathrm{C}_2 \times \mathrm{C}_2$ for which there exists an abelian surface A defined over $\mathbb{Q}$ which is geometrically isogenous to the square of an elliptic curve with CM by M. We first study the interplay between the field of definition of the geometric endomorphisms of A and the field M. This reduces the problem to the situation in which E is a $\mathbb{Q}$-curve in the sense of Gross. We can then conclude our analysis by employing Nakamura's method to compute the endomorphism algebra of the restriction of scalars of a Gross $\mathbb{Q}$-curve.

Contents

1. Introduction

Let A be an abelian variety of dimension $g \geq 1$ defined over a number field k of degree d. Let us denote by $A_{\overline{\mathbb{Q}}}$ its base change to $\overline{\mathbb{Q}}$. We refer to $\mathrm{End}(A_{\overline{\mathbb{Q}}})$, the $\mathbb{Q}$-algebra spanned by the endomorphisms of A defined over $\overline{\mathbb{Q}}$, as the $\overline{\mathbb{Q}}$-endomorphism algebra of A. For a fixed choice of g and d, it is conjectured that the set of possibilities for $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ is finite. A slightly stronger form of this conjecture, applying

---

Date: March 5, 2020.

to endomorphism rings of abelian varieties over number fields, has been attributed to Coleman in [BFGR06].

Hereafter, let A denote an abelian surface defined over $\mathbb{Q}$. In the case that A is geometrically simple (that is, $A_{\overline{\mathbb{Q}}}$ is simple), the previous conjecture stands widely open. If A is principally polarized and has CM it has been shown by Murabayashi and Umegaki [MU01] that $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ is one of 19 possible quartic CM fields. However, narrowing down to a finite set the possible quadratic real fields and quaternion division algebras over $\mathbb{Q}$ which occur as $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ for some A has escaped all attempts of proof. See also [OS18] for recent more general results which prove Coleman's conjecture for CM abelian varieties.

In the present paper, we focus on the case that A is geometrically split, that is, the case in which $A_{\overline{\mathbb{Q}}}$ is isogenous to a product of elliptic curves, which we will assume from now on. Let $\mathcal{A}$ be the set of possibilities for $\mathrm{End}(A_{\overline{\mathbb{Q}}})$, where A is a geometrically split abelian surface over $\mathbb{Q}$.

Let us briefly recall how scattered results in the literature ensure the finiteness of $\mathcal{A}$ (we will detail the arguments in Section 4). Indeed, if $A_{\overline{\mathbb{Q}}}$ is isogenous to the product of two non-isogenous elliptic curves, then the finiteness (and in fact the precise description) of the set of possibilities for $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ follows from [FKRS12, Proposition 4.5]. If, on the contrary, $A_{\overline{\mathbb{Q}}}$ is isogenous to the square of an elliptic curve, then the finiteness of the set of possibilities for $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ was established by Shafarevich in [Sha96] (see also [Gon11] for the determination of the precise subset corresponding to modular abelian surfaces). In the present work, we aim at an effective version of Shafarevich's result. Our starting point is [FG18, Theorem 1.4], which we recall in our particular setting.

Theorem 1.1 ([FG18])**.** *If A is an abelian surface defined over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}}$ is isogenous to the square of an elliptic curve $E/\overline{\mathbb{Q}}$ with complex multiplication (CM) by a quadratic imaginary field M, then the class group of M is* 1, C_2, *or* $\mathrm{C}_2 \times \mathrm{C}_2$.

It should be noted that several other works can be used to see that, in the situation of the theorem, the exponent of the class group of M divides 2 (see [Sch07] or [Kan11], for example).

While it is an easy observation that an abelian surface A as in the theorem can be found for each quadratic imaginary field M with class group 1 or C_2 (see [FG18, Remark 2.20] and also Section 4), the question whether such an A exists for each of the fields M with class group $\mathrm{C}_2 \times \mathrm{C}_2$ is far from trivial. The aforementioned results are thus not sufficient for the determination of the set $\mathcal{A}$. The main contribution of this article is the following theorem.

Theorem 1.2. *Let M be a quadratic imaginary field with class group* $\mathrm{C}_2 \times \mathrm{C}_2$. *There exists an abelian surface defined over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}}$ is isogenous to the square of an elliptic curve $E/\overline{\mathbb{Q}}$ with CM by M if and only if the discriminant of M belongs to the set*

$$\{-84, -120, -132, -168, -228, -280, -372, -408, -435, -483, -520, -532, -595, -627, -708, -795, -1012, -1435\}. \tag{1.1}$$

The only imaginary quadratic fields with class group $\mathrm{C}_2 \times \mathrm{C}_2$ whose discriminant does not belong to (1.1) are

$$\mathbb{Q}(\sqrt{-195}),\ \mathbb{Q}(\sqrt{-312}),\ \mathbb{Q}(\sqrt{-340}),\ \mathbb{Q}(\sqrt{-555}),\ \mathbb{Q}(\sqrt{-715}),\ \mathbb{Q}(\sqrt{-760}). \tag{1.2}$$

With Theorem 1.2 at hand, the determination of the set $\mathcal{A}$ follows as a mere corollary (see §4 for the proof).

Corollary 1.3. *The set $\mathcal{A}$ of $\overline{\mathbb{Q}}$-endomorphism algebras of geometrically split abelian surfaces over $\mathbb{Q}$ is made of:*

i) $\mathbb{Q}\times\mathbb{Q}$, $\mathbb{Q}\times M$, $M_1\times M_2$, *where M, M_1 and M_2 are quadratic imaginary fields of class number* 1*;*

ii) $\mathrm{M}_2(\mathbb{Q})$, $\mathrm{M}_2(M)$, *where M is a quadratic imaginary field with class group* 1, C_2, *or* $\mathrm{C}_2\times\mathrm{C}_2$ *and distinct from those listed in* (1.2).

In particular, the set $\mathcal{A}$ has cardinality 92.

The paper is organized in the following manner. In Section 2 we attach a c-representation ϱ_V of degree 2 to an abelian surface A defined over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}}$ is isogenous to the square of an elliptic curve $E/\overline{\mathbb{Q}}$ with CM by M. It is well known that E is a $\mathbb{Q}$-curve and that one can associate a 2-cocycle c_E to E. A c-representation is essentially a representation up to scalar and it is thus a notion closely related to that of projective representation. In the case of the c-representation ϱ_V attached to A, the scalar that measures the failure of ϱ_V to be a proper representation is precisely the 2-cocycle c_E. Choosing the language of c-representations instead of that of projective representations has an unexpected payoff: the tensor product of a c-representation ϱ and its contragradient c-representation ϱ^* is again a proper representation. We show that $\varrho_V\otimes\varrho_V^*$ coincides with the representation of $G_{\mathbb{Q}}$ on the 4 dimensional M-vector space $\mathrm{End}(A_{\overline{\mathbb{Q}}})$. This representation has been studied in detail in [FS14] and the tensor decomposition of $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ is exploited in Theorems 2.20 and 2.27 to obtain obstructions on the existence of A. These obstructions extend to the general case those obtained in [FG18, §3.1,§3.2] under very restrictive hypotheses. The c-representation point of view also allows us to understand in a unified manner what we called *group theoretic* and *cohomological* obstructions in [FG18]. It should be noted that one can define analogues of ϱ_V in other more general situations. For example, a parallel construction in the context of geometrically isotypic abelian varieties potentially of GL_2-type has been exploited in [FG19] to determine a tensor factorization of their Tate modules. This can be used to deduce the validity of the Sato-Tate conjecture for them in certain cases.

In Section 3, we describe a method of Nakamura to compute the endomorphism algebra of the restriction of scalars of certain Gross $\mathbb{Q}$-curves (see Definition 2.9 below for the precise definition of these curves). Then we apply this method to all Gross $\mathbb{Q}$-curves with CM by a field M of class group $\mathrm{C}_2\times\mathrm{C}_2$. This computation plays a key role in the proof of Theorem 1.2, both in proving the existence of the abelian surfaces for the fields M different from those listed in (1.2), and in proving the non-existence for the fields of (1.2).

In Section 4 we culminate the proofs of Theorem 1.2 and Corollary 1.3 by assembling together the obstructions and existence results from Sections 2 and 3. We essentially show that we can use the results of Section 2 to reduce to the case of Gross $\mathbb{Q}$-curves, and then we deal with this case using the results of Section 3

Notations and terminology. For k a number field, we will work in the category of abelian varieties up to isogeny over k. Note that isogenies become invertible in this category. Given an abelian variety A defined over k, the set of endomorphisms $\mathrm{End}(A)$ of A defined over k is endowed with a $\mathbb{Q}$-algebra structure. More generally, if B is an abelian variety defined over k, we will denote by $\mathrm{Hom}(A,B)$ the $\mathbb{Q}$-vector space of homomorphisms from A to B that are defined over k. We note that for us $\mathrm{End}(A)$ and $\mathrm{Hom}(A,B)$ denote what some other authors call $\mathrm{End}^0(A)$ and $\mathrm{Hom}^0(A,B)$. We will write $A \sim B$ to mean that A and B are isogenous over k. If L/k is a field extension, then A_L will denote the base change of A from k to L. In particular, we will write $A_L \sim B_L$ if A and B become isogenous over L, and we will write $\mathrm{Hom}(A_L, B_L)$ to refer to what some authors write as $\mathrm{Hom}_L(A,B)$.

Acknowledgements. Fité is thankful to the organizers of the workshop "Arithmetic Aspects of Explicit Moduli Problems" held at BIRS (Banff) in May 2017, where he explained Theorem 1.1 and raised the question on the existence of an abelian surface over $\mathbb{Q}$ with $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathrm{M}_2(M)$ for an M with class group $\mathrm{C}_2 \times \mathrm{C}_2$. We thank Andrew Sutherland and John Voight for providing a positive answer to this question by pointing out the existence of an abelian surface (actually the Jacobian of a genus 2 curve) with the desired property for the field $M = \mathbb{Q}(\sqrt{-132})$. We also thank Noam Elkies for providing three additional genus 2 curves over $\mathbb{Q}$, these covering the fields $M = \mathbb{Q}(\sqrt{-408})$, $\mathbb{Q}(\sqrt{-435})$, and $\mathbb{Q}(\sqrt{-708})$. These four examples motivated the present paper.

Fité was funded by the Excellence Program María de Maeztu MDM-2014-0445. Fité was partially supported by MTM2015-63829-P. Guitart was funded by projects MTM2015-66716-P and MTM2015-63829-P. This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 682152).

2. c-representations and k-curves

The goal of this section is to obtain obstructions to the existence of abelian surfaces defined over $\mathbb{Q}$ such that $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathrm{M}_2(M)$, where M is a quadratic imaginary field. To this purpose, we analyze the interplay between the k-curves and c-representations that arise from them.

2.1. c-representations: general definitions.

