HAL open science

Isogenous hyperelliptic and non-hyperelliptic Jacobians with maximal complex multiplication

Bogdan Dina, Sorina Ionica, Jeroen Sijsling

To cite this version:

Bogdan Dina, Sorina Ionica, Jeroen Sijsling. Isogenous hyperelliptic and non-hyperelliptic Jacobians with maximal complex multiplication. Mathematics of Computation, 2023, 92, pp.349-383. hal-03251240

HAL Id: hal-03251240

https://hal.science/hal-03251240v1

Submitted on 6 Jun 2021

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

ISOGENOUS HYPERELLIPTIC AND NON-HYPERELLIPTIC JACOBIANS WITH MAXIMAL COMPLEX MULTIPLICATION

BOGDAN DINA, SORINA IONICA, AND JEROEN SIJSLING

Abstract. We analyze complex multiplication for Jacobians of curves of genus 3, as well as the resulting Shimura class groups and their subgroups corresponding to Galois conjugation over the reflex field. We combine our results with numerical methods to find CM fields K for which there exist both hyperelliptic and non-hyperelliptic curves whose Jacobian has complex multiplication by $\mathbb{Z}_K$. More precisely, we find all sextic CM fields K in the LMFDB for which (heuristically) Jacobians of both types with CM by $\mathbb{Z}_K$ exist. There turn out to be 14 such fields among the 547,156 sextic CM fields that the LMFDB contains. We determine invariants of the corresponding curves, and in the simplest case we also give an explicit defining equation.

Introduction

Because of their singular arithmetic properties and their cryptographic applications, curves of low genus whose Jacobian admits complex multiplication (CM) have historically been at the forefront of research on algebraic curves. By Shimura and Taniyama's theory of complex multiplication, it is well known that the invariants of these curves generate certain abelian extensions of CM fields. There is a wide literature on computing these invariants as well as models for genus 1 and genus 2 hyperelliptic curves with CM (see for instance [2, 17, 18, 46]). In recent years, the frontier has shifted to genus 3, where both hyperelliptic and non-hyperelliptic curves can be considered. A non-trivial hyperelliptic CM curve over $\mathbb{Q}$ was first calculated in [51], whose methods were elaborated in more detail in [50] and [1]. Starting from the observation that the Galois conjugates of a hyperelliptic Jacobian are once more hyperelliptic Jacobians, [13] computes the Rosenhain and Shioda invariants of hyperelliptic curves in the Galois orbit in order to exhibit equations over the corresponding class fields.

Non-hyperelliptic CM curves were first studied in the form of Picard curves, whose first construction goes back to [25], the methods of which were recently generalized in [32]. The reduction properties of CM Picard curves have also been studied in detail [29]. The consideration of general non-hyperelliptic CM curves was taken up in the context of work of Kılıçer, who in her thesis [26] determined the full list of genus-3 CM curves with field of moduli $\mathbb{Q}$. Explicit defining equations of these curves were found in [21] in the hyperelliptic case and [27] in the non-hyperelliptic case, which included 19 non-hyperelliptic, non-Picard CM curves. Reduction properties in the general case were studied in the works [6, 28].

Date: May 18, 2021.

2020 *Mathematics Subject Classification.* 14H40, 14H25; 14H45, 14H50, 14K20, 14K22.

Key words and phrases. Complex multiplication, hyperelliptic curve, plane quartic.

The first and second author acknowledge financial support from the Thomas Jefferson Fund program, which is supported by the Embassy of France in the United States and the FACE Foundation. The third author was supported by the Juniorprofessuren-Programm "Endomorphismen algebraischer Kurven" of the Science Ministry of Baden-Württemberg as well as by a Sachbeihilfe "Abstieg algebraischer Kurven" of the Deutsche Forschungsgemeinschaft. We thank John Boxall and Anna Somoza for bringing the André–Oort conjecture to our attention, as well as Marco Streng and Andrew Sutherland for their helpful comments on a previous version of this article, and last but most definitely not least Tim Evink for his help with proving Proposition 2.2.7.

The explicit defining equations in the works [21, 27, 50] mentioned above are heuristic, in the sense that while the results obtained are exceedingly likely to be correct, their rigorous verification, available in theory by using the methods in [11], is still open because of the long running time of the algorithms in *loc. cit.* The current work, which will obtain defining equations and invariants of CM curves over $\overline{\mathbb{Q}}$, will also take this heuristic approach throughout. Still, we will give multiple reasons to believe in the correctness of its results.

For the CM curves defined over $\mathbb{Q}$ determined in [26], their Jacobian is up to $\overline{\mathbb{Q}}$-isomorphism the unique principally polarized abelian threefold over $\mathbb{Q}$ that admits CM by its endomorphism ring, which is the maximal order of the corresponding CM field. This is often caused by the fact that there is already a single $\overline{\mathbb{Q}}$-isomorphism class of such principally polarized abelian threefolds, see [27, Table 1]. In the cases where this uniqueness over $\overline{\mathbb{Q}}$ fails to hold, it is still true that all curves with CM by the given maximal order are hyperelliptic. The goal of this paper is to explore the opposite of this phenomenon: We ask ourselves whether there are sextic CM fields K for which there exist both a hyperelliptic *and* a non-hyperelliptic curve whose endomorphism ring is isomorphic to the maximal order $\mathbb{Z}_K$ of K.

To achieve our goal, we developed and implemented computational methods that, given a CM field K and a primitive CM type Φ, determine a small set of period matrix representatives of the corresponding isomorphism classes of principally polarized abelian threefolds, up to Galois conjugation over the reflex field K^r of K with respect to Φ. A calculation with theta-null values (using [30]) then allows us to see which of these representatives correspond to hyperelliptic or non-hyperelliptic curves. Our methods are efficient enough to enable us to check all of the 547,156 sextic CM fields included in the LMFDB [47].

Regarding our first goal, our main result is the following.

Main Result 1. *Heuristically, there are 14 sextic CM fields K in the LMFDB for which there exist both a hyperelliptic and a non-hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order $\mathbb{Z}_K$ of K. For all of these fields K we have that* $\mathrm{Gal}(K\,|\,\mathbb{Q}) \simeq C_2^3 \rtimes S_3$.

Though we cannot seriously formulate a conjecture in this direction for lack of mathematical rigor, circumstantial evidence does to some extent suggest that the sextic CM fields obtained in Main Result 1 are in fact all of their kind. Indeed, the largest absolute value of the discriminant of the fields in Main Result 1 equals $5.40 \cdot 10^{10}$, whereas the largest such value for the 494,386 sextic CM fields in the LMFDB with $\mathrm{Gal}(K\,|\,\mathbb{Q}) \simeq C_2^3 \rtimes S_3$ equals $1.78 \cdot 10^{17}$. Sorted by discriminant, the index of the field with largest discriminant in Main Result 1 equals $35,447$.

Our result on the second goal concerning hyperelliptic curves is as follows. For more detailed information, see Section 3.2, and in particular Table 1.

Main Result 2. *Heuristically, including the fields mentioned in Main Result 1, there are 3,422 CM fields K in the LMFDB for which there exists a hyperelliptic curve whose Jacobian has primitive complex multiplication by the maximal order $\mathbb{Z}_K$ of K. Of these fields, 348 (resp. 3,057, resp. 17) have Galois group isomorphic to C_6 (resp. D_6, resp. $C_2^3 \rtimes S_3$). We have $\mathbb{Q}(i) \subset K$ for all but 19 of these fields K. Among the exceptional cases, 2 (resp. 17) have Galois group isomorphic to C_6 (resp. $C_2^3 \rtimes S_3$).*

Note that the classification of possible automorphism groups of hyperelliptic and non-hyperelliptic curves of genus 3 (for example in [38]) shows that if the sextic CM field K contains $\mathbb{Q}(i)$, then any curve whose Jacobian has primitive CM by K is automatically hyperelliptic. This was already used in [50]. Moreover, families of such fields are quickly found, for example by considering those defined by polynomials of the form $x^6 + d^2$. In this sense the exceptional cases with $\mathbb{Q}(i) \not\subset K$ are also the more interesting ones. For the 2 cyclic cases among them, equations for corresponding hyperelliptic curves were already determined in [1]. By contrast, our 3 new exceptional cases with Galois group $C_2^3 \rtimes S_3$ are completely new, as are the fields in Main Result 1.

Besides determining the fields involved, we can also find corresponding invariants. Our final main result even gives a defining equation for the field in the Main Result 1 with the smallest discriminant.

Main Result 3. *Let K be the CM field of discriminant $-1 \cdot 2^8 \cdot 359^2$ defined by the polynomial $t^6+10t^4+21t^2+4$, and let r be a zero of the polynomial t^4-5t^2-2t+1. Consider the hyperelliptic curve*

$$\begin{aligned} X: \quad y^2 = {} & x^8+(-28r^3-4r^2+132r+84)x^7+(-600r^3-160r^2+2920r+2044)x^6 \\ & +(-3532r^3-940r^2+17224r+11944)x^5+(9040r^3+2890r^2-44860r-31460)x^4 \\ & +(167536r^3+49480r^2-824532r-576212)x^3+(-226976r^3-64932r^2+1113648r+776872)x^2 \\ & +(-244204r^3-69572r^2+1197716r+835300)x+(319956r^3+94725r^2-1575062r-1100801) \end{aligned} \tag{0.1}$$

and the smooth plane quartic curve

$$\begin{aligned} Y: \quad & (14106r^3-150652r^2+185086r+292255)x^4+(-171112r^3+44200r^2+916008r+93360)x^3y \\ & +(-120788r^3+49032r^2+382244r+300708)x^3z+(467744r^3-209864r^2-2160704r+183416)x^2y^2 \\ & +(-72248r^3+64768r^2+347488r-362984)x^2yz+(5720r^3-12378r^2-15628r+50692)x^2z^2 \\ & +(-512608r^3+349824r^2+2423616r-580448)xy^3+(202192r^3-151024r^2-1180320r+403568)xy^2z \\ & +(6512r^3-11272r^2+178120r-71336)xyz^2+(-11832r^3+12268r^2-844r+1376)xz^3 \\ & +(263424r^3-176880r^2-1159232r+335040)y^4+(-201216r^3+100448r^2+856096r-249632)y^3z \\ & +(62112r^3+1984r^2-226512r+71624)y^2z^2+(-12520r^3-13112r^2+27736r-5360)yz^3 \\ & +(1526r^3+2411r^2-658r+197)z^4 = 0. \end{aligned} \tag{0.2}$$

Heuristically, there exists an isogeny of degree 2 between the Jacobians of X and Y, and both have CM by the maximal order $\mathbb{Z}_K$.

The paper is structured as follows. In Sections 1 and 2 we recapitulate the theory on CM fields and their Shimura class groups that we need. In particular, we prove general results on the transitivity of the Galois action on CM types and on the image of the reflex type norm that allow us to determine a small set of representatives of principally polarized abelian threefolds with CM by a given ring of integers $\mathbb{Z}_K$ up to Galois conjugacy over the reflex field. In Section 3 we use these results and further speedups to check the 547,156 sextic CM fields in the LMFDB for the existence of a corresponding hyperelliptic curve, which leads to Main Results 1 and 2.

Section 4 discusses techniques for determine explicit defining equations, and includes the proof of the third Main Result. We conclude the paper by some discussions around the relevance of the André–Oort conjecture to our considerations in Section 5.

A full implementation of our techniques in Magma [5] is an essential part of our results. It is available online at [14].

Notations and conventions. In this article a curve over a field k is a separated and geometrically integral scheme of dimension 1 over k. Given an affine equation for a curve, we will identify it with the smooth projective curve that has the same function field. The Jacobian of a curve X is denoted by $\mathrm{Jac}(X)$. We denote the cyclic group with n elements by C_n and the dihedral group with $2n$ elements by D_n.

When the context allows it, we often use the abbreviated notation A for a principally polarized abelian variety (A, E), as well as using the abbrevation ppav to stand for "principally polarized abelian variety". Finally, as in the introduction we will call a curve X of genus g over an algebraically closed field a CM curve if the endomorphism ring of its Jacobian $\mathrm{Jac}(X)$ is an order in a CM field of degree $2g$, so that by this definition, the CM type of a CM curve is primitive.

Contents

Introduction 1
1. Theoretical background 4
1.1. Structure of sextic CM fields 4
1.2. CM types 5
1.3. Geometric relevance 9
2. The Shimura class group and the Galois action 10
2.1. Background 10
2.2. Torsors and moduli spaces 11
2.3. Representatives up to Galois conjugacy 13
3. Running through the LMFDB 16
3.1. Algorithms 16
3.2. Fields 19
3.3. Invariants 20
3.4. The mixed cases 21
4. Explicit defining equations 22
4.1. Hyperelliptic simplification 22
4.2. A plane quartic equation 24
5. Around the André–Oort conjecture 25
5.1. General considerations 25
5.2. Cryptographic implications 27
References 27

1. Theoretical background

For more on the general theory of complex multiplication, we refer to [46, §4]. We supplement this background with some additional considerations, most of them specific to genus 3, that we will need for later results.

1.1. **Structure of sextic CM fields.** A number field K is called a CM field if K is a totally imaginary quadratic extension of a totally real number field. Given K, the latter field is determined uniquely; we denote it by K_0. As [31, p6] shows, for any CM field K there exists a unique element $\varrho \in \mathrm{Aut}(K)$ such that

$$\iota(\varrho(x)) = \overline{\iota(x)} \tag{1.1.1}$$

for all embeddings $\iota : K \hookrightarrow \mathbb{C}$. We call ϱ the complex conjugation on K. Moreover, the Galois closure of a CM field is once again a CM field. We will consider sextic CM fields in this article. The corresponding Galois groups can be described as follows:

Theorem 1.1.2. *Let K be sextic CM field, with Galois closure L. Then $G = \mathrm{Gal}(L \mid \mathbb{Q})$ is isomorphic to one of the following groups:*

(i) C_6;
(ii) D_6;
(iii) $C_2^3 \rtimes C_3$;
(iv) $C_2^3 \rtimes S_3$.

In the latter two cases, the action of C_3 and S_3 on C_2^3 is given by permutation of the indices. Each possible group G above admits a unique embedding $\iota : G \to S_6$ up to conjugation in S_6, under which they become the groups 6T1, 6T3, 6T6, 6T11 from [3].

Proof. The first part follows from [15, Sec. 5.1.1]; see also [6, Proposition 2.1]. The second is a one-off calculation with the conjugacy classes of subgroups of S_6, for example by using GAP [3]. □

The notation 6TX for the groups in Theorem 1.1.2 can be used when searching for corresponding fields in the LMFDB [47].

Remark 1.1.3. The second part of Theorem 1.1.2 in combination with Galois theory shows that we may assume that under the chosen embedding $\iota : G \to S_6$ the subgroup $H = \mathrm{Gal}(L\,|\,K)$ is the stabilizer of 1.

Example 1.1.4. The sextic CM field with smallest absolute discriminant in the LMFDB whose Galois group is isomorphic to $\mathbb{C}_6$ is $\mathbb{Q}(\zeta_7)$. The field of smallest absolute discriminant with Galois group D_6 is defined by $x^6 - 3x^5 + 10x^4 - 15x^3 + 19x^2 - 12x + 3$, that for $C_2^3 \rtimes C_3$ by $x^6 - 2x^5 + 5x^4 - 7x^3 + 10x^2 - 8x + 8$, and that for $C_2^3 \rtimes S_3$ by $x^6 - 3x^5 + 9x^4 - 13x^3 + 14x^2 - 8x + 2$.

1.2. **CM types.** As above, let K be a CM field with complex conjugation ϱ and Galois closure L. We further fix an embedding $\iota_L : L \to \mathbb{C}$.

Definition 1.2.1. A CM type of K (with values in L) is a subset $\Phi \subset \mathrm{Hom}(K, L)$ such that

$$\mathrm{Hom}(K, L) = \Phi \amalg \Phi\varrho. \tag{1.2.2}$$

As in the classical case, we call a CM type of K primitive if it is not induced by a CM type of a strict CM subfield. Similarly, we call two CM types Φ, Φ' equivalent if there exists an automorphism $\alpha \in \mathrm{Aut}(K)$ such that $\Phi' = \Phi\alpha$. As for example in [31], we also call the pair (K, Φ) a CM type.

