Computing the Hilbert Class Fields of Quartic CM Fields Using Complex Multiplication

Jared Asuncion

COMPUTING THE HILBERT CLASS FIELDS OF QUARTIC CM FIELDS USING COMPLEX MULTIPLICATION

JARED ASUNCION

Abstract. Let K be a quartic CM field, that is, a totally imaginary quadratic extension of a real quadratic number field. In a 1962 article titled *On the class-fields obtained by complex multiplication of abelian varieties*, Shimura considered a particular family $\{F_K(m) : m \in \mathbb{Z}_{>0}\}$ of abelian extensions of K, and showed that the Hilbert class field H_K of K is contained in $F_K(m)$ for some positive integer m. We make this m explicit. We then give an algorithm that computes a set of defining polynomials for the Hilbert class field using the field $F_K(m)$. Our proof-of-concept implementation of this algorithm computes a set of defining polynomials much faster than current implementations of the generic Kummer algorithm for certain examples of quartic CM fields.

1. Introduction

An abelian extension of a number field K is a Galois extension L/K whose Galois group $\mathrm{Gal}(L/K)$ is abelian. The Kronecker-Weber Theorem states that every abelian extension L of $\mathbb{Q}$ is contained in $\mathbb{Q}(\exp(2\pi i\tau) : \tau \in \mathbb{Q})$, the field obtained by adjoining to $\mathbb{Q}$ the values of the analytic map $\tau \mapsto \exp(2\pi i\tau)$ evaluated at $\mathbb{Q}$. The twelfth out of the twenty-three problems Hilbert posed in 1900 asks, roughly speaking, whether a statement analogous to the Kronecker-Weber Theorem can be made for number fields K different from $\mathbb{Q}$.

One tool in attacking this problem is the theory of complex multiplication (CM), developed by Shimura [Shi94; Shi98a] during the second half of the 20th century. CM theory works for a specific family of number fields, called CM fields. A CM field K is a totally imaginary quadratic extension of a totally real number field K_0.

For a CM field K, class field theory proves the existence of the family

$$\mathcal{F} = \{H_K(m) : m \in \mathbb{Z}\}$$

of *ray class fields* of K. Every finite degree abelian extension of K is contained in at least one element of $\mathcal{F}$. Given a CM field K and a CM type Φ (defined in Section 2.2), CM theory gives a reflex pair (K^r, Φ^r) consisting of a CM field K^r and CM type Φ^r, and defines a certain field $\mathrm{CM}_{K^r,\Phi^r}(m)$ such that

- $\mathrm{CM}_{K^r,\Phi^r}(m) \subseteq H_{K^r}(m)$, and

INRIA, LFANT, F-33400 Talence, France
CNRS, IMB, UMR 5251, F-33400 Talence, France
Univ. Bordeaux, IMB, UMR 5251, F-33400 Talence, France.
Universiteit Leiden, Postbus 9512, 2300 RA Leiden, The Netherlands.

This project has been supported by a travel grant managed by the Agence Nationale de la Recherche under the program "Investissements d'avenir" and bearing the reference ANR-10-IDEX-03-02.

- $\mathrm{CM}_{K^r,\Phi^r}(m)$ is an algebraic extension of K^r that can be obtained by adjoining to K^r algebraic numbers which are *special values of modular functions*. These are the analogue of $\exp(2\pi i\tau)$.

For the case when K is a CM field of degree 2, it has been shown that $K = K^r$ and $\mathrm{CM}_{K^r,\Phi^r}(m)$ is exactly the ray class field $H_K(m)$. This is not the case for higher-degree CM fields. In fact, the field K is not necessarily equal to K^r for the next simplest case – CM fields of degree 4. One natural question to then ask is: can one use CM theory to compute ray class fields $H_K(m)$ of quartic CM fields K, and if so how?

We answer this question for the case of $H_K(1)$. We show how one can use CM theory to compute the Hilbert class field $H_K(1)$, the largest unramified abelian extension, of a quartic CM field K. Using this theoretical result, we give an algorithm which computes $H_K(1)$ for quartic CM fields satisfying properties elaborated on later in this article. Finally, we write a proof-of-concept implementation of this algorithm, which we use to find defining polynomials of Hilbert class fields of quartic CM fields. Using this implementation, we found that this algorithm succeeds to compute the Hilbert class field of certain quartic CM fields in which current implementations of the well-known Kummer theory algorithm take much longer.

For any number field K and any positive integer m, let $E_K(m)$ be the smallest subfield of $H_K(m)$ containing K such that $\mathrm{Gal}(H_K(m)/E_K(m))$ is of exponent at most 2. The main theoretical result of this article, which we specialize to the case of primitive quartic CM fields in Corollary 1.3, is as follows.

Theorem 1.1. Let K be a number field without real embeddings. Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that

- $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd,
- S contains all prime ideals above 2,
- S contains at least 3 elements.

Let $P_S = \{p : p \text{ is a rational prime below } \mathfrak{p} \text{ for some } \mathfrak{p} \in S\}$. Let $m_S = 4 \cdot \prod_{p\in P_S} p$. Then $H_K(1) \subseteq E_K(m_S)$.

The existence of a positive integer m such that $H_K(1) \subseteq E_K(m)$ was already known by Shimura, via the proof of [Shi62, Theorem 2]. Theorem 1.1 gives a formula for such an m thereby making an effective version of Shimura's result.

We will be using a result of Shimura [Shi62], later refined by Streng, which gives an example of a field that is 'close' but not quite the Hilbert class field.

Theorem 1.2 ([Str10, Theorem I.10.3])**.** Let K be a quartic CM field which is not bicyclic Galois[1] and Φ a CM type of K, and let (K^r, Φ^r) be the reflex CM pair of (K, Φ). Then the Galois group $\mathrm{Gal}(H_{K^r}(m)/H_{K_0^r}(m)\,\mathrm{CM}_{K^r,\Phi^r}(m))$ is abelian of exponent at most 2 for any positive integer m.

There is also analogous result [Str10, Theorem I.10.5] similar to the above theorem when K is bicyclic Galois.

[1]Equivalently, it is either cyclic Galois or not Galois.

Theorem 1.2 tells us that the field $H_{K^r}(1)$ is obtained by adjoining square roots of elements from the compositum $H_{K_0^r}(1)\,\mathrm{CM}_{K^r,\Phi^r}(1)$. One can determine which square roots must be added using a generic algorithm given by Kummer theory. However, the Kummer theory algorithm requires the computation of ray class groups of the compositum $H_{K_0^r}(1)\,\mathrm{CM}_{K^r,\Phi^r}(1)$. Algorithms to compute class groups are known to not perform very well [Bel04, page 3] for large-degree number fields. We avoid this issue by instead computing a larger field containing the Hilbert class field $H_{K^r}(1)$ and using Galois theory to eventually find a defining polynomial for $H_{K^r}(1)$. Our method only involves computing ray class groups of number fields of degree at most 4.

Suppose that m is an integer and that (K,Φ) and (K^r,Φ^r) are as in the assumptions of Theorem 1.2. We denote by $(\star_m)$ the expression

$$(\star_m) \qquad H_{K^r}(1) \subseteq H_{K_0^r}(m)\,\mathrm{CM}_{K^r,\Phi^r}(m).$$

Corollary 1.3. Let (K,Φ) be a CM pair, with K being a quartic CM field which is not bicyclic Galois, and let (K^r,Φ^r) be its reflex CM pair. Let m_S be as in Theorem 1.1. Then $(\star_{m_S})$ holds.

Proof. Theorem 1.2 gives

$$H_K(1) \subseteq E_K(m_S)$$

and Theorem 1.1 gives

$$E_K(m_S) \subseteq H_{K_0^r}(m)\,\mathrm{CM}_{K^r,\Phi^r}(m).$$

■

Using this corollary, one can compute

$$H_{K_0^r}(m_S)\,\mathrm{CM}_{K^r,\Phi^r}(m_S)$$

then use Galois theory to finally compute a defining polynomial for the subfield we are interested in, the Hilbert class field $H_{K^r}(1)$.

This article is divided into several sections. In Section 2, we define objects and recall results from class field theory and CM theory that we use for the rest of the article. In Section 3, we prove Theorem 1.1. In Section 4, we give an algorithm that tells us whether or not $(\star_m)$ holds for any integer m.

In Section 5, we discuss how to obtain, in the case where $(\star_2)$ holds, a set $\boldsymbol{\beta}$ of algebraic numbers such that $H_{K^r}(1) = K^r(\boldsymbol{\beta})$. In that section, we also discuss how our implementation of this algorithm fares against the generic Kummer theory algorithm.

One may note that the formula for m_S in Corollary 1.3 implies that $m_S \geq 8$. An algorithm to compute a defining polynomial for $\mathrm{CM}_{K^r,\Phi^r}(m)/K^r$ where $m > 2$ will be the topic of a future article.

2. Preliminaries

In this section, we define the mathematical objects informally introduced in Section 1.

Section 2.1 is dedicated to reviewing class field theory and the ray class field $H_K(m)$ of a number field K.

Section 2.2 reviews the theory of complex multiplication, CM theory. There, we define CM fields, their reflexes, type norms and the field $\mathrm{CM}_{K^r,\Phi^r}(m)$ referenced in this article's introduction.

2.1. **Class Field Theory.** This section is concerned with defining class field theory concepts needed for this article. For a more thorough treatment of class field theory, see [Neu99].

Let F be a number field and denote by $\mathcal{O}_F$ its ring of integers.

A *fractional ideal* of $\mathcal{O}_F$ is an $\mathcal{O}_F$-submodule $\mathfrak{n}$ of F such that there exists a $d \in \mathbb{Z}$ such that $d\mathfrak{n}$ is a nonzero ideal of $\mathcal{O}_F$. Denote by I_F the group of fractional ideals of $\mathcal{O}_F$ and denote by P_F its subgroup of fractional ideals generated by a single element. The quotient I_F/P_F forms a finite group which we call *the ideal class group* of F, denoted by Cl_F.

