On polarised class groups of orders in quartic CM-fields

Gaetan Bisson* Marco Streng†

August 8, 2016

Abstract

We give an explicit necessary condition for pairs of orders in a quartic CM-field to have the same polarised class group. This generalises a simpler result for imaginary quadratic fields.

We give an application of our results to computing endomorphism rings of abelian surfaces over finite fields, and we use our results to extend a completeness result of Murabayashi and Umegaki [14] to a list of abelian surfaces over the rationals with complex multiplication by arbitrary orders.

1 Introduction

Let $\mathcal{A}$ be a principally polarised abelian surface defined over a characteristic-zero field k, and assume that $\mathcal{A}$ has *complex multiplication (CM)*, by which we mean that its endomorphism ring $R = \mathrm{End}(\mathcal{A}_{\overline{k}})$ is an order in a quartic number field K. Then K is a CM-field, that is, a totally imaginary quadratic extension of a totally real field K_0. The Galois group of the extension K/K_0 is generated by an element of order two, which we denote by $x \mapsto \overline{x}$ and call *complex conjugation* since it coincides with complex conjugation for every embedding $K \to \mathbf{C}$.

Our object of study is the *polarised class group* $\mathfrak{C}(R)$ of R defined as follows.

Definition 1. *Let I_R be the group of pairs $(\mathfrak{a}, \alpha)$ where $\mathfrak{a}$ is an invertible fractional ideal of R and $\alpha \in K_0$ is a totally positive element satisfying $\mathfrak{a}\overline{\mathfrak{a}} = \alpha R$. Let P_R be the subgroup formed by pairs of the form $(xR, x\overline{x})$ for $x \in K^\times$. The quotient I_R/P_R is called the* polarised ideal class group *of R and is written $\mathfrak{C}(R)$.*

This group was first introduced by Shimura and Taniyama [16, §14] in the case of the ring of integers $R = \mathbf{Z}_K$. It is significant to a number of problems regarding abelian varieties.

For instance, the group $\mathfrak{C}(R)$ acts faithfully on the set of isomorphism classes of principally polarised abelian surfaces with endomorphism ring R and the same *CM-type* as $\mathcal{A}$. Bisson exploits this to compute endomorphism rings of abelian surfaces [2]. This requires telling orders R apart using the structure of their groups $\mathfrak{C}(R)$, and our work will allow us to establish in how far this is possible. See Section 6.2.

*University of French Polynesia. http://gaati.org/bisson/

†Universiteit Leiden, The Netherlands. http://www.math.leidenuniv.nl/~streng/

We also use polarised class groups to extend van Wamelen's list of principally polarised abelian surfaces with conjectural CM by maximal orders [23]. We extend the list to arbitrary orders and then prove that it is correct and complete. The completeness result extends a result of Murabayashi and Umegaki [14] regarding the original list, and the correctness result is new in the sense that it completes a partial proof of van Wamelen [25]. See Section 6.1.

This paper is organised as follows. First, we introduce the necessary notation and state our results in Section 2. Section 3 then translates the relevant groups from a setting with ideals into a setting with elements of finite rings; this is where most of the work is done in comparing polarised class groups for varying orders. In Sections 4 and 5, the work of Section 3 is used in order to derive explicit bounds on the index between orders that have the same polarised class group. Finally, Section 6 presents our applications mentioned above.

We conclude this section by briefly recalling how the polarised ideal class group relates to the classical one; although this relationship is not used in this paper, we hope it might give the reader a better understanding of this group. Put $R_0 = R \cap K_0$ and let $\mathrm{Pic}_\infty(R_0)$ be the narrow class group of R_0, that is, the ray class group of the order R_0 for the infinite modulus. The order R is stable under complex conjugation because of the Rosati involution of $\mathcal{A}$, hence the norm is a map $N_{K/K_0} : R \to R_0$. The sequence

$$1 \longrightarrow R_0^{++}/N_{K/K_0}(R^\times) \longrightarrow \mathfrak{C}(R) \xrightarrow{\text{forget } \alpha} \mathrm{Pic}(R) \xrightarrow{N_{K/K_0}} \mathrm{Pic}_\infty(R_0),$$

is exact, where the map from the multiplicative group of totally positive elements R_0^{++} to $\mathfrak{C}(R)$ is $\alpha \mapsto ((1), \alpha)$.

2 Statement of the results

As before, let $\mathcal{A}$ be a principally polarised abelian surface with complex multiplication, denote by R its endomorphism ring, by $K = \mathbf{Q} \otimes R$ its CM-field, and by K_0 the totally real subfield of K. We note that this excludes abelian varieties that are not simple over the algebraic closure.

In what follows, we restrict ideals of I_R and P_R to be coprime to a fixed integer f; this has no effect on the group $\mathfrak{C}(R)$, but it allows us to compare the groups more effectively as the order R varies. Indeed, for any two orders $S \subset R$, the invertible ideals of S coprime to the index $f = [\mathbf{Z}_K : S]$ are in natural bijection with those of R via the map $\mathfrak{a} \mapsto \mathfrak{a}R$. This extends trivially to injections $I_S \to I_R$ and $P_S \to P_R$ which yield a natural morphism $\mathfrak{C}(S) \to \mathfrak{C}(R)$. We will use these maps implicitly and say for instance that an ideal $\mathfrak{a} \subset S$ is principal in R when we actually mean that $\mathfrak{a}R$ is.

To compare $\mathfrak{C}(S)$ and $\mathfrak{C}(R)$ in a computationally efficient manner, the algorithm of Bisson [2] uses certain elements of $\mathfrak{C}(S)$ best generated through the *reflex type norm* map. At the same time, the complex multiplication theory that describes the field of moduli of $\mathcal{A}$ is also phrased in terms of this map. For these reasons, our main results are formulated in terms of this map, which we now define.

In the following, let K be a CM-field of arbitrary degree. A CM-type Φ of K with values in $\mathbf{C}$ is a complete set of representatives for the embeddings

$K \to \mathbf{C}$ up to complex conjugation. The *reflex field* $K^r \subset \mathbf{C}$ of Φ is the subfield generated by the image of the *type norm*

$$\mathrm{N}_\Phi : K \to \mathbf{C} : x \mapsto \prod_{\phi \in \Phi} \phi(x).$$

The type norm is a half-norm in the sense that $\mathrm{N}_\Phi(x)\overline{\mathrm{N}_\Phi(x)} = N_{K/\mathbf{Q}}(x)$.

Example 2. CM-fields of degree 4 are either cyclic Galois, non-Galois with Galois group D_4 of order 8, or biquadratic Galois (with Galois group $C_2 \times C_2$). It is known that in the biquadratic Galois case, the abelian surface is non-simple and has a matrix ring as endomorphism ring, so this paper restricts to the non-biquadratic case.

In the C_4-case, let $\mathrm{Gal}(K/\mathbf{Q}) = \langle \rho \rangle$ and, in the D_4-case, let $\mathrm{Gal}(K^c/K) = \langle \sigma \rangle$ and $\mathrm{Gal}(K^c/\mathbf{Q}) = \langle \sigma, \rho \rangle$ with $\rho^4 = \sigma^2 = \sigma\rho\sigma\rho = \mathrm{id}$, where K^c denotes the normal closure of K. In both cases, we have $\rho^2 = \bar{\cdot}$ and there exists an embedding $\phi : K^c \to \mathbf{C}$ such that $\Phi = \{\phi, \phi \circ \rho\}$. In the C_4-case, we have $K^r = \phi(K) \cong K$. In the non-Galois case, we have $K^r = \phi(K') \not\cong K$, where $K' \subset K^c$ is the fixed field of $\langle \rho\sigma \rangle \subset \mathrm{Gal}(K^c/\mathbf{Q})$.

The *reflex type* [16, §8] is the set $\Phi^r = \{\psi^{-1}_{|K^r} : \psi \in S\}$ of embeddings of K^r into the normal closure K^c of K, where S is the set of all embeddings of K^c into $\mathbf{C}$ that extend elements of Φ.

Example 3. Concretely in the quartic non-biquadratic situation above, we have a map $\phi^{-1} : K^r \to K^c$ and $\Phi^r = \{\phi^{-1}, \rho^{-1} \circ \phi^{-1}\}$.

