The CM class number one problem for curves

Pinar Kiliçer

The CM class number one problem for curves

Proefschrift
ter verkrijging van
de graad van Doctor aan de Universiteit Leiden
op gezag van Rector Magnificus prof. mr. C.J.J.M. Stolker,
volgens besluit van het College voor Promoties
te verdedigen op 5 juli 2016
klokke 13 : 45 uur

door

Pınar Kılıçer
geboren te Kayseri, Turkije
in 1986

Samenstelling van de promotiecommissie:

Promotor: Prof. dr. Peter Stevenhagen

Promotor: Prof. dr. Andreas Enge (Université de Bordeaux)

Copromotor: Dr. Marco Streng

Overige leden:

Dr. Elisa Lorenzo García

Prof. dr. Aad van der Vaart

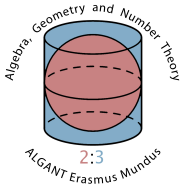
Prof. dr. Hendrik Lenstra

Prof. dr. Bart de Smit

Prof. dr. Jaap Top (Rijksuniversiteit Groningen)

Prof. dr. Florian Hess (Carl von Ossietzky Universität Oldenburg)

This work was funded by Algant-Doc Erasmus Action and was carried out at Universiteit Leiden and l'Université de Bordeaux.



THÈSE

présentée à

L'UNIVERSITÉ DE BORDEAUX

ÉCOLE DOCTORALE DE MATHÉMATIQUES ET INFORMATIQUE

par Pınar Kılıçer

POUR OBTENIR LE GRADE DE

DOCTEUR

SPECIALITÉ : Mathématiques Pures

The CM class number one problem for curves

Soutenue le : 5 juillet 2016 à Leiden

Devant la commission d'examen formée de :

ENGE, Andreas	Professeur	Université de Bordeaux	Directeur
STRENG, Marco	Docteur	Universiteit Leiden	Directeur
TOP, Jaap	Professeur	Rijksuniversiteit Groningen	Rapporteur
HESS, Florian	Professeur	Universität Oldenburg	Rapporteur

Contents

Preface

This thesis has four chapters and is organized as follows.

Chapter 1 is an introduction to abelian varieties and complex multiplication theory. It also contains facts from unramified class field theory. We present facts that we will use in later chapters, including the main theorem of complex multiplication. The results in this chapter are not new and most are due to Shimura and Taniyama [40].

Chapter 2 is a joint work with Marco Streng that appeared as *The CM class number one problem for curves of genus* 2 [18]. In Sections 2.3 and 2.4, we give a solution to the *CM class number one problem* for curves of genus 2 (Theorems 2.3.15 and 2.4.5).

Chapter 3 deals with the *CM class number one problem* for curves of genus 3 with a simple Jacobian. We give a partial solution to this problem. We restrict ourselves to the case where the sextic CM field corresponding to such a curve contains an imaginary quadratic subfield. We give the complete list of such sextic CM fields in Table 3.1 (unconditional) and Tables 3.3–3.12 (under GRH).

Chapter 4 gives the complete list of sextic CM fields K for which there exist principally polarized simple abelian threefolds with CM by $\mathcal{O}_K$ with rational field of moduli.

List of Notation

$\mathcal{O}_K$	the ring of integers (maximal order) of a number field K
I_K	the group of fractional ideals of a number field K
P_K	the group of principal fractional ideals of a number field K
Cl_K	the quotient I_K/P_K
h_K	the order of Cl_K
$F_{\gg 0}$	the group of totally positive elements of a totally real number field F
P_K^+	the group of principal ideals that are generated by the elements of $F_{\gg 0}$
W_K	the group of roots of unity of K
μ_K	the order of the group of roots of unity W_K
$\mathcal{O}_K^\times$	the unit group of $\mathcal{O}_K$
d_K	the discriminant of K
K/F	a number field extension of finite degree
$\mathrm{Gal}(K/F)$	the Galois group of K over F
$f_{K/F}$	the finite part of the conductor of K/F
$\mathfrak{D}_{K/F}$	the different of K over F, an ideal of $\mathcal{O}_K$
$N_{K/F}$	the ideal norm from K to F
$\mathrm{tr}_{K/F}$	the trace from K to F

t_K	the number of primes in F that are ramified in K
h_K^*	the relative class number h_K/h_F of K/F
$\mathrm{D}_{\mathfrak{p}}$	the decomposition group of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$
$\mathrm{I}_{\mathfrak{p}}$	the inertia group of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$
$\left(\frac{K/F}{\mathfrak{P}}\right)$	the Frobenius automorphism in $\mathrm{Gal}(K/F)$ corresponding to a prime ideal $\mathfrak{P} \subset \mathcal{O}_K$, page 2
Q_K	the Hasse unit index $[\mathcal{O}_K^\times : W_K \mathcal{O}_F^\times]$ of K/F, page 24
K_1K_2	the smallest field in $\overline{\mathbb{Q}}$ that contains the fields K_1 and K_2 (for K_1, $K_2 \subset \overline{\mathbb{Q}}$)
(K, Φ)	a CM pair, where K is a CM field and Φ is a CM type of K
(K^r, Φ^r)	the reflex of (K, Φ)
F^r	the maximal totally real subfield of K^r
N_Φ	the type norm map from K to K^r, page 5
$I_0(\Phi)$	an ideal group generated by the elements $\mathfrak{a}$ of I_K such that $\mathrm{N}_\Phi(\mathfrak{a}) = (\alpha) \in P_{F^r}$ and $\alpha\overline{\alpha} \in \mathbb{Q}$, page 17
A^*	the dual abelian variety of an abelian variety A
$\mathrm{End}(A)$	the ring of endomorphisms of A/k over $\overline{k}$
$\mathrm{End}_0(A)$	$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$
P	a polarized abelian variety of a CM type (K, Φ), page 17
M_J	the field of moduli of $P\|_J = (A, \theta\|_J, \mathcal{C})$, page 75
$\mathfrak{f}(P)$	an ideal in $\mathcal{O}_F$ determined by P, page 15

Chapter 1

Preliminaries

ABSTRACT. In this chapter, we give the main ingredients that we will use in the later chapters. This chapter contains facts from class field theory, complex multiplication theory and facts related to abelian varieties.

"All the truths of mathematics are linked to each other, and all means of discovering them are equally admissible."

Adrien-Marie Legendre

1.1 Global class field theory

In this section, we follow Neukirch [32].

Let K be a number field and $\mathcal{O}_K$ its ring of integers. We denote places by $\mathfrak{p}$. A *cycle* or *modulus* of K is a formal product

$$\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n(\mathfrak{p})},$$

where $\mathfrak{p}$ runs over all places of K with $n(\mathfrak{p}) \in \mathbb{Z}_{\geq 0}$ such that $n(\mathfrak{p}) = 0$ for almost all places of K. Here $n(\mathfrak{p})$ is 0 or 1 if $\mathfrak{p}$ is real, and 0 if $\mathfrak{p}$ is complex.

Frobenius automorphisms

Let L/K be a Galois extension of number fields and $\mathfrak{m}$ be a cycle of K divisible by all ramified primes of L/K. Given $\mathfrak{P} \nmid \mathfrak{m}$ lying above a finite prime $\mathfrak{p}$ of K, there exists a *unique* automorphism $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(L/K)$ satisfying

$$\sigma_{\mathfrak{P}}(x) \equiv x^q \bmod \mathfrak{P} \text{ for all } x \in \mathcal{O}_L,$$

where $\mathcal{O}_L$ is the ring of integers of L and $q = |\mathcal{O}_K/\mathfrak{p}|$. This automorphism is called the *Frobenius automorphism of* $\mathfrak{P}$ and is denoted by

$$\sigma_{\mathfrak{P}} = \left(\frac{L/K}{\mathfrak{P}}\right).$$

The Artin map for unramified abelian extensions

Let L/K be an unramified *abelian* extension of number fields. Let $\mathfrak{P}$ be a finite prime of L lying above a prime $\mathfrak{p}$ of K and let $\sigma_{\mathfrak{P}} = \left(\frac{L/K}{\mathfrak{P}}\right)$ be its *Frobenius automorphism*. For any element $\tau \in \mathrm{Gal}(L/K)$, we have

$$\left(\frac{L/K}{\tau(\mathfrak{P})}\right) = \tau \left(\frac{L/K}{\mathfrak{P}}\right) \tau^{-1} = \left(\frac{L/K}{\mathfrak{P}}\right).$$

Hence the Frobenius automorphisms $\sigma_{\tau\mathfrak{P}}$ of the primes $\tau\mathfrak{P}$ are the same, hence the Frobenius automorphisms in $\mathrm{Gal}(L/K)$ depends only on $\mathfrak{p} = \mathfrak{P} \cap K$, not on $\mathfrak{P}$ itself. For abelian extensions we use the notation $\left(\frac{L/K}{\mathfrak{p}}\right)$ for $\left(\frac{L/K}{\mathfrak{P}}\right)$ and call this the Frobenius automorphism of $\mathfrak{p}$.

Let I_K be the group of fractional ideals of $\mathcal{O}_K$, which is the free abelian group generated by the prime ideals of K.

Then for any $\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{v(\mathfrak{p})} \in I_K$ with $v(\mathfrak{p}) \in \mathbb{Z}$, we define

$$\left(\frac{L/K}{\mathfrak{a}}\right) = \prod_{\mathfrak{p}} \left(\frac{L/K}{\mathfrak{p}}\right)^{v(\mathfrak{p})}.$$

It is a theorem (Theorem VI.7.1 in Neukirch [32]) that the homomorphism

$$\begin{aligned} r_{K/L} : I_K &\to \mathrm{Gal}(L/K) \\ \mathfrak{a} &\mapsto \left(\frac{L/K}{\mathfrak{a}}\right) \end{aligned} \tag{1.1.1}$$

is surjective. This map is called the *Artin map* for the unramified abelian extension L/K.

Unramified class fields

A number field extension $K \subset L$ is *unramified* if it is unramified at all places of K (including the infinite places). When we say that an infinite place of L is unramified in L/K, we mean that it is not a complex place lying over a real place of K.

Let $P_K \subset I_K$ be the group of principal ideals of K. The *ideal class group* (or *class group*) Cl_K of K is the quotient group I_K/P_K.

Theorem 1.1.1. *(Proposition VI.6.9 [32]) Given a number field K, there is an unramified finite abelian extension H_K of K such that the* Artin map *(1.1.1) induces an isomorphism*

$$r_K : I_K/P_K \xrightarrow{\sim} \mathrm{Gal}(H_K/K). \qquad \square$$

The field H_K in Theorem 1.1.1 is called the *Hilbert class field* of K. It is the maximal abelian extension of K that is unramified at all places of K (see page 399 in Neukirch [32]).

1.2 CM fields and CM types

In this section, we mainly follow Lang [20] and Shimura–Taniyama [40].

Definition 1.2.1. A *CM field* is a totally imaginary quadratic extension K of a totally real number field F. In other words, a CM field is a field $K = F(\sqrt{-\delta})$ for a totally real number field F and a totally positive element $\delta \in F$.

Let $\bar{\cdot} : \mathbb{C} \to \mathbb{C}$ denote the complex conjugation automorphism of $\mathbb{C}$. For every CM field K there exists an automorphism ρ such that for every embedding $\tau : K \to \mathbb{C}$ we have $\bar{\cdot} \circ \tau = \tau \circ \rho$; we call it *complex conjugation* and denote it by ρ or $\bar{\cdot}$. Let ϕ be an embedding of a CM field K into any field N. Then we denote $\phi \circ \bar{\cdot}$ by $\overline{\phi}$. Note that if N is a CM field or $\mathbb{C}$

then we have $\bar{\cdot} \circ \phi = \overline{\phi}$ because the composite of ϕ with any embedding $N \to \mathbb{C}$ is an embedding $K \to \mathbb{C}$.

Let K be a CM field of degree $2g$ and N' be a number field that contains a subfield that is isomorphic over $\mathbb{Q}$ to a normal closure over $\mathbb{Q}$ of K.

Definition 1.2.2. Let K and N' be as above. A *CM type* of K with values in N' is a set Φ of embeddings $\phi : K \to N'$ such that exactly one embedding of each of the g complex conjugate pairs ϕ, $\overline{\phi} : K \to N'$ is in Φ. We say that (K, Φ) is a *CM pair* or *CM type*.

Let K_0 be a proper CM subfield of K. Let Φ_{K_0} be a CM type of K_0 with values in N'. Then the CM type of K *induced* by Φ_{K_0} is $\{\phi \in \mathrm{Hom}(K, N') : \ \phi|_{K_0} \in \Phi_{K_0}\}$.

We say that a CM type Φ of a CM field is *primitive* if it is not induced from a CM type of a proper CM subfield. The following proposition is a criterion for the primitiveness of a CM type.

If γ is an automorphism of K, then we define CM type $\Phi\gamma$ as the set of embeddings $\phi \circ \gamma$ for $\phi \in \Phi$, and if γ is an automorphism of N', then we define CM type $\gamma\Phi$ as the set of embeddings $\gamma \circ \phi$ for $\phi \in \Phi$.

Proposition 1.2.3. *(Shimura–Taniyama [40, Propostion 26]) Let K be a CM field and let N be a normal closure over $\mathbb{Q}$ of K. Then N is a CM field. Let N' be as above.*

Let Φ be a CM type of K with values in N' and let Φ_N be the CM type of N with values in N' induced from Φ. Then (K, Φ) is primitive if and only if

$$\mathrm{Gal}(N/K) = \{\gamma \in \mathrm{Gal}(N/\mathbb{Q}) : \Phi_N\gamma = \Phi_N\}. \qquad \square$$

Corollary 1.2.4. *With the notation in Proposition 1.2.3, suppose that K is normal over $\mathbb{Q}$. Then (K, Φ) is primitive if and only if there is no non-trivial element $\gamma \in \mathrm{Gal}(K/\mathbb{Q})$ satisfying $\Phi\gamma = \Phi$.* $\square$

We say that CM types Φ_1 and Φ_2 of K are *equivalent* if there is an automorphism σ of K such that $\Phi_1 = \Phi_2\sigma$ holds.

Let K be a CM field of degree $2g$ and N' be a number field that contains a subfield that is isomorphic over $\mathbb{Q}$ to a normal closure over $\mathbb{Q}$

of K. We make N' smaller and from now on we assume $N \cong N'$. Let Φ be a CM type of K with values in N' and let Φ_N be the CM type of N with values in N' induced from Φ. Here Φ_N is a set of isomorphisms $\phi : N \to N'$, so we can take the inverses $\phi^{-1} : N' \to N$. Let $\Phi_N^{-1} = \{\phi^{-1} : \phi \in \Phi_N\}$. Then the subfield K^r of N' corresponding to the subgroup $\{\gamma : \gamma \in \mathrm{Gal}(N'/\mathbb{Q}),\ \Phi_N^{-1}\gamma = \Phi_N^{-1}\}$ is a CM field with the *primitive* CM type $\Phi^r = \Phi_N^{-1}|_{K^r}$. Moreover, we have

$$K^r = \mathbb{Q}(\{\sum_{\phi\in\Phi} \phi(x) \mid x \in K\}) \subset N'.$$

For details, see Shimura–Taniyama [40, Proposition 28].

The field K^r is called the *reflex field* of (K, Φ) and Φ^r is called the *reflex type* of (K, Φ). The pair (K^r, Φ^r) is called the *reflex* of (K, Φ).

Lemma 1.2.5. *Let K be a CM field and let Φ be a CM type of K. Then the reflex field K^{rr} of (K^r, Φ^r) is a subfield of K with the primitive CM type Φ^{rr}. If Φ is primitive, then $K^{rr} = K$ and $\Phi^{rr} = \Phi$.*

Proof. This follows from the definition of the *reflex field* and Proposition 1.2.3. □

The *type norm* of a CM pair (K, Φ) is the multiplicative map

$$\begin{aligned} \mathrm{N}_\Phi : K &\to K^r, \\ x &\mapsto \prod_{\phi\in\Phi} \phi(x). \end{aligned}$$

Proposition 1.2.6. *(Shimura–Taniyama [40, Proposition 29]) Let K be a CM field and let Φ be a CM type of K with values in N'. Let $\mathfrak{a} \in I_K$ and $x \in K$. Then there is an ideal $\mathrm{N}_\Phi(\mathfrak{a})$ of K^r such that $\mathrm{N}_\Phi(\mathfrak{a})\mathcal{O}_{N'} = \prod_{\phi\in\Phi} \phi(\mathfrak{a})\mathcal{O}_{N'}$ and we have*

$$\begin{aligned} \mathrm{N}_\Phi(\mathfrak{a})\overline{\mathrm{N}_\Phi(\mathfrak{a})} &= \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_{K^r}, \\ \mathrm{N}_\Phi(x)\overline{\mathrm{N}_\Phi(x)} &= \mathrm{N}_{K/\mathbb{Q}}(x) \in \mathbb{Q}. \end{aligned}$$ □

1.3 Abelian varieties

In this chapter, we refer to Lang [20] and Shimura–Taniyama [40].

Let k be a field. In this thesis, we will use the following definitions. By a *variety* over k, we mean a geometrically integral, separated scheme of finite type over $\mathrm{Spec}(k)$. Curves, respectively surfaces, respectively threefolds are varieties are of dimension 1, respectively 2, respectively 3. We will always assume that curves, surfaces and threefolds are projective, smooth over k.

By an *abelian variety* over k, we mean a complete irreducible group variety over k. It is known that abelian varieties are smooth, projective, and commutative. Let A and B be abelian varieties over k. A *morphism* λ of A to B is a morphism of varieties that respects the group structure. If A and B are of the same dimension and λ is surjective, then it is called an *isogeny*. If an isogeny $\lambda : A \to B$ exists, then A and B are called *isogenous*. A non-zero abelian variety is said to be *simple* if it is not isogenous to a product of abelian varieties of lower dimensions.

We denote by $\mathrm{End}(A)$ the ring of homomorphisms of A to itself over $\overline{k}$ and we put $\mathrm{End}_0(A) = \mathrm{End}(A) \otimes \mathbb{Q}$.

1.3.1 Polarizations and the dual variety

This section basically follows Lang [20, 3.4].

By a divisor on a variety, we always mean a *Cartier* divisor. We say that two divisors X_1 and X_2 on an abelian variety A over a field k are *algebraically equivalent* ($X_1 \sim X_2$) if there is a connected algebraic set T, two points $t_1,\ t_2 \in T$ and a divisor Z on $A \times T$ such that $Z|_{t_i} = X_i$ for $i = 1,\ 2$. The divisors X_1 and X_2 are *linearly equivalent* if there is a rational function $f \in k(A)^\times$ such that $X_1 = X_2 + (f)$. For details, see Hartshorne [15].

Let $\mathcal{D}_a(A)$ and $\mathcal{D}_l(A)$ respectively be the group of divisors on A over $\overline{k}$ that are algebraically equivalent to 0 and the group of divisors on A over $\overline{k}$ that are linearly equivalent to 0. There exists an abelian variety A^*, that is called the *dual variety* of A, whose group of $\overline{k}$-points is canonically isomorphic to $\mathrm{Pic}^0(A) := \mathcal{D}_a(A)/\mathcal{D}_l(A)$. Let X be an ample divisor over $\overline{k}$ on an abelian variety A and let $[X]$ denote the linear equivalence class

of X. Let X_a be the translation of X by an element $a \in A$. Then the map

$$\begin{aligned} \varphi_X : A &\to \mathrm{Pic}^0(A) \\ a &\mapsto [X_a - X], \end{aligned} \tag{1.3.1}$$

induces an isogeny $\varphi_X : A \to A^*$.

Proposition 1.3.1. *(Serre [37]) Two divisors X_1 and X_2 are algebraically equivalent if and only if $\varphi_{X_1} = \varphi_{X_2}$.* □

Definition 1.3.2. An isogeny $\varphi : A \to A^*$ induced by (1.3.1) is called a *polarization* of A. It is said to be a *principal polarization* if φ is an isomorphism.

We understand by a *polarized abelian variety* a pair (A, φ) formed by an abelian variety A and a polarization φ of A. We say that a polarized abelian variety (A, φ) is defined over a field k if A and φ are defined over k.

Every polarization φ on A induces an involution as follows. Each endomorphism $\lambda \in \mathrm{End}_0(A)$ has a dual

$$\lambda^* : A^* \to A^* : \quad [Y] \mapsto [\lambda^{-1}(Y)] \tag{1.3.2}$$

and for every $\lambda \in \mathrm{End}_0(A)$, we define

$$\lambda' = \varphi^{-1} \lambda^* \varphi \in \mathrm{End}_0(A).$$

The map sending λ to λ' is an involution of A and called the *Rosati involution determined by* φ.

Let (A_1, φ_1) and (A_2, φ_2) be two polarized abelian varieties of the same dimension. A homomorphism λ of A_1 to A_2 is called a *homomorphism* of (A_1, φ_1) to (A_2, φ_2) if the following diagram

$$\begin{array}{ccc} A_1 & \xrightarrow{\lambda} & A_2 \\ {\scriptstyle \varphi_1}\downarrow & & \downarrow{\scriptstyle \varphi_2} \\ A_1^* & \longrightarrow & A_2^* \end{array}$$

commutes.

Proposition 1.3.3. *(Shimura–Taniyama [40, Theorem 2 and Proposition 14]) Let (A, φ) be a polarized abelian variety over a characteristic 0 field k. Then there exists a field $k_0 \subset k$ with the following property: For all $\sigma : k \to \overline{k}$, it holds that (A, φ) and $(\sigma A, \sigma\varphi)$ are isomorphic over $\overline{k}$ if and only if σ is the identity map on k_0.* □

Definition 1.3.4. The field k_0 in Proposition 1.3.3 is called the *the field of moduli* of (A, φ).

Jacobian of curves

The *Jacobian* $J(C)$ of a curve C/k of genus g is a certain *principally polarized* abelian variety of dimension g such that we have $J(C)(\overline{k}) = \mathrm{Pic}^0(C_{\overline{k}})$; for details we refer to [29].

Theorem 1.3.5. *(Torelli) Two algebraic curves over $\mathbb{C}$ are isomorphic if and only if their Jacobians are isomorphic as polarized abelian varieties.*

Proof. This is Theorem 11.1.7 of Birkenhake–Lange [6]. □

Theorem 1.3.6.

(i) (Weil) Every principally polarized abelian surface over $\mathbb{C}$ is either a product of elliptic curves with the product polarization or the Jacobian of a smooth projective curve of genus 2.

(ii) (Matsusaka–Ran) Every principally polarized abelian threefold over $\mathbb{C}$ is either the Jacobian of a smooth curve of genus 3 or a principally polarized product of a principally polarized abelian surface with an elliptic curve or of three elliptic curves.

Proof. The assertion (i) is Satz 2 of Weil [47]. The assertions (i) and (ii) are consequences of the Matsusaka–Ran criterion in [28, 35], also see Corollary 11.8.2 in Birkenhake–Lange [6]. □

1.3.2 Complex abelian varieties

A *lattice* in $\mathbb{C}^g$ is a discrete subgroup of maximal rank in $\mathbb{C}^g$. It is a free abelian group of rank $2g$. The quotient $\mathbb{C}^g/\Lambda$ is called a *complex torus*. A *Riemann form* on $\mathbb{C}^g$ is a skew symmetric $\mathbb{R}$-bilinear map E such that the form $\mathbb{C}^g \times \mathbb{C}^g \to \mathbb{C} : (x, y) \mapsto E(x, iy)$ is positive definite symmetric.

If A is a g-dimensional abelian variety over $\mathbb{C}$, then there is a complex torus $\mathbb{C}^g/\Lambda$ that is isomorphic (as a complex Lie group) to A via an analytic isomorphism $\iota : \mathbb{C}^g/\Lambda \to A$. Following Lang [20, 3.4] we describe the notion of *polarization* in the complex analytic setting as follows. Let X be an *ample* divisor on an abelian variety A over $\mathbb{C}$ and let φ_X be a polarization on A. Then $\iota^{-1}(X)$ is an analytic divisor of $\mathbb{C}^g/\Lambda$, and its pull back to $\mathbb{C}^g$ is defined by a *theta function* f_X. There is a Riemann form E_X associated to f_X . It is obtained from the functional equation of f_X, see Lang [20, page 68]. We say that E_X is associated to X via ι. Two divisors are algebraically equivalent if and only if the associated Riemann forms are the same.

Let X be an ample divisor on an abelian variety A and E be the Riemann form associated to X via $\iota : \mathbb{C}^g/\Lambda \to A$. We can consider $\mathbb{C}^g$ as the dual vector space of itself over $\mathbb{R}$ with respect to the Riemann form E that is, we identify $y \in \mathbb{C}^g$ with $E(\cdot, y)$. Let us denote by Λ^* the set of all vectors of $x \in \mathbb{C}^g$ such that $E(x, y) \in \mathbb{Z}$ for every $y \in \Lambda$. Then Λ^* is a discrete group in $\mathbb{C}^g$ and $\mathbb{C}^g/\Lambda^*$ is a complex torus, which we call the *dual* of the complex torus $\mathbb{C}^g/\Lambda$. Then there is an analytic isomorphism $\iota^* : \mathbb{C}^g/\Lambda^* \to A^*$ making the following diagram commutative

$$\begin{array}{ccc} \mathbb{C}^g/\Lambda & \xrightarrow{\ \iota\ } & A \\ {\scriptstyle \lambda : x \mapsto x}\downarrow & & \downarrow{\scriptstyle \varphi_X} \\ \mathbb{C}^g/\Lambda^* & \xrightarrow{\ \iota^*\ } & A^* \end{array} .$$

1.4 Abelian varieties with complex multiplication

This section is a summary of Birkenhake–Lange [6, 13.3] and Lang [20, 1.4].

We say that an abelian variety A over a field k of dimension g has *complex multiplication* (CM) by a CM field K if K has degree $2g$ and there is an embedding $\theta : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$. We say that A has CM by an order $\mathcal{O} \subset K$ if there is an embedding $\theta : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$ such that $\theta^{-1}(\mathrm{End}(A)) = \mathcal{O}$.

The *tangent space* $\mathrm{Tgt}_0(A)$ of A at the unit point 0 of A is a vector space over k of dimension g.

Let A be an abelian variety over $\mathbb{C}$ with CM by K via the embedding $\theta : K \hookrightarrow \mathrm{End}(A) \otimes \mathbb{Q}$. Then there exists a unique set Φ of embeddings $K \to \mathbb{C}$ such that the representation of K on $\mathrm{End}_{\mathbb{C}}(\mathrm{Tgt}_0(A))$ via θ is equivalent to $\oplus_{\phi \in \Phi} \phi$, see Shimura–Taniyama [40, §5.2]. We call Φ the *CM type* of K. The CM type Φ is uniquely determined by (A, θ). We say that (A, θ) is an *abelian variety of type* (K, Φ). Furthermore, if $\theta(\mathcal{O}_K) \subset \mathrm{End}(A)$ holds, then we say that (A, θ) is an *abelian variety of type* (K, Φ) *with CM by* $\mathcal{O}_K$.

We say that (A, θ) is defined over a field k if A is defined over k and every element of $\theta(\mathcal{O}_K) \subset \mathrm{End}(A)$ is defined over k.

Theorem 1.4.1 (Shimura, §8.2)**.** *Let K be a CM field and let Φ be a CM type of K. An abelian variety (A, θ) of type (K, Φ) is simple if and only if Φ is primitive.* □

1.4.1 Construction of abelian varieties with CM

By a *lattice* in an algebraic number field K of finite degree over $\mathbb{Q}$, we mean a finitely generated $\mathbb{Z}$-submodule of K that spans K over $\mathbb{Q}$.

Let K be a CM field of degree $2g$. To every CM type Φ of K and $\mathbb{Z}$-lattice $\mathfrak{m}$ of K, we associate an abelian variety $A_{\Phi,\mathfrak{m}}$ as follows. The tensor product $K \otimes_{\mathbb{Q}} \mathbb{R}$ is an $\mathbb{R}$-vector space of dimension $2g$. The CM type $\Phi = \{\phi_1, \ldots, \phi_g\}$ induces a $\mathbb{C}$-algebra structure on $K \otimes_{\mathbb{Q}} \mathbb{R}$ via the $\mathbb{R}$-algebra isomorphism

$$\begin{aligned}\tilde{\Phi} : K \otimes_{\mathbb{Q}} \mathbb{R} &\to \mathbb{C}^g \\ \alpha \otimes a &\mapsto {}^t(a\phi_1(\alpha), \ldots, a\phi_g(\alpha)).\end{aligned}$$

By $\tilde{\Phi}(\mathfrak{m})$, we mean the group of all elements $\tilde{\Phi}(\alpha)$ with $\alpha \in \mathfrak{m}$. Then $\tilde{\Phi}(\mathfrak{m})$ is a lattice in $\mathbb{C}^g$ and $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m})$ is a *complex torus*. Hence the quotient $A_{\Phi,\mathfrak{m}} := (K \otimes_{\mathbb{Q}} \mathbb{R})/\mathfrak{m}$ is isomorphic to the complex torus $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m})$.

Proposition 1.4.2. *(Birkenhake–Lange [6, Proposition 13.3.1] and Lang [20, Theorem 1.4.1-(iii)]) With the notation above, the complex torus $A_{\Phi,\mathfrak{m}}$ is an abelian variety and has a natural CM structure given by the action of $\mathcal{O}_K$ on $\mathfrak{m}$.* □

In this thesis, we use the complex torus $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m})$ instead of $A_{\Phi,\mathfrak{m}}$ as a realization of an abelian variety over $\mathbb{C}$ conforming to the notation of Lang [20] and Shimura–Taniyama [40].

For each $\alpha \in K$, we let $\mathrm{S}_\Phi(\alpha)$ be the matrix $\mathrm{diag}(\phi_1(\alpha), \ldots, \phi_g(\alpha))$.