Let $\mathcal{P}$ be the union of the set of prime ideals of $\mathcal{O}_F$ (finite places) and the set of real embeddings and conjugate pairs of complex embeddings of F (infinite places). A *modulus* $\mathfrak{m}$ for F is a function $\mathfrak{m} : \mathcal{P} \to \mathbb{Z}_{\geq 0}$ such that $\mathfrak{m}(\mathfrak{p}) = 0$ for all but finitely many prime ideals $\mathfrak{p}$, and $\mathfrak{m}(\sigma) \leq 1$ when σ is a real embedding of F, and $\mathfrak{m}(\sigma) = 0$ when σ is a complex embedding of F. If F is totally imaginary, meaning that is has no real embeddings, then the map

$$\mathfrak{a} \quad \mapsto \quad \left(\mathfrak{m}_\mathfrak{a} : \mathfrak{p} \mapsto \begin{cases} \mathrm{ord}_\mathfrak{p}(\mathfrak{a}) & \mathfrak{p} \text{ is a finite place} \\ 0 & \mathfrak{p} \text{ is an infinite place} \end{cases} \right)$$

is a bijection from the set of nonzero ideals of $\mathcal{O}_F$ to the set of moduli on F. In such a case, we may interchangeably use the terms 'modulus' and 'ideal of $\mathcal{O}_F$'.

For a modulus $\mathfrak{m}$, we denote by $I_F(\mathfrak{m})$ the subgroup of I_F composed of the fractional prime ideals $\mathfrak{p}$ of $\mathcal{O}_F$ which satisfy $\mathfrak{m}(\mathfrak{p}) = 0$. We define $F_{\mathfrak{m},1}$ to be the set of $a \in F^\times$ such that $\mathrm{ord}_\mathfrak{p}(a-1) \geq \mathfrak{m}(\mathfrak{p})$ for all finite primes $\mathfrak{p}$ with $\mathfrak{m}(\mathfrak{p}) \geq 0$ and $\sigma(a) > 0$ for any σ such that $\mathfrak{m}(\sigma) = 1$. The statement '$a \in F_{\mathfrak{m},1}$' is more commonly denoted as $a \equiv 1 \bmod^* \mathfrak{m}$. The latter notation takes preference in this article. Denote by $P_F(\mathfrak{m})$ the subgroup of $I_F(\mathfrak{m})$ generated by fractional ideals of $\mathcal{O}_F$ generated by elements of $F_{\mathfrak{m},1}$. The quotient $I_F(\mathfrak{m})/P_F(\mathfrak{m})$ is a finite group which we call *the ray class group* of F for the modulus $\mathfrak{m}$, denoted by $\mathrm{Cl}_F(\mathfrak{m})$.

One of the main results of class field theory is: given a modulus $\mathfrak{m}$, there exists a finite abelian extension $H_F(\mathfrak{m})/F$, called the *ray class field* of F for the modulus $\mathfrak{m}$, which satisfies

- $H_F(\mathfrak{m})$ is unramified at all primes $v \in \mathcal{P}$ with $\mathfrak{m}(v) > 0$,
- $\mathrm{Cl}_F(\mathfrak{m})$ and $\mathrm{Gal}(H_F(\mathfrak{m})/F)$ are isomorphic via the Artin map [Neu99, Theorem VI.5.5].

A subgroup C of $I_F(\mathfrak{m})$ such that $P_F(\mathfrak{m}) \subseteq H$ is called *a congruence subgroup* modulo $\mathfrak{m}$. Let $\mathfrak{m}$ be a modulus for F. Galois theory gives a bijection between the set of congruence subgroups modulo $\mathfrak{m}$ and the abelian extensions L/F of F such that $L \subseteq H_F(\mathfrak{m})$. In particular, if C is a congruence subgroup modulo $\mathfrak{m}$ which corresponds to the abelian extension L of F, contained in $H_F(\mathfrak{m})$, then

$$\mathrm{Gal}(H_F(\mathfrak{m})/L) \cong C/P_F(\mathfrak{m}) \qquad \text{and} \qquad \mathrm{Gal}(L/F) \cong I_F(\mathfrak{m})/C.$$

If $n \in \mathbb{Z}_{>0}$, and $\mathfrak{n}(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}(n)$ for all prime ideals of $\mathcal{O}_F$ and $\mathfrak{n}(\sigma) = 0$ for all real embeddings of F, then we may write $I_F(n), P_F(n), \mathrm{Cl}_F(n)$ and $H_F(n)$ instead of $I_F(\mathfrak{n}), P_F(\mathfrak{n})$, $\mathrm{Cl}_F(\mathfrak{n})$ and $H_F(\mathfrak{n})$. With this notation, $H_F = H_F(1)$ is *the Hilbert class field* of F. On the other hand, if $\mathfrak{n}(\mathfrak{p}) = \mathrm{ord}_{\mathfrak{p}}(n)$ for all prime ideals of $\mathcal{O}_F$ and $\mathfrak{n}(\sigma) = 1$ for all real embeddings of $\mathcal{O}_F$, then we may write $I_F^+(n), P_F^+(n), \mathrm{Cl}_F^+(n)$ and $H_F^+(n)$ instead of $I_F(\mathfrak{n}), P_F(\mathfrak{n})$, $\mathrm{Cl}_F(\mathfrak{n})$ and $H_F(\mathfrak{n})$. With this notation, $H_F^+ = H_F^+(1)$ is *the narrow Hilbert class field* of F.

2.2. **CM Theory.** In this section, we set notation and recall results of complex multiplication (CM) theory that we use to define $\mathrm{CM}_{K^r,\Phi^r}(m)$ and other objects introduced in later chapters. For a more complete treatment of CM theory, the reader is referred to [Shi98a; Str10].

A *CM field* K is a totally imaginary number field which is a quadratic extension of a totally real field K_0. The degree of a CM field is its degree as a number field. Hence, any CM field has even degree. For the rest of Section 2.2, we fix a CM field K of degree $2g$.

Denote by ρ the sole generator of the group $\mathrm{Gal}(K/K_0)$, a group of order 2. This can be thought of as the *complex conjugation* morphism because for any embedding $\phi : K \hookrightarrow \mathbb{C}$, we have $\phi(\rho(x)) = \overline{\phi(x)}$.

Let L be the Galois closure of the CM field K, and fix an embedding $\iota_{\mathbb{C}} : L \to \mathbb{C}$. The CM field K has g complex conjugate pairs of embeddings into $\mathbb{C}$. By applying the 'inverse' of $\iota_{\mathbb{C}}$ to each embedding $\sigma : K \to \mathbb{C}$, we can think of these $2g$ complex embeddings as embeddings into L. A set Φ is called a *CM type* of F if it contains g complex embeddings of F into L such that for any $\phi, \phi' \in \Phi$, $\phi' \neq \phi \circ \rho$.

Let K_2/K_1 be an extension of CM fields, with L_2 the Galois closure of K_2. Let Φ_1 be a CM type on K_1. The CM type *induced by* Φ_1 *on* K_2 is defined to be

$$\Phi_2 = \{\phi : K_2 \hookrightarrow L_2 : \phi|_{K_1} \in \Phi_1\}.$$

A CM type of K is said to be *primitive* if it is not induced from a CM type of a strict CM subfield of K. Two CM types of Φ, Φ' are *equivalent* if there is an automorphism σ of K such that $\Phi' = \Phi\sigma$ holds.

We call a pair (K, Φ) *a CM pair*. If Φ is a primitive CM type on K, we say that a CM pair (K, Φ) is *primitive*. Denote by Φ_L the CM type induced by Φ on the Galois closure L, which is also a CM field. Since the elements of Φ_L are automorphisms of L, we can define the set $\Phi_L^{-1} = \{\phi^{-1} : \phi \in \Phi_L\}$. This set Φ_L^{-1} is a CM type of L. There exists a unique subfield K^r of L and a unique CM type Φ^r on K^r such that Φ^r is a primitive CM-type which induces Φ_L^{-1}. The CM pair (K^r, Φ^r) is called the *reflex* of Φ. One property of the reflex field K^r is that

$$\mathrm{Gal}(L/K^r) = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) : \sigma\Phi = \Phi\}. \tag{2.1}$$

If Φ is a primitive CM type of K, then the reflex (K^{r^r}, Φ^{r^r}) of Φ^r is actually equal to (K, Φ).

Let (K, Φ) be a quartic CM pair and let L be its Galois closure. There are three possibilities for the Galois group $G = \mathrm{Gal}(L/\mathbb{Q})$: $G \cong C_2 \times C_2$, $G \cong C_4$ or $G \cong D_4$. For the second and third possibilities, Φ is a primitive CM type, regardless of the choice of Φ.

Let (K, Φ) be a primitive CM pair and let (K^r, Φ^r) be its reflex. Then we have a map $N_{\Phi^r} : K^r \to L$ defined by $y \mapsto \prod_{\phi^r \in \Phi^r} \phi^r(y)$. By Equation (2.1), this is in fact a map to the reflex $K^{rr} = K$ of K^r. We refer to this map as the (reflex) *type norm* map. Some articles refer to it as a *half norm* map since it uses half the number of embeddings as the usual norm map.

Similar to the usual norm map, the type norm map induces maps

$$N_{\Phi^r} : I_{K^r}(m) \to I_K(m) \qquad \text{and} \qquad N_{\Phi^r} : \mathrm{Cl}_{K^r}(m) \to \mathrm{Cl}_K(m)$$

for any positive integer m using [Str10, Lemma I.8.3], which uses [Lan83, Remark on page 63] and [Shi98b, Proposition 29] in its proof. The notation N_{Φ^r} will be used to denote any of the above three maps and the domain will be specified whenever the context of the discussion does not make it clear.