The reflex type is a CM-type of K^r with values in K^c and reflex field K, hence defines a type norm $\mathrm{N}_{\Phi^r} : K^r \to K$. This norm can be extended into a homomorphism from the group $I_{K^r} = I_{K^r}(f)$ of invertible ideals $\mathfrak{a}$ of R_{K^r} coprime to f to the analogous group for R. In turn, this defines a map

$$\begin{aligned} I_{K^r}(f) &\longrightarrow \mathfrak{C}(R), \\ \mathfrak{a} &\longmapsto (\mathrm{N}_{\Phi^r}(\mathfrak{a}), \mathrm{N}_{K^r/\mathbf{Q}}(\mathfrak{a})). \end{aligned} \tag{1}$$

We denote its kernel by Ω_R. It is an important object because the image $I_{K^r}(f)/\Omega_R$ appears naturally as the Galois group of the field of moduli of the abelian surfaces of type Φ with endomorphism ring R [16, Main Theorem 3 on page 142]. Our main results are the following two theorems, together with their ingredients from Section 3 and applications in Section 6.

Theorem 4. *For any order T stable under complex conjugation in a quartic non-biquadratic CM-field $K \not\cong \mathbf{Q}(\zeta_5)$ satisfying $\Omega_{\mathbf{Z}_K} \subset \Omega_T$ we have*

$$[\mathbf{Z}_K : T]^2 \ \mid\ 2^{40}3^{16} N_{K_0/\mathbf{Q}}(\Delta_{K/K_0}).$$

Throughout this paper, we let R and T be any two orders stable under complex conjugation in a quartic non-biquadratic CM-field K. We define $S = R \cap T$ and denote the intersection of any of these orders with the totally real subfield K_0 (which gives an order in K_0) by adding a subscript 0 to it.

Theorem 5. *Let the notation be as above. If $\Omega_R \subset \Omega_T$ and $R \not\cong \mathbf{Z}[\zeta_5]$, then the quotient $[R : S]/[R_0 : S_0]$ is an integer dividing $2^{10}3^4$.*

We do not claim that the constants are optimal, but we do show in Example 15 that the index $[R_0 : S_0]$ is necessary in Theorem 5. On the other hand, it remains an open question whether the discriminant factor is necessary in Theorem 4.

For the excluded case $R = \mathbf{Z}[\zeta_5]$, we show in Section 6.1 that if $\Omega_{\mathbf{Z}[\zeta_5]} \subset \Omega_T$, then $[\mathbf{Z}[\zeta_5] : T]$ divides one of 2^4, 3^2 and 5^2.

3 From ideals to elements

If R and T are two orders of a quartic non-biquadratic CM-field K, we obviously have the implication $R \subset T \Rightarrow \Omega_R \subset \Omega_T$. The goal of Section 4 is to establish a partial converse to this statement, that is, to obtain an explicit condition on R and T necessary for $\Omega_R \subset \Omega_T$ to hold. To help with that, we first express some relevant groups in terms of ring *elements*, as opposed to ideals. Recall that S denotes the intersection of R and T, and fix $f = [\mathbf{Z}_K : S]$ once and for all.

Lemma 6. *All squares of elements of $\mathfrak{C}(S)$ are in the image of the type norm map* (1)*.*

Proof. The key to this result is the following observation, which is also [21, Lemma 2.6] and, in the case of maximal orders, [20, Lemma I.8.4]. Let $\tau = \rho_{|K_0}$ be the nontrivial automorphism of K_0. For every invertible R-ideal $\mathfrak{a}$, we have $N_{\Phi^r}(N_\Phi(\mathfrak{a})) = \mathfrak{a}^2\tau(\mathfrak{a}\overline{\mathfrak{a}})$. The proof of this follows directly from Examples 2 and 3 since

$$N_{\Phi^r}(N_\Phi(\mathfrak{a})) = {}^{(1+\rho^{-1})\phi^{-1}}({}^{\phi(1+\rho)}\mathfrak{a}) = {}^{(2+\rho^{-1}+\rho)}\mathfrak{a} = \tau(\mathfrak{a}\overline{\mathfrak{a}})\mathfrak{a}^2.$$

For any $(\mathfrak{a}, \alpha) \in I_S$ we have

$$(\mathfrak{a}, \alpha)^2 = (\tau(\alpha)S, (\tau(\alpha))^2)^{-1}(\mathfrak{a}^2\tau(\mathfrak{a}\overline{\mathfrak{a}}), N_{K_0/\mathbf{Q}}(\alpha)^2). \tag{2}$$

The first factor is trivial in $\mathfrak{C}(S)$, and the second factor is obtained from $\mathfrak{a}$ via the map of (1). This proves that the class of $(\mathfrak{a}, \alpha)^2$ is in the image. □

By Lemma 6, a necessary condition for $\Omega_R \subset \Omega_T$ is

$$\ker(\mathfrak{C}(S)^2 \to \mathfrak{C}(R)) \quad \subset \quad \ker(\mathfrak{C}(S)^2 \to \mathfrak{C}(T)), \tag{3}$$

and, to write these kernels in terms of ring elements, we use the following lemma.

Lemma 7. *Denote by ϕ the natural morphism $\mathfrak{C}(S) \to \mathfrak{C}(R)$ and consider the relative norm*

$$\psi : \frac{(R/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times \mu_R} \longrightarrow \frac{(R_0/f\mathbf{Z}_{K_0})^\times}{(S_0/f\mathbf{Z}_{K_0})^\times}. \tag{4}$$

We have $\ker\phi = \ker\psi$ *and* $\operatorname{coker}\phi \subset \operatorname{coker}\psi$*.*

To prove the above we first require a simple technical result.

Lemma 8. *An ideal $\mathfrak{a}$ of S is coprime to f (that is, it satisfies $\mathfrak{a} + fS = S$) if and only if it satisfies $\mathfrak{a} + f\mathbf{Z}_K = S$.*

Proof. Recall that $f\mathbf{Z}_K \subset S$. The "only if" part is trivial. Now for the converse, suppose that $\mathfrak{a}$ satisfies $\mathfrak{a} + f\mathbf{Z}_K = S$; it follows that $(\mathfrak{a} + f\mathbf{Z}_K)^2 = S$. Since $(\mathfrak{a} + f\mathbf{Z}_K)^2 \subset \mathfrak{a} + (f\mathbf{Z}_K)^2$ and $(f\mathbf{Z}_K)^2 \subset fS$, we deduce that $\mathfrak{a} + fS = S$. □

We may now prove Lemma 7 and make free and implicit use of Lemma 8.

Proof of Lemma 7. Recall $R_0 = R \cap K_0$ and $S_0 = S \cap K_0$. The diagram

$$\begin{tikzcd}
1 \arrow[r] & P_S \arrow[r] \arrow[d, hook] & I_S \arrow[r] \arrow[d, hook] & \mathfrak{C}(S) \arrow[r] \arrow[d, "\phi"'] & 1 \\
1 \arrow[r] & P_R \arrow[r] & I_R \arrow[r] & \mathfrak{C}(R) \arrow[r] & 1
\end{tikzcd}$$

has exact rows and, as we restrict to ideals coprime to f, its two leftmost vertical arrows are injective. The snake lemma thus tells us that

$$(\mathrm{co})\ker \phi = (\mathrm{co})\ker \left(\frac{P_R}{P_S} \to \frac{I_R}{I_S} \right).$$

It now suffices to give a natural isomorphism and an embedding

$$\frac{P_R}{P_S} = \frac{(R/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times \mu_R}, \qquad \frac{I_R}{I_S} \hookrightarrow \frac{(R_0/f\mathbf{Z}_{K_0})^\times}{(S_0/f\mathbf{Z}_{K_0})^\times}$$

such that the induced map is ψ. For these maps, we take $(xR, x\overline{x}) \mapsto x$ (for integral representatives $(xR, x\overline{x})$ of elements of P_R/P_S) and $(\mathfrak{a}, \alpha) \mapsto \alpha$ (for integral representatives $(\mathfrak{a}, \alpha)$ of elements of I_R/I_S).

On P_R, the first map is well-defined, as $(xR, x\overline{x})$ determines x up to roots of unity in R. The kernel then consists of those pairs $(xR, x\overline{x})$ with x in S invertible modulo f, that is, such that xS is coprime to f. In other words, the kernel is P_S, so the map is indeed well-defined and injective on P_R/P_S. Surjectivity is obvious.

The second map is well-defined on I_R/I_S. Now suppose that $(\mathfrak{a}, \alpha)$ is in the kernel, again without loss of generality with $\mathfrak{a}$ integral. Then αS_0 is coprime to f, so αS is also coprime to f. Denoting by $\mathfrak{b}$ the unique S-ideal coprime to f satisfying $\mathfrak{a} = \mathfrak{b}R$, we have $\mathfrak{b}\overline{\mathfrak{b}}R = \alpha R$ and, as αS and $\mathfrak{b}$ are coprime to f, we find $(\mathfrak{b}, \alpha) \in I_S$ which implies $(\mathfrak{a}, \alpha) \in I_S$ by abuse of notation. This proves injectivity.