Remark 1.2.3. Our choice of an embedding $\iota_L : L \to \mathbb{C}$ yields a map

$$\Phi \mapsto \{\iota_L \circ \tau : \tau \in \Phi\} \tag{1.2.4}$$

which furnishes a bijection between the CM types in Definition 1.2.1 and the CM types of K in the classical sense of a set of embeddings into $\mathbb{C}$. For our purposes, it is more useful to consider the former type.

Remark 1.2.5. Let $H = \mathrm{Gal}(L\,|\,K)$. Then the natural map

$$\begin{aligned} \mathrm{Gal}(L\,|\,\mathbb{Q}) &\to \mathrm{Hom}(K, L) \\ \sigma &\mapsto \sigma|_K \end{aligned} \tag{1.2.6}$$

induces a bijection $G/H \to \mathrm{Hom}(K, L)$. We can and therefore will consider the individual embeddings $\tau : K \to L$ in a CM type as cosets σH in G/H. Under this interpretation, a CM type is nothing but a section of the natural projection map

$$G/H \to \langle\varrho\rangle\backslash G/H. \tag{1.2.7}$$

Alternatively, it is a subset $\Phi \subset G/H$ on which the restriction of this projection map induces an bijection.

The normalizer $N = N_G(H)$ of H in G acts on the set of sections $s : \langle\varrho\rangle\backslash G/H \to G/H$ via right composition, and using the natural isomorphism $N/H \cong \mathrm{Aut}(K)$ induced by restriction, we see that the corresponding quotient is in bijection with the set of CM types up to equivalence. We determine this normalizer in the following proposition.

Proposition 1.2.8. *Let $G = \mathrm{Gal}(L \mid \mathbb{Q})$ be one of the Galois groups in Theorem 1.1.2 and let $H = \mathrm{Gal}(L\,|\,K)$. Let $N = N_G(H)$ be the normalizer of H in G. Then we have $N = \langle H, \varrho\rangle$ except if $G = C_6$, in which case $N = G$.*

Proof. We have realized our Galois groups as the explicit subgroups 6T1, 6T3, 6T6, 6T11, and Remark 1.1.3 shows that we may take H to be the stabilizer of 1. We can choose our embeddings $G \to S_6$ in such a way that we have the following, as used throughout the paper:

(i) $G = C_6 = \langle\sigma\rangle$: $H = 1$, $\varrho = \sigma^3$.
(ii) $G = D_6 = \langle\sigma, \tau\rangle$: $H = \langle\tau\rangle$, $\varrho = \sigma^3$.
(iii) $G = C_2^3 \rtimes C_3$: $H = \langle((1,0,0),e),((0,1,0),e)\rangle$, $\varrho = ((1,1,1),e)$, where $e \in C_3$ is the identity.
(iv) $G = C_2^3 \rtimes S_3$: $H = \langle((1,0,0),e),((0,1,0),e),((0,0,0),(1,2))\rangle$, $\varrho = ((1,1,1),e)$, where $e \in S_3$ is the identity.

The result is now an unenlightening and unproblematic calculation. □

Definition 1.2.9. There is a natural left action of the Galois group G on CM types Φ of K. As subsets $\Phi \subset G/H$, we have

$$\sigma\Phi = \{\sigma\varphi : \varphi \in \Phi\} \tag{1.2.10}$$

for $\sigma \in G$. On CM types considered as sections s of the projection map $G/H \to \langle\varrho\rangle\backslash G/H$, the action is defined by

$$(\sigma s)(\langle\varrho\rangle cH) = \sigma \cdot s(\langle\varrho\rangle\sigma^{-1}cH) \tag{1.2.11}$$

for $\sigma, c \in G$. Note that these actions are well-defined because ϱ is central in G. We call the resulting equivalence on the set of CM types of K the Galois equivalence.

Proposition 1.2.12. *Let K be a sextic CM field with Galois group C_6. Then K admits 2 CM types up to equivalence, 1 of them primitive and 1 imprimitive. The same is true when replacing equivalence with Galois equivalence.*

Proof. We can identify a CM type on K with a subset $S \subset C_6 = \mathbb{Z}/6\mathbb{Z}$ of cardinality 3 such that S and $3 + S$ cover $\mathbb{Z}/6\mathbb{Z}$. By Proposition 1.2.8, two such CM types S, S' are equivalent if they are related by a translation, so that $S' = i + S$ for some $i \in \mathbb{Z}/6\mathbb{Z}$, and the same is true for Galois equivalence. As is readily verified, representatives up to equivalence are given by $\{0, 1, 2\}$ and $\{0, 2, 4\}$. The latter CM type is imprimitive, since it is induced from the quotient $\mathbb{Z}/2\mathbb{Z}$ of $\mathbb{Z}/6\mathbb{Z}$ that corresponds to the unique CM quadratic subfield of K. The former type is primitive. See [6, §3.1] for a different point of view. □

Proposition 1.2.13. *Let K be a sextic CM field with Galois group D_6. Then K admits 4 CM types up to equivalence, 3 of them primitive and 1 imprimitive. Up to Galois equivalence, K admits 2 CM types, 1 of them primitive and 1 imprimitive.*

Proof. In this case we can choose a standard representation $D_6 = \langle\sigma, \tau\rangle$ and embed it into S_6 by identifying σ with $(1\,2\,3\,4\,5\,6)$ and τ with $(2\,6)(3\,5)$. As we have seen in Proposition 1.2.8, the complex conjugation ϱ is given by the central element σ^3 and $\mathrm{Gal}(L\,|\,K) = \langle\tau\rangle$. The embeddings of K into L can therefore be identified with powers σ^i, or for that matter with elements i of $\mathbb{Z}/6\mathbb{Z}$. We are in a similar situation as Proposition 1.2.12, except that the notion of equivalence is stricter, as Proposition 1.2.8 shows that this time the only other CM type equivalent to a given type $\{a, b, c\}$ is $\{a + 3, b + 3, c + 3\}$, which corresponds to applying complex conjugation.

Up to equivalence, we obtain the 4 CM types $\{0, 1, 2\}$, $\{0, 1, 5\}$, $\{0, 2, 4\}$, $\{0, 4, 5\}$. Of these types, $\{0, 2, 4\}$ is induced by the unique quadratic CM subfield of K and is therefore imprimitive, while the other types are primitive.

Applying Galois equivalence allows us to multiply with σ, so as in Proposition 1.2.12 we can apply arbitrary shifts to our subsets of $\mathbb{Z}/6\mathbb{Z}$ to our CM types. Once more this reduces us to the two types $\{0, 1, 2\}$ and $\{0, 2, 4\}$, the former primitive and the latter imprimitive. See [6, §3.2] for a different point of view. □

Proposition 1.2.14. *Let K be a sextic CM field with Galois group $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$. Then K admits 4 CM types up to equivalence, which are all primitive. Up to Galois equivalence, K admits 1 CM type.*

Proof. The first statement follows as in Proposition 1.2.13, since in light of Proposition 1.2.8 applying equivalence once again comes down to identifying complex conjugate CM types, leaving 4 equivalence classes of the original 8 types. All of these types are primitive because the group H corresponding to K in the notation of Proposition 1.2.8 is not contained in any subgroup of G of index 2, or in other words because K has no proper quadratic subfields, let alone proper CM subfields.

As for working up to Galois equivalence, in the case $G = C_2^3 \rtimes C_3$ we have that

$$\begin{aligned} H &= \{((*,*,0),e)\}\,, \\ \sigma H &= \{((0,*,*),(1\,2\,3))\}\,, \\ \sigma^2 H &= \{((*,0,*),(1\,3\,2))\}\,, \\ \varrho H &= \{((*,*,1),e)\}\,, \\ \sigma\varrho H &= \{((1,*,*),(1\,2\,3))\}\,, \\ \sigma^2\varrho H &= \{((*,1,*),(1\,3\,2))\}\,, \end{aligned} \tag{1.2.15}$$

where $*$ denotes an element of C_2 that can be chosen freely, and where $\sigma = ((0,0,0),(1\,2\,3))$. We see that $\Phi_0 = \{H, \sigma H, \sigma^2 H\}$ is a CM type. Moreover, the definition of the Galois action along with that of the group structure on G implies that for $n_1 = ((1,0,0),e)$ we have

$$\begin{aligned} n_1 H &= \{((*,*,0),e)\} = H \\ n_1\sigma H &= \{((1,*,*),(1\,2\,3))\} = \sigma\varrho H \\ n_1\sigma^2 H &= \{((*,*,0),(1\,3\,2))\} = \sigma^2 H. \end{aligned} \tag{1.2.16}$$

Similarly, $n_2 = ((0,1,0),e)$ sends Φ_0 to $\{H, \sigma H, \sigma^2\varrho H\}$ and $n_0 = ((0,0,1),e)$ sends Φ_0 to $\{\varrho H, \sigma H, \sigma^2 H\}$. Combining the action of these three elements is enough to obtain transitivity of the Galois action on the full set of CM types $\{\varrho^*, \sigma\varrho^*, \sigma^2\varrho^*\}$. The considerations for $G = C_2^3 \rtimes S_3$ are completely identical, with the small difference that

$$\begin{aligned} H &= \{((*,*,0),e \text{ or } (1\,2))\}\,, \\ \sigma H &= \{((0,*,*),(1\,2\,3) \text{ or } (1\,3))\}\,, \\ \sigma^2 H &= \{((*,0,*),(1\,3\,2) \text{ or } (2\,3))\}\,, \\ \varrho H &= \{((*,*,1),e \text{ or } (1\,2))\}\,, \\ \sigma\varrho H &= \{((1,*,*),(1\,2\,3) \text{ or } (1\,3))\}\,, \\ \sigma^2\varrho H &= \{((*,1,*),(1\,3\,2) \text{ or } (2\,3))\}\,. \end{aligned} \tag{1.2.17}$$

□

Given a CM type (K,Φ), there is a reflex CM type (K^r,Φ^r) to (K,Φ), which is constructed as follows. We can lift Φ to a CM type Φ_L on L, where elements in Φ_L are identified by elements in $\mathrm{Gal}(L|\mathbb{Q})$. Inverting elements in Φ_L gives rise to a CM type on L denoted by

$$\Phi_L^{-1} = \{\varphi^{-1} : \varphi \in \Phi_L\}. \tag{1.2.18}$$

The reflex CM type (K^r,Φ^r) is defined in [31, Lemma 2.2]: The CM field K^r is the fixed field of the group

$$H^r = \{\sigma \in \mathrm{Gal}(L\,|\,\mathbb{Q}) : \sigma\Phi_L = \Phi_L\}, \tag{1.2.19}$$

and Φ^r is the unique CM type on K^r that induces Φ_L^{-1}.

In the case where the sextic CM field K is Galois with abelian Galois group C_6, we directly obtain the following result as the left and right stabilizers of Φ coincide:

Proposition 1.2.20. *Let (K, Φ) be a sextic CM type where K has Galois group C_6. If Φ is primitive, then $(K^r, \Phi^r) = (K, \Phi)$. If Φ is imprimitive, then (K^r, Φ^r) is the restriction of (K, Φ) to the quadratic CM subfield of K.*

To deal with the case $G = D_6$, we first prove the following general statement.

Proposition 1.2.21. *Let Φ, Ψ be two CM types of a given field K, and suppose that $\Psi = \sigma\Phi$ for $\sigma \in G = \mathrm{Gal}(L \,|\, \mathbb{Q})$. Let (K^r, Φ^r) be the reflex CM type of (K, Φ). Then the reflex CM type of (K, Ψ) is given by*

$$(\sigma(K^r), \Phi^r\sigma^{-1}), \tag{1.2.22}$$

where

$$\Phi^r\sigma^{-1} = \left\{(\varphi\sigma^{-1})|_{\sigma(K^r)} : \varphi \in \Phi^r\right\}. \tag{1.2.23}$$

Proof. For the extensions of Φ and Ψ to L we have $\Psi_L = \sigma\Phi_L$. For the corresponding left stabilizers H_Φ and H_Ψ we therefore have $H_\Psi = \sigma H_\Phi \sigma^{-1}$, which already shows that the reflex field of Ψ equals $\sigma(K)$. By construction, we have

$$\Phi_L^{-1} = \coprod_{\varphi \in \Phi^r} \varphi H_\Phi, \tag{1.2.24}$$

so that

$$\Psi_L^{-1} = \Phi_L^{-1}\sigma^{-1} = \coprod_{\varphi \in \Phi^r} \varphi H_\Phi \sigma^{-1} = \coprod_{\varphi \in \Phi^r} \varphi\sigma^{-1} H_\Psi. \tag{1.2.25}$$

Restricting to the reflex field of Ψ, we obtain the statement of the proposition. □

Proposition 1.2.26. *Let (K, Φ) be a sextic CM type where K has Galois group D_6. If Φ is primitive, then write $\Phi = \sigma\Phi_0$, where Φ_0 corresponds to the set $\{0, 1, 5\}$ in the notation of Proposition 1.2.13. Then $(K^r, \Phi^r) = (\sigma(K^r), \Phi_0^r\sigma^{-1})$. If Φ is imprimitive, then (K^r, Φ^r) is the restriction of (K, Φ) to the quadratic CM subfield of K.*

Proof. This follows from 1.2.21 because the left stabilizer of Φ_0 is again generated by the element τ in Proposition 1.2.13. □

The reflex fields for the remaining Galois groups are described in the upcoming propositions.

Proposition 1.2.27. *Let K be a sextic CM field with Galois group $C_2^3 \rtimes C_3$, and let $\sigma = ((0, 0, 0), (1\,2\,3))$ and $\varrho = ((1, 1, 1), e)$ as in Proposition 1.2.8. Let*

$$\Phi_1 = \{\mathrm{id}\,|_K, \sigma|_K, \sigma^2|_K\}, \qquad \Phi_2 = \{\mathrm{id}\,|_K, \sigma\varrho|_K, \sigma^2|_K\},$$
$$\Phi_3 = \{\mathrm{id}\,|_K, \sigma|_K, \sigma^2\varrho|_K\}, \qquad \Phi_4 = \{\mathrm{id}\,|_K, \sigma\varrho|_K, \sigma^2\varrho|_K\}$$

be representatives of the primitive CM types of K up to equivalence. Then the reflex field K^r of (K, Φ_i) is fixed by the group $H_i^r \subset \mathrm{Gal}(L|\mathbb{Q})$, where

$$H_1^r = \langle\sigma\rangle,\ H_2^r = \langle\sigma n_0 n_1\rangle,\ H_3^r = \langle\sigma n_1 n_2\rangle,\ H_4^r = \langle\sigma n_0 n_2\rangle, \tag{1.2.28}$$

with n_i as defined in the proof of Proposition 1.2.14. We have

$$K_2^r = n_1(K_1^r),\ K_3^r = n_2(K_1^r),\ K_4^r = n_1 n_2(K_1^r). \tag{1.2.29}$$

The reflex CM types Φ_i^r are all given by

$$\Phi_1^r = \Phi_2^r = \Phi_3^r = \Phi_4^r = \{\mathrm{id}\,|_{K_i^r}, n_1|_{K_i^r}, n_2|_{K_i^r}, n_1 n_2|_{K_i^r}\}. \tag{1.2.30}$$

Proof. Let $H = \{e, n_1, n_2, n_1 n_2\}$ be the subgroup of the Galois group corresponding to K. First consider the CM type Φ_1. The induced CM type $\Phi_{1,L}$ on L is the union

$$H \cup \sigma H \cup \sigma^2 H = \{((*, *, 0), e)\} \cup \{((0, *, *), (1\,2\,3))\} \cup \{((*, 0, *), (1\,3\,2))\}. \tag{1.2.31}$$

From this explicit presentation, one obtains that the left stabilizer H_1^r of $\Phi_{1,L}$ is generated by σ. Using equalities similar to (1.2.16) shows that $\Phi_2 = n_1\Phi_1$, $\Phi_3 = n_2\Phi_1$, and $\Phi_4 = n_1n_2\Phi_1$. The corresponding stabilizers are therefore given generated by $n_1\sigma n_1^{-1} = \sigma n_0 n_1$, $n_2\sigma n_2^{-1} = \sigma n_1 n_2$, and $n_1n_2\sigma(n_1n_2)^{-1} = \sigma n_0 n_2$.