Keeping the notation from the previous paragraph, let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ and denote by m the smallest positive integer in $\mathfrak{m}$. Define the subgroup $I_{K^r,\Phi^r}(\mathfrak{m})$ of $I_{K^r}(m)$ to be

$$I_{K^r,\Phi^r}(\mathfrak{m}) = \left\{ \mathfrak{a} \in I_{K^r}(m) : \begin{array}{c} \exists x \in K^\times \text{ such that} \\ \begin{array}{rcl} N_{\Phi^r}(\mathfrak{a}) & = & x\mathcal{O}_K \\ N_{K^r/\mathbb{Q}}(\mathfrak{a}) & = & x\overline{x} \\ x & \equiv & 1 \bmod^* \mathfrak{m} \end{array} \end{array} \right\}.$$

Noticing that $N_{K^r/\mathbb{Q}}(x) = N_{\Phi^r}(x)\overline{N_{\Phi^r}(x)}$ for every $x \in K^r$, we find that $I_{K^r,\Phi^r}(\mathfrak{m})$ is a congruence subgroup modulo m. As a congruence subgroup, this corresponds to a field extension $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ of K^r contained in $H_{K^r}(m)$.

3. An integer m for which $\star_m$ holds.

The aim of this section is to prove Theorem 1.1, which gives a formula to find an integer m such that $(\star_m)$ holds. In Section 3.1, we discuss embedding problems, which we use in Section 3.2 to prove Theorem 1.1.

3.1. **Embedding problems.**

We state a result of Richter used in Shimura's original proof [Shi62, Proof of Theorem 2].

Lemma 3.1. Let a be a non-negative integer. Let F be a totally imaginary number field. Let L/F be an unramified cyclic Galois extension of degree 2^a. Then there exists a cyclic Galois extension M/F of degree 2^{a+1} which contains L.

Even though Lemma 3.1 is a special case of [Ric36b, Satz 1b], we will prove it to keep this article self-contained. The proof concerns *embedding problems*, which we define in this section.

Let G and A be groups. A *central group extension of G by A* is an exact sequence

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1 \tag{3.2}$$

such that $\iota(A)$ is in the center of E.

Definition 3.3. By an *embedding problem*, we will mean a pair $(L/F, \varepsilon)$ where L/F is a Galois extension and ε is a central group extension given by an exact sequence

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$$

where $G = \mathrm{Gal}(L/F)$. A *solution* to such an embedding problem is a Galois extension M/F containing L such that there exists an isomorphism $\phi : \mathrm{Gal}(M/F) \to E$ which induces a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(M/L) & \longrightarrow & \mathrm{Gal}(M/F) & \longrightarrow & G & \longrightarrow & 1 \\ & & \downarrow & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \mathrm{id}_G} & & \\ 1 & \longrightarrow & A & \xrightarrow{\iota} & E & \xrightarrow{\pi} & G & \longrightarrow & 1. \end{array}$$

If the fields F and L are global fields, such as number fields, then we call it a *global embedding problem*.

Let a be a non-negative integer. Let L/F be a cyclic extension of degree 2^a. Denote $\mathrm{Gal}(L/F)$ by G. Consider any central group extension of the form

$$1 \to C_2 \to C_{2^{a+1}} \to G \to 1,$$

and denote it by ε_2. Note that ε_2 is unique up to non-unique isomorphism.

Example 3.4. For example, take L/F to be $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ and denote its Galois group by G.

1. The embedding problem $(L/F, \varepsilon_2)$ has $\mathbb{Q}(\zeta_5)$ as a solution.
2. The embedding problem $(L/F, \varepsilon)$ in which ε is of the form
$$1 \ \to \ C_2 \ \to \ C_2 \ \times \ C_2 \ \to \ G \ \to \ 1$$
has $\mathbb{Q}(\sqrt{5}, i)$ as a solution. ▲

A global embedding problem $(L/F, \varepsilon)$ has one or more associated local embedding problems for each place of L as follows.

Definition 3.5. Let $(L/F, \varepsilon)$ be a global embedding problem where ε is an exact sequence $1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1$. Let w be a place of L over a place v of F and denote by $\widetilde{G}$ the decomposition group $D(w/v)$, which is the Galois group of L_w/F_v. Let $\widetilde{E}$ be a subgroup of E such that

$$\pi(\widetilde{E}) = \widetilde{G}. \tag{3.6}$$

Let $\widetilde{A} = \iota^{-1}(\widetilde{E})$ and denote by $\widetilde{\varepsilon}$ the following exact sequence

$$1 \to \widetilde{A} \xrightarrow{\iota} \widetilde{E} \xrightarrow{\pi} \widetilde{G} \to 1.$$

Then $(L_w/F_v, \widetilde{\varepsilon})$ is the *local embedding problem induced by the global embedding problem* $(L/F, \varepsilon)$ *with respect to the place* w *and the subgroup* $\widetilde{E}$ *of* E.

The following lemma gives a sufficient condition to conclude that a global embedding problem has no solution.

Lemma 3.7 (Richter, [Ric36a, Satz 5])**.** If a global embedding problem $(L/F, \varepsilon)$ is solvable, then for each place w of L there exists a subgroup $\widetilde{E}$ of E such that the local embedding problem with respect to w and $\widetilde{E}$ is solvable.

Example 3.8. Let L/F be $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ with Galois group $\mathrm{Gal}(L/F)$. Consider the embedding problem $(L/F, \varepsilon_2)$. Here ε_2 is the exact sequence $1 \to C_2 \to C_4 \to C_2 \to 1$. Let w a real place of $\mathbb{Q}(\sqrt{5})$ over the unique (real) archimedean place v of $\mathbb{Q}$. Note that $L_w = \mathbb{R}$ and $F_v = \mathbb{R}$ and the decomposition group $D(w/v) = \widetilde{G}$ is trivial. The subgroups of C_4 which satisfy (3.6) are exactly the trivial group and the unique subgroup of order 2.

1. The field $M = \mathbb{R}$ is a solution to the local embedding problem induced by the global embedding problem $(L/F, \varepsilon_2)$ with respect to the place w and the trivial subgroup of C_4 since $\mathrm{Gal}(M/\mathbb{R}) \cong 1$.
2. The field $M = \mathbb{C}$ is a solution to the local embedding problem induced by the global embedding problem $(L/F, \varepsilon_2)$ with respect to the place w and the unique subgroup C_2 of order 2 of E since $\mathrm{Gal}(M/\mathbb{R}) \cong C_2$. ▲

Example 3.9. Let L/F be $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. Let w be the complex place of L, which is above the unique (real) archimedean place v of $\mathbb{Q}$. The decomposition group $D(w/v)$ in this case is of order 2. Consider the embedding problem $(L/F, \varepsilon_2)$ where ε_2 is the exact sequence $1 \to C_2 \to C_4 \to C_2 \to 1$. Take $\widetilde{E} = E = C_4$, and note that this is the only subgroup of E which satisfies (3.6). There does not exist a number field M' such that $\mathrm{Gal}(M'/\mathbb{R}) \cong \widetilde{E} = C_4$. So, this induced local embedding problem is not solvable. Moreover, since C_4 is the only subgroup of E satisfying (3.6), this is the only induced local embedding problem and hence all induced local problems are not solvable. As all valid candidates of $\widetilde{E}$ result in a local problem which is not solvable, then there does not exist a cyclic field extension of $\mathbb{Q}$ of degree 4 which contains $\mathbb{Q}(\sqrt{-5})$. ▲

Example 3.10. If F has no real embeddings, then all its archimedean places are complex and hence $\widetilde{G}$ is always trivial. In this case, taking the trivial group is the only valid choice for $\widetilde{E}$. Hence, for each *archimedean* place w of L, the global embedding problem $(L/F, \varepsilon)$ induces a local embedding problem with respect to w which is solvable. ▲

We are mainly interested in the case where L/F is unramified. The following lemma shows that in this case, for each *nonarchimedean* place w of L, the global embedding problem $(L/F, \varepsilon)$ induces a local embedding problem with respect to w which is solvable.

Lemma 3.11 ([Ric36a, Satz 6])**.** Let ℓ, m, n, u be positive integers. Let K be a non-archimedean local field of characteristic 0 with unique prime ideal $\mathfrak{p}$. Suppose that K contains the ℓ^u-th roots of unity, but not all ℓ^{u+1}st roots of unity. Let L be a cyclic extension of K of degree ℓ^n. Then, there exists a Galois extension M of K containing L such that $\mathrm{Gal}(M/K) = C_{\ell^{m+n}}$ if and only if at least one of the following is true:

1. $\mathfrak{p}$ is unramified in L.
2. $\mathfrak{p} \nmid \ell$, and $u \geq m + s$, where ℓ^s is the ramification index of $\mathfrak{p}$ in L
3. $\mathfrak{p} \mid \ell$, and one of the following is true
   - $u = 0$
   - $u \geq n + m$
   - $0 < u < n + m$ and $\zeta_{\ell^{\min(u,m)}} \in N_{L/K}(L)$.

Finally, we conclude by a lemma stating that a *local-global principle* for our case.

Lemma 3.12. For any non-negative integer a and any cyclic field extension L/F of degree 2^a, the global embedding problem $(L/F, \varepsilon)$ is solvable if and only if for every place w of L, the unique induced local embedding problem is solvable.

Proof. This is a special case of [Ric36a, Satz 9] obtained by substituting ℓ, m, and n with $2, 1$, and a respectively and noticing that the condition $B(2)$, defined in [Ric36a, Definition 3], is trivially satisfied. ∎

Finally, we end this subsection with a proof of Lemma 3.1.

Proof (of Lemma 3.1). We are interested in the solvability of the embedding problem $(L/F, \varepsilon)$ where ε is of the form $1 \to C_2 \to C_{2^{a+1}} \to G \to 1$, where $G = \mathrm{Gal}(L/F) = C_{2^a}$. If we show that the global embedding problem is solvable, then we will have proven the lemma. Since F has no real embeddings, each archimedean place has a local embedding problem which is solvable thanks to Example 3.10. Now, since L/F is unramified, we may use Lemma 3.11 to show that each nonarchimedean place has a local embedding problem which is solvable. Finally, using Lemma 3.12, we find that since each place of F has an induced local embedding problem which is solvable, then the global embedding problem is solvable. ∎

3.2. **Towards an explicit m.** The following result of Crespo is one of the key ingredients in the proof of our main result.

