FIELDS OF DEFINITION OF ELLIPTIC k-CURVES AND THE REALIZABILITY OF ALL GENUS 2 SATO–TATE GROUPS OVER A NUMBER FIELD

FRANCESC FITÉ AND XAVIER GUITART

ABSTRACT. Let $A/\mathbb{Q}$ be an abelian variety of dimension $g \geq 1$ that is isogenous over $\overline{\mathbb{Q}}$ to E^g, where E is an elliptic curve. If E does not have complex multiplication (CM), by results of Ribet and Elkies concerning fields of definition of elliptic $\mathbb{Q}$-curves E is isogenous to a curve defined over a polyquadratic extension of $\mathbb{Q}$. We show that one can adapt Ribet's methods to study the field of definition of E up to isogeny also in the CM case. We find two applications of this analysis to the theory of Sato–Tate groups: First, we show that 18 of the 34 possible Sato–Tate groups of abelian surfaces over $\mathbb{Q}$ occur among at most 51 $\overline{\mathbb{Q}}$-isogeny classes of abelian surfaces over $\mathbb{Q}$; Second, we give a positive answer to a question of Serre concerning the existence of a number field over which abelian surfaces can be found realizing each of the 52 possible Sato–Tate groups of abelian surfaces.

CONTENTS

1. INTRODUCTION

It is well known that there exist three possibilities for the Sato–Tate group of an elliptic curve E defined over a number field k: the special unitary group $\mathrm{SU}(2)$ of degree 2, the unitary group $\mathrm{U}(1)$ of degree 1 embedded in $\mathrm{SU}(2)$, and the normalizer

$N(\mathrm{U}(1))$ of $\mathrm{U}(1)$ in $\mathrm{SU}(2)$. These three possibilities are in accordance with the following trichotomy: the elliptic curve does not have complex multiplication (CM), the elliptic curve has CM defined over k, and the elliptic curve has CM but not defined over k.

From this description, it is easy to see that there exists a number field (for example, take any quadratic imaginary field of class number 1) over which three elliptic curves can be defined realizing each of the three Sato–Tate groups $\mathrm{SU}(2)$, $\mathrm{U}(1)$, and $N(\mathrm{U}(1))$.

In [FKRS12], it was shown that there exist 52 possible Sato–Tate groups of abelian surfaces over number fields, all of which occur for some choice of the number field and of the abelian surface defined over it. Let $N_{\mathrm{ST},2}(k)$ denote the number of subgroups of $\mathrm{USp}(4)$ up to conjugacy that arise as Sato–Tate groups of abelian surfaces defined over the number field k. In [FKRS12], it was proven that $N_{\mathrm{ST},2}(\mathbb{Q}) = 34$. Serre has asked the following question.

Question 1.1. *Does there exist a number field k over which* 52 *abelian surfaces can be found realizing each of the* 52 *possible Sato–Tate groups of abelian surfaces over number fields? In other words, does there exist a number field k such that* $N_{\mathrm{ST},2}(k) = 52$?

It is well-known that the connected component of the identity of the Sato–Tate group is invariant under base change. However, its group of components is sensitive to base change, and it is therefore not necessarily true (and in fact, it is not) that the compositum of all fields of definition of the examples in [FKRS12] gives a positive answer to the above question.

The question is thus on whether the conditions imposed on k by each of the possible groups of components are compatible or not among them. Fundamental to this analysis is the existence of an isomorphism between the group of components of the Sato–Tate group of an abelian surface A defined over k and the Galois group $\mathrm{Gal}(K/k)$, where K/k is the minimal extension over which all of the endomorphisms of A are defined.

Let us look at a concrete example of the type of conditions on k imposed by certain groups of components. We will consider abelian surfaces A defined over a number field k satisfying

(P) $\mathrm{Gal}(K/k)$ contains S_4.

One can easily show that (P) implies that A is isogenous over $\overline{\mathbb{Q}}$ to the square of an elliptic curve with CM, say by a quadratic imaginary field M. There are only three Sato–Tate groups (denoted by O, O_1, and $J(O)$ in [FKRS12]) whose group of components contains the symmetric group S_4. The dictionary between Sato–Tate groups and Galois endomorphism types of [FKRS12] ensures that O only arises among A satisfying (P) for which $M \subseteq k$, whereas O_1 and $J(O)$ can occur only for A satisfying (P) with $M \not\subseteq k$.

Up to our knowledge, all the examples in the existing literature of abelian surfaces A satisfying (P) have $M = \mathbb{Q}(\sqrt{-2})$. The lack of a simple construction of such an A with $M \neq \mathbb{Q}(\sqrt{-2})$, together with the fact that the wide computational search of abelian surfaces performed in [FKRS12] yielded only examples of A satisfying (P) with $M = \mathbb{Q}(\sqrt{-2})$, may suggest that indeed $M = \mathbb{Q}(\sqrt{-2})$ might be a necessary condition for A to satisfy (P). If this was the case, then Question 1.1 would have a

negative answer, since in order to realize, for example, both O and $J(O)$ the field k would be forced to contain and not contain $\mathbb{Q}(\sqrt{-2})$ simultaneously.

As a consequence of the preceding discussion, one is naturally led by Question 1.1 to the following question regarding a basic aspect of the arithmetic of abelian varieties over $\mathbb{Q}$.

Question 1.2. *Let A be an abelian variety defined over $\mathbb{Q}$ of dimension $g \geq 1$ that is $\overline{\mathbb{Q}}$-isogenous to E^g, where E is an elliptic curve over $\overline{\mathbb{Q}}$ with CM by M.*
- (A) *Which is the set of possibilities for M?*
- (B) *Let K/M be the minimal extension over which all the endomorphisms of A are defined. Does the prescription of $\mathrm{Gal}(K/M)$ impose further restrictions on M?*

If $g = 1$, then the theory of complex multiplication shows that M is a quadratic imaginary field of class number 1 and thus there are only 9 possibilities for M. In this work, we provide an answer to Question 1.2 for $g = 2$, which sets the basis on which we build a positive answer to Question 1.1.

Main results. As the case $g = 1$ may suggest, an answer to Question 1.2 will follow, via the theory of complex multiplication, from gaining control on the field of definition of the elliptic factor E. The study of the field of definition of E will be carried out in §2.2, whose main result is the following (see Theorem 2.14).

Theorem 1.3. *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by a quadratic imaginary field M such that E^g, for some $g \geq 1$, is $\overline{\mathbb{Q}}$-isogenous to an abelian variety A defined over k. Assume that M is contained in k. Let K/k be the minimal extension over which all the endomorphisms of A are defined. Then E is $\overline{\mathbb{Q}}$-isogenous to an elliptic curve E^* defined over an abelian subextension F/k of K/k such that every element in $\mathrm{Gal}(F/k)$ has order dividing g.*

Observe that the elliptic curve E in the preceding theorem is an elliptic k-curve in the sense of Ribet (the notion of elliptic k-curve and, more generally, of abelian k-variety, will be recalled in §2.1). A characterization of the field of definition of an elliptic k-curve C without CM (achieved by Ribet [Rib94] and Elkies [Elk04] by means of completely different methods) is well known: C admits a model up to isogeny defined over a polyquadratic[1] extension of k. We will show that in our particular situation Ribet's methods can also be applied to the CM case. The crucial idea is that E^g admitting a model over k implies that the gth power of the cohomology class $\gamma_E \in H^2(G_k, M^*)$ naturally attached to E is trivial, a property that does not necessarily hold for an arbitrary CM elliptic k-curve C.

Combining Theorem 1.3 with bounds on the degree of K/k (deduced from the methods of [Sil92] and [GK16]), one obtains the following answer to part (A) of Question 1.2.

Theorem 1.4. *With the notations as in Question 1.2, the class group $\mathrm{Cl}(M)$ of M has exponent dividing g. If moreover g is prime, then*

$$\mathrm{Cl}(M) = \begin{cases} 1, \mathrm{C}_g, \ or \ \mathrm{C}_g \times \mathrm{C}_g & if \ g = 2, \\ 1 \ or \ \mathrm{C}_g & otherwise. \end{cases}$$

In particular, if $g = 2$, there are at most 51 possibilities for M.

---

[1] That is, the composition of a finite number of quadratic extensions.

We refer the reader to Theorem 3.21 for a more precise version of the above theorem in the case $g = 2$, which accounts also for part (B) of Question 1.2. Just to show the flavour of the result, let us state a particular instance of it: if for example $\text{Gal}(K/M) \simeq S_4$, then M is either $\mathbb{Q}(\sqrt{-2})$ or a quadratic imaginary field of class number 2 and distinct from $\mathbb{Q}(\sqrt{-15})$, $\mathbb{Q}(\sqrt{-35})$, $\mathbb{Q}(\sqrt{-51})$, and $\mathbb{Q}(\sqrt{-115})$.

These kind of constraints on M are obtained by means of two different methods. First, we consider obstructions coming from group representation theory. These are obtained by pushing a bit further the study in [FS14, §3] of the Galois module structure of the ring of endomorphisms of an abelian surface that is $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve. This is done in §3.1. Second, we consider obstructions coming from group cohomology. These are obtained by means of a detailed study of the endomorphism algebra of the Weil's restriction of scalars $\text{Res}_{K/k} E$ in the case $\text{Gal}(K/k) \simeq S_4$. We again benefit from a technique exploited in Ribet's work: we look at this algebra as a twisted group algebra. A key step towards determining its structure is to compute its center; we devote §3.2 to that calculation. In §3.3, it only remains to combine the results of §3.1 and §3.2.

Thanks to the dictionary between Sato–Tate groups and Galois endomorphism types, there is an equivalent formulation of Theorem 1.4 in the case $g = 2$.

Theorem 1.5. *Among the* 34 *possibilities for the Sato–Tate group of an abelian surface defined over* $\mathbb{Q}$*, the* 18 *with identity component isomorphic to* $\text{U}(1)$ *occur among at most* 51 $\overline{\mathbb{Q}}$*-isogeny classes of abelian surfaces over* $\mathbb{Q}$*.*

We refer to Theorem 4.1 for a more precise version of the above statement. At this stage, we are ready to provide an affirmative answer to Question 1.1, which is the main result of this paper (see Theorem 4.2).

Theorem 1.6. *One has* $N_{\text{ST},2}(k_0) = 52$ *for*
$$k_0 := \mathbb{Q}(\sqrt{-40}, \sqrt{-51}, \sqrt{-163}, \sqrt{-67}, \sqrt{19 \cdot 43}, \sqrt{-57}).$$

After the discussion following Question 1.1, it is clear that constructing an abelian surface defined over k satisfying (P) and for which $M \neq \mathbb{Q}(\sqrt{-2})$ is a crucial step in the proof. We devote the whole of §3.4 to construct an abelian surface A defined over $k = \mathbb{Q}(\sqrt{-40})$, $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve with CM by $M = \mathbb{Q}(\sqrt{-40})$, and for which $\text{Gal}(K/k) \simeq S_4$. This abelian surface A is obtained as a simple factor of the restriction of scalars of a certain elliptic curve with CM by $\mathbb{Q}(\sqrt{-40})$ over a suitable extension K/k; in the construction, we make crucial use of the techniques developed in §3.2. The construction of the remaining abelian surfaces, which is carried out in §4, requires less elaborate techniques, though still forces k_0 to contain a few more additional quadratic fields.

Notations and terminology. Throughout this article, k will be a number field assumed to be contained in a fixed algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. We will write G_k for the absolute Galois group $\text{Gal}(\overline{\mathbb{Q}}/k)$. All field extensions of k considered will be assumed to be algebraic and contained in $\overline{\mathbb{Q}}$. By ζ_r we will denote a primitive rth root of unity, and g will be an integer ≥ 1. We will work in the category of abelian varieties up to isogeny over k. This means that isogenies become invertible in this category and therefore, if A is an abelian variety defined over k, we will write $\text{End}(A)$ to denote the $\mathbb{Q}$-algebra of endomorphisms defined over k (what some authors write $\text{End}(A) \otimes \mathbb{Q}$ or $\text{End}^0(A)$). Similarly, if B is an abelian variety defined over k, then $\text{Hom}(A, B)$ will denote the $\mathbb{Q}$-vector space of homomorphisms from A to B that

are defined over k. Although isogenies will be the isomorphisms of our working category, we will still 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, and we will write $A_L \sim B_L$ if A and B become isogenous over L (in particular, we will write $\mathrm{Hom}(A_L, B_L)$ to refer to what some authors write as $\mathrm{Hom}_L(A, B)$). If C is an abelian variety over L, for short, we will say that C admits a model up to isogeny over k if there exists an abelian variety C_0 defined over k such that $C_{\overline{\mathbb{Q}}} \sim C_{0, \overline{\mathbb{Q}}}$. Finally, if $\mathcal{B}$ is an algebra we will denote by $Z(\mathcal{B})$ its center.

Acknowledgments. Fité is thankful to CIRM and ICERM for invitations in May and in September of 2015, respectively, which facilitated fruitful conversations with Drew Sutherland regarding this work. Thanks to Carlos de Vera, Elisa Lorenzo, and Mark Watkins for helpful comments. We are thankful to Kiran Kedlaya and Jordi Quer for their inspiring suggestions, specially regarding the proof of Corollary 2.17.

2. Fields of definition of elliptic k-curves

In this section we study fields of definition up to isogeny of certain elliptic curves E with CM. Namely, those with the property that the CM field is contained in k and such that E^g admits a model up to isogeny over k. The main tool that we use is to exploit the fact that, in this setting, E is an elliptic k-curve.

2.1. **Preliminary results on k-varieties.** In this section we collect some background and preliminary results on abelian k-varieties. In fact, we are mainly interested in the 1-dimensional case of elliptic k-curves. The reader can consult [Rib94], [Que00], and [Pyl02] as general references for k-curves and k-varieties.

Definition 2.1 (After Ribet). An abelian variety $B/\overline{\mathbb{Q}}$ is called an abelian k-variety (or just a k-variety, for short) if for all $\sigma \in G_k$ there exists an isogeny $\mu_\sigma \colon {}^\sigma B \to B$ which is compatible with $\mathrm{End}(B)$, in the sense that the diagram

$$(2.1) \qquad \begin{array}{ccc} {}^\sigma B & \xrightarrow{\mu_\sigma} & B \\ \downarrow{}^{\sigma}\varphi & & \downarrow \varphi \\ {}^\sigma B & \xrightarrow{\mu_\sigma} & B \end{array}$$

commutes for all $\varphi \in \mathrm{End}(B)$.

A simple calculation shows that the property of being a k-variety only depends on the $\overline{\mathbb{Q}}$-isogeny class of B. In fact, if K is an extension of k one says that B is a k-variety defined over K if B is defined over K and $B_{\overline{\mathbb{Q}}}$ is a k-variety.

Let B be a k-variety with endomorphism algebra $\mathcal{B} = \mathrm{End}(B)$, and let $R = Z(\mathcal{B})$ denote its center. The variety B has a model defined over a number field. By enlarging this field if necessary, we can assume that it is also a field of definition of the isogenies between B and its conjugates. Thus we can (and do) fix a system of compatible isogenies $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$ which is locally constant. For every $\sigma, \tau \in G_k$ define

$$c_B(\sigma, \tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}.$$

A short computation shows that $c_B(\sigma, \tau)$ lies in R^*, and that the map

$$\sigma, \tau \mapsto c_B(\sigma, \tau)$$

is a continuous 2-cocycle of G_k with values in R^* (considered as a G_k-module with trivial action). Denote by $\gamma_B \in H^2(G_k, R^*)$ the cohomology class of c_B. To the best of our knowledge this cohomology class was introduced by Ribet in [Rib92], and it is one of the main tools for studying the arithmetic of k-varieties. The next proposition summarizes some of the main properties of c_B and γ_B.

Proposition 2.2. *i) If c'_B is a cocycle cohomologous to c_B, there exist compatible isogenies $\lambda_\sigma \colon {}^\sigma B \to B$ such that $c'_B(\sigma, \tau) = \lambda_\sigma \circ {}^\sigma\lambda_\tau \circ \lambda_{\sigma\tau}^{-1}$.*

ii) The cohomology class $\gamma_B \in H^2(G_k, R^*)$ only depends on the $\overline{\mathbb{Q}}$-isogeny class of B. More precisely, if $\beta \colon A \to B$ is an isogeny, then $\gamma_A = \gamma_B$, under the identification of centers $Z(\mathcal{B}) \simeq Z(\mathrm{End}(A))$ provided by β.

iii) For every $n \in \mathbb{Z}_{\geq 1}$ the isotypical variety B^n is also a k-variety, and $\gamma_B = \gamma_{B^n}$, under the identification $Z(\mathcal{B}) \simeq Z(\mathcal{B}^n)$.

Proof. For *i)*, the cocycle c'_B can be written as $c'_B(\sigma, \tau) = c_B(\sigma, \tau) \circ a_\sigma \circ a_\tau \circ a_{\sigma\tau}^{-1}$ for some $a_\sigma, a_\tau, a_{\sigma\tau} \in R^*$. Then, for every $s \in G_k$ the isogeny $\lambda_s = a_s \circ \mu_s$ is compatible, because $a_s \in R^*$, and it satisfies the required property.

As for *ii)* one can define isogenies $\lambda_\sigma \colon {}^\sigma A \to A$ as $\lambda_\sigma = \beta^{-1} \circ \mu_\sigma \circ {}^\sigma\beta$. It is easy to check that they are compatible and that $c_A(\sigma, \tau) = \beta^{-1} \circ c_B(\sigma, \tau) \circ \beta$.