The embeddings in the reflex CM type of Φ_1 are in bijective correspondence with the elements of

$$\Phi_{1,L}^{-1} = H^{-1} \cup H^{-1}\sigma^{-1} \cup H^{-1}\sigma^{-2} = H \cup H\sigma^{-1} \cup H\sigma^{-2} \tag{1.2.32}$$

up to the action of the right stabilizer $H_1^r = \langle\sigma\rangle$. These are therefore represented by the elements of H, which yields the second statement of the proposition for Φ_1. Since $\Phi_2 = n_1\Phi_1$, $\Phi_3 = n_2\Phi_1$, and $\Phi_4 = n_1n_2\Phi_1$, representatives of the corresponding inverse CM types up to the right action of the corresponding stabilizers are furnished by n_1H, n_2H, and n_1n_2H. These are all equal to H, and therefore we obtain the second statement for all CM types Φ_i. □

Proposition 1.2.33. *Let K be a sextic CM field with Galois group $C_2^3 \rtimes S_3$, let $\sigma = ((0,0,0),(1\,2\,3))$, let $\tau = ((0,0,0),(1\,2))$, let $\varrho = ((1,1,1),e)$, and let*

$$\Phi_1 = \{\mathrm{id}\,|_K, \sigma|_K, \sigma^2|_K\}, \qquad \Phi_2 = \{\mathrm{id}\,|_K, \sigma\varrho|_K, \sigma^2|_K\},$$
$$\Phi_3 = \{\mathrm{id}\,|_K, \sigma|_K, \sigma^2\varrho|_K\}, \qquad \Phi_4 = \{\mathrm{id}\,|_K, \sigma\varrho|_K, \sigma^2\varrho|_K\}$$

be representatives of the primitive CM types of K up to equivalence. Then the reflex field K^r of (K,Φ_i) is fixed by the group $H_i^r \subset \mathrm{Gal}(L|\mathbb{Q})$, where

$$H_1^r = \langle\sigma,\tau\rangle,\ H_2^r = \langle\sigma n_0 n_1, \tau n_1 n_2\rangle,\ H_3^r = \langle\sigma n_1 n_2, \tau n_1 n_2\rangle,\ H_4^r = \langle\sigma n_0 n_2, \tau\rangle, \tag{1.2.34}$$

with n_i as defined in the proof of Proposition 1.2.14. We have

$$K_2^r = n_1(K_1^r),\ K_3^r = n_2(K_1^r),\ K_4^r = n_1n_2(K_1^r). \tag{1.2.35}$$

The reflex CM types Φ_i^r are all given by

$$\Phi_1^r = \Phi_2^r = \Phi_3^r = \Phi_4^r = \{\mathrm{id}\,|_{K_i^r}, n_1|_{K_i^r}, n_2|_{K_i^r}, n_1n_2|_{K_i^r}\}. \tag{1.2.36}$$

Proof. The proof is similar to that of the previous proposition. □

Corollary 1.2.37. *Let K be a sextic CM field. Then all primitive CM types of K are Galois equivalent.*

Proof. We proved this result in Propositions 1.2.12, 1.2.13, and 1.2.14, which cover all individual cases in Theorem 1.1.2. □

Remark 1.2.38. In genus 4, it is no longer true that all primitive CM types are Galois equivalent. Let K be an octic CM field with Galois group C_8, for example $\mathbb{Q}(\zeta_{32} + \zeta_{32}^{15})$. Then (with notation as in the case C_6 above) the CM types $\{0,1,2,3\}$ and $\{0,1,2,6\}$ are primitive, yet they are not related even when combining the two equivalences.

1.3. **Geometric relevance.** Let K be a CM field of degree $2g$. As in [46], we consider pairs $(\mathfrak{a},\xi)$, where $\mathfrak{a}$ is a fractional $\mathbb{Z}_K$-ideal and where $\xi \in K$ is a totally imaginary element such that $(\xi) = (\mathfrak{a}\bar{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$. Such a pair $(\mathfrak{a},\xi)$ uniquely determines a CM type Φ that consists of those embeddings φ of K into $\mathbb{C}$ for which the imaginary part of $\varphi(\xi)$ is positive. In what follows, we will consider the pairs $(\mathfrak{a},\xi)$ and the corresponding triples $(\Phi,\mathfrak{a},\xi)$ interchangeably. Either gives rise to a ppav $A(\mathfrak{a},\xi) = (\mathbb{C}^g/\Phi(\mathfrak{a}), E)$ over $\mathbb{C}$ whose endomorphism ring is isomorphic to $\mathbb{Z}_K$. The polarization E that comes with $A(\mathfrak{a},\xi)$ is induced by the trace pairing on K.

Conversely, given a ppav A over $\mathbb{C}$ whose endomorphism algebra is isomorphic to $\mathbb{Z}_K$, we can consider the representation of K on the tangent space after choosing some isomorphism $\mathrm{End}(A) \otimes \mathbb{Q} \simeq K$. The set of embeddings that thus appear yield a primitive CM type Φ of K. It is important

to note that the representation of K depends on the chosen isomorphism, which means that given the ppav A, only the *equivalence class* of the CM type Φ is well-defined.

The following is shown in [46, Theorem 4.2]:

Proposition 1.3.1. *Let K be a CM field of degree $2g$, and let Φ be a* primitive *CM type of K. Then the association*

$$(\mathfrak{a}, \xi) \mapsto A(\mathfrak{a}, \xi) = (\mathbb{C}^g/\Phi(\mathfrak{a}), E) \tag{1.3.2}$$

defined above yields a bijection between the set of pairs $(\mathfrak{a}, \xi)$ at the beginning of this section up to the equivalence

$$(\mathfrak{a}, \xi) \sim (\mathfrak{a}', \xi') \text{ if } (\mathfrak{a}', \xi') = (\gamma\mathfrak{a}, (\gamma\overline{\gamma})^{-1}\xi) \text{ for } \gamma \in K^* \tag{1.3.3}$$

and the set of isomorphism classes of principally polarized abelian varieties that admit CM by $\mathbb{Z}_K$ of type Φ up to equivalence.

Definition 1.3.4. We say that two pairs $(\mathfrak{a}, \xi)$ and $(\mathfrak{a}', \xi')$ are *equivalent* if there exists an element $\alpha \in \mathrm{Aut}(K)$ such that $(\alpha^{-1}(\mathfrak{a}), \alpha(\xi))$ and $(\mathfrak{a}', \xi')$ are equivalent in the sense of Proposition 1.3.1.

The following is shown in [46, Proposition 4.11]:

Proposition 1.3.5. *Two pairs $(\mathfrak{a}, \xi)$ and $(\mathfrak{a}', \xi')$ are equivalent if and only if $A(\mathfrak{a}, \xi)$ and $A(\mathfrak{a}', \xi')$ are isomorphic as principally polarized abelian varieties.*

Recall that we have fixed an embedding of the Galois closure L into $\mathbb{C}$.

Proposition 1.3.6. *Let A be a principally polarized abelian variety over $\mathbb{C}$ with CM by K of type Φ up to equivalence, and let $\sigma \in \mathrm{Aut}(\mathbb{C})$. Denoting the restriction of σ to L by σ again, we have that the conjugate principally polarized abelian variety σA has CM by K of type $\sigma\Phi$ up to equivalence.*

Proof. This follows from the fact that the formation of the tangent space is functorial. Alternatively, if $T \in M_g(\mathbb{C})$ is the tangent representation of a given endomorphism α with respect to a basis of differentials B of A, then σT is a representation of an endomorphism of σA with respect to σB. This means that if after our choice of embedding $K \hookrightarrow \mathrm{End}(A)$ we can write the representation ϱ of K on the tangent space of A as a direct sum

$$\varrho \cong \varphi_1 \oplus \cdots \oplus \varphi_g,$$

we also obtain a representation $\sigma\varrho$ of K on the tangent space of σA given by

$$\sigma\varrho \cong \sigma\varphi_1 \oplus \cdots \oplus \sigma\varphi_g,$$

which proves the proposition. □

Corollary 1.3.7. *Let A be a principally polarized abelian variety over $\mathbb{C}$ with* primitive *CM by K up to equivalence, and suppose that $\mathrm{Gal}(L \,|\, \mathbb{Q})$ is isomorphic to D_6 (resp. $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$). Then the degree of the field of moduli of A over $\mathbb{Q}$ is a multiple of 3 (resp. 4).*

Proof. This follows because the subgroup of $\mathrm{Aut}(\mathbb{C})$ that fixes the field of moduli has to fix the primitive CM type up to equivalence of A by Proposition 1.3.6, combined with the transitivity of the Galois action proved in Corollary 1.2.37. □

2. The Shimura class group and the Galois action

2.1. **Background.** We recall some fundamental notions. Throughout, we let K be a CM field.

Definition 2.1.1. The Shimura class group $\mathcal{C}_K$ of K is the abelian group of equivalence classes

$$\mathcal{C}_K = \left\{(\mathfrak{b}, \beta) : \mathfrak{b} \text{ is fractional } \mathbb{Z}_K\text{-ideal},\ \beta \in K_0^* \text{ totally positive with } \mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K\right\} / \sim \tag{2.1.2}$$

where $(\mathfrak{b}, \beta) \sim (\mathfrak{b}', \beta')$ if $(\mathfrak{b}', \beta') = (x\mathfrak{b}, x\overline{x}\beta)$ for $x \in K^*$.

As was shown in [8, Theorem 3.1], the structure of $\mathcal{C}_K$ is given by the sequence

$$1 \to (\mathbb{Z}_{K_0}^*)^+/N_{K|K_0}(\mathbb{Z}_K^*) \xrightarrow{u \longmapsto (\mathbb{Z}_K, u)} \mathcal{C}_K \xrightarrow{(\mathfrak{b},\beta) \longmapsto \mathfrak{b}} \mathrm{Cl}(K) \xrightarrow{N_{K|K_0}} \mathrm{Cl}^+(K_0), \tag{2.1.3}$$

where $(\mathbb{Z}_{K_0}^*)^+ \subset \mathbb{Z}_{K_0}^*$ is the group of totally positive units, and $\mathrm{Cl}^+(K_0)$ is the narrow class group of K_0.

Remark 2.1.4. As is discussed in [8], the final map in (2.1.3) is surjective if a finite prime ramifies in the extension $K \mid K_0$. This turns out to be the case for all fields considered in this article, as follows by checking that the relative different $\mathcal{D}_{K|K_0} = \{\alpha - \varrho(\alpha) : \alpha \in \mathbb{Z}_K\}$ is a proper ideal (also see the proof of [46, Proposition 4.4]). Under this hypothesis, denoting $h(K) = |\mathrm{Cl}(K)|$ and $h^+(K_0) = |\mathrm{Cl}^+(K_0)|$, we have

$$|\mathcal{C}_K| = \frac{h(K)}{h^+(K_0)} \cdot \left|(\mathbb{Z}_{K_0}^*)^+/N_{K|K_0}(\mathbb{Z}_K^*)\right|. \tag{2.1.5}$$

Let $N = N_{K^r|\mathbb{Q}} : K^r \to \mathbb{Q}_{>0}$ be the absolute norm map. Combining this map with the reflex type norm

$$\begin{aligned} N_{\Phi^r} : \mathrm{Cl}(K^r) &\to \mathrm{Cl}(K) \\ [\mathfrak{a}] &\mapsto \left[\mathbb{Z}_K \cap \prod_{\varphi \in \Phi^r} \varphi(\mathfrak{a})\mathbb{Z}_L\right], \end{aligned} \tag{2.1.6}$$

we obtain a map from the regular class group of K^r to the Shimura class group of K, namely

$$\begin{aligned} \mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) &\to \mathcal{C}_K \\ [\mathfrak{a}] &\mapsto (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})). \end{aligned} \tag{2.1.7}$$

2.2. **Torsors and moduli spaces.** We denote by $\mathcal{M}_{\mathbb{Z}_K}$ the set of isomorphism classes of ppavs with primitive CM by $\mathbb{Z}_K$. Given a primitive CM type Φ, we denote by $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ the set of isomorphism classes of ppavs that admit CM of type Φ.

Proposition 2.2.1. *There is a disjoint union $\mathcal{M}_{\mathbb{Z}_K} = \bigcup_\Phi \mathcal{M}_{\mathbb{Z}_K}(\Phi)$, where Φ runs over a set of representatives of the equivalence classes of primitive CM types of K.*

Proof. This follows from the fact that given a ppav (A, E) with primitive CM by K, the CM type of (A, E) is uniquely determined up to equivalence, as recapitulated at the beginning of Section 1.3. □

Similar to $\mathcal{C}_K$, we define the group

$$C = \left\{(\mathfrak{b}, \beta) : \mathfrak{b} \text{ is fractional } \mathbb{Z}_K\text{-ideal},\ \beta \in K^* \text{ with } \mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K\right\} / \sim \tag{2.2.2}$$

where $(\mathfrak{b}, \beta) \sim (\mathfrak{b}', \beta')$ if $(\mathfrak{b}', \beta') = (x\mathfrak{b}, x\overline{x}\beta)$ for $x \in K^*$. Then there is a tautological injection of groups

$$\mathcal{C}_K \hookrightarrow C. \tag{2.2.3}$$

The group C acts on the pairs $(\mathfrak{a}, \xi)$ from Section 1.3 via

$$(\mathfrak{b}, \beta)(\mathfrak{a}, \xi) = (\mathfrak{b}^{-1}\mathfrak{a}, \beta\xi). \tag{2.2.4}$$

Proposition 2.2.5. *Let $c = (\mathfrak{b}, \beta) \in C$, and let $(\mathfrak{b}, \beta)(\mathfrak{a}, \xi) = (\mathfrak{a}', \xi')$. Let Φ' be the CM type of $(\mathfrak{a}', \xi')$. Then $\Phi' = \Phi$ if and only if $c \in \mathcal{C}_K$.*

Proof. This follows because the imaginary parts of ξ and ξ' have positive signs at the same complex embeddings if and only if β is totally positive. □

Let $c = (\mathfrak{b}, \beta) \in C$ and $(\mathfrak{a}, \xi)$ be as above. If $\mathfrak{b}$ is integral, then $\mathfrak{b}^{-1}\mathfrak{a}$ properly contains $\mathfrak{a}$. Proposition 2.2.5 shows that if $c \in \mathcal{C}_K$, the pairs $(\mathfrak{a}, \xi)$ and $c(\mathfrak{a}, \xi)$ have the same CM type Φ. This means that for $c \in \mathcal{C}_K$ the inclusion $\Phi(\mathfrak{a}) \subset \Phi(\mathfrak{b}^{-1}\mathfrak{a})$ furnishes a canonical isogeny

$$A(\mathfrak{a}, \xi) \to A((\mathfrak{b}, \beta)(\mathfrak{a}, \xi)). \tag{2.2.6}$$

Proposition 2.2.7. *Let K be a sextic CM field, and let Φ be a fixed primitive CM type. Then the set $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ is a torsor under the action of $\mathcal{C}_K$.*

Proof. Proposition 1.3.1 shows that $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ is a torsor if it is non-empty. Since $\mathcal{M}_{\mathbb{Z}_K} = \bigcup_\Phi \mathcal{M}_{\mathbb{Z}_K}(\Phi)$, where Φ runs over the primitive CM types of K up to equivalence, and since the Galois action on the components is transitive by Corollary 1.2.37, it suffices to prove that $\mathcal{M}_{\mathbb{Z}_K} \neq \emptyset$ in order to show that that one, and hence all, of the $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ with Φ primitive are torsors under $\mathcal{C}_K$.

For this, let $(\mathfrak{a}_0, \xi_0)$ be the pair explicitly constructed in [46, Proposition 4.4], which has CM by $\mathbb{Z}_K$. If the CM type Φ_0 associated to $(\mathfrak{a}_0, \xi_0)$ is primitive, then we are done. So suppose that Φ_0 is imprimitive. Then we consider the narrow Hilbert class field H_0^+ of K_0 and the Hilbert class field H of K. The final map in (2.1.3) fits into a commutative diagram

$$\begin{array}{ccc} \mathrm{Cl}(K) & \xrightarrow{N_{K|K_0}} & \mathrm{Cl}^+(K_0) \\ \downarrow\sim & & \downarrow\sim \\ \mathrm{Gal}(H\,|\,K) & \xrightarrow{\mathrm{res}} & \mathrm{Gal}(H_0^+\,|\,K_0) \end{array} \tag{2.2.8}$$

where the map on the bottom is restriction. The inclusion $KH_0^+ \subset H$ yields a surjective restriction map $\mathrm{Gal}(H\,|\,K) \to \mathrm{Gal}(KH_0^+\,|\,K)$. By Galois theory, the latter group is isomorphic to $\mathrm{Gal}(H_0^+\,|\,K \cap H_0^+)$. Since $K \cap H_0^+$ is an at most quadratic extension of K_0, we see that the image N of $N_{K|K_0}$ is of index at most 2 in $\mathrm{Cl}^+(K_0)$.