Let V be a vector space of finite dimension over a field k and let G be a finite group. We say that a map

$$\varrho_V : G \to \mathrm{GL}(V)$$

is a c-representation (of the group G) if $\varrho_V(1) = 1$ and there exists a map

$$c_V : G \times G \to k^\times$$

such that for every $\sigma, \tau \in G$ one has

$$\varrho_V(\sigma)\varrho_V(\tau) = \varrho_V(\sigma\tau)c_V(\sigma,\tau)\,. \tag{2.1}$$

Remark 2.1. The following properties follow easily from the definition:

i) Note that we have

$$\varrho_V(\sigma^{-1}) = \varrho_V(\sigma)^{-1}c_V(\sigma^{-1},\sigma) \quad \text{and} \quad \varrho_V(\sigma^{-1}) = \varrho_V(\sigma)^{-1}c_V(\sigma,\sigma^{-1})\,.$$

In particular, $c_V(\sigma,\sigma^{-1}) = c_V(\sigma^{-1},\sigma)$.

ii) Note that if $c_V(\cdot,\cdot) = 1$, the notion of c-representation corresponds to the usual notion of representation.

Let V and W be c-representations of the group G. Let $T = \mathrm{Hom}(V, W)$ denote the space of k-linear maps from V to W. A homomorphism of c-representations from V to W is a k-linear map $f \in T$ such that

$$f(v) = \varrho_W(\sigma)(f(\varrho_V(\sigma)^{-1}v))$$

for every $v \in V$ and $\sigma \in G$.

Consider now the map

$$\varrho_T : G \to \mathrm{GL}(\mathrm{Hom}(V, W)),$$

defined by

$$(\varrho_T(\sigma)f)(v) = \varrho_W(\sigma)(f(\varrho_V(\sigma)^{-1}v)).$$

Proposition 2.2. *The map ϱ_T together with the map $c_T : G \times G \to k^\times$ defined by $c_T = c_V^{-1} \cdot c_W$ equip T with the structure of a c-representation.*

Before proving the proposition we show a particular case. In the case that W is k equipped with the trivial action of G, let us write $V^* = T$ and $\varrho^* = \varrho_T$. In this case, $\varrho^*(\sigma)$ is the inverse transpose of $\varrho_V(\sigma)$. The assertion of the proposition is then immediate from (2.1).

The following two lemmas, whose proof is straightforward, imply the proposition.

Lemma 2.3. *The maps*

$$\varrho_\otimes : G \to \mathrm{GL}(V \otimes W),$$

defined by $\varrho_\otimes(\sigma)(v \otimes w) = \varrho_V(\sigma)(v) \otimes \varrho_W(\sigma)(w)$ and $c_\otimes = c_V \cdot c_W$ endow $V \otimes W$ with a structure of c-representation.

Lemma 2.4. *The map*

$$\phi : W \otimes V^* \to T$$

defined by $\phi(w \otimes f)(v) = f(v)w$ is an isomorphism of c-representations.

Corollary 2.5. *When $V = W$, the c-representation T is in fact a representation.*

2.2. **k-curves: general definitions.** We briefly recall some definitions and results regarding $\mathbb{Q}$-curves and, more generally, k-curves with complex multiplication. More details can be found in [FG18, §2.1] and the references therein (especially [Que00], [Rib92], and [Nak04]).

Let $E/\overline{\mathbb{Q}}$ be an elliptic curve and let k be a number field, whose absolute Galois group we denote by G_k.

Definition 2.6. We say that E is a *k-curve* if for every $\sigma \in G_k$ there exists an isogeny $\mu_\sigma : {}^\sigma E \to E$.

Definition 2.7. We say that E is a *Ribet k-curve* if E is a k-curve and the isogenies μ_σ can be taken to be compatible with the endomorphisms of E, in the sense that the following diagram

$$\begin{array}{ccc} {}^\sigma E & \xrightarrow{\mu_\sigma} & E \\ \big\downarrow {}^\sigma\varphi & & \big\downarrow \varphi \\ {}^\sigma E & \xrightarrow{\mu_\sigma} & E \end{array} \tag{2.2}$$

commutes for all $\sigma \in G_k$ and all $\varphi \in \mathrm{End}(E)$.

Remark 2.8. i) Observe that if E does not have CM, then E is a k-curve if and only if it is a Ribet k-curve. If E has CM (say by a quadratic imaginary field M), it is well known that E is isogenous to all of its Galois conjugates and hence it is always a k-curve; it is a Ribet k-curve if and only if $M \subseteq k$ (cf. [Sil94, Theorem 2.2]).

ii) We warn the reader that in the present paper we are using a slightly different terminology from that of [FG18]: as in [FG18] the only relevant notion was that of a Ribet k-curve, we called Ribet k-curves simply k-curves.

Let K be a number field containing k. We say that an elliptic curve E/K is a k-curve *defined over* K (resp. a Ribet k-curve *defined over* K) if $E_{\overline{\mathbb{Q}}}$ is a k-curve (resp. a Ribet k-curve). We will say that E is *completely defined over* K if, in addition, all the isogenies $\mu_\sigma\colon {}^\sigma E \to E$ can be taken to be defined over K.

Definition 2.9. Let H denote the Hilbert class field of M and let E/H be an elliptic curve with CM by M. We say that E is a *Gross* $\mathbb{Q}$*-curve* if E is completely defined over H.

The next proposition characterizes the existence of Gross $\mathbb{Q}$-curves and Ribet M-curves with CM by M defined over the Hilbert class field H.

Proposition 2.10. *Let M be a quadratic imaginary field and let D denote its discriminant. Then:*

i) There exists a Ribet M-curve E^* with CM by M and completely defined over H.

ii) There exists a Gross $\mathbb{Q}$-curve E^* with CM by M (and completely defined over H) if and only if D is not of the form

$$D = -4p_1 \dots p_{t-1}\,, \tag{2.3}$$

where $t \geq 2$ and $p_1, \dots, p_{t-1}$ are primes congruent to 1 modulo 4.

The first part of the previous proposition is a weaker form of [Shi71, Proposition 5, p. 521] (see also [Nak01, Remark 1]). For the second part, we refer to [Gro80, §11] and [Nak04, Proposition 5]. Discriminants of the form (2.3) are called *exceptional*.

Suppose from now on that E is a k-curve defined over K with CM by an imaginary quadratic field M. Fix a system of isogenies $\{\mu_\sigma : {}^\sigma E \to E\}_{\sigma\in G_k}$. By enlarging K if necessary, we can always assume that K/k is Galois and that E is completely defined over K. We will equip $\mathrm{End}(E)$ with the following action. For $\sigma \in \mathrm{Gal}(K/k)$ and $\varphi \in \mathrm{End}(E)$ define

$$\sigma \star \varphi = \mu_\sigma \circ {}^\sigma\varphi \circ \mu_\sigma^{-1}\,.$$

Note that if E is a Ribet k-curve, then this action is trivial. If we regard M as a $\mathrm{Gal}(K/k)$-module by means of the natural Galois action (which is actually the trivial action when k contains M) and $\mathrm{End}(E)$ endowed with the action defined above, then the identification of $\mathrm{End}(E)$ with M becomes a $\mathrm{Gal}(K/k)$-equivariant isomorphism. The map

$$\begin{array}{rccc} c_E^K\colon & \mathrm{Gal}(K/k)\times\mathrm{Gal}(K/k) & \longrightarrow & M^\times \\ & (\sigma,\tau) & \longmapsto & \mu_{\sigma\tau}\circ {}^\sigma\mu_\tau^{-1}\circ\mu_\sigma^{-1} \end{array}$$

satisfies the condition

$$(\varrho \star c_E^K(\sigma,\tau)) \cdot c_E^K(\varrho\sigma,\tau)^{-1} \cdot c_E^K(\varrho,\sigma\tau) \cdot c_E^K(\varrho,\sigma)^{-1} = 1, \tag{2.4}$$

for $\varrho, \sigma, \tau \in \mathrm{Gal}(K/k)$, and is then a 2-cocycle[1]. Denote by γ_E^K the cohomology class in $H^2(\mathrm{Gal}(K/k), M^\times)$ corresponding to c_E^K. The class γ_E^K only depends on the K-isogeny class of E.

The next result is a consequence of Weil's descent criterion, extended to varieties up to isogeny by Ribet ([Rib92, §8]).

Theorem 2.11 (Ribet–Weil)**.** *Suppose that E is a Ribet k-curve completely defined over K (and hence $M \subseteq k$). Let L be a number field with $k \subseteq L \subseteq K$, and consider the restriction map*

$$\mathrm{res}\colon H^2(\mathrm{Gal}(K/k), M^\times) \longrightarrow H^2(\mathrm{Gal}(K/L), M^\times).$$

If $\mathrm{res}(\gamma_E^K) = 1$, there exists an elliptic curve C/L such that $E \sim C_K$.

2.3. **M-curves from squares of CM elliptic curves.** Let M be a quadratic imaginary field. Let A be an abelian surface defined over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}}$ is isogenous to E^2, where E is an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by M. Let $K/\mathbb{Q}$ denote the minimal extension over which

$$\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathrm{End}(A_K)\,.$$

By the theory of complex multiplication, K contains the Hilbert class field H of M. Note also that $K/\mathbb{Q}$ is Galois and the possibilities for $\mathrm{Gal}(K/\mathbb{Q})$ can be read from [FKRS12, Table 8]. For our purposes, it is enough to recall that

$$\mathrm{Gal}(K/M) \simeq \begin{cases} \mathrm{C}_r & \text{for } r \in \{1,2,3,4,6\}, \\ \mathrm{D}_r & \text{for } r \in \{2,3,4,6\}, \\ A_4, S_4\,. \end{cases} \tag{2.5}$$

Here, C_r denotes the cyclic group of r elements, D_r denotes the dihedral group of $2r$ elements, and A_4 (resp. S_4) stands for the alternating (resp. symmetric) group on 4 letters.

We can (and do) assume that E is in fact defined over K, and then we have that $A_K \sim E^2$. For $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have that $({}^\sigma E)^2 \sim {}^\sigma A_K = A_K \sim E^2$. Therefore, Poincaré's decomposition theorem implies that E is a $\mathbb{Q}$-curve completely defined over K.

For the purposes of this article, we need to consider the following (slightly more general) situation: Let N/M be a Galois subextension of K/M, and let E^* be a Ribet M-curve which is completely defined over N and such that $E_{\overline{\mathbb{Q}}} \sim E^*_{\overline{\mathbb{Q}}}$. Observe that there always exist N and E^* satisfying these conditions, for example by taking $N = K$ and $E^* = E$; but in §2.4 and §2.5 below we will exploit certain situations where $N \subsetneq K$ and $E^* \neq E$.