Theorem 3.13 ([Cre89, Theorem 6])**.** Let L/K be a Galois extension of a number field K, unramified outside a finite set S of prime ideals of the ring of integers $\mathcal{O}_K$ of K. Let n be a positive integer, $G = \mathrm{Gal}(L/K)$, and A an abelian group of exponent n. Assume S contains the prime ideals dividing n. For each prime number p dividing n, we denote by a_p the p-rank of A, by r_p the p-rank of $\mathrm{Hom}(G, A)$ and let $\delta_p = 0$ if K contains a primitive $p^{v_p(n)}$-th root of unity and $\delta_p = 1$ if it does not. Suppose that

1. the order h_S of the S-class group is coprime to n, and
2. for every prime number $p \mid n$, we have $r_p + a_p + \delta_p < \#S$.

Then every solvable embedding problem $(L/K, \varepsilon)$, where ε is a central group extension of G by A, has a solution M such that M/K is unramified outside S.

Given a finite abelian extension L/K, we denote its conductor, as defined in [Coh00, Chapter 2], by $\mathfrak{f}_{L/K}$. One key property of the conductor that we use is that it is the minimal modulus $\mathfrak{m}$ such that $H_K(\mathfrak{m}) \supseteq L$.

Lemma 3.14. Let a be a non-negative integer. Let K be a number field with no real embeddings. Let L/K be an unramified cyclic Galois extension of degree 2^a. Let S be a finite set of prime ideals of K such that

- $|\mathrm{Cl}_K(1)/\langle S \rangle|$ is odd,
- S contains all prime ideals above 2,
- S contains at least 3 elements.

Then there exists a cyclic Galois extension M/K of degree 2^{a+1}, unramified outside S, containing L.

Proof. Lemma 3.1 shows that the embedding problem $(L/K, \varepsilon_2)$ is solvable. Keeping the notation of Theorem 3.13, the 2-rank a_2 of $A = C_2$ for this embedding problem is 1. Moreover, $\mathrm{Hom}(\mathrm{Gal}(L/K), C_2) \cong C_2$ and hence $r_2 = 1$. Finally $\delta_2 = 0$ since K contains the second roots of unity. Using Theorem 3.13, we prove the lemma. ∎

Denote by $\mathfrak{d}_{L/K}$ the relative discriminant ideal of a field extension L/K, as defined in [Coh00, Chapter 2, Section 2.4] and in [Neu99, Section III.2.8].

We now state the following lemma.

Lemma 3.15 (Cohen, [Coh00, Proposition 3.3.21])**.** Let L/K be an abelian extension of degree n such that $L \subseteq H_K(\mathfrak{m})$ for some modulus $\mathfrak{m}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{f}_{L/K}(\mathfrak{p}) \neq 0$. Finally, let ℓ be the prime number below $\mathfrak{p}$.

1. If $\ell \nmid n$, then $\mathfrak{f}_{L/K}(\mathfrak{p}) = 1$.
2. If $\gcd(n, N_{L/K}(\mathfrak{p}) - 1) = 1$ and n is a power of ℓ, then $\mathfrak{f}_{L/K}(\mathfrak{p}) \geq 2$.

From Lemma 3.15, we conclude that since 2 is the only prime divisor of $[M : L]$, with M, L as in Lemma 3.14, then for a prime ideal $\mathfrak{P}$ of L not above 2, we have $v_{\mathfrak{P}}(\mathfrak{f}_{M/L}) \leq 1$.

Using [Coh00, Corollary 10.1.24] gives us the bound $\mathfrak{f}_{M/L}(\mathfrak{P}_2) \leq 2e(\mathfrak{P}_2/2) + 1$ for any $\mathfrak{P}_2$ above 2, where $e(\mathfrak{P}_2/2)$ is the ramification index of $\mathfrak{P}_2$ over 2. To summarize, for any prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$, we have:

$$\mathfrak{f}_{M/L}(\mathfrak{P}) \leq \begin{cases} 2e(\mathfrak{P}/2) + 1 & \mathfrak{P} \mid 2 \\ 1 & \mathfrak{P} \nmid 2. \end{cases} \tag{3.16}$$

Proposition 3.17, below, enables us to bound the valuation of $\mathfrak{f}_{M/K}$ at the primes $\mathfrak{p}$ of $\mathcal{O}_K$ using the bounds on the valuations of $\mathfrak{f}_{M/L}$ at the primes $\mathfrak{P}$ of $\mathcal{O}_L$.

Proposition 3.17. Let K be a number field and let L be an unramified extension of K of degree 2^a. Let M be a cyclic extension of K of degree 2^{a+1} which contains L. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_K$. Let c be an integer and suppose $\mathfrak{f}_{M/L}(\mathfrak{P}) \leq c$ for every prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ above $\mathfrak{p}$. Then

$$\mathfrak{f}_{M/K}(\mathfrak{p}) \leq c.$$

Proof. Note that

$$\mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\mathfrak{f}_{M/L})) = \sum_{\mathfrak{P} \mid \mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\mathfrak{P})) \cdot \mathrm{ord}_{\mathfrak{P}}(\mathfrak{f}_{M/L}),$$

where $\sum_{\mathfrak{P}|\mathfrak{p}}$ denotes a sum that runs through all primes $\mathfrak{P}$ over $\mathfrak{p}$. Using the assumption that $\mathfrak{f}_{M/L}(\mathfrak{P}) \leq c$ for every prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$ above $\mathfrak{p}$, we get

$$\mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\mathfrak{f}_{M/L})) \leq c \cdot \sum_{\mathfrak{P} \mid \mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\mathfrak{P})).$$

Let g be the number of prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ above $\mathfrak{p}$. For each of these g prime ideals, the norm $N_{L/K}(\mathfrak{P})$ is given by the residue class degree $f = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$. Hence, we have $\sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\mathfrak{P})) = fg$. Now, since L/K is unramified, we have $2^a = [L : K] = fg$. Corollary III.2.10 of [Neu99] states that for a tower of fields $K \subseteq L \subseteq M$ one has

$$\mathfrak{d}_{M/K} = \mathfrak{d}_{L/K}^{[M:L]} N_{L/K}(\mathfrak{d}_{L/K}). \tag{3.18}$$

The conductor-discriminant formula [Neu99, Section VII.11.9] gives us

$$\mathfrak{d}_{M/L} = \mathfrak{f}_{M/L}, \qquad \mathfrak{d}_{M/K} = \mathfrak{f}_{M/K}^{2^a} \tag{3.19}$$

Combining (3.18), (3.19) and the fact that $\mathfrak{d}_{L/K} = 1$ since L/K is unramified, we obtain

$$\mathfrak{f}_{M/K}^{2^a} = N_{L/K}\left(\mathfrak{f}_{M/L}\right).$$

And thus

$$2^a \cdot \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_{M/K}) = \mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\mathfrak{f}_{M/L})) \leq 2^a \cdot c$$

and so $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_{M/K}) \leq c$. ∎

For each number field K and for each integer $\mathfrak{m}$, let $E_K(\mathfrak{m})$ be the smallest subfield of $H_K(\mathfrak{m})$ containing K such that $\mathrm{Gal}(H_K(\mathfrak{m})/E_K(\mathfrak{m}))$ is of exponent at most 2.

Theorem 3.20. Let K be a number field without real embeddings. Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that

- $|\mathrm{Cl}_K(1)/\langle S\rangle|$ is odd,
- S contains all prime ideals above 2,
- S contains at least 3 elements.

Let $\mathfrak{m}_S = 4 \cdot \prod_{\mathfrak{p}\in S} \mathfrak{p}$. Then $H_K(1) \subseteq E_K(\mathfrak{m}_S)$.

Proof. Suppose $\mathrm{Gal}(H_K(1)/K)$ is

$$\mathrm{Gal}(H_K(1)/K) = G_0 \times G_1 \times \cdots \times G_t$$

where G_0 is the largest subgroup of $\mathrm{Gal}(H_K(1)/K)$ of odd order, and G_i is a cyclic group of order 2^{a_i} generated by σ_i for $i \in \{1, \ldots, t\}$. For each $j \in \{0, 1, \ldots, t\}$, let L_j be the fixed field of

$$G_0 \times \cdots \times G_{i-1} \times \langle 1\rangle \times G_{i+1} \times \cdots \times G_t$$

by Galois theory. Fix an $i \in \{1, \ldots, t\}$. Since L_i/K is an unramified cyclic number field extension of degree 2^{a_i}, Lemma 3.14 gives us the existence of a field extension M_i of K containing L_i which is unramified outside S. Let $\mathfrak{P}_i$ be a prime ideal of $\mathcal{O}_{L_i}$ above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and a rational prime ℓ. Since L_i/K is unramified, we find that $e(\mathfrak{P}/\ell) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/\ell) = e(\mathfrak{p}/\ell)$. Equation (3.16) and Proposition 3.17 then tell us that

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_{M_i/K}) \leq \begin{cases} 2e(\mathfrak{p}/\ell) + 1 & \ell = 2 \\ 1 & \ell \neq 2. \end{cases}$$

Since the conductor of a compositum of fields divides the least common multiple of the conductors of the fields being composed, the field $L_0M_1 \cdots M_t$ has a conductor which divides

$$\mathfrak{m} = \prod_{\mathfrak{p}|2} \mathfrak{p}^{2e(\mathfrak{p}/2)} \prod_{\mathfrak{p}\in S} \mathfrak{p} = 4 \prod_{\mathfrak{p}\in S} \mathfrak{p}.$$

Denote by $\boldsymbol{G}_{K'}$ the Galois group $\mathrm{Gal}(H_K(\mathfrak{m})/K')$ where K' is an abelian extension of K contained in $H_K(\mathfrak{m})$. We want to show that $H_K(1) \subseteq E_K(\mathfrak{m})$. To do this, we show the equivalent condition

$$\boldsymbol{G}_{E_K(\mathfrak{m})} \subseteq \boldsymbol{G}_{H_K(1)}.$$

Let $\sigma \in \boldsymbol{G}_{E_K}(\mathfrak{m})$ and note that $\sigma^2 = 1$. Note that $[\boldsymbol{G}_K : \boldsymbol{G}_{L_0}]$ is an odd integer and hence $\sigma \in \boldsymbol{G}_{L_0}$. On the other hand, for each $i \in \{1, \ldots, t\}$, since $\sigma^2 = \mathrm{id} \in \boldsymbol{G}_{M_i}$ then by definition of M_i, $\sigma \in \boldsymbol{G}_{L_i}$. Hence σ fixes $L_0L_1 \cdots L_t = H_K(1)$. And therefore $\sigma \in \boldsymbol{G}_{H_K(1)}$. ∎

The smallest positive integer m contained in $\mathfrak{m}$ is given by $m = 4P$ where P is the product of all primes p such that p is below some $\mathfrak{p} \in S$. With this observation and the fact that $E_K(\mathfrak{m}) \subseteq E_K(\mathfrak{n})$ when $\mathfrak{m} \mid \mathfrak{n}$, Theorem 1.1 becomes a direct consequence of Theorem 3.20.