Let $\mathfrak{Id}(K_0)$ be the group of fractional $\mathbb{Z}_{K_0}$-ideals. Fix an enumeration of the real embeddings of K_0, and given an element $\alpha \in K_0^*$, let $\mathrm{sgn}_i(\alpha)$ denote the sign of α under the ith embedding. Then under the map $[\mathfrak{a}] \mapsto [(\mathfrak{a}, (1,1,1))]$ the narrow class group $\mathrm{Cl}^+(K_0)$ becomes isomorphic to the group $\mathfrak{Id}(K_0) \times \langle -1 \rangle^3$ modulo the equivalence relation

$$(\mathfrak{a}, (s_1, s_2, s_3)) \sim (\mathfrak{a}', (s_1', s_2', s_3'))$$
$$\text{if there exists } \alpha \in K_0^* \text{ such that } \mathfrak{a}' = \alpha\mathfrak{a} \text{ and } s_i' = \mathrm{sgn}_i(\alpha) s_i.$$

The exact sequence

$$0 \to \langle -1 \rangle^3 \to \mathfrak{Id}(K_0) \times \langle -1 \rangle^3 \to \mathfrak{Id}(K_0) \to 0 \tag{2.2.9}$$

induces

$$0 \to S \to \mathrm{Cl}^+(K_0) \to \mathrm{Cl}(K_0) \to 0 \tag{2.2.10}$$

where S is the quotient of $\langle -1 \rangle^3$ by the image of $\mathbb{Z}_{K_0}^*$ under the sign maps.

As before, let N be the image of $\mathrm{Cl}(K)$ in $\mathrm{Cl}^+(K_0)$ under the norm map. Since [49, Theorem 10.1] shows that the norm map $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ is surjective, and N is of index at most 2 in $\mathrm{Cl}^+(K_0)$, we see that $N \cap S$ is of index at most 2 in S. By (2.2.10) this implies that there exists a $\mathbb{Z}_K$-ideal $\mathfrak{b}$ such that $\mathfrak{b}\overline{\mathfrak{b}}$ is generated by an element $\beta \in K_0$ whose signs at the infinite places of K_0 do not all coincide.

Now let $(\mathfrak{a}, \xi) = (\mathfrak{b}, \beta)(\mathfrak{a}_0, \xi_0)$. Then because of the sign property of β, the CM type Φ corresponding to $(\mathfrak{a}, \xi)$ differs from both Φ_0 and $\overline{\Phi}_0$. Our classification of the CM types of sextic CM fields in Section 1 then shows that Φ is primitive. Therefore $\mathcal{M}_{\mathbb{Z}_K}$ is non-empty, since it contains the ppav corresponding to $(\mathfrak{a}, \xi)$. $\square$

As in [46, Proposition 4.4], we define the quotient

$$s_K = \frac{\mathrm{Cl}(K)}{\mathrm{Cl}(K_0)} \left| \mathbb{Z}_{K_0}^* / N_{K|K_0}(\mathbb{Z}_K^*) \right|.$$

It is shown in *loc. cit.* that s_K is the number of pairs (Φ, A), where Φ is a CM type of K (not necessarily primitive) and where A is an isomorphism class of ppavs that admits Φ as a CM type.

Corollary 2.2.11. *Let K be a sextic CM field with Galois closure L. Then we have*

$$|\mathcal{M}_{\mathbb{Z}_K}| = \begin{cases} |\mathcal{C}_K| = s_K/8 & \text{if } K \text{ is Galois,} \\ 3\,|\mathcal{C}_K| = 3s_K/8 & \text{if } \mathrm{Gal}(L\,|\,\mathbb{Q}) \cong D_6, \\ 4\,|\mathcal{C}_K| = s_K/2 & \text{if } \mathrm{Gal}(L\,|\,\mathbb{Q}) \cong C_2^3 \rtimes C_3 \text{ or } C_2^3 \rtimes S_3. \end{cases} \tag{2.2.12}$$

Proof. The first equalities involving $|\mathcal{C}_K|$ follow by combining Proposition 2.2.1, 1.2.12, 1.2.13, and 1.2.14. As for the second equalities, if $\mathrm{Gal}(L\,|\,\mathbb{Q})$ is isomorphic to either $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, then all CM types Φ of K are primitive and Proposition 2.2.7 shows that $s_K = 8\,|\mathcal{C}_K|$. If $\mathrm{Gal}(L\,|\,\mathbb{Q})$ is isomorphic to C_6 or D_6, then Proposition 2.2.7 shows that $|M_K(\Phi)| = |\mathcal{C}_K|$ for all 6 primitive CM types of K. If $|M_K(\Phi)| = 0$ for one (and hence both) of the imprimitive CM types of K, then we would have $s_K = 6\,|\mathcal{C}_K|$. On the other hand, comparing the exact sequence in [46, Proposition 4.4] with (2.1.3) shows that $s_K/\,|\mathcal{C}_K|$ is a power of 2. This contradiction shows that $s_K = 8\,|\mathcal{C}_K|$ for all cases, which yields the statement. □

Corollary 2.2.13. *The statement of Proposition 2.2.7 also holds for imprimitive CM types Φ of sextic CM fields.*

Proof. This follows from the proof of Corollary 2.2.11. □

2.3. **Representatives up to Galois conjugacy.** Let us fix a primitive CM type Φ of K. Then the set $\mathcal{M}_K(\Phi)$ is stable under the action of $G^r = \mathrm{Gal}(\overline{\mathbb{Q}}\,|\,K^r)$, and the orbits of $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ under the action of the group G^r correspond to the elements of the quotient $\mathcal{C}_K/\,\mathrm{im}(\mathcal{N}_{\Phi^r})$. More precisely, we have the following result.

Theorem 2.3.1 (Main Theorem of Complex Multiplication)**.** *Let $(A, E) \cong A(\mathfrak{a}, \xi)$ in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$, and let $\sigma \in G^r$. Suppose that under the Artin map, the element σ correspond the class of the ideal $\mathfrak{b}$. Then*

$$\sigma(A(\mathfrak{a}, \xi)) \cong A(\mathcal{N}_{\Phi^r}(\mathfrak{b})(\mathfrak{a}, \xi)). \tag{2.3.2}$$

We will use this reciprocity law to prove Theorem 2.3.23, which shows that given $A(\mathfrak{a}_0, \xi_0)$ in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$, we can obtain any other isomorphism class $A(\mathfrak{a}, \xi)$ in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ as a Galois conjugate of an abelian variety $A(\mathfrak{b}\mathfrak{a}_0, \eta_0)$, where $\mathfrak{b}$ runs through a fixed (small) set of representatives of G_2/eG_2, where $G_2 = \ker(N_{K|K_0}) \subset \mathrm{Cl}(K)$ and where $e|4$. The usefulness of this result stems from the fact that G_2/eG_2 is usually far smaller than G_2 itself. We start with a general observation.

Proposition 2.3.3. *Let Φ and Ψ be Galois equivalent CM types. Then there is an equality of double reflex maps*

$$N_{\Phi^r} \circ N_\Phi = N_{\Psi^r} \circ N_\Psi. \tag{2.3.4}$$

Proof. Let $\Psi = \sigma(\Phi)$ for $\sigma \in \mathrm{Gal}(L\,|\,\mathbb{Q})$. Then we have

$$N_\Psi(\mathfrak{a}) = \prod_{\psi \in \Psi} \psi(\mathfrak{a}) = \prod_{\varphi \in \Phi} \sigma(\varphi(\mathfrak{a})) = \sigma(\prod_{\varphi \in \Phi} \varphi(\mathfrak{a})) = \sigma(N_\Phi(\mathfrak{a})) \tag{2.3.5}$$

for all ideals $\mathfrak{a}$ of $\mathbb{Z}_K$. Moreover, by Proposition 1.2.21 we have

$$N_{\Psi^r}(\mathfrak{b}) = \prod_{\psi \in \Psi^r} \psi(\mathfrak{b}) = \prod_{\varphi \in \Phi^r} \varphi(\sigma^{-1}(\mathfrak{b})) \tag{2.3.6}$$

for all ideals $\mathfrak{b}$ of $\mathbb{Z}_{K^r}$. Therefore

$$N_{\Psi^r}(N_\Psi(\mathfrak{a})) = N_{\Psi^r}(\sigma(N_\Phi(\mathfrak{a}))) = \prod_{\varphi\in\Phi^r} \varphi(\sigma^{-1}(\sigma(N_\Phi(\mathfrak{a})))) = \prod_{\varphi\in\Phi^r} \varphi(N_\Phi(\mathfrak{a})) = N_{\Phi^r}(N_\Phi(\mathfrak{a})) \quad (2.3.7)$$

for all ideals $\mathfrak{a}$ of $\mathbb{Z}_K$, which proves our claim. □

For the next statement, also see [45, Theorem 2.2] and [26].

Lemma 2.3.8. *Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6. Then there exists a primitive CM type Ψ such that for all primitive CM types Φ and for all fractional $\mathbb{Z}_K$-ideals $\mathfrak{a}$ we have an equality of fractional $\mathbb{Z}_L$-ideals*

$$N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_{K|\mathbb{Q}}(\mathfrak{a})\mathfrak{a}\overline{\mathfrak{a}}^{-1}N_\Psi(\mathfrak{a}). \quad (2.3.9)$$

If Φ is imprimitive, then $N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_\Phi(\mathfrak{a})$.

Proof. We prove the statement for the case where the Galois group is isomorphic to D_6. The Galois case is similar. Using the notation in Proposition 1.2.13, let $H = \mathrm{Gal}(L\,|\,K) = \langle\tau\rangle$, and let σ be the generator of the set of embeddings of K into L. By Proposition 2.3.3, it suffices to consider the case $\Phi_L = \{0,1,2\}$. Then $\Phi_L^r = \{0,5,4\}$, and the double norm computation gives rise to the element

$$(1+\sigma^5+\sigma^4)(1+\sigma+\sigma^2) = 3+2\sigma+\sigma^2+\sigma^4+2\sigma^5 \quad (2.3.10)$$

in the group algebra of $\mathrm{Gal}(L\,|\,\mathbb{Q})$. If we consider the elements in this sum up to right multiplication by elements of the group H, we get

$$3H+2\sigma H+\sigma^2H+\sigma^4H+2\sigma^5H = (H+\sigma H+\sigma^2H+\sigma^3H+\sigma^4H+\sigma^5H) \quad (2.3.11)$$
$$+ (H-\sigma^3H) + (H+\sigma H+\sigma^5H). \quad (2.3.12)$$

The first two terms correspond to $N_{K|\mathbb{Q}}(\mathfrak{a})$ and $\mathfrak{a}\overline{\mathfrak{a}}^{-1}$, respectively. The last sum corresponds to the CM type $\Psi_L = \{0,1,5\}$, and is independent of the choice of Φ_L.

In the imprimitive case we can take $\Phi_L = \{0,2,4\}$. The reflex field is then the unique quadratic CM subfield of K, and the reflex type its canonical inclusion, which shows our claim. □

Proposition 2.3.13. *Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6, and let Φ be a primitive CM type of K. If $[\mathfrak{b}] \in \mathrm{Cl}(K)$ satisfies $\mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K$ for $\beta \in K_0^*$, then $[\mathfrak{b}^2]$ is in the image of the reflex type norm $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$.*

Proof. First let Ψ be the distinguished primitive CM type in Lemma 2.3.8. If $\mathfrak{a} = N_\Psi(\mathfrak{b})\mathbb{Z}_L$, then by Lemma 2.3.8 we have an equality of fractional $\mathbb{Z}_L$-ideals

$$N_{\Psi^r}(\mathfrak{a}) = N_{\Psi^r}(N_\Psi(\mathfrak{b})) = N_{K|\mathbb{Q}}(\mathfrak{b})\mathfrak{b}\overline{\mathfrak{b}}^{-1}N_\Psi(\mathfrak{b}) = N_{K|\mathbb{Q}}(\mathfrak{b})\beta^{-1}N_{\Psi^r}(\mathfrak{b})\mathfrak{b}^2. \quad (2.3.14)$$

We therefore have that $N_{\Psi^r}([\mathfrak{a}]) = N_{\Psi^r}([\mathfrak{b}])[\mathfrak{b}^2]$ and $[\mathfrak{b}^2] = N_{\Psi^r}([\mathfrak{a}\mathfrak{b}^{-1}]) \in \mathrm{im}(N_{\Psi^r})$. But Proposition 1.2.21 implies that if $\Phi = \sigma(\Psi)$, then $\Phi^r = \Psi^r\sigma^{-1}$, so that N_{Φ^r} and N_{Ψ^r} have equal images in $\mathrm{Cl}(K)$. (Indeed, if $\mathfrak{b} = N_{\Psi^r}(\mathfrak{c})$, then $\mathfrak{b} = N_{\Phi^r}(\sigma(\mathfrak{c}))$.) Since all primitive CM types are Galois equivalent, we obtain our claim. □

Proposition 2.3.15. *Let K be a sextic CM field with Galois group isomorphic to C_6 or D_6. For any primitive CM type Φ of K and any equivalence class $(\mathfrak{b},\beta)$ in $\mathcal{C}_K$ the equivalence class of $(N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2)$ is in the image of the map $\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K$. Furthermore, if $N_\Psi(\mathfrak{b}) = \mu\mathbb{Z}_K$ is a principal $\mathbb{Z}_K$-ideal, then said image $(N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2)$ is equivalent to $(\mathfrak{b}^2,\beta^2)$.*

Proof. With $\mathfrak{a} = N_\Phi(\mathfrak{b})\mathbb{Z}_L$ and Proposition 2.3.13 we get that

$$\begin{aligned}\mathcal{N}_{\Phi^r}(\mathfrak{a}) &= (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})) = (N_{\Phi^r}(N_\Phi(\mathfrak{b})), N(N_\Phi(\mathfrak{b})))\\ &= (N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^{-1}N_\Phi(\mathfrak{b})\mathfrak{b}^2\overline{N(\mathfrak{b})\beta^{-1}N_\Phi(\mathfrak{b})\mathfrak{b}^2})\\ &= (N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})^2N_\Phi(\mathfrak{b})\overline{N_\Phi(\mathfrak{b})})\\ &= (N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})^3)\end{aligned}$$

where

$$\begin{aligned}N_{K|K_0}(N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2) &= N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2\overline{N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2}\\ &= N(\mathfrak{b})^2(\mathfrak{b}\overline{\mathfrak{b}})^{-1}\overline{(\mathfrak{b}\overline{\mathfrak{b}})^{-1}}N_\Psi(\mathfrak{b})\overline{N_\Psi(\mathfrak{b})}\mathfrak{b}^2\overline{\mathfrak{b}}^2\\ &= N(\mathfrak{b})^3\mathbb{Z}_K.\end{aligned}$$

Then since $\beta \in K_0$, the equivalence relation (2.1.2) yields

$$(N(\mathfrak{b})\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})^3) \sim (\beta^{-1}N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})) \sim (N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2),$$

This shows the first claim. If $N_\Psi(\mathfrak{b}) = \mu\mathbb{Z}_K$ is a principal ideal, then

$$(N_\Psi(\mathfrak{b})\mathfrak{b}^2, N(\mathfrak{b})\beta^2) \sim (\mu\mathfrak{b}^2, N(\mathfrak{b})\beta^2) \sim (\mathfrak{b}^2, (\mu\overline{\mu})^{-1}N(\mathfrak{b})\beta^2) \sim (\mathfrak{b}^2, \beta^2)$$

which shows the second claim. □

Lemma 2.3.16. *Let K be a sextic CM field with Galois group isomorphic to $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, and let Φ be a CM type of K. Then for all fractional $\mathbb{Z}_K$-ideals $\mathfrak{a}$ we have an equality of fractional $\mathbb{Z}_L$-ideals*

$$N_{\Phi^r}(N_\Phi(\mathfrak{a})) = N_{K|\mathbb{Q}}(\mathfrak{a})^2(\mathfrak{a}\overline{\mathfrak{a}}^{-1})^2. \tag{2.3.17}$$