Then we can consider two cohomology classes: the class γ_E^K attached to E, and the class $\gamma_{E^*}^N$ attached to E^*. We recall the following key result about γ_E^K, which is a particular case of [FG18, Corollary 2.4].

Theorem 2.12. *The cohomology class γ_E^K is 2-torsion.*

Denote by U the set of roots of unity of M and put $P = M^\times/U$. The same argument of [FG18, Proof of Theorem 2.14] proves the following decomposition of

[1] Actually, this is the inverse of the cocycle considered in [FG18], but this does not affect any of the results that we will use.

the 2-torsion of $H^2(\mathrm{Gal}(K/M), M^\times)$:

$$H^2(\mathrm{Gal}(K/M), M^\times)[2] \simeq H^2(\mathrm{Gal}(K/M), U)[2] \times \mathrm{Hom}(\mathrm{Gal}(K/M), P/P^2)\,. \tag{2.6}$$

If $M \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ this particularizes to

$$H^2(\mathrm{Gal}(K/M), M^\times)[2] \simeq H^2(\mathrm{Gal}(K/M), \{\pm 1\}) \times \mathrm{Hom}(\mathrm{Gal}(K/M), P/P^2). \tag{2.7}$$

For $\gamma \in H^2(\mathrm{Gal}(K/M), M^\times)[2]$ we will denote by $(\gamma_\pm, \bar\gamma)$ its components under the isomorphism (2.7); we will refer to $\gamma_\pm$ as the sign component and to $\bar\gamma$ as the degree component.

In order to study the relation between γ_E^K and $\gamma_{E^*}^N$, define L/K to be the smallest extension such that E_L^* and E_L are isogenous. Since all the endomorphisms of E are defined over K, this is also the smallest extension L/K such that $\mathrm{Hom}(E_L^*, E_L) = \mathrm{Hom}(E_{\overline{\mathbb{Q}}}^*, E_{\overline{\mathbb{Q}}})$. The extension $L/\mathbb{Q}$ is Galois. Indeed, for $\sigma \in G_\mathbb{Q}$ put $L' = {}^\sigma L$ and let $\beta_\sigma \colon {}^\sigma E^* \to E^*$ and $\mu_\sigma \colon {}^\sigma E \to E$ be isogenies defined over N and over K respectively; then, if $\phi \colon E_L^* \to E_L$ is an isogeny defined over L we find that $\mu_\sigma \circ {}^\sigma\phi \circ \beta_\sigma^{-1}$ is an isogeny defined over L' between $E_{L'}^*$ and $E_{L'}$, so that $L \subseteq L'$ and therefore $L = L'$.

One can also characterize L/K as the minimal extension such that

$$\mathrm{Hom}(E_{\overline{\mathbb{Q}}}^*, A_{\overline{\mathbb{Q}}}) \simeq \mathrm{Hom}(E_L^*, A_L)\,.$$

Denote by

$$\mathrm{inf}_N^K : H^2(\mathrm{Gal}(N/M), M^\times) \longrightarrow H^2(\mathrm{Gal}(K/M), M^\times)$$

the inflation map in Galois cohomology.

Lemma 2.13. *Suppose that* $M \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. *Then*

$$\mathrm{inf}_N^K(\gamma_{E^*}^N) = w \cdot \gamma_E^K\,,$$

for some $w \in H^2(\mathrm{Gal}(K/M), \{\pm 1\})$.

Proof. Since $E_L \sim (E_*)_L$ we have that

$$\mathrm{inf}_N^L(\gamma_{E^*}^N) = \mathrm{inf}_K^L(\gamma_E^K). \tag{2.8}$$

Now consider the following piece of the inflation–restriction exact sequence

$$H^1(\mathrm{Gal}(L/K), M^\times) \xrightarrow{t} H^2(\mathrm{Gal}(K/M), M^\times) \xrightarrow{\mathrm{inf}_K^L} H^2(\mathrm{Gal}(L/M), M^\times). \tag{2.9}$$

Equality (2.8) implies that $\mathrm{inf}_N^K(\gamma_{E^*}^N)$ and γ_E^K have the same image under the inflation map inf_K^L, and therefore

$$\mathrm{inf}_N^K(\gamma_{E^*}^N) = t(v) \cdot \gamma_E^K$$

for some $v \in H^1(\mathrm{Gal}(L/K), M^\times)$. If $M \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ we have that

$$H^1(\mathrm{Gal}(L/K), M^\times) \simeq \mathrm{Hom}(\mathrm{Gal}(L/K), \{\pm 1\})$$

and therefore $t(v)$ belongs to $H^2(\mathrm{Gal}(K/M), \{\pm 1\})$. □

Observe that from Theorem 2.12 one cannot deduce that the class $\gamma_{E^*}^N$ is 2-torsion, since A_N is not isogenous to $(E^*)^2$ in general. By Lemma 2.13, what we do deduce is that $\inf_N^K(\gamma_{E^*}^N)^2 = 1$. Therefore, once again by the inflation–restriction exact sequence

$$H^1(\mathrm{Gal}(K/N), M^\times) \xrightarrow{t} H^2(\mathrm{Gal}(N/M), M^\times) \xrightarrow{\inf_N^K} H^2(\mathrm{Gal}(K/M), M^\times) \tag{2.10}$$

we have that

$$(\gamma_{E^*}^N)^2 = t(\mu) \text{ for some } \mu \in H^1(\mathrm{Gal}(K/N), M^\times). \tag{2.11}$$

The following technical lemma will be used in §2.5 below.

Lemma 2.14. *Suppose that N/M is abelian and that $M \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$. Let $c_{E^*}^N$ be a cocycle representing the class $\gamma_{E^*}^N$. Then $c_{E^*}^N(\sigma,\tau) = \pm c_{E^*}^N(\tau,\sigma)$ for all $\sigma,\tau \in \mathrm{Gal}(N/M)$.*

Proof. Since $M \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ we have that

$$H^1(\mathrm{Gal}(K/N), M^\times) = \mathrm{Hom}(\mathrm{Gal}(K/N), \{\pm 1\}). \tag{2.12}$$

By (2.11) and (2.12) we can suppose that there exists a map $d : \mathrm{Gal}(N/M) \to M^\times$ such that

$$c_{E^*}^N(\sigma,\tau)^2 = d(\sigma)d(\tau)d(\sigma\tau)^{-1} \cdot t(\mu)(\sigma,\tau),$$

where $t(\mu)(\sigma,\tau) \in \{\pm 1\}$. Therefore

$$c_{E^*}^N(\sigma,\tau)^2 = \pm d(\sigma)d(\tau)d(\sigma\tau)^{-1} = \pm d(\sigma)d(\tau)d(\tau\sigma)^{-1} = \pm c_{E^*}^N(\tau,\sigma)^2.$$

We see that $\frac{c_{E^*}^N(\sigma,\tau)}{c_{E^*}^N(\tau,\sigma)}$ is a root of unity in M, hence ± 1. □

2.4. ***c*-representations from squares of CM elliptic curves.** Keep the notations from Section 2.3. We will denote by V the M-module $\mathrm{Hom}(E_L^*, A_L)$. Fix a system of isogenies $\{\mu_\sigma : {}^\sigma E^* \to E^*\}_{\sigma \in \mathrm{Gal}(L/M)}$. We do not have a natural action of $\mathrm{Gal}(L/M)$ on V, but the next lemma says that we can use the chosen system of isogenies to define a *c*-action on V.

Lemma 2.15. *The map*

$$\varrho_V : \mathrm{Gal}(L/M) \to \mathrm{GL}(V)$$

defined by

$$\varrho_V(f) = {}^\sigma f \circ \mu_\sigma^{-1} \qquad \text{for } \sigma \in \mathrm{Gal}(L/M),\ f \in V$$

and the 2-cocycle $c_{E^*}^L$ endow the module V with a structure of a c-representation.

Proof. This is tautological:

$$\varrho_V(\sigma)\varrho_V(\tau)(f) = {}^{\sigma\tau} f \circ {}^\sigma\mu_\tau^{-1} \circ \mu_\sigma^{-1} = {}^{\sigma\tau} f \circ \mu_{\sigma\tau}^{-1} \cdot c_{E^*}^L(\sigma,\tau) = \varrho_V(\sigma\tau)(f) c_{E^*}^L(\sigma,\tau)\,.$$

□

Let now R denote the M-module $\mathrm{End}(A_K)$. It is equipped with the natural Galois conjugation action of $\mathrm{Gal}(L/M)$, which factors through $\mathrm{Gal}(K/M)$ and which we sometimes will write as $\varrho_R(\sigma)(\psi) = {}^\sigma\psi$. Let T denote $\mathrm{Hom}(V,V)$, equipped with the *c*-representation structure given by Lemma 2.15 and Proposition 2.2. Note that by Corollary 2.5, we know that T is actually a $M[\mathrm{Gal}(L/M)]$-module.

Lemma 2.16. *The map*

$$\Phi : R \to T \simeq V \otimes V^* \qquad \Phi(\psi)(f) = \psi \circ f, \text{for } f \in V, \psi \in \mathrm{End}(A_K)$$

is an isomorphism of c-representations (and thus of $M[\mathrm{Gal}(L/M)]$-modules).

Proof. The fact that Φ is a morphism of c-representations is straightforward:

$$\begin{aligned}\varrho_T(\sigma)(\Phi({}^{\sigma^{-1}}\psi))(f) &= \varrho_V(\sigma)(\Phi({}^{\sigma^{-1}}\psi)(\varrho_V(\sigma)^{-1}(f)))\,,\\ &= \varrho_V(\sigma)({}^{\sigma^{-1}}\psi\circ\varrho_V(\sigma^{-1})(f)c^L_{E^*}(\sigma^{-1},\sigma)^{-1})\,,\\ &= \psi\circ f\circ{}^{\sigma}\mu^{-1}_{\sigma^{-1}}\mu^{-1}_{\sigma}c^L_{E^*}(\sigma^{-1},\sigma)^{-1}\,,\\ &= \Phi(\psi)(f)\,,\end{aligned}$$

where we have used Remark 2.1 in the second and last equalities. The lemma follows by noting that Φ is clearly injective and that both R and T have dimension 4 over M. □

We now describe the $M[\mathrm{Gal}(K/M)]$-module structure of R. It follows from (2.5) that the order r of an element $\sigma\in\mathrm{Gal}(K/M)$ is 1, 2, 3, 4, or 6.

Lemma 2.17. $\mathrm{Tr}\,\varrho_R(\sigma)=2+\zeta_r+\overline{\zeta}_r$*, where* ζ_r *is a primitive* r*-th root of unity.*

Remark 2.18. Note that this lemma is proven in [FS14, Proposition 3.4] under the strong running hypothesis of that paper: in our setting that hypothesis would say that there exists E^* defined over M such that $A_{\overline{\mathbb{Q}}}\sim E^{*2}_{\overline{\mathbb{Q}}}$ (i.e., that N can be taken to be M, in the notation of the previous section).