Theorem 1.4.3. *(Lang [20, Theorem 1.4.1-(ii)]) Let (K,Φ) be a CM pair and let (A,θ) be an abelian variety of type (K,Φ) with CM by $\mathcal{O}_K$. Then there is a fractional ideal $\mathfrak{m} \in I_K$ and an analytic isomorphism $\iota : \mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}) \to A(\mathbb{C})$ such that the diagram*

$$\begin{array}{ccc} \mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}) & \longrightarrow & A(\mathbb{C}) \\ {\scriptstyle S_\Phi(\alpha)}\downarrow & & \downarrow{\scriptstyle \theta(\alpha)} \\ \mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}) & \longrightarrow & A(\mathbb{C}) \end{array}$$

commutes for all $\alpha \in \mathcal{O}_K$. □

Definition 1.4.4. We say that an *abelian variety* (A,θ) *of type* (K,Φ) *is of type* $(K,\Phi,\mathfrak{m})$ if there is a fractional ideal $\mathfrak{m} \in I_K$ and an analytic isomorphism $\iota : \mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}) \to A(\mathbb{C})$.

Definition 1.4.5. Let (A,θ) be an abelian variety of type (K,Φ) and let X be an ample divisor on A. We say that (A,θ) is Φ-*admissible* with respect to the polarization φ_X if $\theta(K)$ is stable under the *Rosati* involution.

Theorem 1.4.6. *(Lang [20, Theorem 1.4.5-(iii)] If an abelian variety* (A,θ) *of type* $(K,\Phi,\mathfrak{m})$ *is* simple*, then it is* Φ-admissible *with respect to every polarization.* □

Definition 1.4.7. Let (A_1,θ_1) and (A_2,θ_2) be abelian varieties of type (K,Φ) with CM by $\mathcal{O}_K$. A *homomorphism* λ from A_1 to A_2 is called a homomorphism from (A_1,θ_1) to (A_2,θ_2) if it satisfies

$$\lambda\theta_1(\alpha) = \theta_2(\alpha)\lambda$$

for every $\alpha \in \mathcal{O}_K$.

Proposition 1.4.8. *(Shimura–Taniyama [40, Proposition 1 in §14]) Let* (K,Φ) *be a primitive CM type. Let* (A_1,θ_1) *and* (A_2,θ_2) *be abelian varieties over* $k \subset \mathbb{C}$ *of type* (K,Φ)*. Then every homomorphism from* A_1 *into* A_2 *over* k *is a homomorphism from* (A_1,θ_1) *to* (A_2,θ_2) *over* k*.* □

Let (A,θ) be a g-dimensional abelian variety of CM type (K,Φ). Let $\mathfrak{a}$ be a $\mathbb{Z}$-lattice in K. Let $(\alpha_1,\dots,\alpha_{2g})$ be a basis of $\mathfrak{a}$ over $\mathbb{Z}$. We obtain a homomorphism

$$\lambda_{\mathfrak{a}} : A \to A^{2g}$$

such that $x \mapsto (\alpha_1 x,\dots,\alpha_{2g}x)$ for all $x \in A$. If $\mathfrak{a} \neq 0$, then $\lambda_{\mathfrak{a}}$ is an isogeny to its image $\lambda_{\mathfrak{a}}(A)$ (see page 56 in Lang [20]).

A homomorphism λ of (A_1,θ_1) onto (A_2,θ_2) is called an $\mathfrak{a}$-*multiplication* if there is a commutative diagram

$$\begin{array}{ccc} (A_1,\theta_1) & \xrightarrow{\quad\lambda_{\mathfrak{a}}\quad} & (\lambda_{\mathfrak{a}}(A_1),\lambda_{\mathfrak{a}}\theta_1) \\ & {\scriptstyle\lambda}\searrow \quad \swarrow{\scriptstyle\cong} & \\ & (A_2,\theta_2) & \end{array}$$

of homomorphisms as in Definition 1.4.7.

An $\mathfrak{a}$-multiplication is uniquely determined up to an isomorphism, for the details, see Lang [20, 3.2] and Shimura–Taniyama [40, 7.1].

Let (A_1,θ_1) and (A_2,θ_2) be g-dimensional abelian varieties over $\mathbb{C}$ of a primitive CM type (K,Φ), analytically represented by $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_1)$ and

$\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_2)$ respectively. If a non-zero $\gamma \in K$ is such that $\gamma\mathfrak{m}_1 \subset \mathfrak{m}_2$, then there exists a homomorphism $\gamma_{\theta_1,\theta_2}$ such that the following diagram

$$\begin{array}{ccc} \mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_1) & \longrightarrow & A_1 \\ {\scriptstyle \mathrm{S}_\Phi(\gamma)}\downarrow & & \downarrow{\scriptstyle \gamma_{\theta_1,\theta_2}} \\ \mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_2) & \longrightarrow & A_2 \end{array}$$

is commutative with $S_\Phi(\gamma)$ as on page 11. Observe that $\gamma_{\theta_1,\theta_2}$ gives an isogeny of (A_1,θ_1) onto (A_2,θ_2).

Proposition 1.4.9. *(Lang [20, Proposition 3.2.6], Shimura–Taniyama [40, Proposition 15 in 7.4]) Let K be a CM field and let Φ be a primitive CM type of K. Let (A_1,θ_1) and (A_2,θ_2) be abelian varieties over $\mathbb{C}$ of types $(K,\Phi,\mathfrak{m}_1)$ and $(K,\Phi,\mathfrak{m}_2)$ respectively (see Definition 1.4.4). If $\gamma \neq 0$ is an element of $\mathfrak{m}_1^{-1}\mathfrak{m}_2$, then $\gamma_{\theta_1,\theta_2}$ is a $\gamma\mathfrak{m}_2^{-1}\mathfrak{m}_1$-multiplication of (A_1,θ_1) onto (A_2,θ_2). Every isogeny of (A_1,θ_1) onto (A_2,θ_2) is equal to $\gamma_{\theta_1,\theta_2}$ for some such γ.* □

Corollary 1.4.10. *Any two abelian varieties of the same primitive CM type (K,Φ) are isogenous to each other.* □

Proposition 1.4.11. *Let (K,Φ) be a primitive CM pair and let (A_1,θ_1) and (A_2,θ_2) be g-dimensional abelian varieties over $\mathbb{C}$ of types $(K,\Phi,\mathfrak{m}_1)$ and $(K,\Phi,\mathfrak{m}_2)$ respectively (see Definition 1.4.4). Let $[\mathfrak{m}_i]$ denote the class of $\mathfrak{m}_i$ in the class group Cl_K. Then (A_1,θ_1) and (A_2,θ_2) are isomorphic if and only if $[\mathfrak{m}_1] = [\mathfrak{m}_2]$.*

Proof. Suppose that λ is an isomorphism of (A_1,θ_1) onto (A_2,θ_2). By Proposition 1.4.9 there is a non-zero $\gamma \in \mathfrak{m}_1^{-1}\mathfrak{m}_2$ such that $S(\gamma)$ gives an isomorphism between $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_1)$ and $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_2)$. Therefore we get $S(\gamma)\tilde{\Phi}(\mathfrak{m}_1) = \tilde{\Phi}(\mathfrak{m}_2)$ and hence $\gamma\mathfrak{m}_1 = \mathfrak{m}_2$, so we have $[\mathfrak{m}_1] = [\mathfrak{m}_2]$.

Conversely, if $[\mathfrak{m}_1] = [\mathfrak{m}_2]$ then there is a non-zero $\alpha \in \mathcal{O}_K$ such that $\alpha\mathfrak{m}_1 = \mathfrak{m}_2$. Therefore, the map $S(\alpha)$ gives an isomorphism between $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_1)$ and $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_2)$. Hence by Proposition 1.4.8, the map $S(\alpha)$ induces an isomorphism between (A_1,θ_1) and (A_2,θ_2). □

Proposition 1.4.12. *(Shimura–Taniyama [40, Proposition 30 in 8.5]) Let A be a simple abelian variety over a field $k \subset \mathbb{C}$ with CM by K via $\theta : K \hookrightarrow \mathrm{End}_0(A)$ of CM type Φ. Then θ is over k if and only if the reflex field K^r of (K, Φ) is contained in k.* □

Proposition 1.4.13. *(Shimura [39, (5.5.17) and Proposition 5.14]) Let (K, Φ) be a primitive CM pair and let (A, θ) be an abelian variety over $\mathbb{C}$ and of type (K, Φ). If an automorphism σ of $\mathbb{C}$ is the identity map on the reflex field K^r, then $(\sigma A, \sigma\theta)$ is of type (K, Φ).* □

1.5 Polarized simple abelian varieties with complex multiplication

Let K be a CM field and let Φ be a primitive CM type of K. Let (A, θ) be an abelian variety of type $(K, \Phi, \mathfrak{m})$ with CM by $\mathcal{O}_K$. Let X be an ample divisor on A and $E(u, w)$ be the Riemann form on $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m})$ associated to X. Then there is an element $t \in K^\times$ (see Shimura–Taniyama [40, Theorem 4 in §6.2] and use Theorem 1.4.6) such that

$$E(\tilde{\Phi}(x), \tilde{\Phi}(y)) = \mathrm{tr}_{K/\mathbb{Q}}(tx\overline{y}) \tag{1.5.1}$$

for every $(x, y) \in K \times K$, and the element t satisfies

$$\overline{t} = -t, \ \mathrm{Im}(\phi(t)) > 0 \quad \text{for all } \phi \in \Phi. \tag{1.5.2}$$

Since we obtained t from an ample divisor, by (1.3) in Shimura [38], we have

$$\mathrm{tr}_{K/\mathbb{Q}}(t\mathfrak{m}\overline{\mathfrak{m}}) = \mathbb{Z}. \tag{1.5.3}$$

Let φ be the polarization corresponding to X. Then we say that the polarized abelian variety $P := (A, \theta, \varphi)$ is *of type* $(K, \Phi, t, \mathfrak{m})$.

Let A^* be the dual variety of A (recall the definition of A^* from Section 1.3.1). For every $\alpha \in K$, put

$$\theta^*(\alpha) = \theta(\overline{\alpha})^*,$$

where $\theta(\alpha)^*$ is the transpose homomorphism of $\theta(\alpha)$. In [40, 3.3 & 6.3], Shimura shows that θ^* is an isomorphism of K into $\mathrm{End}_0(A^*)$ and (A^*, θ^*)

is of type (K,Φ), and (A^*,θ^*) is analytically represented by the complex torus $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}^*)$, where

$$\mathfrak{m}^* = \{\beta \in K \mid \mathrm{tr}_{K/\mathbb{Q}}(\beta\overline{\mathfrak{m}}) \subset \mathbb{Z}\}. \tag{1.5.4}$$

Proposition 1.5.1. *Let (A_1,θ_1) and (A_2,θ_2) be abelian varieties of primitive CM type (K,Φ). If an isogeny λ from (A_1,θ_1) onto (A_2,θ_2) is an $\mathfrak{a}$-multiplication, then λ^* from (A_1^*,θ_1^*) onto (A_2^*,θ_2^*) is an $\overline{\mathfrak{a}}$-multiplication.*

Proof. It is Proposition 6 in Shimura–Taniyama [40, 14.4]. □

Let $\mathfrak{D}_{K/\mathbb{Q}}$ be the *different* (the inverse of the dual of $\mathcal{O}_K$ relative to the trace form on $K/\mathbb{Q}$) of K.

Proposition 1.5.2. *Let $P=(A,\theta,\varphi)$ be a polarized abelian variety of type $(K,\Phi,t,\mathfrak{m})$. Then the isogeny $\varphi: A \to A^*$ is a $t\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$-multiplication.*

Moreover, if P is principally polarized, then $t\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}} = \mathcal{O}_K$.

Proof. By the definition of $\mathfrak{m}^*$ (1.5.4), we have

$$\mathfrak{m}^* = (\mathfrak{D}_{K/\mathbb{Q}}\overline{\mathfrak{m}})^{-1}.$$

Then by (1.3.1), the isogeny $\varphi: A \to A^*$ is represented by the matrix $\mathrm{S}_\Phi(t)$. Hence by Proposition 1.4.9, the polarization φ is a $t\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$-multiplication from (A,θ) onto (A^*,θ^*) (also see Shimura–Taniyama [40, 14.3]).

Moreover, the kernel of $S_\Phi(t)$ is $\tilde{\Phi}(t^{-1}\mathfrak{m}^*)/\tilde{\Phi}(\mathfrak{m})$, which is isomorphic to $t^{-1}\mathfrak{m}^*/\mathfrak{m}$. Hence we have $\ker(\varphi) = (t\mathfrak{D}_{K/\mathbb{Q}}\overline{\mathfrak{m}})^{-1}/\mathfrak{m}$. This implies that if P is *principally* polarized, that is $\ker(\varphi)=1$, then we have $t\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}} = \mathcal{O}_K$. □

Put $\mathfrak{f} := t\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$. We now show that there is an $\mathcal{O}_F$-ideal $\mathfrak{f}_0$ such that $\mathfrak{f} = \mathfrak{f}_0\mathcal{O}_K$. By definition, we have $\mathfrak{D}_{K/\mathbb{Q}} = \mathfrak{D}_{K/F}\mathfrak{D}_{F/\mathbb{Q}}$ and moreover the ideal $\mathfrak{D}_{K/F}$ is generated by the elements $(\alpha-\overline{\alpha})$ for $\alpha \in \mathcal{O}_K$. Since $\overline{t} = -t$, we have $t(\alpha-\overline{\alpha}) \in F$ for every $\alpha \in \mathcal{O}_K$. Hence there is an $\mathcal{O}_F$-ideal $\mathfrak{f}_1$ such that $t\mathfrak{D}_{K/F} = \mathfrak{f}_1\mathcal{O}_K$. On the other hand, the ideal $\mathfrak{D}_{F/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$ is an $\mathcal{O}_F$-ideal. So if we put $\mathfrak{f}_0 = \mathfrak{f}_1\mathfrak{D}_{F/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$, then we get $\mathfrak{f} = \mathfrak{f}_0\mathcal{O}_F$.

Remark that by definition, the ideal $\mathfrak{f}$ is determined by $P=(A,\theta,\varphi)$. Set $\mathfrak{f}(P) := \mathfrak{f}$. We say that P is *of type* $(K,\Phi,\mathfrak{f}(P))$.

Proposition 1.5.3. *(Shimura–Taniyama [40, Proposition 2 in 14.2]) Let (A,θ) be an abelian variety over $\mathbb{C}$ of type $(K,\Phi,\mathfrak{m})$. Let F be the maximal totally real subfield of K. Let X_1 and X_2 be two ample divisors on A, and let E_1, E_2 be the Riemann forms on $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m})$ associated to X_1, X_2 respectively. Let t_i be the element of $K^\times$ satisfying* (1.5.2) *for the form E_i. Then $t_1^{-1}t_2$ is a totally positive element in F and we have*

$$\varphi_{X_1}^{-1}\varphi_{X_2} = \theta(t_1^{-1}t_2) \in \mathrm{End}(A)\otimes\mathbb{Q}. \qquad \square$$

Proposition 1.5.4. *(Shimura–Taniyama [40, Proposition 3 in 14.2]) Let the notation be as in Proposition 1.5.3. The polarized abelian varieties (A,φ_{X_1}) and (A,φ_{X_2}) are isomorphic if and only if there exist $\epsilon \in \mathcal{O}_K^\times$ such that $t_1^{-1}t_2 = \epsilon\bar{\epsilon}$.* $\square$

1.5.1 Classes of polarized simple abelian varieties with CM

For a given *polarized simple abelian variety* $P=(A,\theta,\varphi)$ over $\mathbb{C}$ of primitive CM type (K,Φ) we can find a $\mathbb{Z}$-lattice $\mathfrak{m}$ in K such that A is isomorphic to $\mathbb{C}^g/\tilde{\Phi}(\mathfrak{m})$. There exists $t\in K^\times$ satisfying (1.5.1) and (1.5.2) such that $P=(A,\theta,\varphi)$ is *of type* $(K,\Phi,t,\mathfrak{m})$. We say that P is *of type* $(t,\mathfrak{m})$ if (K,Φ) is fixed. Put $\mathfrak{f}(P) := t\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$. We call $(t,\mathfrak{m})$ and $(t',\mathfrak{m}')$ equivalent if the following holds

$$t = b\bar{b}t' \text{ and } \mathfrak{m}b = \mathfrak{m}' \text{ with } b\in K^\times.$$

For given $(t,\mathfrak{m})$ satisfying (1.5.2) and (1.5.3), there is a polarized simple abelian variety $P=(A,\theta,\varphi)$ of type $(K,\Phi,t,\mathfrak{m})$, which is unique up to isomorphism (see page 67 in Shimura [38]).

We denote the group of totally positive elements in F by $F_{\gg 0}$. Set

$$\mathfrak{C}_K := (F_{\gg 0}\times I_K)/\{(x\overline{x}, x\mathcal{O}_K) : x\in K^\times\}.$$

We define the multiplication of two classes $[(\xi_1,\mathfrak{c}_1)]$ and $[(\xi_2,\mathfrak{c}_2)]$ in $\mathfrak{C}_K$ by

$$[(\xi_1,\mathfrak{c}_1)][(\xi_2,\mathfrak{c}_2)] = [(\xi_1\xi_2,\mathfrak{c}_1\mathfrak{c}_2)].$$

This set becomes a group with the identity element $[(1, \mathcal{O}_K)]$. It is clear that the group $\mathfrak{C}_K$ is abelian.

Let $P_i = (A_i, \theta_i, \varphi_i)$ be of type $(K, \Phi, t_i, \mathfrak{m}_i)$ for $i \in \{1,\ 2\}$. By (1.5.2), we have $t_1^{-1}t_2 \in F_{\gg 0}$, hence we get an element $[(t_1^{-1}t_2, \mathfrak{m}_1\mathfrak{m}_2^{-1})]$ in $\mathfrak{C}_K$. We define

$$(P_2 : P_1) := [(t_1^{-1}t_2, \mathfrak{m}_1\mathfrak{m}_2^{-1})] = [(\xi, \mathfrak{c})] \in \mathfrak{C}_K. \tag{1.5.5}$$

Then by the definition of $\mathfrak{f}(P_i)$, we have

$$\mathfrak{f}(P_1)\mathfrak{f}(P_2)^{-1} = \xi^{-1}\mathrm{N}_{K/F}(\mathfrak{c}). \tag{1.5.6}$$

Proposition 1.5.5. *(Shimura–Taniyama [40, Proposition 10 in 14.7])* *We have $(P_2 : P_1) = [(1, \mathcal{O}_K)]$ if and only if P_2 is isomorphic to P_1.* □

1.5.2 The first main theorem of CM

Theorem 1.5.6 (The first main theorem of complex multiplication, [40, Main Theorem 1])**.** *Let (K, Φ) be a primitive CM type with $[K : \mathbb{Q}] = 2g$ and let (K^r, Φ^r) be its reflex. Let $P = (A, \theta, \varphi)$ be a polarized simple abelian variety of type (K, Φ) with CM by $\mathcal{O}_K$. Let M be the field of moduli of (A, φ). Then $K^r \cdot M$ is the unramified class field over K^r corresponding to the ideal group*

$$I_0(\Phi^r) := \{\mathfrak{b} \in I_{K^r} :\ \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\alpha),\ \alpha\overline{\alpha} \in \mathbb{Q} \text{ for some } \alpha \in K^\times\}.$$

We give a part of the proof because we will use ideas from this in Chapter 4.

Proof. Let $P = (A, \theta, \varphi)$ be of type $(K, \Phi, t, \mathfrak{m})$ with CM by $\mathcal{O}_K$. Put $\mathfrak{f}(P) = t\mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}$. Let (A, θ, φ) be defined over an algebraic number field of finite degree k such that k is normal over K^r. Since there are only finitely many σA up to $\mathbb{C}$-isomorphism of A over K^r, such a field k exists and the field of moduli M of (A, φ) is contained in k.

Let $\sigma \in \mathrm{Gal}(k/K^r)$. Then by Proposition 1.4.13 the abelian variety $(\sigma A, \sigma\theta)$ is of type (K, Φ) and hence by Corollary 1.4.10, the abelian variety (A, θ) is isogenous to $(\sigma A, \sigma\theta)$. Let X be the ample divisor satisfying $\varphi = \varphi_X$. By Proposition 1.5.2, the isogeny φ_X is an $\mathfrak{f}(P)$-multiplication.

Let $\mathfrak{m}' \in I_K$ and $t' \in K$ such that σP is of type $(K, \Phi, t', \mathfrak{m}')$. The dual of $(\sigma A, \sigma\theta)$ is $(\sigma A^*, \sigma\theta^*)$ and $\varphi_{(\sigma X)} = \sigma\varphi_X$ is an $\mathfrak{f}(P)$-multiplication, see page 124 Shimura–Taniyama [40]. So we have $\mathfrak{f}(\sigma P) = \mathfrak{f}(P)$ hence by (1.5.6), we get

$$\mathrm{N}_{K/F}(\mathfrak{m}'^{-1}\mathfrak{m}) = t^{-1}t'.$$

This concludes $(\sigma P : P) = (\mathrm{N}_{K/F}(\mathfrak{m}'^{-1}\mathfrak{m}), \mathfrak{m}'^{-1}\mathfrak{m}) \in \mathfrak{C}_K$.

On the other hand, for every $\sigma_1, \sigma_2 \in \mathrm{Gal}(k/K^r)$, we have

$$(\sigma_2\sigma_1 P : P) = (\sigma_1 P : P)(\sigma_2 P : P)$$

and the map

$$\begin{aligned} \psi : \mathrm{Gal}(k/K^r) &\to \mathfrak{C}_K \\ \sigma \quad &\mapsto (\sigma P : P), \end{aligned}$$

gives a surjective homomorphism see §15.2 in Shimura–Taniyama [40].

By Proposition 1.5.5, we have $\sigma \in \ker(\psi)$ if and only if σP and P are isomorphic. Moreover, by the definition of M and by Proposition 1.4.8, it holds that σP and P are isomorphic if and only if σ fixes the field M. Therefore, we have $\ker(\psi) = \mathrm{Gal}(k/MK^r)$ and hence the image of ψ in $\mathfrak{C}_K$ is isomorphic to $\mathrm{Gal}(MK^r/K^r)$. Since $\mathfrak{C}_K$ is abelian, the image of ψ in $\mathfrak{C}_K$ is abelian and so the extension MK^r/K^r is abelian.

It remains to show that MK^r is unramified over K^r corresponding to the subgroup $I_0(\Phi^r)$. For this, we refer to page 127 in Shimura–Taniyama [40, §15]. □

We say that a curve C has CM by an order of a CM field K if the endomorphism ring of its Jacobian $J(C)$ is an order in K. Moreover, we say that a curve C is *of type* (K, Φ), if its Jacobian $J(C)$ *is of type* (K, Φ).

Corollary 1.5.7. *If a curve C is of primitive type (K, Φ) with CM by $\mathcal{O}_K$ and defined over K^r, then the CM class group $I_{K^r}/I_0(\Phi^r)$ is trivial.* □

Definition 1.5.8. Let the notation be as in the preceding theorem. The quotient $I_{K^r}/I_0(\Phi^r)$ is called the *CM class group* of (K, Φ). We say that the CM field K has *CM class number one* if there exists a primitive CM type Φ such that (K, Φ) satisfies $I_0(\Phi^r) = I_{K^r}$.

Definition 1.5.9.

- The *CM class number one problem for CM fields of degree* $2g$ is the problem of finding all CM class number one pairs (K, Φ) of degree $2g$.
- The *CM class number one problem for curves of genus* g is the problem of finding all curves of genus g that have a simple Jacobian with CM by the maximal order of a CM class number one field of degree $2g$.

We skip the second and the third main theorems of complex multiplication as we do not need them.

Chapter 2

The CM class number one problem for curves of genus 2

ABSTRACT. In this chapter, we list all quartic CM fields that correspond to CM curves of genus 2 *defined over the reflex field. This chapter is an adaptation of a joint work with Marco Streng that appears as* The CM class number one problem for curves of genus 2 *[18]. The facts in Section 2.2 are presented only for quartic CM fields in the paper [18] and are presented in a more general form in this thesis so that they can be used in Chapter 3.*

2.1 Introduction

Let K be a non-biquadratic quartic (i.e., $\mathrm{Gal}(K/\mathbb{Q}) \ncong C_2 \times C_2$) CM field and Φ be a primitive CM type of K. Let C be a curve of genus 2 with *simple* Jacobian $J(C)$ of type (K, Φ) with CM by $\mathcal{O}_K$. Let (K^r, Φ^r) be the reflex of (K, Φ) and let N_{Φ^r} be the type norm of (K^r, Φ^r) as defined in (1.2.1). Recall

$$I_0(\Phi^r) := \{\mathfrak{b} \in I_{K^r} : \ \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\alpha),\ \alpha\overline{\alpha} \in \mathbb{Q} \text{ for some } \alpha \in K^\times\}.$$

Theorem 1.5.6 implies that if C is defined over the reflex field K^r, then

the CM class group $I_{K^r}/I_0(\Phi^r)$ is trivial. Murabayashi and Umegaki [31] listed all quartic CM fields K corresponding to the rational abelian surfaces with CM by $\mathcal{O}_K$. This list contains only cyclic quartic CM fields, but not the generic dihedral quartic CM fields because curves cannot be defined over $\mathbb{Q}$ in the dihedral case. The reason for this is that in the dihedral case the reflex field K^r is not normal over $\mathbb{Q}$ (see Figure 2.1) and hence the curve C is not defined over $\mathbb{Q}$ by Proposition 5.17 in Shimura [39] (see also Proposition 4.2.1 in Chapter 4). In this chapter, we give the *complete* list of CM class number one non-biquadratic quartic fields, thereby solving the *CM class number one problem for curves of genus* 2 and showing the list in Bouyer–Streng [9] is complete.

In the genus-2 case, the quartic CM field K is either cyclic Galois, biquadratic Galois, or non-Galois with Galois group D_4 (Shimura [40, Example 8.4(2)]). We restrict ourselves to CM curves with a simple Jacobian, which therefore have primitive CM types by Theorem 1.4.1. The corresponding CM fields of such curves are not biquadratic, by Example 8.4-(2) in Shimura [40]

Theorem 2.1.1. *There exist exactly* 63 *isomorphism classes of non-normal quartic CM fields with CM class number one. The fields are listed in Theorem 2.3.15.*

Theorem 2.1.2. *There exist exactly* 20 *isomorphism classes of cyclic quartic CM fields with CM class number one. The fields are listed in Theorem 2.4.5.*

Remark that the list in Theorem 2.4.5 contains the list in [31].

Corollary 2.1.3. *There are exactly* 125 *curves of genus* 2*, up to isomorphism over* $\overline{\mathbb{Q}}$*, defined over the reflex field with CM by* $\mathcal{O}_K$ *for some non-biquadratic quartic CM field* K*. The fields are the fields in Theorems 2.1.1 and 2.1.2, and the curves are those of Bouyer–Streng [9, Tables 1a, 1b, 2b, and 2c].*

Proof. This follows from the list given by Bouyer–Streng in [9] and Theorems 2.1.1–2.1.2. □

Corollary 2.1.4. *There are exactly* 21 *simple CM curves of genus* 2 *defined over* $\mathbb{Q}$*, up to isomorphism over* $\overline{\mathbb{Q}}$*. The fields and* 19 *of the*

curves are given in van Wamelen [45]. The other two curves are $y^2 = x^6 - 4x^5 + 10x^3 - 6x - 1$ *and* $y^2 = 4x^5 + 40x^4 - 40x^3 + 20x^2 + 20x + 3$ *given in Theorem 14 of Bisson–Streng [7].*

Proof. The 19 curves given in [9] are the curves of genus 2 defined over $\mathbb{Q}$ with CM by $\mathcal{O}_K$, see [31] or Corollary 2.1.3. In [7], Bisson–Streng prove that there are only 2 curves of genus 2 defined over $\mathbb{Q}$ with CM by a non-maximal order inside one of the fields of Theorem 2.4.5. Theorem 2.1.2 and Proposition 5.17 in Shimura [39] (see also Proposition 4.2.1 in Chapter 4) finish the proof. □

Corollary 2.1.5. *There are only finitely many simple CM curves of genus* 2 *defined over the reflex field. The corresponding CM fields are those of Theorems 2.1.1–2.1.2, the complete list of orders can be computed using the methods of [7] and the curves using the methods of [9].* □

In Section 2.2, we present general facts about CM fields that we need in this chapter and Chapter 3. Then in Section 2.3, we prove Theorem 2.1.1. The strategy is as follows. We first show that there are only finitely many non-biquadratic quartic CM fields with CM class number one by bounding their absolute discriminant. The bound will be too large for practical purposes, but by using ramification theory and L-functions, we improve the bound which we then use to enumerate the CM fields. Section 2.4 proves Theorem 2.1.2 using the same strategy as in Section 2.3.

2.2 The relative class number

Let K be a CM field with the maximal totally real subfield F of degree g and $h_K^* := h_K/h_F$. In this section, we will present the sufficient conditions for CM class number one fields to satisfy $h_K^* = 2^{t_K - 1}$, where t_K is the number of primes in F that are ramified in K.

Recall that I_K is the group of fractional ideals in K and P_K is the group of principal fractional ideals in K.

Lemma 2.2.1. *Let K be a CM field and let F be the maximal totally real subfield of K. Let H denote the group* $\mathrm{Gal}(K/F)$. *Put* $I_K^H = \{\mathfrak{b} \in I_K \mid \overline{\mathfrak{b}} =$

$\mathfrak{b}\}$ *and* $P_K^H = P_K \cap I_K^H$. *Then we have* $h_K^* = 2^{t_K}\frac{[I_K : I_K^H P_K]}{[P_K^H : P_F]}$, *where* t_K *is the number of primes in* F *that are ramified in* K.