Finally, *iii)* is proved by considering the isogenies $\mu_\sigma^{\oplus n} \colon {}^\sigma B^n \to B$, which are compatible and can be thus used to compute $c_{B^n}(\sigma, \tau)$, which is seen to coincide with $c_B^{n\oplus}$. $\qquad\square$

Proposition 2.3. *Let $B/\overline{\mathbb{Q}}$ be a simple abelian k-variety and suppose that $\mathrm{End}(B)$ has Schur index t. Suppose that there exists a variety A/k such that $A_{\overline{\mathbb{Q}}} \sim B^n$. Then γ_B lies in $H^2(G_k, R^*)[nt]$; that is, $(\gamma_B)^{nt} = 1$.*

Proof. Let $\{\mu_\sigma \colon {}^\sigma B \to B\}_{\sigma \in G_k}$ be a compatible system of isogenies and let $c_B(\sigma, \tau) = \mu_\sigma \circ {}^\sigma\mu_\tau \circ \mu_{\sigma\tau}^{-1}$ be the corresponding cocycle. By Proposition 2.2 *ii)* we have that $A_{\overline{\mathbb{Q}}}$ is a k-variety as well, and therefore there exists a compatible system of isogenies $\alpha_\sigma \colon {}^\sigma A \to A$ such that

$$(2.2) \qquad\qquad c_A(\sigma, \tau) = \alpha_\sigma \circ {}^\sigma\alpha_\tau \circ \alpha_{\sigma\tau}^{-1}.$$

Since A is defined over k, we see that α_s lies in $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ for every $s \in G_k$. In particular, the compatibility condition applied to the endomorphism α_τ then reads ${}^\sigma\alpha_\tau = \alpha_\sigma^{-1} \circ \alpha_\tau \circ \alpha_\sigma$. Plugging this into (2.2) gives

$$c_A(\sigma, \tau) = \alpha_\tau \circ \alpha_\sigma \circ \alpha_{\sigma\tau}^{-1}.$$

Now by Proposition 2.2 *ii)* we have that $\gamma_A = \gamma_{B^n}$; by *iii)* we also see that $\gamma_A = \gamma_B$ and by *i)* we can in fact assume that the cocycles are equal:

$$(2.3) \qquad\qquad c_B(\sigma, \tau) = c_A(\sigma, \tau) = \alpha_\tau \circ \alpha_\sigma \circ \alpha_{\sigma\tau}^{-1},$$

where the term $c_B(\sigma, \tau)$ is seen as lying in $\mathrm{End}(A_{\overline{\mathbb{Q}}})$ by means of the identification $R \simeq Z(\mathrm{End}(A_{\overline{\mathbb{Q}}}))$. In turn, we can interpret (2.3) as an equality in $\mathrm{M}_n(\mathcal{B})$ thanks to the isomorphism $\mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \mathrm{M}_n(\mathcal{B})$. Now we take reduced norms and we use the fact that $c_B(\sigma, \tau)$ lies in F, so that its reduced norm equals $c_B(\sigma, \tau)^{nt}$. Thus we obtain:

$$c_B(\sigma, \tau)^{nt} = \mathrm{nr}(\alpha_\tau) \circ \mathrm{nr}(\alpha_\sigma) \circ \mathrm{nr}(\alpha_{\sigma\tau})^{-1}.$$

This expresses c_B^{nt} as the coboundary of the map $s \mapsto \mathrm{nr}(\alpha_s) \in R^*$. $\qquad\square$

Corollary 2.4. *Suppose that A/k is an abelian variety such that $A_{\overline{\mathbb{Q}}} \sim C^g$, for some k-curve $C/\overline{\mathbb{Q}}$. Then γ_C lies in $H^2(G_k, R^*)[g]$.*

Proof. It follows directly from the fact that $\mathrm{End}(C)$ has Schur index 1. $\qquad\square$

Remark 2.5. Ribet showed [Rib94, Prop. 3.2] that if C is a k-curve without CM then γ_C has order dividing 2. This is not true in general for CM k-curves. The point of Corollary 2.4 is that an analogous statement holds in the case that C has CM and C^g admits a model up to isogeny defined over k.

Proposition 2.6. *Let $L \subset \overline{\mathbb{Q}}$ be an extension of k and let A/L be a k-variety. Then $Z(\mathrm{End}(A_{\overline{\mathbb{Q}}})) \subseteq \mathrm{End}(A)$.*

Proof. For all $\sigma \in G_L$ we have that $^{\sigma}A = A$. Then the isogeny $\mu_{\sigma} \colon {}^{\sigma}A \to A$ can be identified with an element of $\mathrm{End}(A)$. For any $\varphi \in Z(\mathrm{End}(A_{\overline{\mathbb{Q}}}))$ we have that $^{\sigma}\varphi = \mu_{\sigma}^{-1} \circ \varphi \circ \mu_{\sigma} = \varphi$. $\qquad\square$

The main examples of k-varieties that we will consider in this note are CM elliptic curves whose field of CM is contained in k. The following result is well-known (it follows, for instance, from [Sil94, Thm. 2.2]).

Proposition 2.7. *Let E/L be an elliptic curve with CM by an imaginary quadratic field M. If L contains M, then E is an M-curve. In particular, it is a k-curve for any k containing M.*

For further reference, we record the following consequence of the results we have seen so far.

Proposition 2.8. *Let A be an abelian surface defined over a number field k. Suppose that $A_{\overline{\mathbb{Q}}} \sim E^2$, where E is an elliptic curve with CM by M, and assume that $M \subseteq k$. Then $Z(\mathrm{End}(A_{\overline{\mathbb{Q}}})) \subseteq \mathrm{End}(A)$.*

Proof. Since E is a CM elliptic curve defined over an extension of k and $M \subseteq k$ we see that E is a k-curve. Now by Proposition 2.2 A is also a k-variety, and the result is then a direct consequence of Proposition 2.6. $\qquad\square$

We will use the notion of k-varieties completely defined over a field, a terminology which was introduced in [Que00, p. 2].

Definition 2.9. Let B be a k-variety defined over a number field K. One says that B is completely defined over K if there exist compatible isogenies $\{\mu_{\sigma}\}_{\sigma \in G_k}$ that are defined over K.

If B is completely defined over K the map

$$(2.4) \qquad c_B^K \colon \mathrm{Gal}(K/k) \times \mathrm{Gal}(K/k) \longrightarrow R^*, \quad c_B^K(\sigma, \tau) = \mu_{\sigma} \circ {}^{\sigma}\mu_{\tau} \circ \mu_{\sigma\tau}^{-1}$$

is a two-cocycle and its cohomology class $\gamma_B^K \in H^2(\mathrm{Gal}(K/k), R^*)$ only depends on the K-isogeny class of B.

Remark 2.10. It follows from the definitions that the image of γ_B^K under the inflation map $H^2(\mathrm{Gal}(K/k), R^*) \to H^2(G_k, R^*)$ is precisely the cohomology class γ_B defined earlier. In many applications, for instance when one is interested in studying properties of the K-isogeny class of B, it is important to work with the cohomology class γ_B^K.

2.2. **Powers of CM elliptic k-curves.** Throughout this section, let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by a quadratic imaginary field M such that E^g is $\overline{\mathbb{Q}}$-isogenous to an abelian variety A defined over k. Assume that M is contained in k. Note that, in view of Proposition 2.7, E is a k-curve.

Let K/k denote the smallest extension such that $\operatorname{End}(A_K) = \operatorname{End}(A_{\overline{\mathbb{Q}}})$. The main result of this section is Theorem 2.14, which ensures the existence of an abelian subextension of K/k with Galois group killed by g over which E admits a model up to isogeny.

Remark 2.11. Ribet [Rib94] and Elkies [Elk04] have given two alternative proofs of the fact that any k-curve without CM admits a model up to isogeny defined over a polyquadratic extension of k. Theorem 2.14 may be seen as a extension of Ribet's and Elkies' result to the case in which E has CM, but under the restrictive assumption that E^g admits a model up to isogeny over k.

Before proceeding to the proof of Theorem 2.14, we introduce some notation and we recall Weil's descent criterion, a fundamental result in our arguments.

Note that the definition of K/k implies that $A_K \sim E_1^g$, where E_1 is an elliptic curve defined over K. Since

$$^{\sigma}E_1^g \sim {}^{\sigma}A_K \sim A_K \sim E_1^g \,,$$

for $\sigma \in G_k$, by Poincaré's decomposition theorem there exists an isogeny

$$\mu_\sigma \colon {}^{\sigma}E_1 \to E_1$$

defined over K. Note that E_1 is a model of E up to isogeny defined over K. Even more, according to the terminology of Definition 2.9, E_1 is an elliptic k-curve completely defined over K. Define the 2-cocycle

$$c_{E_1} \colon G_k \times G_k \to M^* \,, \qquad c_{E_1}(\sigma, \tau) = \mu_\sigma \circ {}^{\sigma}\mu_\tau \circ \mu_{\sigma\tau}^{-1},$$

and let $\gamma = \gamma_{E_1}$ denote its cohomology class in $H^2(G_k, M^*)$. By Remark 2.10, the class γ lies in the image of the inflation map

$$\operatorname{Inf} \colon H^2(\operatorname{Gal}(K/k), M^*) \longrightarrow H^2(G_k, M^*).$$

The following result [Rib92, Thm. 8.2], written in the spirit of [Rib94, Prop. 3.1], is crucial for our purposes.

Proposition 2.12 (Weil's descent criterion)**.** *Let F/k be an algebraic extension. If γ lies in the kernel of the restriction map*

$$H^2(G_k, M^*) \to H^2(G_F, M^*) \,,$$

then E_1 admits a model up to isogeny defined over F.

Proof. Of course it is enough to prove that $\gamma = 1$, implies that E_1 admits a model up to isogeny defined over k. But $\gamma = 1$ means that there is a locally constant function $d \colon G_k \to M^*$ such that $c_{E_1}(\sigma\tau) = d(\sigma)d(\tau)/d(\sigma\tau)$. Then the isogenies $\lambda_\sigma := 1/d(\sigma) \circ \mu_\sigma$ satisfy $\lambda_\sigma \circ {}^{\sigma}\lambda_\tau \circ \lambda_{\sigma\tau}^{-1} = 1$, and then one concludes by applying [Rib92, Thm. 8.2]. $\qquad\square$

Remark 2.13. Let $\gamma^K \in H^2(\operatorname{Gal}(K/k), M^*)$ be the cohomology class constructed as in (2.4). Since γ^K is constructed in terms of isogenies that are defined over K,

the argument above can be adapted to show that if F/k is subextension of K/k and γ^K lies in the kernel of the restriction map

$$H^2(\mathrm{Gal}(K/k), M^*) \longrightarrow H^2(\mathrm{Gal}(K/F), M^*),$$

then E_1 is K-isogenous to an elliptic curve defined over F.

Theorem 2.14. *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by a quadratic imaginary field M such that E^g, for $g \geq 1$, is $\overline{\mathbb{Q}}$-isogenous to an abelian variety A defined over k. Assume that M is contained in k. Let H denote the Hilbert class field of M and write $F = Hk$. Then, E admits a model up to isogeny defined over the abelian subextension F/k of K/k and every element of $\mathrm{Gal}(F/k)$ has order dividing g.*

Proof. Of course, it is enough to prove the equivalent statement for E_1 (where E_1 is attached to E as above). We will follow the strategy of [Rib94, Thm. 3.3]. Although, Ribet's result is stated under different hypotheses, we will show that $\gamma = \gamma_{E_1}$ lying in $H^2(G_k, M^*)[g]$ is essentially all that is needed to run his argument. Let U denote the group of roots of unity[2] of M and write $P := M^*/U$. As in [Rib94, Lemma 3.5], it follows from Dirichlet's unit theorem that P is a free abelian group. Therefore, the exact sequence

$$1 \to U \to M^* \to P \to 1$$

is split. This yields a decomposition

(2.5) $$H^2(G_k, M^*)[g] \simeq H^2(G_k, U)[g] \times \mathrm{Hom}(G_k, P/P^g) \,.$$

Indeed, the long exact cohomology sequence associated to the exact sequence

$$1 \to P \xrightarrow{x \mapsto x^g} P \to P/P^g \to 1 \,,$$

together with the freeness of P, implies that we have an isomorphism

$$H^2(G_k, P)[g] \simeq \mathrm{Hom}(G_k, P/P^g) \,.$$

Note that by Corollary 2.4, the class γ belongs to $H^2(G_k, M^*)[g]$. Let γ_U (resp. $\overline{\gamma}$) be the projection of γ onto the first (resp. second) factor of the decomposition (2.5). Since γ is the inflation of a class in $H^2(\mathrm{Gal}(K/k), M^*)$, we see that the component $\overline{\gamma}$ lies in the image of the inflation map

$$\mathrm{Inf}\colon \mathrm{Hom}(\mathrm{Gal}(K/k), P/P^g) \longrightarrow \mathrm{Hom}(G_k, P/P^g).$$

In particular, if we let L be the subfield of K fixed by the subgroup of $\mathrm{Gal}(K/k)$ generated by the g-th powers of the elements of $\mathrm{Gal}(K/k)$, it is clear that the restriction of $\overline{\gamma}$ to G_L is trivial. But now, by Lemma 2.15 below, γ is trivial over G_L and thus, by Proposition 2.12, E_1 admits a model E_2 over L up to isogeny. Let $\mathcal{O}_c$ be the order, say of conductor c, by which E_2 has CM, and let $H_c = M(j(E_2))$ denote the ray class field of conductor c of M. Since E_2 is defined over L, we have

(2.6) $$kH_c = k(j(E_2)) \subseteq L.$$

Let $\mathcal{O}$ be the maximal order of M and let E^* be an elliptic curve with CM by $\mathcal{O}$ defined over $F = kH$. Note that E^* is $\overline{\mathbb{Q}}$-isogenous to E_2. We have

(2.7) $$F = k(j(E^*)) = kH \subseteq kH_c.$$

---

[2]More explicitly, $U = \{\pm 1\}$, unless E_1 has CM by $M = \mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-3})$, in which case $U = \langle \zeta_4 \rangle$ or $\langle \zeta_6 \rangle$, respectively.

The theorem now follows from (2.6), (2.7), and the fact that $\mathrm{Gal}(L/k)$ is killed by g. $\qquad \square$

Lemma 2.15. *With the notations as in the proof of Theorem 2.14, if $\overline{\gamma}$ trivializes over a subextension L/k of K/k, then so does γ_U. That is, if $\overline{\gamma}$ has trivial restriction to $H^2(G_L, M^*)$, then so does γ_U.*

Proof. It is enough to prove that if $\overline{\gamma} = 1$ then $\gamma_U = 1$. To show this, we will follow Ribet again. As proven in [Rib94, §4], we have

$$H^1(G_k, (M \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})^*) = 1, \quad H^2(G_k, (M \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})^*) \simeq H^2(G_k, \overline{\mathbb{Q}}^*) \oplus H^2(G_k, \overline{\mathbb{Q}}^*),$$

where G_k acts trivially on M and via the natural Galois action on $\overline{\mathbb{Q}}$.

Then, the exact sequence

$$1 \to M^* \to (M \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})^* \to (M \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})^*/M^* \to 1,$$

yields the following long exact sequence in cohomology

$$1 \to H^1(G_k, (M \otimes_{\mathbb{Q}} \overline{\mathbb{Q}})^*/M^*) \xrightarrow{\delta} H^2(G_k, M^*) \to H^2(G_k, \overline{\mathbb{Q}}^*) \oplus H^2(G_k, \overline{\mathbb{Q}}^*) \to \cdots .$$

As in [Rib94, Lem. 4.3], one finds that γ lies in the image of δ. Indeed, in our case $M \otimes \overline{\mathbb{Q}} \simeq \overline{\mathbb{Q}} \oplus \overline{\mathbb{Q}}$ as G_k-modules. Fix an invariant differential ω of E_1. For every $\sigma \in G_k$ there is a unique $\lambda_\sigma \in \overline{\mathbb{Q}}$ characterized by the identity $\mu_\sigma^*(\omega) = \lambda_\sigma \cdot {}^\sigma \omega$. Then the map $\sigma \mapsto (\lambda_\sigma, \overline{\lambda}_\sigma)$, where the bar stands for complex conjugation, gives rise to a cohomology class in $H^1(G_k, (M \otimes \overline{\mathbb{Q}})^*/M)$, whose image under δ coincides with γ.

Since $\overline{\gamma}$ is trivial, this means that γ_U lies in the kernel of the map

$$j\colon H^2(G_k, U)[g] \to H^2(G_k, \overline{\mathbb{Q}}^*) \oplus H^2(G_k, \overline{\mathbb{Q}}^*).$$

Observe that U is contained in k so that the trivial action of G_k on U coincides with the natural Galois action. Since $H^2(G_k, U) \simeq H^2(G_k, \overline{\mathbb{Q}}^*)[n]$ (here $\overline{\mathbb{Q}}$ is endowed with the natural Galois action of G_k, and n is the cardinality of U), we see that j is injective and thus γ_U must be trivial. $\qquad \square$

Corollary 2.16. *Let A be an abelian variety defined over $\mathbb{Q}$ of dimension g that is $\overline{\mathbb{Q}}$-isogenous to E^g, where E is an elliptic curve over $\overline{\mathbb{Q}}$ with CM by M. Then every element in $\mathrm{Cl}(M)$ has order dividing g.*

Proof. Applying Theorem 2.14 to the base change A_M of A to M, we deduce that every element in $\mathrm{Gal}(H/M)$ has order dividing g, where H stands for the Hilbert class field of M. The corollary follows from the fact that $\mathrm{Gal}(H/M)$ is isomorphic to $\mathrm{Cl}(M)$. $\qquad \square$

Corollary 2.17. *Let A be an abelian variety defined over $\mathbb{Q}$ that is $\overline{\mathbb{Q}}$-isogenous to E^g, where E is an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by a quadratic imaginary field M and g is a prime number. Then*

$$\mathrm{Cl}(M) = \begin{cases} 1, \mathrm{C}_g, \text{ or } \mathrm{C}_g \times \mathrm{C}_g & \text{if } g = 2, \\ 1 \text{ or } \mathrm{C}_g & \text{otherwise.} \end{cases}$$

In particular, if $g = 2$, there are at most 51 possibilities for M.