Proof. We claim that $\mathrm{Tr}(\varrho_R)\in M$ is in fact rational. Let us postpone the proof of this claim until the end of the proof of the lemma. Assuming it, we have that

$$\mathrm{Tr}_{M/\mathbb{Q}}(\mathrm{Tr}(\varrho_R(\sigma)))=2\,\mathrm{Tr}(\varrho_R)(\sigma)\,. \tag{2.13}$$

But if $\varrho_{R_\mathbb{Q}}$ is the representation afforded by R regarded as an 8 dimensional module over $\mathbb{Q}$, we have

$$\mathrm{Tr}_{M/\mathbb{Q}}(\mathrm{Tr}(\varrho_R(\sigma)))=\mathrm{Tr}(\varrho_{R_\mathbb{Q}})(\sigma)=2(2+\zeta_r+\overline{\zeta}_r), \tag{2.14}$$

where the last equality is [FKRS12, Proposition 4.9]. The comparison of (2.13) and (2.14) concludes the proof of the lemma.

We turn now to prove the rationality of $\mathrm{Tr}\,\varrho_R$. We first recall the aforementioned proof (that of [FS14, Proposition 3.4]) which uses the fact that we can choose E^* to be defined over M. In this case, we have that V is an $M[\mathrm{Gal}(L/M)]$-module, that $\mathrm{Tr}(\varrho_{V^*})$ is a sum of roots of unity so that $\mathrm{Tr}(\varrho_{V^*})=\overline{\mathrm{Tr}(\varrho_V)}$, and hence that $\mathrm{Tr}(\varrho_R)=\mathrm{Tr}(\varrho_V)\cdot\overline{\mathrm{Tr}\,\varrho_V}$ belongs to $\mathbb{Q}$.

For the general case, assume that $\mathrm{Tr}\,\varrho_R$ does not belong to $\mathbb{Q}$. Since it is a sum of roots of unity of orders diving either 4 or 6, then M would be $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$, but then we could take a model of E^* defined over M, and by the above paragraph, the trace $\mathrm{Tr}\,\varrho_R$ would be rational, which is a contradiction. □

2.5. **Obstructions.** Keep the notations from Section 2.4 and Section 2.3. Let S denote the normal subgroup of $\mathrm{Gal}(K/M)$ generated by the square elements. In this section, we make the following hypotheses.

Hypothesis 2.19. *i) There exists a Ribet* M*-curve* E^* *with CM by* M *completely defined over* N*, where* N/M *is the subextension of* K/M *fixed by* S*.*
ii) $M\neq\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$.

Let $\sigma\in\mathrm{Gal}(K/M)$ be an element of order $r\in\{4,6\}$. Let

$$\bar{\cdot}:\mathrm{Gal}(K/M)\to\mathrm{Gal}(N/M)\simeq\mathrm{Gal}(K/M)/S \tag{2.15}$$

denote the natural projection map. Note that $\mathrm{Gal}(N/M)$ is a group of exponent dividing 2.

Theorem 2.20. *Under Hypothesis 2.19, we have:*

i) If $r = 4$, then $2c^N_{E^*}(\bar\sigma, \bar\sigma)$ belongs to $\pm(M^\times)^2$.
ii) If $r = 6$, then $3c^N_{E^*}(\bar\sigma, \bar\sigma)$ belongs to $\pm(M^\times)^2$.

Proof. First of all, note that E^* is completely defined over N. Thus we can, and do, assume that $c^L_{E^*}$ is the inflation of $c^N_{E^*}$. Let $s \in \mathrm{Gal}(L/M)$ be a lift of σ. By part ii) of Hypothesis 2.19, we have that $[L : K] \leq 2$. Therefore, the order of s divides $2r$. We then have

$$\varrho_V(s)^{2r} = \varrho_V(s^2)^r c^N_{E^*}(\bar\sigma, \bar\sigma)^r = \varrho_V(s^{2r}) c^N_{E^*}(\bar\sigma, \bar\sigma)^r = c^N_{E^*}(\bar\sigma, \bar\sigma)^r\,, \tag{2.16}$$

where we have used that $c^N_{E^*}(\bar\sigma^{2e}, \bar\sigma^{2e'}) = 1$ for any pair of integers e, e'. Let α and β be the eigenvalues of $\varrho_V(s)$. By (2.16), we have that $\alpha^{2r} = c^N_{E^*}(\bar\sigma, \bar\sigma)^r$, from which we deduce that $\omega_r\alpha^2 = c^N_{E^*}(\bar\sigma, \bar\sigma) \in M^\times$, where ω_r is a (not necessarily primitive) r-th root of unity.

Since the eigenvalues of $\varrho_{V^*}(s)$ are $1/\alpha$ and $1/\beta$, by Lemmas 2.17 and 2.16 we have that

$$2 + \zeta_r + \overline{\zeta}_r = (\alpha + \beta)\left(\frac{1}{\alpha} + \frac{1}{\beta}\right); \text{ equivalently, } \alpha^2 + \beta^2 = (\zeta_r + \overline{\zeta}_r)\alpha\beta\,. \tag{2.17}$$

This means that α/β satisfies the r-th cyclotomic polynomial and thus, by reordering α and β if necessary, we have that $\alpha = \beta\zeta_r$.

Combining this with (2.17), we get

$$(2 + \zeta_r + \overline{\zeta}_r)c^N_{E^*}(\bar\sigma, \bar\sigma) = (2 + \zeta_r + \overline{\zeta}_r)\omega_r\alpha^2 = (2 + \zeta_r + \overline{\zeta}_r)\alpha\beta\omega_r\zeta_r = (\alpha + \beta)^2\omega_r\zeta_r\,.$$

Since the left-hand side is in $M^\times$, the fact that $\alpha+\beta \in M^\times$ tells us that $\omega_r\zeta_r \in M^\times$. If $\omega_r\zeta_r$ is not rational, then $M = \mathbb{Q}(\zeta_r)$, which contradicts part ii) of Hypothesis 2.19. If $\omega_r\zeta_r \in \mathbb{Q}$, since it is a root of unity, it must be ±1 and thus we get

$$\pm(2 + \zeta_r + \overline{\zeta}_r)c^N_{E^*}(\bar\sigma, \bar\sigma) = (\alpha + \beta)^2\,.$$

Therefore, $(2 + \zeta_r + \overline{\zeta}_r)c^N_{E^*}(\bar\sigma, \bar\sigma)$ belongs to $\pm(M^\times)^2$. □

Remark 2.21. Note that it follows from the above proof that if $r = 4$, then any lift $s \in \mathrm{Gal}(L/M)$ of σ has order $2r = 8$. Indeed, if the order of s was r, then arguing as in (2.16), we would obtain $\varrho_V(s)^r = c^N_{E^*}(\bar\sigma, \bar\sigma)^{r/2}$, from which we would infer $\omega_{r/2}\alpha^2 = c^N_{E^*}(\bar\sigma, \bar\sigma)$, for some (not necessarily primitive) $r/2$-th root of unity. We could then run the same argument as above, but since $\omega_{r/2}\zeta_r$ is never rational, we would deduce now that $M = \mathbb{Q}(i)$. Note that if $r = 6$ it can certainly happen that $\omega_{r/2}\zeta_r \in \mathbb{Q}$.

Until the end of this section, we make the following additional assumption on M.

Hypothesis 2.22. *i)* $\mathrm{Gal}(K/M) \simeq \mathrm{D}_4$ *or* D_6.
ii) $M \neq \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-3})$.

Hypothesis i) implies that N/M is a biquadratic extension. By part i) of Proposition 2.10, there exists a Ribet M-curve E^* with CM by M completely defined over the Hilbert class field H of M. Using [FG18, Theorem 2.14], it is immediate to see that $H \subseteq N$, so that Hypothesis 2.22 implies Hypothesis 2.19.

The next two propositions describe the structure of the group $\mathrm{Gal}(L/M)$.

Proposition 2.23. *If* $\mathrm{Gal}(K/M) \simeq \mathrm{D}_4$*, then* $\mathrm{Gal}(L/M)$ *is isomorphic to either the dihedral group* D_8*; the generalized dihedral group* QD_8 *of order* 16*; or the generalized quaternion group* Q_{16}[2].

Proof. If $\mathrm{Gal}(K/M) \simeq \mathrm{D}_4$, then by Remark 2.21 we have that any element of $\mathrm{Gal}(L/M)$ projecting onto an element of $\mathrm{Gal}(K/M)$ of order 4 must have order 8. The groups of order 16 with a quotient isomorphic to D_4 satisfying the previous property are those in the statement of the proposition. □

Proposition 2.24. *If* $\mathrm{Gal}(K/M) \simeq \mathrm{D}_6$*, there exists a Ribet* M*-curve* E^* *completely defined over* N *with CM by* M *such that* $E \sim E^*_K$ *and hence* $L = K$ *and* $\mathrm{Gal}(L/M) \simeq \mathrm{D}_6$.

Proof. Recall the cohomology class $\gamma_E^K \in H^2(\mathrm{Gal}(K/M), M^\times)[2]$ attached to E and consider the restriction map

$$\mathrm{res} : H^2(\mathrm{Gal}(K/M), M^\times) \to H^2(\mathrm{Gal}(K/N), M^\times)\,.$$

We will first see that $\gamma = \mathrm{res}\gamma_E^K$ is trivial. Recall the decomposition (2.7) of the 2-torsion cohomology classes into degree and sign components

$$H^2(\mathrm{Gal}(K/N), M^\times)[2] \simeq H^2(\mathrm{Gal}(K/N), \{\pm 1\}) \times \mathrm{Hom}(\mathrm{Gal}(K/N), P/P^2),$$

and the notation $\gamma_\pm$ (resp. $\bar\gamma$) for the sign component (resp. degree component) of γ. Since $\mathrm{Gal}(K/N) \simeq \mathrm{C}_3$ is the subgroup of $\mathrm{Gal}(K/M)$ generated by the squares, we have that $\bar\gamma$ is trivial. Since

$$H^2(\mathrm{Gal}(K/N), \{\pm 1\}) \simeq H^2(\mathrm{C}_3, \{\pm 1\}) = 0\,,$$

we see that $\gamma_\pm$ is also trivial. By Theorem 2.11, there exists an elliptic curve E^* defined over N such that $E^*_K \sim E$. To see that E^* is completely defined over N, on the one hand, note that since $M \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$, then E^* and any Galois conjugate ${}^\sigma E^*$ of it are isogenous over a quadratic extension of N. On the other hand, since $E^*_K \sim E$ and E is completely defined over K, we have that the smallest field of definition of $\mathrm{Hom}(E^*_{\overline{\mathbb{Q}}}, {}^\sigma E^*_{\overline{\mathbb{Q}}})$ is contained in K. Since K/N is a cubic extension, we deduce that E^* and ${}^\sigma E^*$ are in fact isogenous over N. □

Corollary 2.25. *If* $\mathrm{Gal}(K/M) \simeq \mathrm{D}_r$ *for* $r = 4$ *or* 6*, there exists a Ribet* M*-curve* E^* *with CM by* M *completely defined over* N *for which* $\mathrm{Gal}(L/M)$ *contains*

i) an element s *of order* 8 *if* $r = 4$ *and of order* 6 *if* $r = 6$*;*
ii) an element t *such that* $tst^{-1} = t^a$ *for* $1 \leq a \leq 2r$ *such that* $a \equiv -1 \pmod r$.