Proof. We have the exact sequence

$$1 \to I_F \to I_K^H \to \bigoplus_{\mathfrak{p} \text{ prime of } F} \mathbb{Z}/e_{K/F}(\mathfrak{p})\mathbb{Z} \to 1 \tag{2.2.1}$$

and

$$\bigoplus_{\mathfrak{p} \text{ prime of } F} \mathbb{Z}/e_{K/F}(\mathfrak{p})\mathbb{Z} \qucong (\mathbb{Z}/2\mathbb{Z})^{t_K}.$$

The map $\varphi : I_K^H \to I_K/P_K$ induces an isomorphism

$$I_K^H/P_K^H \cong \mathrm{im}(\varphi) = I_K^H P_K/P_K$$

so by (2.2.1), we have

$$h_F = [I_F : P_F] = \frac{[I_K^H : P_K^H][P_K^H : P_F]}{[I_K^H : I_F]} = 2^{-t_K}[I_K^H P_K : P_K][P_K^H : P_F],$$

hence

$$h_K^* := \frac{h_K}{h_F} = 2^{t_K}\frac{[I_K : I_K^H P_K]}{[P_K^H : P_F]}.$$

□

Lemma 2.2.2. *Let* K *be a CM field with the maximal totally real subfield* F. *Let* W_K *be the group of roots of unity of* K. *If the Hasse unit index* $Q_K := [\mathcal{O}_K^\times : W_K\mathcal{O}_F^\times]$ *is* 1, *then we have* $[P_K^H : P_F] = 2$ *and* $h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K]$.

Proof. Define $\varphi : \mathcal{O}_K^\times \to \mathcal{O}_K^\times$ by $\varphi(\epsilon) = \epsilon/\overline{\epsilon}$. Then by the assumption $\mathcal{O}_K^\times = W_K\mathcal{O}_F^\times$, we have $\varphi(\epsilon) = \zeta/\overline{\zeta} = \zeta^2$, where $\epsilon = \zeta\epsilon_0$ with $\zeta \in W_K$ and $\epsilon_0 \in \mathcal{O}_F^\times$. Hence $\mathrm{Im}\,\varphi = W_K^2$.

There is a surjective group homomorphism $\lambda : P_K^H \to W_K/W_K^2$ given by $\lambda((\alpha)) = \alpha/\overline{\alpha}$. The map λ is well-defined because every generator of (α) equals $u \cdot \alpha$ for some $u \in \mathcal{O}_K^\times$ and $u/\overline{u} \in W_K^2$. It now suffices to prove that the kernel is P_F. Suppose $\alpha \in F^\times$. Then $\lambda((\alpha)) = \alpha/\overline{\alpha} = 1$, hence

$(\alpha) \in \ker(\lambda)$. Conversely, suppose $\lambda((\alpha)) \in W_K^2$. Then we have $\alpha \in F^\times$, hence $(\alpha) \in P_F$. It follows that $\ker(\lambda) = P_F$.

The latter equality follows from Lemma 2.2.1 and the fact $[P_K^H : P_F] = 2$.

□

Recall

$$I_0(\Phi^r) := \{\mathfrak{b} \in I_{K^r} : \ \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\alpha),\ \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b}) = \alpha\overline{\alpha} \text{ for some } \alpha \in K^\times\}.$$

Lemma 2.2.3. *Let (K, Φ) be a primitive CM pair. If for every $\mathfrak{a} \in I_K$, we have*

$$\mathrm{N}_{\Phi^r}\mathrm{N}_\Phi(\mathfrak{a}) = (\alpha)\mathfrak{a}\overline{\mathfrak{a}}^{-1} \text{ and } \alpha\overline{\alpha} \in \mathbb{Q}, \tag{2.2.2}$$

where $\alpha \in K^\times$, then we have $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$.

Proof. To prove the assertion, we show that the kernel of the map $\mathrm{N}_\Phi : I_K \to I_{K^r}/I_0(\Phi^r)$ is contained in $I_K^H P_K$. Suppose $\mathrm{N}_\Phi(\mathfrak{a}) \in I_0(\Phi^r)$. Then by (2.2.2), we have $(\alpha)\mathfrak{a}\overline{\mathfrak{a}}^{-1} = (\lambda)$, where $\lambda \in K^\times$ and $\lambda\overline{\lambda} = \alpha\overline{\alpha} \in \mathbb{Q}$. Then $\mathfrak{a}\overline{\mathfrak{a}}^{-1} = (\delta)$ with $\delta = \lambda/\alpha$, and hence $\delta\overline{\delta} = 1$. There is a $\gamma \in K^\times$ such that $\delta = \frac{\overline{\gamma}}{\gamma}$ (this is a special case of Hilbert's Theorem 90, but can be seen directly by taking $\gamma = \overline{\epsilon} + \overline{\delta}\epsilon$ for any $\epsilon \in K$ with $\gamma \neq 0$). Thus we have $\mathfrak{a} = \overline{\gamma\mathfrak{a}} \cdot (\frac{1}{\gamma}) \in I_K^H P_K$ and therefore $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$. □

Proposition 2.2.4. *Let K be a CM field and let F be the maximal totally real subfield of K. Suppose $I_0(\Phi^r) = I_{K^r}$. If K satisfies (2.2.2), then we have $h_K^* = 2^T$ with $T \in \{t_K,\ t_K - 1\}$, where t_K is the number of primes in F that are ramified in K. Moreover, if $\mathcal{O}_K^\times = W_K\mathcal{O}_F^\times$ then $T = t_K - 1$.*

Proof. By Lemma 2.2.1, we have

$$h_K^* = 2^{t_K}\frac{[I_K : I_K^H P_K]}{[P_K^H : P_F]}.$$

Lemma 2.2.3 with the assumption $I_0(\Phi^r) = I_{K^r}$ implies $[I_K : I_K^H P_K] = 1$. Hence it follows that $h_K^* = 2^{t_K}[P_K^H : P_F]^{-1} = 2^T$ with $T \in \{t_K,\ t_K - 1\}$ as $[P_K^H : P_F] \in \{1,\ 2\}$.

Moreover, if $\mathcal{O}_K^\times = W_K\mathcal{O}_F^\times$, then by Lemma 2.2.2, we get $[P_K^H : P_F] = 1$ and hence $h_K^* = 2^{t_K - 1}$. □

2.3 Non-normal quartic CM fields

This section, which is the largest in this chapter, proves Theorem 2.1.1. The case of cyclic CM fields is much easier and is treated in Section 2.4.

Suppose that $K/\mathbb{Q}$ is a non-normal quartic CM field and F is the real quadratic subfield of K. The normal closure N is a dihedral CM field of degree 8 with Galois group $G := \mathrm{Gal}(N/\mathbb{Q}) = \langle x,\, y : y^4 = x^2 = (xy)^2 = \mathrm{id}\rangle$. Complex conjugation $\bar{\cdot}$ is y^2 in this notation and the CM field K is the subfield of N fixed by $\langle x\rangle$. Let Φ be a CM type of K with values in N'. We can (and do) identify N with a subfield of N' in such a way that $\Phi = \{\mathrm{id}, y|_K\}$. Then the reflex field K^r of Φ is the fixed field of $\langle xy\rangle$, which is a non-normal quartic CM field non-isomorphic to K with reflex type $\Phi^r = \{\mathrm{id}, y^3|_{K^r}\}$, (see [40, Examples 8.4., 2(C)]). Denote the quadratic subfield of K^r by F^r.

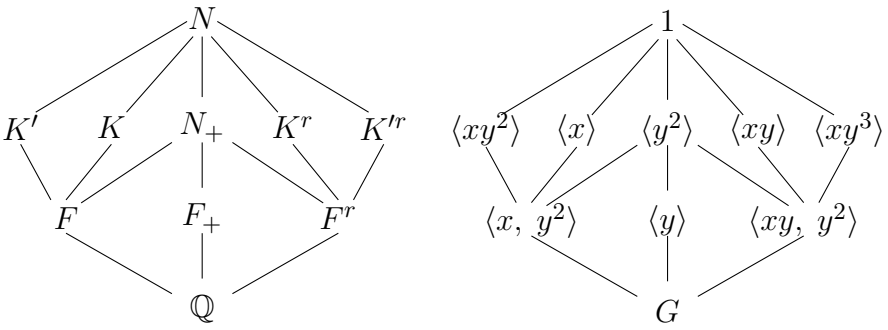


Figure 2.1: Lattice of subfields and subgroups

Let N_+ be the maximal totally real subfield of N, and let F_+ be the quadratic subfield of N_+ such that N/F_+ is cyclic.

2.3.1 An effective bound for CM class number one non-normal quartic fields

In this section, we find an effective upper bound for the absolute discriminant of non-normal quartic CM fields with CM class number one.

Proposition 2.3.1. *Let K be a non-biquadratic quartic CM field and let F be the real quadratic subfield of K. Assuming $I_0(\Phi^r) = I_{K^r}$, we have $h_K^* = 2^{t_K - 1}$, where t_K is the number of primes in F that are ramified in K.*

Moreover, we have $h_{K^r}^* = 2^{t_{K^r} - 1}$, where t_{K^r} is the number of primes in F^r that are ramified in K^r.

Proof. Since $\mu_K = \{\pm 1\}$, by Lemma 2.2.2, we have $h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K]$. For any $\mathfrak{a} \in I_K$, we can compute (see [38, (3.1)])

$$\mathrm{N}_{\Phi^r}\mathrm{N}_{\Phi}(\mathfrak{a}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\mathfrak{a}\overline{\mathfrak{a}}^{-1}.$$

Then, by Lemma 2.2.3, under the assumption $I_0(\Phi^r) = I_{K^r}$, the quotient $I_K / I_K^H P_K$ is trivial. Therefore, we have $h_K^* = 2^{t_K - 1}$.

For the second statement, we claim $[I_{K^r} : I_{K^r}^{H'} P_{K^r}] \leq [I_{K^r} : I_0(\Phi^r)]$, where $H' = \mathrm{Gal}(K^r / F^r)$. For any $\mathfrak{b} \in I_{K^r}$, by [38, (3.2)], we have

$$\mathrm{N}_{\Phi}\mathrm{N}_{\Phi^r}(\mathfrak{b}) = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{b})\mathfrak{b}\overline{\mathfrak{b}}^{-1}.$$

Suppose $\mathfrak{b} \in I_0(\Phi^r)$. Then $N_{K^r/\mathbb{Q}}(\mathfrak{b})\mathfrak{b}\overline{\mathfrak{b}}^{-1} = (\alpha)$, where $\alpha \in K^{r\times}$ and $\alpha\overline{\alpha} = N_{\Phi}(N_{K^r/\mathbb{Q}}(\mathfrak{b})) = N_{K^r/\mathbb{Q}}(\mathfrak{b})^2 \in \mathbb{Q}$. We finish the proof of $\mathfrak{b} \in I_{K^r}^{H'} P_{K^r}$ exactly as in Lemma 2.2.3. So this proves $I_0(\Phi^r) \subset I_{K^r}^{H'} P_{K^r}$, hence the claim follows.

Since $\mu_{K^r} = \{\pm 1\}$, by Lemma 2.2.2, we have $h_{K^r}^* = 2^{t_{K^r} - 1}[I_{K^r} : I_{K^r}^{H^r} P_{K^r}]$. By the assumption $I_0(\Phi^r) = I_{K^r}$, the claim above implies $[I_{K^r} : I_{K^r}^{H^r} P_{K^r}] = 1$, hence we get $h_{K^r}^* = 2^{t_{K^r} - 1}$.

□

Remark 2.3.2. In the case where $K/\mathbb{Q}$ is cyclic quartic, this result is $(i) \Rightarrow (iii)$ of Proposition 4.5 in Murabayashi [30].

On the other hand, if K is a non-normal quartic CM field, Louboutin proves $h_K^* \approx \sqrt{d_K/d_F}$ with an effective error bound, see Proposition 2.3.3. Putting this together with the result in Proposition 2.3.1 gives approximately $\sqrt{d_K/d_F} \leq 2^{t_K - 1}$. As the left hand side grows more quickly than the right, this relation will give a bound on the absolute value of the discriminant, precisely see Proposition 2.3.4.

The next step is to use the following bound from analytic number theory.

Let d_M denote the absolute value of the discriminant (absolute discriminant) of a number field M.

Proposition 2.3.3. *(Louboutin [26], Remark 27 (1)) Let N be the normal closure of a non-normal quartic CM field K with Galois group D_4. Assume $d_N^{1/8} \geq 222$. Then*

$$h_K^* \geq \frac{2\sqrt{d_K/d_F}}{\sqrt{e}\pi^2(\log(d_K/d_F)+0.057)^2}. \qquad \square \tag{2.3.1}$$

Proposition 2.3.4. *Let K be a non-normal quartic CM field and let F be the real quadratic subfield of K. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have $d_K/d_F \leq 2 \cdot 10^{15}$.*

Proof. Let

$$f(D) = \frac{2\sqrt{D}}{\sqrt{e}\pi^2(\log(D)+0.057)^2} \quad \text{and} \quad g(t) = 2^{-t+1} f(\Delta_t),$$

where $\Delta_k = \prod_{j=1}^{k} p_j$ and p_j is the j-th prime.

Here, if $D = d_K/d_F$, then f is the right hand side of the inequality (2.3.1) in Proposition 2.3.3. The quotient d_K/d_F is divisible by the product of rational primes that are ramified in K/F, so $d_K/d_F \geq \Delta_{t_K}$.

On the other hand, the function f is monotonically increasing for $D > 52$, so if $t_K \geq 4$ then $f(d_K/d_F) \geq f(\Delta_{t_K})$. Therefore, by Proposition 2.3.1, we get that if $I_0(\Phi^r) = I_{K^r}$, then

$$2^{t_K - 1} \geq f(d_K/d_F) \geq f(\Delta_{t_K}) \tag{2.3.2}$$

and hence $1 \geq g(t_K)$. The function g is monotonically increasing for $t_K \geq 4$ and is greater than 1 if $t_K > 14$. Therefore, we get $t_K \leq 14$ and $h_K^* \leq 2^{13}$, hence $d_K/d_F < 2 \cdot 10^{15}$. $\square$

The bound that we get in Proposition 2.3.4 is unfortunately too large to list all the fields. In the following section we study ramification of primes in $N/\mathbb{Q}$ and find a sharper upper bound for d_{K^r}/d_{F^r}, see Proposition 2.3.14.

2.3.1.1 Almost all ramified primes are inert in F and F^r

In this section, under the assumption $I_0(\Phi^r) = I_{K^r}$, we study the ramification behavior of primes in $N/\mathbb{Q}$, and prove that almost all rational primes that are ramified in K^r/F^r are inert in F^r. We precisely prove the following proposition.

Proposition 2.3.5. *Let K be a non-normal quartic CM field and let F be its real quadratic subfield. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Moreover, all the rational primes (distinct from p and q) that are ramified in K^r/F^r are inert in F and F^r.*

This proposition implies that d_{K^r}/d_{F^r} grows as the square of the product of such ramified primes and we get a lower bound on $f(d_{K^r}/d_{F^r})$ of (2.3.2) that grows even faster with t_{K^r} than what we had in the proof of Proposition 2.3.4. Hence we obtain a better upper bound on d_{K^r}/d_{F^r}, see Proposition 2.3.14.

We begin the proof of Proposition 2.3.5 with exploring the ramification behavior of primes in $N/\mathbb{Q}$, under the assumption $I_0(\Phi^r) = I_{K^r}$.

Ramification of primes in $N/\mathbb{Q}$

Lemma 2.3.6. *Let M/L be a Galois extension of number fields and $\mathfrak{q}$ be a prime of M over an odd prime ideal $\mathfrak{p}$ (that is, the prime $\mathfrak{p}$ lies over an odd prime in $\mathbb{Q}$) of L. Then there is no surjective homomorphism from a subgroup of $I_\mathfrak{q}$ to a Klein four group V_4.*

Proof. For an odd prime ideal $\mathfrak{p}$ in L, suppose that there is a surjective homomorphism from a subgroup of $\mathrm{I}_\mathfrak{q}$ to V_4. In other words, suppose a prime of F over $\mathfrak{p}$ is totally ramified in a biquadratic intermediate extension E/F of M/L. Assume without loss of generality $E = M$ and $F = L$. The biquadratic intermediate extension E/F has three quadratic intermediate extensions $E_i = F(\sqrt{\alpha_i})$ for $i = 1,\ 2,\ 3$. Without loss of generality, take $\mathrm{ord}_\mathfrak{p}(\alpha_i) \in \{0, 1\}$ for each i. Note $\mathcal{O}_{E_i}$ contains $\mathcal{O}_F[\sqrt{\alpha_i}]$ of relative discriminant $4\alpha_i$ over $\mathcal{O}_F$. Since $\mathfrak{p}$ is odd, this implies that the relative discriminant $\Delta(E_i/F)$ of $\mathcal{O}_{E_i}$ has $\mathrm{ord}_\mathfrak{p}(\Delta(E_i/F)) = \mathrm{ord}_\mathfrak{p}(\alpha_i)$. At

the same time, we have $E_3 = F(\sqrt{\alpha_1\alpha_2})$ so $\mathfrak{p}$ ramifies in E_i for an even number of i's. In particular, $\mathfrak{p}$ is not totally ramified in E/F. □

Lemma 2.3.7. *Let K be a non-normal quartic CM field and let F be the real quadratic subfield of K. Let Φ be a primitive CM type of K and K^r be the reflex field of (K, Φ) with the quadratic subfield F^r. Then the following assertions hold.*

(i) If a prime p is ramified in both F and F^r, then it is totally ramified in $K/\mathbb{Q}$ and $K^r/\mathbb{Q}$.

(ii) If an odd prime p is ramified in F (in F^r, respectively) as well as in F_+, then p splits in F^r (in F, respectively). Moreover, at least one of the primes above p in F^r is ramified in K^r/F^r (in K/F, respectively).

Proof. The statements (i) and (ii) are clear from Table 2.1 on page 32. Alternatively, one can also prove the statements as follows:

(i) Let $\mathfrak{p}_N$ be a prime of N above p that is ramified in both $F/\mathbb{Q}$ and $F^r/\mathbb{Q}$. Then the maximal unramified subextension of $N/\mathbb{Q}$ is contained in F_+. Therefore, the inertia group of $\mathfrak{p}_N$ contains $\mathrm{Gal}(N/F_+) = \langle y \rangle$. By computing ramification indices in the diagram of subfields one by one, we see that the prime p is totally ramified in K and K^r.

(ii) Let p be an odd prime that is ramified in $F/\mathbb{Q}$ and $F_+/\mathbb{Q}$ and $\mathfrak{p}_N$ be a prime above p in N. The inertia group of an odd prime cannot be a biquadratic group by Lemma 2.3.6, so $\mathrm{I}_{\mathfrak{p}_N}$ is a proper subgroup of $\mathrm{Gal}(N/F^r)$. Since $\mathrm{I}_{\mathfrak{p}_N}$ is a normal subgroup in $\mathrm{D}_{\mathfrak{p}_N}$, the group $\mathrm{D}_{\mathfrak{p}_N}$ cannot be the full Galois group $\mathrm{Gal}(N/\mathbb{Q})$. So $\mathrm{D}_{\mathfrak{p}_N}$ is a proper subgroup of $\mathrm{Gal}(N/F^r)$ and hence p splits in F^r. Moreover, since p is ramified in F, hence in K, hence in K^r, at least one of the primes above p in F^r is ramified in K^r. Since F and F^r are symmetric in $N/\mathbb{Q}$, the same argument holds for F^r as well.

□

Lemma 2.3.8. *Let the notation be as in Lemma 2.3.7. Assuming $I_0(\Phi^r) = I_{K^r}$, if K^r has a prime $\mathfrak{p}$ of prime norm p with $\overline{\mathfrak{p}} = \mathfrak{p}$, then $F = \mathbb{Q}(\sqrt{p})$.*

Proof. By the assumption, we have

$$\mathrm{N}_{\Phi^r}(\mathfrak{p}) = (\alpha) \text{ for some } \alpha \in K^{\times} \text{such that } \alpha\overline{\alpha} = \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{p}) = p.$$

Since $\overline{\mathfrak{p}} = \mathfrak{p}$, we have $(\alpha) = (\overline{\alpha})$, and so $\alpha = \epsilon\overline{\alpha}$ for a unit ϵ in $\mathcal{O}_K^{\times}$ with absolute value 1 (hence a root of unity). Since $\mu_K = \{\pm 1\}$, we get $\alpha^2 = \pm p$. The case $\alpha^2 = -p$ is not possible, since K has no imaginary quadratic intermediate field. Hence we have $\alpha^2 = p$ and so $\sqrt{p} \in F$. □

Corollary 2.3.9. *The notation being as in Lemma 2.3.7, suppose $I_0(\Phi^r) = I_{K^r}$. If p is totally ramified in $K^r/\mathbb{Q}$, or splits in $F^r/\mathbb{Q}$ and at least one of the primes over p in F^r ramifies in K^r/F^r, then $F = \mathbb{Q}(\sqrt{p})$.* □

Proposition 2.3.10. *Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$, where p is a rational prime.*

Proof. Suppose that there is an odd prime p that is ramified in F. Then p is ramified either in F and F^r or in F and F_+.

If p is ramified in both F and F^r, then by Lemma 2.3.7-(i), the prime p is totally ramified in $K^r/\mathbb{Q}$. If p is ramified in F and F_+, then by Lemma 2.3.7-(ii), the prime p splits in F^r and at least one of the primes over p in F^r ramifies in K^r/F^r. In both cases, Corollary 2.3.9 tells us that $F = \mathbb{Q}(\sqrt{p})$.

Therefore, if an odd prime p is ramified in F, then we have $F = \mathbb{Q}(\sqrt{p})$. If no odd prime ramifies in F, then the only prime that ramifies in F is 2 so we have $F = \mathbb{Q}(\sqrt{2})$. □

Table 2.1: Ramification table of a non-normal quartic CM field

Table 2.3.1.1 lists all 19 pairs (I,D) where $1 \neq \mathrm{I} \triangleleft \mathrm{D} \leq D_4 = \langle x,\ y \rangle$ and D/I is cyclic, partitioned into 15 conjugacy classes (1) – (15). In particular, it contains all possible inertia and decomposition groups of ramified primes of N. This table is a corrected subset of [14, Table 3.5.1]. We restricted to $\mathrm{I} \neq 1$, added the case 8-(b), which is missing in [14, Table 3.5.1], and corrected the type norm column of some cases. The cases (11) – (15) can only occur for the prime 2, see Lemma 2.3.6. If there is a checkmark in the last column, then by Lemma 2.3.8, such splitting implies $\sqrt{p} \in F$ (i.e., $F = \mathbb{Q}(\sqrt{p})$) under the assumption $I_0(\Phi^r) = I_{K^r}$. The cases with * do not occur under the assumption $I_0(\Phi^r) = I_{K^r}$ because p is not ramified in F in these cases, but on the other hand $\sqrt{p} \in F$ by Lemma 2.3.8.

Case	I	D	decomp. of p in N	decomp. of p in K	decomp. of p in F	decomp. of p in F_+	decomp. of p in F^r	decomp. of p in K^r	$N_{\Phi^r}(\mathfrak{p}_{K^r,1})$	$\sqrt{p} \in F$
(1)*	$\langle y^2 \rangle$	$\langle y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,x}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,xy}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	✓
(2)	$\langle y^2 \rangle$	$\langle y \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(3)	$\langle y^2 \rangle$	$\langle x,\, y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(4)*	$\langle y^2 \rangle$	$\langle xy,\, y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}$	✓
(5) (a)	$\langle x \rangle$	$\langle x \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2\mathfrak{p}_{K,y^2}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	
(b)	$\langle xy^2 \rangle$	$\langle xy^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2\mathfrak{p}_{K,y^3}$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$	
(6) (a)	$\langle x \rangle$	$\langle x,\, y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2$	p	
(b)	$\langle xy^2 \rangle$	$\langle x,y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^2$	p	
(7) (a)	$\langle xy \rangle$	$\langle xy \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2\mathfrak{p}_{K,y^3}$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}\mathfrak{p}_{K^r,y^3}$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y^3}$	✓
(b)	$\langle xy^3 \rangle$	$\langle xy^3 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2\mathfrak{p}_{N,y^2}^2\mathfrak{p}_{N,y^3}^2$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}\mathfrak{p}_{K^r,y^2}$	$\mathfrak{p}_{K,1}^2$	✓
(8) (a)	$\langle xy \rangle$	$\langle xy,y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}$	$\mathfrak{p}_{K,1}$	✓
(b)	$\langle xy^3 \rangle$	$\langle xy,y^2 \rangle$	$\mathfrak{p}_{N,1}^2\mathfrak{p}_{N,y}^2$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}\mathfrak{p}_{K^r,y}^2$	p	✓
(9)	$\langle y \rangle$	$\langle y \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}\mathfrak{p}_{F_+,y}$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓
(10)	$\langle y \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓
(11)*	$\langle x,y^2 \rangle$	$\langle x,y^2 \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^2\mathfrak{p}_{K,y}^2$	$\mathfrak{p}_{F,1}\mathfrak{p}_{F,y}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}\mathfrak{p}_{K,y}$	✓
(12)*	$\langle x,y^2 \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^2$	$\mathfrak{p}_{F,1}$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}$	✓
(13)	$\langle xy,y^2 \rangle$	$\langle xy,y^2 \rangle$	$\mathfrak{p}_{N,1}^4\mathfrak{p}_{N,y}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}\mathfrak{p}_{F^r,y}$	$\mathfrak{p}_{K^r,1}^2\mathfrak{p}_{K^r,y}^2$	$\mathfrak{p}_{K,1}^2$	✓
(14)	$\langle xy,y^2 \rangle$	G	$\mathfrak{p}_{N,1}^4$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}$	$\mathfrak{p}_{K^r,1}^2$	p	
(15)	G	G	$\mathfrak{p}_{N,1}^8$	$\mathfrak{p}_{K,1}^4$	$\mathfrak{p}_{F,1}^2$	$\mathfrak{p}_{F_+,1}^2$	$\mathfrak{p}_{F^r,1}^2$	$\mathfrak{p}_{K^r,1}^4$	$\mathfrak{p}_{K,1}^2$	✓

Lemma 2.3.11. *Suppose $I_0(\Phi^r) = I_{K^r}$. Then the following assertions are true.*

(i) If a rational prime l is unramified in both $F/\mathbb{Q}$ and $F^r/\mathbb{Q}$, but is ramified in $K/\mathbb{Q}$ or $K^r/\mathbb{Q}$, then all primes above l in F and F^r are ramified in K/F and K^r/F^r and l is inert in F^r.

(ii) If $F = \mathbb{Q}(\sqrt{p})$ with a prime number $p \equiv 3 \pmod 4$, then 2 is inert in F^r.

Proof. (i) It follows from Table 2.1 except for the statement that l is inert in F^r.

Suppose that l splits in F^r. Then by Corollary 2.3.9, we have $\sqrt{l} \in F$, contradicts unramifiedness of l in F. Therefore, the prime l is inert in F^r.

(ii) The prime 2 is ramified in F since $p \equiv 3 \pmod 4$. If 2 is also ramified in F^r, then by Lemma 2.3.7-(i), the prime 2 is totally ramified in K and K^r. If 2 splits in F^r, then by Table 2.1, at least one of the primes in F^r above 2 ramifies in K^r. In both cases by Corollary 2.3.9, we have $F = \mathbb{Q}(\sqrt{p})$ with $p = 2$, a contradiction. This implies that 2 is inert in F^r.

□

Equality of t_K and t_{K^r}

In the previous section, we proved that the primes that are unramified in F and F^r, but are ramified in K^r/F^r are inert in F^r. Thus these primes contribute to t_{K^r} (the number of primes in F^r that are ramified in K^r) with one prime, on the other hand they contribute to t_K (the number of primes in F that are ramified in K) with at least one prime and exactly two if the prime splits in $F/\mathbb{Q}$. So if we could prove $t_K = t_{K^r}$, then that would approximately say that all such primes are inert in both F and F^r.

Proposition 2.3.12. *(Shimura, [38, Proposition A.7.]) Let the notation be as above. Then we have $h_K^* = h_{K^r}^*$.*

Proof. The idea of the proof is to first show

$$\zeta_K(s)/\zeta_F(s) = \zeta_{K^r}(s)/\zeta_{F^r}(s) \tag{2.3.3}$$

and then use the analytic class number formula at $s = 0$. Louboutin [23, Theorem A] shows the equality (2.3.3) by writing the Dedekind zeta functions of K, K^r, F and F^r as a product of Artin L-functions and finding relations between these combinations of L-functions (see [23, Theorem A]).

We can also get this equality by comparing the local factors of the Euler products of the Dedekind ζ-functions of the fields. By Table 2.1, we see that each ramified prime in $N/\mathbb{Q}$ has the same factors in the Euler products of the quotients of the Dedekind ζ-functions on both sides of (2.3.3). As an example, we take a rational prime p with ramification type (6 a) in Table 2.1, where the local factors for p of the Dedekind ζ-functions are as follows:

$$\begin{aligned}
\zeta_K(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K,1}{}^{-s}} \cdot \frac{1}{1-\mathrm{N}\mathfrak{p}_{K,y}{}^{-s}} = \frac{1}{1-(p^2)^{-s}} \cdot \frac{1}{1-p^{-s}}, \\
\zeta_F(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{F,1}{}^{-s}} \cdot \frac{1}{1-\mathrm{N}\mathfrak{p}_{F,y}{}^{-s}} = \left(\frac{1}{1-p^{-s}}\right)^2, \\
\zeta_{K^r}(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K^r,1}{}^{-s}} = \frac{1}{1-(p^2)^{-s}}, \\
\zeta_{F^r}(s)_p &= \frac{1}{1-\mathrm{N}\mathfrak{p}_{K^r,1}{}^{-s}} = \frac{1}{1-p^{-s}}.
\end{aligned}$$

So for such a prime, we get

$$\zeta_K(s)_p/\zeta_F(s)_p = \frac{1}{1+p^{-s}} = \zeta_{K^r}(s)_p/\zeta_{F^r}(s)_p.$$

Similarly, by using Table 3.5.1 in [14], we can get this equality for the unramified primes as well.

The analytic class number formula at $s = 0$ (see, [46, Chapter 4]) says that the Dedekind zeta function $\zeta_M(s)$ of an algebraic number field M has a zero at $s = 0$ and the derivative of $\zeta_M(s)$ at $s = 0$ has the value

$$-\frac{h_M \cdot R_M}{\mu_M},$$

where h_M is the class number; R_M is the regulator; and μ_M is the order of the group of roots of unity W_M.