Proof. By Corollary 2.16, the group $\mathrm{Cl}(M)$ is a quotient of $\mathrm{Gal}(K/M)$ of the form $C_g{}^r$, for some $r \geq 0$. For $g = 2$, the possibilities for $\mathrm{Gal}(K/M)$ are well known (see Remark 3.1 in the next section, for example) and it turns out that $r \leq 2$. It is well known that the number of quadratic imaginary fields with class group isomorphic to the trivial group, C_2, $C_2 \times C_2$ are respectively 9, 18, 24 (see Table 3 for the complete list).

Suppose now that $g \geq 3$. For p a prime number, define

$$(2.8) \qquad r(g,p) := \sum_{j \geq 0} \left\lfloor \frac{2g}{p^j(p-1)} \right\rfloor .$$

By [Sil92, Thm. 4.1], the maximal power of p dividing the order of $\mathrm{Gal}(K/M)$ is $r(g,p)$. Guralnick and Kedlaya [GK16, Thm. 1.1] have shown that the same holds true if one replaces $r(g,p)$ by

$$r'(g,p) := \begin{cases} r(g,p) - g - 1 & \text{if } p = 2, \\ \max\{r(g,p) - 1, 0\} & \text{if } p \text{ is a Fermat prime}, \\ r(g,p) & \text{otherwise.} \end{cases}$$

This bound is sharp in the context of general abelian varieties (see [GK16, Thm. 6.3]). However, if A is as in the statement of the corollary (that is, geometrically isogenous to the power of an elliptic curve with CM), one can do better. Indeed, one can specialize the proof of [GK16, Thm. 5.4] to the particular case in which $V \simeq W^g$ as G^0-modules, as in our setting $A_K \sim E_1^g$ for an elliptic curve E_1 defined over K. Therefore $\mathrm{End}_{G^0}(W) = M$, $\mathrm{End}_{G^0}(V) = \mathrm{M}_g(M)$, and $Z(\mathrm{End}_{G^0}(W)) = M$. In the notations of [GK16, Thm. 5.4], this is yields the values

$$a = 2, \qquad b = 1, \qquad c = g .$$

Then, one deduces that the maximal power of g dividing the order of $\mathrm{Gal}(K/M)$ is bounded by

$$r(\mathrm{GL}(bc)_M, g) = r(\mathrm{GL}(g)_M, g) := m(M,g) \left\lfloor \frac{g}{t(M,g)} \right\rfloor + \left\lfloor \frac{1}{t(M,g)} \right\rfloor ,$$

where, as defined in [GK16, Rmk. 3.6], we have

$$m(M,g) := \min\{m \geq 1 \mid M \cap \mathbb{Q}(\mu_{g^m}) = M \cap \mathbb{Q}(\mu_{g^\infty})\}$$

and

$$t(M,g) := [\mathbb{Q}(\mu_{g^{m(M,g)}}) : M \cap \mathbb{Q}(\mu_{g^{m(M,g)}})] .$$

Since $\mathbb{Q}(\mu_{g^{m(M,g)}})$ ramifies only at g, we have that either $t(M,g) = g^{m(M,g)-1}(g-1)$ or $M = \mathbb{Q}(\sqrt{-g})$ and $g \equiv 3 \pmod 4$. In the first case, one trivially checks that $r(\mathrm{GL}(g)_M, g) \leq 1$ (here we use $g \neq 2$). In the second case, $\mathrm{Cl}(M)$ is necessarily trivial; indeed, by the reduction theory of positive definite binary quadratic forms (see for example [Cox89, Chap. I, §2]) one knows that $\mathrm{Cl}(M) \leq \frac{2}{3}g$. $\qquad \square$

Remark 2.18. There is a finite number of quadratic imaginary fields of fixed class number (see [Hei34]). Using Sage and Pari one can compute the number of imaginary quadratic fields with class group C_g, for $3 \leq g \leq 97$ prime, relying on the bounds for their fundamental discriminants provided by [Wat03, Table 4].

Remark 2.19. Also for g not necessarily prime, one can proceed as in the proof of Corollary 2.17 to gain control on the size of $\mathrm{Cl}(M)$. In general, one obtains that $\mathrm{Cl}(M)$ has exponent dividing g and order dividing $\prod_{p|g} p^{r'(g,p)}$.

Remark 2.20. One may wonder which of the cases allowed by Corollary 2.17 actually arise. By taking g-th powers (resp. Weil restrictions of scalars) of elliptic curves it is clear that all quadratic imaginary fields of class number 1 (resp. with class group C_g) do appear. It would be an interesting problem to determine the exact set of possibilities for the M with $Cl(M) \simeq C_2 \times C_2$ for which an abelian surface A as in the corollary exists.

The above corollary answers part (A) of Question 1.2. Providing an answer to part (B) of the question for $g = 2$ will be the goal of §3. Before, for the sake of completeness, we state a result analogous to Theorem 2.14 for the non-CM case.

Theorem 2.21. *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ without CM such that E^g is $\overline{\mathbb{Q}}$-isogenous to an abelian variety A defined over k. Then E admits a model up to isogeny defined*

i) over k if g is odd; or
ii) over a polyquadratic subextension of K/k if g is even.

Proof. Let γ denote the cohomology class attached to E. On the one hand, by Proposition 2.3, the class γ^g is trivial. On the other hand, [Rib94, Prop. 3.2] asserts that γ has order dividing 2. Proposition 2.12 implies then that i) holds. It is straightforward to adapt the proof of Theorem 2.14 to justify that the polyquadratic extension over which γ trivializes is in fact contained in K/k. □

3. The case of dimension $g = 2$

In this section, E will denote an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by a quadratic imaginary field M such that E^2 is $\overline{\mathbb{Q}}$-isogenous to an abelian surface A defined over k. We assume that M is contained in k, so that E is a k-curve, and we let K/k denote the smallest extension such that $End(A_K) = End(A_{\overline{\mathbb{Q}}})$.

Our goal is to obtain a more precise version of Corollary 2.17. This will be achieved by Theorem 3.21. We will benefit from the fact that for $g = 2$, the structure of $Gal(K/k)$ is very well understood.

Remark 3.1. It is well known that if $M \subseteq k$ the possibilities for $Gal(K/k)$ are the cyclic group C_n for $n \in \{1, 2, 3, 4, 6\}$, the dihedral group D_n for $n \in \{2, 3, 4, 6\}$, the alternating group A_4, and the symmetric group S_4. There are at least two ways in which this can be deduced: first, by means of the analysis of the finite subgroups of $PGL_2(M)$, (see [Bea10], [CF00]); second, as a byproduct of the classification of Sato–Tate groups of abelian surfaces (see [FKRS12, §4]).

Let $r(A)$ be defined in terms of $Gal(K/k)$ as specified on Table 1. In other words, $r(A)$ is the maximum value of r for which there exists a Galois subextension F/k of K/k with $Gal(F/k) \simeq C_2{}^r$.

Proposition 3.2. *Let E be an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by a quadratic imaginary field M such that E^2 is $\overline{\mathbb{Q}}$-isogenous to an abelian surface A/k. Assume that $M \subseteq k$. Then E admits a model up to isogeny E^* defined over a Galois subextension F/k of K/k such that $Gal(F/k) \simeq C_2{}^{r(A)}$.*

The above proposition can certainly be deduced from Theorem 2.14 and Remark 3.1, but we wish to present a slightly different argument that renders, for $g = 2$, a shortcut in the proof.

$r(A)$	$\mathrm{Gal}(K/k)$	$r(A)$	$\mathrm{Gal}(K/k)$
0	C_1	2	D_2
1	C_2	1	D_3
0	C_3	2	D_4
1	C_4	2	D_6
1	C_6	0	A_4
		1	S_4

TABLE 1. The rank $r(A)$ in terms of $\mathrm{Gal}(K/k)$.

Proof. Recover decomposition (2.5), specialize it to $g = 2$, and resume with the final argument in the proof of [Rib94, Thm. 3.3]. If $\mathrm{Br}(k)$ denotes the Brauer group of k, then we have

$$H^2(G_k, M^*)[2] \simeq \mathrm{Br}(k)[2] \times \mathrm{Hom}(G_k, P/P^2)\,.$$

If we let $\gamma = \gamma_E$ denote the cohomology class attached to E and $(\gamma_U, \overline{\gamma})$ its components under the above decomposition, then $\overline{\gamma}$ factors through a polyquadratic extension k' of k. Moreover, a theorem of Merkur'ev [Mer81] shows that $\mathrm{Br}(k)[2]$ is generated by the classes of quaternion algebras over k, and it is well known that each quaternion algebra over k is split over a quadratic extension of k. Proposition 2.12 thus tells us that E admits a model E_2 up to isogeny over a polyquadratic extension k_2/k.

Now let E_1/K be an elliptic curve such that $A_K \sim E_1^2$. We thus have that

(3.1) $$\mathbb{Q}(j(E_1)) \subseteq K \quad \text{and} \quad \mathbb{Q}(j(E_2)) \subseteq k_2\,.$$

We can now conclude in a similar manner as we did with the proof of Theorem 2.14. Let $\mathcal{O}$ be the maximal order of M and let E^* be an elliptic curve with CM by $\mathcal{O}$. Both E_1 and E_2 are $\overline{\mathbb{Q}}$-isogenous to E^*. Let $\mathcal{O}_i$ denote the order by which E_i has CM, for $i = 1, 2$, and let c_i be its conductor. Since the ray class field $H_{c_i} = M(j(E_i))$ of conductor c_i contains the Hilbert class field $H = M(j(E^*))$, we have that $M(j(E^*)) \subseteq M(j(E_i))$. It follows from (3.1) that

$$F := k(j(E^*)) \subseteq K \cap k_2\,.$$

Since $[K \cap k_2 : k] \leq 2^{r(A)}$, we have that E_F^* is a model up to isogeny of E enjoying the properties stated in the proposition. $\qquad\square$

Remark 3.3. It follows from the above proof that any elliptic curve with CM by the maximal order of M can be taken as the model E^* of Proposition 3.2, in which case F can be taken equal to $k(j(E^*))$.

Remark 3.4. If E does not have CM, then the possibilities for $\mathrm{Gal}(K/k)$ are those of Remark 3.1 excluding A_4 and S_4. Theorem 2.21 has then the following consequence. Let E be an elliptic curve without CM defined over $\overline{\mathbb{Q}}$ such that E^2 has a model up to isogeny defined over k. Then E admits a model up to isogeny E^* defined over a biquadratic subextension F/k of K/k.

In the following §3.1 and §3.2, we will gather constraints on the field M imposed by $\mathrm{Gal}(K/M)$. In §3.3, we will achieve a refinement of Corollary 2.17 by putting together Proposition 3.2 and all of these constraints.

3.1. **Galois module structures: group representation obstructions.** We continue with the same notation for A, E, K/k, and M. By Proposition 3.2, E admits a model up to isogeny E^* defined over a subextension F/k of K/k. We will consider the following hypotheses:

(H_4) $\mathrm{Gal}(K/F)$ contains an element τ of order 4.
(H_6) $\mathrm{Gal}(K/F)$ contains an element τ of order 6.
(A_4) $\mathrm{Gal}(K/F)$ contains A_4.
(S_4) $\mathrm{Gal}(K/F)$ contains S_4 (equivalently, $\mathrm{Gal}(K/F) \simeq S_4$).

The main result of this section is the following proposition, which imposes conditions on M in terms of $\mathrm{Gal}(K/F)$.

Proposition 3.5. *One has:*

  i) If (H_4) holds, then $M = \mathbb{Q}(\sqrt{-1})$ or $M = \mathbb{Q}(\sqrt{-2})$.
  ii) If (H_6) holds, then $M = \mathbb{Q}(\sqrt{-3})$.
  iii) If (A_4) holds, then M splits the quaternion algebra $(-1, -1)_{\mathbb{Q}}$. [3]
  iv) If (S_4) holds, then $M = \mathbb{Q}(\sqrt{-2})$.

The proof is built on some results of [FS14], which we now recall. We note also that the proofs of statements *i)* and *ii)*, and of *iii)* and *iv)* require slightly different techniques, so we will treat them separately. First, let us introduce some notations and make some basic observations. Denote by L/F the minimal extension over which $\mathrm{Hom}(E_L^*, A_L) \simeq \mathrm{Hom}(E_{\overline{\mathbb{Q}}}^*, A_{\overline{\mathbb{Q}}})$. Observe that K is contained in L.

Lemma 3.6. *One has that $\mathrm{Gal}(L/K) \subseteq C_n$, where n is the number of roots of unity in M.*

Proof. First observe that L/F is a Galois extension by the minimality condition defining it. Let E_1 be an elliptic curve defined over K such that $A_K \sim E_1^2$. Then L/F may be characterized by the fact that L/K is the minimal extension over which E_1 and E_K^* become isogenous. Let $\psi \colon E_{1,\overline{\mathbb{Q}}} \to E_{\overline{\mathbb{Q}}}^*$ be an isogeny. Since G_K acts trivially on $M = \mathrm{End}(E_1)$, the map

$$\xi \colon G_K \to M^*, \qquad \xi(\sigma) := \psi^{-1} \circ {}^\sigma \psi$$

is a homomorphism. But then

$$\mathrm{Gal}(L/K) \simeq G_K / \ker(\xi) \simeq \mathrm{Im}(\xi) \subseteq C_n \,,$$

as desired. $\qquad\square$

Observe that the action of $M \simeq Z(\mathrm{End}(A_{\overline{\mathbb{Q}}}))$ on $\mathrm{Hom}(E_L^*, A_L)$ commutes with that of G_F, since $Z(\mathrm{End}(A_{\overline{\mathbb{Q}}})) \subseteq \mathrm{End}(A)$ by Proposition 2.8. By letting G_F act naturally on the first factor and trivially on M, the tensor product

$$\mathrm{Hom}(E_L^*, A_L) \otimes_{M, \iota} M \qquad (\text{resp.} \quad \mathrm{End}(A_L) \otimes_{M, \iota} M) \,,$$

taken with respect to any of the two automorphisms $\iota \in \{\mathrm{id}, c\}$ of M, becomes a $M[\mathrm{Gal}(L/F)]$-module of dimension 2 (resp. 4). Here, c denotes the non-trivial automorphism[4] of M. Let $\theta_\iota(E^*)$ (resp. $\theta_\iota(A)$) denote the representation afforded by this module.

Let $\pi \colon \mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$ be the natural projection. Note that $\theta_\iota(E^*)$ is (by the definition of L/F) a faithful representation of $\mathrm{Gal}(L/F)$, whereas $\theta_\iota(A)$

---

[3]Recall that $M = \mathbb{Q}(\sqrt{-d})$, with d square free, splits $(-1, -1)_{\mathbb{Q}}$ if and only if $d \not\equiv 7 \mod 8$.
[4]To ease notation, for $a \in M$, we will simply write $\bar{a}$ to denote ${}^c a$.

is only faithful (by the definition of K/k) as a representation of $\mathrm{Gal}(K/F)$. The following lemma is a restatement of [FS14, Prop. 3.2] and [FS14, Prop. 3.4] in our setting.

Lemma 3.7. *One has:*

i) $\mathrm{Tr}(\theta_\iota(A)) = \mathrm{Tr}(\theta_{\mathrm{id}}(E^*)) \cdot \mathrm{Tr}(\theta_c(E^*)) \in \mathbb{Q}$. *Thus, $\theta_{\mathrm{id}}(A) \simeq \theta_c(A) =: \theta(A)$.*

ii) *For $\sigma \in \mathrm{Gal}(L/F)$, let r denote the order of $\pi(\sigma)$. Then r is 1, 2, 3, 4, or 6, and*

$$\mathrm{Tr}(\theta(A)(\sigma)) = 2 + \zeta_r + \overline{\zeta}_r .$$

Proof of i) and ii) of Proposition 3.5. Let r denote the order (4 or 6) of τ. Let $\tilde{\tau} \in \mathrm{Gal}(L/F)$ be such that $\pi(\tilde{\tau}) = \tau$. Let ξ, ω be the eigenvalues of $\theta_\iota(E^*)(\tilde{\tau})$. Then, i) and ii) of Lemma 3.7, give

$$(3.2) \qquad\qquad (\xi + \omega)(\overline{\xi} + \overline{\omega}) = 2 + \zeta_r + \overline{\zeta}_r .$$

Without loss of generality, we may reorder ξ and ω so that (3.2) implies that $\xi = \zeta_r \omega$. The condition

$$\mathrm{Tr}(\theta_\iota(E^*)(\tilde{\tau})) = \omega(1 + \zeta_r) \in M$$

forces ω to belong to the biquadratic extension $M(\zeta_r)$. Therefore, there are only the following possibilities for the value of the order t of ω: 1, 2, 3, 4, 6, 8, 12. Suppose that $r = 4$. It is straightforward to check that:

- if $t = 1, 2, 4$, then $\omega(1 + \zeta_r) \in \mathbb{Q}(\sqrt{-1}) \setminus \mathbb{Q}$;
- if $t = 8$, then $\omega(1 + \zeta_r) \in \mathbb{Q}(\sqrt{-2}) \setminus \mathbb{Q}$;
- the values $t = 3, 6, 12$ are incompatible with $\omega(1 + \zeta_r)$ belonging to a quadratic imaginary field.