Finally, the induced map ψ is indeed the relative norm, as x maps via $(xR, x\overline{x})$ to $x\overline{x}$. □

Using Lemma 7, the necessary condition (3) becomes as follows.

Proposition 9. *Let R and T be orders in a quartic non-biquadratic CM-field K and let $S = T \cap R$. If we have $\Omega_R \subset \Omega_T$, then the kernel*

$$\ker \left(\psi : \frac{(R/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times \mu_R} \to \frac{(R_0/f\mathbf{Z}_{K_0})^\times}{(S_0/f\mathbf{Z}_{K_0})^\times} \right) \tag{5}$$

is of exponent at most two.

Proof. By (3), if $\Omega_R \subset \Omega_T$, then we have

$$\begin{aligned}\ker\left(\mathfrak{C}(S) \to \mathfrak{C}(R)\right)^2 &\subset \ker\left(\mathfrak{C}(S)^2 \to \mathfrak{C}(R)\right) \\ &\subset \ker\left(\mathfrak{C}(S)^2 \to \mathfrak{C}(T)\right) \subset \ker\left(\mathfrak{C}(S) \to \mathfrak{C}(T)\right),\end{aligned}$$

hence

$$\ker\left(\mathfrak{C}(S)\to\mathfrak{C}(R)\right)^2 \quad\subset\quad \ker\left(\mathfrak{C}(S)\to\mathfrak{C}(T)\right)\cap\ker\left(\mathfrak{C}(S)\to\mathfrak{C}(R)\right). \tag{6}$$

We wish to apply Lemma 7 to both R and T and compare the results, so we need some common supergroup for

$$\frac{(R/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times\mu_R} \quad\text{and}\quad \frac{(T/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times\mu_T}$$

to compare them in. We start by proving that the natural map

$$\iota_R : \frac{(R/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times\mu_R} \to \frac{(\mathbf{Z}_K/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times\mu_{\mathbf{Z}_K}}$$

is injective and compatible with the natural isomorphisms to P_R/P_S and $P_{\mathbf{Z}_K}/P_S$ of the proof of Lemma 7. The latter is trivial, as we take ideals coprime to $f\mathbf{Z}_K$ in K. The former then follows by injectivity of the inclusion $P_R/P_S \subset P_{\mathbf{Z}_K}/P_S$.

Next, note that we have $\operatorname{im}(\iota_R)\cap\operatorname{im}(\iota_T) = 1$. Indeed, if $\overline{x} = (x + f\mathbf{Z}_K) \in (\mathbf{Z}_K/f\mathbf{Z}_K)^*$ represents an element X of the intersection, then $\overline{x} \in (R + f\mathbf{Z}_K)^*$ and $\overline{x} \in (T + f\mathbf{Z}_K)^*$, so $\overline{x} \in (S + f\mathbf{Z}_K)^*$, hence X is trivial.

Applying Lemma 7 to both R and T, equation (6) becomes

$$\begin{aligned}
&\ker\left(\frac{(R/f\mathbf{Z}_K)^\times}{(S/f\mathbf{Z}_K)^\times\mu_R} \to \frac{(R_0/f\mathbf{Z}_{K_0})^\times}{(S_0/f\mathbf{Z}_{K_0})^\times}\right)^2 \\
\subset\quad &\ker\left(\operatorname{im}(\iota_R) \to \frac{(\mathbf{Z}_{K_0}/f\mathbf{Z}_{K_0})^\times}{(S_0/f\mathbf{Z}_{K_0})^\times}\right) \cap \ker\left(\operatorname{im}(\iota_T) \to \frac{(\mathbf{Z}_{K_0}/f\mathbf{Z}_{K_0})^\times}{(S_0/f\mathbf{Z}_{K_0})^\times}\right) \\
\subset\quad &\ker\left((\operatorname{im}(\iota_R)\cap\operatorname{im}(\iota_T)) \to \frac{(\mathbf{Z}_{K_0}/f\mathbf{Z}_{K_0})^\times}{(S_0/f\mathbf{Z}_{K_0})^\times}\right) = 1. \qquad\square
\end{aligned}$$

Note that, unless $R \cong \mathbf{Z}[\zeta_5]$, the unit group $\mu_R = \{\pm 1\}$ can be absorbed into $(S/f\mathbf{Z}_K)^\times$.

4 Explicit bounds

We shall now derive from Proposition 9 a more explicit necessary condition for $\Omega_R \subset \Omega_T$ on the indices of the relevant orders. First, let us give a weak but natural result bounding the size of the quotient groups of (5) in terms of these indices.

Proposition 10. *Let $S \subset R$ be two orders in a number field K of degree n, and let f be a multiple of the index $[R:S]$; we have*

$$[R:S]\prod_{p\mid f}(1-1/p)^n \le \left|\frac{(R/fR)^\times}{(S/fR)^\times}\right| \le [R:S]\prod_{p\mid f}(1-1/p)^{-n}.$$

Proof. Decomposing the ring R/fR over prime ideals $\mathfrak{p}$ of R dividing f yields

$$\left|(R/fR)^\times\right| = |(R/fR)|\prod_{\mathfrak{p}}(1-1/\operatorname{N}(\mathfrak{p})).$$

Since there are at most n such $\mathfrak{p}$ dividing each prime factor p of f, we derive

$$\frac{|(R/fR)^\times|}{|(S/fR)^\times|} \geq \frac{|(R/fR)|}{|(S/fR)|}\prod_{\mathfrak{p}}(1-1/\,\mathrm{N}(\mathfrak{p})) \geq [R:S]\prod_{p|f}(1-1/p)^n$$

and the second inequality follows similarly. ☐

Proposition 10 immediately leads to the following bounds.

Lemma 11. *Given a quartic CM-field K and orders as in the previous sections, let $v = \mathrm{val}_p([R:S]/[R_0:S_0])$. If the group (5) is of exponent one or two, we have $p^{v-6}(p-1)^6 \leq 2^3\#\mu_R$.*

In particular, if $R \not\cong \mathbf{Z}[\zeta_5]$, then for $p=2$ we have $v \leq 10$, and for $p=3$ we have $v \leq 4$. Finally, if $v \geq 1$, then $p < 10\#\mu_R$.

Proof. By Proposition 10, the domain in (5) has order greater than or equal to

$$[R:S]\frac{(1-1/p)^4}{\#(\mu_R/\{\pm 1\})},$$

while the codomain has order at most $[R_0:S_0](1-1/p)^{-2}$, hence the kernel has order $\geq p^v(1-1/p)^6/\#(\mu_R/\{\pm 1\})$. On the other hand, the kernel is generated by a set of at most four elements, so, if it has exponent at most 2, then its order is at most 2^4, which yields the first bound.

The other bounds are specialisations of this first bound, using the fact that $R \not\cong \mathbf{Z}[\zeta_5]$ implies $\mu_R = \{\pm 1\}$. ☐

The bounds on v of Lemma 11 can easily be sharpened with elementary observations about the groups involved, but it is hard to make them completely sharp, so we leave them as they are. Instead, we sharpen the bound on the prime p by looking more closely at the structure of the groups.

Proposition 12. *If the kernel (5) contains no element of order greater than two, then for every prime p we have $v := \mathrm{val}_p([R:S]/[R_0:S_0]) = 0$, except possibly for $p \leq 3$, and except possibly for $p \leq 19$ if $R = \mathbf{Z}[\zeta_5]$.*

Proof. Assume that the kernel (5) is of exponent one or two, and suppose that there exists a prime $p \geq 5$ at which the quotient $[R:S]/[R_0:S_0]$ is nontrivial.