Proof. We prove this for the CM type Φ_1 and Galois group $C_2^3 \rtimes C_3$: The statement for the other CM types follows from Proposition 2.3.3, and the argument for the group $C_2^3 \rtimes S_3$ is similar. Using the notation in Proposition 1.2.27, the extensions of Φ_1 and Φ_1^r to L are given by $\{1, \sigma, \sigma^2\}$ and $\{1, n_1, n_2, n_1n_2\}$, respectively. Considering the given double norm comes down to studying the element

$$(1+n_1+n_2+n_1n_2)(1+\sigma+\sigma^2) = 1+n_1+n_2+n_1n_2+\sigma+n_1\sigma+n_2\sigma+n_1n_2\sigma+\sigma^2+n_1\sigma^2+n_2\sigma^2+n_1n_2\sigma^2 \tag{2.3.18}$$

in the group algebra of $\mathrm{Gal}(L\,|\,\mathbb{Q})$, where we consider the elements in this sum up to right multiplication by elements of the subgroup $H = \langle n_1, n_2\rangle$ corresponding to the field K. In terms of the cosets in (1.2.15), this yields

$$\begin{aligned}&H + n_1H + n_2H + n_1n_2H + \sigma H + n_1\sigma H + n_2\sigma H + n_1n_2\sigma H + \sigma^2H + n_1\sigma^2H + n_2\sigma^2H + n_1n_2\sigma^2H\\ =&H + H + H + H + \sigma H + \sigma\varrho H + \sigma H + \sigma\varrho H + \sigma^2H + \sigma^2H + \sigma^2\varrho H + \sigma^2\varrho H\\ =&4H + 2\sigma H + 2\sigma^2H + 2\sigma\varrho H + 2\sigma^2\varrho H\\ =&(2H + 2\sigma H + 2\sigma^2H + 2\varrho H + 2\sigma\varrho H + 2\sigma^2\varrho H) + (2H - 2\varrho H),\end{aligned} \tag{2.3.19}$$

which shows the claim. □

Proposition 2.3.20. *Let K be a sextic CM field with Galois group isomorphic to $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$, and let Φ be a CM type of K. If $[\mathfrak{b}] \in \mathrm{Cl}(K)$ satisfies $\mathfrak{b}\overline{\mathfrak{b}} = \beta\mathbb{Z}_K$ for $\beta \in K_0^*$, then $[\mathfrak{b}^4]$ is in the image of the reflex type norm $N_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathrm{Cl}(K)$.*

Proof. Once more we only give the proof for the Galois group $C_2^3 \rtimes C_3$. If $\mathfrak{a} = N_\Phi(\mathfrak{b})\mathbb{Z}_L$, then by Lemma 2.3.16 we have an equality of fractional $\mathbb{Z}_L$-ideals

$$N_{\Phi^r}(\mathfrak{a}) = N_{\Phi^r}(N_\Phi(\mathfrak{b})) = N_{K|\mathbb{Q}}(\mathfrak{b})^2\left(\mathfrak{b}\overline{\mathfrak{b}}^{-1}\right)^2 = N_{K|\mathbb{Q}}(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4. \tag{2.3.21}$$

We therefore have that $N_{\Phi^r}([\mathfrak{a}]) = [\mathfrak{b}^4]$, which shows the claim. □

Proposition 2.3.22. *Let K be a sextic CM field with Galois group isomorphic to $C_2^3 \rtimes C_3$ or $C_2^3 \rtimes S_3$. For any CM type Φ of K and any equivalence class $(\mathfrak{b}, \beta)$ in $\mathcal{C}_K$, the equivalence class of $(\mathfrak{b}^4, \beta^4)$ is in the image of the map $\mathcal{N}_{\Phi^r} : \mathrm{Cl}(K^r) \to \mathcal{C}_K$.*

Proof. With $\mathfrak{a} = N_\Phi(\mathfrak{b})\mathbb{Z}_L$ and Proposition 2.3.20 we get

$$\begin{aligned}\mathcal{N}_{\Phi^r}(\mathfrak{a}) &= (N_{\Phi^r}(\mathfrak{a}), N(\mathfrak{a})) = (N_{\Phi^r}(N_\Phi(\mathfrak{b})), N(N_\Phi(\mathfrak{b}))) = (N(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4, N(\mathfrak{b})^2(\mathfrak{b}\overline{\mathfrak{b}}^{-1})^2\overline{N(\mathfrak{b})^2(\mathfrak{b}\overline{\mathfrak{b}}^{-1})^2})\\ &= (N(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4, N(\mathfrak{b})^4),\end{aligned}$$

Since $\beta \in K_0$, using the equivalence relation in Shimura class group yields that

$$(N(\mathfrak{b})^2\beta^{-2}\mathfrak{b}^4, N(\mathfrak{b})^4) \sim (\beta^{-2}\mathfrak{b}^4, 1) \sim (\mathfrak{b}^4, \beta^4),$$

which shows the claim. □

We can now state the main result of this section:

Theorem 2.3.23. *Let $G_2 = \ker(N_{K|K_0}) \subset \mathrm{Cl}(K)$ be the subgroup of classes $[\mathfrak{b}]$ with the property that $\mathfrak{b}\overline{\mathfrak{b}}$ is generated by a totally positive element of K_0. Let B be a set of ideals that furnishes representatives of the quotient $Q = G_2/eG_2$, where $e = 2$ if $\mathrm{Gal}(K) \in \{C_6, D_6\}$ and where $e = 4$ if $\mathrm{Gal}(K) \in \{C_2^3 \rtimes C_3, C_2^3 \rtimes S_3\}$. Similarly, let V be a set of units that furnishes representatives of the quotient $(\mathbb{Z}_{K_0}^*)^+/N_{K|K_0}(\mathbb{Z}_K^*)$.*

Fix $A(\mathfrak{a}_0, \xi_0)$ in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$, and let $A(\mathfrak{a}, \xi)$ in $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ be given. Then the Galois orbit of $A(\mathfrak{a}, \xi)$ under the action of $G^r = \mathrm{Gal}(\overline{\mathbb{Q}} \mid K^r)$ contains an abelian variety isomorphic to $A(\mathfrak{b}\mathfrak{a}_0, v\beta^{-1}\xi_0)$, where $\mathfrak{b} \in B$, where $\beta \in K_0$ generates $\mathfrak{b}\overline{\mathfrak{b}}$, and where $v \in V$.

Proof. Proposition 2.2.7 along with (2.1.3) shows that $A(\mathfrak{a}, \xi)$ is isomorphic to $A(\mathfrak{b}\mathfrak{a}_0, v\beta^{-1}\xi_0)$ for some ideal $\mathfrak{b}$ with $[\mathfrak{b}] \in G_2$ and for some $v \in V$. Propositions 2.3.13 and 2.3.20 show that the first component of the map $\mathcal{N}_{\Phi_r}$ surjects onto eG_2. Applying a corresponding Galois conjugation to $A(\mathfrak{a}, \xi)$ if needed, we may therefore assume that $\mathfrak{b} \in B$, after which another invocation of (2.1.3) shows our claim. □

3. Running through the LMFDB

3.1. **Algorithms.** Let K be a sextic CM field. The considerations in the previous sections give rise to a method to determine representatives of the set of ppavs with CM by $\mathbb{Z}_K$ up to isomorphism and Galois conjugacy. We split up the steps of this method into several algorithms. Throughout, we fix not only the CM field K but also a primitive CM type Φ of K with values in $\mathbb{C}$. (It is in fact not essential that Φ be primitive, but this is the case that interests us in the current article.) Similar algorithms were considered in lower genus in the previous works [18] and [46]. We discuss differences in our approach in passing.

Algorithm 3.1.1. *(Precomputation step)*

Input: *A sextic CM field K.*

Output: *Precomputed data used in the later Algorithms 3.1.3, 3.1.7, and 3.1.9.*

(1) *Determine the class group and unit group $\mathrm{Cl}(K), \mathbb{Z}_K^*$ of K and the class group, narrow class group and unit group $\mathrm{Cl}(K_0), \mathrm{Cl}^+(K_0), \mathbb{Z}_{K_0}^*$ of its totally real subfield K_0;*

(2) *Determine the subgroup* $G_1 \subset \mathrm{Cl}(K)$ *of classes* $[\mathfrak{a}] \in \mathrm{Cl}(K)$ *with the property that* $\mathfrak{a}\overline{\mathfrak{a}}$ *is generated by an element of* K_0*;*
(3) *Determine the subgroup* $G_2 \subset \mathrm{Cl}(K)$ *of classes* $[\mathfrak{a}] \in G_1$ *with the property that* $\mathfrak{a}\overline{\mathfrak{a}}$ *is generated by a totally positive element of* K_0*;*
(4) *Let* $Q = G_2/eG_2$*, where* $e = 2$ *if* $\mathrm{Gal}(K) \in \{C_6, D_6\}$ *and where* $e = 4$ *if* $\mathrm{Gal}(K) \in \{C_2^3 \rtimes C_3, C_2^3 \rtimes S_3\}$*;*
(5) *Determine a set of ideals* C *of* $\mathbb{Z}_K$ *that furnishes representatives of the quotient* G_1/G_2*, as well as a set of ideals* B *of* $\mathbb{Z}_K$ *that furnishes representatives of the quotient* $Q = G_2/eG_2$*;*
(6) *Determine the subgroup* $U_1 \subset \mathbb{Z}_{K_0}^*$ *of totally positive units in* $\mathbb{Z}_{K_0}^*$*;*
(7) *Determine the subgroup* $U_2 \subset U_1$ *of units in* $\mathbb{Z}_{K_0}^*$ *that are norms from* $\mathbb{Z}_K^*$*;*
(8) *Determine a set of units* W *that furnishes representatives of the quotient* $\mathbb{Z}_{K_0}^*/U_1$*, as well as a set of units* V *that furnishes representatives of the quotient* U_1/U_2*.*

The steps in this algorithm can be performed by using classical algorithms for class and unit groups. We restrict ourselves to some remarks on steps that are somewhat less standard.

Remark 3.1.2. (i) Under the generalized Riemann hypothesis, the calculation of the class und unit group of K and K_0 in Step (1) speeds up tremendously. We have therefore used this assumption while performing our calculations.

(ii) We can determine the subgroup G_1 in Step (2) as the kernel of the homomorphism $\mathrm{Cl}(K) \to \mathrm{Cl}(K_0)$ given by $[\mathfrak{a}] \mapsto [\mathfrak{a}\overline{\mathfrak{a}}]$, and G_2 as the kernel of a similar homomorphism to $\mathrm{Cl}^+(K_0)$. Similar considerations apply to the determination of U_1 and U_2 in Steps (6) and (7).

(iii) It is important that the representatives returned by Algorithm 3.1.1 be minimized, since otherwise large precision loss will occur in later steps. In [18, §4.1], this minimization is also mentioned as being useful when working with the Shimura class group in the genus-2 case. For our purposes this is not merely useful, but also indispensable in practice, as the class groups involved are of considerable size and working with large powers of ideal class generators without reducing these already causes unacceptable precision loss when determining the corresponding lattices in $\mathbb{C}^3$ in Algorithm 3.1.9. We therefore spend a few lines on this reduction step.

For an ideal representative in B and C, this observation means that it should be multiplied with a principal ideal in such a way that the norm of the resulting product is smaller than the Minkowski bound M of K. This can be done as follows. Given an ideal $\mathfrak{a}$ to be minimized, one computes the lattice Γ in $\mathbb{C}^3$ that is the image of $\mathfrak{a}^{-1}$ under the complex embeddings of K. One then determines a short vector α in Γ, and the corresponding element α of $\mathfrak{a}^{-1}$ will satisfy $N_{K|\mathbb{Q}}(\alpha) \leq M N_{K|\mathbb{Q}}(\mathfrak{a}^{-1})$. Therefore the norm of the ideal $\alpha\mathfrak{a}$ is at most M, and we use this product as a minimized ideal representative.

For a unit that furnishes a representative in V, resp. W, being small means the following. Let $\ell : \mathbb{Z}_{K_0}^* \to \mathbb{R}^2$ be the log map whose image is the Dirichlet lattice of the unit group $\mathbb{Z}_{K_0}^*$. Then given an element u of V (resp. W) to be minimized, we can use closest vector algorithms to find an element u_1 (resp. u_2) of U_1 (resp. U_2) such that that $\ell(u) + \ell(u_1)$ (resp. $\ell(u) + \ell(u_2)$) is small, and we use the corresponding product $u \cdot u_1$ (resp. $u \cdot u_2$) as a minimized unit representative.

(iv) Note that in contrast to the methods in [18], our precomputation does not require the computation of the Shimura class group or the image of the reflex norm, which simplifies its description.

Algorithm 3.1.3. *(Determining an initial triple* $(\Phi, \mathfrak{a}, \xi)$*)*

INPUT: *A sextic CM field* K *and a primitive CM type* Φ *of* K*.*

OUTPUT: *A single triple* $(\Phi, \mathfrak{a}, \xi)$*, with* $\mathfrak{a}$ *a fractional* $\mathbb{Z}_K$*-ideal and with* $\xi \in K$ *totally imaginary, such that* $(\Phi, \mathfrak{a}, \xi)$ *represents a principally polarized abelian threefold* A *with CM by* K *of* Φ*.*

(1) Determine a pair $(\mathfrak{a}_0, \xi_0)$ such that $(\xi_0) = (\mathfrak{a}_0\overline{\mathfrak{a}_0}\mathfrak{D}_{K|\mathbb{Q}})^{-1}$. If the imaginary part of ξ_0 is positive for all embeddings in Φ, then return $(\Phi, \mathfrak{a}_0, \xi_0)$. Otherwise, proceed to the next step.
(2) Run through the elements $\mathfrak{c}$ of C, and let $\gamma \in K_0$ be a generator of $\mathfrak{c}\overline{\mathfrak{c}}$.
(3) Within the previous loop, run through the elements w of W, and consider $(\mathfrak{a}, \xi) = (\mathfrak{c}\mathfrak{a}_0, w\gamma^{-1}\xi_0)$. If $(\mathfrak{a}, \xi)$ admits Φ as a CM type, or in other words, if ξ has positive imaginary part for the embeddings in Φ, then return $(\Phi, \mathfrak{a}, \xi)$.

Proof. If the algorithm returns a triple, then it is correct by construction. It therefore remains to show that the algorithm does always furnish an output.

First note that the existence of a triple $(\Phi, \mathfrak{a}, \xi)$ as in the Output step follows from Proposition 2.2.7. Now suppose that we have determined a pair $(\mathfrak{a}_0, \xi_0)$ as in Step (1) of the algorithm. Then since both $\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}}^{-1}$ and $\mathfrak{a}_0\overline{\mathfrak{a}}_0\mathfrak{D}_{K|\mathbb{Q}}^{-1}$ are principal, and generated by totally imaginary elements of K, we have that the class of $\mathfrak{a}\mathfrak{a}_0^{-1}$ belongs to G_1. Let $\mathfrak{c} \in C$ be an element representing this class, and let $\gamma \in K_0$ be the chosen generator of $\mathfrak{c}\overline{\mathfrak{c}}$. We can then write $\mathfrak{a} = \delta\mathfrak{c}\mathfrak{a}_0$ with $\delta \in K^*$. Let $\mathfrak{b} = \mathfrak{c}\mathfrak{a}_0$. Then

$$(\delta\overline{\delta}\xi) = ((\delta\overline{\delta})^{-1}\mathfrak{a}\overline{\mathfrak{a}}\mathfrak{D}_{K|\mathbb{Q}})^{-1} = (\mathfrak{b}\overline{\mathfrak{b}}\mathfrak{D}_{K|\mathbb{Q}})^{-1} \tag{3.1.4}$$

and

$$(\gamma^{-1}\xi_0) = ((\mathfrak{c}\overline{\mathfrak{c}})\mathfrak{a}_0\overline{\mathfrak{a}}_0\mathfrak{D}_{K|\mathbb{Q}})^{-1} = (\mathfrak{b}\overline{\mathfrak{b}}\mathfrak{D}_{K|\mathbb{Q}})^{-1}, \tag{3.1.5}$$

so since ξ and ξ_0 are totally imaginary, we have $\delta\overline{\delta}\xi = u\gamma^{-1}\xi_0$ for a unit $u \in \mathbb{Z}_{K_0}^*$. Let $w \in W$ be a representative of the class corresponding to u. Then $(\mathfrak{c}\mathfrak{a}_0, w\gamma^{-1}\xi_0)$ has the property that the imaginary parts of $w\gamma^{-1}\xi_0$ has the same signs as $\delta\overline{\delta}\xi$, and hence as ξ. These are exactly the signs compatible with Φ. Therefore since the algorithm encounters this triple as it runs, it is indeed guaranteed to return the requested output. □

Remark 3.1.6. (i) Finding a pair $(\mathfrak{a}_0, \xi_0)$ as in Step (1) of Algorithm 3.1.3 is possible by using the methods of [46, Proposition 4.4]: In fact the pair $(\mathfrak{a}_0, yz)$ in *loc. cit.* can be used.
(ii) For all cases in the LMFDB, Algorithm 3.1.3 did in fact find a triple $(\Phi, \mathfrak{a}, \xi)$. This is the case because the final condition in Corollary 1.2.37 is satisfied for all sextic CM fields in the LMFDB.