4. Given an integer m, does $\star_m$ hold?

Let (K, Φ) be a primitive CM pair and let (K^r, Φ^r) be its reflex pair.

The goal of this section is to describe an algorithm that, given a positive integer m, outputs whether or not $(\star_m)$ holds.

From this section onwards, denote by $\langle g \rangle_e$ the cyclic group generated by an element g of order e. Note that e may be ∞.

As the fields $H_{K^r}(1)$, $K^r H_{K_0^r}(m)$, $\mathrm{CM}_{K^r,\Phi^r}(m)$, and $H_{K^r}(m)$ are all abelian extensions of K^r contained in $H_{K^r}(m)$, we may use Galois theory to rewrite $(\star_m)$ in terms of subgroups of the finite abelian group $\mathrm{Gal}(H_{K^r}(m)/K^r)$ as

$$(\star\star_m) \qquad \boldsymbol{G}(\, H_{K^r}(1)\,) \supseteq \boldsymbol{G}(\, K^r H_{K_0^r}(m)\,) \cap \boldsymbol{G}(\, \mathrm{CM}_{K^r,\Phi^r}(m)\,),$$

where $\boldsymbol{G}(\, K'\,)$ is the subgroup of $\mathrm{Gal}(H_{K^r}(m)/K^r)$ fixing K'.

As a subfield of $H_{K^r}(m)$, the field $H_{K^r}(1)$ corresponds to the congruence subgroup

$$\{\mathfrak{a} \in I_{K^r}(m) : \mathfrak{a} = a\mathcal{O}_{K^r} \text{ for some } a \in K^r\}$$

of $I_{K^r}(m)$. The Galois group $\boldsymbol{G}(\, H_{K^r}(1)\,)$ is the kernel of the natural surjective map

$$\pi_m : \mathrm{Cl}_{K^r}(m) \to \mathrm{Cl}_{K^r}(1). \tag{4.1}$$

In the same vein, the field $K^r H_{K_0^r}(m)$ corresponds to the congruence subgroup

$$\{\mathfrak{a} \in I_{K^r}(m) : \mathfrak{a}\overline{\mathfrak{a}} = (a) \text{ for some } a \in K_0^r,\ a \equiv 1 \bmod^* m\}.$$

Hence, the Galois group $\boldsymbol{G}(\, K^r\, H_{K_0^r}(m)\,)$ is also isomorphic to a kernel, the kernel of the relative norm map

$$\eta = N_{K/K_0} : \mathrm{Cl}_{K^r}(m) \to \mathrm{Cl}_{K_0^r}(m). \tag{4.2}$$

We can also compute the Galois group $\boldsymbol{G}(\, \mathrm{CM}_{K^r,\Phi^r}(m)\,)$ as a kernel of a map r which we define in Section 4.1. The codomain of r is the Shimura class group studied in [BGL11, Section 3.1]. We generalize this Shimura class group by defining, in the same section, the Shimura *ray* class group of K for a modulus m, which we denote by $\mathfrak{C}_K(m)$.

Let m be a positive integer. Section 4.2 provides our algorithm to compute the generators of $\mathfrak{C}_K(m)$, their respective orders as group elements, and a discrete logarithm algorithm for $\mathfrak{C}_K(m)$. The end of the section details how we can extract and use information about the group $\mathfrak{C}_K(m)$ to determine whether or not $(\star\star_m)$ holds for the given integer m.

4.1. The Shimura ray class group.

Let (K, Φ) be a CM pair and (K^r, Φ^r) its reflex pair. The Shimura class group of K, in conjunction with a group morphism involving the type norm map, was used in [ET14, Section 2.2] to compute the Galois group $\boldsymbol{G}(\, \mathrm{CM}_{K^r,\Phi^r}(1)\,)$. This section generalizes the Shimura class group and introduces the concept of a *Shimura ray class group* for each modulus $\mathfrak{m}$ of K. We define it as follows.

Definition 4.3 (Shimura ray class group for the modulus $\mathfrak{m}$)**.** Let $\mathfrak{m}$ be a modulus of a CM field K. The Shimura ray class group $\mathfrak{C}_K(\mathfrak{m})$ is the group given by

$$\mathfrak{C}_K(\mathfrak{m}) = \frac{\{(\mathfrak{a}, a) \in I_K(\mathfrak{m}) \times K_0^\times : \mathfrak{a}\overline{\mathfrak{a}} = a\mathcal{O}_K, a \gg 0\}}{\{(x\mathcal{O}_K, x\overline{x}) \in I_K(\mathfrak{m}) \times K_0^\times : x \in K^\times, x \equiv 1 \bmod^* \mathfrak{m}\}}.$$

Multiplication of elements in $\mathfrak{C}_K(\mathfrak{m})$ is done by component-wise multiplication.

Notice that the definition of the Shimura ray class group of a CM field K is independent of CM types and also does not concern reflex fields.

For any positive integer m and any CM pair (K, Φ), the type norm map induces a map from the ray class group of K^r to the Shimura ray class group of K as follows

$$\begin{aligned} r : \mathrm{Cl}_{K^r}(m) &\to \mathfrak{C}_K(m) \\ [\mathfrak{b}] &\mapsto [\big(N_{\Phi^r}(\mathfrak{b}), N_{K^r/\mathbb{Q}}(\mathfrak{b})\big)]. \end{aligned} \tag{4.4}$$

The kernel of the map r, by definition of $I_{K^r,\Phi^r}(m)$, is exactly $I_{K^r,\Phi^r}(m)/P_{K^r}(m)$ and is thus isomorphic to $\boldsymbol{G}(\,\mathrm{CM}_{K^r,\Phi^r}(m)\,)$.

Just like the case when $\mathfrak{m} = 1$, the Shimura *ray* class group for a modulus $\mathfrak{m}$ fits as the 'B'-term term of a short exact sequence $1 \to A \to B \to C \to 1$ for some computable A and C. We start by introducing and computing the ingredients of A and C.

Let K_0 be the real subfield of a CM field K. Write $\mathcal{O}_{K_0}^\times$ for the group of units of the ring of integers of K_0 and write $\mathcal{O}_{K_0}^{\times+}$ for the subgroup of $\mathcal{O}_{K_0}^\times$ consisting of only the totally positive units of K_0.

Example 4.5. Let K be a quartic CM field different from $\mathbb{Q}(\zeta_5)$. Dirichlet's unit theorem gives us

$$\mathcal{O}_{K_0}^\times = \langle -1 \rangle_2 \times \langle \varepsilon_0 \rangle_\infty$$

for some fundamental unit ε_0. Furthermore, we find that $\mathcal{O}_{K_0}^{\times+} = \langle \varepsilon_0^+ \rangle$ where

$$\varepsilon_0^+ = \begin{cases} \varepsilon_0 & \varepsilon_0 \gg 0 \\ -\varepsilon_0 & \varepsilon_0 \ll 0 \\ \varepsilon_0^2 & \text{otherwise.} \end{cases}$$

▲

Denote by $\mathcal{O}_{K,\mathfrak{m},1}^\times$ the kernel of the natural map

$$s : \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times \tag{4.6}$$

The image $N_{K/K_0}\left(\mathcal{O}_{K,\mathfrak{m},1}^\times\right)$ is easily observed to be contained in $\mathcal{O}_{K_0}^{\times+}$. Indeed, we have $K = K_0(\sqrt{-z})$ for some totally positive element $z \in K_0$ and the relative norm of a nonzero element $x = a + b\sqrt{-z} \in K$ is $a^2 + b^2 z$, which is a totally positive element. Thus, the norm $N_{K/K_0} : K \to K_0$ induces maps

$$N_1 := N_{K/K_0} : \mathcal{O}_{K,\mathfrak{m},1}^\times \to \mathcal{O}_{K_0}^{\times+} \qquad : \qquad x \mapsto x\overline{x}. \tag{4.7}$$

and

$$N_2 := N_{K/K_0} : \mathrm{Cl}_K(\mathfrak{m}) \to \mathrm{Cl}_{K_0}^+(1) \qquad : \qquad [\mathfrak{a}] \mapsto [\mathfrak{a}\overline{\mathfrak{a}}]. \tag{4.8}$$

We define the maps f and g as follows

$$\begin{aligned} f : \mathcal{O}_{K_0}^{\times +} &\to \mathfrak{C}_K(m) \\ u &\mapsto [(\mathcal{O}_K, u)] \end{aligned} \qquad \text{and} \qquad \begin{aligned} g : \mathfrak{C}_K(m) &\to \mathrm{Cl}_K(\mathfrak{m}) \\ [(\mathfrak{a}, a)] &\mapsto [\mathfrak{a}]. \end{aligned}$$

We are now ready to state and prove the following lemma.