Since $\mu_K = 2 = \mu_F$ and $R_K = 2R_F$ (see Washington, [46, Proposition 4.16]), the analytic class number formula at $s = 0$ gives

$$\lim_{s\to 0} \frac{\zeta_K(s)}{\zeta_F(s)} = 2h_K^*.$$

Therefore, the equality of h_K^* and $h_{K^r}^*$ follows from the identity (2.3.3). □

Corollary 2.3.13. *The notation being as above, assuming $I_0(\Phi^r) = I_{K^r}$, we have $t_K = t_{K^r}$.*

Proof. By Proposition 2.3.1, we have $h_K^* = 2^{t_K - 1}$ and $h_{K^r}^* = 2^{t_{K^r}-1}$. Then by Proposition 2.3.12, we get $t_K = t_{K^r}$. □

Proof of Proposition 2.3.5

Proposition 2.3.5. *Let K be a non-normal quartic CM field and let F be its real quadratic subfield. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Moreover, all the rational primes (distinct from p and q) that are ramified in K^r/F^r are inert in F and F^r.*

Proof. We first prove that if a prime l ramifies in both F and F^r, then it is equal to p, where $F = \mathbb{Q}(\sqrt{p})$.

Indeed, by Lemma 2.3.7-(i), the prime l is totally ramified in $K^r/\mathbb{Q}$ and hence by Corollary 2.3.9, we get $F = \mathbb{Q}(\sqrt{l})$, so $l = p$.

Now we see that there are four types of prime numbers that ramify in $N/\mathbb{Q}$:

(I) The prime p, which is ramified in F and possibly in F^r.

(II) The primes that are unramified in F, but ramified in F^r, say $q_1, \ldots, q_s$.

(III) The primes that are unramified in F and F^r, but ramified in K, say $r_1, \ldots, r_m$.

(IV) If $p \equiv 3 \pmod 4$, then $2 \neq p$ is ramified in F and is inert in F^r by Lemma 2.3.11-(ii).

We will compute the contribution of each ramification type to t_K (the number of primes in F that are ramified in K) and t_{K^r} (the number of primes in F^r that are ramified in K^r). Let f_p and f_p^r be the contributions of the primes over p to t_K and t_{K^r}, respectively. Set $i_2 = 1$ if $p \equiv 3 \pmod 4$, and $i_2 = 0$ if $p \not\equiv 3 \pmod 4$.

Claim. We have $t_K \geq f_p + s + m + i_2$ with equality only if all primes of type (III) are inert in F and $t_{K^r} = f_p^r + m + i_2$.

Proof. By Table 2.1 including Lemma 2.3.8, we see that for $i = 1, \ldots, s$ *exactly* one of the primes above q_i in F ramifies in K/F and the unique prime above q_i in F^r does not ramify in K^r/F^r. By Lemma 2.3.11-(i), we see that for $j = 1, \ldots, m$ the prime r_j is inert in F^r so contributes with *exactly* one prime to t_{K^r}, and with *at least* one prime to t_K and with exactly one if and only if r_j is inert in $F/\mathbb{Q}$. If $p \equiv 3 \pmod 4$, then by Lemma 2.3.11-(ii), the prime 2 is inert in F^r. As furthermore 2 is ramified in F and $F \ncong \mathbb{Q}(\sqrt{2})$, the prime 2 has the decomposition (14) in Table 2.1, so it contributes *exactly* with one prime to t_K and t_{K^r}. So we get $t_K \geq f_p + s + m + i_2$ with equality if and only if all primes of type (III) are inert in F and $t_{K^r} = f_p^r + m + i_2$, which proves the claim.

We observe that $s > 0$ holds. Indeed, if $s = 0$, then all primes that ramify in F^r also ramify in F. Hence d_{F^r} divides d_F, which is equal to p if $p \equiv 1 \pmod 4$ and $4p$ otherwise. So $F^r \cong F$, a contradiction.

If p ramifies in both F and F^r, then by Lemma 2.3.7-(i), we have $f_p = f_p^r = 1$. The same is true if p is of type (14) in Table 2.1. By Corollary 2.3.13, we have $t_K = t_{K^r}$, so in this case $m + i_2 \geq s + m + i_2$, so $s = 0$, a contradiction. Therefore, the prime p is not ramified in F^r and is not of type (14), leaving only the possibility $(q/p) = 1$. By Table 2.1, we see that $f_p^r - f_p = 1$. Hence $t_K = t_{K^r}$ implies that all primes of type (III) are inert in F and $s = 1$. In particular, since p is unramified in F^r, we get $F^r = \mathbb{Q}(\sqrt{q})$ for a prime $q \not\equiv 3 \pmod 4$. Moreover, Table 2.1 implies $(p/q) = 1$. □

A sharper bound for d_{K^r}/d_{F^r}

Proposition 2.3.14. *Let K be a non-normal quartic CM field and let F be its real quadratic subfield. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$ and $d_N^{1/8} \geq 222$. Then we have $h^*_{K^r} \leq 2^5$ and $d_{K^r}/d_{F^r} \leq 3 \cdot 10^{10}$.*

Proof. Under the assumption $I_0(\Phi^r) = I_{K^r}$, in Propositions 2.3.10 and 2.3.5 we proved $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers. Additionally, we proved that at least one of the ramified primes above p in F^r is ramified in K^r/F^r, and the other ramified primes in K^r/F^r are inert in F^r, say $r_1, \ldots, r_{t_{K^r}-1}$. Therefore, we have $d_{K^r}/d_{F^r} \geq pqr_1^2 \cdots r_{t_{K^r}-1}^2$.

Let

$$f(D) = \frac{2\sqrt{D}}{\sqrt{e}\pi^2(\log(D)+0.057)^2} \quad \text{and} \quad g(t) = 2^{-t+1} f(p_t p_{t+1} \Delta_{t-1}^2),$$

where p_j is the j-th prime and $\Delta_k = \prod_{j=1}^k p_j$. If $D = d_{K^r}/d_{F^r}$, then we have $h_{K^r} \geq f(D)$ by Proposition 2.3.3.

Recall that, by the proof of Proposition 2.3.4, the function f is monotonically increasing for $D > 52$. Therefore, if $t_{K^r} > 3$, then we have $f(d_{K^r}/d_{F^r}) > f(p_{t_{K^r}} p_{t_{K^r}+1} \Delta_{t_{K^r}-1}^2)$. So in that case by Proposition 2.3.1 and Corollary 2.3.13, we have $h^*_{K^r} = 2^{t_{K^r}-1}$, hence we get $g(t_{K^r}) \leq 1$. Further, the function g is monotonically increasing for $t_{K^r} \geq 4$ and is greater than 1 for $t_{K^r} = 7$. So we get $t_{K^r} \leq 6$. □

2.3.2 Enumerating the fields

To specify non-biquadratic quartic CM fields, we use the following notation of the ECHIDNA database [13]. Given a non-biquadratic quartic CM field K, let D be the discriminant of the real quadratic subfield F of K. Write $K = F(\sqrt{-\alpha})$ where α is a totally positive element of $\mathcal{O}_F$ and take α such that $A := \mathrm{Tr}_{F/\mathbb{Q}}(\alpha) > 0$ is minimal and let $B := \mathrm{N}_{F/\mathbb{Q}}(-\alpha)$. We choose α with minimal B if there is more than one B with the same A. We use the triple $[D, A, B]$ to uniquely represent the isomorphism class of the CM field $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B)$.

Theorem 2.3.15. *There exist exactly* 63 *isomorphism classes of CM class number one non-normal quartic CM fields. The fields are given by* $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B) \supset \mathbb{Q}(\sqrt{D})$ *where* $[D, A, B]$ *ranges over*

$[5,13,41]$, $[5,17,61]$, $[5,21,109]$, $[5,26,149]$, $[5,34,269]$, $[5,41,389]$,
$[8,10,17]$, $[8,18,73]$, $[8,22,89]$, $[8,34,281]$, $[8,38,233]$, $[13,9,17]$,
$[13,18,29]$, $[13,29,181]$, $[13,41,157]$, $[17,5,2]$, $[17,15,52]$, $[17,46,257]$,
$[17,47,548]$, $[29,9,13]$, $[29,26,53]$, $[41,11,20]$, $[53,13,29]$, $[61,9,5]$,
$[73,9,2]$, $[73,47,388]$, $[89,11,8]$, $[97,94,657]$, $[109,17,45]$,
$[137,35,272]$, $[149,13,5]$, $[157,25,117]$, $[181,41,13]$, $[233,19,32]$,
$[269,17,5]$, $[281,17,2]$, $[389,37,245]$

with class number 1*;*

$[5,11,29]$, $[5,33,261]$, $[5,66,909]$, $[8,50,425]$, $[8,66,1017]$, $[17,25,50]$,
$[29,7,5]$, $[29,21,45]$, $[101,33,45]$, $[113,33,18]$, $[8,14,41]$, $[8,26,137]$,
$[12,8,13]$, $[12,10,13]$, $[12,14,37]$, $[12,26,61]$, $[12,26,157]$, $[44,8,5]$,
$[44,14,5]$, $[76,18,5]$, $[172,34,117]$, $[236,32,20]$

with class number 2*;*
$[257,23,68]$
with class number 3*;*
$[8,30,153]$, $[12,50,325]$, $[44,42,45]$
with class number 4*.*

We begin the proof by combining the ramification results into the following explicit form for K^r.

Proposition 2.3.16. *Let* K *be a non-normal quartic CM field and let* F *be its real quadratic subfield. Let* Φ *be a primitive CM type of* K*. Suppose* $I_0(\Phi^r) = I_{K^r}$*. Then there exist prime numbers* p*,* q*, and* $s_1 < \cdots < s_u$ *with* $u \in \{t_{K^r} - 1,\ t_{K^r} - 2\}$ *such that all of the following hold. We have* $F = \mathbb{Q}(\sqrt{p})$ *and* $F^r = \mathbb{Q}(\sqrt{q})$ *with* $q \not\equiv 3 \pmod 4$ *and* $(p/q) = (q/p) = 1$*. There exists a prime* $\mathfrak{p}$ *lying above* p *in* F^r *that ramifies in* K^r*, an odd* $j \in \mathbb{Z}_{>0}$ *and a totally positive generator* π *of* $\mathfrak{p}^j$*. Moreover, for exactly one such* $\mathfrak{p}$ *and each such* π *and* j*, we have* $K^r \cong \mathbb{Q}(\sqrt{-\pi s_1 \cdots s_u})$*.*

Proof. By Proposition 2.3.5, we have $F=\mathbb{Q}(\sqrt{p})$ and $F^r=\mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q\not\equiv 3 \pmod 4$ and $(p/q)=(q/p)=1$.

There exists a totally positive element β in $(F^r)^\times$ such that $K^r=F^r(\sqrt{-\beta})$, where β is uniquely defined up to $((F^r)^\times)^2$ (without loss of generality, we can take β in $\mathcal{O}_{F^r}$).

Since $\mathcal{O}_{K^r}\supset\mathcal{O}_{F^r}[\sqrt{-\beta}]\supset\mathcal{O}_{F^r}$, the quotient of the discriminant ideals $\Delta(\mathcal{O}_{K^r}/\mathcal{O}_{F^r})/\Delta(\mathcal{O}_{F^r}[\sqrt{-\beta}]/\mathcal{O}_{F^r})=\Delta(\mathcal{O}_{K^r}/\mathcal{O}_{F^r})/(-4\beta)$ is a square ideal in $\mathcal{O}_{F^r}$ (see Cohen [10, pp.79]). As β is unique up to squares, and we can take $\mathfrak{l}$-minimal $\beta'\in\beta(F^\times)^2$ for each prime $\mathfrak{l}$ of $\mathcal{O}_{F^r}$, we get

$$\mathrm{ord}_{\mathfrak{l}}((\beta))\equiv\begin{cases}1 \pmod 2 & \text{if } \mathfrak{l} \text{ is ramified in } K^r/F^r \text{ and } \mathfrak{l}\nmid 2,\\ 0 \pmod 2 & \text{if } \mathfrak{l} \text{ is not ramified in } K^r/F^r,\\ 0 \text{ or } 1 \pmod 2 & \text{if } \mathfrak{l} \text{ is ramified in } K^r/F^r \text{ and } \mathfrak{l}|2.\end{cases} \tag{2.3.4}$$

Let $\mathfrak{l}_1,\dots,\mathfrak{l}_{t_{K^r}}\subseteq\mathcal{O}_{F^r}$ be the primes above the prime numbers $l_1,\dots,l_{t_{K^r}}$ that ramify in K^r/F^r respectively. Let $n_i>0$ be minimal such that $\mathfrak{l}_i^{n_i}$ is generated by a totally positive $\lambda_i\in\mathcal{O}_{F^r}$. Since $F^r=\mathbb{Q}(\sqrt{q})$ with prime $q\not\equiv 3 \pmod 4$, genus theory implies that $\mathrm{Cl}_{F^r}=\mathrm{Cl}^+_{F^r}$ has odd order so n_i is odd. Let

$$\alpha=\prod_{i=1}^{t_{K^r}}\lambda_i^{(\mathrm{ord}_{\mathfrak{l}_i}((\beta)) \bmod 2)}.$$

By proving the following two claims we finish the proof.

Claim 1. We have $\alpha/\beta\in(F^{r\times})^2$.

Claim 2. We have $\alpha=\pi s_1\cdots s_u$ with π, s_i and u as in the statement.

Proof of Claim 1. We first prove that $(\alpha/\beta)=(\alpha)/(\beta)$ is a square ideal in F^r. Let $\mathfrak{l}$ be any prime of F^r. If $\mathfrak{l}$ is unramified in K^r/F^r, then by (2.3.4), we have $\mathrm{ord}_{\mathfrak{l}}((\beta))\equiv 0 \pmod 2$. So by the definition of α, we have $\mathrm{ord}_{\mathfrak{l}}((\alpha))=0$. If $\mathfrak{l}$ is ramified in K^r/F^r, then there exists $\mathfrak{l}_i$ such that $\mathfrak{l}=\mathfrak{l}_i$, so we get

$$\mathrm{ord}_{\mathfrak{l}}((\alpha))\equiv\mathrm{ord}_{\mathfrak{l}_i}((\beta))\mathrm{ord}_{\mathfrak{l}_i}((\lambda_i))\equiv\mathrm{ord}_{\mathfrak{l}_i}((\beta)) \pmod 2$$

as $n_i=\mathrm{ord}_{\mathfrak{l}_i}((\lambda_i))$ is odd. Therefore, the ideal (α/β) is a square of an ideal $\mathfrak{a}$ in $\mathcal{O}_{F^r}$. Thus $\mathfrak{a}^2$ is generated by the totally positive α/β. So the

ideal class $[\mathfrak{a}]$ is of 2-torsion in $\mathrm{Cl}^+_{F^r}$, which has an odd order, so there is a totally positive element $\mu \in (F^r)^\times$ that generates $\mathfrak{a}$. So $\alpha/\beta = \mu^2 \cdot v$ for some $v \in (\mathcal{O}^\times_{F^r})^+$. Moreover, since $\mathrm{Cl}_{F^r} = \mathrm{Cl}^+_{F^r}$, the norm of the fundamental unit ϵ is negative. Therefore, a unit in $\mathcal{O}_{F^r}$ is totally positive if and only if it is a square in $\mathcal{O}_{F^r}$. Hence v is a square in $\mathcal{O}_{F^r}$ so we get $\alpha/\beta \in (F^{r\times})^2$.

Proof of Claim 2. For any given i, if l_i is inert in $F^r/\mathbb{Q}$, then $n_i = 1$ and $\lambda_i = l_i \in \mathbb{Z}_{>0}$ is prime. If l_i is not inert in $F^r/\mathbb{Q}$ then $l_i \in \{p,\ q\}$, by Proposition 2.3.5. If $l_i = q$, then $\mathfrak{l}_i$ is not ramified in K^r/F^r, otherwise by Corollary 2.3.9 we get $\sqrt{q} \in F$. So $l_i = p$.

Let

$$\{s_1, \ldots, s_u\} = \{l_i \ : l_i \text{ is inert in } F^r/\mathbb{Q} \text{ and ramified in } K^r/F^r \text{ and } \mathrm{ord}_{\mathfrak{l}_i}((\beta)) \equiv 1 \pmod 2\}.$$

Then $u \in \{t_{K^r} - 1,\ t_{K^r} - 2,\ t_{K^r} - 3\}$ by (2.3.4).

Let $p\mathcal{O}_{F^r} = \mathfrak{p}\mathfrak{p}'$. Then we have $\alpha = \pi^a \pi'^{a'} \prod_{i=1}^u s_i^{(1 \pmod 2)}$, where π and π' are totally positive generators of $\mathfrak{p}^j$ and $\mathfrak{p}'^j$ for some odd $j \in \mathbb{Z}_{>0}$. Here, we have $\prod_{i=1}^u s_i^{(1 \pmod 2)} \in \mathbb{Z}$ and $a,\ a' \in \{0,\ 1\}$. If $a = a'$, then $\alpha \in \mathbb{Z}$, which leads to a contradiction since K^r is non-biquadratic. So for a unique $\mathfrak{p}$, we can take $a_1 = 1$ and $a_2 = 0$. In particular, we have $u \in \{t_{K^r} - 1,\ t_{K^r} - 2\}$. □

Combining Proposition 2.3.16 and the bound on the discriminant in Proposition 2.3.14, we now have a good way of listing the fields. Next, we need a fast way of eliminating fields from our list if they have CM class number > 1.

The following lemma is a special case of Theorem D in Louboutin [23].

Lemma 2.3.17. *Let K be a non-biquadratic quartic CM field and let F be its real quadratic subfield. Let d_K and d_F be the absolute values of the discriminants of K and F. Then assuming $I_0(\Phi^r) = I_{K^r}$, if a rational prime l splits completely in $K^r/\mathbb{Q}$, then $l \geq \frac{\sqrt{d_K/{d_F}^2}}{4}$.*

Proof. Let l be a prime that splits completely in $K^r/\mathbb{Q}$. Let $\mathfrak{l}_{K^r}$ be a prime ideal in K^r above l. By the assumption $I_0(\Phi^r) = I_{K^r}$, there exists $\tau \in K^\times$ such that $\mathrm{N}_{\Phi^r}(\mathfrak{l}_{K^r}) = (\tau)$ and $\tau\overline{\tau} = l$. Here $\tau \neq \overline{\tau}$, since

$\sqrt{l} \notin K$. Then since $\mathcal{O}_K \supset \mathcal{O}_F[\tau]$ and $\Delta(\mathcal{O}_F[\tau]/\mathcal{O}_F) = (\tau - \overline{\tau})^2$, we have $d_K/d_F^2 = \mathrm{N}_{F/\mathbb{Q}}(d_{K/F}) = \mathrm{N}_{F/\mathbb{Q}}(\Delta(\mathcal{O}_K/\mathcal{O}_F)) \leq \mathrm{N}_{F/\mathbb{Q}}((\tau-\overline{\tau})^2)$. Moreover, since $\tau\overline{\tau} = l$, we have $\phi(\tau-\overline{\tau})^2 \leq (2\sqrt{l})^2$ for all embeddings $\phi : F \hookrightarrow \mathbb{R}$, hence $d_K/d_F^2 \leq \mathrm{N}_{F/\mathbb{Q}}((\tau-\overline{\tau})^2) \leq 16l^2$. □

Every prime s_i as in Proposition 2.3.16 divides $\Delta(K^r/F^r)$ so $s_i^2 | d_{K^r}$, hence $s_i^4 | d_N$. The primes p and q are ramified in F and F^r, so p^4 and q^4 divide the discriminant d_N of the normal closure N of degree 8. Hence $d_N \geq p^4 q^4 s_1^4 \cdots s_{t-1}^4$.

Algorithm 2.3.18. ***Output:*** *$[D,\ A,\ B]$ representations of all non-normal quartic CM fields K satisfying $I_0(\Phi^r) = I_{K^r}$.*

Step 1. Find all square-free integers smaller than $3 \cdot 10^{10}$ having at most 8 prime divisors and find all square-free integers smaller than 222^2.

Step 2. Order the prime factors of each of these square-free integers as tuples of primes $(p, q, s_1, \ldots, s_u)$ with $s_1 < \cdots < s_u$ in $(u+1)(u+2)$-ways, then take only the tuples satisfying $q \not\equiv 3 \pmod 4$, $(p/q) = (q/p) = 1$ and $(p/s_i) = (q/s_i) = -1$ for all i.

Step 3. For each $(p, q, s_1, \ldots, s_u)$, let $F^r = \mathbb{Q}(\sqrt{q})$, write $p\mathcal{O}_{F^r} = \mathfrak{p}\mathfrak{p}'$, and take $\alpha = \pi \cdot s_1 \cdots s_u \in F^r$, where π is a totally positive generator of $\mathfrak{p}^j$ for the minimal $j \in \mathbb{Z}_{>0}$. Construct $K^r = F^r(\sqrt{-\alpha})$.

Step 4. Eliminate the fields K^r that have totally split primes in K^r below the bound $\sqrt{d_K/d_F^2}/4$.

Step 5. For each $\mathfrak{q}$ with norm Q below $12\log(|d_{K^r}|)^2$, check whether it is in $I_0(\Phi^r)$ as follows. List all quartic Weil Q–polynomials, that is, monic integer polynomials of degree 4 such that all roots in $\mathbb{C}$ have absolute value $\sqrt{Q}$. For each, take its roots in K and check whether $\mathrm{N}_{\Phi^r}(\mathfrak{q})$ is generated by such a root. If not, then $\mathfrak{q}$ is not in $I_0(\Phi^r)$, so we throw away the field.

Step 6. For each K^r, compute the class group of K^r and for a CM type Φ of K test $I_0(\Phi^r)/P_{K^r} = I_{K^r}/P_{K^r}$.

Step 7. Find $[D,\ A,\ B]$ *representations for the reflex fields* K *of the remaining pairs* (K^r, Φ^r).

Proof. Note that Step 4 and Step 5 of the algorithm above do not affect the validity of the algorithm by Lemma 2.3.17. These two steps are only to speed up the computation. In Step 4 we eliminate most of the CM fields.

Suppose that a non-normal quartic CM field K satisfies $I_0(\Phi^r) = I_{K^r}$. Then by Proposition 2.3.16, we have $F = \mathbb{Q}(\sqrt{p})$ and $F^r = \mathbb{Q}(\sqrt{q})$, where p and q are prime numbers with $q \not\equiv 3 \pmod 4$ and $(p/q) = (q/p) = 1$. Also by Proposition 2.3.16, there exist a prime $\mathfrak{p}$ lying above p in F^r that ramifies in K^r and a totally positive element $\alpha = \pi s_1 \cdots s_u$, where π is a totally positive generator of $\mathfrak{p}^j$ for some odd $j \in \mathbb{Z}_{>0}$ such that $K^r = F^r(\sqrt{-\alpha})$. By Proposition 2.3.5, the ramified primes in K^r/F^r that are distinct from $\mathfrak{p}$ are inert in F and F^r. As $s_1, \ldots,\ s_u$ are such primes, we have $(p/s_i) = -1$ and $(q/s_i) = -1$. By Lemma 2.3.14, we have either $h^*_{K^r} = 2^{t_{K^r}-1} \leq 2^5$ and $d_{K^r}/d_{F^r} \leq 3 \cdot 10^{10}$ or $d_N < 222^8$. Therefore, the CM field K is listed. □

We implemented the algorithm in SAGE [36, 33, 42] and obtained the list of the fields in Theorem 2.3.15. The implementation is available online at [17]. This proves Theorems 2.3.15 and 2.1.1. □

This computation takes few weeks on a computer.

Remark 2.3.19. There are no fields eliminated in Step 6, because they turned out to be already eliminated in Step 5.

2.4 Cyclic quartic CM fields

In [31], Murabayashi and Umegaki determined *cyclic* quartic CM fields corresponding to simple CM curves of genus 2 defined over $\mathbb{Q}$. Such fields have CM class number one, however there are more examples, for example, the fields in Table 1b of [9] have CM class number one, but the CM curves corresponding to these cyclic sextic CM fields do not have a model over $\mathbb{Q}$. We apply the strategy in the previous section to cyclic quartic CM fields and list all of those with CM class number one.

Murabayashi [30, Proposition 4.5] proves that the relative class number of cyclic quartic CM fields with CM class number one is 2^{t_K-1}, where t_K is the number of primes in F that are ramified in K. This result also follows from Proposition 2.3.1 in Section 2.3.1.

Suppose that $K/\mathbb{Q}$ is a cyclic quartic CM field with $\mathrm{Gal}(K/\mathbb{Q}) = \langle y \rangle$. Since $K/\mathbb{Q}$ is normal, we consider CM types with values in K. The CM type, up to equivalence, is $\Phi = \{\mathrm{id}, y\}$, which is primitive. The reflex field K^r is K and the reflex type of Φ is the CM type $\{\mathrm{id}, y^3\}$ (Example 8.4(1) of Shimura [40]). In this notation complex conjugation $\bar{\cdot}$ is y^2.

Suppose $K \cong \mathbb{Q}(\zeta_5)$, where ζ_m denotes a primitive m-th root of unity. Then the class group of K is trivial, so the equality $I_0(\Phi^r) = I_K$ holds. Hence $K = \mathbb{Q}(\zeta_5)$ will occur in the list of cyclic quartic CM fields satisfying $I_0(\Phi^r) = I_K$.

From now on, suppose $K \ncong \mathbb{Q}(\zeta_5)$.

Lemma 2.4.1. *(Murabayashi [30], Lemma 4.2) If $I_0(\Phi^r) = I_{K^r}$, then there is exactly one totally ramified prime in $K/\mathbb{Q}$ (i.e., $F = \mathbb{Q}(\sqrt{p})$ with prime $p \not\equiv 3 \pmod 4$) and the other ramified primes of $K/\mathbb{Q}$ are inert in $F/\mathbb{Q}$.* □

Example 2.4.2. *Suppose $I_0(\Phi^r) = I_{K^r}$. The relative class number h_K^* equals 1 if and only if K/F has exactly one ramified prime. This ramified prime is $\sqrt{p}$ when $F = \mathbb{Q}(\sqrt{p})$.*

We now determine such CM fields by using a lower bound on their relative class numbers from analytic number theory.

Theorem 2.4.3. *(Louboutin [24], Theorem 5) Let K be a cyclic quartic CM field of conductor f_K and absolute discriminant d_K. Then we have*

$$h_K^* \geq \frac{2}{3e\pi^2}\left(1 - \frac{4\pi e^{1/2}}{d_K^{1/4}}\right)\frac{f_K}{(\log(f_K) + 0.05)^2}. \tag{2.4.1}$$

□

Proposition 2.4.4. *Let the notation be as above. Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have $h_K^* \leq 2^5$ and $f_K < 2.1 \cdot 10^5$.*

Proof. Under the assumption $I_0(\Phi^r) = I_{K^r}$, Lemma 2.4.1 implies that there is exactly one totally ramified prime in $K/\mathbb{Q}$ and the other ramified primes of $K/\mathbb{Q}$ are inert in $F/\mathbb{Q}$.

Let Δ_t be the product of the first t primes. Since the ramified primes in $K/\mathbb{Q}$ divide the conductor f_K, we have $f_K > \Delta_{t_K}$. Further, by Propositions 11.9 and 11.10 in Chapter VII [32], we have $d_K = f_K^2 \cdot d_F$ so $d_K > \Delta_{t_K}^2$. The right hand side of (2.4.1) is monotonically increasing with $f_K > 2$. Further, by Proposition 2.3.1, we have $h_K^* = 2^{t_K - 1}$ so by dividing both sides of (2.4.1) by 2^{t_K-1}, we obtain

$$1 \geq \frac{2}{3e\pi^2}\left(1 - \frac{4\pi e^{1/2}}{\Delta_{t_K}^{1/2}}\right)\frac{\Delta_{t_K}}{2^{t_K}(\log(\Delta_{t_K}) + 0.05)^2}. \tag{2.4.2}$$

The right hand side of (2.4.2) is monotonically increasing with $t_K \geq 2$, and if $t_K = 7$, then the right hand side is greater than 1. Hence $t \leq 6$. So we get $h_K^* \leq 2^5$, and therefore, we get $f_K < 2.1 \cdot 10^5$. □

Theorem 2.4.5. *There exist exactly* 20 *isomorphism classes of CM class number one cyclic quartic CM fields. The fields are given by* $K \cong \mathbb{Q}[X]/(X^4 + AX^2 + B) \supset \mathbb{Q}(\sqrt{D})$ *where* $[D, A, B]$ *ranges over*

$$[5,5,5],\ [8,4,2],\ [13,13,13],\ [29,29,29],$$

$$[37,37,333],\ [53,53,53],\ [61,61,549]$$

with class number 1*;*

$$[5,65,845],\ [5,85,1445],\ [5,10,20],\ [8,12,18],$$

$$[8,20,50],\ [13,65,325],\ [13,26,52],\ [17,119,3332]$$

with class number 2*;*

$$[5,30,180],\ [5,35,245],\ [5,15,45],\ [5,105,2205],\ [17,255,15300]$$

with class number 4*.*

We begin the proof with the following proposition.

Proposition 2.4.6. *If a cyclic quartic CM field* K *satisfies* $I_0(\Phi^r) = I_K$*, then there exist prime numbers* p*,* $s_1, \ldots, s_u \in \mathbb{Z}$ *such that* $F = \mathbb{Q}(\sqrt{p})$ *with* $p \not\equiv 3 \pmod 4$ *and* $(p/s_i) = -1$ *for all* i*, and we have* $K^r \cong \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u \sqrt{p}})$ *with* $u \in \{t_K - 1,\ t_K - 2\}$ *for every* $\epsilon \in \mathcal{O}_F^\times$ *with* $\epsilon\sqrt{p} \gg 0$*.*

Proof. By Proposition 2.4.1, we have $F = \mathbb{Q}(\sqrt{p})$, where p is a prime with $p \not\equiv 3 \pmod 4$. If there are t_K ramified primes in K/F, the ones that are distinct from the one above p are inert in $F/\mathbb{Q}$, by Proposition 2.4.1; denote them by $s_1, \ldots, s_{t_K}$.