Proof. This is obvious when $\mathrm{Gal}(L/M)$ is dihedral. For the other options allowed by Proposition 2.23, recall that

$$\mathrm{QD}_8 \simeq \langle s, t \,|\, s^8, t^2, tsts^5 \rangle\,, \qquad \mathrm{Q}_{16} \simeq \langle s, t \,|\, s^8, t^2s^4, tst^{-1}s \rangle\,.$$

□

Remark 2.26. It is clear from the proof of Proposition 2.24 that, in the case that $N = H$ and H is not exceptional, we can choose E^* in the above corollary to be a Gross $\mathbb{Q}$-curve.

[2]The gap identification numbers of QD_8 and Q_{16} are $\langle 16, 8\rangle$ and $\langle 16, 9\rangle$, respectively.

Until the end of this section, we will assume that E^* is as in the previous corollary. Let s and t be also as in the corollary, and let σ and τ be the images of s and t under the projection map

$$\operatorname{Gal}(L/M) \to \operatorname{Gal}(K/M)\,.$$

Recall also the projection map $\bar{\cdot} : \operatorname{Gal}(K/M) \to \operatorname{Gal}(N/M)$ and note that $\bar\sigma$ and $\bar\tau$ are non-trivial elements of $\operatorname{Gal}(N/M)$.

Theorem 2.27. *Under Hypothesis 2.22, we have $c^N_{E^*}(\bar\tau,\bar\tau) = \pm 1$.*

Proof. By Lemma 2.14, we have that $c^N_{E^*}(g,g') = \pm c^N_{E^*}(g',g)$ for every $g,g' \in \operatorname{Gal}(N/M)$. Moreover, the 2-cocycle condition (2.4) asserts that

$$c^N_{E^*}(\bar\tau,\bar\tau) = c^N_{E^*}(\bar\tau,\bar\tau)c^N_{E^*}(\bar\sigma,1) = c^N_{E^*}(\bar\sigma\bar\tau,\bar\tau)c^N_{E^*}(\bar\sigma,\bar\tau)\,.$$

Then, we have

$$\begin{aligned} \varrho_V(t)\varrho_V(s)\varrho_V(t)^{-1} &= \varrho_V(t)\varrho_V(s)\varrho_V(t^{-1})c^N_{E^*}(\bar\tau,\bar\tau) = \\ &= \varrho_V(ts)\varrho_V(t^{-1})c^N_{E^*}(\bar\tau,\bar\sigma)c^N_{E^*}(\bar\tau,\bar\tau) = \\ &= \varrho_V(tst^{-1})c^N_{E^*}(\bar\tau\bar\sigma,\bar\tau)c^N_{E^*}(\bar\tau,\bar\sigma)c^N_{E^*}(\bar\tau,\bar\tau) = \\ &= \pm\varrho_V(s^a)c^N_{E^*}(\bar\tau,\bar\tau)^2\,. \end{aligned} \tag{2.18}$$

It is easy to observe that

$$\varrho_V(s)^a = \varrho_V(s^a)c^N_{E^*}(\bar\sigma,\bar\sigma)^{(a-1)/2}\,. \tag{2.19}$$

Letting α and β be the eigenvalues of $\varrho_V(s)$, taking traces of (2.18), and applying (2.19), we obtain

$$(\alpha+\beta) = \pm\left(\alpha^a+\beta^a\right)c^N_{E^*}(\bar\sigma,\bar\sigma)^{-(a-1)/2}c^N_{E^*}(\bar\tau,\bar\tau)^2$$

But as in the proof of Theorem 2.20, we have $\beta = \zeta_r\alpha$ and $c^N_{E^*}(\bar\sigma,\bar\sigma) = \omega_r\alpha^2$, where ζ_r and ω_r are r-th roots of unity and ζ_r is primitive. This, together with the fact that $a \equiv -1 \pmod r$, permits to write the above equation as

$$\pm\frac{1+\zeta_r}{\omega_r^{-(a-1)/2}(1+\overline{\zeta}_r)} = c^N_{E^*}(\bar\tau,\bar\tau)^2 \in (M^\times)^2.$$

One easily verifies that $(1+\zeta_r)/(1+\overline{\zeta}_r)$ is an r-th root of unity. Therefore, the left-hand side of the above equation is a root of unity in $M^\times$, and hence it must be ± 1. □

3. Restriction of scalars of Gross $\mathbb{Q}$-curves

For the convenience of the reader, in this section we review some results of Nakamura [Nak04] on Gross $\mathbb{Q}$-curves, to which we refer for more details and proofs.

Let M be an imaginary quadratic field. Throughout this section, we make the following hypothesis.

Hypothesis 3.1. *i) M is non-exceptional.*
ii) M has class group isomorphic to $\mathrm{C}_2\times\mathrm{C}_2$.

Remark 3.2. If M has class group isomorphic to $\mathrm{C}_2\times\mathrm{C}_2$, then the discriminant D of M belongs to the set

$$\{-84,-120,-132,-168,-195,-228,-280,-312,-340,-372,-408,-435,-483,\\ -520,-532,-555,-595,-627,-708,-715,-760,-795,-1012,-1435\}.$$

This list can be easily obtained from [Wat04], for example. Among them, only -340 is exceptional.

Then, by Proposition 2.10, there exists a Gross $\mathbb{Q}$-curve E with CM by M, which is thus completely defined over the Hilbert class field H of M. The aim of the present section is to describe Nakamura's method for computing the endomorphism algebra of the restriction of scalars of a Gross $\mathbb{Q}$-curve, which we will then apply to all Gross $\mathbb{Q}$-curves attached to M satisfying Hypothesis 3.1. Our account of Nakamura's method will be only in the particular case where M has class group $\mathrm{C}_2 \times \mathrm{C}_2$, which is the case of interest to us.

As seen in Section 2.2, one can associate to E a cohomology class $\gamma_E := \gamma_E^H$ in the group $H^2(\mathrm{Gal}(H/\mathbb{Q}), M^\times)$. The set of cohomology classes arising from Gross $\mathbb{Q}$-curves over H has cardinality 8 (cf. [Nak04, Proposition 4]), and we regard the set of Gross $\mathbb{Q}$-curves over H as partitioned into 8 equivalence classes according to their cohomology class.

Let $\mathrm{Res}_{H/M}(E)$ denote Weil's restriction of scalars of E. This variety is a priori defined over M, but it can be defined over $\mathbb{Q}$, in the sense that $\mathrm{Res}_{H/M}(E) \simeq (B_E)_M$ for some variety $B_E/\mathbb{Q}$. It turns out that the endomorphism algebra $\mathcal{D}_E = \mathrm{End}(B_E)$ only depends on the cohomology class γ_E [Nak04, Proposition 6]. Nakamura devised a method for computing $\mathcal{D}_E$ in terms of the Hecke character attached to E, which he applied to compute all the endomorphism algebras arising in this way from Gross $\mathbb{Q}$-curves in the cases where $D = -84$ and $D = -195$. We extend his computation to the remaining 21 non-exceptional discriminants of Remark 3.2.

3.1. **Hecke characters of Gross $\mathbb{Q}$-curves.** The first step is to compute a set of Hecke characters whose associated elliptic curves represent all the equivalence classes of Gross $\mathbb{Q}$-curves.

Local characters. We begin by defining certain local characters that will be used to describe the Hecke characters. Let $\mathbb{I}_M$ be the group of ideles of M. If $\mathfrak{p}$ is a prime of M, we denote by $U_\mathfrak{p} = \mathcal{O}_{M,\mathfrak{p}}^\times$ the group of local units. Also, for a rational prime p put $U_p = \prod_{\mathfrak{p}|p} U_\mathfrak{p}$.

Suppose that p is odd and inert in M. Then define η_p as the unique character $\eta_p \colon U_p \to \{\pm 1\}$ such that $\eta_p(-1) = (-1)^{\frac{p-1}{2}}$.

Suppose now that 2 is ramified in M and write $D = 4m$. If m is odd, then

$$U_2/U_2^2 \simeq (\mathbb{Z}/2\mathbb{Z})^3 \simeq \langle \sqrt{m}, 3 - 2\sqrt{m}, 5 \rangle.$$

Define $\eta_{-4} \colon U_2 \to \{\pm 1\}$ to be the character with kernel $\langle 3 - 2\sqrt{m}, 5\rangle$. If m is even then

$$U_2/U_2^2 \simeq (\mathbb{Z}/2\mathbb{Z})^3 \simeq \langle 1 + \sqrt{m}, -1, 5 \rangle.$$

Define η_8 to be the character with kernel $\langle 1 + \sqrt{m}, -1\rangle$ and η_{-8} the character with kernel $\langle 1 + \sqrt{m}, -5\rangle$.

Hecke characters. Let $U_M = \prod_\mathfrak{p} U_\mathfrak{p}$ be the maximal compact subgroup of $\mathbb{I}_M$. Let S be a finite set of primes of M and put $U_S = \prod_{\mathfrak{p}\in S} U_\mathfrak{p}$. Suppose that $\eta \colon U_S \to \{\pm 1\}$ is a continuous homomorphism such that $\eta(-1) = -1$. Next, we explain how to construct from η a Hecke character $\phi : \mathbb{I}_M \to \mathbb{C}^\times$ (not uniquely determined) that gives rise, in certain cases, to a Gross $\mathbb{Q}$-curve.

First of all, extend η to a character that we denote by the same name $\eta\colon U_M \to \{\pm 1\}$ by composing with the projection $U_M \to U_S$. Now this character η can be extended to a character $\tilde{\eta}\colon U_M M^\times M_\infty^\times \longrightarrow \mathbb{C}^\times$ by imposing that

$$\tilde{\eta}(M^\times) = 1, \quad \tilde{\eta}(z) = z^{-1} \text{ for } z \in M_\infty^\times. \tag{3.1}$$

Let $\phi\colon \mathbb{I}_M \to \mathbb{C}^\times$ be a Hecke character that extends $\tilde{\eta}$ (there are $[H : M] = 4$ such extensions, cf. [Shi71, p. 523]). For future reference, it will be useful to have the following formula for ϕ evaluated at certain principal ideals.