Suppose that $r = 6$. Then one readily checks that

- if $t = 1, 2, 3, 6$, then $\omega(1 + \zeta_r) \in \mathbb{Q}(\sqrt{-3}) \setminus \mathbb{Q}$;
- the values $t = 4, 8, 12$ are incompatible with $\omega(1 + \zeta_r)$ belonging to a quadratic imaginary field.

$\square$

Remark 3.8. One could wonder whether $\mathrm{Gal}(K/F)$ containing an element τ of order $r = 3$ imposes some condition on M. However, the argument of the proof of Proposition 3.5 can not be applied, since $\omega(1 + \zeta_r)$ make take the rational value $\zeta_3(1 + \zeta_3) = -1$.

Lemma 3.9. *One has:*

i) *If (A_4) holds and $M \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, then $\mathrm{Gal}(L/F)$ is isomorphic to the binary tetrahedral group $\mathrm{B_T}$.*

ii) *If (S_4) holds, then $\mathrm{Gal}(L/F)$ is isomorphic to either the binary octahedral group $\mathrm{B_O}$ or to the group[5] $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$.*

Proof. In the course of this proof, let us say that a finite group is *2-embeddable* if it possesses a faithful representation of dimension 2 with coefficients in $\overline{\mathbb{Q}}$. In case i), we have that L/K is at most quadratic by Lemma 3.6. The existence of the faithful representation $\theta_\iota(E^*)\colon \mathrm{Gal}(L/F) \to \mathrm{GL}_2(M)$ implies that $\mathrm{Gal}(L/F)$ is 2-embeddable (it fact, it implies a bit more: $\mathrm{Gal}(L/F)$ has a faithful representation

---

[5]The Gap identification numbers of $\mathrm{B_T}$, $\mathrm{B_O}$, and $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ are $\langle 24, 3\rangle$, $\langle 48, 28\rangle$, and $\langle 48, 29\rangle$, respectively.

of dimension 2 with coefficients in a quadratic imaginary field, but we will not need that). Since A_4 is not 2-embeddable, we have that $L \neq K$. There are two extensions of A_4 by C_2: B_T and $A_4 \times C_2$. The lemma then follows from the fact that $A_4 \times C_2$ is not 2-embeddable.

As for ii), we first note that (H$_4$) holds; then $M = \mathbb{Q}(\sqrt{-1})$ or $M = \mathbb{Q}(\sqrt{-2})$ by statement i) of Proposition 3.5. In particular Lemma 3.6 implies that $\mathrm{Gal}(L/K) \subseteq C_4$. There are nine groups that are extensions of S_4 by C_4, none of which is 2-embeddable. Since neither is S_4, we deduce that L/K is quadratic. Up to isomorphism, there are four extensions of S_4 by C_2, only two of which are 2-embeddable: B_O and $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$. $\qquad\square$

Proof of iii) and iv) of Proposition 3.5. Assume that we are in case *iii*). We may suppose that $M \neq \mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3})$, since in this case the proposition is trivially true. Then, by Lemma 3.9 we have a faithful representation

$$\theta_\iota(E^*)\colon B_T \to \mathrm{GL}_2(M).$$

Inspecting the character table of B_T, we realize that it has three faithful representations of dimension 2: one has rational trace (call it ϱ), and the other two have trace taking values in $\mathbb{Q}(\sqrt{-3}) \setminus \mathbb{Q}$ on elements of order 3 and 6. Since we have assumed that $M \neq \mathbb{Q}(\sqrt{-3})$, we have that $\theta_\iota(E^*) \simeq \varrho$. Let Q denote the subgroup of B_T isomorphic to the quaternion group. It is well-known that the restriction of ϱ to Q, sometimes called the quaternionic representation of Q, although having rational trace, is realizable over a field M if and only if M splits the quaternion algebra $(-1, -1)_\mathbb{Q}$ (see [Ser98, Cor. to Prop. 35]).

Case *iv*) is immediate from Lemma 3.9: one readily checks that the trace of any faithful representation of dimension 2 of B_O or $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ takes values in $\mathbb{Q}(\sqrt{-2}) \setminus \mathbb{Q}$ on elements of order 8. $\qquad\square$

3.2. Restriction of scalars: cohomological obstructions.
In this section, let M be an imaginary quadratic field of discriminant D. Assume that

(0) D is different from $-3, -4$, and -8.

Suppose that A/k is an abelian surface satisfying the following conditions:

(1) k contains M;
(2) $A_K \sim E^2$, where E/K is an elliptic curve with CM by M;
(3) the field K is the smallest such that $\mathrm{End}(A_K) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$; and
(4) the Galois group $G = \mathrm{Gal}(K/k)$ is isomorphic to S_4.

Note that E is then a k-curve completely defined over K (cf. Definition 2.9). Let $\gamma_E^K \in H^2(G, M^*)$ be the cohomology class attached to E as in (2.4). Since K will be fixed through this section, let us denote γ_E^K simply by γ_E.

In §3.1 we have found that the above assumptions impose conditions on the field M. For example, since condition (A$_4$) holds, Proposition 3.5 implies that M necessarily splits the quaternion algebra $(-1, -1)_\mathbb{Q}$. The goal of this section is to give some more necessary conditions on M, under the following additional condition (which we assume from now on):

(NE) If D is even, then it is either divisible by 8 or by some prime $p \equiv 3 \mod 4$.

Recall the model E^* of E up to isogeny introduced in Remark 3.3. It is any elliptic curve with CM by the maximal order of M and defined over the field $F = k(j_{E^*})$.

We next show that condition (NE) allows for a particular choice of E^* that will be key to our computations.

First of all we note that $[F : k] = 2$. Indeed, F/k is a polyquadratic extension and, since $F \subseteq K$, we see that $[F : k]$ is either 1 or 2. If $F = k$, then Proposition 3.5 implies that $M = \mathbb{Q}(\sqrt{-2})$, which contradicts our assumption (0); therefore we must have $[F : k] = 2$. Let H be the Hilbert class field of M. Thanks to the assumption (NE), by [Gro80, §11] there exists an elliptic curve $\tilde{E}/H$ with CM by M that is H-isogenous to its $\mathrm{Gal}(H/\mathbb{Q})$-conjugates. Since $H \subseteq F$, we can (and do) take as E^* the curve $\tilde{E}_F$.

For this particular choice, E^* is a k-curve completely defined over F; namely, E^* is F-isogenous to its $\mathrm{Gal}(F/k)$-conjugate. In particular, the cohomology class $\gamma_{E^*} = \gamma_{E^*}^K$ lies in the image of the inflation map

$$H^2(\mathrm{Gal}(F/k), M^*) \to H^2(G, M^*),$$

and a cocycle c_{E^*} representing γ_{E^*} is of the form

$$(3.3) \qquad c_{E^*}(\sigma, \tau) = \begin{cases} m \text{ if } \sigma_{|F} \neq \mathrm{Id} \text{ and } \tau_{|F} \neq \mathrm{Id}, \\ 1 \text{ otherwise,} \end{cases}$$

for some $m \in M^*$. Observe that γ_{E^*} only depends on the class of $m \mod (M^*)^2$, for replacing c_{E^*} by a cohomologous cocycle changes m by an element of $(M^*)^2$.

The aim of this section is to prove the following result.

Proposition 3.10. *Either $2m$ or $-2m$ is a square in M.*

The proof follows from an explicit computation of the decomposition into simple varieties of the variety $R = \mathrm{Res}_{K/k} E$, the restriction of scalars of E. This is justified by the observation that A is one of the factors of such decomposition.

Lemma 3.11. *The abelian variety A is a simple factor of R. More precisely,*

$$R \sim A^2 \times A',$$

for some abelian variety A' that does not contain any factor isogenous to A.

Proof. By the universal property of the restriction of scalars we have an isomorphism of $\mathbb{Q}$-vector spaces

$$(3.4) \qquad \mathrm{Hom}(A, R) = \mathrm{Hom}(A_K, E) \simeq M^2.$$

We claim that $\mathrm{End}(A) \simeq M$ as $\mathbb{Q}$-vector spaces (and, in fact, as $\mathbb{Q}$-algebras). Indeed, the Galois endomorphism type (as described in [FKRS12, §4]) of A is $\mathbf{F}[\mathrm{S}_4]$, and then by [FKRS12, Table 8], one deduces that $\mathrm{End}(A)$ has dimension 2 over $\mathbb{Q}$. The isomorphism then follows from Proposition 2.8.

Therefore, we see that two (and only two) copies of A appear in the decomposition of R into simple varieties and this finishes the proof. $\square$

In order to further determine the decomposition of R, we will compute the decomposition of its endomorphism algebra into simple algebras. By [Gro80, §15] (cf. also [Rib92, Lemma 6.4] for the non-CM case), there is an isomorphism of algebras

$$(3.5) \qquad \mathrm{End}(R) \simeq M^{c_E}[G],$$

where $M^{c_E}[G]$ denotes the *twisted group algebra* of G by a cocycle c_E representing γ_E. This is the M-algebra with M-basis the symbols $\{u_\sigma\}_{\sigma \in G}$ and multiplication given by the rule

$$(3.6) \qquad u_\sigma \cdot u_\tau = c_E(\sigma, \tau) u_{\sigma\tau}.$$

In order to relate c_{E^*} and c_E we need two basic lemmas.

Lemma 3.12. *Let C/K_1 and C'/K_1 be elliptic curves with CM by a field M_1 contained in K_1 and different from $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. Then there exists an element $\beta \in K_1$ such that C' is K_1-isogenous to C_β, the $K_1(\sqrt{\beta})$-twist of C.*

Proof. Since C and C' have CM by M_1 there exists a $\overline{\mathbb{Q}}$-isogeny $\lambda \colon C'_{\overline{\mathbb{Q}}} \to C_{\overline{\mathbb{Q}}}$. The fact that G_{K_1} acts trivially on M_1 implies that the map

$$(3.7) \qquad \begin{array}{ccc} G_{K_1} & \longrightarrow & M_1^* \\ \sigma & \longmapsto & \lambda^{-1} \circ {}^\sigma\lambda \end{array}$$

is a homomorphism. Its image is finite, because λ is defined over some finite extension of K_1, and therefore contained in $\{\pm 1\}$ by our hypothesis on M_1. If the image is trivial then λ is defined over K_1; otherwise, it is defined over a field of the form $L_1 = K_1(\sqrt{\beta})$ for some $\beta \in K_1^* \setminus (K_1^*)^2$. The set $\operatorname{Hom}(\operatorname{Gal}(L_1/K_1), M_1^*) = H^1(\operatorname{Gal}(L_1/K_1), M_1^*)$ parametrizes the elliptic curves which are L_1-isogenous to C, up to K_1-isogeny. The curve C_β also corresponds to the homomorphism (3.7), and therefore C' is K_1-isogenous to C_β. $\qquad\square$

In the following statement we use the interpretation of $H^2(G, \{\pm 1\})$ as a group classifying (classes of) central extensions of G by $\{\pm 1\}$.

Lemma 3.13. *Let C be a k_1-curve completely defined over a field K_1. Suppose that C has CM by a field M_1 contained in k_1, and let $\gamma_C \in H^2(\operatorname{Gal}(K_1/k_1), M_1^*)$ be the corresponding cohomology class. Let $L_1 = K_1(\sqrt{\beta})$ for some $\beta \in K_1$, and let C_β be the L_1-twist of C. The curve C_β is completely defined over K_1 if and only if L_1 is Galois over k_1. Moreover, in that case the cohomology classes $\gamma_C, \gamma_{C_\beta} \in H^2(\operatorname{Gal}(K_1/k_1, M_1^*))$ satisfy the relation*

$$\gamma_{C_\beta} = \gamma_C \cdot \gamma_{L_1},$$

where $\gamma_{L_1} \in H^2(\operatorname{Gal}(K_1/k_1), \{\pm 1\})$ stands for the cohomology class attached to

$$1 \longrightarrow \operatorname{Gal}(L_1/K_1) \simeq \{\pm 1\} \longrightarrow \operatorname{Gal}(L_1/k_1) \longrightarrow \operatorname{Gal}(K_1/k_1) \longrightarrow 1.$$

Proof. This is proved in [GQ14, Lemma 6.1] in the non-CM case. The same argument works in the CM case, with just a small remark: in the course of the argument of loc. cit. one constructs isogenies $\nu_\sigma \colon {}^\sigma C_\beta \to C_\beta$ and uses the fact that if the curve is completely defined over K_1 then these ν_σ are necessarily defined over K_1. This is obvious in the non-CM case; in the CM case, if follows from our hypothesis that $M_1 \subseteq k_1$, because then all the endomorphisms of C_β are defined over K_1. $\quad\square$

Since E and E^* are k-curves completely defined over K, the above lemmas imply that E and E^* become isogenous over a quadratic extension L/K such that L/k is Galois, and that

$$(3.8) \qquad \gamma_E = \gamma_{E^*} \cdot \gamma_L,$$

where γ_L is the cohomology class attached L/K.

Remark 3.14. Observe that γ_L in principle belongs to $H^2(G, \{\pm 1\})$; in expressions like (3.8), we make the slight abuse of notation of using the same symbol to denote the image of γ_L under the natural map

$$H^2(G, \{\pm 1\}) \to H^2(G, M^*)[2]. \tag{3.9}$$

This is justified by the fact that (3.9) is injective. This follows, for instance, from the following decomposition, which is analogous to (2.5):

$$H^2(G, M^*)[2] \simeq H^2(G, \{\pm 1\}) \times H^2(G, M^*/\{\pm 1\})[2].$$

Recall that $G \simeq S_4$. The cohomology group $H^2(S_4, \{\pm 1\})$ is known to be iso-morphic to $C_2 \times C_2$ (see, e.g., [Ser84, §1.5] and the references therein). Besides the trivial cohomology class there is one symmetric cohomology class and two non-symmetric ones. The corresponding possibilities for $\mathrm{Gal}(L/k)$ are also well-known, and we are only interested in the non-symmetric classes, which correspond to B_O (the binary octahedral group introduced in §3.1) and to $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$.

Lemma 3.15. *The cohomology class γ_L in (3.8) is non-symmetric. That is, $\mathrm{Gal}(L/k)$ is isomorphic to B_O or $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$.*

Proof. Suppose that γ_L is symmetric. It turns out that the symmetric classes in $H^2(S_4, \{\pm 1\})$ are precisely those that have trivial restriction to A_4. Since $\mathrm{Gal}(K/F) \simeq A_4$, and γ_{E^*} has trivial restriction to $\mathrm{Gal}(K/F)$, we see that γ_E has trivial restriction to $\mathrm{Gal}(K/F)$. Therefore, E is K-isogenous to a curve defined over F (cf. Remark 2.13). But this is a contradiction with Lemma 3.9, which implies that the minimal extension of K over which this can happen is non-trivial. $\square$

From now on we denote by $\gamma_- \in H^2(G, \{\pm 1\})$ the class corresponding to B_O and by γ_+ the one corresponding to $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ (and, as usual c_+ and c_- denote cocycles representing them). So far we have seen that

$$\gamma_E = \gamma_{E^*} \cdot \gamma_\pm, \quad \text{where } \gamma_{E^*} \text{ is given by (3.3) and } \gamma_\pm \in \{\gamma_+, \gamma_-\}. \tag{3.10}$$

The next step is to compute the center of $M^{c_E}[G]$. As a previous calculation, we need to determine the center of $M^{c_\pm}[G]$. For this we will use the characterization of the center of a twisted group algebra $M^c[G]$ given in [Kar87, p. 321]. Given a two-cocycle $c \in Z^2(G, M^*)$, an element $g \in G$ is said to be *c-regular* if

$$c(g, h) = c(h, g) \quad \text{for all } h \text{ in the centralizer } C_G(g) \text{ of } g. \tag{3.11}$$

All conjugates of a c-regular element are also c-regular. Let X denote a set of representatives of the c-regular conjugacy classes. For $x \in X$ let T_x denote a system of representatives of $G/C_G(x)$. For every $x \in X$, the element

$$k_x = \sum_{g \in T_x} u_g u_x u_g^{-1} \tag{3.12}$$

belongs to the center of $M^c[G]$. Moreover, $\{k_x\}_{x \in X}$ is an M-basis of the center. Observe that, by making use of (3.6), the element k_x can also be expressed as

$$k_x = \sum_{g \in T_x} u_g u_x u_g^{-1} = \sum_{g \in T_x} c(gx, g^{-1}) c(g, x) c(g, g^{-1})^{-1} u_{gxg^{-1}}. \tag{3.13}$$

Lemma 3.16. *The center of $M^{c_\pm}[G]$ is isomorphic to $M \times M[t]/(t^2 \mp 2)$.*

Proof. This is an explicit computation with the cocycle $c_{\pm}$. The computation is elementary, but lengthy. For this reason, we have used the software Magma [BCP97] to carry it out.[6] We reproduce here the details only for c_+; they are very similar for c_-.

To begin with, Magma implements routines that allow for the explicit computation the cocycle c_+. Alternatively, one can compute it using the exact sequence

$$1 \to \{\pm 1\} \to \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z}) \to \mathrm{S}_4 \simeq G \to 1$$

as follows: For each $\sigma \in G$ fix a lift $\tilde{\sigma} \in \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$; then $c_+(\sigma, \tau) = \tilde{\sigma} \cdot \tilde{\tau} \cdot \widetilde{\sigma\tau}^{-1}$.