There exists a totally positive element β in $F^\times$ (without loss of generality, we can take β in $\mathcal{O}_F$) such that $K = F(\sqrt{-\beta})$, where β is uniquely defined up to $(F^\times)^2$. As in the proof of Proposition 2.3.16 in the previous section, we will define a totally positive element $\alpha \in F^\times$ with respect to the ramified primes in K/F and show that α and β differ by a factor in $(F^\times)^2$.

Let $\epsilon \in \mathcal{O}_F^\times$ such that $\epsilon\sqrt{p} \gg 0$. Such an element exists since $p \not\equiv 3 \pmod 4$. As β is unique up to squares and we can take $\mathfrak{l}$-minimal $\beta' \in \beta(F^\times)^2$ for each prime $\mathfrak{l}$ of $\mathcal{O}_F$, then we get the cases in (2.3.4) for $\mathrm{ord}_{\mathfrak{l}}((\beta))$.

If $p \neq 2$ and the prime (2) in $\mathcal{O}_F$ is ramified in K/F with $\mathrm{ord}_{(2)}((\beta)) \equiv 0 \pmod 2$, then take $\alpha := \epsilon s_1 \cdots s_u\sqrt{p}$ with $u = t_K - 2$. If $p = 2$ and $\mathrm{ord}_{(\sqrt{2})}((\beta)) \equiv 0 \pmod 2$, then take $\alpha := s_1 \cdots s_u$ with $u = t_K - 1$. For all other cases in (2.3.4), take $\alpha := \epsilon s_1 \cdots s_u\sqrt{p}$ with $u = t_K - 1$.

By the definition of α, for all ideals $\mathfrak{l} \subset \mathcal{O}_F$ we have $\mathrm{ord}_{\mathfrak{l}}((\alpha/\beta)) \equiv 0 \pmod 2$. So $(\alpha/\beta) = \mathfrak{a}^2$ for a fractional $\mathcal{O}_F$-ideal $\mathfrak{a}$. The ideal $\mathfrak{a}$ is a 2-torsion element in Cl_F. Moreover, since $F = \mathbb{Q}(\sqrt{p})$ with $p \not\equiv 3 \pmod 4$, genus theory implies that $\mathrm{Cl}_F = \mathrm{Cl}_F^+$ has odd order. Therefore, there is a totally positive element μ that generates $\mathfrak{a}$. So $\alpha/\beta = \mu^2 \cdot v$ for some $v \in \mathcal{O}_F^+$. Furthermore, since $\mathrm{Cl}_F = \mathrm{Cl}_F^+$, the fundamental unit has a negative norm, and so $\mathcal{O}_F^+ = (\mathcal{O}_F)^2$. Hence v is a square in $\mathcal{O}_F$, and therefore we get $\alpha/\beta \in (F^\times)^2$.

In the case $p = 2$ and $\mathrm{ord}_{(\sqrt{2})}((\beta)) \equiv 0 \pmod 2$, we get the biquadratic field $K = F(\sqrt{-s_1 \cdots s_u})$ over $\mathbb{Q}$, contradiction. Therefore, we have

$$K = \mathbb{Q}(\sqrt{-\epsilon s_1 \cdots s_u\sqrt{p}}) \text{ with } u \in \{t_{K-1},\ t_{K-2}\}.$$

□

Algorithm 2.4.7. ***Output:*** *$[D,\ A,\ B]$ representations of all cyclic quartic CM fields K satisfying $I_0(\Phi^r) = I_K$.*

Step 1. Find all square-free integers less than $2.1 \cdot 10^5$ and having at most 6 prime divisors.

Step 2. *Order the prime factors of each of these square-free integers as tuples of primes $(p, s_1, \ldots, s_u)$ with $s_1 < \ldots < s_u$ in $(u+1)$-ways, then take only the tuples satisfying $p \not\equiv 3 \pmod 4$ and $(p/s_i) = -1$ for all i.*

Step 3. *For each $(p, s_1, \ldots, s_u)$, let $F = \mathbb{Q}(\sqrt{p})$ and take a totally positive element $\alpha = \epsilon s_1 \cdots s_u \sqrt{p}$, where ϵ is a fundamental unit in F such that $\epsilon\sqrt{p} \gg 0$. Construct $K = F(\sqrt{-\alpha})$.*

Step 4. *Eliminate the fields K that have totally split primes in K below the bound $\sqrt{d_K/d_F^2}/4$. (In this step we eliminate most of the CM fields.)*

Step 5. *For each $\mathfrak{q}$ with norm Q below $12\log(|d_{K^r}|)^2$, check whether it is in $I_0(\Phi^r)$ as follows. List all quartic Weil Q-polynomials, that is, monic integer polynomials of degree 4 such that all roots in $\mathbb{C}$ have absolute value $\sqrt{Q}$. For each, take its roots in K and check whether $\mathrm{N}_{\Phi^r}(\mathfrak{q})$ is generated by such a root. If not, then $\mathfrak{q}$ is not in $I_0(\Phi^r)$, so we throw away the field.*

Step 6. *For each K compute the class group of the fields K and for a primitive CM type Φ of K test $I_0(\Phi^r)/P_K = I_K/P_K$.*

Step 7. *Find $[D,\ A,\ B]$ representations for the quartic CM class number one fields K.*

Proof. The idea of the proof of this algorithm is exactly as the proof of Algorithm 2.3.18. In this algorithm, Step 1 follows from Proposition 2.4.4; Step 2 and 3 follow from Proposition 2.4.6; Step 4 follows from Lemma 2.3.17. □

We implemented the algorithm in SAGE [36, 33, 42] and obtained the list of the fields in Theorem 2.4.5. The implementation is available online at [17]. This proves Theorems 2.1.2 and 2.4.5. □

This computation takes few days on a computer.

Chapter 3

The CM class number one problem for curves of genus 3

ABSTRACT. In this chapter, we give the complete list of CM class number one Galois sextic fields, and under GRH, the complete list of CM class number one non-normal sextic CM fields containing an imaginary quadratic field. We will see in Chapter 4 that the first list is the complete list of CM fields corresponding to CM curves of genus 3 *with rational field of moduli.*

3.1 Introduction

Let K be a sextic CM field and let Φ be a primitive CM type of K. Further, let C be a curve of genus 3 with a simple Jacobian $J(C)$ over $\mathbb{C}$ of type (K,Φ) with CM by $\mathcal{O}_K$. Let (K^r,Φ^r) be the reflex of (K,Φ). Recall that Theorem 1.5.6 implies that if C is defined over the reflex field K^r, then

$$\begin{aligned} I_0(\Phi^r) &:= \{\mathfrak{b} \in I_{K^r} : \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\alpha) \text{ and } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b}) = \alpha\overline{\alpha} \text{ for some } \alpha \in K^\times\} \\ &= I_{K^r}. \end{aligned}$$

We say that K is a *CM class number one field* if there exists a primitive CM type Φ such that (K,Φ) has $I_0(\Phi^r) = I_{K^r}$. In this chapter, we

will list CM class number one sextic fields by using a similar strategy as in Chapter 2.

We will restrict ourselves to the fields K that contain an imaginary quadratic field. This restriction is not too bad because it covers the most interesting cases:

- CM fields with known explicit CM constructions of genus-3 CM curves:
  - hyperelliptic curves with $K \supset \mathbb{Q}(i)$, Weng [48],
  - Picard curves, Koike and Weng [19],
- all cases where K is Galois over $\mathbb{Q}$ see Section 3.3,
- all CM curves of genus 3 over $\mathbb{Q}$ (see Chapter 4).

Remark 3.1.1. Dodson [12, Section 5.1.1] gives the Galois groups of the remaining sextic CM fields K, i.e., those that do not contain an imaginary quadratic field. For those fields, $K/\mathbb{Q}$ is not normal and the Galois group of a normal closure of K is isomorphic to $(C_2)^3 \rtimes G_0$, where $G_0 \in \{C_3,\ S_3\}$ acts on $(C_2)^3$ by permuting the indices.

Let K be a sextic CM field containing an imaginary quadratic field k and let F be the totally real cubic subfield of K. Since k and F are linearly disjoint over $\mathbb{Q}$, we have $K = Fk$. Totally real cubic fields F are either cyclic or non-normal over $\mathbb{Q}$. If F is non-normal, then the normal closure N_+ of F is a totally real field with Galois group isomorphic to S_3. Let N be a Galois closure of K. Then we have $\mathrm{Gal}(N/\mathbb{Q}) = \mathrm{Gal}(N_+/\mathbb{Q}) \times \mathrm{Gal}(k/\mathbb{Q})$, see Lang [22, Theorem 1.14 in IV]. In particular, we have either $\mathrm{Gal}(N/\mathbb{Q}) = C_3 \times C_2 \cong C_6$ or $\mathrm{Gal}(N/\mathbb{Q}) = S_3 \times C_2 \cong D_6$. Note that N_+ is the maximal totally real subfield of N, whence our notation.

In Section 3.3, we will consider the case that $K/\mathbb{Q}$ is Galois and prove the following.

Theorem 3.1.2. *There exist exactly* 37 *isomorphism classes of cyclic sextic CM fields K such that there exists a primitive CM type Φ satisfying $I_0(\Phi^r) = I_{K^r}$. These fields are exactly the fields listed in Table 3.1.*

In Section 3.4, non-normal sextic CM fields will be considered and the following will be proved.

Theorem 3.1.3. *Assuming GRH, the complete list of the isomorphism classes of CM class number one non-normal sextic CM fields containing an imaginary quadratic field is given in Tables 3.3–3.12.*

3.2 Sextic CM fields containing an imaginary quadratic field

The main result of this section is the following. We will use this result in Sections 3.3 and 3.4 to prove Theorems 3.1.2 and 3.1.3.

Proposition 3.2.1. *Let K be a sextic CM field and let Φ be a CM type of K. Let (K^r, Φ^r) be the reflex of (K, Φ). Suppose that $K^r \cong K$. If K contains a class number one imaginary quadratic field k and $h_K^* = 2^{t_K - 1}$, then*

$$\begin{aligned} I_0(\Phi^r) &:= \{\mathfrak{b} \in I_{K^r} : \mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\alpha) \text{ and } \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{b}) = \alpha\overline{\alpha} \text{ for some } \alpha \in K^\times\} \\ &= I_{K^r}. \end{aligned}$$

Lemma 3.2.2. *Let K be a sextic CM field containing an imaginary quadratic field k. Then we have*

$$\mathcal{O}_K^\times = W_K \mathcal{O}_F^\times,$$

where W_K is the group of roots of unity of K.

Proof. This follows from Theorem 5-(i) in Louboutin, Okazaki, Olivier [27]. □

Lemma 3.2.3. *Let K be a sextic CM field containing an imaginary quadratic field k and Φ be a CM type of K. Let F be totally cubic subfield of K. Put $I_K^H = \{\mathfrak{b} \in I_K \mid \overline{\mathfrak{b}} = \mathfrak{b}\}$, where $H := \mathrm{Gal}(K/F)$. Then we have*

$$h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K].$$

Proof. Lemma 2.2.2 tells us that if $\mathcal{O}_K^\times = W_K \mathcal{O}_F^\times$, then $h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K]$. Combine this with Lemma 3.2.2. □

Proof of Proposition 3.2.1. Identify K with K^r via an isomorphism. By Lemma 3.2.3, we have

$$h_K^* = 2^{t_K - 1} \text{ if and only if } I_K = I_K^H P_K.$$

For any $\mathfrak{b} \in \mathrm{I}_F$, we have $\mathrm{N}_{\Phi^r}(\mathfrak{b}) = (\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{b}))$, where $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{b}) \in \mathbb{Z}$. Hence $I_F P_K \subset I_0(\Phi^r)$. We can see from the exact sequence (2.2.1)

$$1 \to I_F \to I_K^H \to \bigoplus_{\mathfrak{p} \text{ prime of } F} \mathbb{Z}/e_{K/F}(\mathfrak{p})\mathbb{Z} \to 1$$

that the elements of I_K^H / I_F are represented by the products of the primes in K that are ramified in K/F. For any such prime $\mathfrak{P}$, let $\mathfrak{p}\mathbb{Z} = \mathfrak{P} \cap F$ and $p = \mathfrak{p} \cap \mathbb{Q}$. Then the following holds

$$\mathrm{N}_{\Phi^r}(\mathfrak{P})^2 = \mathrm{N}_{\Phi^r}(\mathfrak{p}\mathcal{O}_K) = \mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K, \tag{3.2.1}$$

where $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p}) \in \{p,\ p^2, p^3\}$ depending on the splitting behavior of p in F.

The prime $\mathfrak{P}$ lies over a rational prime p that is ramified in k, see Lang [21, Proposition 4.8-(ii) in II]. Moreover, the prime p is the unique ramified prime in $k/\mathbb{Q}$. Indeed, by genus theory, if the class number of an imaginary quadratic field k is odd then there is one and only one ramified prime in $k/\mathbb{Q}$. By (3.2.1), we have

$$\mathrm{N}_{\Phi^r}(\mathfrak{P}) = \sqrt{\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p})\mathcal{O}_K}. \tag{3.2.2}$$

If $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p}) = p$, then the right hand side of (3.2.2) is generated by $\sqrt{-p}$ if $k \ncong \mathbb{Q}(i)$ and generated by $i+1$ if $k \cong \mathbb{Q}(i)$. Therefore, in both cases we have a generator π in k of $\mathrm{N}_{\Phi^r}(\mathfrak{P})$ such that $\pi\overline{\pi} \in \mathbb{Q}$. Similarly, in cases $\mathrm{N}_{F/\mathbb{Q}}(\mathfrak{p}) = p^2$ or p^3, there exists a generator π in k of $\mathrm{N}_{\Phi^r}(\mathfrak{P})$ such that $\pi\overline{\pi} \in \mathbb{Q}$.

Hence every element of $I_K^H P_K$, which is I_K, is in $I_0(\Phi^r)$. In particular, we get $I_K = I_0(\Phi^r)$. □

3.3 Cyclic sextic CM fields

In this section, we will prove Theorem 3.1.2. We begin with proving the following proposition which is the main ingredient of the proof of Theorem 3.1.2.

Proposition 3.3.1. *Let K be a cyclic sextic CM field with a primitive CM type Φ. It holds $I_0(\Phi^r) = I_{K^r}$ if and only if $h_K^* = 2^{t_K - 1}$ and $h_k = 1$, where t_K is the number of primes in F that are ramified in K.* □

Let K be a cyclic sextic CM field with $G := \mathrm{Gal}(K/\mathbb{Q}) = \langle y \rangle$. In this notation, complex conjugation $\bar{\cdot}$ is y^3. Then K has a totally real cubic subfield F and an imaginary quadratic subfield k. So $K = kF$.

Proposition 3.3.2. *Given (K, Φ) such that K is a cyclic sextic CM field and Φ is a primitive CM type of K with values in N'. There is an embedding $K \hookrightarrow N'$ such that Φ is $\{\mathrm{id},\ y,\ y^{-1}\}$. Moreover, we then have $K^r = K$ and $\Phi^r = \Phi$.*

Proof. There are 2^3 CM types of K with values in N'. Two of them are induced by the CM types of k and the remaining six are primitive. For simplicity, we consider CM types with values in K. In other words, we identify K with a subfield of N'. The CM type $\{\mathrm{id},\ y,\ y^{-1}\}$ of K is primitive by Corollary 1.2.4 and if we translate this type with the elements of $\mathrm{Gal}(K/\mathbb{Q})$, we get six equivalent primitive CM types. Hence by changing the embedding $K \hookrightarrow N'$, without loss of generality, we have $\Phi = \{\mathrm{id},\ y,\ y^{-1}\}$.

Since K is normal and Φ is primitive, the reflex field K^r is K. Moreover, the reflex type Φ^r is $\Phi^{-1} = \Phi$. □

We now prove the converse of Proposition 3.2.1 for cyclic sextic CM fields.

Proposition 3.3.3. *Let K be a cyclic sextic CM field with a primitive CM type Φ. Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have $h_k = 1$.*

Proof. As K has degree 6, the order μ_K of the group of roots of unity W_K of K is 2, 4, 6, 14, or 18 and it is greater than 2 only if $k = \mathbb{Q}(\sqrt{-d})$

with $d = 1$ 3, 7, or 3 respectively, so in that case we are done as $h_k = 1$ if $d = 1$ 3, or 7. We now suppose $W_K = \{\pm 1\}$.

For any $\mathfrak{a} \in I_k$, we have

$$\mathrm{N}_{\Phi^r}(\mathfrak{a}\mathcal{O}_K) = \mathfrak{a}\overline{\mathfrak{a}}^2\mathcal{O}_K = \overline{\mathfrak{a}}\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_K.$$

Then by the assumption $I_0(\Phi^r) = I_K$, we have $\mathfrak{a}\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_K = \pi\mathcal{O}_K$ for some $\pi \in K^\times$ such that $\pi\overline{\pi} \in \mathbb{Q}$. Let $\nu = \pi/\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a})$. Then $\nu\overline{\nu} \in \mathbb{Q}$ and $\nu\mathcal{O}_K = \mathfrak{a}\mathcal{O}_K$. This makes ν unique up to a root of unity hence up to a sign.

The map $\phi : \mathrm{Gal}(K/k) \to \{\pm 1\}$ given by $\phi(\sigma) = \sigma(\nu)/\nu$ is a homomorphism. Since the order of $\mathrm{Gal}(K/k)$ is 3, the map ϕ is trivial. Hence $\sigma(\nu) = \nu$ for every $\sigma \in \mathrm{Gal}(K/k)$. This implies $\nu \in k^\times$ and hence $\mathfrak{a}$ is principal in k. As $\mathfrak{a}$ was arbitrary, we then have $h_k = 1$.

□

Remark 3.3.4. It is known that the imaginary quadratic fields with *class number one* are $k = \mathbb{Q}(\sqrt{-d})$ with $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$ (see Baker, Heegner, and Stark [2, 16, 41]).

Proposition 3.3.5. *Let K be a cyclic sextic CM field and let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have $h_K^* = 2^{t_K - 1}$, where t_K is the number of primes in F that are ramified in K.*

Proof. Recall that without loss of generality we have $\Phi = \{\mathrm{id},\ y,\ y^{-1}\}$ and $K^r = K$. By Lemma 3.2.3, we have $h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K]$, where $I_K^H = \{\mathfrak{b} \in I_K \mid \overline{\mathfrak{b}} = \mathfrak{b}\}$. So it is enough to show $[I_K : I_K^H P_K] = 1$ under the assumption $I_0(\Phi^r) = I_{K^r}$. For any $\mathfrak{b} \in I_K$, we have the following equality

$$\mathrm{N}_{\Phi^r}(y^{-1}(\mathfrak{b})/y^{-2}(\mathfrak{b})) = \mathfrak{b}\overline{\mathfrak{b}}^{-1}.$$

By the assumption $I_0(\Phi^r) = I_{K^r}$, we get $\mathfrak{b}\overline{\mathfrak{b}}^{-1} = (\beta)$, where $\beta \in K^\times$ and $\beta\overline{\beta} \in \mathbb{Q}$. Here we have $(\beta\overline{\beta}) = (\mathrm{N}_{K^r/\mathbb{Q}}((y^{-1}\mathfrak{b})/(y^{-2}\mathfrak{b}))) = (1)$, by the property of the type norm in Proposition 1.2.6 hence $\beta\overline{\beta} = 1$.

Then the proof continues as in the proof of Lemma 2.2.3: there is a $\gamma \in K^\times$ such that $\beta = \overline{\gamma}\gamma^{-1}$ by Hilbert's Theorem 90. Thus we have $\mathfrak{b} = \overline{\gamma\mathfrak{b}} \cdot (\frac{1}{\gamma}) \in I_K^H P_K$ and therefore $I_K = I_K^H P_K$. □

Proof of Proposition 3.3.1. It follows from Propositions 3.2.1, 3.3.2, 3.3.3, and 3.3.5. □

Theorem 3.1.2. *There exist exactly* 37 *isomorphism classes of cyclic sextic CM fields K such that there exists a primitive CM type Φ satisfying $I_0(\Phi^r) = I_{K^r}$. These fields are exactly the fields listed in Table 3.1.*

Proof. By Proposition 3.3.1, we have

$$I_0(\Phi^r) = I_{K^r} \text{ if and only if } h_K^* = 2^{t_K - 1} \text{ and } h_k = 1.$$

If $h_k = 1$, then there is only one ramified prime in k, say p. Under the assumption $I_0(\Phi^r) = I_{K^r}$, we have $h_k = 1$ and hence all ramified primes in K/F lie over p (see Proposition 4.8-(ii) in II of Lang [21]). So if $I_0(\Phi^r) = I_{K^r}$, then we have $t_K \leq 3$ and therefore, we get $h_K^* = 2^{t_K - 1} \leq 2^2$. Thanks to Park and Kwon [34], we have the list of cyclic sextic CM fields with $h_K^* \leq 4$. And of all the sextic cyclic CM fields listed in Table 3 in Kwon and Park [34], those that satisfy $h_K^* = 2^{t_K - 1}$ and $h_k = 1$ are listed in Table 3.1. □

In Table 3.1, K is a cyclic sextic CM field that contains an imaginary quadratic field k, and F is the totally real cubic subfield that is defined as being the splitting field of an irreducible monic polynomial $p(X)$. Furthermore, d_k is the absolute value of the discriminant of k and h_F is the class number of F. In column C some CM fields have $*$, this indicates that a rational model of the corresponding CM curve is known, see Section 4.4.

Table 3.1: All CM class number one cyclic sextic CM fields

$h_K^* = 1$							
d_k	$p(X)$	h_F	C	$\lvert d_k\rvert$	$p(X)$	h_F	C
3	X^3+X^2-4X+1	1	*	7	X^3-3X-1	1	
3	X^3+X^2-2X-1	1	*	7	$X^3+8X^2-51X+27$	3	
3	X^3-3X-1	1	*	7	X^3+6X^2-9X+1	3	
3	$X^3+X^2-10X-8$	1	*	7	$X^3+X^2-30X+27$	3	
3	$X^3+X^2-14X+8$	1	*	7	$X^3+4X^2-39X+27$	3	
3	$X^3+3X^2-18X+8$	3		8	X^3+X^2-4X+1	1	
3	X^3+6X^2-9X+1	3		8	X^3+X^2-2X-1	1	
3	$X^3+3X^2-36X-64$	3		11	X^3+X^2-2X-1	1	
4	X^3+2X^2-5X+1	1	*	19	X^3+2X^2-5X+1	1	
4	X^3-3X-1	1	*	19	$X^3+9X^2-30X+8$	3	
4	X^3+X^2-2X-1	1	*	19	$X^3+7X^2-66X-216$	3	
7	X^3+X^2-4X+1	1		43	$X^3+X^2-14X+8$	1	
7	X^3+X^2-2X-1	1	*	67	$X^3+2X^2-21X-27$	1	

$h_K^* = 4$							
d_k	$p(X)$	h_F	C	d_k	$p(X)$	h_F	C
3	$X^3+4X^2-15X-27$	1		7	X^3+2X^2-5X+1	1	
3	$X^3+2X^2-21X-27$	1		8	$X^3+X^2-10X-8$	1	
4	$X^3+X^2-14X+8$	1		11	$X^3+X^2-14X+8$	1	
4	$X^3+X^2-10X-8$	1	*	11	X^3+2X^2-5X+1	1	
4	$X^3+3X^2-18X+8$	3		19	X^3-3X-1	1	
7	$X^3+X^2-24X-27$	1					

3.4 Non-normal sextic CM fields

In this section, we will prove Theorem 3.1.3. As in Section 3.3, we begin with proving the following proposition, which is the analogue of Proposition 3.3.1 in the case of non-normal sextic CM fields.

Proposition 3.4.1. *Let K be a non-normal sextic CM field containing an imaginary quadratic field k. Let Φ be a primitive CM type of K. Let F be the totally real cubic subfield of K. Then $I_0(\Phi^r) = I_{K^r}$ holds if and only if $h_K^* = 2^{t_K-1}$ and $h_k = 1$, where t_K is the number of primes in F that are ramified in K.*

Let K be a non-normal sextic CM field containing $\mathbb{Q}(\sqrt{-d})$, where $d \in \mathbb{Z}_{>0}$. The normal closure N of K is a dihedral CM field of degree 12

with Galois group $G := \mathrm{Gal}(N/\mathbb{Q}) = \langle x,\ y : y^6 = x^2 = 1,\ xyxy = 1\rangle$, where $\langle x\rangle$ fixes K. The complex conjugation $\bar{\cdot}$ is y^3 in this notation. The normal closure of F is the maximal totally real subfield N_+ of N, which is fixed by $\langle y^3\rangle$. We have the following diagram of some of the subfields of N.

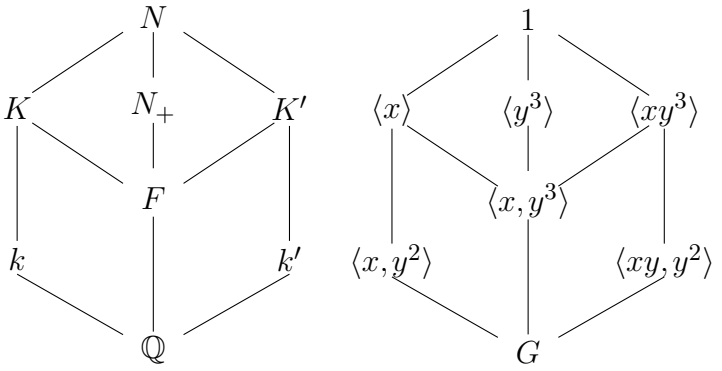


Figure 3.1: Some subfields and subgroups

The extension N/F is biquadratic, and the extensions N/k, N/k' and $N_+/\mathbb{Q}$ are dihedral Galois of degree 6.

Let N' be a number field that contains a subfield isomorphic to N.

Proposition 3.4.2. *Given (K, Φ) such that K is a non-normal sextic CM field that contains an imaginary quadratic subfield and Φ is a primitive CM type of K with values in N'. There is an embedding $N \hookrightarrow N'$ such that Φ is $\{\mathrm{id},\ y|_K,\ y^{-1}|_K\}$. Moreover, the reflex field K^r is K and the reflex type Φ^r is Φ.*

Proof. There are 2^3 CM types of K with values in N'. Two of them are induced by the CM types of k. The remaining six are primitive. For simplicity, we consider CM types with values in N. In other words, we identify N with a subfield of N'. The CM type $\{\mathrm{id},\ y|_K,\ y^{-1}|_K\}$ of K is primitive by Proposition 1.2.3 and if we translate this type with the elements of the unique cyclic subgroup of order 6, we get six equivalent primitive CM types. Hence by changing the embedding $N \hookrightarrow N'$ by an appropriate power of y, without loss of generality, we have $\Phi = \{\mathrm{id},\ y|_K,\ y^{-1}|_K\}$.

The CM type $\Phi_N = \{\mathrm{id}, y, y^{-1}, x, xy, xy^{-1}\}$ of N is induced by the CM type Φ. By definition (see page 5), the reflex field K^r is the fixed

field of $\{\gamma : \gamma \in \mathrm{Gal}(N/\mathbb{Q}),\ \Phi_N^{-1}\gamma = \Phi_N^{-1}\} = \langle x \rangle$. Hence the reflex field K^r is K and the reflex type Φ^r is Φ. □

Proposition 3.4.3. *Let K be a non-normal sextic CM field containing an imaginary quadratic field and let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then $h_K^* = 2^{t_K - 1}$, where t_K is the number of primes in F that are ramified in K.*

Proof. The idea is similar to the proof of Proposition 3.3.5.

Put $I_K^H = \{\mathfrak{b} \in I_K \mid \overline{\mathfrak{b}} = \mathfrak{b}\}$ and $P_K^H = P_K \cap I_K^H$, where $H := \mathrm{Gal}(K/F)$. Then by Lemma 3.2.3 we have

$$h_K^* = 2^{t_K - 1}[I_K : I_K^H P_K].$$

On the other hand, Lemma 2.2.3 tells us the following. If for every $\mathfrak{b} \in I_K$, we have

$$\mathrm{N}_{\Phi^r}\mathrm{N}_{\Phi}(\mathfrak{b}) = (\beta)\mathfrak{b}\overline{\mathfrak{b}}^{-1} \text{ and } \beta\overline{\beta} \in \mathbb{Q} \tag{3.4.1}$$

with $\beta \in K^\times$, then $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)]$.

Without loss of generality, we can take $\Phi = \{\mathrm{id},\ y|_K,\ y^{-1}|_K\}$. Then for any $\mathfrak{a} \in I_K$, we have the following equality

$$\mathrm{N}_{\Phi^r}\mathrm{N}_{\Phi}(\mathfrak{a}) = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\mathrm{N}_{\Phi^r}(\mathfrak{a})\mathfrak{a}\overline{\mathfrak{a}}^{-1}. \tag{3.4.2}$$

By the assumption $I_0(\Phi^r) = I_{K^r}$, there exists $\alpha \in K^\times$ such that $\mathrm{N}_{\Phi^r}(\mathfrak{a}) = (\alpha)$ and $\alpha\overline{\alpha} \in \mathbb{Q}$. Moreover, the assumption $I_0(\Phi^r) = I_{K^r}$ also implies that there is a $\beta \in K^\times$ such that $\mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})\mathfrak{a}\overline{\mathfrak{a}}^{-1}(\alpha) = (\beta)$ and $\beta\overline{\beta} \in \mathbb{Q}$. So the CM type (K, Φ) satisfies (3.4.1), by the assumption $I_0(\Phi^r) = I_{K^r}$. Therefore, Lemma 2.2.3 implies $[I_K : I_K^H P_K] \leq [I_{K^r} : I_0(\Phi^r)] = 1$. Hence the result follows. □

Proposition 3.4.4. *Let K be a non-normal sextic CM field and let k be an imaginary quadratic field such that K contains k. Let Φ be a primitive CM type of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then we have either*

(i) $k = \mathbb{Q}(\sqrt{-d})$ with $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$ or

(ii) $k=\mathbb{Q}(\sqrt{-d})$ *with* $d\in\{23,\ 31,\ 59,\ 83,\ 107,\ 139,\ 211,\ 283,\ 307,\ 331,\ 379,\ 499,\ 547,\ 643,\ 883,\ 907\}$ *and for every* $[\mathfrak{a}]\in \mathrm{Cl}_k$ *of order* 3*, we have* $K=k(\sqrt[3]{\alpha})$ *for all* $\alpha\in k$ *such that* $\mathfrak{a}^3=(\alpha)$.