Lemma 3.3. *Suppose that (α) is a principal ideal of M such that $v_{\mathfrak{p}}(\alpha) = 0$ for all $\mathfrak{p} \in S$, and denote by $\alpha_S \in U_S$ the natural image of α in U_S. Then*

$$\phi((\alpha)) = \eta(\alpha_S)\alpha_\infty, \tag{3.2}$$

where α_∞ denotes the image of α in $M_\infty = \mathbb{C}$.

Proof. If we write $(\alpha) = \prod_{\mathfrak{q}\in T} \mathfrak{q}^{v_{\mathfrak{q}}(\alpha)}$, where T denotes the support of (α), then

$$\phi((\alpha)) = \prod_{\mathfrak{q}\in T} \phi_{\mathfrak{q}}(\alpha_{\mathfrak{q}}),$$

where $\phi_{\mathfrak{q}}$ denotes the restriction of ϕ to $M_{\mathfrak{q}}$ and $\alpha_{\mathfrak{q}}$ the image of α in $M_{\mathfrak{q}}$. Observe that by hypothesis $S \cap T = \emptyset$, and that if $\mathfrak{q} \notin S \cup T$, then $\phi_{\mathfrak{q}}(\alpha_{\mathfrak{q}}) = 1$, since $\alpha_{\mathfrak{q}}$ belongs to $U_{\mathfrak{q}}$ and $\phi_{|U_{\mathfrak{q}}} = \tilde{\eta}_{|U_{\mathfrak{q}}} = 1$. Therefore, we can write

$$\phi((\alpha)) = \prod_{\mathfrak{q}\in T} \phi_{\mathfrak{q}}(\alpha_{\mathfrak{q}}) \prod_{\mathfrak{q}\notin T} \phi_{\mathfrak{q}}(\alpha_{\mathfrak{q}}) \prod_{\mathfrak{q}\in S} \phi_{\mathfrak{q}}^{-1}(\alpha_{\mathfrak{q}}) = \left(\prod_{\mathfrak{q}} \phi_{\mathfrak{q}}(\alpha_{\mathfrak{q}})\right) \eta(\alpha_S),$$

where we have used that η has order 2. Then, by (3.1) we have that

$$\phi((\alpha)) = \left(\phi_\infty(\alpha_\infty) \prod_{\mathfrak{q}} \phi_{\mathfrak{q}}(\alpha_{\mathfrak{q}})\right) \phi_\infty(\alpha_\infty)^{-1}\eta(\alpha_S) = \phi(\alpha)\alpha_\infty\eta(\alpha_S) = \alpha_\infty\eta(\alpha_S).$$

□

Define now a Hecke character of H by means of $\psi = \phi \circ \mathrm{N}_{H/M}$, where

$$\mathrm{N}_{H/M}\colon \mathbb{I}_H \to \mathbb{I}_M$$

denotes the norm on ideles. By a result of Shimura [Shi71, Proposition 9], the Hecke character ψ is attached to a Gross $\mathbb{Q}$-curve if and only if $\bar{\phi} = \phi$, where the bar denotes the action of complex conjugation.

For example, if D has some prime factor $q \equiv 3 \pmod 4$, put $\eta_0 = \eta_q$. If all the odd primes dividing D are congruent to 1 modulo 4, then $D = 8m$ for some odd m and we define η_0 to be η_{-8}. If we denote by $\phi_0\colon \mathbb{I}_M \to \mathbb{C}^\times$ a Hecke character attached to η_0 by the above construction, then the Hecke character $\psi_0 = \phi_0 \circ \mathrm{N}_{H/M}$ is the Hecke character attached to a Gross $\mathbb{Q}$-curve over H.

Let W be the set of characters $\theta\colon U_M \to \{\pm 1\}$ such that $\theta(-1) = 1$ and $\bar{\theta} = \theta$. Denote also by W_0 the set of $\theta \in W$ such that $\theta = \kappa \circ \mathrm{N}_{M/\mathbb{Q}}$ for some Dirichlet character κ. By [Nak04, Proposition 3], the group W/W_0 is generated by two characters that can be described explicitly in terms of the characters $\eta_p, \eta_{-4}, \eta_{-8}$, and η_8. More precisely:

(1) If $D = -pqr$ with p, q, and r primes congruent to 3 modulo 4, then $W/W_0 = \langle \eta_p\eta_q, \eta_p\eta_r \rangle$.

(2) If $D = -pqr$ with p and q primes congruent to 1 modulo 4, and $r \equiv 3 \pmod 4$, then $W/W_0 = \langle \eta_p, \eta_q \rangle$.
(3) If $D = -4pq$ with p and q congruent to 3 modulo 4, then $W/W_0 = \langle \eta_{-4}, \eta_p\eta_q \rangle$.
(4) If $D = -8pq$ with p and q congruent to 3 modulo 4 then $W/W_0 = \langle \eta_{-8}\eta_p, \eta_{-8}\eta_q \rangle$.
(5) If $D = -8pq$ with $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ then $W/W_0 = \langle \eta_8, \eta_p \rangle$.
(6) If $D = -8pq$ with p and q congruent to 1 modulo 4, then $W/W_0 = \langle \eta_p, \eta_q \rangle$.

Denote by $\tilde{\omega}_1, \tilde{\omega}_2$ the generators of W/W_0, and define $\omega_i = \tilde{\omega}_i \circ \mathrm{N}_{H/M}$.

Now let k/H be a quadratic extension such that $k/\mathbb{Q}$ is Galois and k/M is non-abelian. Such quadratic extensions exist by [Nak04, Theorem 1]. Denote by $\chi\colon \mathbb{I}_H \to \{\pm 1\}$ the Hecke character attached to k/H.

By [Nak04, Theorem 2], the eight equivalence classes of $\mathbb{Q}$-curves over H are represented by the Hecke characters $\psi_0 \cdot \omega$ with $\omega \in \langle \omega_1, \omega_2, \chi \rangle$. Observe that, in particular, this set of Hecke characters does not depend on the choice of k (any k which is Galois over $\mathbb{Q}$ and non-abelian over M will produce the same set of Hecke characters).

3.2. **Method for computing the endomorphism algebra.** Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be prime ideals of M that generate the class group and that are coprime to the conductors of ψ_0, ω_1, ω_2, and χ. Let L_i be the decomposition field of $\mathfrak{p}_i$ in H, and F_i the maximal totally real subfield of L_i.

Suppose that E is a Gross $\mathbb{Q}$-curve over H with Hecke character of the form $\psi = \psi_0\omega_1^a\omega_2^b$ for some $a, b \in \{0, 1\}$. We can write $\psi = \phi \circ \mathrm{N}_{H/M}$, where $\phi = \phi_0\tilde{\omega}_1^a\tilde{\omega}_2^b$. Then $\phi(\mathfrak{p}_i) + \phi(\bar{\mathfrak{p}}_i)$ generates a quadratic number field $\mathbb{Q}(\sqrt{n_i})$, and the endomorphism algebra $\mathcal{D}_E = \mathrm{End}(B_E)$ is isomorphic to the biquadratic field $\mathbb{Q}(\sqrt{n_1}, \sqrt{n_2})$ (cf. [Nak04, Proposition 7, Theorem 3]).

Remark 3.4. Observe that $\phi(\mathfrak{p}_i) + \phi(\bar{\mathfrak{p}}_i)$ can be computed if one knows the two quantities $\phi(\mathfrak{p}_i^2)$ and $\phi(\mathfrak{p}_i\bar{\mathfrak{p}}_i)$. Since $\mathfrak{p}_i^2$ and $\mathfrak{p}_i\bar{\mathfrak{p}}_i$ are principal, one can compute $\phi(\mathfrak{p}_i^2)$ and $\phi(\mathfrak{p}_i\bar{\mathfrak{p}}_i)$ by means of (3.2).

Suppose now that the Hecke character of E is of the form $\psi = \psi_0\chi\omega_1^a\omega_2^b$. Then $\mathcal{D}_E$ is a quaternion algebra over $\mathbb{Q}$, say $\mathcal{D}_E \simeq \left(\frac{t_1, t_2}{\mathbb{Q}}\right)$. The t_i can be computed as follows (see [Nak04, Proposition 7]). First of all, let n_1 and n_2 be the rational numbers defined as in the previous paragraph for the character $\psi/\chi = \psi_0\omega_1^a\omega_2^b$.

(1) Suppose that $\mathrm{Gal}(k/L_i) \simeq \mathrm{C}_2 \times \mathrm{C}_2$. Then:
   (a) If k/F_i is abelian then $t_i = n_i$.
   (b) If k/F_i is non-abelian, then $t_i = D/n_i$.
(2) Suppose that $\mathrm{Gal}(k/L_i) \simeq \mathrm{C}_4$. Then:
   (a) If k/F_i is abelian, then $t_i = -n_i$.
   (b) If k/F_i is non-abelian, then $t_i = -D/n_i$.

3.3. **Computations and tables.** For each of the 23 non-exceptional imaginary quadratic fields of class group $\mathrm{C}_2 \times \mathrm{C}_2$, we have computed the 8 endomorphism algebras arising from restriction of scalars of Gross $\mathbb{Q}$-curves. The results are displayed in Table 1. The notation is as follows: for the biquadratic fields, the notation (a, b) indicates the field $\mathbb{Q}(\sqrt{a}, \sqrt{b})$; for the quaternion algebras, we write the discriminant of the algebra.

For a Gross $\mathbb{Q}$-curve E, recall that we denote by B_E the abelian variety over $\mathbb{Q}$ such that $\operatorname{Res}_{H/M} E \sim (B_E)_M$. Since B_E is isogenous to its quadratic twist over M, this implies that

$$\operatorname{Res}_{H/\mathbb{Q}} E \sim (B_E)^2.$$

We observe in Table 1 that for all discriminants except -195, -312, -555, -715, and -760, at least one of the quaternion algebras is the split algebra $\mathrm{M}_2(\mathbb{Q})$ of discriminant 1. This implies that for the corresponding Gross $\mathbb{Q}$-curve E the variety B_E decomposes as

$$B_E \sim A^2,$$

with $A/\mathbb{Q}$ an abelian surface. Therefore, $\operatorname{Res}_{H/\mathbb{Q}} E$ decomposes as the fourth power of an abelian surface.

On the other hand, for the discriminants -195, -312, -555, -715, and -760 we see that B_E is always simple: its endomorphism algebra is either a biquadratic field or a quaternion division algebra over $\mathbb{Q}$. Therefore, $\operatorname{Res}_{H/\mathbb{Q}} E \sim W^2$ for some simple variety W of dimension 4. We record these findings in the following statement.