To better work with this kernel, we first write the domain and codomain of the relative norm map of (5) more explicitly by decomposing the p-part of the ring $R/f\mathbf{Z}_K$ over primes ideals $\mathfrak{q}$ of R dividing $(p) = pR$; this gives

$$(R/(f\mathbf{Z}_K)_{(p)})^\times = \prod_{\mathfrak{q}}(R/(f\mathbf{Z}_K)_{(\mathfrak{q})})^\times \cong \prod_{\mathfrak{q}}(R/\mathfrak{q})^\times \times \frac{1+\mathfrak{q}}{1+(f\mathbf{Z}_K)_{(\mathfrak{q})}},$$

where $I_{(\mathfrak{q})}$ denotes the $\mathfrak{q}$-primary part of I, that is, $I_{(\mathfrak{q})} = (I\cdot R_{\mathfrak{q}})\cap R = I + \mathfrak{q}^n$ for all sufficiently large n (see [18]). Therefore, omitting the case $R \cong \mathbf{Z}[\zeta_5]$ for now, we find that dividing out by $\mu_R = \{\pm 1\}$ is trivial and the domain from (5) can be written locally at p as

$$D := \frac{(R/(f\mathbf{Z}_K)_{(p)})^\times}{(S/(f\mathbf{Z}_K)_{(p)})^\times} \cong \frac{\prod_{\mathfrak{q}}(R/\mathfrak{q})^\times}{\prod_{\mathfrak{p}}(S/\mathfrak{p})^\times}\times A_p;$$

for some p-group A_p. Similarly, the codomain can be written locally at p as

$$C := \frac{(R_0/(f\mathbf{Z}_{K_0})_{(p)})^\times}{(S_0/(f\mathbf{Z}_{K_0})_{(p)})^\times} \cong \frac{\prod_{\mathfrak{q}_0}(R_0/\mathfrak{q}_0)^\times}{\prod_{\mathfrak{p}_0}(S_0/\mathfrak{p}_0)^\times} \times A_{0,p}.$$

The rightmost factors $A_{0,p} \subset A_p$ are p-groups and, as p is odd and the kernel (5) has exponent at most two, they are equal.

Since R_0 and S_0 are quadratic, the non-p-part of the codomain C is cyclic and of order 1, $p-1$ or $p+1$. Correspondingly, the p-part $[R_0 : S_0]_p$ of the index is $\#A_{0,p}$ in the first case and $p \cdot \#A_{0,p}$ in the other cases.

On the other hand, the domain D is a product of cyclic groups with orders of the form p^e, $p^f - 1$ and $(p^g - 1)/(p^h - 1)$ where the exponents f, g, h, are in $\{1, 2, 4\}$ and $h < g$. The valuation at p of the index $[R : S]$ is then the sum of all e's, f's and $(g-h)$'s. As the exponent of the kernel is at most two, the order of each of the coprime-to-p cyclic factors must divide the non-p-part of $2\#C$, which is 2, $2(p-1)$ or $2(p+1)$.

As $p \geq 5$, it is easy to see that $p^f - 1$ and $(p^g - 1)/(p^h - 1)$ do not divide $2\#C$, except when they are equal to $\#C/\#A_{0,p} \in \{p-1, p+1\}$. As these numbers are greater than three, this observation also shows that if there were multiple such cyclic factors in D, it would contradict the fact that a quotient by a 2-torsion subgroup is contained in C.

In particular, we get $\mathrm{val}_p([R : S]) \in \{\#A_p, \#A_p + 1\}$, where the second case is only possible when $[R_0 : S_0] = \#A_{0,p} + 1$. We thus conclude $\mathrm{val}_p([R : S]) = \mathrm{val}_p([R_0 : S_0])$.

It remains to consider the case $R \cong \mathbf{Z}[\zeta_5]$ where $\mu_R \simeq \mathbf{Z}/10\mathbf{Z}$. In this case, the orders of the cyclic factors of D must divide $10\#C$, and the proof goes through for $p > 19$. ☐

Theorem 5. *If $\Omega_R \subset \Omega_T$ and $R \not\cong \mathbf{Z}[\zeta_5]$, then the quotient $[R : S]/[R_0 : S_0]$ is an integer dividing $2^{10}3^4$.*

Proof. This is a combination of Lemma 11 and Propositions 9 and 12. ☐

5 Stronger result in the maximal case

The result of Proposition 12, namely that $\mathrm{val}_p[R : S] = \mathrm{val}_p[R_0 : S_0]$ for all but finitely many primes p, may not seem very strong. Only when $R_0 = S_0$ does it immediately imply that R and S are identical locally at all $p > 3$. The goal of this section is to prove that, in the case $R = \mathbf{Z}_K$ and $T = S$, Proposition 12 further implies that R and T are identical locally if we rule out a few more primes p.

Theorem 4. *For any order S stable under complex conjugation in a quartic non-biquadratic CM-field $K \not\cong \mathbf{Q}(\zeta_5)$ satisfying $\Omega_{\mathbf{Z}_K} \subset \Omega_S$ we have*

$$[\mathbf{Z}_K : S]^2 \ \mid \ 2^{40}3^{16} N_{K_0/\mathbf{Q}}(\Delta_{K/K_0}).$$

To prove the theorem, we first show that $[\mathbf{Z}_{K_0} : S_0]^2$ almost divides $[\mathbf{Z}_K : S]$.

Lemma 13. *Let $K_0/\mathbf{Q}$ be a quadratic field and K/K_0 a finite Galois extension of degree n. Let S be an order of K stable under* $\mathrm{Gal}(K/K_0)$*, and let $S_0 = S \cap K_0$. We have*

$$[\mathbf{Z}_{K_0} : S_0]^{2n} \ \mid \ N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})\ [\mathbf{Z}_K : S]^2. \tag{7}$$

Proof. Write the orders as $\mathbf{Z}_{K_0} = \mathbf{Z} + \omega\mathbf{Z}$ and $S_0 = \mathbf{Z} + c\omega\mathbf{Z}$ where $c = [\mathbf{Z}_{K_0} : S_0]$, and let $\delta = 2\omega - \mathrm{tr}_{K_0/\mathbf{Q}}(\omega)$. Note that (δ) is the different of K_0.

First of all, we have $\mathrm{tr}_{K/\mathbf{Q}}(\delta^{-1}S) = \mathrm{tr}_{K_0/\mathbf{Q}}(\mathrm{tr}_{K/K_0}(\delta^{-1}S))$. Using the fact that K/K_0 is Galois and S is stable under Galois, we find $\mathrm{tr}_{K/K_0}(S) \subset S_0$, so $\mathrm{tr}_{K/\mathbf{Q}}(\delta^{-1}S) \subset \mathrm{tr}_{K_0/\mathbf{Q}}(\delta^{-1}S_0) = c\mathbf{Z}$. In particular, $(c\delta)^{-1}S$ is contained in the trace dual S^* of S, so the following index is an integer:

$$\begin{aligned}
[S^* : (c\delta)^{-1}S] &= N_{K/\mathbf{Q}}(c\delta)^{-1}[S^* : {\mathbf{Z}_K}^*][{\mathbf{Z}_K}^* : \mathbf{Z}_K][\mathbf{Z}_K : S] \\
&= c^{-2n}\Delta_{K_0/\mathbf{Q}}^{-n}[S^* : {\mathbf{Z}_K}^*]\Delta_{K/\mathbf{Q}}[\mathbf{Z}_K : S] \\
&= c^{-2n}N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})[S^* : {\mathbf{Z}_K}^*][\mathbf{Z}_K : S].
\end{aligned}$$

Linear algebra gives us $[S^* : {\mathbf{Z}_K}^*] = [\mathbf{Z}_K : S]$, and the result follows. $\square$

Proof of Theorem 4. Let $S = T$. Then Theorem 5 and Lemma 13 give

$$[\mathbf{Z}_K : S]^4 \ \mid \ (2^{10}3^4)^4[\mathbf{Z}_{K_0} : S_0]^4 \ \mid \ 2^{40}3^{16}N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})[\mathbf{Z}_K : S]^2.$$

Dividing both sides by $[\mathbf{Z}_K : S]$ yields the result. $\square$

Example 14. The factor $N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$ on the right hand side of (7) cannot be omitted. Consider for instance the order

$$S = \mathbf{Z}[5\sqrt{7}] + \sqrt{5 \cdot (-3 + \sqrt{7})}\mathbf{Z}[\sqrt{7}]$$

of which the real order is $S_0 = \mathbf{Z}[5\sqrt{7}]$. The indices $[\mathbf{Z}_K : S]$ and $[\mathbf{Z}_{K_0} : S_0]$ are both 5, so Lemma 13 would be false without that factor.

Example 15. The index $[R_0 : S_0]$ is required in Theorem 5. Indeed, let K be any quartic CM-field with $\mathbf{Z}_K = \mathbf{Z}[\beta]$, where β is a square root of a totally negative number in K_0; fix a positive odd integer F and let

$$\begin{aligned}
R &= \mathbf{Z} + F^2\beta\mathbf{Z} + F^2\beta^2\mathbf{Z} + F^2\beta^3\mathbf{Z}; \\
R' &= \mathbf{Z} + F^2\beta\mathbf{Z} + F\beta^2\mathbf{Z} + F^2\beta^3\mathbf{Z}.
\end{aligned}$$

Note $R \subset T$. The corresponding real orders are

$$\begin{aligned}
R_0 &= \mathbf{Z} + F^2\beta^2\mathbf{Z}; \\
T_0 &= \mathbf{Z} + F\beta^2\mathbf{Z}.
\end{aligned}$$

We have $(R/F^2\mathbf{Z}_K) = (R_0/F^2\mathbf{Z}_{K_0})$ and $(T/F^2\mathbf{Z}_K) = (T_0/F^2\mathbf{Z}_{K_0})$; their respective unit groups have order $(F-1)F^3$ and $(F-1)F$. Thus, the map ψ from Proposition 9 with $f = F^2$ maps x to $x\overline{x} = x^2$ on a group of odd order F^2; therefore we have $\ker(\psi) = 1$ which implies $\Omega_R = \Omega_T$.