Knowing the values $c_+(\sigma, \tau)$ for all $\sigma, \tau \in \mathrm{S}_4$ (here we are identifying G with S_4), one can compute the set X: it consists of the conjugacy classes of Id, $(1, 2, 4)$, and $(1, 4, 3, 2)$. This already implies that the center has dimension 3 over M.

It remains to compute the structure of the center as an algebra. For this, consider the element k_y with $y = (1, 4, 3, 2)$, which can be computed explicitly by means of (3.13) with $c = c_+$. It turns out that

(3.14) $$k_y = \sum_{g \in T_y} c_+(gy, g^{-1})c_+(g, y)c_+(g, g^{-1})^{-1}u_{gyg^{-1}}$$

(3.15) $$= u_{(1,2,3,4)} + u_{(1,4,3,2)} + u_{(1,3,4,2)} + u_{(1,3,2,4)} - u_{(1,4,2,3)} - u_{(1,2,4,3)}.$$

Using the multiplication formula in the twisted group algebra, namely $u_\sigma \cdot u_\tau = c_+(\sigma, \tau)u_{\sigma\tau}$, one computes that

$$k_y^2 = 3(-u_{(1,3,2)} + u_{(1,2,3)} - u_{(1,4,3)} + u_{(1,3,4)} - u_{(1,4,2)} + 2u_{\mathrm{Id}}$$
$$- u_{(2,4,2)} + u_{(1,2,3)} - u_{(2,3,4)})$$

and

$$k_y^3 = 18(u_{(1,2,3,4)} + u_{(1,4,3,2)} + u_{(1,3,4,2)} + u_{(1,3,2,4)} - u_{(1,4,2,3)} - u_{(1,2,4,3)}).$$

We see that $k_y^3 - 18k_y = 0$ and that the powers of k_y do not satisfy any linear relation of lower degree. Thus the minimal polynomial of k_y is $t(t^2 - 18)$ which implies that the center of $M^{c_\pm}[G]$ is isomorphic to $M \times M[t]/(t^2 - 2)$.

The same calculation for c_- gives the minimal polynomial $t(t^2 + 18)$. $\qquad\square$

Lemma 3.17. *The center of $M^{c_E}[G]$ is isomorphic to $M \times M[t]/(t^2 \mp 2m)$.*

Proof. Again we just explicit the calculations for c_+; the case of c_- is analogous. By (3.10) we can assume that $c_E = c_{E^*} \cdot c_+$. Recall that c_{E^*} is a symmetric cocycle (cf. formula (3.3)) which lies in the image of the inflation map

$$H^2(\mathrm{Gal}(F/k), M^*) \to H^2(G, M^*).$$

Since c_{E^*} is symmetric, in view of (3.11) an element $g \in G$ is c_E-regular if and only if it is c_+-regular. This implies that the center of $M^{c_E}[G]$ has the same dimension as the center of $M^{c_+}[G]$. We next determine its algebra structure.

One of the elements of the center of $M^{c_E}[G]$ is

$$\tilde{k}_y = \sum_{g \in T_y} c_E(gy, g^{-1})c_E(g, y)c_E(g, g^{-1})^{-1}u_{gyg^{-1}},$$

where we can take $y = (1, 4, 2, 3)$ as before. Using formula (3.3) and the fact that $g \notin A_4$ for $g \in T_y$ it is easy to check that

$$c_{E^*}(gy, g^{-1})c_{E^*}(g, y)c_{E^*}(g, g^{-1})^{-1} = 1.$$

---

[6]In https://github.com/xguitart/sato-tate the interested reader can find the Magma script that we used.

Therefore, we have that

(3.16) $$\tilde{k}_y = \sum_{g \in T_y} c_+(gy, g^{-1})c_+(g, y)c_+(g, g^{-1})^{-1} u_{gyg^{-1}}$$

(3.17) $$= u_{(1,2,3,4)} + u_{(1,4,3,2)} + u_{(1,3,4,2)} + u_{(1,3,2,4)} - u_{(1,4,2,3)} - u_{(1,2,4,3)}.$$

Observe that $\tilde{k}_y$ has the same expression as the element k_y found in (3.15) in terms of the basis $\{u_\sigma\}_{\sigma \in G}$. We remark that the two elements lie in different algebras though: k_y lies in $M^{c\pm}[G]$ and $\tilde{k}_y$ lies in $M^{c_E}[G]$. Thus, in order to compute $\tilde{k}_y^2$ we need to use now the multiplication of the twisted group algebra $M^{c_E}[G]$:

$$u_\sigma \cdot u_\tau = c_E(\sigma, \tau) u_{\sigma\tau}.$$

But observe that the group elements appearing in (3.17) do not belong to A_4. Therefore, in order to compute $\tilde{k}_y^2$ only the values $c_E(\sigma, \tau)$ with $\sigma, \tau \notin A_4$ are involved in the calculation. For $\sigma, \tau \notin A_4$ we have that $c_E(\sigma, \tau) = m \cdot c_+(\sigma, \tau)$. This means that $\tilde{k}_y^2$ has the same expression in terms of the basis as $m \cdot k_y^2$; that is

$$\tilde{k}_y^2 = 3m(-u_{(1,3,2)} + u_{(1,2,3)} - u_{(1,4,3)} + u_{(1,3,4)} - u_{(1,4,2)} + 2u_{\mathrm{Id}}$$
$$- u_{(2,4,2)} + u_{(1,2,3)} - u_{(2,3,4)})$$

Now the group elements appearing in the above expression of $\tilde{k}_y^2$ belong to A_4. Therefore, in the product $\tilde{k}_y^3 = \tilde{k}_y^2 \cdot \tilde{k}_y$ all the products of basis elements are of the form $u_\sigma \cdot u_\tau$ with $\sigma \in A_4$ and $\tau \notin A_4$, so that $c_E(\sigma, \tau) = c_+(\sigma, \tau)$. This implies that $\tilde{k}_y^3$ has the same expression in terms of the basis elements as $m \cdot k_y^3$, namely

$$\tilde{k}_y^3 = 18m(u_{(1,2,3,4)} + u_{(1,4,3,2)} + u_{(1,3,4,2)} + u_{(1,3,2,4)} - u_{(1,4,2,3)} - u_{(1,2,4,3)}).$$

Therefore, $\tilde{k}_y^3 - 18m\tilde{k}_y = 0$ and the minimal polynomial of $\tilde{k}_y$ is $t^3 - 18mt$ as we aimed to see. $\qquad\square$

From the above lemma we see that $M^{c_E}[G]$ decomposes into the product of either two or three simple algebras, depending on whether $\mp 2m$ is a square in M or not. Before determining the structure of the center, we record the following piece of information about $M^{c_E}[G]$, which we will use in §3.4 below.

Lemma 3.18. *Each simple factor of $M^{c_E}[G]$ contains $\mathrm{M}_2(M)$ as a subalgebra.*

Proof. The first step is to prove that $M^{c_E}[G]$ contains a subalgebra isomorphic to $\mathrm{M}_2(M)$. Indeed, let H be the unique normal subgroup of G isomorphic to $C_2 \times C_2$. The only normal subgroup of S_4 isomorphic to $C_2 \times C_2$ is contained in A_4; since $\mathrm{Gal}(K/F) \simeq A_4$ we see that $H \subseteq \mathrm{Gal}(K/F)$. Thus $c_E(x, y) = c_\pm(x, y)$ for $x, y \in H$ because c_{E^*} has trivial restriction to $\mathrm{Gal}(K/F)$.

Now let s and t be generators of H. The elements u_1, u_s, u_t, and u_{st} generate a subalgebra of $M^{c_E}[G]$ isomorphic to $(a, b)_M$ with $a, b \in \{\pm 1\}$. Indeed, one can check that

(3.18) $$c_\pm(s, s) \in \{\pm 1\}; \ c_\pm(t, t) \in \{\pm 1\}; \ c_\pm(s, t)c_\pm(t, s) = -1,$$

so that

$$u_s^2 = \pm 1, \ u_t^2 = \pm 1; \ u_s u_t = -u_t u_s.$$

Therefore, u_s and u_t generate an algebra which is isomorphic to $(\pm 1, \pm 1)_M$. As we have observed before, by Proposition 3.5 $iii)$ the field M splits the algebra $(-1, -1)_{\mathbb{Q}}$, so that $(\pm 1, \pm 1)_M \simeq \mathrm{M}_2(M)$.

Let B be a simple factor of $M^{c_E}[G]$ with projection $\pi\colon M^{c_E}[G] \to B$. The composition

$$\mathrm{M}_2(M) \hookrightarrow M^{c_E}[G] \overset{\pi}{\to} B$$

is a homomorphism of M-algebras. Since $\mathrm{M}_2(M)$ is simple, it does not have non-trivial ideals and the kernel of the above composition is trivial. Thus the homomorphism $\mathrm{M}_2(M) \to B$ is injective and $\mathrm{M}_2(M)$ is a subalgebra of the simple factor B. $\qquad\square$

Remark 3.19. Observe that in the proof of Lemmas 3.17 and 3.18 we have not used that E is the elliptic quotient of A. This will play a role in Proposition 3.20 below, but the statements of Lemma 3.17 and Lemma 3.18 are valid for any k-curve completely defined over K, with $\mathrm{Gal}(K/k) \simeq \mathrm{S}_4$ and whose cohomology class is as in (3.10). This will be used in §3.4.

Proposition 3.20. *The center of $M^{c_E}[G]$ is isomorphic to $M \times M \times M$.*

Proof. From Lemma 3.17 the center of $M^{c_E}[G]$ is isomorphic to either $M \times M \times M$ or $M \times L$, with $[L\colon M] = 2$. Suppose that the center is $M \times L$. This implies that

$$M^{c_E}[G] \simeq M_{r_1}(B_1) \times M_{r_2}(B_2),$$

where B_1 stands for an M-central division algebra, say of Schur index c_1, and B_2 for an L-central division algebra of Schur index c_2. Since $M^{c_E}[G]$ has dimension 24 over M we have that

(3.19) $$r_1^2 c_1^2 + 2 r_2^2 c_2^2 = 24.$$

Now by Lemma 3.11 one of the simple factors of $M^{c_E}[G]$ is isomorphic to $\mathrm{M}_2(M)$. This forces $r_1 = 2$ and $c_1 = 1$, but then (3.19) does not have any solution which is a contradiction. $\qquad\square$

Proof of Proposition 3.10. The statement is now a direct consequence of Proposition 3.20 and Lemma 3.17. $\qquad\square$

Some explicit computations. To illustrate the usefulness of Proposition 3.10 we have computed the cohomology class associated to certain curves with CM by a field M of class number 2, in the particular case where $k = M$. The calculations that we next describe have been done using Sage.[7]

Let M be one of the imaginary quadratic fields of Table 2. Let j_0 and j_1 be the roots of the Hilbert class polynomial attached to the discriminant D of M. The field $\mathbb{Q}(j_0)$ is real quadratic and the Hilbert class field of M is given by $H = M \cdot \mathbb{Q}(j_0)$. In particular, since we take $k = M$, the field F coincides with H.

As a first step, we have computed an elliptic curve $E_0/\mathbb{Q}(j_0)$ with j-invariant j_0 (this is easy; one can use for instance the explicit formula of [Sil86, Prop. 1.4]). Then, with a simple search method we have been able to find an element $\beta \in \mathbb{Q}(j_0)$ such that the curve $(E_0)_\beta$, the twist of E_0 by β, is F-isogenous to its $\mathrm{Gal}(F/k)$-conjugate.[8] Put $E^* = (E_0)_\beta$, and denote by σ a generator of $\mathrm{Gal}(F/k)$.

Using Sage routines we have computed an isogeny $\mu_\sigma\colon E^* \to {}^\sigma E^*$ explicitly; that is, we have found the rational functions that define μ_σ. Then it is easy to

---

[7]The reader can find the scripts in `https://github.com/xguitart/sato-tate`.

[8]Since D satisfies (NE) there exists a curve over F, with CM by M, and which is F-isogenous to its $\mathrm{Gal}(F/k)$-conjugate. However, it is not clear to us that one can always find a model over $\mathbb{Q}(j_0)$ of such curve, as we did for the curves of Table 2.

compute its Galois conjugate ${}^\sigma\mu_\sigma$ and the composition ${}^\sigma\mu_\sigma \circ \mu_\sigma$. Having explicitly the rational functions giving the isogeny ${}^\sigma\mu_\sigma \circ \mu_\sigma$ allows for the calculation of the kernel polynomial of this isogeny. In each of the entries of Table 2 we have checked that such kernel polynomial agrees with the kernel polynomial of the isogeny "multiplication by m", where m is the one displayed in the second column. This means that ${}^\sigma\mu_\sigma \circ \mu_\sigma$ equals multiplication by $\pm m$ (the indeterminacy in the sign comes from the fact that the kernel polynomial determines the isogeny up to composing with -1). We remark that the isogeny μ_σ that we begin with is non-canonical; a different choice of μ_σ would change m by an element of $(M^*)^2$.

As an example, we give the computations for the case $k = M = \mathbb{Q}(\sqrt{-40})$. The Hilbert class field in this case is $F = \mathbb{Q}(\sqrt{-40}, \sqrt{5})$. The curve

$$E^*\colon y^2 = x^3 + (135\sqrt{5} - 1125)x + 6480\sqrt{5} - 54000$$

has CM by the ring of integers of M. There is an isogeny $\mu_\sigma\colon E_F^* \to {}^\sigma E_F^*$ with kernel polynomial

$$x + 6\sqrt{5} - 30.$$

The Galois conjugate ${}^\sigma\mu_\sigma$ has kernel polynomial

$$x - 6\sqrt{5} - 30.$$

One can check that the kernel polynomial of ${}^\sigma\mu_\sigma \circ \mu_\sigma$ equals the kernel polynomial of the multiplication by 2 map on E^*.

On Table 2, we have computed the value of $m \mod (M^*)^2$ for some discriminants D of quadratic imaginary fields M of class number 2. Note that for $M = \mathbb{Q}(\sqrt{-35})$, $\mathbb{Q}(\sqrt{-51})$, or $\mathbb{Q}(\sqrt{-115})$, none of $2m$ or $-2m$ is a square of M^*, and thus Proposition 3.10 provides an obstruction to the existence of an abelian surface A/k with $\mathrm{Gal}(K/k) \simeq \mathrm{S}_4$ and the elliptic quotient E having CM by M. Observe, however, that for $D = -40$ and $D = -24$, we have that either $2m$ or $-2m$ is a square in M, since $m = \pm 2$. Therefore Proposition 3.10 does not yield any obstruction in these cases. In fact, in §3.4 below we will exhibit an example of an abelian surface A/k with $\mathrm{Gal}(K/k) \simeq \mathrm{S}_4$ and the elliptic quotient E having CM by $\mathbb{Q}(\sqrt{-40})$.

D (discriminant of M)	$m \mod (M^*)^2$
-24	± 2
-35	± 5
-40	± 2
-51	± 3
-115	± 5

TABLE 2. Values of $m \mod (M^*)^2$ for certain curves E^* with CM by fields of class number 2.

3.3. **Abelian surfaces over $\mathbb{Q}$.** In this section, let A be an abelian surface defined over k satisfying that $A_{\overline{\mathbb{Q}}} \sim E^2$, where E is an elliptic curve over $\overline{\mathbb{Q}}$ with CM, say by a quadratic imaginary field M. Let K/k be the minimal extension such that $\mathrm{End}(A_K) \simeq \mathrm{End}(A_{\overline{\mathbb{Q}}})$. Denote by $\mathcal{M}^1$ (resp. $\mathcal{M}^2$) the finite set of quadratic imaginary fields of class number 1 (resp. of class number 2). We also denote by $\mathcal{M}^{2,2}$ the finite set of imaginary quadratic fields with class group isomorphic to

$C_2 \times C_2$. On Table 3 below we list the discriminants D of the quadratic imaginary fields in $\mathcal{M}^1$, $\mathcal{M}^2$, and $\mathcal{M}^{2,2}$, respectively.

$\mathcal{M}^1$	$-3, -4, -7, -8, -11, -19, -43, -67, -163$
$\mathcal{M}^2$	$-15, -20, -24, -35, -40, -51, -52, -88, -91, -115$
	$-123, -148, -187, -232, -235, -267, -403, -427$
$\mathcal{M}^{2,2}$	$-84, -120, -132, -168, -195, -228, -280, -312, -340, -372, -408, -435$
	$-483, -520, -532, -555, -595, -627, -708, -715, -760, -795, -1012, -1435$

TABLE 3. Discriminants of the imaginary quadratic fields with class group isomorphic to C_1, C_2, and $C_2 \times C_2$.

Theorem 3.21. *Let A be an abelian surface defined over a number field k that is $\overline{\mathbb{Q}}$-isogenous to the square E^2 of an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by M. If k is either $\mathbb{Q}$ or M, the set of possibilities for M provided that $\mathrm{Gal}(K/M) \simeq G$ is contained in $\mathcal{M}(G)$, where the set $\mathcal{M}(G)$ is as defined on Table 4.*

$\mathrm{Gal}(K/M)$	$\mathcal{M}(\mathrm{Gal}(K/M))$
C_1	$\mathcal{M}^1$
C_2	$\mathcal{M}^1 \cup \mathcal{M}^2$
C_3	$\mathcal{M}^1$
C_4	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2$
C_6	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2$
D_2	$\mathcal{M}^1 \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
D_3	$\mathcal{M}^1 \cup \mathcal{M}^2$
D_4	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
D_6	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
A_4	$\mathcal{M}^1 \setminus \{\mathbb{Q}(\sqrt{-7})\}$
S_4	$\{\mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \setminus \{\mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-35}), \mathbb{Q}(\sqrt{-51}), \mathbb{Q}(\sqrt{-115})\}$

TABLE 4. Possibilities for the field M depending on $\mathrm{Gal}(K/M)$.