Theorem 3.5. *Let M be an imaginary quadratic field of discriminant D and Hilbert class field H. Suppose that D is non-exceptional and that* $\operatorname{Gal}(H/M) \simeq \mathrm{C}_2 \times \mathrm{C}_2$. *If $D \neq -195, -312, -555, -715, -760$, there exists a Gross $\mathbb{Q}$-curve E/H such that*

$$\operatorname{Res}_{H/\mathbb{Q}} E \sim A^4, \text{ for some simple abelian surface } A/\mathbb{Q}.$$

If $D = -195, -312, -555, -715, -760$, then for every Gross $\mathbb{Q}$-curve E/H we have that

$$\operatorname{Res}_{H/\mathbb{Q}} E \sim W^2, \text{ for some simple abelian variety } W/\mathbb{Q} \text{ of dimension } 4.$$

Remark 3.6. As mentioned above, the cases of $D = -84$ and $D = -195$ were already computed by Nakamura ([Nak04, §6]). We note what appears to be a typo in Nakamura's table in page 647: the last biquadratic field should be $\mathbb{Q}(\sqrt{-14}, \sqrt{42})$, instead of $\mathbb{Q}(\sqrt{-14}, \sqrt{-42})$.

We have used the software Sage [S+14] and Magma [BCP97] to perform the computations of Table 1. The interested reader can find the code we used in `https://github.com/xguitart/restriction_of_scalars_of_Q_curves`.

D	Biquadratic fields	Quaternion Algebras
-84	$(-14,-2),(-6,2),(-6,-42),(-14,42)$	$2,1,2,1$
-120	$(-5,10),(5,-10),(-5,-10),(5,10)$	$1,6,3,1$
-132	$(22,-2),(-6,-2),(6,-66),(-22,-66)$	$1,2,1,2$
-168	$(-14,-2),(3,-21),(14,21),(-3,2)$	$2,1,1,1$
-195	$(13,-5),(-13,-5),(-13,5),(13,5)$	$13,39,26,39$
-228	$(-38,-2),(6,-2),(-6,-114),(38,-114)$	$2,1,2,1$
-280	$(-10,-5),(-10,5),(10,-5),(10,5)$	$2,1,14,14$
-312	$(13,-26),(-13,26),(-13,-26),(13,26)$	$13,39,26,39$
-372	$(-62,31),(-6,-3),(-6,31),(-62,-3)$	$2,1,2,1$
-408	$(-17,34),(-17,-34),(17,-34),(17,34)$	$2,1,1,1$
-435	$(-29,-5),(-29,5),(29,-5),(29,5)$	$2,1,1,1$
-483	$(-23,7),(23,-69),(-21,-7),(21,69)$	$2,1,1,1$
-520	$(-13,-5),(13,-5),(-13,5),(13,5)$	$1,1,1,2$
-532	$(-38,-19),(-14,7),(-14,-19),(-38,7)$	$1,2,1,2$
-555	$(37,-5),(-37,-5),(-37,5),(37,5)$	$37,111,74,111$
-595	$(-17,85),(17,-85),(-17,-85),(17,85)$	$7,1,1,14$
-627	$(19,-11),(-19,-57),(-33,11),(33,57)$	$1,2,1,1$
-708	$(118,-59),(-6,3),(6,-59),(-118,3)$	$1,2,1,2$
-715	$(-13,-65),(13,-65),(-13,65),(13,65)$	$5,10,55,55$
-760	$(-10,5),(10,-5),(-10,-5),(10,5)$	$5,95,10,95$
-795	$(-53,-5),(53,-5),(-53,5),(53,5)$	$6,1,1,3$
-1012	$(-46,23),(-22,-11),(-22,23),(-46,-11)$	$2,1,2,1$
-1435	$(-41,205),(-41,-205),(41,-205),(41,205)$	$2,1,1,1$

Table 1. Endomorphism algebras of the restriction of scalars of Gross $\mathbb{Q}$-curves. For the biquadratic fields, the notation (a,b) indicates the field $\mathbb{Q}(\sqrt{a},\sqrt{b})$; for the quaternion algebras, we write the discriminant of the algebra

4. Proof of the main theorems

We begin with a Lemma that will be used in the proof of Theorem 1.2.

Lemma 4.1. *Let E be a Gross $\mathbb{Q}$-curve with CM by a field M of discriminant D, and suppose that $\mathrm{Gal}(H/M)$ is isomorphic to $\mathrm{C}_2 \times \mathrm{C}_2$. Denote by γ_E^H the class in $H^2(\mathrm{Gal}(H/M), M^\times)$ attached to E, and by c_E a cocycle representing γ_E^H. If $\sigma \in \mathrm{Gal}(H/M)$ is non-trivial, then $\pm d \cdot c_E(\sigma,\sigma) \in (M^\times)^2$ for some divisor d of D such that d is not a square in $M^\times$.*

Proof. Let $\mathcal{O}_M$ denote the ring of integers of M. Denote by p_1, p_2, p_3 the primes dividing D. Observe that $p_i\mathcal{O}_M = \mathfrak{p}_i^2$, with $\mathfrak{p}_i$ a non-principal prime ideal of $\mathcal{O}_M$. It is clear that we can always find p_i, p_j such that $\pm p_i p_j$ is not a square in $M^\times$, and therefore $\mathfrak{p}_i\mathfrak{p}_j$ is not principal. Thus $\mathfrak{p}_i, \mathfrak{p}_j$ generate the class group. Therefore, we can assume that any non-trivial element of $\mathrm{Gal}(H/K)$ is of the form $\sigma_\mathfrak{q}$ for some unramified prime $\mathfrak{q}$ which is equivalent to either $\mathfrak{p}_i$, $\mathfrak{p}_j$ or $\mathfrak{p}_i \cdot \mathfrak{p}_j$. Here $\sigma_\mathfrak{q}$ stands for the Frobenius automorphism of H/K at $\mathfrak{q}$.

Now we argue (and use the same notation) as in [Nak04, Proof of Theorem 3]. Namely, denote by $u(\mathfrak{q})$ the $\mathfrak{q}$-multiplication isogenies

$$u(\mathfrak{q}) : {}^{\sigma_\mathfrak{q}}E \longrightarrow E,$$

and denote by c the 2-cocycle associated to E using the system of isogenies $u(\mathfrak{q})$ (together with the identity isogeny for $1 \in \mathrm{Gal}(H/M)$). Note that c_E is any cocycle representing γ_E^H, and it may be different from c. But in any case they are cohomologous, which in particular implies that

$$c(\sigma_\mathfrak{q}, \sigma_\mathfrak{q}) = b_\mathfrak{q}^2 \cdot c_E(\sigma_\mathfrak{q}, \sigma_\mathfrak{q}) \text{ for some } b_\mathfrak{q} \in M^\times. \tag{4.1}$$

From display (6) and the display after that of loc. cit., since the order n of $\sigma_\mathfrak{q}$ is 2 in our case, we see that

$$c(\sigma_\mathfrak{q}, \sigma_\mathfrak{q})\mathcal{O}_M = \mathfrak{q}^2.$$

The proof is finished by observing that $\mathfrak{q}^2 = \alpha\mathcal{O}_M$, where $\alpha \in M^\times$ is, up to an element of $(M^\times)^2$, equal to $\pm p_i$, $\pm p_j$, or $\pm p_i \cdot p_j$. ☐

Proof of Theorem 1.2. For all the quadratic imaginary fields not listed in (1.2), we have constructed in the first part of Theorem 3.5 abelian surfaces defined over $\mathbb{Q}$ satisfying the hypothesis of the theorem. To rule out the remaining 6 fields, we proceed in the following way.

Let M be one of the fields in the list (1.2) and suppose that an abelian surface A satisfying the hypothesis of the theorem exists for M. Resume the notations from Section 2.4. As $\mathrm{Gal}(H/M) \simeq \mathrm{C}_2 \times \mathrm{C}_2$ and $H \subseteq K$ (by [FG18, Theorem 2.14]), the only possibilities for $\mathrm{Gal}(K/M)$ are $\mathrm{C}_2 \times \mathrm{C}_2$, D_4, and D_6.

Suppose that $\mathrm{Gal}(K/M)$ is $\mathrm{C}_2 \times \mathrm{C}_2$. Then $K = H$ and thus E is a Gross $\mathbb{Q}$-curve. By Proposition 2.10, we have that M is not exceptional and thus we cannot have $M = \mathbb{Q}(\sqrt{-340})$. For the other possibilities for M, we have seen in the second part of Theorem 3.5 that $\mathrm{Res}_{H/\mathbb{Q}} E$ does not have any simple factor of dimension 2, but this is a contradiction with the fact that A should be a factor of $\mathrm{Res}_{H/\mathbb{Q}} E$ (indeed, the universal property of Weil's restriction of scalars implies that $\mathrm{Hom}(A, \mathrm{Res}_{H/\mathbb{Q}} E) = \mathrm{Hom}(A_H, E) \simeq M^2$, and thus $\mathrm{Hom}(A, \mathrm{Res}_{H/\mathbb{Q}} E) \neq 0$).

Suppose that $\mathrm{Gal}(K/M)$ is D_4 or D_6. Resume the notations of Section 2.5. Let E^* be a Ribet M-curve completely defined over H with CM by M which we chose as in Corollary 2.25 (and which exists because of Proposition 2.10). Note that Hypothesis 2.22 is satisfied. Then, by Theorem 2.27, there is a non-trivial element $\overline{\tau} \in \mathrm{Gal}(N/M) = \mathrm{Gal}(H/N)$ such that

$$c^H_{E^*}(\overline{\tau}, \overline{\tau}) = \pm 1. \tag{4.2}$$

If M is non-exceptional, as noted in Remark 2.26, we can suppose that E^* is in fact a Gross $\mathbb{Q}$-curve. Then (4.2) is a contradiction with Lemma 4.1.

It remains to show that (4.2) also brings a contradiction if $M = \mathbb{Q}(\sqrt{-340})$ is the exceptional field. Put $T = H^{\langle \overline{\tau} \rangle}$, the fixed field by $\overline{\tau}$. Observe that $M \subsetneq T \subsetneq H$. If $c^H_{E^*}(\overline{\tau}, \overline{\tau}) = 1$ then by Theorem 2.11 the curve E^* is isogenous to a curve defined over T, and this is a contradiction with the fact that $M(j_{E^*}) = H$.

Suppose now that $c^H_{E^*}(\overline{\tau}, \overline{\tau}) = -1$. We will see that we can apply the above argument to an appropriate quadratic twist of E^*.