Concretely, the field $K = \mathbf{Q}(\beta)$ with $\beta = \sqrt{-3 + \sqrt{2}}$ satisfies $\mathbf{Z}_K = \mathbf{Z}[\beta]$. But really the assumption $\mathbf{Z}_K = \mathbf{Z}[\beta]$ is only there to simplify the argument.

6 Applications

6.1 Abelian surfaces with complex multiplication over the rationals

6.1.1 Statements

Van Wamelen [23] gives a conjectural list of curves of genus two defined over $\mathbf{Q}$ with complex multiplication by maximal orders. Our results allow us to finish the proof of this list, as well as generalise it to arbitrary orders.

Theorem 16 (Extending results of Murabayashi-Umegaki [14] and Van Wamelen [25])**.** *The* 19 *curves given in [23] are (up to $\overline{\mathbf{Q}}$-isomorphism) exactly the curves $C/\mathbf{Q}$ of genus two with* $\mathrm{End}(J(C)_{\overline{\mathbf{Q}}}) \cong \mathbf{Z}_K$ *for a quartic CM-field K.*

Theorem 17. *The curves*

$$\begin{aligned} C &: y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1 \qquad \textit{and} \\ D &: y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3 \end{aligned}$$

have endomorphism rings

$$\begin{aligned} \mathrm{End}(J(C)_{\overline{\mathbf{Q}}}) &\cong \mathbf{Z} + 2\zeta_5\mathbf{Z} + (\zeta_5^2 + \zeta_5^3)\mathbf{Z} + 2\zeta_5^3\mathbf{Z} \qquad \textit{and} \\ \mathrm{End}(J(D)_{\overline{\mathbf{Q}}}) &\cong \mathbf{Z} + (\zeta_5 + 3\zeta_5^3)\mathbf{Z} + (\zeta_5^2 + \zeta_5^3)\mathbf{Z} + 5\zeta_5^3\mathbf{Z}. \end{aligned}$$

Moreover, they are (up to $\overline{\mathbf{Q}}$-isomorphism) the only curves of genus two with field of moduli $\mathbf{Q}$ such that $\mathrm{End}(J(C)_{\overline{\mathbf{Q}}})$ *is a* non-*maximal order in any of the fields in Tables 1 and 2 below.*

Pınar Kılıçer, with the second-named author, proves that all cyclic quartic CM-fields K with $\Omega_{\mathbf{Z}_K} = I_{K^r}$ appear in Tables 1 and 2. In particular, the 21 curves of Theorems 16 and 17 are (up to $\overline{\mathbf{Q}}$-isomorphism) exactly the curves $C/\mathbf{Q}$ of genus two such that $\mathrm{End}(J(C)_{\overline{\mathbf{Q}}}) \otimes \mathbf{Q}$ is a quartic field. See [10].

We give the proofs of Theorems 16 and 17 in Sections 6.1.4 and 6.1.5.

6.1.2 Background

We start by explaining what in Theorem 16 was already proven, and what remained to be. Murabayashi and Umegaki [14] prove that the 13 fields in Table 1 are the only quartic fields whose maximal orders are endomorphism rings of genus-two curves over $\mathbf{Q}$.

Van Wamelen [23] computes that each of the 13 fields in this list has 1 or 2 curves corresponding to it, and determines these curves numerically to high precision. This yields his list of 19 curves referenced in the theorem. Van Wamelen [25] later proved that each of his 19 curves does have complex multiplication, and though he does not prove that the endomorphism ring is the *maximal* order, he suggests how to prove this by numerical approximation. We will use our methods to finish the proof that the order is maximal while avoiding numerical approximation.

Another proof of correctness appears in [6], which is based on interval arithmetic and formulas of [13]. Our proof predates that proof and, while it is more complicated, our proof requires no numerical approximations.

6.1.3 Relation of Theorems 16 and 17 to our results

Denote by $I_{K^r}(f)$ the group of fractional ideals of R_{K^r} coprime to a fixed integer f. We will first explain how its subgroup Ω_R relates to Theorems 16 and 17. Let C/k be a curve of genus two over a number field, and suppose that the endomorphism ring $\mathrm{End}(J(C)_{\overline{k}})$ is isomorphic to an order R in a quartic field K.

Then K is a CM-field, and the theory of complex multiplication gives us some CM-type belonging to the isomorphism $R \to \mathrm{End}(J(C)_{\overline{k}})$. Let (K^r, Φ^r) be the reflex of (K, Φ). By the Main Theorem of Complex Multiplication for arbitrary orders [16, §17.3, Main Theorem 3], the composite $k \cdot K^r$ contains the unramified class field k_1 of K^r corresponding to the ideal group $\Omega_R \subset I_{K^r}(f)$.

In particular, if $k = \mathbf{Q}$, then $k_1 = K^r$, so the inclusions $\Omega_R \subset \Omega_{\mathbf{Z}_K} \subset I_{K^r}(f)$ are equalities. The following result explicitly generates a minimal order with this property.

Lemma 18. *Let $K \not\cong \mathbf{Q}(\zeta_5)$ be a non-biquadratic quartic CM-field with $\Omega_{\mathbf{Z}_K} = I_{K^r}$. Let the ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset \mathbf{Z}_{K^r}$ be generators of the ray class group of K^r modulo f, and let $\mu_i \in K^\times$ be generators of $N_{\Phi^r}(\mathfrak{a}_i)$ such that $\mu_i\overline{\mu_i} \in \mathbf{Q}$.*

Let R be an order in K such that $f\mathbf{Z}_K \subset R$. We have $\Omega_R = I_{K^r}$ if and only if $R \supset R_{\min,f} := \mathbf{Z}[\mu_i : i \in \{1, \ldots, n\}] + f\mathbf{Z}_K$.

Proof. The $\mu_i \in \mathbf{Z}_K$ exist as $\Omega_{\mathbf{Z}_K} = I_{K^r}$, and they are uniquely determined up to roots of unity, hence uniquely determined up to sign as $K \not\cong \mathbf{Q}(\zeta_5)$. Since R is a ring and $\Omega_R = I_{K^r}$, both μ_i and $-\mu_i$ are in R for each i, hence R contains $R_{\min,f}$. Conversely, if R contains $R_{\min,f}$, then $\Omega_R = I_{K^r}$. $\square$

6.1.4 The case of maximal orders (proof of Theorem 16)

The first curve $y^2 = x^5 + 1$ is well-known to have endomorphism ring $\mathbf{Z}[\zeta_5]$ [16, Example 15.4.2], and van Wamelen computed (as mentioned above) that it is unique with this property.

Next, [25], or more precisely, its data set [24], gives, for each of the other 12 fields in Table 1, an order R' with a proof that $R := \mathrm{End}(J(C)_{\overline{\mathbf{Q}}}) \supset R'$ holds for the curve(s) corresponding to that field. We give these orders in Table 1. As $J(C)$ is principally polarised, the Rosati involution maps R into itself, and since the Rosati involution acts as complex conjugation on $K = \mathbf{Q}(R)$, this implies $R \supset R' + \overline{R'} =: R''$. At the same time, as K has no imaginary quadratic subfields, the endomorphism ring R is an order in K by [11, Theorem 1.3.3].

Next, we take f such that $f\mathbf{Z}_K \subset R''$ and compute $R_{\min,f}$ as in Lemma 18 using Sage [17]. That lemma then gives $R \supset R'' + R_{\min,f} =: R'''$, so we compute the latter ring. Note that this ring does not depend on the CM-type Φ appearing in Lemma 18. Indeed, the reflex field $K^r \subset \mathbf{C}$ is the unique subfield isomorphic to K, and as $\mathrm{Gal}(K^r/\mathbf{Q}) \cong C_4$, all CM-types of K^r with values in K are of the form $\Phi^r \circ \sigma$ with $\sigma \in \mathrm{Gal}(K^r/\mathbf{Q})$, so $N_{\Phi^r \circ \sigma}(\mathfrak{a}_i) = N_{\Phi^r}(\sigma(\mathfrak{a}_i))$.