Given an initial triple $(\Phi, \mathfrak{a}, \xi)$ returned by Algorithm 3.1.3, the others can be determined quickly by using the precomputed data from Algorithm 3.1.1:

Algorithm 3.1.7. *(Determining all triples $(\Phi, \mathfrak{a}, \xi)$)*
Input: A sextic CM field K and a primitive CM type Φ of K.
Output: A set S of triples $(\Phi, \mathfrak{a}, \xi)$ as in [46, Theorem 4.2]*, so that $(\mathfrak{a}, \xi)$ represents a principally polarized abelian threefold A that admits CM by K of Φ. Moreover, S satisfies the following property: Up to Galois conjugacy over the reflex field K^r, any pair (Φ, A), where A is a principally polarized abelian threefold that admits CM by $\mathbb{Z}_K$, is isomorphic over $\mathbb{C}$ to an abelian variety corresponding to one of the elements of S.*

(1) Let $(\Phi, \mathfrak{a}_0, \xi_0)$ be the triple from Algorithm 3.1.3.
(2) Run through the elements $\mathfrak{b}$ of B, and let $\beta \in K_0$ be a generator of $\mathfrak{b}\overline{\mathfrak{b}}$.
(3) Within the previous loop, run through the elements v of V, and add $(\mathfrak{a}, \xi) = (\mathfrak{b}\mathfrak{a}_0, v\beta^{-1}\xi_0)$ to S.
(4) Return S once the loops above have terminated.

Proof. The correctness of Algorithm 3.1.7 follows from Theorem 2.3.23. □

Remark 3.1.8. (i) We do not claim that the given set S is in actual bijection with the set of isomorphism classes of pairs (Φ, A) up to Galois conjugacy, and indeed this is not the

case in general. For our purposes, it suffices that the abelian varieties associated map surjectively to the latter set of equivalence classes, and we do not impose additionally that this natural map be injective.

(ii) As was shown in Equation (2.1.5), the size of $\mathcal{M}_{\mathbb{Z}_K}(\Phi)$ is well approximated by $h(K)/h^+(K_0)$. When $G = C_2^3 \rtimes S_3$, the largest size of the quotient $h(K)/h^+(K_0)$ in (2.1.5) was 11287, whereas the largest size of the group Q was 128, thus showing the speed gain that our taking into account Galois conjugacy provides.

Algorithm 3.1.9. *(Determining period matrices)*

Input: A sextic CM field K and a primitive CM type Φ of K.

Output: The small period matrices τ corresponding to the elements of the set S in Algorithm 3.1.7, sorted into two sets T_H and T_N that (heuristically) give rise to hyperelliptic and non-hyperelliptic curves, respectively.

(1) Determine the set S from Algorithm 3.1.7, and initialize T_H and T_N to be empty sets.

(2) Let $(\Phi, \mathfrak{a}, \xi)$ be in S. Calculate the corresponding principally polarized abelian threefold (A, E) in the usual manner [46, §4], setting $A = \mathbb{C}^3/\Phi(\mathfrak{a})$ and letting E be the $\mathbb{R}$-linear extension of the trace pairing $(\alpha, \beta) \mapsto \mathrm{Tr}_{K|\mathbb{Q}}(\xi\alpha\overline{\beta})$.

(3) Determine a Frobenius alternating form of E to find some big period matrix $P \in M_{3,6}(\mathbb{C})$ for A, and from it, a small period matrix $\tau \in M_{3,3}(\mathbb{C})$.

(4) Reduce τ by using the methods from [27, §2].

(5) Use algorithms, for example those by Labrande [30], to determine whether τ has 1 or 0 vanishing even theta-null values to some high precision (typically 100 digits). In the former case, add τ to T_H; in the latter, add it to T_N.

Remark 3.1.10. (i) Note that our algorithms differ from those in [46], as we fix our primitive CM type Φ throughout. When considering CM curves up to Galois conjugacy, we are justified in doing so because of Corollary 1.2.37.

(ii) Because we have insisted that Φ be a primitive CM type, the associated abelian threefolds are indeed Jacobians of genus-3 curves. The criterion for said Jacobian to be hyperelliptic in terms of even theta-null values is [20, Lemmata 10 and 11].

(iii) Like the minimization of representatives in Algorithm 3.1.1, Steps (4) of Algorithm 3.1.9 is essential to keep its running time short.

(iv) Our own run of Algorithm 3.1.9 used the native Magma implementation in Step (5) instead of the algorithms from [30]. The even theta values were computed to 100 digits of precision, and decided to be numerically equal to zero when their absolute value is at most 10^{-50}. Setting `Labrande := true` in the implementation at [14] allows for an alternative verification of these results using [30] instead.

(v) Using interval arithmetic or the fast decay of the terms intervening in the sum that define a even theta-null value, it is in principle possible to prove rigorously that all such values are non-zero. This enables one to prove that a ppav A that Algorithm 3.1.9 suspects to come from a non-hyperelliptic indeed comes from such a curve. By contrast, showing that A comes from a hyperelliptic curve is more involved. For the moment, we see no other rigorous method to check this than to calculate an equation for a corresponding curve X as in 4 and to show that $\mathrm{Jac}(X)$ has CM using the algorithms in [11]. We discuss some further sanity checks in the next section.

3.2. **Fields.** With the algorithms from Section 3.1 in hand, we considered the sextic CM fields in the LMFDB [47]. We list our results, which imply Main Results 1 and 2, Table 1. Its first column lists the possible Galois groups, whereas its second column gives the corresponding number of sextic CM fields in the LMFDB.

We have applied our algorithms, implemented in MAGMA [5] and available at [14], to all of these $547,156$ fields, except for 2 fields with Galois group D_6 whose root discriminant exceeds 10^{12} and for which the calculation of the class and unit group did not finish in a timely fashion even when assuming the generalized Riemann hypothesis. The total computation required 4 days on 20 cores when working to relatively high precision to absolutely exclude rounding errors.

The second column of Table 1 indicates the number of CM fields K in the database whose Galois group is isomorphic to that indicated in the first column. specified Galois The third column of Table 1 indicates the number of CM fields K considered for which the set T_H from Algorithm 3.1.9 is non-empty, or in other words those fields K for which there (heuristically) exists a hyperelliptic curve whose Jacobian has *primitive* CM by $\mathbb{Z}_K$. For simplicity, we call such a CM field K hyperelliptic.

As was already known, and as can be deduced from the classification in [38], if a CM field K contains $\mathbb{Q}(i)$, then any curve whose Jacobian has primitive CM by $\mathbb{Z}_K$ is automatically hyperelliptic. We call a hyperelliptic CM field K that does *not* include $\mathbb{Q}(i)$ exceptional hyperelliptic. The fourth column of Table 1 lists the number of hyperelliptic fields K that are exceptional.

The fifth column of Table 1 indicates the number of fields for which both sets H and N from Algorithm 3.1.9 there heuristically exists both a hyperelliptic and a non-hyperelliptic curve whose Jacobian has CM by $\mathbb{Z}_K$. For simplicity, we call such a sextic CM field K mixed. Note that all mixed fields are exceptional hyperelliptic.

Galois group	$\#K$	# hyp. K	# exc. hyp. K	# mixed K
C_6	10,067	348	2	0
D_6	32,544	3,057	0	0
$C_2^3 \rtimes C_3$	10,159	0	0	0
$C_2^3 \rtimes S_3$	494,386	17	17	14
Total	547,156	3,422	19	14

TABLE 1. CM fields in the LMFDB

3.3. **Invariants.** Let $\tau \in M_{g,g}(\mathbb{C})$ be a small period matrix. This section briefly recapitulates what is known on calculating and algebraizing the invariants of the curve over X associated to τ, as well as verifying the correctness of the resulting curve.

Algorithm 3.1.9 shows that we can calculate an approximation to τ to a given high precision, as all that we need to do is to determine the image of a basis of a (minimized) representative $\mathfrak{a}$ under the given CM type Φ. What is considerably more complicated is to calculate the even theta-null values associated to τ. Here it is in general essential to use the more sophisticated algorithms by Labrande [30] to keep the running time within reasonable bounds. We have noticed in passing that the available implementation of this algorithm does not always function, but still managed to get by in the cases that interested us, either by using the naive method from [30] to lower precision or by determining the even theta-null values for only a single element of a given Galois orbit and conjugating afterwards.

Given the even theta-null values, we can determine a model of X over $\mathbb{C}$ to the given precision, either by using the Rosenhain invariants as in [1] or by using the Weber model from [27]. We can then calculate a normalized weighted representative I of the corresponding invariants (using the Shioda invariants in the hyperelliptic case and the Dixmier–Ohno invariants in the non-hyperelliptic case). The field of moduli of X then coincides with the field generated by the entries of I.

Algebraization. It remains to algebraize the invariants I. A first possible method is the usual application of the LLL algorithm to determine putative minimal polynomials of the entries of I over $\mathbb{Q}$ and thus to obtain I as elements of a number field. One corresponding implementation is `NumberFieldExtra` in [10]. A second method is to symmetrize and use class polynomials, as in

[13, 18]. Both of these methods became prohibitive in the cases that we considered because of the large heights of the algebraic numbers that were involved. Indeed, one of the mixed fields, defined by the polynomial $x^6 - 2x^5 + 11x^4 + 42x^3 - 11x^2 + 340x + 950$, gives rise to a tuple of normalized Dixmier–Ohno invariants whose first non-trivial entry I_6 has height $\approx 2.94 \cdot 10^{431}$, with I_{27} having a height that larger by an exponential factor of about $27/6$. Another reason for us not to use the class polynomial method from [18] is that this would necessitate later factorization to determine the Galois orbits, which is superfluous when algebraizing the individual I directly.

Instead we exploited the fact that that the Shimura reciprocity law implies that the entries of I are the complex embeddings of elements of Hilbert class field H of the reflex field K^r. This replaces the problem of determining minimal polynomials to the more tractable one of trying to algebraize the elements of I in H or its subfields, which also reduces to an application of LLL (for example in the form of the routine `AlgebraizeElementsExtra` in [10]). In the aforementioned complicated case we needed $20,000$ digits of precision for our algebraization, but usually around $3,000$ digits were enough. Incidentally, note that while the reflex K^r itself can be costly to determine via the usual Galois theory, since the closure L becomes quite large, it can still be quickly recovered numerically as a subfield of $\mathbb{C}$, namely by applying the methods from the previous paragraph.

Verification. Once we have algebraized the elements of I, we have applied heuristic numerical methods twice, both in the determination of I itself and in the algebraization of its elements. One may well ask why one should trust the algebraic invariant values thus obtained to be correct. Here are several reasons:

(i) For all algebraizations I that we found, the resulting invariants satisfy the known algebraic dependencies between the Shioda invariants (which can be found in [36]) or the Dixmier–Ohno invariants (which can be found in [37]). There is no reason whatsoever for this to hold in the case of incorrect or badly algebraized I.

(ii) Reducing the values of I modulo various large primes, one can apply the reconstruction algorithms from [34] or [35] and then calculate Weil polynomials to check that the resulting curves indeed have CM by an order in K for all these primes.

(iii) Conversely, one can bound the primes of bad reduction from I and check that the set thus obtained contains the primes found in [22].

(iv) In principle one can verify all results obtained over $\overline{\mathbb{Q}}$ by using [11]. That said, these algorithms still need substantial speedups for these verifications to be feasible for plane quartic curves over number fields.

This is why we do not harbor any doubts about our results being correct, even though they are by no means mathematically rigorous yet.

3.4. **The mixed cases.** Table 2 describes the results for the 17 fields K from Table 1 with Galois group $C_2^3 \times S_3$ that are exceptional. Note that there are also 2 exceptional hyperelliptic fields with Galois group C_6, but these were already considered in [21]: Corresponding polynomials are given by $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1$ and $x^6 - 14x^3 + 63x^2 + 168x + 161$.

The first column of Table 2 gives the polynomial defining the CM field K; this column is sorted by the absolute discriminant of the ring of integers $\mathbb{Z}_K$. The second column describes the length of the various hyperelliptic Galois orbits under conjugation by $\mathrm{Gal}(\overline{\mathbb{Q}} \,|\, \mathbb{Q})$; for example, an entry $4^2 8^1$ stands for 2 Galois orbits of length 4 along with single Galois orbit of length 8. Similarly, the third column describes the length of the non-hyperelliptic Galois orbits under $\mathrm{Gal}(\overline{\mathbb{Q}} \,|\, \mathbb{Q})$. An empty entry means that there does not exist such a curve for the field K. Note that Corollary 1.3.7 shows why the length of the Galois orbits in the table are all a multiple of 4. The final column describes the quotient $\mathcal{C}_K / \operatorname{im}(\mathcal{N}_\Phi)$ of the Shimura class group by the image of the reflex type norm. Note that this independent of the chosen primitive CM type Φ because of Proposition 1.2.21 and Corollary 1.2.37.

The invariants obtained for the fields in Table 2 are available at [14]. As mentioned above, they are occasionally on the gargantuan side.

CM field	hyp. orbits	non-hyp. orbits	$\mathcal{C}_K/\operatorname{im}(\mathcal{N}_\Phi)$
$x^6+10x^4+21x^2+4$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6-3x^5+14x^4-23x^3+28x^2-17x+4$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6-2x^5+12x^4-31x^3+59x^2-117x+121$	4^1	$4^1 8^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6+14x^4+43x^2+36$	4^1		1
$x^6-3x^5+9x^4+4x^3+12x^2+84x+236$	4^1	$4^1 8^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6-2x^5+x^4-4x^3+5x^2-50x+125$	4^1	4^3	$(\mathbb{Z}/2\mathbb{Z})^2$
$x^6+29x^4+246x^2+512$	4^1		1
$x^6-3x^5+10x^4+8x^3+x^2+90x+236$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6+21x^4+60x^2+4$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6+30x^4+169x^2+200$	4^1	4^1	$(\mathbb{Z}/2\mathbb{Z})^2$
$x^6+23x^4+112x^2+36$	4^1		1
$x^6-2x^5+12x^4-44x^3+242x^2-672x+1224$	12^1	12^3	$(\mathbb{Z}/2\mathbb{Z})^2$
$x^6+26x^4+177x^2+128$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6+29x^4+226x^2+252$	4^1	$4^1 8^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6-2x^5-7x^4+45x^3-63x^2-162x+729$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$
$x^6-2x^5+11x^4+42x^3-11x^2+340x+950$	8^1	$8^1 16^1$	$\mathbb{Z}/4\mathbb{Z}$
$x^6-3x^5+29x^4-53x^3+200x^2-174x+71$	4^1	4^1	$\mathbb{Z}/2\mathbb{Z}$

TABLE 2. Generic hyperelliptic and mixed fields with Galois group $C_2^3 \rtimes S_3$ and the lengths of the corresponding Galois orbits

4. Explicit defining equations

In this section we further consider the mixed CM field K defined by $x^6+10x^4+21x^2+4$, which corresponds to the first entry of Table 2. Our goal is to indicate how to obtain the (heuristic) explicit defining equations from Main Result 3. The actual calculations are performed in [14]; here we briefly explain the ideas that underlie them.