Claim 4.2. *There exists a quadratic extension S/H such that S/M is Galois with* $\mathrm{Gal}(S/M) \simeq \mathrm{D}_4$ *and such that $\overline{\tau}$ lifts to an element of order* 4 *of* $\mathrm{Gal}(S/M)$*.*

We now show how this claim allows us to produce the appropriate twisted curve (and we will prove the claim later on). Define C to be the S/H quadratic twist of E^*. By [FG18, Lemma 3.13], the curve C is an M-curve completely defined over H and the cohomology classes of E^* and C are related by

$$\gamma^H_C = \gamma^H_{E^*} \cdot \gamma_S,$$

where $\gamma_S \in H^2(\mathrm{Gal}(H/M), \{\pm 1\})$ is the cohomology class attached to the exact sequence

$$1 \longrightarrow \mathrm{Gal}(S/H) \simeq \{\pm 1\} \longrightarrow \mathrm{Gal}(S/M) \simeq \mathrm{D}_4 \longrightarrow \mathrm{Gal}(H/M) \longrightarrow 1. \tag{4.3}$$

If we identify $\mathrm{Gal}(S/M) \simeq \langle s, t | s^4, t^2, stst \rangle$, then $\mathrm{Gal}(S/H)$ can be identified with the subgroup generated by s^2 and we can assume that $\overline{\tau}$ lifts to s. Let c_S be a cocycle representing γ_S. The usual construction that associates a cohomology class to (4.3) gives that $c_S(\overline{\tau}, \overline{\tau}) = s \cdot s$. Since s^2 is the non-trivial element of $\mathrm{Gal}(S/H)$, it corresponds to -1 under the isomorphism $\mathrm{Gal}(S/H) \simeq \{\pm 1\}$, so that $c_S(\overline{\tau}, \overline{\tau}) = -1$.

We conclude that $c^H_C(\overline{\tau}, \overline{\tau}) = c^H_{E^*}(\overline{\tau}, \overline{\tau}) c_S(\overline{\tau}, \overline{\tau}) = 1$, and as before this implies that C can be defined over T, which is a contradiction.

Proof of Claim 4.2. The Hilbert class field of M is $H = \mathbb{Q}(i, \sqrt{5}, \sqrt{17})$. If we write $H = M(\sqrt{a}, \sqrt{b})$ and suppose that $\overline{\tau}(\sqrt{b}) = \sqrt{b}$, it is well known (see, e.g. [Led01, §0.4]) that the obstruction to the existence of S is given by the quaternion algebra $\left(\frac{a, ab}{M}\right)$ being nonsplit. There are 3 possibilities for T, namely $T = M(\sqrt{5})$, $T = M(\sqrt{17})$, or $T = M(\sqrt{5 \cdot 17})$, each one giving a different obstruction. The resulting quaternion algebras giving the obstruction are

$$\left(\frac{17 \cdot 5, 5}{M}\right), \left(\frac{17 \cdot 5, 17}{M}\right), \left(\frac{17, 5}{M}\right).$$

Since they are all the split, the field S does exist in all three cases.

Remark 4.3. As a byproduct of the above proof, we see that there do not exist abelian surfaces over $\mathbb{Q}$ such that $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathrm{M}_2(M)$ with M a quadratic imaginary field with class group $\mathrm{C}_2 \times \mathrm{C}_2$ and $\mathrm{Gal}(K/M) \simeq \mathrm{D}_4$ or D_6. As shown by the table of [Car01, p. 112], there do exist abelian surfaces over $\mathbb{Q}$ such that $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathrm{M}_2(M)$

with M a quadratic imaginary field with class group C_2 and $\mathrm{Gal}(K/M) \simeq \mathrm{D}_4$ (resp. D_6). If M is not exceptional, Theorem 2.20 and Lemma 4.1 imply that 2 (resp. 3) divide the discriminant of M is a necessary condition for the existence of such an A. The examples of the table of [Car01, p. 112] show that this is actually a necessary and sufficient condition.

Proof of Corollary 1.3. Suppose that A is an abelian surface defined over $\mathbb{Q}$ such that $A_{\overline{\mathbb{Q}}} \sim E \times E'$, where E and E' are elliptic curves defined over $\overline{\mathbb{Q}}$. If E and E' are not isogenous, then $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ is

$$\mathbb{Q} \times \mathbb{Q}\,, \qquad M \times \mathbb{Q} \qquad \text{or} \qquad M_1 \times M_2\,,$$

where M, $M_1 \not\simeq M_2$ are quadratic imaginary fields, depending on whether none of E and E' has CM, only one of E and E' has CM, or both of E and E' have CM. In any case, note that by [FKRS12, Proposition 4.5], both E and E' can be defined over $\mathbb{Q}$, whereby the class number of M, M_1, and M_2 must be 1. Recalling that there are 9 quadratic imaginary fields of class number 1, this accounts for 46 distinct $\overline{\mathbb{Q}}$-endomorphism algebras.

If E and E' are isogenous, we have that $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ is $\mathrm{M}_2(M)$ or $\mathrm{M}_2(\mathbb{Q})$, where M is a quadratic imaginary field, depending on whether E has CM or not. Assume that we are in the former case. By Theorem 1.1, we have that M has class group 1, C_2, or $\mathrm{C}_2 \times \mathrm{C}_2$. As explained in [FG18, Remark 2.20], for all fields M with class group 1 (resp. C_2), abelian surfaces A over $\mathbb{Q}$ with $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathrm{M}_2(M)$ can be easily found. Indeed, let E be an elliptic curve with CM by the maximal order of M and defined over $\mathbb{Q}$ (resp. $\mathbb{Q}(j_E)$). Then consider the square (resp. the restriction of scalars from $\mathbb{Q}(j_E)$ down to $\mathbb{Q}$) of E. If M has class group $\mathrm{C}_2 \times \mathrm{C}_2$, invoke Theorem 1.2 to obtain 18 possibilities for M. Taking into account that there are 18 quadratic imaginary fields of class group C_2 (see [Wat04] for example), we obtain 46 possibilities for the endomorphism algebra of a geometrically split abelian surface over $\mathbb{Q}$ with $\overline{\mathbb{Q}}$-isogenous factors.

An open problem. We wish to conclude the article with an open question.

Question 4.4. *Which is the subset of $\mathcal{A}$ made of the $\overline{\mathbb{Q}}$-endomorphism algebras $\mathrm{End}(\mathrm{Jac}(C)_{\overline{\mathbb{Q}}})$ of geometrically split Jacobians of genus 2 curves C defined over $\mathbb{Q}$?*

Again the most intriguing case is to determine how many of the 45 possibilities for $\mathrm{M}_2(M)$, with M a quadratic imaginary field, allowed by Theorem 1.2 for geometrically split abelian surfaces defined over $\mathbb{Q}$ still occur among geometrically split Jacobians of genus 2 curves C defined over $\mathbb{Q}$. Looking at the more restrictive setting that requires $\mathrm{Jac}(C)$ to be *isomorphic* to the square of an elliptic curve with CM by the *maximal order* of M, Gélin, Howe, and Ritzenthaler [GHR19] have shown that there are 13 possibilities for such an M (all with class number ≤ 2).

References

[BCP97] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[BFGR06] Nils Bruin, E. Victor Flynn, Josep González, and Victor Rotger. On finiteness conjectures for endomorphism algebras of abelian surfaces. *Math. Proc. Cambridge Philos. Soc.*, 141(3):383–408, 2006.

[Car01] Gabriel Cardona. *Models racionals de corbes de gènere 2*. PhD thesis, Universitat Politècnica de Catalunya, 2001.

[FG18] Francesc Fité and Xavier Guitart. Fields of definition of elliptic k-curves and the realizability of all genus 2 Sato–Tate groups over a number field. *Trans. Amer. Math. Soc.*, 370(7):4623–4659, 2018.

[FG19] Francesc Fité and Xavier Guitart. Tate module tensor decompositions and the Sato-Tate conjecture for certain abelian varieties potentially of GL_2-type, 2019, Preprint, arXiv: 1909.11712.

[FKRS12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.

[FS14] Francesc Fité and Andrew V. Sutherland. Sato-Tate distributions of twists of $y^2 = x^5 - x$ and $y^2 = x^6 + 1$. *Algebra Number Theory*, 8(3):543–585, 2014.

[GHR19] Alexandre Gélin, Everett Howe, and Christophe Ritzenthaler. Principally polarized squares of elliptic curves with field of moduli equal to $\mathbb{Q}$. *The Open Book Series*, 2(1):257–274, Jan 2019.

[Gon11] Josep González. Finiteness of endomorphism algebras of CM modular abelian varieties. *Rev. Mat. Iberoam.*, 27(3):733–750, 2011.

[Gro80] Benedict H. Gross. *Arithmetic on elliptic curves with complex multiplication*, volume 776 of *Lecture Notes in Mathematics*. Springer, Berlin, 1980. With an appendix by B. Mazur.

[Kan11] Ernst Kani. Products of CM elliptic curves. *Collect. Math.*, 62(3):297–339, 2011.

[Led01] Arne Ledet. Embedding problems and equivalence of quadratic forms. *Math. Scand.*, 88(2):279–302, 2001.

[MU01] Naoki Murabayashi and Atsuki Umegaki. Determination of all $\mathbf{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces. *J. Algebra*, 235(1):267–274, 2001.

[Nak01] Tetsuo Nakamura. On abelian varieties associated with elliptic curves with complex multiplication. *Acta Arith.*, 97(4):379–385, 2001.

[Nak04] Tetsuo Nakamura. A classification of $\mathbf{Q}$-curves with complex multiplication. *J. Math. Soc. Japan*, 56(2):635–648, 2004.

[OS18] Martin Orr and Alexei N. Skorobogatov. Finiteness theorems for K3 surfaces and abelian varieties of CM type. *Compos. Math.*, 154(8):1571–1592, 2018.

[Que00] Jordi Quer. $\mathbf{Q}$-curves and abelian varieties of GL_2-type. *Proc. London Math. Soc. (3)*, 81(2):285–317, 2000.

[Rib92] Kenneth A. Ribet. Abelian varieties over $\mathbf{Q}$ and modular forms. In *Algebra and topology 1992 (Taejŏn)*, pages 53–79. Korea Adv. Inst. Sci. Tech., Taejŏn, 1992.

[S$^+$14] W. A. Stein et al. *Sage Mathematics Software (Version 6.3)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[Sch07] Matthias Schütt. Fields of definition of singular $K3$ surfaces. *Commun. Number Theory Phys.*, 1(2):307–321, 2007.

[Sha96] I. R. Shafarevich. On the arithmetic of singular $K3$-surfaces. In *Algebra and analysis (Kazan, 1994)*, pages 103–108. de Gruyter, Berlin, 1996.

[Shi71] Goro Shimura. On the zeta-function of an abelian variety with complex multiplication. *Ann. of Math. (2)*, 94:504–533, 1971.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[Wat04] Mark Watkins. Class numbers of imaginary quadratic fields. *Math. Comp.*, 73(246):907–938, 2004.

Department of Mathematics, Massachussetts Institute of Technology, 77 Massachussetts Avenue, 02139 Cambridge, Massachussetts, USA

Email address: `ffite@mit.edu`

URL: `http://www-math.mit.edu/~ffite/`

Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran via de les Corts Catalanes, 585, 08007 Barcelona, Catalonia

Email address: `xevi.guitart@gmail.com`

URL: `http://www.maia.ub.es/~guitart/`