The resulting orders R''' are equal to $\mathbf{Z}_K$ in all but two cases. In the other two, we use Sage [17] to compute the principally polarised ideal classes of R''' as in [7, Section 4.3], and find that each of them has CM by the maximal order. This proves Theorem 16. $\square$

$[D, A, B]$	n	χ	i_1	i_2	i_3
$[5, 5, 5]$	1				
$[8, 4, 2]$	1	$x^4 + 4x^2 + 2$	1	1	1
$[13, 13, 13]$	1	$x^4 - x^3 + 2x^2 + 4x + 3$	3	1	1
$[5, 10, 20]$	2	$x^4 + 10x^2 + 20$	4	4	2
$[5, 65, 845]$	2	$x^4 - x^3 + 16x^2 - 16x + 61$	19	1	1
$[29, 29, 29]$	1	$x^4 - x^3 + 4x^2 - 20x + 23$	7	1	1
$[5, 85, 1445]$	2	$x^4 - x^3 + 21x^2 - 21x + 101$	29	1	1
$[37, 37, 333]$	1	$x^4 - x^3 + 5x^2 - 7x + 49$	21	3	1
$[8, 20, 50]$	2	$x^4 + 20x^2 + 50$	25	25	1
$[13, 65, 325]$	2	$x^4 - x^3 + 15x^2 + 17x + 29$	23	1	1
$[13, 26, 52]$	2	$x^4 + 26x^2 + 52$	36	36	2
$[53, 53, 53]$	1	$x^4 - x^3 + 7x^2 + 43x + 47$	13	1	1
$[61, 61, 549]$	1	$x^4 - x^3 + 8x^2 - 42x + 117$	39	3	1

Table 1: In Section 6.1.4, we define orders R', R'', R''' of indices i_1, i_2, i_3 in their normal closures as follows. Let $R' := \mathbf{Z}[x]/(\chi)$, then its field of fractions K is isomorphic to $\mathbf{Q}[X]/(X^4 + AX^2 + B)$ and contains the real quadratic field of discriminant D. Van Wamelen proves that his n curves corresponding to K have endomorphism ring containing R'. We prove that this implies that the endomorphism ring contains $R'' = R' + \overline{R'}$ and $R''' = R'' + R_{\min, i_2}$.

6.1.5 The case of non-maximal orders

Next, we explain how our results and some additional computations prove Theorem 17. Details of the computations are available online [19] as a Sage [17] file, and we give the main steps and ideas here.

We start with the completeness. Let $C/\mathbf{Q}$ satisfy $R \cong \mathrm{End}(J(C)_{\overline{\mathbf{Q}}})$ for some order R in some quartic number field K. Then as in Section 6.1.3, we have $\Omega_{\mathbf{Z}_K} = I_{K^r}$. We took all known cyclic quartic CM-fields with this property from Bouyer-Streng [6] which gave the 20 fields listed in Tables 1 and 2.

For each of the $20 - 1 = 19$ fields $K \not\cong \mathbf{Q}(\zeta_5)$, we did the following computations. For each prime $p \mid 2 \cdot 3 \cdot N_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$, we use Sage [17] to compute the sequence of rings $A_k = R_{\min, p^k}$ for $k = 0, 1, \ldots$ until it stabilises, which we recognise as follows.

$[D, A, B]$
$[5, 15, 45]$
$[5, 30, 180]$
$[5, 35, 245]$
$[5, 105, 2205]$
$[8, 12, 18]$
$[17, 119, 3332]$
$[17, 255, 15300]$

Table 2: The known fields with $\Omega_{\mathbf{Z}_K} = I_{K^r}$ that are not in Table 1, given by triples $[D, A, B]$ with $K = \mathbf{Q}[X]/(X^4 + AX^2 + B)$ and $\Delta_{K_0} = D$.

Lemma 19. *If $A_{k+1} = A_k$, then for all $l \geq k$, we have $A_l = A_k$.*

Proof. Let $A = A_{k+2}$. It suffices to prove $A = A_{k+1}$. Note that for $n \leq k+2$, we have $A_n = A + p^n \mathbf{Z}_K$. In particular, we have $A \subset A_{k+1} = A + p^k \mathbf{Z}_K$, where the quotient for the inclusion is a power of $(\mathbf{Z}/p\mathbf{Z})$. Therefore, multiplying on the right with p reverses the inclusion, so $A \supset pA + p^{k+1}\mathbf{Z}_K$, so $A \supset A + p^{k+1}\mathbf{Z}_K$, which is what we needed to show. $\square$

For our list of 19 fields, it turns out that the chain always stabilises at $p^k = 1$, except in the case $p = 2$ for 7 of the fields, where it stabilises at 2^1 with $[\mathbf{Z}_K : R_{\min,2}] \in \{2, 4\}$. In particular, as no odd prime power greater than one appears, we have $R_{\min,f} = R_{\min,2^k}$ for $k \in \{0, 1\}$ for all our 19 fields K. For the 7 fields with $k = 1$, we compute all non-maximal superorders of $R_{\min,2}$ and their principally polarised ideal classes using Sage. We can check the existence of $(2, 2)$-isogenies in a proven manner on the level of these principally polarised ideal classes, as the polarised complex tori corresponding to $(\mathfrak{a}_1, \xi_1)$ and $(\mathfrak{a}_2, \xi_2)$ are (ℓ, ℓ)-isogenous if and only if there exists $\mu \in K^\times$ with $\mathfrak{a}_1 \subset \mu^{-1}\mathfrak{a}_2$ and $\xi_1 = \ell\mu\overline{\mu}\xi_2$. The computations above yield the following result.

Lemma 20. *Each principally polarised ideal class with multiplier ring a non-maximal order R with $\Omega_R = I_{K^r}$ in one of our 19 fields $K \not\cong \mathbf{Q}(\zeta_5)$ is $(2,2)$-isogenous to a unique principally polarised ideal class of the maximal order of K.* $\square$

This proves Theorem 17 for the fields in Table 2: as the (unique $(2, 2)$-isogenous) curves with CM by the maximal order are not stable under $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, neither are the curves with CM by the non-maximal orders.

For the $13 - 1 = 12$ fields $K \not\cong \mathbf{Q}(\zeta_5)$ in Table 1, we used the AVIsogenies [3] Magma [5] package to compute all principally polarised abelian surfaces over $\mathbf{Q}$ that are $(2, 2)$-isogenous to those of Theorem 16. This yielded no curves not covered by Theorem 16, hence proves Theorem 17 outside of the case $K = \mathbf{Q}(\zeta_5)$.

This leaves the field $K = \mathbf{Q}(\zeta_5)$, where Lemma 18 does not directly apply. There we do have $R \supset \mathbf{Z}[\zeta_5^{e_i}\mu_i : i] + f\mathbf{Z}_K$ with $0 \leq e_i < 5$, so the computations are still finite, but a little more complicated. In the end, this yields 7 orders, the indices of which all happen to be prime powers (dividing 2^4, 3^2 or 5^2 to be precise). We compute the corresponding period matrices, and they all turn out to be related to $y^2 = x^5 + 1$ by a $(3, 3)$-isogeny, a $(5, 5)$-isogeny or a chain of at most two $(2, 2)$-isogenies.

In the case of the $(5, 5)$-isogeny, we found a unique period matrix and evaluated the absolute Igusa invariants in them with interval arithmetic to an additive error less than $2^{-1}5^{-8}$. These Igusa invariants are in $\mathbf{Q}$ and we were advised by Kristin Lauter that the denominator bounds of Lauter and Viray [13] hold also for Igusa invariants of curves with CM by non-maximal orders of the form $\mathbf{Z}_{K_0}[\eta]$. The relevant order is of that form for $\eta = \zeta_5 + 3\zeta_5^3$ and we computed using their formulas that the denominator of the Igusa invariants in $\mathbf{Q}$ divides 5^8. Together, this proves correctness of the Igusa invariants that we computed, hence proves correctness of the curve.

For the $(3, 3)$-isogeny, we find using AVIsogenies that over $\overline{\mathbf{F}_{23}}$, there are 40 curves that are $(3, 3)$-isogenous to $F : y^2 = x^5 + 1$, none of which have their moduli in $\mathbf{F}_{23}$. As these are the reductions of the 40 curves over $\overline{\mathbf{Q}}$ that are $(3, 3)$-isogenous to F, we find that none of them are defined over $\mathbf{Q}$.