Proof. By Baker, Heegner, Stark [2, 16, 41], the list *(i)* consists of all imaginary quadratic fields whose class number is 1 and by Arno [1], the list *(ii)* consists of all imaginary quadratic fields whose class number is 3.

Let N, K, F, k, and k' be as in Figure 3.1. Denote the Galois group of $N/\mathbb{Q}$ by G. Without loss of generality, we can take $\Phi=\{\mathrm{id},\ y|_K,\ y^{-1}|_K\}$ and $K^r=K$. Given $\mathfrak{a}\in I_k$, we have

$$\begin{aligned}\mathrm{N}_{\Phi^r}(\overline{\mathfrak{a}}\mathcal{O}_{K^r})\mathcal{O}_N &= (\overline{\mathfrak{a}}\mathcal{O}_N)y(\overline{\mathfrak{a}}\mathcal{O}_N)y^{-1}(\overline{\mathfrak{a}}\mathcal{O}_N)\\ &= \mathfrak{a}^2\overline{\mathfrak{a}}\mathcal{O}_N=\mathfrak{a}\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_N.\end{aligned}$$

Then by the assumption $I_0(\Phi^r)=I_K$, we have $\mathfrak{a}\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a})\mathcal{O}_N=\pi\mathcal{O}_N$ for some $\pi\in K^\times$ such that $\pi\overline{\pi}\in\mathbb{Q}$.

Let $\nu=\pi/\mathrm{N}_{k/\mathbb{Q}}(\mathfrak{a})$. Then $\nu\overline{\nu}\in\mathbb{Q}$ and $\nu\mathcal{O}_N=\mathfrak{a}\mathcal{O}_N$. We would like to imitate the proof of Proposition 3.3.3 and show $\nu\in k^\times$ in order to conclude $h_k=1$. Since K is the field fixed by $\langle x\rangle$, to show that ν is fixed by $\mathrm{Gal}(N/k)=\langle x,\ y^2\rangle$ it would be enough to prove $y^2\nu=\nu$.

However, we cannot prove this. Instead we will show that if $h_k\neq 1$, then $h_k=3$ and $K=k(\sqrt[3]{\alpha})$, where $(\alpha)=\mathfrak{a}^3$ for every ideal class $[\mathfrak{a}]\in\mathrm{Cl}_k$ with order 3.

Suppose that $h_k\neq 1$.

Claim 1. The subgroup $\langle y^2\rangle\subset G$ fixes all elements of the group W_N of roots of unity.

Proof. Suppose that $\mu_N=m$. Then $\mathbb{Q}(\zeta_m)$ is contained in the maximal abelian subfield M of N. Since the Galois group of M is $G/[G,G]\cong\langle x,y\rangle/\langle y^2\rangle$, every element in W_N is fixed by $\langle y^2\rangle$. This proves the claim.

The map $\phi:\langle y^2\rangle\to W_N$ given by $\phi(y^2)=(y^2\nu)/\nu$ is a 1-cocyle. But y^2 acts trivially as $y^2|_M$ is the identity map, hence ϕ is a homomorphism. It depends only on $\mathfrak{a}$ because y^2 fixes the elements of W_N. So we denote this homomorphism ϕ by $\phi_{\mathfrak{a}}$.

Claim 2. The map

$$\begin{aligned}\psi: I_k &\to \mathrm{Hom}(\langle y^2\rangle, W_N)\\ \mathfrak{a} &\mapsto \phi_{\mathfrak{a}}\end{aligned}$$

is a homomorphism and induces an injective homomorphism from the class group Cl_k to $\mathrm{Hom}(\langle y^2\rangle, W_N)$.
Proof. For $i=1,\ 2$ let $\mathfrak{a}_i$ be a fractional ideal of I_k and ν_i be an element in $K^\times$ such that $\mathfrak{a}_i\mathcal{O}_N = \nu_i\mathcal{O}_N$ and $\nu_i\overline{\nu}_i \in \mathbb{Q}$. We have

$$\begin{aligned}\psi(\mathfrak{a}_1\mathfrak{a}_2)(y^2) = (y^2(\nu_1\nu_2))/\nu_1\nu_2 &= ((y^2\nu_1)/\nu_1)((y^2\nu_2)/\nu_2)\\ &= (\psi(\mathfrak{a}_1)\psi(\mathfrak{a}_2))(y^2),\end{aligned}$$

hence ψ is a homomorphism. Moreover, we clearly have $P_k \subset \ker\psi$. On the other hand, if $\mathfrak{a} \in \ker\psi$, then $\psi(\mathfrak{a})$ is the identity homomorphism and so ν is fixed by y^2. This implies that ν is fixed by $\mathrm{Gal}(N/k)$ as $\nu \in K$ is also fixed by x. So we have $\nu \in k$, and hence $\mathfrak{a} \in P_k$. Then the isomorphism theorem proves the claim.

Since the order of $\langle y^2\rangle$ is 3, the order of the image of ψ is divisible by 3. So h_k divides 3 and since we assumed $h_k \neq 1$, we get $h_k = 3$. For every generator $[\mathfrak{a}]$ of Cl_k, there is $\nu \in K^\times$ and $\alpha \in k$ such that $\mathfrak{a}^3 = \alpha\mathcal{O}_k$, $\nu = \mathfrak{a}\mathcal{O}_K$ and $\nu_i\overline{\nu}_i \in \mathbb{Q}$. Hence $\nu^3 = \alpha$ up to a root of unity in K, so up to ± 1. So $\nu = \sqrt[3]{\alpha} \in K$ and hence we have $K = k(\sqrt[3]{\alpha})$.

Therefore, we proved that the imaginary quadratic field in a sextic non-normal CM field satisfying $I_0(\Phi^r) = I_{K^r}$ is one of the fields in the proposition. □

Proposition 3.4.5. *None of the fields K in (ii) in Proposition 3.4.4 are sextic CM fields with CM class number one.*

Proof. Let k be any of the imaginary quadratic fields in *(ii)* in Proposition 3.4.4. For a generator $[\mathfrak{a}]$ of Cl_k such that $\mathfrak{a}^3 = \alpha\mathcal{O}_k$, we let $K = k(\sqrt[3]{\alpha})$. Let F be the maximal totally real subfield of the CM field K. A direct computation gives $h_K^* \neq 2^{t_K-1}$, therefore, by Proposition 3.4.3, the CM field K is not a CM class number one field. □

Proof of Proposition 3.4.1. If $I_0(\Phi^r) = I_{K^r}$, then by Proposition 3.4.3 we have $h_K^* = 2^{t_K-1}$, and by Propositions 3.4.4 and 3.4.5 we have that the imaginary quadratic fields is as required.

Conversely, if k is one of the imaginary quadratic fields in the proposition and $h_K^* = 2^{t_K-1}$, then by Propositions 3.2.1 and 3.4.2 we have $I_0(\Phi^r) = I_{K^r}$. □

By combining the following two theorems, under GRH, we give a lower bound for the relative class number h_K^* of a non-normal sextic CM field K containing an imaginary quadratic field. Then using this result, under GRH, we give an upper bound on the discriminant of the totally real cubic subfield F of a *CM class number one* non-normal sextic CM field K, see Proposition 3.4.9.

Theorem 3.4.6. *(Louboutin [25, Theorem 2]) If F is a totally real cubic number field, then*

$$\mathrm{Res}_{s=1}(\zeta_F) \leq \frac{1}{8}\log^2 d_F,$$

where ζ_F is the Dedekind zeta function and d_F is the discriminant. □

Theorem 3.4.7. *(J. Oesterlé) For any number field K different from $\mathbb{Q}$ for which the Riemann Hypothesis for the Dedekind zeta function ζ_K holds, we have*

$$\mathrm{Res}_{s=1}(\zeta_K) \geq \frac{e^{-3/2}}{\sqrt{\log|d_K|}} \exp\left(\frac{-1}{\sqrt{\log|d_K|}}\right).$$

Proof. See Theorem 14 in Bessassi [5]. □

Combining these theorems with the analytic class number formula (see page 35), we get the following.

Theorem 3.4.8. *Let K be a non-normal sextic CM field containing an imaginary quadratic field and let F be the totally real cubic subfield of K. Then, under the Riemann Hypothesis (RH) for $\zeta_K(s)$, we have*

$$h_K^* \geq \frac{\mu_K}{e^{3/2}\pi^3} \frac{\sqrt{|d_K|/d_F}}{(\log d_F)^2\sqrt{\log(|d_K|)}} \exp\left(\frac{-1}{\sqrt{\log|d_K|}}\right), \tag{3.4.3}$$

where μ_K is the order of the group of roots of unity W_K of K.

Proof. Recall $Q_K := [\mathcal{O}_K^\times : W_K\mathcal{O}_F^\times]$. We have (see Washington [46, Chapter 4]):

$$h_K^* = \frac{Q_K\mu_K}{8\pi^3}\sqrt{\frac{|d_K|}{d_F}}\frac{\mathrm{Res}_{s=1}(\zeta_K)}{\mathrm{Res}_{s=1}(\zeta_F)}.$$

If we assume the Riemann Hypothesis for ζ_K, then combining Theorem 3.4.6 and Theorem 3.4.7, we obtain the lower bound (3.4.3). □

Proposition 3.4.9. *Let K be a* CM class number one *non-normal sextic CM field containing an imaginary quadratic field k. Let F be the totally real cubic subfield of K. Then we have $k = \mathbb{Q}(\sqrt{-d})$ with $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$ and an upper bound on d_F is given in Table 3.2.*

$\lvert d_k \rvert$	$d_F \leq$
3	$6 \cdot 10^9$
4	$3 \cdot 10^{10}$
7	$1.4 \cdot 10^{10}$
8	$7 \cdot 10^{10}$
11	$8 \cdot 10^9$
19	$4 \cdot 10^9$
43	$1.4 \cdot 10^9$
67	$8 \cdot 10^8$
163	$3 \cdot 10^8$

Table 3.2: Upper bounds on d_F for *CM class number one* non-normal sextic CM fields K containing an imaginary quadratic field k.

Proof. By Proposition 3.4.1, the CM field K contains one of the imaginary quadratic fields in the proposition and $h_K^* = 2^{t_K - 1}$. Since $h_k = 1$ we have $t_k \leq 3$. Moreover, the factor $\exp(-1/\sqrt{\log |d_K|})$ increases monotonically with $|d_K|$ and $|d_K| / \log |d_K|$ increases monotonically with $|d_K| > 2$. Hence for every fixed d_F, the right hand side of (3.4.3) increases monotonically with $|d_K| > e$.

Furthermore, we have $|d_K| = d_F^2 d_r$, where $d_r := |\mathrm{N}_{F/\mathbb{Q}}(\Delta_{K/F})|$. If we replace $|d_K|$ with $d_F^2 d_r$ and divide both sides of (3.4.3) by the constant $\mu_K / (e^{3/2} \pi^3)$, then we get

$$\frac{h_K^* e^{3/2} \pi^3}{\mu_K} \geq \sqrt{\frac{d_r d_F}{(\log d_F)^4 \log(d_r d_F^2)}} \exp\left(\frac{-1}{\sqrt{\log(d_r d_F^2)}}\right). \tag{3.4.4}$$

For every fixed d_r, each of the two factors of the right hand side of (3.4.4) increases monotonically with $d_F > 103$. Hence the right hand side of (3.4.4) increases monotonically with d_F for every fixed d_r.

Claim. Let p be the prime that ramifies in k. Then we have

(i) $d_r \geq |d_k|$ if $t_K = 1$,

(ii) $d_r \geq \max\{p^2, |d_k|\}$ if $t_K = 2$,

(iii) $d_r \geq |d_k|^3$ if $t_K = 3$.

Proof. By Lemma 20 in Louboutin, Okazaki, Olivier [27], we have that $|d_k|$ divides d_r.

Every prime $\mathfrak{p}$ of F that ramifies in K/F divides $\Delta_{K/F}$. So $\Delta_{K/F}$ has at least t_K prime factors. Hence $\mathrm{N}_{F/\mathbb{Q}}(\Delta_{K/F})$ has at least t_K prime factors with multiplicity. And these factors all must be equal to p because it is the unique prime that ramifies in $k/\mathbb{Q}$. So this proves (ii).

If $t_K = 3$, then p splits completely in F and all the primes above p in F ramify in K. So $\gcd(d_k, d_F) = 1$. Since $|d_k|^3$ divides $|d_k|^3|\mathrm{N}_{k/\mathbb{Q}}(\Delta_{K/k})|$ $= |d_K| = d_F^2 d_r$ and $\gcd(d_k, d_F) = 1$, we have that $|d_k|^3$ divides d_r. This proves the last assertion. Hence we proved the claim.

For every d_k in Table 3.2 and every $t_K \in \{1, 2, 3\}$, if we take d_F from the right hand side of the table, use $h_K^* = 2^{t_K - 1}$, $\mu_K = \mu_k$ and use the lower bound on d_r from (i)–(iii), then we get that the right hand side of (3.4.4) is larger than the left hand side. By monotonicity of the right hand side of (3.4.4) in terms of d_r and d_F, this gives a contradiction with (3.4.4) for every d_F larger than the bound in Table 3.2. □

By Proposition 3.3.3, we know that every CM class number one sextic CM field K contains a *class number one* imaginary quadratic field k. Thus there is only one prime that ramifies in k. On the other hand, the ramified primes in K/F are lying above the prime that ramifies in k (see Proposition 4.8-(ii) in II of Lang [21]). Hence the relative class number h_K^* is at most 4, and so by Proposition 3.4.9, we get that if $I_0(\Phi^r) = I_{K^r}$ and the *RH* holds for ζ_K, then the bound for d_F is given in Table 3.2.

We will list all fields up to that bound. Then the following lemma will help us eliminate sextic CM fields that do not have trivial CM class group.

Lemma 3.4.10. *Let K be a non-normal sextic CM field containing an imaginary quadratic field k. Assuming $I_0(\Phi^r) = I_{K^r}$, if a rational prime l splits completely in $K/\mathbb{Q}$, then $l \geq \sqrt{d_F/(6|d_k|)}$.*

Proof. Let l be a rational prime that splits completely in K and $\mathfrak{l}$ be a prime in K lying above l. By the assumption $I_0(\Phi^r) = I_{K^r}$, there exists $\pi \in K^\times$ such that $\mathrm{N}_{\Phi^r}(\mathfrak{l}) = \pi\mathcal{O}_K$ and $\pi\overline{\pi} = l$.

We claim that $K = \mathbb{Q}(\pi)$. Let N be a normal closure of K with $\mathrm{Gal}(N/\mathbb{Q}) = \langle x,\ y : y^6 = x^2 = 1,\ xyxy = 1\rangle$, where K is fixed by $\langle x\rangle$.

If $\sigma\pi$ and π have the same ideal factorization in N, then σ satisfies

$$(\sigma \mathrm{N}_{\Phi^r}(\mathfrak{l}))\mathcal{O}_N = (\mathrm{N}_{\Phi^r}(\mathfrak{l}))\mathcal{O}_N. \tag{3.4.5}$$

Since N is a normal closure of K, the rational prime l splits completely in N. Then the equality (3.4.5) holds only if $\sigma\Phi_N^r = \Phi_N^r$, equivalently $\Phi_N\sigma = \Phi_N$. Since Φ is primitive, this implies that $\sigma \in \langle x\rangle$. So if $\sigma\pi = \pi$, then $\sigma \in \mathrm{Gal}(N/K)$, hence $\mathbb{Q}(\pi) = K$.

We claim that $\{1, \pi, \overline{\pi}\}$ is linearly independent over k. Assume that they are linearly dependent over k. Then there exist $a, b \in k$ such that $\overline{\pi} = a + b\pi$. Then we have $b\pi^2 + a\pi - l = 0$, hence $\{1, \pi, \pi^2\}$ are linearly dependent over k. But this is a contradiction since the degree of K/k is 3.

Therefore, we have

$$\Delta_{K/k} \le |\mathrm{disc}(1, \pi, \overline{\pi})| = \begin{vmatrix} 1 & \pi & \overline{\pi} \\ \pi & \pi^2 & l \\ \overline{\pi} & l & \overline{\pi}^2 \end{vmatrix} \le 3! \cdot l^2 \tag{3.4.6}$$

as $|\pi| = \sqrt{l}$ for every $K \hookrightarrow \mathbb{C}$. Hence we get $|\mathrm{N}_{k/\mathbb{Q}}(\Delta_{K/k})| \le (6l^2)^2$.

By Lemma 20 in [27], we have $|d_K| \ge |d_k| d_F^2$. So we get

$$|d_k| d_F^2 \le |d_K| = |\mathrm{N}_{k/\mathbb{Q}}(\Delta_{K/k})||d_k|^3 \le (6l^2)^2 |d_k|^3.$$

Hence we get $\sqrt{d_F/(6|d_k|)} \le l$. □

Algorithm 3.4.11. ***Output:*** *Assuming GRH, the output is the complete list of non-normal sextic CM fields with a primitive CM type Φ satisfying $I_0(\Phi^r) = I_{K^r}$ and containing an imaginary quadratic field k.*

Step 1. Enumerate all totally real non-normal cubic number fields F up to $d_F \le 7 \cdot 10^{10}$, using the algorithm in Belabas [4].

Step 2. *For each F construct $K = F(\sqrt{-d})$, where $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$.*

Step 3. *Eliminate fields K that have totally split primes under the bound $\sqrt{d_F/(6|d_k|)}$.*

Step 4. *For each sextic CM field K, compute the class numbers of K and its totally real subfield F under the GRH. Then test whether $h_K^* = 2^{t_K - 1}$, where t_K is the number of primes in F that are ramified in K.*

Proof. Note that Step 3 of the algorithm does not affect the validity of the algorithm by Lemma 3.4.10, only speeds up the computation.

Suppose that a non-normal sextic CM field $K = F(\sqrt{-d})$ with $d \in \mathbb{Z}_{>0}$ satisfies $I_0(\Phi^r) = I_{K^r}$. Then by Proposition 3.4.1, we have $h_K^* = 2^{t_K - 1}$, and without loss of generality $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$. Therefore, there are at most 3 ramified primes in K/F. This implies $t_K \leq 3$ and hence $h_K^* = 2^{t_K - 1} \leq 4$. Then by Proposition 3.4.9, under GRH, for each k we get the upper bound for d_F as in Table 3.2. Hence $d_F < 7 \cdot 10^{10}$. Therefore, the CM field K is listed by the algorithm. Conversely, all the listed fields satisfy $I_0(\Phi^r) = I_{K^r}$ by Propositions 3.2.1 and 3.4.2. □

We implemented the algorithm in SageMath [36] using Belabas' *cubic* software [3] for Step 1 and using Pari [33]'s bnfinit function with flag $= 0$ for computing the class numbers under the GRH without computing the generators of the unit group. The fields that we obtained are in Tables 3.3–3.12. The implementation is online at [18]. This computation takes few weeks on a computer.

So we proved Theorem 3.1.3.

In Tables 3.3–3.12, the notation is as follows: K is a non-normal sextic CM field that contains $\mathbb{Q}(\sqrt{-d})$ for some $d \in \mathbb{Z}_{>0}$; F is the totally real cubic subfield of K and F is defined by a monic irreducible polynomial $p(X)$; h_K^* is the relative class number h_K/h_F, where h_K and h_F are the class numbers of K and F, respectively.

Table 3.3: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-3})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 6X - 2$	1	$X^3 + 3X^2 - 24X + 8$	1
$X^3 - 6X - 1$	1	$X^3 + 4X^2 - X - 2$	1
$X^3 - 9X - 2$	1	$X^3 + 4X^2 - 3X - 3$	1
$X^3 - 18X - 12$	1	$X^3 + 4X^2 - 5X - 3$	1
$X^3 + X^2 - 3X - 1$	1	$X^3 + 4X^2 - 7X - 4$	1
$X^3 + X^2 - 4X - 1$	1	$X^3 + 4X^2 - 12X - 12$	1
$X^3 + X^2 - 7X - 1$	1	$X^3 + 4X^2 - 16X - 4$	1
$X^3 + X^2 - 9X - 3$	1	$X^3 + 4X^2 - 18X - 12$	1
$X^3 + X^2 - 16X + 8$	1	$X^3 + 4X^2 - 22X + 8$	1
$X^3 + X^2 - 20X - 12$	1	$X^3 + 5X^2 - X - 2$	1
$X^3 + X^2 - 22X - 16$	1	$X^3 + 5X^2 - 6X - 6$	1
$X^3 + X^2 - 30X - 18$	1	$X^3 + 5X^2 - 10X - 2$	1
$X^3 + 2X^2 - 3X - 2$	1	$X^3 + 5X^2 - 12X - 6$	1
$X^3 + 2X^2 - 4X - 2$	1	$X^3 + 5X^2 - 18X - 24$	1
$X^3 + 2X^2 - 5X - 3$	1	$X^3 + 5X^2 - 22X - 8$	1
$X^3 + 2X^2 - 14X - 12$	1	$X^3 + 6X^2 - 2$	1
$X^3 + 2X^2 - 15X - 6$	1	$X^3 + 6X^2 - 3X - 2$	1
$X^3 + 2X^2 - 22X + 4$	1	$X^3 + 6X^2 - 3X - 6$	1
$X^3 + 3X^2 - 3X - 2$	1	$X^3 + 6X^2 - 6X - 12$	1
$X^3 + 3X^2 - 4X - 2$	1	$X^3 + 6X^2 - 9X - 4$	1
$X^3 + 3X^2 - 6X - 2$	1	$X^3 + 6X^2 - 21X - 36$	1
$X^3 + 3X^2 - 6X - 3$	1	$X^3 + 7X^2 - 3$	1
$X^3 + 3X^2 - 9X - 5$	1	$X^3 + 7X^2 + X - 3$	1
$X^3 + 3X^2 - 12X - 8$	1	$X^3 + 7X^2 - 8X - 12$	1
$X^3 + 3X^2 - 18X - 8$	1	$X^3 + 7X^2 - 14X - 24$	1
$X^3 + 3X^2 - 18X - 16$	1	$X^3 + 9X^2 - 6X - 24$	1

Table 3.4: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-3})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 2$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 5X - 1$	1	$X^3 + 2X^2 - 5X - 1$	1
$X^3 - 8X - 2$	1	$X^3 + 2X^2 - 14X - 4$	1
$X^3 - 14X - 4$	1	$X^3 + 3X^2 - 8X - 8$	1
$X^3 + X^2 - 5X + 1$	1	$X^3 + 3X^2 - 14X - 8$	1
$X^3 + X^2 - 6X - 2$	1	$X^3 + 4X^2 - 2X - 2$	1
$X^3 + X^2 - 8X - 2$	1	$X^3 + 4X^2 - 5X - 2$	1
$X^3 + X^2 - 9X + 1$	1	$X^3 + 5X^2 - X - 3$	1
$X^3 + X^2 - 12X - 8$	1	$X^3 + 6X^2 + X - 2$	1
$X^3 + 2X^2 - 3X - 1$	1		

$h_K^* = 4$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 22X - 12$	1	$X^3 + 3X^2 - 16X - 12$	1
$X^3 + 3X^2 - 4X - 3$	1	$X^3 + 6X^2 - X - 3$	1
$X^3 + 3X^2 - 10X - 6$	1	$X^3 + 6X^2 - 4X - 12$	1
$X^3 + 3X^2 - 7X - 3$	1		

Table 3.5: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-4})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 6X - 2$	1	$X^3 + 3X^2 - 8X - 2$	1
$X^3 - 14X - 4$	1	$X^3 + 3X^2 - 24X - 18$	1
$X^3 - 22X - 12$	1	$X^3 + 4X^2 - 3X - 4$	1
$X^3 + X^2 - 3X - 1$	1	$X^3 + 4X^2 - 22X - 4$	1
$X^3 + X^2 - 4X - 1$	1	$X^3 + 4X^2 - 27X - 36$	1
$X^3 + X^2 - 5X + 1$	1	$X^3 + 5X^2 - 4X - 6$	1
$X^3 + X^2 - 7X - 1$	1	$X^3 + 5X^2 - 8X - 6$	3
$X^3 + X^2 - 12X - 8$	1	$X^3 + 5X^2 - 12X - 8$	1
$X^3 + X^2 - 36X + 18$	1	$X^3 + 6X^2 - 3X - 2$	1
$X^3 + 2X^2 - 3X - 2$	1	$X^3 + 6X^2 - 4X - 12$	1
$X^3 + 2X^2 - 4X - 2$	1	$X^3 + 6X^2 - 7X - 6$	1
$X^3 + 2X^2 - 11X - 6$	1	$X^3 + 8X^2 + X - 4$	1
$X^3 + 2X^2 - 18X - 8$	1	$X^3 + 8X^2 - 15X - 36$	1
$X^3 + 2X^2 - 18X + 8$	1	$X^3 + 13X^2 + 12X - 12$	1
$X^3 + 3X^2 - 4X - 2$	1		

$h_K^* = 2$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 4X - 1$	1	$X^3 + 3X^2 - 6X - 2$	1
$X^3 + X^2 - 6X - 2$	1	$X^3 + 3X^2 - 8X - 8$	1
$X^3 + X^2 - 10X + 2$	1	$X^3 + 3X^2 - 10X - 6$	1
$X^3 + X^2 - 16X - 4$	1	$X^3 + 3X^2 - 16X - 12$	1
$X^3 + X^2 - 16X + 8$	1	$X^3 + 4X^2 - X - 2$	1
$X^3 + 2X^2 - 4X - 1$	1	$X^3 + 4X^2 - 5X - 2$	1
$X^3 + 2X^2 - 6X - 3$	1	$X^3 + 5X^2 - X - 2$	1
$X^3 + 2X^2 - 14X - 12$	1	$X^3 + 5X^2 - 2X - 2$	1
$X^3 + 2X^2 - 18X - 12$	1	$X^3 + 6X^2 - 6X - 12$	1
$X^3 + 3X^2 - 3X - 2$	1	$X^3 + 7X^2 + 2X - 2$	1

$h_K^* = 4$	
$p(X)$	h_F
$X^3 + 3X^2 - 10X - 8$	1

Table 3.6: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-7})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 6X - 2$	1	$X^3 + 3X^2 - 30X - 9$	1
$X^3 + X^2 - 16X - 1$	3	$X^3 + 4X^2 - 7X - 3$	1
$X^3 + X^2 - 8X - 1$	1	$X^3 + 4X^2 - 7X - 7$	1
$X^3 + X^2 - 36X + 27$	1	$X^3 + 4X^2 - 9X - 1$	1
$X^3 + X^2 - 42X - 45$	1	$X^3 + 5X^2 - 6X - 3$	1
$X^3 + 2X^2 - 4X - 1$	1	$X^3 + 5X^2 - 18X - 27$	1
$X^3 + 2X^2 - 7X - 3$	1	$X^3 + 6X^2 - 5X - 7$	1
$X^3 + 2X^2 - 39X + 27$	1	$X^3 + 6X^2 - 5X - 3$	1
$X^3 + 3X^2 - 10X - 3$	1	$X^3 + 8X^2 - X - 5$	1
$X^3 + 3X^2 - 10X - 7$	1	$X^3 + 9X^2 - 3$	1
$X^3 + 3X^2 - 16X - 9$	1		

$h_K^* = 2$	
$p(X)$	h_F
$X^3 + X^2 - 4X - 1$	1
$X^3 + 2X^2 - 5X - 3$	1
$X^3 + 2X^2 - 3X - 1$	1

$h_K^* = 4$	
$p(X)$	h_F
$X^3 - 7X - 1$	1
$X^3 + 5X^2 - 2X - 3$	1
$X^3 + 3X^2 - 6X - 1$	1

Table 3.7: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-8})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 + X^2 - 3X - 1$	1	$X^3 + X^2 - 24X - 4$	1
$X^3 + 2X^2 - 13X - 4$	1	$X^3 + X^2 - 16X - 8$	3
$X^3 + 3X^2 - 6X - 2$	1	$X^3 + 3X^2 - 8X - 8$	1
$X^3 + 4X^2 - X - 2$	1	$X^3 + 4X^2 - 18X - 16$	1
$X^3 + 5X^2 - 6X - 2$	1	$X^3 + 6X^2 - 10X - 20$	1
$X^3 + 8X^2 - 9X - 2$	1	$X^3 + 6X^2 - 22X - 20$	1

$h_K^* = 2$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 4X - 1$	1	$X^3 + 5X^2 - 2X - 2$	1
$X^3 - 13X - 2$	1	$X^3 + 6X^2 - X - 4$	1
$X^3 + X^2 - 10X - 2$	1	$X^3 + 8X^2 + 3X - 2$	1
$X^3 + 2X^2 - 3X - 2$	1	$X^3 + 3X^2 - 16X - 8$	1
$X^3 + 3X^2 - 4X - 2$	1	$X^3 + 4X^2 - 14X - 16$	1
$X^3 + 4X^2 - 3X - 4$	1	$X^3 + 4X^2 - 10X - 8$	1
$X^3 + 5X^2 - 2$	1		

Table 3.8: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-11})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 - 5X - 1$	1	$X^3 + 2X^2 - 18X - 8$	1
$X^3 + X^2 - 7X - 2$	1	$X^3 + 4X^2 - 5X - 2$	1
$X^3 + X^2 - 8X - 1$	1	$X^3 + 4X^2 - 6X - 1$	1
$X^3 + X^2 - 16X - 2$	1	$X^3 + 5X^2 - 26X - 8$	1
$X^3 + X^2 - 16X - 8$	3	$X^3 + 5X^2 - 26X - 32$	1
$X^3 + 2X^2 - 18X + 4$	1	$X^3 + 7X^2 - 14X - 16$	1

$h_K^* = 2$	
$p(X)$	h_F
$X^3 + 2X^2 - 3X - 2$	1

$h_K^* = 4$	
$p(X)$	h_F
$X^3 + 5X^2 - 2X - 2$	1

Table 3.9: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-19})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$			
$p(X)$	h_F	$p(X)$	h_F
$X^3 + 2X^2 - 8X - 3$	1	$X^3 + 6X^2 - 6X - 12$	1
$X^3 + 4X^2 - 3X - 3$	1	$X^3 + 7X^2 - 30X - 54$	1
$X^3 + 4X^2 - 14X - 8$	1	$X^3 + 8X^2 + X - 3$	1
$X^3 + 6X^2 - X - 4$	1		

Table 3.10: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-43})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$	
$p(X)$	h_F
$X^3 + X^2 - 22X - 8$	1
$X^3 + 2X^2 - 18X - 12$	1
$X^3 - 5X - 1$	1

Table 3.11: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-67})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$	
$p(X)$	h_F
$X^3 + 2X^2 - 4X - 1$	1

Table 3.12: Under GRH, the complete list of $p(X) \in \mathbb{Q}[X]$ such that $K = \mathbb{Q}(\sqrt{-163})[X]/p(X)$ is a CM class number one non-normal sextic CM field.