Lemma 4.9. The sequence

$$\mathcal{O}_{K,\mathfrak{m},1}^{\times} \xrightarrow{N_1} \mathcal{O}_{K_0}^{\times +} \xrightarrow{f} \mathfrak{C}_K(\mathfrak{m}) \xrightarrow{g} \mathrm{Cl}_K(\mathfrak{m}) \xrightarrow{N_2} \mathrm{Cl}_{K_0}^{+}(1)$$

is exact. Consequently, the sequence

$$1 \to \operatorname{coker} N_1 \xrightarrow{f} \mathfrak{C}_K(\mathfrak{m}) \xrightarrow{g} \ker Ntwo \to 1$$

is exact.

Proof. We first prove exactness at $\mathcal{O}_{K_0}^{\times +}$. Let $u \in \mathcal{O}_{K_0}^{\times +}$ such that $[(\mathcal{O}_K, u)]$ is trivial in $\mathfrak{C}_K(m)$. Since $[(\mathcal{O}_K, u)]$ is the trivial class, the unit u is of the form $x\overline{x}$ where $x \equiv 1 \bmod^* \mathfrak{m}$. Hence $u = x\overline{x}$ for some $x \in \mathcal{O}_{K,\mathfrak{m},1}^{\times}$. Thus, $\ker f \subseteq \operatorname{im} N_1$. Moreover, for $x \in \mathcal{O}_{K,\mathfrak{m},1}^{\times}$, we have $f(N_1(x)) = [(\mathcal{O}_K, x\overline{x})]$. This element is trivial in $\mathfrak{C}_K(m)$. Hence $\operatorname{im} N_1 \subseteq \ker f$.

We prove exactness at $\mathfrak{C}_K(\mathfrak{m})$. Given $[(\mathfrak{a}, a)] \in \ker g$, we have $\mathfrak{a} = \alpha\mathcal{O}_K$ for some $\alpha \in K$ with $\alpha \equiv 1 \bmod^\star \mathfrak{m}$. And so $\alpha\overline{\alpha}\mathcal{O}_K = \mathfrak{a}\overline{\mathfrak{a}} = a\mathcal{O}_K$. Hence $\alpha\overline{\alpha}u = a$ for some unit $u \in \mathcal{O}_K$. Since $\alpha\overline{\alpha}$ is a relative norm for the extension K/K_0, it is in K_0 and totally positive. Moreover, tle element a is also in K_0 and totally positive by definition of $\mathfrak{C}_K(m)$. Thus u must also be in K_0 and totally positive and hence $u \in \mathcal{O}_{K_0}^{\times +}$. Since

$$[(\mathfrak{a}, a)] = [(\alpha\mathcal{O}_K, \alpha\overline{\alpha}u)] = [(\mathcal{O}_K, u)],$$

the class $[(\mathfrak{a}, a)]$ is evidently in the image of the f. And so $\ker g \subseteq \operatorname{im} f$. Now, for any $u \in \mathcal{O}_{K_0}^{\times +}$, we have $g(f(u)) = [\mathcal{O}_K]$. Hence, $\operatorname{im} f \subseteq \ker g$.

We prove exactness at $\mathrm{Cl}_K(\mathfrak{m})$. Suppose $[\mathfrak{a}] \in \mathrm{Cl}_K(\mathfrak{m})$ is such that $[\mathfrak{a}\overline{\mathfrak{a}}] = a\mathcal{O}_{K_0}$ for some $a \in K_0$ with a totally positive. And so $[\mathfrak{a}, a] \in \mathfrak{C}_K(m)$ and $g([\mathfrak{a}, a]) = [\mathfrak{a}]$. Hence, $\ker N_2 \subseteq \operatorname{im} g$. Suppose $[(\mathfrak{a}, a)] \in \mathfrak{C}_K(m)$. First $g([(\mathfrak{a}, a)]) = [\mathfrak{a}]$. By definition of $\mathfrak{C}_K(m)$, we have $N_2([\mathfrak{a}]) = a\mathcal{O}_{K_0}$ for some $a \in K_0$ with a totally positive. Thus $N_2(g([(\mathfrak{a}, a)]))$ is trivial. Thus $\operatorname{im} g \subseteq \ker N_2$. ∎

4.2. **Computing the Shimura Ray Class Group.** Lemma 4.9 states that $\mathfrak{C}_K(\mathfrak{m})$ fits as the 'B-term' in a short exact sequence of the form $1 \to A \to B \to C \to 1$. In this section, we compute each term in that short exact sequence using algorithms on finitely generated abelian groups found in [CDO01] and [Coh00, Chapter 4]. All algorithms discussed in this section are efficient and practical in the sense that

- fast implementations are available[2] in PARI/GP [Par19] or Magma [BCP97], and
- when these implementations are used for our examples in Section 5, they are in practice not the dominant step of the computation.

[2]Available either as one of the built-in functions, or implemented by the author.

Let G be a finitely generated abelian group. By the fundamental theorem of finitely generated abelian groups, there exist unique non-negative integers $1 \neq d_1, \ldots, d_n$ such that $d_n \mid d_{n-1} \mid \cdots \mid d_1$ and there exists *a discrete logarithm isomorphism*

$$\gamma_G : G \to V_G := \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \cdots \times \frac{\mathbb{Z}}{d_n\mathbb{Z}}$$

Given such an isomorphism γ_G, we say that the *standard set of generators* with respect to γ_G is the set of inverse images of all $\mathbf{e}_i \in V_G$, where $\mathbf{e}_i$ is the vector in V_G whose entries are all 0, save for the ith entry, which is 1.

We say that a finitely generated abelian group G is *computed* if the integers $d_1, \ldots, d_n$ of V_G are known and there exists a discrete logarithm isomorphism γ_G from G to V_G such that

CG1 the inverse images under γ_G of the generators $\mathbf{e}_1, \ldots, \mathbf{e}_n$ are known, and
CG2 an algorithm that outputs $\gamma_G(g)$ given $g \in G$ is known.

A subgroup H of a computed group G is said to be *computed with respect to* γ_G if we know an $n \times n$ matrix $\widehat{H} = (h_{i,j})$ in column Hermite normal form (HNF) such that

$$\left\{\gamma_G^{-1}\left(\begin{bmatrix} h_{1,j} & \cdots & h_{n,j}\end{bmatrix}^{\intercal}\right) : j = 1, \ldots, n\right\}$$

generates H. With such a Hermite normal form matrix, one can use a Smith normal form (SNF) algorithm [Coh00, Algorithm 4.1.3] to compute H as in **CG1** and **CG2**.

Let K be a quartic CM field and $\mathfrak{m}$ be a modulus of K. From Lemma 4.9, the group $\mathfrak{C}_K(\mathfrak{m})$ fits as the middle term of the exact sequence

$$1 \to \operatorname{coker} N_1 \xrightarrow{f} \mathfrak{C}_K(\mathfrak{m}) \xrightarrow{g} \ker N_2 \to 1. \tag{4.10}$$

We would like to compute this middle term. We use the group extension algorithm [Coh00, Algorithm 4.1.8] to compute $\mathfrak{C}_K(\mathfrak{m})$. To compute the middle term of (4.10) using this algorithm, we need:

GEXT1 to compute the group $\ker N_2$,
GEXT2 to compute the group $\operatorname{coker} N_1$,
GEXT3 an algorithm which, given $[\mathfrak{b}, \beta] \in \operatorname{im} f$, outputs $a \in \operatorname{coker} N_1$ such that $f(a) = [\mathfrak{b}, \beta] \in \operatorname{im} f$.

We first compute the kernel $\ker N_2 : \mathrm{Cl}_K(\mathfrak{m}) \to \mathrm{Cl}^+_{K_0}(1)$ using the inverse image algorithm found in [Coh00, Algorithm 4.1.11]. In order to use this algorithm, we need:

KER1 to compute the groups $\mathrm{Cl}_K(\mathfrak{m})$ and $\mathrm{Cl}^+_{K_0}(1)$, and
KER2 an algorithm which gives $\gamma_{\mathrm{Cl}^+_{K_0}(1)}(N_2([\mathfrak{a}]))$ given $[\mathfrak{a}] \in \mathrm{Cl}_K(\mathfrak{m})$.

The groups mentioned in **KER1** can be computed using [Coh00, Algorithm 4.3.1]. For **KER2**, if we choose an ideal class representative $\mathfrak{a}$ in $\mathrm{Cl}_K(\mathfrak{m})$ and apply the relative norm map $N_{K/K_0} : I_K(\mathfrak{m}) \to I^+_{K_0}(1)$ on ideals using [Coh00, Algorithm 2.5.2], then $N_{K/K_0}(\mathfrak{a})$ is a representative of the image of the ideal class $[\mathfrak{a}]$ under N_2. Hence, we can compute $\gamma_{\mathrm{Cl}^+_{K_0}(1)}(N_2([\mathfrak{a}]))$ by using [Coh00, Algorithm 4.3.2].

We compute the quotient group

$$\operatorname{coker} N_1 = \mathcal{O}^{\times +}_{K_0} / N_{K/K_0}(\mathcal{O}^{\times}_{K,\mathfrak{m},1})$$

using [Coh00, Algorithm 4.1.7]. In order to use this algorithm, we need:

QUO1 to compute the group $\mathcal{O}_{K_0}^{\times +}$, and
QUO2 to compute $N_{K/K_0}(\mathcal{O}_{K,\mathfrak{m},1}^{\times})$ with respect to the discrete logarithm isomorphism $\gamma_{\mathcal{O}_{K_0}^{\times +}}$ obtained from doing item **QUO1**

For **QUO1**, we simply compute $\mathcal{O}_{K_0}^{\times}$ using [Coh93, Algorithm 6.5.7] and then use Example 4.5 to obtain generators and a discrete logarithm isomorphism $\gamma_{\mathcal{O}_{K_0}^{\times +}}$ for $\mathcal{O}_{K_0}^{\times +}$. With this, for any $x \in \mathcal{O}_{K_0}^{\times}$, we can find $\gamma_{\mathcal{O}_{K_0}^{\times +}}(s)$ if we know $\gamma_{\mathcal{O}_{K_0}^{\times}}(s)$.