For the $(2,2)$-isogenies, we used the Richelot isogeny code of AVIsogenies directly over $\mathbf{Q}$. It returned the curve C from Theorem 17, which is $(2,2)$-isogenous to F, and no other curve over $\mathbf{Q}$ that is $(2,2)$-isogenous to C or F. This shows that F has CM by a non-maximal order $R \supset 1 + 2\mathbf{Z}_K$. The only such order with $\Omega_R = I_{K^r}$ for which period matrices exist is the one given in Theorem 17. A Sage computation with principally polarised ideal classes shows that every curve with CM by an order R with $\Omega_R = I_{K^r}$ and even index in $\mathbf{Z}_K$ is $(2,2)$-isogenous to C or F, and we check using AVIsogenies that no such curve exists other than C and F themselves; this proves Theorem 17 for the one remaining field $\mathbf{Q}(\zeta_5)$.

6.2 Computation of endomorphism rings

Let $\mathcal{A}$ be an ordinary principally polarised abelian variety defined over a finite field k of cardinality q. The characteristic polynomial of its Frobenius endomorphism π may be computed in polynomial time in $\log(q)$ [15]; this gives the CM-field $K = \mathbf{Q}(\pi)$ of which the endomorphism ring of $\mathcal{A}$ is an order $\mathrm{End}(\mathcal{A})$ containing $\mathbf{Z}[\pi, \overline{\pi}]$ and stable under complex conjugation [26].

The order $\mathrm{End}(\mathcal{A})$ is a finer invariant than the characteristic polynomial of π, but until recently all known methods for computing it had exponential complexity. The sub-exponential method Bisson and Sutherland obtained for elliptic curves [4, 1] proved to be very efficient and has since enabled various applications [8, 22]. Bisson then generalised it to abelian varieties [2], which also improved existing applications [12], but his generalisation relies on several unproven heuristic assumptions. Using our results, we will show that a particular one was false in general, but that it holds for almost all abelian surfaces of typical families.

6.2.1 Background

To evaluate the endomorphism ring $\mathrm{End}(\mathcal{A})$ of an abelian surface $\mathcal{A}$ such as above, Bisson [2] uses isogeny computation to determine the structure of the polarised class group $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$. The endomorphism ring $\mathrm{End}(\mathcal{A})$ is then identified amongst orders R satisfying $\mathfrak{C}(R) = \mathfrak{C}(\mathrm{End}(\mathcal{A}))$ by computing it locally at primes that divide the index between such orders.

Fix $f = [\mathbf{Z}_K : \mathbf{Z}[\pi, \overline{\pi}]]$ and restrict to ideals coprime to f so that the groups $P_R \subset I_R \subset I_{\mathbf{Z}_K}$ may be compared as R ranges through candidate endomorphism rings. Rather than computing $\mathfrak{C}(R) = I_R/P_R$ by finding many elements of P_R, this method fixes an arbitrary CM-type Φ of K and only uses elements of $\mathrm{N}_{\Phi^r}(\mathrm{N}_\Phi(p_R))$, where p_R stands for the group of principal ideals of R, since determining whether such elements are trivial in $\mathfrak{C}(\mathrm{End}(\mathcal{A}))$ can be done in sub-exponential time in $\log(q)$. Then, it incurs a polynomial cost in $v_\ell = \ell^{\mathrm{val}_\ell(f)}$ to compute the endomorphism ring locally at ℓ using [9] for each prime factor ℓ of

$$\mathrm{lcm}\left\{[R+T : R\cap T] : \begin{array}{c} \mathrm{N}_\Phi(p_R) \subset \Omega_T \\ \mathrm{N}_\Phi(p_T) \subset \Omega_R \end{array}\right\}, \tag{8}$$

where R and T range through all orders of K containing $\mathbf{Z}[\pi, \overline{\pi}]$ stable under complex conjugation, and the map N_Φ takes an ideal of p_R (respectively p_T) to I_{K^r}.

At first, Bisson expected (8) to be uniformly bounded for all quartic CM-fields K; the cost of this local computation would then be negligible. Example 15 disproves this expectation since it gives pairs of orders with $\Omega_R = \Omega_S$ and arbitrarily large indices $[R : S]$. However, we will now see that, under certain heuristics, (8) is almost always small.

6.2.2 Bounding the cost of local endomorphism ring computations

Our results would apply directly if (8) had $\mathrm{N}_\Phi(p_R)$ replaced by Ω_R and $\mathrm{N}_\Phi(p_T)$ by Ω_T; nevertheless, those two groups are closely related as the following lemma shows.

Lemma 21. *For any order R in a quartic non-biquadratic CM-field K and any CM-type Φ of K, we have*

$$(\Omega_R \cap \mathrm{N}_\Phi(I_R))^2 \subset \mathrm{N}_\Phi(p_R) \subset \Omega_R.$$

Proof. Consider the composition $I_K \xrightarrow{\mathrm{N}_\Phi} I_{K^r} \xrightarrow{\mathrm{N}_{\Phi^r}} I_{\mathbf{Z}_K}$ where I_K and I_{K^r} are the groups of invertible fractional ideals of $\mathbf{Z}_K$ and $\mathbf{Z}_{K^r}$ respectively, and recall from the proof of Lemma 6 that $\mathrm{N}_{\Phi^r}\,\mathrm{N}_\Phi(\mathfrak{a}) = \tau(\mathfrak{a}\overline{\mathfrak{a}})\mathfrak{a}^2$; if $\mathfrak{a}$ admits a generator coprime to f in R, its image through $\mathrm{N}_{\Phi^r} \circ \mathrm{N}_\Phi$ thus also does. Therefore the type norm maps p_R to a subset of Ω_R.

Let $\mathfrak{b}$ lie in the intersection of Ω_R and $\mathrm{N}_\Phi(I_R)$. This means that, for some $(\mathfrak{a}, \alpha) \in I_R$, we have $\mathfrak{b} = \mathrm{N}_\Phi(\mathfrak{a}, \alpha) := \mathrm{N}_\Phi(\mathfrak{a})$ and $\mathrm{N}_{\Phi^r}\,\mathrm{N}_\Phi(\mathfrak{a}) \in P_R$. Equation (2) then states that $(\mathfrak{a}, \alpha)^2$ belongs to P_R; by composing with N_Φ we find that $\mathfrak{b}^2$ lies in $\mathrm{N}_\Phi(P_R)$ and hence in $\mathrm{N}_\Phi(p_R)$. □

Therefore $\mathrm{N}_\Phi(p_R)$ is not much different from Ω_R; in fact, similarly to Theorem 5 we have:

Corollary 22. *Let R and T be two orders satisfying the conditions of* (8)*. The indices $[R : S]$ and $[R_0 : S_0]$ have the same valuation at all primes $\ell > 41$, and further $\ell > 7$ when $R \ncong \mathbf{Z}[\zeta_5]$.*

Proof. By the above lemma, the conditions of (8) imply $(\Omega_R \cap \mathrm{N}_\Phi(I_R))^2 \subset \Omega_T$; as in Section 3 we deduce

$$\ker(\mathfrak{C}(S) \to \mathfrak{C}(R))^4 \subset \ker(\mathfrak{C}(S) \to \mathfrak{C}(T)).$$

Indeed, let $(\mathfrak{a}, \alpha)^4$ represent a class of the first kernel. By (2) we obtain $(\mathfrak{a}, \alpha)^4 = \mathrm{N}_{\Phi^r}\,\mathrm{N}_\Phi(\mathfrak{a})^2$ in $\mathfrak{C}(S)$ and, by assumption, $\mathrm{N}_\Phi(\mathfrak{a})^2$ belongs to $(\Omega_R \cap \mathrm{N}_\Phi(I_R))^2$. In particular, we have $\mathrm{N}_{\Phi^r}\,\mathrm{N}_\Phi(\mathfrak{a})^2 \in \mathrm{N}_{\Phi^r}(\Omega_T)$ so the class of $(\mathfrak{a}, \alpha)^4$ in $\mathfrak{C}(S)$ becomes trivial in $\mathfrak{C}(T)$.

Now, using the same proof as for Proposition 9 (albeit replacing two's by four's in the exponents) we deduce that, for any two orders R and T satisfying the conditions of (8), the kernel (5) is of exponent at most four. The proof of Proposition 12 then carries through for all primes $p > 7$ assuming $R \ncong \mathbf{Z}[\zeta_5]$, and $p > 41$ in general. □

As a consequence, we now establish that the sum $\sum_\ell v_\ell$ where ℓ ranges through prime factors of (8) is almost always small, assuming that the v_i satisfy typical divisibility conditions.