$h_K^* = 1$	
$p(X)$	h_F
$X^3 + 3X^2 - 8X - 8$	1

Chapter 4

Simple CM curves of genus 3 over $\mathbb{Q}$

ABSTRACT. In this chapter, we will study the isomorphism classes of principally polarized simple CM abelian threefolds with field of moduli $\mathbb{Q}$. In Section 4.3, we will determine the sextic CM fields corresponding to simple CM curves of genus 3 with field of moduli $\mathbb{Q}$.

4.1 Introduction

It is known that there are only finitely many CM elliptic curves over $\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$. An equivalent formulation of this statement is that there are only finitely many class number one imaginary quadratic fields. The complete list of such fields is given by Heegner [16] (1952), Baker [2] (1966) and Stark [41] (1967). A list of simple CM curves of genus 2 defined over $\mathbb{Q}$, up to isomorphism over $\overline{\mathbb{Q}}$, is given by van Wamelen [45] and the completeness of the list of van Wamelen is shown by Murabayashi and Umegaki [31].

In this chapter, we determine the sextic CM fields corresponding to simple CM curves of genus 3 with field of moduli $\mathbb{Q}$. One way to do this would be to compute the curves corresponding to the CM fields of Chapter 3. However, the current techniques are not sufficient to compute

all CM curves of genus 3, see Section 4.4. Instead, in this chapter, we will use an alternative method inspired by Murabayashi [30] and Shimura [38].

It is known that every *principally polarized simple abelian variety* over $\mathbb{C}$ of dimension g with $g \leq 3$ is isomorphic to the *Jacobian variety* of a curve of genus g (see Theorem 1.3.6). By the fact that the *Torelli map* is injective on $\mathbb{C}$-points, *the field of moduli* of $J(C)$ is the same as the field of moduli of the curve C. Therefore, we will be interested in finding the CM fields corresponding to the *principally polarized simple CM abelian threefolds* with rational field of moduli.

Theorem 4.1.1. *There exist exactly* 37 *CM points over* $\mathbb{Q}$ *in the moduli space of principally polarized abelian threefolds that are simple over* $\overline{\mathbb{Q}}$ *and have CM by a maximal order. In fact, it is exactly one point for each field in Table 3.1.*

Remark 4.1.2. For some of these abelian threefolds, we know that they can be defined over $\mathbb{Q}$, for others we do not know. See Section 4.4.

4.2 Polarized CM abelian varieties over $\mathbb{Q}$

Let K be a CM field and Φ be a primitive CM type of K. Let $P := (A, \theta, \varphi)$ be a polarized abelian variety over $\mathbb{C}$ of type $(K, \Phi, t, \mathfrak{m})$ (for the definition see page 14) such that $\theta^{-1}(\mathrm{End}(A)) = \mathcal{O}_K$. Let M be the field of moduli of (A, φ). By the first main theorem of CM (Theorem 1.5.6), we can determine MK^r as a class field over K^r. This theorem does not provide information about the size of M. We will see that sometimes the field M depends on the *isomorphim class* of (A, φ) whereas MK^r is determined only by (K, Φ).

To say something about M requires investigation of the behavior of P under an automorphism of $\mathbb{C}$ that does not necessarily fix K^r.

Let $\sigma \in \mathrm{Aut}(\mathbb{C})$. By Proposition 1.4.13, the abelian variety $\sigma(A, \theta)$ is of type $(K, \sigma\Phi)$ and if σ is the identity map on K^r, then $\sigma(A, \theta)$ is of type (K, Φ). In this chapter, we broaden our perspective from only the automorphisms in $\mathrm{Aut}(\mathbb{C}/K^r)$, to all the ones $\sigma \in \mathrm{Aut}(\mathbb{C})$ for which there exists $[\sigma] \in \mathrm{Aut}(K)$ such that we have $\sigma \circ \Phi = \Phi \circ [\sigma]$ as sets.

Note that if Φ is primitive, then $[\sigma]$ is uniquely determined by σ and Φ if it exists.

For a given $P := (A, \theta, \varphi)$, we denote by $\theta|_J$, for any subfield J of K, the restriction of θ to J and by M_J the field of moduli of $(A, \theta|_J, \varphi)$. Throughout this chapter, every P of CM type (K, Φ) is assumed to have CM by $\mathcal{O}_K$.

Proposition 4.2.1. *(Shimura) Let (K, Φ) be a primitive CM pair, and let (K^r, Φ^r) be its reflex. Let $P = (A, \theta, \varphi)$ be of CM type (K, Φ) and defined over $\mathbb{C}$. Let J be a subfield of K, $\theta|_J$ be the restriction of θ to J and M_J be the field of moduli of $(A, \theta|_J, \varphi)$. Then the following assertions hold.*

(i) *$M_J K^r$ is the field of moduli of P.*

(ii) *K^r is normal over $M_J \cap K^r$.*

(iii) *$M_J K^r$ is normal over M_J and $\mathrm{Gal}(M_J K^r / M_J)$ is isomorphic to a subgroup of $\mathrm{Aut}(K/J)$ via the map*

$$\sigma|_{M_J K^r} \mapsto [\sigma]$$

for $\sigma \in \mathrm{Aut}(\mathbb{C}/M_J)$, where $[\sigma] \in \mathrm{Aut}(K/J)$ is such that $\sigma\Phi = \Phi[\sigma]$.

Proof. This is Shimura [39, Proposition 5.17] except that Shimura does not explicitly give the map in *(iii)*. Therefore, we reprove the second part of *(iii)*.

Let $\sigma \in \mathrm{Aut}(\mathbb{C}/M_J)$ and let λ be an isomorphism from $(A, \varphi, \theta|_J)$ to $(\sigma A, \sigma\varphi, {}^{\sigma}\theta|_J)$, where ${}^{\sigma}\theta(\alpha) = \sigma\theta([\sigma]^{-1}\alpha)$ for all $\alpha \in K$. Since A is simple, we have $\theta(K) = \mathrm{End}_0(A) := \mathrm{End}(A) \otimes \mathbb{Q}$. Let $[\sigma] \in \mathrm{Aut}(K/J)$ be given by $[\sigma](\alpha) = \theta^{-1}(\lambda^{-1}\sigma(\theta(\alpha))\lambda)$. Then we get that $\sigma\theta$ and $\theta[\sigma]$ have the same CM type, hence $\sigma\Phi = \Phi[\sigma]$. Recall that $[\sigma]$ is uniquely defined by $\sigma\Phi = \Phi[\sigma]$ as Φ is primitive.

We have $[\sigma] = \mathrm{id}_K$ if and only if $\sigma\Phi = \Phi$ if and only if $\sigma|_{M_J K^r} = \mathrm{id}_{M_J K^r}$. Hence the map $\sigma|_{M_J K^r} \mapsto [\sigma]$ is a well-defined injection, so $\mathrm{Gal}(M_J K^r / M_J)$ is isomorphic to a subgroup of $\mathrm{Aut}(K/J)$. □

Remark 4.2.2. If K is abelian over $\mathbb{Q}$ and embedded inside $\mathbb{C}$ and Φ is a primitive CM type of K, then we have $[\sigma] = \sigma|_K$ as $\sigma\Phi = \Phi\sigma$.

Proposition 4.2.3. *Let $P = (A, \theta, \varphi)$ be of a primitive CM type (K, Φ). Let J be a subfield of K such that $M_J = \mathbb{Q}$. Then $J = \mathbb{Q}$ and $M_K = K^r \cong K$ is Galois over $\mathbb{Q}$.*

Proof. Suppose that J is a subfield of K and $M_J = \mathbb{Q}$. By Proposition 4.2.1-*(ii)*, the reflex field K^r is normal over $\mathbb{Q}$; and by *(iii)*, the Galois group $\mathrm{Gal}(K^r/\mathbb{Q})$ is isomorphic to a subgroup of $\mathrm{Aut}(K/J)$. In particular, we get

$$[K^r : \mathbb{Q}] = \#\mathrm{Gal}(K^r/\mathbb{Q}) \leq \#\mathrm{Aut}(K/J) \leq [K : J]. \tag{4.2.1}$$

On the other hand, since Φ is primitive, we get $K^{rr} = K$ by Lemma 1.2.5. Furthermore, since $K^r/\mathbb{Q}$ is normal, the reflex field K^{rr} is isomorphic to a subfield of K^r. Hence we have $K^{rr} = K \subset K^r$, and therefore, by (4.2.1) we get $J = \mathbb{Q}$ and $K^r \cong K$ and by Proposition 4.2.1-(i), we get $M_K = M_J K^r = K^r$. □

Note that $M_{\mathbb{Q}} := M$. For $\sigma \in \mathrm{Aut}(\mathbb{C}/M_{\mathbb{Q}})$, we define

$$^{\sigma}P = (\sigma A, {}^{\sigma}\theta, \sigma\varphi), \tag{4.2.2}$$

where ${}^{\sigma}\theta(\alpha) = \sigma\theta([\sigma]^{-1}\alpha)$ for all $\alpha \in K$.

Proposition 4.2.4. *(Shimura [38, page 69]) For $\sigma \in \mathrm{Aut}(\mathbb{C}/M_{\mathbb{Q}})$, the polarized simple abelian variety ${}^{\sigma}P = (\sigma A, {}^{\sigma}\theta, \sigma\varphi)$ is of type (K, Φ).*

Proof. Proposition 4.2.1-*(iii)* tells us $\Phi = \sigma\Phi[\sigma]^{-1}$ and then the result follows from the definition of ${}^{\sigma}\theta$. □

Recall the notation $(P' : P) \in \mathfrak{C}_K$ from (1.5.5).

Proposition 4.2.5. *(Shimura [38, Proposition 2]) Let K be a CM field and Φ be its CM type. Let P and P' be polarized simple abelian varieties of CM type (K, Φ) and defined over $k \subset \mathbb{C}$. For any $\sigma,\ \gamma \in \mathrm{Aut}(\overline{k}/\mathbb{Q})$, the following holds.*

(i) If $(P' : P) = [(b, \mathfrak{c})]$, then we have $({}^{\sigma}P' : {}^{\sigma}P) = [([\sigma]b, [\sigma]\mathfrak{c})]$.

(ii) If $({}^{\sigma}P : P) = [(b, \mathfrak{c})]$ and $({}^{\gamma}P : P) = [(d, \mathfrak{e})]$, then we have

$$({}^{\gamma\sigma}P : P) = [(([\gamma]b)d, ([\gamma]\mathfrak{c})\mathfrak{e})].$$

(iii) *If* $(P' : P) = [(b, \mathfrak{c})]$ *and* $({}^{\sigma}P : P) = [(d, \mathfrak{e})]$, *then we have*

$$({}^{\sigma}P' : P') = [(([\sigma]b)b^{-1}d, ([\sigma]\mathfrak{c})\mathfrak{c}^{-1}\mathfrak{e})].$$ □

Proof. (i) See Proposition 2-(i) in Shimura [38].

(ii) We have $({}^{\gamma\sigma}P : P) = ({}^{\gamma\sigma}P : {}^{\gamma}P)({}^{\gamma}P : P)$ and by *(i)*, we have $({}^{\gamma\sigma}P : {}^{\gamma}P) = [([\gamma]b, [\gamma]\mathfrak{c})]$. It follows

$$({}^{\gamma\sigma}P : P) = [([\gamma]b, [\gamma]\mathfrak{c})][(d, \mathfrak{e})].$$

(iii) We have $({}^{\sigma}P' : P') = ({}^{\sigma}P' : {}^{\sigma}P)({}^{\sigma}P : P)(P' : P)^{-1}$. By *(i)*, we have $({}^{\sigma}P' : {}^{\sigma}P) = [([\sigma]b, [\sigma]\mathfrak{c})]$. Hence the result follows from the following

$$({}^{\sigma}P' : P') = [([\sigma]b, [\sigma]\mathfrak{c})][(d, \mathfrak{e})][(b, \mathfrak{c})]^{-1}.$$

□

4.3 Principally polarized simple CM abelian threefolds

In this chapter, our interest will be determining the sextic CM fields that correspond to principally polarized CM abelian threefolds with rational field of moduli.

In this section, we will prove the following.

Theorem 4.3.1.

(i) *If a principally polarized simple CM abelian threefold over* $\mathbb{C}$ *with CM by the ring of integer of a CM field* K *has field of moduli* $\mathbb{Q}$, *then* K *is one of the cyclic sextic CM fields in Table 3.1; in particular* $h_K^* = 2^{t_K - 1} = 1$ *or* 4, *where* t_K *is the number of primes in* F *that are ramified in* K.

(ii) *For every cyclic sextic CM field* K *with* $h_K^* = 1$, *up to isomorphism, there exists a* unique *principally polarized simple abelian threefold over* $\mathbb{C}$ *that has CM by* $\mathcal{O}_K$, *and such principally polarized abelian threefolds have field of moduli* $\mathbb{Q}$.

(iii) For every cyclic sextic CM field K with $h_K^* = 4$ and a primitive CM type Φ that satisfies $I_0(\Phi^r) = I_{K^r}$, there are four isomorphism classes of principally polarized simple abelian threefolds over $\mathbb{C}$ that have CM by $\mathcal{O}_K$. Among these four isomorphism classes, one of them has rational field of moduli and the other three have field of moduli F, which is the cubic subfield of K.

Lemma 4.3.2. *Let K be a CM field of degree $2g$ with an odd prime g and let Φ be a CM type of K. Let $P = (A, \theta, \varphi)$ be a g-dimensional polarized abelian variety of type (K, Φ) with CM by $\mathcal{O}_K$.*

If A is simple over $\mathbb{C}$ and the field of moduli $M_{\mathbb{Q}}$ of (A, φ) is $\mathbb{Q}$ then K is cyclic over $\mathbb{Q}$, the CM type Φ is primitive and we have $I_0(\Phi^r) = I_{K^r}$.

Proof. Suppose that A is simple over $\mathbb{C}$. Then by Theorem 1.4.1 the CM type Φ of A is primitive. By Proposition 4.2.3, we have that K is Galois over $\mathbb{Q}$. Hence the maximal totally real subfield F is also normal over $\mathbb{Q}$ with an odd prime degree g. Every group with a prime order is cyclic, hence $\mathrm{Gal}(F/\mathbb{Q})$ is cyclic. Let k be the subfield of K that is fixed by the order-g cyclic subgroup of $\mathrm{Gal}(K/\mathbb{Q})$. Since K is a CM field of order $2g$ and F is totally real, we have $\rho \in \mathrm{Gal}(K/F)$ and $\mathrm{Gal}(K/F) = 2$. Therefore, the subfield k is imaginary quadratic over $\mathbb{Q}$. Moreover, since ρ commutes with every element in $\mathrm{Gal}(K/k)$, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian hence cyclic of degree $2g$.

Moreover, recall that the first main theorem of Complex Multiplication (Theorem 1.5.6) says that $M_{\mathbb{Q}}K^r$ is the unramified class field over K^r corresponding to the ideal group $I_0(\Phi^r)$. Hence if $M_{\mathbb{Q}} = \mathbb{Q}$, then (K, Φ) satisfies $I_0(\Phi^r) = I_{K^r}$. □

Lemma 4.3.2 proves *(i)* of Theorem 4.3.1 as follows. If $M_{\mathbb{Q}} = \mathbb{Q}$, then K is cyclic over $\mathbb{Q}$, the CM type Φ is primitive and (K, Φ) satisfies $I_0(\Phi^r) = I_{K^r}$. By Theorem 3.1.2, the cyclic sextic CM fields that satisfy $I_0(\Phi^r) = I_{K^r}$ for a primitive CM type are listed in Table 3.1. Therefore, we have $h_K^* \in \{1,\ 4\}$.

Remark 4.3.3. We can also see $h_K^* \in \{1,\ 4\}$ directly as follows. Since K is cyclic over $\mathbb{Q}$, the totally real cubic subfield F is also *cyclic* over $\mathbb{Q}$. Moreover, Proposition 3.3.3 tells us that K contains a *class number one* imaginary quadratic field. So there is only one rational prime that is

ramified in K/F (see Proposition 4.8-(ii) in II of Lang [21]). Since F is a cubic field, the number t_K of primes in F that are ramified in K is at most 3. Furthermore, since K is cyclic, we have $t_K \neq 2$. Hence $t_K \in \{1, 3\}$ and so $h_K^* = 2^{t_K - 1} \in \{1,\ 4\}$.

Lemma 4.3.4. *Let K be a cyclic sextic CM field in Table 3.1 and let F be the totally real cubic subfield of K. Let $(\mathcal{O}_F^\times)^+$ be the group of totally positive units in $\mathcal{O}_F$. Then we have $(\mathcal{O}_F^\times)^+ = (\mathcal{O}_F^\times)^2$. Moreover, we have $\mathrm{Cl}_F = \mathrm{Cl}_F^+$.*

Proof. For each field in Table 3.1, using Sage [36], we check that the map

$$\mathrm{sign} : \mathcal{O}_F^\times \to (C_2)^3 \tag{4.3.1}$$

is surjective. On the other hand, since F is a totally real cubic field, we have $[\mathcal{O}_F^\times : (\mathcal{O}_F^\times)^2] = 8$ by the Dirichlet unit theorem. Hence the kernel of the map (4.3.1) is $(\mathcal{O}_F^\times)^2$, and therefore the first equality follows.

Moreover, since the map (4.3.1) is surjective, we have $\mathrm{Cl}_F = \mathrm{Cl}_F^+$. □

Proposition 4.3.5. *(Shimura [38, Proposition 1]) Let K be a CM field and let Φ be a primitive CM type of K. If $\mathfrak{D}_{K/F} \neq \mathcal{O}_K$, then there is a principally polarized abelian variety $P = (A, \theta, \varphi)$ of type (K, Φ).* □

Corollary 4.3.6. *For every CM class number one sextic cyclic CM field K and every primitive CM type Φ of K, there exists a principally polarized abelian threefold of type (K, Φ).*

Proof. Theorem 3.1.2 proves that all CM class number one cyclic sextic CM fields K are in Table 3.1 and we can see that all the fields in this table satisfy $\mathfrak{D}_{K/F} \neq \mathcal{O}_K$. Therefore, the result follows from Proposition 4.3.5. □

The following is a variant of Proposition 4.4 in Streng [43].

Proposition 4.3.7. *Let K be a CM field of degree $2g$ and let F be the maximal totally real subfield of K. Let Φ be a primitive CM type of K. Suppose $(\mathcal{O}_F^\times)^+ = N_{K/F}(\mathcal{O}_K^\times)$. If there exists a principally polarized abelian variety over $\mathbb{C}$ of type (K, Φ), then there are exactly h_K^* isomorphism classes of such principally polarized abelian varieties.*

Proof. Set

$$\mathrm{H}_\Phi := \{(t,\mathfrak{m}) \in K^\times \times I_K : \ \mathrm{Im}(\phi(t)) > 0 \text{ for all } \phi \in \Phi,\ \bar{t} = -t, \\ \text{and } t^{-1}\mathcal{O}_K = \mathfrak{D}_{K/\mathbb{Q}}\mathfrak{m}\overline{\mathfrak{m}}\}.$$

The group $K^\times$ acts on H_Φ via $x(t,\mathfrak{m}) = ((x\overline{x})^{-1}t, x\mathfrak{m})$ for $x \in K^\times$. Let $\mathrm{H}'_\Phi := \mathrm{H}_\Phi/\{((x\overline{x})^{-1}, x\mathcal{O}_K) : x \in K^\times\}$.

Let CM_Φ be the set of isomorphism classes of principally polarized g-dimensional abelian varieties of type (K,Φ). Let $P_i = (A_i, \theta_i, \varphi_i)$ be a principally polarized g-dimensional abelian varietiy of type (K,Φ). Then there is a $\mathbb{Z}$-lattice $\mathfrak{m}_i$ in K and $t_i \in K^\times$ such that $A_i \cong \mathbb{C}^g/\tilde{\Phi}(\mathfrak{m}_i)$, and $\phi(t_i) > 0$ for all $\phi \in \Phi$ and $\bar{t}_i = -t_i$, see page 14. By Proposition 1.5.5, it holds that P_1 and P_2 are isomorphic if and only if $(P_1 : P_2) := [(t_1^{-1}t_2, \mathfrak{m}_1\mathfrak{m}_2^{-1})] = [(1, \mathcal{O}_K)]$, which holds if and only if there exists $x \in K^\times$ such that $\mathfrak{m}_2 = x\mathfrak{m}_1$ and $t_2(x\overline{x})^{-1} = t_1$. So CM_Φ is bijective to H'_Φ.

Recall $\mathfrak{C}_K := (F_{\gg 0} \times I_K)/\{(x\overline{x}, x\mathcal{O}_K) : x \in K^\times\}$. Define

$$\mathfrak{C}'_K = \{[(b,\mathfrak{c})] \in \mathfrak{C}_K : \mathfrak{c}\overline{\mathfrak{c}} = b\mathcal{O}_F\}.$$

Suppose $\mathfrak{D}_{K/F} \neq \mathcal{O}_K$. Then by Proposition 4.3.5, there exists an element $(t_0, \mathfrak{m}_0)$ in H_Φ. We observe that the map $\mathfrak{C}'_K \to \mathrm{H}'_\Phi : [(b,\mathfrak{c})] \mapsto [(b^{-1}t_0, \mathfrak{c}\mathfrak{m}_0)]$ is a bijection. Hence we have $|\mathfrak{C}'_K| = |\mathrm{H}'_\Phi| = |\mathrm{CM}_\Phi|$.

Moreover, by the assumption $(\mathcal{O}_F^\times)^+ = N_{K/F}(\mathcal{O}_K^\times)$, for every $[(b,\mathfrak{c})] \in \mathfrak{C}'_K$ there is $\epsilon \in \mathcal{O}_K^\times$ such that $b = \epsilon\overline{\epsilon}$. This means that for every $\mathfrak{c} \in I_K$, there is a *unique* class in $\mathfrak{C}'_K$. Hence the group $\mathfrak{C}'_K$ injects into Cl_K via the map $[(b,\mathfrak{c})] \mapsto [\mathfrak{c}]$.

We claim $\mathfrak{C}'_K \cong \ker(\mathrm{Cl}_K \to \mathrm{Cl}_F)$.

By definition, for every $[(b,\mathfrak{c})] \in \mathfrak{C}'_K$, we have $\mathrm{N}_{K/F}(\mathfrak{c}) = b\mathcal{O}_K$ and $b \in F_{\gg 0}$. Therefore, we get $\mathfrak{C}'_K \subset \ker(\mathrm{Cl}_K \to \mathrm{Cl}_F)$ via the injection $[(b,\mathfrak{c})] \mapsto [\mathfrak{c}]$. On the other hand, if $[\mathfrak{a}] \in \ker(\mathrm{Cl}_K \to \mathrm{Cl}_F)$, then we have $\mathrm{N}_{K/F}(\mathfrak{a}) \in P_F$ and $P_F^+ = P_F$ by the assumption $(\mathcal{O}_F^\times)^+ = N_{K/F}(\mathcal{O}_K^\times)$. This proves the claim.

The norm map $\mathrm{N}_{K/F} : \mathrm{Cl}_K \to \mathrm{Cl}_F$ is surjective by Theorem 10.1 in Washington [46] and the fact that the infinite primes ramify in K/F. By the isomorphism theorem we have $\mathrm{Cl}_K/\mathfrak{C}'_K \cong \mathrm{Cl}_F$. Therefore, we get $h_K^* := |\mathrm{Cl}_K|/|\mathrm{Cl}_F| = |\mathfrak{C}'_K| = |\mathrm{CM}_\Phi|$. □

Corollary 4.3.8. *Let K be a cyclic sextic CM field in Table 3.1 on page 56 and let Φ be a primitive CM type of K. Then there are $h_K^* \in \{1, 4\}$ isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$ of type (K, Φ) with CM by $\mathcal{O}_K$.*

Proof. The existence of a principally polarized abelian threefold of type (K, Φ) is guaranteed by Corollary 4.3.6. On the other hand, by Lemma 4.3.4, we have $(\mathcal{O}_F^\times)^+ = N_{K/F}(\mathcal{O}_K^\times)$, hence the result follows from Proposition 4.3.7. □

The following proposition is *(ii)* in Theorem 4.3.1.

Proposition 4.3.9. *For every cyclic sextic CM field K with $h_K^* = 1$, up to isomorphism, there exists a* unique *principally polarized simple abelian threefold (A, φ) over $\mathbb{C}$ with $\mathrm{End}(A) \cong \mathcal{O}_K$, and such a principally polarized simple abelian threefold has field of moduli $\mathbb{Q}$.*

Proof. Let CM_K be the set of isomorphism classes of principally polarized simple abelian threefold (A, φ) over $\mathbb{C}$ with $\mathrm{End}(A) \cong \mathcal{O}_K$.

We claim that for every primitive CM type Φ of K, there is a bijection between CM_Φ and CM_K. Given any $(A, \varphi) \in \mathrm{CM}_K$, there is an embedding $\theta : \mathcal{O}_K \to \mathrm{End}(A)$ for (A, φ). Let Φ' be the CM type of A. Since A is simple, by Theorem 1.4.1, the CM type Φ' is primitive. Then there is a *unique* $\sigma \in \mathrm{Aut}(K)$ such that $\Phi = \Phi'\sigma$, see the proof of Proposition 3.3.2. So we have $(A, \theta\sigma, \varphi) \in \mathrm{CM}_\Phi$ and this proves the claim.

Since CM_Φ and CM_K are bijective and $|\mathrm{CM}_\Phi| = 1$ by Proposition 4.3.7, we have $|\mathrm{CM}_K| = 1$. This means that for every cyclic sextic CM field K with $h_K^* = 1$, there exists a unique principally polarized simple abelian threefold of type (K, Φ) and every representative (A, φ) of the isomorphism class in CM_K satisfies $(A, \varphi) \cong (\sigma A, \sigma\varphi)$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$. Hence $M_\mathbb{Q} = \mathbb{Q}$. □

We now suppose that K is a cyclic sextic CM field in Table 3.1 with $h_K^* = 4$ and prove (iii) in Theorem 4.3.1.

Lemma 4.3.10. *Let P be a principally polarized simple abelian threefold over $\mathbb{C}$ that has CM by the maximal order of a CM class number one sextic CM field K. Then we have*

$$({}^\rho P : P) = 1,$$

where ρ is complex conjugation.

Proof. Let Φ be a primitive CM type of K and let P be of type $(K, \Phi, t, \mathfrak{m})$, see page 14. By Proposition 3.5.5 in Lang [20], the principally polarized simple abelian threefold ${}^{\rho}P$ is of type $(K, \Phi, t, \overline{\mathfrak{m}})$. Then by (1.5.5), we have $({}^{\rho}P : P) = [(1, \mathfrak{m}/\overline{\mathfrak{m}})]$. So we get $({}^{\rho}P : P) = 1$ if and only if $\mathfrak{m}/\overline{\mathfrak{m}} \in P_K$ and is generated by an $\alpha \in K^{\times}$ with $\alpha\overline{\alpha} = 1$.

Since all the fields K in Table 3.1 satisfy $I_0(\Phi^r) = I_{K^r}$, by Proposition 3.3.5, we have $I_K = I_K^H P_K$, where $I_K^H = \{\mathfrak{b} \in I_K \mid \overline{\mathfrak{b}} = \mathfrak{b}\}$. So there is $\mathfrak{a} \in I_K^H$ and $(\beta) \in P_K$ such that $\mathfrak{m} = \mathfrak{a}(\beta)$. Then it follows that $\mathfrak{m}/\overline{\mathfrak{m}} = (\beta/\overline{\beta}) =: (\alpha)$ and $\alpha\overline{\alpha} = 1$ since we have $\mathrm{N}_{K/F}(\mathcal{O}_K^{\times}) = (\mathcal{O}_F^{\times})^+$ by Lemmata 3.2.2 and 4.3.4. So we get $({}^{\rho}P : P) = 1$. □

Recall $\mathfrak{C}_K := (F_{\gg 0} \times I_K)/\{(x\overline{x}, x\mathcal{O}_K) : x \in K^{\times}\}$ and $\mathfrak{C}'_K = \{[(b, \mathfrak{c})] \in \mathfrak{C}_K : \mathfrak{c}\overline{\mathfrak{c}} = b\mathcal{O}_F\}$.

Lemma 4.3.11. *Let K be a cyclic sextic CM field with $h_K^* = 4$ and let Φ be a primitive CM type of K. Let F be the totally real cubic subfield of K. Let $p\mathcal{O}_F = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ and $\mathfrak{p}_i\mathcal{O}_K = \mathfrak{P}_i^2$. Suppose $I_0(\Phi^r) = I_{K^r}$.*

Then there is $t_i \in F_{\gg 0}$ such that $\mathfrak{p}_i^{h_F} = t_i\mathcal{O}_F$ for each $i \in \{1, 2, 3\}$ and we have

$$\mathfrak{C}'_K = \{[(1, \mathcal{O}_K)]\} \cup \{[(t_i, \mathfrak{P}_i^{h_F})] : i = 1, 2, 3\}$$

of order 4.