For **QUO2**, we first compute the groups $\mathcal{O}_K^{\times}$ and $(\mathcal{O}_K/\mathfrak{m})^{\times}$ using [Coh00, Algorithm 4.2.21] and [Coh00, Algorithm 4.1.11], respectively. Let

$$s : \mathcal{O}_K^{\times} \to (\mathcal{O}_K/\mathfrak{m})^{\times}$$

be the map induced by the natural map $\mathcal{O}_K \to \mathcal{O}_K/\mathfrak{m}$. We are interested in $\mathcal{O}_{K,\mathfrak{m},1}^{\times}$, which is $\ker s$. An algorithm to compute $\gamma_{(\mathcal{O}_K/\mathfrak{m})^{\times}}(s(x))$ which takes as input $x \in \mathcal{O}_K^{\times}$ is given by [Coh93, Algorithm 6.5.7]. With such an algorithm and the fact that we have computed both $\mathcal{O}_K^{\times}$ and $(\mathcal{O}_K/\mathfrak{m})^{\times}$, we can use [Coh00, Algorithm 4.1.11] to compute $\mathcal{O}_{K,\mathfrak{m},1}^{\times}$ with respect to $\gamma_{\mathcal{O}_K^{\times}}$. From there, we can use [Coh00, Algorithm 4.1.11] to compute the image $N_{K/K_0}(\mathcal{O}_{K,\mathfrak{m},1}^{\times})$ with respect to $\gamma_{\mathcal{O}_{K_0}^{\times +}}$.

Example 4.11. Let K_0 be the real quadratic field $\mathbb{Q}[\alpha_0] \,/\, (\alpha_0^2 + 53\ \alpha_0 + 500)$. Consider the quartic CM field $K = K_0(\alpha)$ where α is a root of $X^2 - \alpha_0$. Solving for fundamental units of $\mathcal{O}_K^{\times}$ and $\mathcal{O}_{K_0}^{\times}$, we get

$$\varepsilon = 30506849866\alpha^2 + 374579495409$$

and

$$\varepsilon_0 = 30506849866\alpha_0 + 374579495409,$$

respectively. Having $\varepsilon = \varepsilon_0$ corresponds to one of the three possible cases as discussed in Example 4.5. Using the notation we established in Section 4, we have

$$\mathcal{O}_K^{\times} = \langle -1 \rangle_2 \times \langle \varepsilon \rangle_0 \qquad \text{and} \qquad \mathcal{O}_{K_0}^{\times} = \langle -1 \rangle_2 \times \langle \varepsilon_0 \rangle_0.$$

Meanwhile, the group $(\mathcal{O}_K/2\mathcal{O}_K)^{\times}$ is given by

$$(\mathcal{O}_K/2\mathcal{O}_K)^{\times} = \langle -1/10\alpha^3 - \alpha^2 - 33/10\alpha - 26 \rangle_2 \times \langle -\alpha^2 - \alpha - 27 \rangle_2.$$

Since

$$-1 \equiv 1 \bmod 2 \qquad \text{and} \qquad \varepsilon = 30506849866\alpha^2 + 374579495409 \equiv 1 \bmod 2,$$

we find that the map $s : \mathcal{O}_K^{\times} \to (\mathcal{O}_K/2\mathcal{O}_K)^{\times}$ sends all elements of its domain to 1. Hence, $\mathcal{O}_{K,2,1}^{\times} = \mathcal{O}_K^{\times}$. The image of $\mathcal{O}_{K,2,1}^{\times}$ under the relative norm map N_{K/K_0} is the index 4 subgroup

$$N_{K/K_0}\left(\mathcal{O}_{K,2,1}^{\times}\right) = \langle \varepsilon_0^2 \rangle \subseteq \mathcal{O}_{K_0}^{\times}.$$

Note that ε_0 is not totally positive since the norm $N_{K_0/\mathbb{Q}}(\varepsilon_0)$ of ε_0 is -1. Thus, we find that

$$\mathcal{O}_{K_0}^{\times +} = \langle \varepsilon_0^2 \rangle$$

And so $\operatorname{coker} N_1$ is the trivial group.

We now compute $\ker N_2$. The ray class groups $\mathrm{Cl}_K(2)$ and $\mathrm{Cl}_{K_0}^{+}(1)$ are given by

$$\mathrm{Cl}_K(2) = \langle [\mathfrak{a}_1] \rangle_8 \times \langle [\mathfrak{a}_2] \rangle_4 \qquad \text{where} \qquad \mathfrak{a}_1 = (7, \alpha - 2) \quad \text{and} \quad \mathfrak{a}_2 = (7159, \alpha - 2627),$$

and

$$\mathrm{Cl}_{K_0}^{+}(1) = 1.$$

The codomain is trivial and so $\ker N_2 = \mathrm{Cl}_K(2)$. ▲

We now give an algorithm that **GEXT3** asks for. This algorithm is based on the remark below [Coh00, Algorithm 4.1.8].

Algorithm 4.12. Finding inverse images of $f : \operatorname{coker} N_1 \to \mathfrak{C}_K(\mathfrak{m})$.
INPUT. $[\mathfrak{b}, \beta] \in \operatorname{im} f$
OUTPUT. $a \in \operatorname{coker} N_1$ such that $f(a) = [\mathfrak{b}, \beta] \in \operatorname{im} f$

1. Compute $\mathrm{Cl}_K(m)$ using [Coh00, Algorithm 4.3.1].
2. Find x such that $\mathfrak{b} = x\mathcal{O}_K$ using [Coh00, Algorithm 4.3.2]. This algorithm uses the computation from the previous step.
3. Let $\alpha = \beta/(x\overline{x})$.
4. Return $[\alpha]$.

If one wishes to take inverse images of multiple elements in $\operatorname{im} f$, one can compute $\mathrm{Cl}_K(m)$ once and for all as it does not depend on the input $[\mathfrak{b}, \beta]$ and proceed with the second step.

Now that we have done **GEXT1**, **GEXT2**, and **GEXT3**, we use [Coh00, Algorithm 4.1.8] and the paragraph below it to compute $\mathfrak{C}_K(\mathfrak{m})$ in the sense of **CG1** and **CG2**.

4.3. **Using the Shimura ray class group to determine whether m, does $\star_m$ holds.** Let (K, Φ) be a primitive quartic CM pair and let (K^r, Φ^r) be its reflex. Let m be a positive integer.

We have established in Section 4.1 that $\ker r$ is exactly $I_{K^r,\Phi^r}(m)/P_{K^r}(m)$, which is isomorphic to $\mathrm{Gal}(H_{K^r}(m)/\mathrm{CM}_{K^r,\Phi^r}(m))$ via the Artin map. Recall the functions π_m and η defined in (4.1) and (4.2), respectively. We have the following isomorphisms via the Artin map:

$$\begin{aligned} \mathrm{Gal}(H_{K^r}(m)/H_{K^r}(1)) &\cong \ker \pi_m = \ker(\mathrm{Cl}_{K^r}(m) \to \mathrm{Cl}_{K^r}(1)), \\ \mathrm{Gal}(H_{K^r}(m)/H_{K_0^r}(m)) &\cong \ker \eta = \ker(\mathrm{Cl}_{K^r}(m) \to \mathrm{Cl}_{K_0^r}(m)), \\ \mathrm{Gal}(H_{K^r}(m)/\mathrm{CM}_{K^r,\Phi^r}(m)) &\cong \ker r = \ker(\mathrm{Cl}_{K^r}(m) \to \mathfrak{C}_K(m)). \end{aligned} \tag{4.13}$$

Therefore, we can rewrite $(\star\star_m)$ as

$$\ker \pi_m \supseteq \ker \eta \cap \ker r. \tag{4.14}$$

All groups involved are subgroups of $\mathrm{Cl}_{K^r}(m)$. So, we end up with the following algorithm.

Algorithm 4.15. INPUT. A primitive quartic CM pair (K, Φ) with reflex (K^r, Φ^r) and a positive integer m.
OUTPUT. Returns YES if $(\star_m)$ holds for the integer m. Otherwise, returns NO.

1. Compute the groups $\mathrm{Cl}_{K^r}(m), \mathrm{Cl}_{K^r}(1), \mathrm{Cl}_{K_0^r}(m), \mathfrak{C}_K(m)$.
2. Compute the kernels of the maps π_m, η, r.
3. Compute the intersection $I = \ker \eta \cap \ker r$, a subgroup of $\mathrm{Cl}_{K^r}(m)$.
4. Compute the intersection $J = \ker \pi_m \cap I$, a subgroup of $\mathrm{Cl}_{K^r}(m)$.
5. If $I = J$, return YES. Otherwise, return NO.

The author has implemented the algorithm that finds $\mathfrak{C}_K(\mathfrak{m})$ when K is a primitive quartic CM field, and the above Algorithm 4.15 in PARI/GP [Par19], both of which use algorithms involving morphisms between finitely generated abelian groups, particularly ray class groups. These morphism algorithm implementations are implemented by the author as functions in PARI/GP, collected in a file `fgag.gp`.

Example 4.11 (continuing from p. 16)**.** Having explicitly computed the groups $\operatorname{coker} N_1$ and $\ker N_2$, we compute

$$\mathfrak{C}_K(2) = \langle [\mathfrak{a}_1, a_1] \rangle_8 \times \langle [\mathfrak{a}_2, a_2] \rangle_4,$$

where

$$a_1 = -18\alpha_0 - 733 \qquad \text{and} \qquad a_2 = -14752\alpha_0 - 600723.$$

The reflex of the quartic CM pair (K^r, Φ^r) of (K, Φ) with $K^r = \mathbb{Q}[\alpha_r] \,/\, (\alpha_r^4 + 106\,\alpha_r^2 + 809)$. The ray class field $H_{K_0^r}(2)$ of its totally real subfield K_0^r is isomorphic to $K_0^r \cong \mathbb{Q}(\sqrt{5})$.