Proposition 23. *Let $(\mathcal{A}_i/\mathbf{F}_{q_i})_{i\in\mathbf{N}}$ be a sequence of ordinary abelian varieties defined over fields of monotonously increasing cardinality $q_i \to \infty$. Denote by $v_i = [R_{\mathbf{Q}(\pi_i)} : \mathbf{Z}[\pi_i, \overline{\pi}_i]]$ their conductor gaps, and by $n_i = \mathrm{N}_{K_0/\mathbf{Q}}(\Delta_{K/K_0})$ the norm of the relative discriminant of their CM-fields $K = \mathbf{Q}(\pi_i)$. Assume that there exists a constant C such that, for all positive integers u and m:*

- *the proportion of indices $i < m$ for which $u|v_i$ is at most C/u;*
- *the proportion of indices $i < m$ for which $u|v_i$ and $u|n_i$ is at most C/u^2.*

Then, for any $\tau > 0$, all prime factors ℓ of (8) are such that $v_{i,\ell} = \ell^{\mathrm{val}_\ell v_i}$ is smaller than $L(q_i)^\tau$, except for a zero-density subset of indices $i \in \mathbf{N}$, where $L(x) = \exp\sqrt{\log x \cdot \log\log x}$.

Proof. Fix an index i and let ℓ be a prime factor of v_i. If ℓ^2 does not divide v_i, then, locally at ℓ, out of two distinct orders containing $\mathbf{Z}[\pi_i, \overline{\pi}_i]$, one must be maximal; by the proof of Theorem 4, the quantity (8) thus has no ℓ-part unless $\ell \leq 41$ or $\ell|n_i$. As a consequence, for any fixed integer $M \geq 41$, all pairs of indices $i < m$ and primes ℓ dividing (8) such that $v_{i,\ell} > L(q_i)^\tau$ satisfy at least one of the following conditions:

- the index i satisfies $L(q_i)^\tau \leq M$;
- $\mathrm{val}_\ell v_i = 1$ and $\ell > M$ divides $\gcd(v_i, n_i)$;
- $\mathrm{val}_\ell v_i > 1$ and $v_{i,\ell} > M$ divides v_i.

Since $v_i < 64q_i^2$ [2, Lemma 3.2] we have $v_{i,\ell} < 64q_m^2$ for all primes ℓ and indices $i < m$, thanks to the monotony of q_i. Hence the proportion of indices $i < m$ for which (8) admits a prime factor ℓ such that $v_{i,\ell} > L(q_i)^\tau$ is bounded by

$$\frac{\#\{i : L(q_i)^\tau \leq M\}}{m} + \sum_{M<\ell<64q_m^2} \frac{C}{\ell^2} + \sum_{2\leq\alpha\leq 6+2\log_2 q_m} \left(\sum_{M^{1/\alpha}<\ell\leq M^{1/(\alpha-1)}} \frac{C}{\ell^\alpha} \right)$$

where each term corresponds to one of the above conditions, and the variable α represents $\mathrm{val}_\ell v_i$. Note that the bound $\ell \leq M^{1/(\alpha-1)}$ in the last sum is here to prevent counting the same prime ℓ for multiple values of α.

By bounding each sum, we further deduce that the density of such indices is less than

$$\lim_{m\to\infty} \left(\frac{\#\{i : L(q_i)^\tau < M\}}{m} + \frac{C}{M} + \sum_{\alpha>1} \frac{C}{\alpha-1} \left(\frac{1}{M^{\frac{\alpha-1}{\alpha}}} - \frac{1}{M} \right) \right)$$

For M large enough, the second and third terms can be made arbitrarily small; then, the first term vanishes as m goes to infinity. The above density is thus zero. ☐

6.2.3 Conclusion

The conditions of Proposition 23 on the integers v_i are typical divisibility properties that are satisfied by integers drawn uniformly at random (say, from $\{1, \ldots, 64q_i^2\}$) and independently from the n_i. Furthermore, they are experimentally observed to hold for the two main families which are of interest to [2], namely random isomorphism classes of abelian varieties and random isomorphism classes of abelian varieties with complex multiplication by a prescribed field, defined over finite fields of increasing cardinality.

The method of [2] rests on several unproven heuristics, including the generalised Riemann hypothesis and that the quantity (8) remains small. Although the latter is false in general, Proposition 23 shows that it holds for almost all abelian varieties of families such as above. Under heuristic assumptions, it therefore establishes that the method of [2] terminates in average sub-exponential time.

Acknowledgements

The authors would like to thank David Gruenewald, Kristin Lauter and Bianca Viray for helpful discussions. The first-named author further wishes to thank the Mathematics Research Centre of the University of Warwick for their hospitality while part of this work was done. The second-named author acknowledges the support of EPSRC grant EP/G004870/1 and NWO through DIAMANT and Vernieuwingsimpuls.

References

[1] Gaetan Bisson. Computing endomorphism rings of elliptic curves under the GRH. *Journal of Mathematical Cryptology.*, 5(2):101–113, 2011.

[2] Gaetan Bisson. Computing endomorphism rings of abelian varieties of dimension two. *Mathematics of Computation*, 84(294):1977–1989, 2015.

[3] Gaetan Bisson, Romain Cosset, and Damien Robert. *AVIsogenies, a library for computing isogenies between abelian varieties*, 2010. `http://avisogenies.gforge.inria.fr/`.

[4] Gaetan Bisson and Andrew V. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 131(5):815–831, 2011.

[5] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system: the user language. *Journal of Symbolic Computation*, 24(3–4):235–265, 1997.

[6] Florian Bouyer and Marco Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015. `http://arxiv.org/abs/1307.0486`.

[7] Reinier Bröker, Kristin Lauter, and Marco Streng. Abelian surfaces admitting an (l, l)-endomorphism. *Journal of Algebra*, 394:374–396, 2013. `http://arxiv.org/abs/1106.1884`.

[8] Reinier Bröker, Kristin Lauter, and Andrew V. Sutherland. Modular polynomials via isogeny volcanoes. *Mathematics of Computation*, 81(278):1201–1231, 2012.

[9] Kirsten Eisenträger and Kristin E. Lauter. A CRT algorithm for constructing genus 2 curves over finite fields. In François Rodier and Serge Vladut, editors, *Arithmetic, Geometry and Coding Theory — AGCT 2010*, volume 21 of *Séminaires et Congrès*, pages 161–176. Société Mathématique de France, 2009.

[10] Pınar Kılıçer and Marco Streng. The CM class number one problem for curves of genus 2. `http://arxiv.org/abs/1511.04869`, 2015.

[11] Serge Lang. *Complex Multiplication*, volume 255 of *Grundlehren der mathematischen Wissenschaften*. Springer, 1983.

[12] Kristin Lauter and Damien Robert. Improved CRT algorithm for class polynomials in genus 2. In Everett Howe and Kiran Kedlaya, editors, *Algorithmic Number Theory — ANTS-X*. Mathematical Science Publishers, 2012.

[13] Kristin Lauter and Bianca Viray. An arithmetic intersection formula for denominators of Igusa class polynomials. *Amer. J. Math.*, 137(2):497–533, 2015. `http://arxiv.org/abs/1210.7841`.

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

[15] Jonathan Pila. Frobenius maps of abelian varieties and finding roots of unity in finite fields. *Mathematics of Computation*, 55(192):745–763, 1990.

[16] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*, volume 6 of *Publications of the Mathematical Society of Japan*. The Mathematical Society of Japan, 1961.

[17] William A. Stein et al. *Sage Mathematics Software (Version 5.2)*. The Sage Development Team, 2012. `http://www.sagemath.org/`.

[18] Peter Stevenhagen. The arithmetic of number rings. In Joseph P. Buhler and Peter Stevenhagen, editors, *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography*, volume 44 of *Mathematical Sciences Research Institute Publications*, pages 209–266. Cambridge University Press, 2008.

[19] Marco Streng. Sage package for using Shimura's reciprocity law for Siegel modular funcions. `http://www.math.leidenuniv.nl/~streng/recip`.

[20] Marco Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010. `http://www.math.leidenuniv.nl/~streng/thesis.pdf`.

[21] Marco Streng. An explicit reciprocity law for Siegel modular functions. `http://arxiv.org/abs/1201.0020`, 2011.

[22] Andrew V. Sutherland. Computing Hilbert class polynomials with the Chinese remainder theorem. *Mathematics of Computation*, 80(273):501–538, 2011.

[23] Paul van Wamelen. Examples of genus two CM curves defined over the rationals. *Mathematics of Computation*, 68(225):307–320, 1999.

[24] Paul van Wamelen. Genus 2 CM curves defined over the rationals. `https://www.math.lsu.edu/~wamelen/CMcurves.txt`, 1999.

[25] Paul van Wamelen. Proving that a genus 2 curve has complex multiplication. *Mathematics of Computation*, 68(228):1663–1677, 1999.

[26] William C. Waterhouse. Abelian varieties over finite fields. *Annales Scientifiques de l'École Normale Supérieure*, 2(4):521–560, 1969.