Proof. Suppose first that $k = M$. By Proposition 3.2, E admits a model E^* up to isogeny defined over a subextension F/k of K/k, with $\mathrm{Gal}(F/k) \simeq C_2{}^r$ for some $r \leq r(A)$, where $r(A)$ is as defined in Remark 3.1. By Remark 3.3 we can actually suppose that E^* is an elliptic curve with CM by the maximal order of M, and that $F = k(j(E^*))$. The fact that $k = M$ implies that F is the Hilbert class field of M. Therefore, $\mathrm{Gal}(F/M) = \mathrm{Gal}(F/k) \simeq C_2{}^r$ with $r \leq r(A)$ and necessarily M lies in $\mathcal{M}^1 \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$. This proves the rows of Table 4 corresponding to C_1, C_2, C_3, D_2, and D_3.

The remaining rows except of the last one follow by combining the above result with Proposition 3.5. Indeed, for rows C_4 and D_4 observe that, if M has class number 1, then $F = M$ and $\mathrm{Gal}(K/F)$ contains an element of order 4, so that $i)$ of Proposition 3.5 forces M to be $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. Similarly, rows C_6 and D_6 are a consequence of $ii)$ of Proposition 3.5. The row A_4 follows from $iii)$: $\mathbb{Q}(\sqrt{-7})$ does not split $(-1, -1)_{\mathbb{Q}}$ so it can not appear in the list.

Finally, for the row S_4, besides from the above considerations, one needs to invoke Proposition 3.10 and Table 2. Indeed, first note that if the class number is 1, then M can only be $\mathbb{Q}(\sqrt{-2})$ because of statement iv) of Proposition 3.5; second, $\mathbb{Q}(\sqrt{-15})$ can not appear, because it does not split $(-1,-1)_{\mathbb{Q}}$; third, the quadratic imaginary fields of class number 2 and discriminants $D = -35$, $D = -51$, and $D = -115$ cannot occur because the respective values of $\pm 2m$ (as listed on Table 2) are not squares in M.

This finishes the case where $k = M$. The case $k = \mathbb{Q}$ now follows by applying the previous case to the base change A_M. $\square$

We note that Table 4 is to be read as follows: if M does not belong to $\mathcal{M}(G)$, then there does not exists any A/k such that $\mathrm{Gal}(K/M) \simeq G$ and its absolutely simple factor has CM by M. We do not claim, however, that for any pair (G, M) with $M \in \mathcal{M}(G)$ there does exist such an A. In other words, it might be that some of the pairs of (G, M) in Table 4 cannot be realized by any abelian surface.

In §4.2, we will illustrate several approaches that one can take to finding examples of abelian surfaces realizing a concrete pair (G, M). For example, one can perform a search over equations of genus 2 curves and try to identify the endomorphism algebra of its Jacobian and the minimum field of definition of its endomorphisms; or one can look for equations over families of genus 2 curves parametrizing those with a specified group of automorphisms. A slightly less explicit method (in the sense that one does not get the equation of a genus 2 curve out of it) is to find A as a simple factor of the restriction of scalars of a suitable elliptic curve with CM by M. We illustrate this in the following remark, which sumarizes a result of T. Nakamura in [Nak04].

Remark 3.22. The pair $(G, M) = (C_2 \times C_2, \mathbb{Q}(\sqrt{-84}))$ is realized by an abelian surface defined over M. Indeed, let K be the Hilbert class field of M, so that $\mathrm{Gal}(K/M) \simeq C_2 \times C_2$, and let E be an elliptic curve with CM by M and with the property that E is defined over K and it is K-isogenous to all of its $\mathrm{Gal}(K/\mathbb{Q})$-conjugates. Such elliptic curves exist; in fact, in [Nak04, p. 190] it is shown that there are 8 of them, up to K-isogeny. Let $R = \mathrm{Res}_{K/M} E$ denote the restriction of scalars, which is an abelian variety over M of dimension 4. Nakamura shows that $\mathrm{End}(R)$ is isomorphic to the quaternion algebra $(a, b)_M$, where the pair (a, b) is one of the entries in the table of [Nak04, p. 190]. It turns out that, for all the entries in that table, there is an isomorphism $(a, b)_M \simeq M_2(M)$, and therefore $R \sim A^2$ for some A/M such that $A_K \sim E^2$. It follows from the theory of complex multiplication that K is the smallest field of definition of the endomorphisms of A.

A similar approach can be used to realize the pair $(S_4, \mathbb{Q}(\sqrt{-40}))$. The argument is a bit lengthier though, and we devote §3.4 below to it.

3.4. **An abelian surface with** $\mathrm{Gal}(K/k) \simeq S_4$ **and** $M \neq \mathbb{Q}(\sqrt{-2})$**.** In this section we provide an example of abelian surface A/k that satisfies conditions (0), (1), (2), (3), and (4) described at the beginning of §3.2. The strategy is to begin with a suitable choice of the fields K, k, and M, and of the curve E/K. Then we construct A as a simple factor of the restriction of scalars of E, a step in which we will take advantage of the explicit calculations performed in §3.2.

We begin by describing the number fields involved in the construction. Let K_0 be the number field with defining polynomial[9] $x^4 - x^3 + 5x^2 - 5x + 2$. The Galois closure K_0' of K_0 has Galois group isomorphic to S_4 and contains $\mathbb{Q}(\sqrt{5})$ as a subfield.

Consider also the imaginary quadratic field $M = \mathbb{Q}(\sqrt{-40})$. For the construction we take $k = M$ and $K = K_0' \cdot k$. The splitting field of the Hilbert class polynomial attached to $D = -40$ is $\mathbb{Q}(\sqrt{5})$, so that $F = M \cdot \mathbb{Q}(\sqrt{5})$ is the Hilbert class field of M. Thus the diagram of fields is the following:

$$
\begin{array}{c}
K \\
\Big| \; 12 \\
F = M \cdot \mathbb{Q}(\sqrt{5}) \\
\end{array}
$$
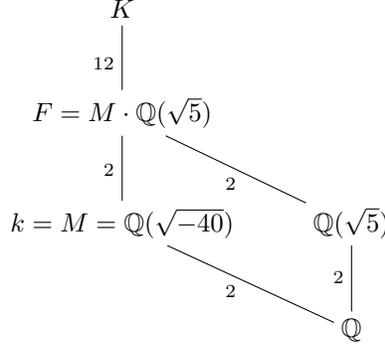
with $\mathrm{Gal}(K/k) \simeq S_4$ and $\mathrm{Gal}(K/F) \simeq A_4$. For future reference we also put $K_1 = K_0 \cdot k$ (note that K_1 is of degree 4 over k and its Galois closure is K).

The discriminant of M satisfies condition (NE) of §3.2, so there exists an elliptic curve E^*/F which is F isogenous to its $\mathrm{Gal}(F/k)$-conjugate. Thus E^* is a k-curve completely defined over F and one can attach to it a cohomology class $\gamma_{E^*}^F$, which lies in $H^2(\mathrm{Gal}(F/k), M^*)$ and it is non-trivial since E^* does not admit a model up to isogeny over k. In fact, it will be more convenient for us to regard E^* as a k-curve completely defined over K. In particular, we will be concerned with the cohomology class $\gamma_{E^*}^K \in H^2(\mathrm{Gal}(K/k), M^*)$, which is nothing more than the image of $\gamma_{E^*}^F$ under the inflation map

$$H^2(\mathrm{Gal}(F/k), M^*) \to H^2(\mathrm{Gal}(K/k), M^*).$$

Throughout this section, let us simply write $\gamma_{E^*} = \gamma_{E^*}^K$. Therefore, as in (3.3), the cocycle c_{E^*} representing γ_{E^*} is of the form

$$(3.20) \qquad c_{E^*}(\sigma, \tau) = \begin{cases} m \text{ if } \sigma_{|F} \neq \mathrm{Id} \text{ and } \tau_{|F} \neq \mathrm{Id}, \\ 1 \text{ otherwise,} \end{cases}$$

for some $m \in M^* \setminus (M^*)^2$. The cohomology class γ_{E^*} is determined by the element m of (3.20) (or rather by its class modulo $(M^*)^2$). This is precisely what we computed in the third entry of Table 2; we record the result for future reference.

Lemma 3.23. *The element m of (3.20) equals either 2 or -2, up to multiplication by an element of $(M^*)^2$.*

The curve E^* is the starting point of our the construction of A. The next step is to consider a certain twist of E^*, associated to the solution of a suitable Galois embedding problem of K/k. Recall that the group $H^2(S_4, \{\pm 1\})$, which is isomorphic to $C_2 \times C_2$, classifies central extensions of S_4 by $\{\pm 1\}$. We are interested

---

[9]This is the field [LMFDB, Global Number Field 4.0.5780.1], and it is contained in the degree 8 field [LMFDB, Global Number Field 8.0.835210000.1]

in the two cohomology classes γ_+ and γ_-, introduced in §3.2, that correspond to the extensions $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\mathrm{B_O}$.

Given a cohomology class $\gamma \in H^2(\mathrm{Gal}(K/k), \{\pm 1\})$ a quadratic extension L/K is said to be a solution to the embedding problem defined by γ if the extension

$$1 \longrightarrow \{\pm 1\} \simeq \mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(L/k) \xrightarrow{\text{res}} \mathrm{Gal}(K/k) \longrightarrow 1$$

corresponds to the class of γ. From now on we regard γ_+ and γ_- as elements of $H^2(\mathrm{Gal}(K/k), \{\pm 1\})$ by means of an identification $\mathrm{Gal}(K/k) \simeq \mathrm{S}_4$. In this way, γ_+ and γ_- define two embedding problems of $\mathrm{Gal}(K/k)$.

Lemma 3.24. *There exist solutions to the embedding problems associated to γ_+ and γ_-.*

Proof. Let Q_{K_1} be the quadratic form $x \mapsto \mathrm{Tr}_{K_1/k}(x^2)$ and let $w(Q_{K_1})$ denote its Hasse–Witt invariant. We denote by d_{K_1} the discriminant of K_1/k. By [Que95, Thm. 3.8] the embedding problems corresponding to $\mathrm{B_O}$ and to $\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ are solvable if and only if the following elements in the Brauer group of k are trivial:

$$(3.21) \qquad\qquad w(Q_{K_1}) \otimes (2, d_{K_1}) \text{ and } w(Q_{K_1}) \otimes (-2, d_{K_1}).$$

Since $K_1 = K_0 \cdot k$ the above classes can be regarded as

$$(3.22) \qquad\qquad w(Q_{K_0})_k \otimes (2, d_{K_0})_k \text{ and } w(Q_{K_0})_k \otimes (-2, d_{K_0})_k,$$

where the index k stands for the image under the natural map $\mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(k)$. One checks that $w(Q_{K_0})$ is ramified only at 2 and ∞, and therefore $w(Q_{K_0})_k$ is trivial (since k is imaginary and 2 ramifies in k). Also, the algebras $(\pm 2, d_{K_0})$ are split by k, so that $(\pm 2, d_{K_0})_k$ are trivial. $\qquad\square$

Let $\gamma_\pm \in H^2(\mathrm{Gal}(K/k), \{\pm 1\})$ be the cohomology class defined as follows:

$$(3.23) \qquad\qquad \gamma_\pm = \begin{cases} \gamma_+ \text{ if } m = 2 \mod (M^*)^2 \\ \gamma_- \text{ if } m = -2 \mod (M^*)^2. \end{cases}$$

Let $L = K(\sqrt{\beta})$ be a solution to the embedding problem associated to $\gamma_\pm$ and define $E = (E^*)_\beta$, the quadratic twist of E^* by β. Since L/k is Galois, Lemma 3.13 implies that E is a k-curve completely defined over K with cohomology class

$$(3.24) \qquad\qquad \gamma_E = \gamma_{E^*} \cdot \gamma_\pm.$$

Let $R = \mathrm{Res}_{K/k} E$. In view of Remark 3.19, the statements of Lemma 3.17 and Lemma 3.18 are valid in the present context, and they allow for the computation of $\mathrm{End}(R)$.

Lemma 3.25. *The center of $\mathrm{End}(R)$ is isomorphic to $M \times M \times M$,*

Proof. By Lemma 3.17 the center of $M^{c_E}[\mathrm{Gal}(K/k)]$ is isomorphic to

$$(3.25) \qquad\qquad M \times M[t]/(t^2 \mp 2m).$$

By Lemma 3.23 we have that $m = 2$ or $m = -2$, and thanks to our choice of $\gamma_\pm$ in (3.23) we see that (3.25) becomes

$$M \times M[t]/(t^2 - 4) \simeq M \times M \times M.$$

$\qquad\square$

Proposition 3.26. *One has:*

(3.26) $$\mathrm{End}(R) \simeq \mathrm{M}_2(M) \times \mathrm{M}_2(M) \times B,$$

where B is an M-central simple algebra of M-dimension 16.

Proof. By the above lemma $M^{c_E}[\mathrm{Gal}(K/k)]$ is the product of three M-central simple algebras. Denote by r_1^2, r_2^2, and r_3^2 the M-dimension of each simple factor. Since the dimension of $M^{c_E}[\mathrm{Gal}(K/k)]$ is 24 we have that

$$r_1^2 + r_2^2 + r_3^2 = 24.$$

The only solution (up to permutation) is $r_1 = 2$, $r_2 = 2$ and $r_3 = 4$. That is to say, two factors have dimension 4 and the other factor has dimension 16. Since each simple factor contains $\mathrm{M}_2(M)$ by Lemma 3.18, we see that the algebras of dimension 4 must be isomorphic to $\mathrm{M}_2(M)$, and this proves the proposition. $\square$

The decomposition of $\mathrm{End}(R)$ provided by Proposition 3.26 implies an isotypical decomposition of R of the form

(3.27) $$R \sim A_1^2 \times A_2^2 \times A_3^r,$$

where the A_i are simple abelian varieties, A_1 and A_2 correspond to the factors of the form $\mathrm{M}_2(M)$, and r is equal to either 1, 2 or 4. Let A be either A_1 or A_2. We next show that A satisfies the following properties:

- $\mathrm{End}(A) \simeq M$;
- $A_K \sim E^2$; and
- K is the smallest extension of k satisfying that $\mathrm{End}(A_K) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$.

The first statement above is clear in light of (3.26). We prove the other two in the following lemmas; this will finish the proof that A is an abelian surface satisfying conditions (0)–(4) stated at the beginning of §3.2, as we aimed to see.

Lemma 3.27. *A is an abelian surface; that is, $A_K \sim E^2$.*

Proof. By the universal property of the restriction of scalars functor we have an isomorphism of vector spaces

$$\mathrm{Hom}(A, R) \simeq \mathrm{Hom}(A_K, E);$$

from (3.27) and (3.26) we see that $\mathrm{Hom}(A, R) \simeq M^2$ and therefore $\mathrm{Hom}(A_K, E) \simeq M^2$, which implies that $A_K \sim E^2$. $\square$

Lemma 3.28. *There is no field N with $k \subsetneq N \subsetneq K$ such that $\mathrm{End}(A_N) = \mathrm{End}(A_{\overline{\mathbb{Q}}})$.*

Proof. Suppose that such N exists. Without loss of generality we can assume that it is the smallest field satisfying this property. This implies, in particular, that N/k is a Galois extension. Then $A_N \sim C^2$, for some elliptic curve C over N. Since $A_K \sim E^2$ this implies that $C_K \sim E$. Therefore, the cohomology class γ_E is trivial when restricted to $\mathrm{Gal}(K/N)$. But $\mathrm{Gal}(K/N)$ is a normal subgroup of $\mathrm{Gal}(K/k) \simeq \mathrm{S}_4$, and all normal subgroups of S_4 are contained in A_4; thus $\mathrm{Gal}(K/N)$ is a normal subgroup of $\mathrm{Gal}(K/F) \simeq \mathrm{A}_4$. Since $\gamma_E = \gamma_{E^*} \cdot \gamma_{\pm}$ and the restriction of γ_{E^*} to $\mathrm{Gal}(K/F)$ is trivial, this implies that $\gamma_{\pm}$ restricted $\mathrm{Gal}(K/N)$ is trivial. This is a contradiction, because it turns out that neither γ_+ nor γ_- become trivial when restricted to any normal subgroup of A_4. Indeed, let $H = \langle s, t \rangle$ denote the unique normal subgroup of $\mathrm{Gal}(K/k)$ isomorphic to $\mathrm{C}_2 \times \mathrm{C}_2$. By looking at the

diagram of subgroups of S_4 we see that $\mathrm{Gal}(K/N)$ must contain H. But we have already seen in (3.18) that $\gamma_{\pm}$ restricted to H is non-trivial. □

4. Two applications to Sato–Tate groups

In this section, we give two applications of the results obtained so far to the theory of Sato–Tate groups of abelian surfaces over number fields. The Sato–Tate group of an abelian surface A defined over the number field k, which we will denote by $\mathrm{ST}(A)$, is a compact real Lie subgroup of $\mathrm{USp}(4)$ that conjecturally governs the distribution of the Frobenius elements in the image of ℓ-adic representation attached to A. We refer to [FKRS12, §2] for the precise construction of the Sato–Tate group of an abelian variety defined over a number field. The reader is referred to the original source [Ser12, Chap. 8] for a construction of the Sato–Tate group in a more general context.