There are two Galois orbits in this case, one containing 4 hyperelliptic curves, and one containing 4 non-hyperelliptic curves. Moreover, Corollary 1.2.37 shows that once we fix a CM type Φ, which we do throughout this section, there is exactly one corresponding hyperelliptic curve X and one non-hyperelliptic curve Y. We start by finding an equation for X.

4.1. **Hyperelliptic simplification.** As in Section 3.3, we determine a normalized tuple S of Shioda invariants corresponding to the curve X, which is defined over the quartic field L corresponding to the polynomial x^4-5x^2-2x+1. The field L is in fact the totally real subfield of the reflex field K^r of K.

One can try to apply the generic reconstruction algorithms in genus 3 that are available in MAGMA, but this turns out not to be optimal, as the resulting hyperelliptic curve is returned over a random quadratic extension of L with large defining coefficients. Instead, we directly construct the Mestre conic and quartic C and Q over K from the invariants S, as in [34], and then check whether the conic C admits a rational point. This turns out to be the case. Choosing a parametrization $\mathbb{P}^1 \to C$ over K and pulling back the divisor $C \cap Q$ on C, we obtain a degree-8 divisor on $\mathbb{P}^1$ that corresponds to a monic octic polynomial f with the property that

$$X : y^2 = f \tag{4.1.1}$$

is a curve with CM by $\mathbb{Z}_K$. This is still far from satisfactory, however, as the coefficients of f are extremely large, namely of height up to $4.92 \cdot 10^{1126}$. We show how to obtain a simpler equation. Our approach is essentially ad hoc; while there are minimization and reduction algorithms in Magma over the rationals due to Cremona–Stoll [44], and over real quadratic number fields due to Bouyer–Streng [7], we do not find ourselves in one of these cases, so that we are forced to use other methods.

The octic polynomial f factors as

$$f = f_1 f_2 f_3, \tag{4.1.2}$$

where f_1 and f_2 are quadratic, both defined over a pleasant quadratic extension M of L with defining polynomial $x^8 - 4x^7 + 10x^5 + 7x^4 - 10x^3 - 18x^2 - 6x + 1$ over the rationals. (That this extension is so agreeable is of course no surprise; the extended version of the Main Theorem of Complex Multiplication, applied to the 2-torsion of $\mathrm{Jac}(X)$, shows that we should expect it to be related to the Hilbert class field of L ramifying at its single even prime.)

We now consider f over the quadratic extension M of L, over which field we will construct a simpler polynomial defining the same hyperelliptic curve, which we will the descend back to L. To start our simplification over M, we apply a Möbius transformation in the x-coordinate that sends the roots of f_1 to 0 and ∞ and one of the roots of f_2 to 1. This maps the divisor defined by the octic polynomial f to that defined by a *septic* polynomial g that additionally satisfies $g(0) = g(1) = 0$. We normalize g in such a way that the coefficient of x^4 equals 1, for reasons that will become clear, so that

$$g = c_7 x^7 + c_6 x^6 + c_5 x^5 + x^4 + c_3 x^3 + c_2 x^2 + c_1 x. \tag{4.1.3}$$

Now inspecting the norms of the coefficients c_i shows that we have

$$(c_5) = \mathfrak{p}_2^{-4}(\sigma(c_3)) \tag{4.1.4}$$

where $\mathfrak{p}_2$ is the unique ideal of $\mathbb{Z}_L$ above 2 and where σ is the involution that generates $\mathrm{Gal}(M \,|\, L)$. Following a hunch, we scale x by α^2, where α generates $\mathfrak{p}_2$. Transforming g accordingly, we obtain an equality of ideals

$$(c_i) = (\sigma(c_{8-i})) \tag{4.1.5}$$

for *all* i between 1 and 4.

Our goal is to make Equation (4.1.5) hold on the level of elements, and not merely between ideals. To achieve this, we consider the unit $u = c_5/\sigma(c_3) \in \mathbb{Z}_M^*$. Consider the polynomial h obtained from g by scaling x by vx, where $v \in \mathbb{Z}_M^*$ is another unit, and normalizing the coefficient of x^4 to equal 1. Then for the coefficients d_i of h we have $d_5 = vc_5$ and $d_3 = v^{-1}d_3$. The straight-up equality $d_5 = \sigma(d_3)$ that we are looking for can be rewritten as

$$vu\sigma(c_3) = vc_5 = d_5 = \sigma(d_3) = \sigma(v^{-1})\sigma(c_3) \tag{4.1.6}$$

This is the case if and only if

$$u = v\sigma(v). \tag{4.1.7}$$

Since $\mathbb{Z}_M^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}^5$ and v satisfies this equality if and only of $-v$ does, the equality (4.1.7) reduces to integral linear algebra once the representation of σ in terms of a given basis of $\mathbb{Z}_K^*$ is known. Performing the corresponding computation shows that we can indeed find a v with the requested properties. Rescaling x accordingly, we find a polynomial g as in (4.1.3) such that

$$(c_i) = (\sigma(c_{8-i})) \tag{4.1.8}$$

is satisfied for all $i = 1, \ldots, 4$.

At this point, our manipulations have lead to a polynomial g with coefficients of maximal height $8.64 \cdot 10^{16}$, which is smaller than $4.92 \cdot 10^{1126}$. We can still do a bit better by further scaling x by appropriate units v satisfying $v\sigma(v) = 1$. This does not affect the property (4.1.8). Our goal is to make d_5 as small as possible as an element of the Minkowski lattice up to shifts by units of the

indicated type. This reduces to a closest vector problem as in Remark 3.1.2, an approximation for which is quickly furnished by the usual techniques. Applying the corresponding scaling yields a slightly smaller polynomial g with coefficients of height $1.11 \cdot 10^{16}$.

It now remains to descend our polynomial g with coefficients in M to the original field L. For this, let σ be the involution that generates the Galois group $\mathrm{Gal}(M \mid L)$, and let $B \in \mathrm{GL}_2(M)$ be such that

$$\sigma(B) = AB, \qquad \text{where } A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}. \tag{4.1.9}$$

For example, we can take

$$B = \begin{pmatrix} 1 & \alpha \\ 1 & \sigma(\alpha) \end{pmatrix} \tag{4.1.10}$$

where $\alpha \in M$ is such that $M = L \oplus L\alpha$. The matrix B^{-1} induces a Möbius transformation of the projective line.

Proposition 4.1.11. *Let $D = (g)_0 \cup \{\infty\} \subset \mathbb{P}^1$, where $(g)_0$ is the divisor of zeros of the polynomial g, and let $E_0 = B^{-1}(D)$.*

(i) The divisor $E_0 \subset \mathbb{P}^1$ is defined over L.

(ii) Let f_0 be a polynomial whose divisor of zeros is given by E_0. Then the hyperelliptic curve $X_0 : y^2 = f_0$ over L is isomorphic over $\overline{\mathbb{Q}}$ to the original curve X in (4.1.1).

Proof. (i): The divisor E_0 is defined over M, as B and D are. Moreover, we have

$$\sigma(E_0) = \sigma(B^{-1}D) = \sigma(B)^{-1}\sigma(D) = B^{-1}A^{-1}AD = B^{-1}D = E_0 \tag{4.1.12}$$

This Galois invariance implies our claim.

(ii) This follows from (i) because two hyperelliptic curves are $\overline{\mathbb{Q}}$-isomorphic if (and only if) the corresponding branch loci are related by a Möbius transformation. □

Alternatively, f_0 is the numerator of the transform of g by B^{-1}. This turns out to be still of reasonable size when α is. Replacing X be X_0, we have achieved our aim of simplifying X. The result is the equation for X in Main Result 3. The discriminant of the corresponding hyperelliptic polynomial equals $\mathfrak{p}_4^{120}\mathfrak{p}_7^{12}$, where $\mathfrak{p}_4$ (resp. $\mathfrak{p}_7$) is an ideal of norm 4 (resp. 7).

4.2. **A plane quartic equation.** It remains to construct a plane quartic model for the non-hyperelliptic curve Y from the knowledge of its Dixmier–Ohno invariants I. The direct methods from [35] gives a ternary quartic with coefficients whose size is beyond hopeless. Methods to obtain defining equations of smaller size were sketched in [27, §3], using methods due to Elsenhans and Stoll [16, 43], yet like the methods of Cremona–Stoll in Section 4.1, these are specific to the base field $\mathbb{Q}$, and therefore of no use in the current situation.

Fortunately, now that we have found the equation for the hyperelliptic curve X in Main Result 3, determining the equation for the non-hyperelliptic curve Y becomes tractable. To see this, let $P_X \in M_{3,6}(\mathbb{C})$ be a big period matrix corresponding to X with respect to the canonical basis of differentials $\{dx/y, xdx/y, x^2dx/y\}$ corresponding to the equation (0.1), and let P_Y be the large period matrix of the Weber model $Y : F(x, y, z) = 0$ over $\mathbb{C}$ for Y obtained in the course of using Algorithm 3.1.9. This matrix, and all other big period matrices that follow, should be taken with respect to the canonical basis of differentials $(xdx(\partial F/\partial y)^{-1}, ydx(\partial F/\partial y)^{-1}, dx(\partial F/\partial y)^{-1})$.

Proposition 4.2.1. *There exist matrices $T \in M_{3,3}(\mathbb{C})$ and $R \in M_{6,6}(\mathbb{Z})$ such that R has determinant 2 and*

$$TP_Y = P_X R. \tag{4.2.2}$$

Moreover, the pair (T, R) is uniquely determined up to a minus sign.

Proof. This is a direct consequence of the fact that X and Y are related by an $\mathfrak{a}$-transformation with $N_{K|\mathbb{Q}}(\mathfrak{a}) = 2$. In turn, this statement follows from the fact (see Table 2) that $\mathcal{C}_K/\operatorname{im}(\mathcal{N}) \cong \mathbb{Z}/2\mathbb{Z}$, and that if we factor $(2) = \mathfrak{a}^4\mathfrak{b}^2$ in $\mathbb{Z}_K$, with $N_{K|\mathbb{Q}}(\mathfrak{a}) = N_{K|\mathbb{Q}}(\mathfrak{b}) = 2$, the ideal $\mathfrak{a}$ represents the non-trivial class in this quotient, which therefore induces an isogeny between the two distinct ppavs with CM by K of a fixed type Φ. The uniqueness claim follows from the fact that $\mathfrak{a}$ is the only ideal of norm 2 whose class in $\mathcal{C}_K/\operatorname{im}(\mathcal{N})$ is non-trivial. □

In what follows, given a matrix $T \in M_{3,3}(\mathbb{C})$ and a ternary quartic form $F \in \mathbb{C}[x, y, z]$, we denote the transformation of F under the natural right action of T by $F \cdot T$.

Proposition 4.2.3. *Let F be the ternary quartic form associated to the Weber model whose big period matrix is P_Y, and F_0 be a multiple of $F \cdot T^{-1}$ that is normalized in such a way that one of its coefficients is in L. Then $Y_0 : F_0(x, y, z) = 0$ is a model of Y over L.*

Proof. We know that Y has field of moduli equal to L. Now since the torsion subgroup of $\mathbb{Z}_K^*$ is reduced to $\langle -1\rangle$, the automorphism group $\operatorname{Aut}(Y)$ is trivial, since $\operatorname{Aut}(Y) = \operatorname{Aut}(\operatorname{Jac}(Y))/\langle -1\rangle$ for plane quartic curves Y. Therefore there exists a plane quartic curve $Z \subset \mathbb{P}^2$ defined over L that is isomorphic to Y. Let G be a corresponding form, and let P_Z be a corresponding period matrix. The same argument as above shows that there exists a matrix $U \in M_{3,3}(\mathbb{C})$ such that

$$UP_Z = P_X R. \tag{4.2.4}$$

Because both X and Z are defined over L, the uniqueness of R up to sign implies that $U \in M_3(\overline{\mathbb{Q}})$ and $\sigma(U) = \pm U$ for all $\sigma \in \operatorname{Gal}(\overline{\mathbb{Q}}\,|\,\mathbb{Q})$. Now let $G_0 = G \cdot U^{-1}$, normalized in such a way that one of its coefficients is in L. Since $\sigma(G \cdot U^{-1}) = \sigma(G) \cdot \sigma(U^{-1}) = G \cdot \pm U^{-1}$, we have that the class of $G \cdot U$ up to scalar is Galois stable. Therefore G_0 is defined over L, and its big period matrix is a scalar multiple of $UP_Z = P_X R$. On the other hand, the ternary quartic $F \cdot T$ also has a big period that is a scalar multiple of $TP_Y = P_X R$. Therefore F_0 and G_0 coincide up to a scalar, and because of our normalization F_0 has coefficients in L as well. □

An algebraization in the field L using LLL shows that we can indeed recover the coefficients of the ternary quartic form F_0 defining Y_0 over K. Tweaking its size by scaling x, y, z by units (similar to the closest vector considerations in Section 4.1) makes the equation of Y_0 somewhat smaller still. Replacing Y by Y_0 gives the equation for Y in Main Result 3. Its discriminant factors as $\mathfrak{p}_4^{312}\mathfrak{p}_7^{36}\mathfrak{p}_{19}^{14}\mathfrak{p}_{277}^{14}\mathfrak{p}_{1753}^{14}$, where as before subscripts indicate norms.

Remark 4.2.5. We emphasize once more that the equations obtained in this section have not yet been verified by the methods from [11] because of the considerable effort required to run these algorithms over large number fields.

5. Around the André–Oort conjecture

5.1. **General considerations.** In this section, we review a certain number of results around the André–Oort conjecture. The André–Oort conjecture was formulated in the general context of Shimura varieties and their special points. A proof of this conjecture under the assumption of the Generalized Riemann Hypothesis (GRH) for CM fields has been given by Klingler and Yafaev [24]. For an extensive survey on Shimura varieties and a general statement of the conjecture, the reader is refered to [39].

Although our focus is on genus 3, we start by stating facts that hold for every $g \geq 1$. We denote by $\mathcal{A}_g$ be the moduli space of ppavs of genus g over $\mathbb{C}$ and by $\mathcal{M}_g$ the moduli space of of smooth genus g curves defined over $\mathbb{C}$. Recall that the Torelli morphism

$$j : \mathcal{M}_g \to \mathcal{A}_g \tag{5.1.1}$$

associates to every curve its principally polarized Jacobian. We denote by $\mathcal{T}_g$ the closed Torelli locus, i.e. $\mathcal{T}_g = \overline{j(\mathcal{M}_g)}$.

As a complex variety, $\mathcal{A}_g = \mathrm{Sp}_{2g}(\mathbb{Z})\backslash\mathcal{H}_g$ is a Shimura variety whose special points are exactly the CM points. Recently, Tsimerman [48] proved a result showing the existence of a lower bound on the size of the Galois orbits of CM points in $\mathcal{A}_g$. Building on joint work with Pila [40], Tsimerman concluded in this way a proof of the André-Oort conjecture for $\mathcal{A}_g$ without the GRH assumption.

Theorem 5.1.2 (André–Oort conjecture [48])**.** *Let Γ be a set of CM points in $\mathcal{A}_g$. Then the Zariski closure of Γ is a finite union of Shimura subvarieties.*

Among the Shimura subvarieties of $\mathcal{A}_g$, a well known example is that of the Hilbert modular variety, whose points are polarized abelian varieties whose endomorphism ring contains the ring of integers of a totally real field of genus g. Hilbert modular varieties play an important role when studying the number of CM points in $\mathcal{T}_g$.

Indeed, let us turn our attention to the case of CM fields with Galois group isomorphic to $C_2^g \rtimes S_g$. Chai and Oort call these fields and their corresponding CM points sufficiently general (see [9, (2.13)] for a justification of this definition). We will use the following result given in [9].

Lemma 5.1.3. *Let Y be an irreducible Shimura subvariety of $\mathcal{A}_g$ of positive dimension. Assume that $Y \neq \mathcal{A}_g$ and that Y contains a sufficiently general CM point y in $\mathcal{A}_g$. Then Y is a Hilbert modular variety attached to the totally real subfield of degree g over $\mathbb{Q}$ contained in the CM field attached to y.*

This lemma allowed the authors of [9] to establish the following result for genus $g > 3$.