Proof. The Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\{\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3\}$ transitively, hence they all have the same order in Cl_K.

By the assumption $I_0(\Phi^r) = I_{K^r}$, Proposition 3.3.5 implies $I_K = I_K^H P_K$. By Table 3.1, the class number h_F is odd, so the group Cl_F injects into Cl_K. Therefore, we have

$$\mathrm{Cl}_K = I_K^H P_K / P_K = \langle \mathrm{Cl}_F, [\mathfrak{P}_1], [\mathfrak{P}_2], [\mathfrak{P}_3] \rangle.$$

Since $h_K^* = 4$, the order of $\langle [\mathfrak{P}_1], [\mathfrak{P}_2], [\mathfrak{P}_3] \rangle$ is divisible by 4. Hence $[\mathfrak{P}_i]$ has even order in Cl_K.

By Lemma 4.3.4, there is $t_i \in F_{\gg 0}$ such that $\mathfrak{p}_i^{h_F} = t_i\mathcal{O}_F$. Hence we have $[(t_i, \mathfrak{P}_i^{h_F})] \in \mathfrak{C}'_K$ as $\mathrm{N}_{K/F}(\mathfrak{P}_i^{h_F}) = \mathfrak{p}_i^{h_F} = t_i\mathcal{O}_F$. By Proposition 3.3.1, under the assumption $I_0(\Phi^r) = I_{K^r}$, the imaginary quadratic field $k \subset K$

has class number one. Hence there is only one ramified prime in k, say p. Then we have $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 = \sqrt{-p}\mathcal{O}_K$ if $k = \mathbb{Q}(\sqrt{-d})$ with $d \neq 1$ or $\mathfrak{P}_1\mathfrak{P}_2\mathfrak{P}_3 = (1+i)\mathcal{O}_K$ otherwise. Since $[\mathfrak{P}_i]$ has even order, no two of $[\mathfrak{P}_i^{h_F}]$ for $i \in \{1,2,3\}$ are the same class in Cl_K and none are the trivial class. Moreover, in the proof of Proposition 4.3.7, we proved $|\mathfrak{C}'_K| = h^*_K$. Therefore we get $\mathfrak{C}'_K = \{[(1,\mathcal{O}_K)]\} \cup \{[(t_i, \mathfrak{P}_i^{h_F})] : i = 1,2,3\}$ of order 4. □

The following proves *(iii)* in Theorem 4.3.1.

Proposition 4.3.12. *Let K be a cyclic sextic CM field with $h^*_K = 4$ and let Φ be a primitive CM type of K. Let F be the totally real cubic subfield of K. Suppose $I_0(\Phi^r) = I_{K^r}$. Then there are four isomorphism classes of principally polarized simple abelian threefolds over $\mathbb{C}$.* Exactly *one of these classes has $\mathbb{Q}$ as the field of moduli and the other three have field of moduli F.*

Proof. Let CM_Φ be the isomorphism classes of principally polarized *simple* abelian threefolds over $\mathbb{C}$ of type (K,Φ) with CM by $\mathcal{O}_K$. The set CM_Φ is not empty by Corollary 4.3.6 and, indeed, by Proposition 4.3.7 it holds that $|\mathrm{CM}_\Phi| = 4$.

We first prove that there is *at least* one isomorphism class in CM_Φ with field of moduli $\mathbb{Q}$. Then we prove there is *only* one such isomorphism class in CM_Φ.

Let $\mathrm{Aut}(\mathbb{C})$ act on CM_Φ with $(\sigma,[P]) \mapsto [{}^\sigma P]$. Under the assumption $I_0(\Phi^r) = I_{K^r}$, Theorem 1.5.6 implies that for each $[P] \in \mathrm{CM}_\Phi$, we have $M_\mathbb{Q} \subset K^r \cong K$. Identify K with K^r. Then Theorem 4.2.1-(i) tells us $M_K = K$. Moreover, Lemma 4.3.10 says that ρ acts trivially on CM_Φ and hence $G' = \mathrm{Gal}(K/\mathbb{Q})/\langle\rho\rangle$ acts on CM_Φ. Since $|G'| = 3$, by the orbit-stabilizer theorem (see Lang [22, Proposition 5.5.1 in I]) the size of each orbit is 1 or 3. This means that the action is either trivial or has one orbit of length 1 and one orbit of length 3. This implies that there is *at least* one isomorphism class in CM_Φ with field of moduli $\mathbb{Q}$. We will now show that the action of G' on CM_Φ is not trivial, in other words, we will prove that there is *only* one isomorphism class in CM_Φ with field of moduli $\mathbb{Q}$.

Suppose that G' acts on CM_Φ trivially. This implies that the field of moduli $M_\mathbb{Q}$ of each $[P] \in \mathrm{CM}_\Phi$ is $\mathbb{Q}$ and P is fixed by $\mathrm{Gal}(M_K/\mathbb{Q})$. Hence for every $[P] \in \mathrm{CM}_\Phi$, we have $({}^\sigma P : P) = 1$ for all $\sigma \in \mathrm{Aut}(\mathbb{C})$. Let $[P']$ be an element of CM_Φ such that $P \ncong P'$. Then by Proposition 1.5.2 and (1.5.6), there is a non-trivial $[(b, \mathfrak{c})] \in \mathfrak{C}'_K$ such that $(P' : P) = [(b, \mathfrak{c})]$.

Let $\mathrm{Gal}(K/\mathbb{Q}) = \langle y \rangle$ and let $\sigma \in \mathrm{Aut}(\mathbb{C})$ be such that $\sigma|_K = y$. Then by Proposition 4.2.5-(iii), we have

$$({}^\sigma P' : P') = [((yb)b^{-1}, (y\mathfrak{c})\mathfrak{c}^{-1})] \in \mathfrak{C}'_K.$$

Therefore, we have ${}^\sigma P' \cong P'$ if and only if $(y\mathfrak{c})/\mathfrak{c}$ is a principal ideal.

Let $p\mathcal{O}_F = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$ and $\mathfrak{p}_i\mathcal{O}_K = \mathfrak{P}_i^2$. Then by Lemma 4.3.11, we have

$$\mathfrak{C}'_K = \{[(1, \mathcal{O}_K)]\} \cup \{[(t_i, \mathfrak{P}_i^{h_F})] : i = 1, 2, 3\}$$

Since $\mathrm{Gal}(K/\mathbb{Q}) = \langle y \rangle$ acts on $\{\mathfrak{P}_1, \mathfrak{P}_2, \mathfrak{P}_3\}$ transitively, without loss of generality we have

$$y\mathfrak{P}_1 = \mathfrak{P}_2,\ y\mathfrak{P}_2 = \mathfrak{P}_3, \text{ and } y\mathfrak{P}_3 = \mathfrak{P}_1.$$

So by Lemma 4.3.11, we have $[(t_2t_1^{-1}, (\mathfrak{P}_2\mathfrak{P}_1^{-1})^{h_F})] \neq 0$. Hence ${}^\sigma P'$ is not isomorphic to P' for some $\sigma \in \mathrm{Aut}(\mathbb{C})$. This proves that G' does not act on CM_Φ trivially.

This proves that for exactly one isomorphism class in CM_Φ, we have $M_\mathbb{Q} = \mathbb{Q}$. Moreover, since ρ acts trivially on CM_Φ, the other three isomorphism classes in CM_Φ have field of moduli $F^r = F$. □

4.4 Genus-3 CM curve examples over $\mathbb{Q}$

In this section we give some examples.

Example 4.4.1. *The curve*

$$C : y^2 = x^7 + 1$$

has CM by $\mathbb{Z}[\zeta_7]$ via $\zeta_7(x, y) = (\zeta_7 x, y)$ of type $\Phi = \{1, \overline{3}, \overline{3}^2\} \subset (\mathbb{Z}/7\mathbb{Z})^\times$. It is defined over $\mathbb{Q}$. See (II) on page 76 in Shimura [38]

Example 4.4.2. *The curve*

$$C : y^3 = x^4 - x$$

is a Picard curve which has CM by $\mathbb{Z}[\zeta_9]$ via $\zeta_9(x,y) = (\zeta_9^3 x, \zeta_9 y)$ of type $\Phi = \{1, \overline{2}, \overline{2}^2\} \subset (\mathbb{Z}/9\mathbb{Z})^\times$. It is defined over $\mathbb{Q}$. See Lemma 5.1-(a) in [8].

Example 4.4.3. *The curve*

$$C : y^2 = (x^3 - x^2 - 2x + 1)^2 x - 2x$$

is a hyperelliptic curve over $\mathbb{Q}$ with CM by $\mathbb{Z}[\zeta_7 + \zeta_7^{-1}, i]$ and a primitive CM type $\Phi = \{(\overline{0}, \overline{1}), (\overline{1}, \overline{2}), (\overline{0}, \overline{3})\} \subset \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times (\mathbb{Z}/7\mathbb{Z})^\times / \langle \pm 1 \rangle$. See Proposition 4 in Tautz, Top and Verberkmoes [44].

Example 4.4.4.

(i) For hyperelliptic curves corresponding to the fields $K = F(i)$, where $F \cong \mathbb{Q}[X]/(p(X))$ and

$$p(X) \in \{X^3 - 3X - 1,\ X^3 + 2X^2 - 5X + 1,\\ X^3 + X^2 - 2X - 1,\ X^3 + X^2 - 10X - 8\},$$

models have been computed that are correct up to some precision over $\mathbb{C}$. These models are defined over $\mathbb{Q}$, see Weng [48].

Note that the sextic CM field $K = F(i)$ with $F \cong \mathbb{Q}[X]/(p(X))$, where $p(X) = X^3 + X^2 - 2X - 1$ corresponds to the CM curve in Example 4.4.3.

(ii) For Picard curves corresponding to the fields $K = F(\zeta_3)$, where $F \cong \mathbb{Q}[X]/(p(X))$ and

$$p(X) \in \{X^3 + X^2 - 4X + 1,\ X^3 + X^2 - 2X - 1,\\ X^3 + X^2 - 10X - 8,\ X^3 - 3X - 1,\\ X^3 + X^2 - 14X + 8\}$$

models have been computed that are correct up to some precision over $\mathbb{C}$. These models are defined over $\mathbb{Q}$, see Koike–Weng [19].

Note that the sextic CM field $K = F(\zeta_3)$ with $F \cong \mathbb{Q}[X]/(p(X))$, where $p(X) = X^3 - 3X - 1$ corresponds to the CM curve in Example 4.4.2.

Example 4.4.5. *Let C be a Picard curve defined over a field k_0 with* $\mathrm{char}(k_0) \neq 2$ *and* 3. *Without loss of generality, we may assume that C is given by*

$$C : y^3 = x^4 + g_2x^2 + g_3x + g_4, \text{ where } g_i \in k_0.$$

If $g_2g_3 \neq 0$, then C is defined over the field of moduli, see Koike–Weng [19, page 504].

Bibliography

[1] Steven Arno, Michael L. Robinson, and Ferrell S. Wheeler. Imaginary quadratic fields with small odd class number. *Acta Arith.*, 83(4):295–330, 1998.

[2] Alan Baker. Linear forms in the logarithms of algebraic numbers. I, II, III. *Mathematika 13 (1966), 204-216; ibid. 14 (1967), 102-107; ibid.*, 14:220–228, 1967.

[3] Karim Belabas. Enumerates cubic number fields, version 1.2, 22-07-2011. `http://www.math.u-bordeaux1.fr/~kbelabas/research/software/cubic-1.2.tgz`.

[4] Karim Belabas. A fast algorithm to compute cubic fields. *Math. Comp.*, 66(219):1213–1237, 1997.

[5] Sofiène Bessassi. Bounds for the degrees of CM-fields of class number one. *Acta Arith.*, 106(3):213–245, 2003.

[6] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, second edition, 2004.

[7] Gaetan Bisson and Marco Streng. On polarised class groups of orders in quartic CM-fields. *Accepted for publication in Mathematical Research Letters*, 2015.

[8] Irene Bouw, Jenny Cooley, Kristin E. Lauter, Elisa L. Garcia, Michelle Manes, Rachel Newton, and Ekin Ozman. Bad reduction of genus three curves with Complex Multiplication. `http://arxiv.org/pdf/1407.3589v2.pdf`, 2014.

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

[10] Henri Cohen. *Advanced topics in computational number theory*, volume 193 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000.

[11] David A. Cox. *Primes of the form x^2+ny^2*. Pure and Applied Mathematics (Hoboken). John Wiley & Sons, Inc., Hoboken, NJ, second edition, 2013. Fermat, class field theory, and complex multiplication.

[12] Bruce Dodson. The structure of Galois groups of CM-fields. *Trans. Amer. Math. Soc.*, 283(1):1–32, 1984.

[13] David Kohel et al. Echidna algorithms for algebra and geometry experimentation. `http://echidna.maths.usyd.edu.au/~kohel/dbs/complex_multiplication2.html`.

[14] Eyal Z. Goren and Kristin E. Lauter. Genus 2 curves with complex multiplication. *Int. Math. Res. Not. IMRN*, (5):1068–1142, 2012.

[15] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52.

[16] Kurt Heegner. Diophantische Analysis und Modulfunktionen. *Math. Z.*, 56:227–253, 1952.

[17] Pınar Kılıçer. Sage packages for computing (non-biquadratic) quartic fields with CM class number one. `http://pub.math.leidenuniv.nl/~kilicerp/codes/`, 2015.

[18] Pınar Kılıçer and Marco Streng. The CM class number one problem for curves of genus 2. `http://arxiv.org/pdf/1511.04869v1.pdf`, 2015.

[19] Kenji Koike and Annegret Weng. Construction of CM Picard curves. *Math. Comp.*, 74(249):499–518 (electronic), 2005.

[20] Serge Lang. *Complex multiplication*, volume 255 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, New York, 1983.

[21] Serge Lang. *Algebraic number theory*, volume 110 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994.

[22] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[23] Stéphane Louboutin. On the class number one problem for nonnormal quartic CM-fields. *Tohoku Math. J. (2)*, 46(1):1–12, 1994.

[24] Stéphane Louboutin. CM-fields with cyclic ideal class groups of 2-power orders. *J. Number Theory*, 67(1):1–10, 1997.

[25] Stéphane Louboutin. Explicit upper bounds for residues of Dedekind zeta functions and values of L-functions at $s = 1$, and explicit lower bounds for relative class numbers of CM-fields. *Canad. J. Math.*, 53(6):1194–1222, 2001.

[26] Stéphane Louboutin. Explicit lower bounds for residues at $s = 1$ of Dedekind zeta functions and relative class numbers of CM-fields. *Trans. Amer. Math. Soc.*, 355(8):3079–3098, 2003.

[27] Stéphane Louboutin, Ryotaro Okazaki, and Michel Olivier. The class number one problem for some non-abelian normal CM-fields. *Trans. Amer. Math. Soc.*, 349(9):3657–3678, 1997.

[28] Teruhisa Matsusaka. On a characterization of a Jacobian variety. *Memo. Coll. Sci. Univ. Kyoto. Ser. A. Math.*, 32:1–19, 1959.

[29] James S. Milne. Jacobian varieties. In *Arithmetic geometry (Storrs, Conn., 1984)*, pages 167–212. Springer, New York, 1986.

[30] Naoki Murabayashi. The field of moduli of abelian surfaces with complex multiplication. *J. Reine Angew. Math.*, 470:1–26, 1996.

[31] Naoki Murabayashi and Atsuki Umegaki. Determination of all $\mathbf{Q}$-rational CM-points in the moduli space of principally polarized abelian surfaces. *Sūrikaisekikenkyūsho Kōkyūroku*, (1160):169–176, 2000. Analytic number theory and related topics (Japanese) (Kyoto, 1999).

[32] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[33] PARI. Pari/gp computer algebra system. `http://pari.math.u-bordeaux.fr/`.

[34] Young-Ho Park and Soun-Hi Kwon. Determination of all imaginary abelian sextic number fields with class number ≤ 11. *Acta Arith.*, 82(1):27–43, 1997.

[35] Ziv Ran. On subvarieties of abelian varieties. *Invent. Math.*, 62(3):459–479, 1981.

[36] SageMath. SageMath mathematics software, version 6.0. `http://www.sagemath.org/`.

[37] Jean-Pierre Serre. Quelques propriétés des variétés abéliennes en caractéristique p. *Amer. J. Math.*, 80:715–739, 1958.

[38] Goro Shimura. On abelian varieties with complex multiplication. *Proc. London Math. Soc. (3)*, 34(1):65–86, 1977.

[39] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*, volume 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

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

[41] Harold M. Stark. A complete determination of the complex quadratic fields of class-number one. *Michigan Math. J.*, 14:1–27, 1967.

[42] Marco Streng. RECIP – REpository of Complex multIPlication sage code. `http://pub.math.leidenuniv.nl/~strengtc/recip/`.

[43] Marco Streng. Computing Igusa class polynomials. *Math. Comp.*, 83(285):275–309, 2014.

[44] Walter Tautz, Jaap Top, and Alain Verberkmoes. Explicit hyperelliptic curves with real multiplication and permutation polynomials. *Canad. J. Math.*, 43(5):1055–1064, 1991.

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

[46] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.

[47] André Weil. Zum Beweis des Torellischen Satzes. *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.*, 1957:33–53, 1957.

[48] Annegret Weng. A class of hyperelliptic CM-curves of genus three. *J. Ramanujan Math. Soc.*, 16(4):339–372, 2001.

Summary

Let E be an elliptic curve over $\mathbb{C}$ with *complex multiplication (CM)* by the maximal order $\mathcal{O}_K$ of an imaginary quadratic field K. The first main theorem of complex multiplication for elliptic curves then states that the field extension $K(j(E))$, obtained by adjoining the j-invariant of E to K, is equal to the *Hilbert class field* of K, see Theorem 11.1 in Cox [11]. Note that if E is defined over $\mathbb{Q}$, then the Hilbert class field $K(j(E))$ is equal to K, which implies that the class group Cl_K is trivial.

We can ask for which imaginary quadratic fields K the corresponding elliptic curve with CM by $\mathcal{O}_K$ is defined over $\mathbb{Q}$. This is equivalent to asking to find all imaginary quadratic fields with trivial class group Cl_K. This problem is known as Gauss' class number one problem, which was solved by Heegner in 1952 [16], Baker in 1967 [2], and Stark in 1967 [41]. The imaginary quadratic fields with trivial class group are the fields $\mathbb{Q}(\sqrt{-d})$ with $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$.

In the 1950's, Shimura and Taniyama [39] generalized the first main theorem of CM for elliptic curves to *abelian varieties*. We say that an abelian variety A of dimension g has CM if the endomorphism ring of A contains an order of a *CM field* of degree $2g$. Let K be a CM field of degree $2g$ with maximal order $\mathcal{O}_K$, and let Φ be a *CM type* of K. Let A be a polarized simple abelian variety over $\mathbb{C}$ of dimension g that has CM by $\mathcal{O}_K$. Then the first main theorem of CM says that the field of moduli M of the polarized simple abelian variety A gives an unramified class field H over the *reflex field* K^r of K. Moreover, the class field H corresponds to the ideal group $I_0(\Phi^r)$ (see page 17), which only depends on (K, Φ), see Theorem 1.5.6. Note that the first main theorem of CM implies that if the polarized abelian variety A is defined over K^r, then *the CM class group* $I_{K^r}/I_0(\Phi^r)$ is trivial.

As in the elliptic curve case, we can ask for which CM pairs (K, Φ) the corresponding CM abelian varieties are defined over K^r. Equivalently, we can ask for which CM pairs (K, Φ) the *CM class group* $I_{K^r}/I_0(\Phi^r)$ is

trivial. In this thesis we give an answer to this problem for quartic CM fields (see Chapter 2), and for sextic CM fields containing an imaginary quadratic field (see Chapter 3).

Furthermore, we can ask for which CM fields the corresponding simple CM abelian varieties have field of moduli $\mathbb{Q}$. Murabayashi and Umegaki [31] determined the quartic CM fields that correspond to a simple CM abelian surface with field of moduli $\mathbb{Q}$. In Chapter 4, we determine the sextic CM fields that correspond to a simple CM abelian threefold with field of moduli $\mathbb{Q}$.

Samenvatting

Zij E een elliptische kromme over $\mathbb{C}$ met *complexe vermenigvuldiging (CM)* over de ring van gehelen $\mathcal{O}_K$ van een imaginair kwadratisch lichaam K. Dan stelt de eerste hoofdstelling van de theorie van complexe vermenigvuldiging van elliptische krommen dat de lichaamsuitbreiding $K(j(E))$, verkregen door het adjungeren van de j-invariant van E aan K, het *Hilbertklasselichaam* van K is, zie [11, Theorem 11.1]. Als E gedefinieerd is over $\mathbb{Q}$, dan is $K(j(E))$ gelijk aan K, wat impliceert dat de klassegroep Cl_K triviaal is.

We kunnen ons afvragen voor welke imaginaire kwadratische lichamen K de corresponderende elliptische kromme met CM over $\mathcal{O}_K$ gedefinieerd is over $\mathbb{Q}$. Dit is equivalent met het vinden van alle imaginaire kwadratische lichamen met triviale klassegroep, wat bekend is als het klassegetal-één-probleem van Gauss. Dit probleem is opgelost door Heegner in 1952 [16], door Baker in 1967 [2] en door Stark in 1967 [41]; de imaginaire kwadratische lichamen van klassegetal één zijn de lichamen $\mathbb{Q}(\sqrt{-d})$ met $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$.

In de jaren '50 hebben Shimura en Taniyama [39] de eerste hoofdstelling van de theorie van complexe vermenigvuldiging van elliptische krommen gegeneraliseerd naar *abelse variëteiten*. Een abelse variëteit A van geslacht g heeft CM als de endomorfismering van A een orde bevat in een *CM-lichaam* van graad $2g$. Zij K een CM-lichaam van graad $2g$ met maximale orde $\mathcal{O}_K$ en zij Φ een CM type van K. Zij A een gepolariseerde simpele abelse variëteit over $\mathbb{C}$ van dimensie g met CM over $\mathcal{O}_K$. Dan stelt de eerste hoofdstelling van complexe vermenigvuldiging voor abelse variëteiten dat het lichaam van moduli M van de gepolariseerde simpele abelse variëteit A een onvertakt klasselichaam H over het *reflexlichaam* K^r van K geeft. Het klasselichaam H correspondeert met de ideaalgroep $I_0(\Phi^r)$ (zie pagina 17) die alleen afhankelijk is van (K, Φ), zie Stelling 1.5.6. Merk op dat de eerste hoofdstelling van de complexe vermenigvuldiging impliceert dat als de gepolariseerde simpele

abelse variëteit A gedefinieerd is over K^r, dat dan de *CM-klassegroep* $I_{K^r}/I_0(\Phi^r)$ triviaal is.

Analoog aan het elliptischekrommengeval, vragen we ons af voor welke CM-paren (K, Φ) de corresponderende CM abelse variëteit gedefinieerd is over K^r. Anders gezegd, voor welke CM-paren (K, Φ) is de *CM-klassegroep* $I_{K^r}/I_0(\Phi^r)$ triviaal. In dit proefschrift geven we een antwoord op dit probleem voor vierdegraads CM-lichamen (zie hoofdstuk 2) en voor zesdegraads CM-lichamen die een imaginair kwadratisch lichaam bevatten (zie hoofdstuk 3).

Verder vragen we ons af voor welke CM-lichamen de corresponderende CM abelse variëteiten lichaam van moduli gelijk aan $\mathbb{Q}$ hebben. Murabayashi en Umegaki [31] hebben de vierdegraads CM-lichamen bepaald die corresponderen met een simpel CM abels oppervlak met lichaam van moduli gelijk aan $\mathbb{Q}$. In hoofdstuk 4 bepalen wij de zesdegraads CM-lichamen die corresponderen met een simpele CM abelse variëteit van dimensie 3 met lichaam van moduli gelijk aan $\mathbb{Q}$.

Résumé

Soit E une courbe elliptique sur $\mathbb{C}$ ayant multiplication complexe (CM) par l'ordre maximal $\mathcal{O}_K$ d'un corps quadratique imaginaire K. Le premier théorème principal de la multiplication complexe affirme que le corps $K(j(E))$, obtenu en adjoignant à K le j-invariant de E, est égal au *corps de classes de Hilbert* de K, confer Cox [11, Theorem 11.1]. Notons que lorsque E est définie sur $\mathbb{Q}$, le corps de classes de Hilbert $K(j(E))$ est égal à K et le groupe des classes Cl_K est trivial.

Se pose alors le problème de déterminer les corps quadratiques totalement imaginaires K pour lesquels la courbe elliptique à multiplication complexe par $\mathcal{O}_K$ correspondante est définie sur $\mathbb{Q}$. De façon équivalente, il s'agit de trouver tous les corps quadratiques imaginaires dont le groupe des classes est trivial. Ce problème est connu sous le nom de problème du nombre de classes 1 de Gauss et a été résolu par Heegner en 1952 [16], Baker en 1967 [2] et Stark en 1967 [41]; les corps quadratiques imaginaires dont le groupe des classes est trivial sont les corps $\mathbb{Q}(\sqrt{-d})$, où $d \in \{3, 4, 7, 8, 11, 19, 43, 67, 163\}$.

Dans les années '50, Shimura et Taniyama [39] ont généralisé le premier théorème principal de la multiplication complexe aux *variétés abéliennes*. On dit qu'une variété abélienne A de dimension g a multiplication complexe si son anneau d'endomorphismes contient un ordre d'un *corps CM* de degré $2g$. Soit K un corps CM de degré $2g$ et d'ordre maximal $\mathcal{O}_K$ et soit Φ un type CM de K. Soit A une variété abélienne complexe simplement polarisée de dimension g ayant multiplication complexe par $\mathcal{O}_K$. Le premier théorème principal de la multiplication complexe dans ce cadre affirme que le corps de classes H du corps du modules M de la variété abélienne simplement polarisée A est une extension non ramifiée du *corps reflex* K^r de K. De plus, le corps des classes H correspond au groupe d'idéaux $I_0(\Phi^r)$ (voir page 17) qui ne dépend que de (K, Φ), confer Théorème 1.5.6. Notons que le premier théorème de la multiplication complexe implique que si la variété abélienne polarisée A est définie

sur K^r, le *groupe des classes CM* $I_{K^r}/I_0(\Phi^r)$ est trivial.

Comme dans le cas des courbes elliptiques, on peut alors chercher à déterminer les couples CM (K, Φ) pour lesquels les variétés abéliennes correspondantes sont définies sur K^r. De façon équivalente, il s'agit de déterminer les couples CM (K, Φ) dont le *groupe des classes CM*, $I_{K^r}/I_0(\Phi^r)$, est trivial. Dans cette thèse, on résout ce problème dans le cas des corps CM quartiques imaginaires (voir Chapitre 2) ainsi que dans celui des corps CM sextiques contenant un corps quadratique imaginaire (voir Chapitre 3).

Enfin, on peut se demander quels sont les corps CM pour lesquels la variété abélienne simple à multiplication complexe admet $\mathbb{Q}$ comme corps de module. Murabayashi et Umegaki [31] ont déterminé les corps quartiques CM correspondant aux surfaces abéliennes simples à multiplication complexe de corps du module $\mathbb{Q}$. Dans le chapitre 4, on détermine les corps CM sextiques correspondant aux variétés abéliennes simples à multiplication complexe de dimension 3 de corps du module $\mathbb{Q}$.

Acknowledgement

I wish to sincerely thank my supervisor, Marco Streng, for introducing me to this problem and encouraging me on my journey. His guidance was crucial during the research and the writing stage of the dissertation. I also wish to thank my promotor, Peter Stevenhagen, for always being like a father figure to us all, and my co-supervisor, Andreas Enge, for his support, especially during the writing process. I wish to thank the reading committee for their time and their comments.

I think of Leiden MI as a big family. Since I began my PhD, I have always felt the support and the solidarity in the department. I wish to thank all the professors in MI for always keeping their doors open to the students who need their help. I also wish to thank Kathelijne for making all the procedures easy for us. I am very grateful to the PhD and master students at MI for making the environment more friendly and more fun. I specially want to thank Maarten for helping me with programming in Sage, Djordjo for sharing the stress of the first serious talk of my career, Chloe for organizing the CM seminar together, Rachel for her advice during Post-Doc applications, Elisa for proposing new problems to me, and Gabriel for helping me with the French summary of the thesis.

My dear Leiden family, Martin, Dino, Abtien, Iuliana, Maarten, and Valerio, we had a memorable time together. Thank you for everything we shared.

Pelin and Käthe, I was very lucky to have you as flatmates. We have established a friendship that will remain lifelong. Pelin, thank you for working with me long nights and early mornings, at home and in the library.

Being apart didn't change much, Ayşegül, Neslihan, Özlem, Nicat, Mehmet, Gülen, Ata. Thank you for being with me, despite the distance.

Finally, I would like to thank my parents and my brother for always encouraging and supporting me in all the decisions I have made.

Curriculum Vitae

Pınar Kılıçer was born in Kayseri in Turkey on May 8, 1986.

She graduated from Sami Yangın Anatolian High School, and entered the Mathematics Department of Middle East Technical University, Ankara in 2004. During her bachelor studies, she studied as an Erasmus Mundus exchange student at the University of Pisa, Italy. She finished her undergraduate studies with honours.

In 2009 she entered the Master of Science program at the Koç University, Istanbul, where she graduated in 2011 under the supervision of Kazım Büyükboduk with a thesis entitled *Stark Conjectures and Hilbert's 12th problem*.

In September 2012 she started her PhD-studies with an Erasmus Mundus ALGANT-DOC fellowship under the supervision of Marco Streng, Andreas Enge and Peter Stevenhagen. After submitting her thesis in February 2016, she visited the Max Planck Institute, Bonn for 3 months.