The main result of [FKRS12] establishes the existence of 52 possibilities for the Sato–Tate group of an abelian surface defined over a number field, all of which occur for some choice of the number field and the abelian surface (see [FKRS12, Thm. 4.3]). This result is complemented by establishing a one-to-one correspondence between Sato–Tate groups of abelian surfaces and their *Galois endomorphism types*, an algebraic structure which encaptures both the Galois action on the ring of endomorphisms of the abelian surface and the structure of this ring as an $\mathbb{R}$-algebra (see [FKRS12, Def. 1.3] for a precise definition). Let $N_{\mathrm{ST},2}(k)$ denote the number of subgroups of $\mathrm{USp}(4)$ up to conjugacy that arise as Sato–Tate groups of abelian surfaces defined over the number field k.

We will make use of the notations for Sato–Tate groups and Galois endomorphism types introduced in [FKRS12, §4] from now on. On Table 5 we show the dictionary between Sato–Tate groups and Galois endomorphism types. The groups decorated with a ⋆ are those that arise over $\mathbb{Q}$. Note that we thus have $N_{\mathrm{ST},2}(\mathbb{Q}) = 34$.

There are 6 possibilities for the connected component of the identity of the Sato–Tate group of an abelian surface A defined over k. As customary, we will denote it by $\mathrm{ST}(A)^0$. The dictionary between Sato–Tate groups and Galois endomorphism types establishes that Sato–Tate groups with identity component isomorphic to the unitary group $\mathrm{U}(1)$ of degree 1 correspond to *absolute Galois endomorphism type* **F**, that is, to abelian surfaces that are $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve with CM by a quadratic imaginary field M. A Galois endomorphism type of absolute type **F** consists of the data

$$(4.1) \qquad\qquad \mathbf{F}[\mathrm{Gal}(K/k), \mathrm{Gal}(K/kM), \mathbb{B}],$$

where K/k is the minimal extension over which all the endomorphisms of A are defined, and $\mathbb{B}$ is $\mathbb{H}$ or $\mathrm{M}_2(\mathbb{R})$ depending on whether there exists a subextension K_0/k of K/k such that $\mathrm{End}(A_{K_0}) \otimes \mathbb{R}$ is isomorphic to $\mathbb{H}$ or not. We remove $\mathrm{Gal}(K/kM)$ from the notation in case that it coincides with $\mathrm{Gal}(K/k)$, and similarly we avoid writing $\mathbb{B}$ when the other data is enough to uniquely determine the Galois endomorphism type.

4.1. **A finiteness result.** The first application to the theory of Sato–Tate groups is now an immediate corollary of Theorem 3.21.

Theorem 4.1. *Among the* 34 *possibilities for the Sato–Tate group of an abelian surface A defined over $\mathbb{Q}$, the* 18 *with identity component isomorphic to* $\mathrm{U}(1)$ *only*

G	Galois type	G	Galois type
C_1	$\mathbf{F}[\mathrm{C}_1]$	$D_{4,1}{}^\star$	$\mathbf{F}[\mathrm{D}_4, \mathrm{D}_2]$
C_2	$\mathbf{F}[\mathrm{C}_2]$	$D_{6,1}{}^\star$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathrm{M}_2(\mathbb{R})]$
C_3	$\mathbf{F}[\mathrm{C}_3]$	$D_{3,2}{}^\star$	$\mathbf{F}[\mathrm{D}_3, \mathrm{C}_3]$
C_4	$\mathbf{F}[\mathrm{C}_4]$	$D_{4,2}{}^\star$	$\mathbf{F}[\mathrm{D}_4, \mathrm{C}_4]$
C_6	$\mathbf{F}[\mathrm{C}_6]$	$D_{6,2}{}^\star$	$\mathbf{F}[\mathrm{D}_6, \mathrm{C}_6]$
D_2	$\mathbf{F}[\mathrm{D}_2]$	$O_1{}^\star$	$\mathbf{F}[\mathrm{S}_4, \mathrm{A}_4]$
D_3	$\mathbf{F}[\mathrm{D}_3]$	$E_1{}^\star$	$\mathbf{E}[\mathrm{C}_1]$
D_4	$\mathbf{F}[\mathrm{D}_4]$	$E_2{}^\star$	$\mathbf{E}[\mathrm{C}_2, \mathbb{C}]$
D_6	$\mathbf{F}[\mathrm{D}_6]$	$E_3{}^\star$	$\mathbf{E}[\mathrm{C}_3]$
T	$\mathbf{F}[\mathrm{A}_4]$	$E_4{}^\star$	$\mathbf{E}[\mathrm{C}_4]$
O	$\mathbf{F}[\mathrm{S}_4]$	$E_6{}^\star$	$\mathbf{E}[\mathrm{C}_6]$
$J(C_1)$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathbb{H}]$	$J(E_1)^\star$	$\mathbf{E}[\mathrm{C}_2, \mathbb{R} \times \mathbb{R}]$
$J(C_2)^\star$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathbb{H}]$	$J(E_2)^\star$	$\mathbf{E}[\mathrm{D}_2]$
$J(C_3)$	$\mathbf{F}[\mathrm{C}_6, \mathrm{C}_3, \mathbb{H}]$	$J(E_3)^\star$	$\mathbf{E}[\mathrm{D}_3]$
$J(C_4)^\star$	$\mathbf{F}[\mathrm{C}_4 \times \mathrm{C}_2, \mathrm{C}_4]$	$J(E_4)^\star$	$\mathbf{E}[\mathrm{D}_4]$
$J(C_6)^\star$	$\mathbf{F}[\mathrm{C}_6 \times \mathrm{C}_2, \mathrm{C}_6]$	$J(E_6)^\star$	$\mathbf{E}[\mathrm{D}_6]$
$J(D_2)^\star$	$\mathbf{F}[\mathrm{D}_2 \times \mathrm{C}_2, \mathrm{D}_2]$	F	$\mathbf{D}[\mathrm{C}_1]$
$J(D_3)^\star$	$\mathbf{F}[\mathrm{D}_6, \mathrm{D}_3, \mathbb{H}]$	F_a	$\mathbf{D}[\mathrm{C}_2, \mathbb{R} \times \mathbb{C}]$
$J(D_4)^\star$	$\mathbf{F}[\mathrm{D}_4 \times \mathrm{C}_2, \mathrm{D}_4]$	F_{ab}	$\mathbf{D}[\mathrm{C}_2, \mathbb{R} \times \mathbb{R}]$
$J(D_6)^\star$	$\mathbf{F}[\mathrm{D}_6 \times \mathrm{C}_2, \mathrm{D}_6]$	$F_{ac}{}^\star$	$\mathbf{D}[\mathrm{C}_4]$
$J(T)^\star$	$\mathbf{F}[\mathrm{A}_4 \times \mathrm{C}_2, \mathrm{A}_4]$	$F_{a,b}{}^\star$	$\mathbf{D}[\mathrm{D}_2]$
$J(O)^\star$	$\mathbf{F}[\mathrm{S}_4 \times \mathrm{C}_2, \mathrm{S}_4]$	$G_{1,3}$	$\mathbf{C}[\mathrm{C}_1]$
$C_{2,1}{}^\star$	$\mathbf{F}[\mathrm{C}_2, \mathrm{C}_1, \mathrm{M}_2(\mathbb{R})]$	$N(G_{1,3})^\star$	$\mathbf{C}[\mathrm{C}_2]$
$C_{4,1}$	$\mathbf{F}[\mathrm{C}_4, \mathrm{C}_2]$	$G_{3,3}{}^\star$	$\mathbf{B}[\mathrm{C}_1]$
$C_{6,1}{}^\star$	$\mathbf{F}[\mathrm{C}_6, \mathrm{C}_3, \mathrm{M}_2(\mathbb{R})]$	$N(G_{3,3})^\star$	$\mathbf{B}[\mathrm{C}_2]$
$D_{2,1}{}^\star$	$\mathbf{F}[\mathrm{D}_2, \mathrm{C}_2, \mathrm{M}_2(\mathbb{R})]$	$\mathrm{USp}(4)^\star$	$\mathbf{A}[\mathrm{C}_1]$

TABLE 5. Sato–Tate groups and Galois endomorphism types of abelian surfaces

occur among the set (of cardinality at most 51) of $\overline{\mathbb{Q}}$-isogeny classes of abelian surfaces over $\mathbb{Q}$ that are $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve defined over $\overline{\mathbb{Q}}$ with CM by M in $\mathcal{M}^1 \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$. More precisely, for such an abelian surface A, the set of possibilities for M provided that $\mathrm{ST}(A_M)/\mathrm{ST}(A_M)^0 \simeq G$ is contained in $\mathcal{M}(G)$.

Proof. We have already mentioned that an abelian surface whose Sato–Tate group has identity component isomorphic to U(1) has absolute Galois endomorphism type $\mathbf{F}$. Observe that

$$\mathrm{Gal}(K/M) \simeq \mathrm{ST}(A_M)/\mathrm{ST}(A_M)^0 \simeq \mathrm{ST}(A)^{ns}/\mathrm{ST}(A)^{ns,0} \, .$$

The first isomorphism is [FKRS12, Prop. 2.17]. For the second, as well as for the definition of $\mathrm{ST}(A)^{ns}$, see the paragraph following [FKRS12, Rem. 4.10]. One concludes by readily checking (for example from [FKRS12, Table 2]) that the Sato–Tate groups G on the first column and the ith row of Table 6 are precisely those for which $G^{ns}/G^{ns,0}$ is isomorphic to the finite group appearing in the first column and the ith row of Table 4. $\square$

4.2. **A number field for all genus 2 Sato-Tate groups.** The second application and the main result of the present work is the following.

Sato–Tate groups	$\mathcal{M}(\mathrm{Gal}(K/M))$
$C_{2,1}$	$\mathcal{M}^1$
$J(C_2), D_{2,1}$	$\mathcal{M}^1 \cup \mathcal{M}^2$
$C_{6,1}, D_{3,2}$	$\mathcal{M}^1$
$J(C_4), D_{4,2}$	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2$
$J(C_6), D_{6,2}$	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2$
$J(D_2), D_{4,1}$	$\mathcal{M}^1 \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
$J(D_3), D_{6,1}$	$\mathcal{M}^1 \cup \mathcal{M}^2$
$J(D_4)$	$\{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
$J(D_6)$	$\{\mathbb{Q}(\sqrt{-3})\} \cup \mathcal{M}^2 \cup \mathcal{M}^{2,2}$
$J(T), O_1$	$\mathcal{M}^1 \setminus \{\mathbb{Q}(\sqrt{-7})\}$
$J(O)$	$\{\mathbb{Q}(\sqrt{-2})\} \cup \mathcal{M}^2 \setminus \{\mathbb{Q}(\sqrt{-15}), \mathbb{Q}(\sqrt{-35}), \mathbb{Q}(\sqrt{-51}), \mathbb{Q}(\sqrt{-115})\}$

TABLE 6. Possibilities for the field M depending on the Sato–Tate group.

Theorem 4.2. *Set*

$$k_0 := \mathbb{Q}(\sqrt{-40}, \sqrt{-51}, \sqrt{-163}, \sqrt{-67}, \sqrt{19 \cdot 43}, \sqrt{-57}).$$

Then, $N_{\mathrm{ST},2}(k_0) = 52$. That is, there exist 52 abelian surfaces defined over k_0 realizing each of the 52 possible Sato–Tate groups of abelian surfaces defined over number fields.

Hereafter, we will be concerned with the proof of the previous theorem. We will assemble our constructions of abelian surfaces into six main families. Before proceeding to the proof, we make the following remark.

Remark 4.3. Observe that in §3.4 we have constructed an example of an abelian surface with Galois endomorphism type $\mathbf{F}[\mathrm{S}_4]$ (equiv. Sato–Tate group O) and $M = \mathbb{Q}(\sqrt{-40})$. However, the only examples of abelian surfaces with Galois endomorphism types $\mathbf{F}[\mathrm{S}_4 \times \mathrm{C}_2, \mathrm{S}_4]$ or $\mathbf{F}[\mathrm{S}_4, \mathrm{A}_4]$ (equiv. Sato–Tate groups $J(O)$ or O_1) that we are aware of have $M = \mathbb{Q}(\sqrt{-2})$. This means that we need to require k_0 to contain $\mathbb{Q}(\sqrt{-40})$ and not to contain $\mathbb{Q}(\sqrt{-2})$. Additionally, many of the examples shown in [FKRS12, Table 11] satisfy that K contains either $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$. In order that these examples also serve as such after base change to k_0, we require k_0 not to contain the two latter fields.

The restriction of scalars construction. As mentioned in the above remark, the abelian surface A over $k = \mathbb{Q}(\sqrt{-40})$ defined in §3.4 has Sato–Tate group O. Since $K \cap k_0 = k$, it follows from [FKRS12, Prop. 2.17] that the Sato–Tate group of the base change A_{k_0} remains the same.

Base change constructions. We consider the set of curves $\Sigma_{\mathbb{Q}}$ of [FKRS12, Table 11] which are defined over $k = \mathbb{Q}$. Note that $\Sigma_{\mathbb{Q}}$ has cardinality 34. We have used the software Sage[10] to check that for each $C \in \Sigma_{\mathbb{Q}}$ the number field K

---

[10]In https://github.com/xguitart/sato-tate the interested reader can find the Sage script that we used.

attached to $\mathrm{Jac}(C)$ satisfies that $K \cap k_0 = \mathbb{Q}$. It then follows that[11] $\mathrm{ST}(\mathrm{Jac}(C)) \simeq \mathrm{ST}(\mathrm{Jac}(C)_{k_0})$.

Twisting constructions. We will construct examples of abelian surfaces realizing the Sato–Tate groups C_n for $n \in \{1, 2, 3\}$, D_n for $n \in \{2, 3\}$, and T by using the twisting procedure of [MRS07] or [Mil72, §2]. For our purposes, a particular case of this construction will suffice: given an elliptic curve E defined over k_0 with CM by an order $\mathcal{O}$ in a quadratic imaginary field $M \subseteq k_0$, a finite Galois extension L/k_0, and an Artin representation $\varrho \colon \mathrm{Gal}(L/k_0) \to \mathrm{GL}_2(\mathcal{O})$ with coefficients in $\mathcal{O}$, there is an abelian surface $A := E \otimes \varrho$ defined over k_0 such that $A_L \sim E_L^2$ and there is an isomorphism of G_{k_0}-modules

$$(4.2) \qquad\qquad \mathrm{End}(A_{\overline{\mathbb{Q}}}) \simeq \varrho \otimes \varrho^* \otimes \mathrm{End}(E_{\overline{\mathbb{Q}}}),$$

where ϱ^* denotes the contragredient representation of ϱ ([MRS07, Prop. 1.6. i)]). For example, we may take E to be an elliptic curve with CM by $M := \mathbb{Q}(\sqrt{-163}) \subseteq k_0$ and defined over k_0. It then follows from (4.2) that the minimal extension K/k_0 over which all the endomorphisms of A are defined is the extension cut out by $\varrho \otimes \varrho^*$. For each

$$H \in \{\mathrm{C}_n \text{ for } n \in \{1, 2, 3\}, \mathrm{D}_n \text{ for } n \in \{2, 3\}, \text{ and } \mathrm{A}_4\}$$

take a Galois extension L/k_0 such that $\mathrm{Gal}(L/k_0)$ be, respectively, isomorphic to

$$\tilde{H} \in \{\mathrm{C}_{2n} \text{ for } n \in \{1, 2, 3\}, \mathrm{D}_{2n} \text{ for } n \in \{2, 3\}, \text{ and } \mathrm{B}_\mathrm{T}\}.$$

Take a faithful rational Artin representation ϱ of degree 2 of $\tilde{H}$. By inspection of the character table of H one can compute the trace of $\varrho \otimes \varrho^*$ and see that in all the cases the kernel N of $\rho \otimes \varrho^*$ has order 2, and that the quotient $\tilde{H}/N$ is isomorphic to H; thus, the field cut by $\rho \otimes \varrho^*$ has Galois group isomorphic to H. It follows from the description given in (4.1) that the Galois endomorphism type of A is $\mathbf{F}[H]$. According to Table 5, we have realized the desired Sato–Tate groups.

Remark 4.4. One may try to make similar constructions to realize the groups C_4, D_4, C_6, D_6, and O over k_0. However, in these cases, the corresponding group $\tilde{H}$ does not possess a faithful rational degree 2 representation, but rather one with coefficients in the ring of integers of the fields $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-2})$. Taking a representation with coefficients in these fields would force E to have CM by them, and thus k_0 to contain them. This is a possibility that we have excluded in Remark 4.3.

Cardona and Quer's constructions. We will construct curves whose Jacobians have Sato–Tate groups C_4, D_4, C_6, D_6, and $J(C_3)$, respectively. For this we will recall results of Cardona and Quer parametrizing $\mathbb{Q}$-isomorphism classes of genus 2 curves with prescribed automorphism groups. If $y^2 = f(x)$, with $f(x) \in k[x]$, is a defining equation for a genus 2 curve C defined over k, there is an injective group homomorphism

$$\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \hookrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}})$$

that sends an automorphism

$$(x, y) \mapsto \left(\frac{mx + n}{px + q}, \frac{mq - np}{(px + q)^3} y \right), \quad \text{where } m, n, p, q \in \overline{\mathbb{Q}},$$

---

[11]Note that, since k_0 contains neither $\mathbb{Q}(i)$, nor $\mathbb{Q}(\sqrt{-3})$, nor $\mathbb{Q}(\sqrt{-2})$, no other curve of [FKRS12, Table 11] can be base changed to k_0 in such a way that the Sato–Tate group is preserved.

to the matrix $\begin{pmatrix} m & n \\ p & q \end{pmatrix}$. From now on, we will use matrix notation to write automorphisms of genus 2 curves.