Theorem 5.1.4. *Assume the André–Oort conjecture to be true. Then for every $g > 3$ the number of sufficiently general CM points in $\mathcal{T}_g$ is finite.*

When $g = 3$, the closed Torelli locus $\mathcal{T}_3$ coincides with $\mathcal{A}_3$, but we believe that a similar argument can be adapted to genus 3, as soon as we restrict to the hyperelliptic locus. Indeed, let us denote by $\mathcal{M}_3^{\mathrm{hyp}}$ the image of the subspace of hyperelliptic curves inside the Torelli locus. Then $\mathcal{M}_3^{\mathrm{hyp}}$ contains infinitely many hyperelliptic curves with CM, since all genus 3 curves with CM by a field containing $\mathbb{Q}(i)$ are hyperelliptic. This is certainly in accordance with the Andre–Oort conjecture, since the Shimura surface parametrising points whose endomorphism ring contains $\sqrt{-1}$ is contained in $\mathcal{M}_3^{\mathrm{hyp}}$.

Assume now that $\mathcal{M}_3^{\mathrm{hyp}}$ contains infinitely many sufficiently general CM points. Then by the André–Oort conjecture and Lemma 5.1.3, it contains a Hilbert modular variety attached to a totally real field of degree 3. Recall that among the exceptional hyperelliptic fields listed in Table 2, 14 are mixed, i.e. they allow both a hyperelliptic and non-hyperelliptic curve. This quickly disproves the fact that the Hilbert modular variety corresponding to the real multiplication subfield of each of these fields could be contained in the hyperelliptic locus. For the remaining 3 exceptional hyperelliptic fields listed in the Table, we cannot reach a similar conclusion for the corresponding real multiplication subfields and their Hilbert modular varieties. One way to tackle the question experimentally would be to adapt our implementation to compute points with CM by non-maximal orders, which contain the maximal real multiplication order in these fields. Once the period matrices of these points are determined, it would suffice to use Algorithm 3.1.9 to check heuristically that some of the corresponding curves are not hyperelliptic.

As stated in the introduction, we do not have enough evidence to support the claim that the list of exceptional hyperelliptic CM fields mentioned in Main Result 1 and 2 is complete and we certainly do not claim that. However, the considerations above support the conjecture that the full list of exceptional hyperelliptic CM fields should be finite.

5.2. **Cryptographic implications.** Let us now turn our attention to applications in cryptography. The Discrete Logarithm Problem (DLP) in Jacobians of hyperelliptic curves defined over a finite field $\mathbb{F}_q$ (with $q = p^d$ and p a prime) can be solved in $\widetilde{O}(q^{4/3})$, using the index calculus algorithm of Gaudry, Thériault and Diem [19]. In contrast, Jacobians of non-hyperelliptic curves of genus 3 are amenable to Diem's index calculus algorithm, which requires only $\widetilde{O}(q)$ group operations to solve the DLP [12]. As a consequence, an efficient way of attacking DLP on a genus 3 hyperelliptic Jacobian is by reducing it to a DLP on a non-hyperelliptic Jacobian via an explicit isogeny. Assuming that the kernel of the isogeny will intersect trivially with the subgroup of cryptographic interest, we derive a $\widetilde{O}(q)$ time attack on the hyperelliptic Jacobian (see [42]). So an interesting question is how to find such isogenies.

Idea of the attack. To tackle this question, let us consider A an ordinary ppav defined over $\mathbb{F}_q$ isomorphic to a hyperelliptic Jacobian. The theory of canonical lifts of Serre and Tate allows us to lift A to an ordinary ppav $\widetilde{A}$ defined over $W(\mathbb{F}_q)$, the ring of Witt vectors of $\mathbb{F}_q$, such that $\mathrm{End}(A) \simeq \mathrm{End}(\widetilde{A})$ and $A \to \widetilde{A}$ is functorial (see [4]). After fixing an embedding $W(\bar{\mathbb{F}}_q) \hookrightarrow \mathbb{C}$, we may assume that $\widetilde{A}$ is a ppav defined over $\mathbb{C}$ with CM by the maximal ring of integers of K and CM type Φ. As suggested by our Main Results 1 and 2, hyperelliptic Jacobians with CM are rare, hence most of the times we expect $\widetilde{A}$ to be a non-hyperelliptic Jacobian with hyperelliptic reduction mod p. We now consider the following graph: the vertices are absolutely simple 3-dimensional ppav defined over $\mathbb{C}$ with CM by the maximal order of K and the edges are isogenies between ppavs. In the literature, this is known as the *horizontal isogeny graph* (see for instance [23]). Moreover, by [41, Ch. III, Sec. 11, Prop. 13], the isogenies in this graph will reduce to isogenies defined over $\mathbb{F}_q$ of equal degree.

In this graph, our goal is to find an isogeny from $\widetilde{A}$ to another ppav, which has good quartic reduction at p. The problem is not trivial, since the number of vertices in this graph is $O(\#\mathcal{C}_K)$, hence it grows exponentially with the size of the class group of K. If we construct an isogeny to a p.p.a.v. on the Galois orbit of $\widetilde{A}$ as in Theorem 2.3.1, then the target variety will also have hyperelliptic reduction at p.

Consequently, we will choose an isogeny $\widetilde{I}$ corresponding to a non-trivial element in $\mathcal{C}_K/\operatorname{im}(\mathcal{N})$ (preferably the one which allows an ideal representative of smallest possible norm). We denote by $\widetilde{B}$ the target ppav obtained in this way and by B its reduction $\pmod p$. Heuristically, both $\widetilde{B}$ and B are isomorphic to non-hyperelliptic Jacobians. To support this heuristic, we computed all primes of hyperelliptic reduction for all non-hyperelliptic orbits for a given CM field.

Example 5.2.1. As an example, we revisit the case of the CM field of equation $x^6 - 2x^5 + x^4 - 4x^3 + 5x^2 - 50x + 125$, which is the sixth entry in Table 2. Recall that for this field there is one hyperelliptic orbit of length 4 and three non-hyperelliptic orbits under conjugation by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. The Dixmier-Ohno invariants of plane quartics with CM by this field are defined over a degree 4 extension field of $\mathbb{Q}$ of equation $x^4 - 17x^3 - 24x^2 + 7$. We computed invariants for one curve on each of the non-hyperelliptic orbits (see [14] for the numerical values). With these in hand, we computed the primes of hyperelliptic reduction for these CM points, using the criterion in [33, Theorem 1.10]. We list the results in Table 3, where as before the subscripts denote the norms of the ideals. We can see that the lists of primes of hyperelliptic reduction for different orbits are almost disjoint (only $\mathfrak{p}_{29}$ appears in two of these lists).

References

[1] J. S. Balakrishnan, S. Ionica, K. Lauter, and C. Vincent. Constructing genus-3 hyperelliptic Jacobians with CM. *LMS J. Comput. Math.*, 19(suppl. A):283–300, 2016.

Orbit	Prime ideals of hyperelliptic reduction
1	$\mathfrak{p}_{29}, \mathfrak{p}_{151}, \mathfrak{p}_{331}, \mathfrak{p}_{15937}, \mathfrak{p}_{2986259}$
2	$\mathfrak{p}_{29}, \mathfrak{p}_{53}, \mathfrak{p}_{409}, \mathfrak{p}_{2251}, \mathfrak{p}_{27509}, \mathfrak{p}_{37423}, \mathfrak{p}_{154757110537}$
3	$\mathfrak{p}_{71}, \mathfrak{p}_{827}, \mathfrak{p}_{2207}, \mathfrak{p}_{3181}, \mathfrak{p}_{6133}$

TABLE 3. Hyperelliptic reduction for non-hyperelliptic curves with CM by the field with defining polynomial $x^6 - 2x^5 + x^4 - 4x^3 + 5x^2 - 50x + 125$

[2] J. Belding, R. Bröker, A. Enge, and K. Lauter. Computing Hilbert class polynomials. In *Algorithmic Number Theory- ANTS VIII*, number 5011 in Lecture Notes in Computer Science, pages 282–295. Springer, 2008.

[3] H. U. Besche, B. Eick, and E. O'Brien. The GAP Small Groups Library. Database available at https://www.gap-system.org/Packages/smallgrp.html, 2019.

[4] S. J. Bloch, editor. *Algebraic Geometry - Bowdoin 1985, Part 1. Proceedings of Symposia in Pure Mathematics*, volume 46. American Mathematical Society, 1987.

[5] 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).

[6] I. Bouw, J. Cooley, K. Lauter, E. Lorenzo García, M. Manes, R. Newton, and E. Ozman. Bad reduction of genus three curves with complex multiplication. In *Women in numbers Europe*, volume 2 of *Assoc. Women Math. Ser.*, pages 109–151. Springer, Cham, 2015.

[7] F. Bouyer and M. Streng. Examples of CM curves of genus two defined over the reflex field. *LMS J. Comput. Math.*, 18(1):507–538, 2015.

[8] R. Bröker, D. Gruenewald, and K. Lauter. Explicit CM theory for level 2-structures on abelian surfaces. *Algebra Number Theory*, 5(4):495–528, 2011.

[9] C.-L. Chai and F. Oort. Abelian varieties isogenous to a Jacobian. *Annals of Mathematics*, 176(1):589–635, 2012.

[10] E. Costa, N. Mascot, and J. Sijsling. Rigorous computation of the endomorphism ring of a Jacobian. https://github.com/edgarcosta/endomorphisms/, 2017.

[11] E. Costa, N. Mascot, J. Sijsling, and J. Voight. Rigorous computation of the endomorphism ring of a Jacobian. *Math. Comp.*, 88(317):1303–1339, 2019.

[12] C. Diem. An index calculus algorithm for plane curves of small degree. In F. Hess, S. Pauli, and M. E. Pohst, editors, *Algorithmic Number Theory, 7th International Symposium, ANTS-VII, Berlin, Germany, July 23-28, 2006, Proceedings*, volume 4076 of *Lecture Notes in Computer Science*, pages 543–557. Springer, 2006.

[13] B. Dina and S. Ionica. Genus 3 hyperelliptic curves with CM via Shimura reciprocity. In *Proceedings of the Fourteenth Algorithmic Number Theory Symposium*, volume 4 (1) of *Open Book Series*. Mathematical Sciences Publishers, 2020.

[14] B. Dina, S. Ionica, and J. Sijsling. `cm-calculations`, a Magma package for calculating with CM curves. https://github.com/JRSijsling/cm-calculations, 2021.

[15] B. Dodson. The structure of Galois groups of CM-fields. *Trans. Amer. Math. Soc.*, 283(1), May 1984.

[16] A.-S. Elsenhans. Good models for cubic surfaces. Preprint available at https://math.uni-paderborn.de/fileadmin/mathematik/AG-Computeralgebra/Preprints-elsenhans/red_5.pdf.

[17] A. Enge. The complexity of class polynomial computation via floating point approximations. *Math. Comp.*, 78(266):1089–1107, 2009.

[18] A. Enge and E. Thomé. Computing class polynomials for abelian surfaces. *Exp. Math.*, 23(2):129–145, 2014.

[19] P. Gaudry, E. Thomé, N. Thériault, and C. Diem. A double large prime variation for small genus hyperelliptic index calculus. *Math. Comput.*, 76(257):475–492, 2007.

[20] J.-i. Igusa. Modular forms and projective invariants. *Amer. J. Math.*, 89:817–855, 1967.

[21] S. Ionica, P. Kılıçer, K. Lauter, E. Lorenzo García, A. Mânzăţeanu, M. Massierer, and C. Vincent. Modular invariants for genus 3 hyperelliptic curves. *Res. Number Theory*, 5(1):Paper No. 9, 22, 2019.

[22] S. Ionica, P. Kılıçer, K. Lauter, E. Lorenzo García, A. Mânzăţeanu, and C. Vincent. Counting multiplicities for primes of bad reduction for genus 3 curves. Unpublished manuscript, 2021.

[23] D. Jetchev and B. Wesolowski. Horizontal isogeny graphs of ordinary abelian varieties and the discrete logarithm problem. *Acta Arithmetica*, 187(4):381–404, 2019.

[24] B. Klingler and A. Yafaev. The André-Oort conjecture. *Annals of Mathematics*, 180:867–925, 2014.

[25] K. Koike and A. Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518, 2005.

[26] P. Kılıçer. *The CM class number one problem for curves*. PhD thesis, Universiteit Leiden, 2016.

[27] P. Kılıçer, H. Labrande, R. Lercier, C. Ritzenthaler, J. Sijsling, and M. Streng. Plane quartics over $\mathbb{Q}$ with complex multiplication. *Acta Arith.*, 185(2):127–156, 2018.

[28] P. Kılıçer, K. Lauter, E. Lorenzo García, R. Newton, E. Ozman, and M. Streng. A bound on the primes of bad reduction for CM curves of genus 3. *Proc. Amer. Math. Soc.*, 148(7):2843–2861, 2020.
[29] P. Kılıçer, E. Lorenzo García, and M. Streng. Primes dividing invariants of CM Picard curves. *Canad. J. Math.*, 72(2):480–504, 2020.
[30] H. Labrande. Computing Jacobi's theta in quasi-linear time. *Math. Comp.*, 87(311):1479–1508, 2018.
[31] S. Lang. *Complex Multiplication*. Number 255 in Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin, 1983.
[32] J.-C. Lario, A. Somoza, and C. Vincent. An inverse Jacobian algorithm for Picard curves. Preprint available at arXiv:1611.02582, 2016.
[33] R. Lercier, Q. Liu, E. Lorenzo García, and C. Ritzenhaler. Reduction type of smooth plane quartics. *Algebra & Number Theory*, 2020.
[34] R. Lercier and C. Ritzenthaler. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.
[35] R. Lercier, C. Ritzenthaler, and J. Sijsling. Reconstructing plane quartics from their invariants. *Discrete Comput. Geom.*, 63(1):73–113, 2020.
[36] R. Lercier, C. Ritzenthaler, and J. Sijsling. `hyperelliptic`, a Magma package for reconstruction and isomorphisms of hyperelliptic curves. https://github.com/JRSijsling/hyperelliptic, 2021.
[37] R. Lercier, C. Ritzenthaler, and J. Sijsling. `quartic`, a Magma package for calculating with smooth plane quartic curves. https://github.com/JRSijsling/quartic, 2021.
[38] D. Lombardo, E. Lorenzo García, C. Ritzenthaler, and J. Sijsling. Decomposing jacobians via galois covers. Preprint available at arXiv:2003.07774, to appear in Exp. Math., 2020.
[39] B. Moonen and F. Oort. The Torelli locus and special subvarieties. In *Handbook of Moduli*, volume II, pages 549–594. International Press, 2013.
[40] J. Pila and J. Tsimerman. Ax-Lindemann for $\mathcal{A}_g$. *Annals of Mahematics*, 179:659–681, 2014.
[41] G. Shimura. *Abelian varieties with complex multiplication and modular functions*, volume 46 of *Princeton Mathematical Series*. Princeton University Press, Princeton, NJ, 1998.
[42] B. A. Smith. Isogenies and the discrete logarithm problem in jacobians of genus 3 hyperelliptic curves. In N. P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 163–180. Springer, 2008.
[43] M. Stoll. Reduction theory of point clusters in projective space. *Groups Geom. Dyn.*, 5(2):553–565, 2011.
[44] M. Stoll and J. E. Cremona. On the reduction theory of binary forms. *J. Reine Angew. Math.*, 565:79–99, 2003.
[45] M. Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010.
[46] M. Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014.
[47] The LMFDB Collaboration. The L-functions and modular forms database. http://www.lmfdb.org, 2019. [Online; accessed 30 October 2019].
[48] J. Tsimerman. The André-Oort conjecture for $\mathcal{A}_g$. *Annals of Mathematics*, 187:379–390, 2018.
[49] L. C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1997.
[50] A. Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001.
[51] A. Weng. Constructing hyperelliptic curves using complex multiplication. In *Number theory for the millennium, III (Urbana, IL, 2000)*, pages 385–396. A K Peters, Natick, MA, 2002.

Bogdan Dina, Institut für Algebra und Zahlentheorie, Universität Ulm, Helmholtzstrasse 18, D-89081 Ulm, Germany
Email address: `bogdan.dina@uni-ulm.de`

Sorina Ionica, Laboratoire MIS, Universite de Picardie, 33 Rue St-Leu, 80039 Amiens Cedex 1, France
Email address: `sorina.ionica@u-picardie.fr`

Jeroen Sijsling, Institut für Algebra und Zahlentheorie, Universität Ulm, Helmholtzstrasse 18, D-89081 Ulm, Germany
Email address: `jeroen.sijsling@uni-ulm.de`