The next proposition encompasses weakened versions of [CQ07, Prop. 4.3], [CQ07, Prop. 4.9], and [Car01, Thm. 7.4.1] which are enough for our purposes.

Proposition 4.5. *Let $u, v \in \mathbb{Q}^*$ and $s, z \in \mathbb{Q}$.*

i) If $1 - z^2 u = s^2 uv$, then the curve given by the affine equation

(4.3)
$$\begin{aligned} C_{\mathrm{D}_4} : y^2 &= (1 + 2uz)x^6 - 8suvx^5 + v(3 - 10uz)x^4 + \\ &\quad + v^2(3 - 10uz)x^2 + 8suv^3 x + v^3(1 + 2uz) \end{aligned}$$

has automorphism group isomorphic to D_4. It is generated by the matrices

(4.4)
$$U = \begin{pmatrix} \alpha & \beta \\ \beta/v & -\alpha \end{pmatrix}, \qquad V = \begin{pmatrix} 0 & -\sqrt{v} \\ 1/\sqrt{v} & 0 \end{pmatrix},$$

where

(4.5)
$$\alpha = \sqrt{\frac{1 - z\sqrt{u}}{2}}, \qquad \beta = \sqrt{\frac{v(1 + z\sqrt{u})}{2}}.$$

ii) If $u^3 - z^2 = 3s^2 v$, the curve given by the affine equation

(4.6)
$$\begin{aligned} C_{\mathrm{D}_6} : y^2 &= 27(u + 2z)x^6 - 324svx^5 + 27v(u - 10z)x^4 + 360sv^2 x^3 \\ &\quad + 9v^2(u + 10z)x^2 - 36sv^3 x + v^3(u - 2z) \end{aligned}$$

has automorphism group isomorphic to D_6. It is generated by the matrices

(4.7)
$$U = \frac{1}{\sqrt{u}} \begin{pmatrix} \alpha & \beta \\ 3\beta/v & -\alpha \end{pmatrix}, \qquad V = \frac{1}{2} \begin{pmatrix} 1 & \sqrt{v} \\ -3/\sqrt{v} & 1 \end{pmatrix},$$

where $\alpha, \beta \in \overline{\mathbb{Q}}$ are such that

(4.8)
$$\alpha^3 - \frac{3u}{4}\alpha - \frac{z}{4} = 0, \qquad \alpha^2 + 3\frac{\beta^2}{v} = u.$$

iii) If $u^3 - z^2 = 3s^2 v$, the curve given by the affine equation

(4.9)
$$\begin{aligned} C_{2\mathrm{D}_6} : y^2 &= 27zx^6 - 162svx^5 - 135vzx^4 + \\ &\quad + 180sv^2 x^3 + 45v^2 zx^2 - 18sv^3 x - v^3 z \end{aligned}$$

has automorphism group isomorphic to[12] $2\mathrm{D}_6$. It is generated by the matrices

(4.10)
$$U = \frac{1}{\sqrt{u}} \begin{pmatrix} \alpha & \beta \\ 3\beta/v & -\alpha \end{pmatrix}, \qquad V = \frac{\sqrt{-3}}{2} \begin{pmatrix} 1 & -\sqrt{v}/3 \\ 1/\sqrt{v} & 1 \end{pmatrix},$$

where $\alpha, \beta \in \overline{\mathbb{Q}}$ are such that

(4.11)
$$\alpha^3 - \frac{3u}{4}\alpha - \frac{z}{4} = 0, \qquad \alpha^2 + 3\frac{\beta^2}{v} = u.$$

Remark 4.6. We wish to warn the reader of a minor misprint in the work of Cardona and Quer. In [CQ07, Prop. 3.5] the lower left entry of matrix U is missing a factor of 3 (compare with (4.7) above); we have introduced a similar correction to the second equation of both (4.8) and (4.11).

---

[12]The group $2\mathrm{D}_6$ is a certain double cover of D_6. Its GAP identification number is $\langle 24, 8 \rangle$.

Remark 4.7. It is well known and easy to show that an automorphism group structure of the type D_4, D_6 or $2D_6$ on a genus 2 curve induces a decomposition up to $\overline{\mathbb{Q}}$-isogeny of its Jacobian as the square of an elliptic curve E. In the $2D_6$ case, E has automatically CM by $\mathbb{Q}(\sqrt{-3})$. On [Car01, p. 112], one can find the values of the parameter $u \in \mathbb{Q}^*$ for which E has CM in the D_4 and D_6 cases. For example, in the former case, for $u = 81/320$, E has CM by $\mathbb{Q}(\sqrt{-40})$; in the latter case, for $u = 4/17$, E has CM by $\mathbb{Q}(\sqrt{-51})$.

Lemma 4.8. *Let C denote either C_{D_4}, or C_{D_6}, or C_{2D_6}. Suppose that $z \neq 0$ and that $\mathrm{Jac}(C)$ is $\overline{\mathbb{Q}}$-isogenous to the square of an elliptic curve with CM by M. Then the minimal extension of $\mathbb{Q}$ over which all the endomorphisms of $\mathrm{Jac}(C)$ are defined is $K = M(\alpha, \beta, \sqrt{u}, \sqrt{v})$.*

Proof. By Remark 4.7, K is the composition K' of M and the minimal field over which all the automorphisms of C are defined. The case D_4 is then immediate. For the remaining two cases, we need to check that $K' = M(\alpha/\sqrt{u}, \beta/\sqrt{u}, \sqrt{v})$ agrees with the expression for K given in the statement. But this follows from the fact that

$$\alpha = \left(\alpha^2 - \frac{3u}{4}\right)^{-1} \frac{z}{4} \in K',$$

since $\alpha^2 = u(\alpha/\sqrt{u})^2 \in K'$.   □

On Table 7, C denotes one of the curves C_{D_4}, C_{D_6}, or C_{2D_6} for the choice of parameters $s = 1$, u and z as specified on the second and third columns, and v as determined by the constraints of Proposition 4.5. The fourth and fifth columns are computed using Lemma 4.8. Together with Remark 4.7, they imply all but the last row of the last column.

C	u	z	$K \cap k_0$	$\mathrm{Gal}(Kk_0/k_0)$	$\mathrm{ST}(C_{k_0})$
C_{D_4}	$81/320$	1	$\mathbb{Q}(\sqrt{-40})$	D_4	D_4
C_{D_4}	$81/320$	$-16/9$	$\mathbb{Q}(\sqrt{-40})$	C_4	C_4
C_{D_6}	$4/17$	1	$\mathbb{Q}(\sqrt{-51})$	D_6	D_6
C_{D_6}	$4/17$	$-5/4$	$\mathbb{Q}(\sqrt{-51})$	C_6	C_6
C_{2D_6}	19	$19/2$	$\mathbb{Q}(\sqrt{-57})$	C_6	$J(C_3)$

TABLE 7. A few examples from Cardona's parametrizations.

Suppose that C is as specified in the last row of Table 7. To verify the bottom right entry, it suffices to show that $\mathrm{End}(\mathrm{Jac}(C_{K_0})) \otimes \mathbb{R} \simeq \mathbb{H}$, where $K_0 = \mathbb{Q}(\sqrt{-57}, \alpha)$. This can be easily deduced from the fact that

$$\mathrm{Aut}(C_{K_0}) \simeq \mathrm{Dic}_{12},$$

where Dic_{12} is the Dicyclic group of order 12 (with GAP identification number $\langle 12, 1 \rangle$). This is a group whose faithful representation of degree 2 has Frobenius–Schur index -1 and thus it can not be embedded in $\mathrm{GL}_2(\mathbb{R})$.

Sutherland's additional examples. Besides the examples showed on [FKRS12, Table 11], the wide search performed in [FKRS12], yielded examples that will be useful to realize $J(C_1)$ and $C_{4,1}$ over k_0. We thank Drew Sutherland for pointing out to us the two curves in this paragraph.

Consider the curve

$$C\colon y^2 = 3x^6 + 16x^5 - 15x^4 - 15x^2 - 16x + 3\,.$$

We first show that the minimal extension of $\mathbb{Q}$ over which all of the endomorphisms of $\mathrm{Jac}(C)$ are defined is $K = \mathbb{Q}(\sqrt{-10}, \sqrt{-2})$. This follows from the fact that K is minimal with the property

$$\mathrm{Aut}(C_K) \simeq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})\,.$$

Indeed, any genus 2 curve C such that $\mathrm{Aut}(C_{\overline{\mathbb{Q}}}) \simeq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$ is $\overline{\mathbb{Q}}$-isomorphic to $y^2 = x^5 - x$. Since $\mathrm{Gal}(Kk_0/k_0) \simeq \mathrm{C}_2$, in order to show that $\mathrm{ST}(\mathrm{Jac}(C_{k_0})) = J(C_1)$, all we need to check is that $\mathrm{End}(\mathrm{Jac}(C_{\mathbb{Q}(\sqrt{-10})}) \otimes \mathbb{R} \simeq \mathbb{H}$. But this follows easily from

$$\mathrm{Aut}(C_{\mathbb{Q}(\sqrt{-10})}) \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}).$$

Indeed, $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ contains the group of quaternions Q, whose rational faithful degree 2 representation has Frobenius–Schur index -1. Thus $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ can not be embedded in $\mathrm{GL}_2(\mathbb{R})$.

Consider now the curve

$$C\colon y^2 + (x^3 + x^2 + x + 1)y = -x^5 - 2x^4 - x^3 - 2x^2$$

This is the genus 2 curve [LMFDB, Genus 2 Curve 40000.e.200000.1]. To show that the minimal extension of $\mathbb{Q}$ over which all of the endomorphisms of $\mathrm{Jac}(C)$ are defined is $K = \mathbb{Q}[x]/(x^8 - 2x^6 + 4x^4 - 8x^2 + 16)$, we again check that K is minimal with the property that

$$\mathrm{Aut}(C_K) \simeq \mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})\,.$$

Since $\mathrm{Gal}(Kk_0/k_0) \simeq \mathrm{C}_4$, in order to show that $\mathrm{ST}(\mathrm{Jac}(C_{k_0})) = C_{4,1}$, all we need to check is that $\mathrm{End}(\mathrm{Jac}(C_{K_0}) \otimes \mathbb{R} \simeq \mathbb{H}$, where K_0 is the index 2 subfield of K given by $\mathbb{Q}[x]/(x^4 + 2x^3 + 4x^2 + 8x + 16)$. But this follows easily from

$$\mathrm{Aut}(C_{K_0}) \simeq \mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z}),$$

and the same argument used for the previous curve.

Product constructions. For $D = -19, -43, -67, -163$, let E_D be an elliptic curve defined over k_0 with CM by the quadratic imaginary field of discriminant D. A glimpse at [FKRS12, §4.4.] should suffice to convince the reader that

$$\mathrm{ST}(E_{-67} \times E_{-163}) = F, \quad \mathrm{ST}(E_{-19} \times E_{-67}) = F_a, \quad \mathrm{ST}(E_{-19} \times E_{-43}) = F_{ab}.$$

Finally, one has that $\mathrm{ST}(E_{-67} \times E) = G_{1,3}$, where E is any elliptic curve defined over k_0 without CM.

References

[Bea10]   A. Beauville, *Finite Subgroups of* $\mathrm{PGL}_2(K)$, Contemporary Math. **522** (2010), 23–29.

[Car01]   G. Cardona, *Models racionals de corbes de gènere* 2, Doctoral Thesis, Universitat Politècnica de Catalunya, 2001.

[CF00]   T. Chinburg, E. Friedman, *The finite subgroups of maximal arithmetic Kleinian groups*, Ann. Inst. Fourier Grenoble **50** (2000), 1765–1798.

[Cox89]   Cox, *Primes of the form* $x^2 + ny^2$, John Wiley & Sons, Inc., Canada, 1989.

[CQ07]   G. Cardona, J. Quer, *Curves of genus* 2 *with group of automorphisms isomorphic to* D_8 *or* D_{12}, Transactions of the American Mathematical Society **359**, No.6 (2007), 2831–2849.

[Elk04]   N.D. Elkies, *On elliptic k-curves*, in *Modular curves and abelian varieties*, edited by J. Cremona, J.-C. Lario, J. Quer and K.A. Ribet, Progress in Mathematics **224**, Birkhäuser Verlag, Basel, 2004.

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

[FKRS12] F. Fité, K.S. Kedlaya, A.V. Sutherland, V. Rotger, *Sato–Tate distributions and Galois endomorphism modules in genus 2*, Compositio Mathematica **148** n. 5 (2012), 1390–1442.

[Gro80]   B.H. Gross, *Arithmetic on elliptic curves with complex multiplication.* With an appendix by B. Mazur. Lecture Notes in Mathematics **776**, Springer, Berlin, 1980. iii+95 pp. ISBN: 3-540-09743-0

[GQ14]   X. Guitart, J. Quer, *Modular abelian varieties over number fields*, Canad. J. Math. **66** no. 1 (2014), 170–196.

[GK16]   R. Guralnick, K.S. Kedlaya, *Endomorphism fields of abelian varieties*, preprint, 2016, arXiv:1606.02803.

[Hei34]   H. Heilbronn, *On the class number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. 2 **5** (1934), 150–160.

[Kar87]   G. Karpilovsky, *The algebraic structure of crossed products.* North-Holland Mathematics Studies **142**. Notas de Matematica [Mathematical Notes], 118. North-Holland Publishing Co., Amsterdam, 1987. x+348 pp. ISBN: 0-444-70239-3

[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).

[LMFDB]   The LMFDB Collaboration, The *L*-functions and Modular Forms Database, `http://www.lmfdb.org`, 2013, [Online; accessed 16 September 2013].

[Mer81]   A.S. Merkur'ev, *On the norm residue symbol of degree* 2, Dokl. Akad. Nauk. SSSR **261** (1981), 542–547; Soviet Math. Dokl. **24** (1981), 546–551.

[Mil72]   J. Milne, *On the arithmetic of abelian varieties*, Invent. Math. **17** (1972), 177–190.

[MRS07]   B. Mazur, K. Rubin, A. Silverberg, *Twisting commutative algebraic groups*, Journal of Algebra **314** (2007), 419–438.

[Nak04]   T. Nakamura, *Elliptic $\mathbb{Q}$-curves with complex multiplication*, in *Modular curves and abelian varieties*, edited by J. Cremona, J.-C. Lario, J. Quer and K.A. Ribet, Progress in Mathematics **224**, Birkhäuser Verlag, Basel, 2004.

[Pari2]   The PARI Group, PARI/GP version `2.7.0`, Bordeaux, 2014, `http://pari.math.u-bordeaux.fr/`.

[Pyl02]   E.E. Pyle, *Abelian varieties over $\mathbb{Q}$ with large endomorphism algebras and their simple components over $\overline{\mathbb{Q}}$*, in *Modular curves and abelian varieties*, edited by J. Cremona, J.-C. Lario, J. Quer and K.A. Ribet, Progress in Mathematics **224**, Birkhäuser Verlag, Basel, 2004.

[Que95]   J. Quer, *Liftings of projective* 2-*dimensional Galois representations and embedding problems.* J. Algebra **171** (1995), no. 2, 541–566.

[Que00]   J. Quer, *$\mathbb{Q}$-curves and abelian varieties of GL_2-type.* Proc. London Math. Soc. **81** no. 2 (2000), 285–317.

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

[Rib94]   K. A. Ribet, *Fields of definition of abelian varieties with real multiplication*, Contemporary Math. **174** (1994), 1–12.

[S⁺14]   W. A. Stein et al. *Sage Mathematics Software (Version 6.1.1).* The Sage Development Team, 2014. `http://www.sagemath.org`.

[Ser84]   J.-P. Serre, *L'invariant de Witt de la forme* $\mathrm{Tr}(x^2)$. Comment. Math. Helv. **59** no. 4 (1984), 651–676.

[Ser98]   J.-P. Serre, *Représentations linéaires des groupes finis*, Hermann, Paris, 1998.

[Ser12]   J.-P. Serre, *Lectures on $N_X(p)$*, A.K. Peters, 2012.

[Sil92]   A. Silverberg, *Fields of definition for homomorphisms of abelian varieties*, Journal of Pure and Applied Algebra **77** (1992), 253–262.

[Sil86]   J. H. Silverman, *The arithmetic of elliptic curves.* Graduate Texts in Mathematics **106**, Springer-Verlag, New York, 1986.

[Sil94]   J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves.* Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994. xiv+525 pp. ISBN: 0-387-94328-5

[Wat03]   M. Watkins *Class numbers of imaginary quadratic fields*, Mathematics of Computation **246**, Vol. 73 (2003), 907–938.

Departament de Matemàtiques, Universitat Politècnica de Catalunya, Edifici Omega, C/Jordi Girona 1–3, 08034 Barcelona, Catalonia

  E-mail address: `francesc.fite@gmail.com`

  URL: `https://mat-web.upc.edu/people/francesc.fite/`

Departament d'Àlgebra i Geometria, Universitat de Barcelona, Gran via de les Corts Catalanes, 585, 08007 Barcelona, Catalonia

  E-mail address: `xevi.guitart@gmail.com`

  URL: `http://atlas.mat.ub.edu/personals/guitart/`