We do the first step of Algorithm 4.15. We get

$$\begin{aligned} \operatorname{Cl}_{K^r}(2) &= \langle \mathfrak{b}_1 \rangle_{16} \times \langle \mathfrak{b}_2 \rangle_2, & \ker \eta &= \langle \mathfrak{b}_1 \rangle_{16} \times \langle \mathfrak{b}_2 \rangle_2, \\ \ker \pi_m &= \langle \mathfrak{b}_1^8 \rangle_2 \times \langle \mathfrak{b}_2 \rangle_2, & \ker \eta &= \langle \mathfrak{b}_1^8 \rangle_2, \end{aligned}$$

where $\mathfrak{b}_1 = (11, 1/40\alpha_r^3 + 73/40\alpha_r + 1)$ and $\mathfrak{b}_2 = (-1/20\alpha_r^3 - 1/40\alpha_r^2 - 93/20\alpha_r - 73/40)$. Continuing with the rest of the steps of Algorithm 4.15, we find that $(\star_2)$ holds. ▲

The following example concerns the formula for m_S given in Corollary 1.3.

Example 4.16. We take $K = \mathbb{Q}[\alpha] \,/\, (\alpha^4 + 65\,\alpha^2 + 425)$ and let L be its Galois closure. Fix an embedding $\iota_{\mathbb{C}} : L \to \mathbb{C}$. Choose the CM type Φ of K such that both embeddings send α to the positive imaginary axis. Consider the reflex pair (K^r, Φ^r) of the CM pair (K, Φ). Here, the reflex field is $K^r = \mathbb{Q}[\alpha_r] \,/\, (\alpha_r^4 + 130\,\alpha_r^2 + 2525)$.

There are three prime ideals of $\mathcal{O}_{K^r}$ over the rational prime 2, namely

$$\begin{aligned} \mathfrak{p}_1 &= 2\mathcal{O}_{K^r} + (1/2\alpha_r - 1/2)\mathcal{O}_{K^r}, \\ \mathfrak{p}_2 &= 2\mathcal{O}_{K^r} + (1/2\alpha_r + 1/2)\mathcal{O}_{K^r}, \text{ and} \\ \mathfrak{p}_3 &= (1/20{\alpha_r}^2 + 7/4)\mathcal{O}_{K^r}. \end{aligned}$$

The ideal class group Cl_{K^r} of K^r is cyclic and is generated by the class $[\mathfrak{p}_1]$. We may take $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$. After verifying that this set S satisfies the hypotheses of Corollary 1.3, we find that $m_S = 8$ and conclude that

$$H_{K^r}(1) \subseteq H_{K_0^r}(8)\, \mathrm{CM}_{K^r, \Phi^r}(8).$$

Computing the ray class group of K^r for the modulus 8, we obtain

$$\operatorname{Cl}_{K^r}(8) = \langle [\mathfrak{a}_1] \rangle_{48} \times \langle [\mathfrak{a}_2] \rangle_4 \times \langle [\mathfrak{a}_3] \rangle_2 \times \langle [\mathfrak{a}_4] \rangle_2 \times \langle [\mathfrak{a}_5] \rangle_2$$

for certain ideals $\mathfrak{a}_i$.[3]

[3]The ideals $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4, \mathfrak{a}_5$ are $(443, \frac{1}{2}\alpha_r - \frac{263}{2}), (170999, \frac{1}{2}\alpha_r + \frac{120011}{2}), (41051, \frac{1}{2}\alpha_r - \frac{37351}{2}), (292141, \frac{1}{2}\alpha_r + \frac{198863}{2}), (172229, \frac{1}{2}\alpha_r + \frac{51253}{2})$.

We compute the kernels of π_m, η, r, as defined in (4.13). We find that

$$\begin{aligned}\ker \pi_m &= \langle [\mathfrak{a}_1^8\mathfrak{a}_2^3]\rangle_{12} \times \langle [\mathfrak{a}_1^{24}\mathfrak{a}_2^2]\rangle_2 \times \langle [\mathfrak{a}_3]\rangle_2 \times \langle [\mathfrak{a}_4]\rangle_2 \times \langle [\mathfrak{a}_5]\rangle_2,\\ \ker \eta &= \langle [\mathfrak{a}_1^{25}\mathfrak{a}_4]\rangle_{48} \times \langle [\mathfrak{a}_2^3\mathfrak{a}_4\mathfrak{a}_5]\rangle_4 \times \langle [\mathfrak{a}_3\mathfrak{a}_4]\rangle_2,\\ \ker r &= \langle [\mathfrak{a}_1^{36}\mathfrak{a}_2^2\mathfrak{a}_4\mathfrak{a}_5]\rangle_4,\\ \ker \eta \cap \ker r &= \langle [\mathfrak{a}_1^{24}]\rangle_2.\end{aligned}$$

Neither $\ker \eta$ nor $\ker r$ is contained in $\ker \pi_m$. However, their intersection is. Hence, this is an example for the Hilbert class field $H_{K^r}(1)$ is neither contained in the field $K^r H_{K_0^r}(8)$ nor the field $\mathrm{CM}_{K^r,\Phi^r}(8)$ but is contained in the composite of these two fields.

Moreover one can check using Algorithm 4.15 that, in this example, $(\star_d)$ does not hold for any proper divisors d of $m_S = 8$. In addition, computing the kernels

$$\begin{aligned}\ker\left(\eta' : \mathrm{Cl}_{K^r}(8) \to \mathrm{Cl}_{K_0^r}(4)\right) &= \mathrm{Cl}_{K^r}(8),\\ \ker\left(r' : \mathrm{Cl}_{K^r}(8) \to \mathfrak{C}_K(4)\right) &= \langle [\mathfrak{a}_1^{12}]\rangle_4 \times \langle [\mathfrak{a}_2^2]\rangle_2 \times \langle [\mathfrak{a}_4]\rangle_2 \times \langle [\mathfrak{a}_5]\rangle_2,\end{aligned}$$

and the relevant intersections of groups (analogous to what we did in the previous paragraph), we find that neither $H_{K_0^r}(4)\,\mathrm{CM}_{K^r,\Phi^r}(8)$ nor $H_{K_0^r}(8)\,\mathrm{CM}_{K^r,\Phi^r}(4)$ contains $H_{K^r}(1)$.

Finally, we remark that 8 is not the minimum integer m for which $(\star_m)$ holds. One can verify that the smallest integer for which $(\star_m)$ holds is $m = 5$. This is done by recalling that $(\star_m)$ does not hold $m = 1, 2, 4$ as they are proper divisors of 8 and then applying Algorithm 4.15 to $m = 3$ and then $m = 5$. ▲

5. Computing $H_{K^r}(1)$ under $(\star_2)$

Let K be a primitive quartic CM field and let Φ be a CM type of K. Let (K^r, Φ^r) be the reflex pair of (K, Φ).

The field extension $\mathrm{CM}_{K^r,\Phi^r}(1)$ of K^r is obtained by computing Igusa invariants [Igu67; Spa94] and appending them to the field K^r. In a similar manner, the field extension $\mathrm{CM}_{K^r,\Phi^r}(2)$ is obtained by computing Rosenhain invariants [Wam99] instead of Igusa invariants.

Section 5.1 gives a brief recall of theta functions, Rosenhain invariants and references how to compute these invariants.

In Section 5.2, we discuss how to compute, assuming $(\star_2)$, a defining polynomial for $H_{K^r}(1)$ in terms of these Rosenhain invariants. We also discuss our proof-of-concept implementation in this section. The author is working on how to get similar results when the assumption is $(\star_m)$ for integers $m \geq 3$.

In Section 5.3, we compare our implementation of the CM theory algorithm to the current implementations of the well-known Kummer theory algorithm.

5.1. Theta constants and Rosenhain invariants.

Let $g \in \mathbb{Z}_{>0}$. Let $\mathbb{H}_g$ denote the set of $g \times g$ symmetric matrices over $\mathbb{C}$ with positive definite imaginary part. For any

$\vec{\mathbf{a}}, \vec{\mathbf{b}} \in \mathbb{Q}^g$, the *theta function with characteristic* $\begin{bmatrix}\vec{\mathbf{a}}\\ \vec{\mathbf{b}}\end{bmatrix}$ is the function

$$\theta\begin{bmatrix}\vec{\mathbf{a}}\\ \vec{\mathbf{b}}\end{bmatrix}(\vec{\mathbf{z}}, \boldsymbol{\tau}) = \sum_{\vec{\mathbf{n}}\in\mathbb{Z}^g} \exp\left(\pi i\, (\vec{\mathbf{n}}+\vec{\mathbf{a}})^{\intercal}\, \boldsymbol{\tau}(\vec{\mathbf{n}}+\vec{\mathbf{a}})\right) \exp\left(2\pi i\ (\vec{\mathbf{n}}+\vec{\mathbf{a}})^{\intercal}\, (\vec{\mathbf{z}}+\vec{\mathbf{b}})\right)$$

on $\mathbb{C}^g \times \mathbb{H}_g$.

Let $a_1, a_2, b_1, b_2 \in \{0, 1/2\}$. We use the following short-hand notation, used in [Dup06; Str10; Cos11], for the sixteen theta functions with half-integer characteristics as follows:

$$\theta_{16a_2+8a_1+4b_2+2b_1}(\vec{\mathbf{z}}, \boldsymbol{\tau}) := \theta\begin{bmatrix}(a_1 & a_2)^{\intercal}\\ (b_1 & b_2)^{\intercal}\end{bmatrix}(\vec{\mathbf{z}}, \boldsymbol{\tau}).$$

For each $i \in \{0, \ldots, 15\}$, we denote by $\vartheta_i(\boldsymbol{\tau})$ the function $\theta_i(\vec{\mathbf{0}}, \boldsymbol{\tau})$ on $\mathbb{H}_g$.

Let A be a principally polarized abelian surface. An ordered basis $\mathcal{B} = \{B_1, B_2, B_3, B_4\}$ of the 2-torsion subgroup of A is said to be *symplectic with respect to the Weil pairing* μ_2 if the matrix $[\mu_2(B_i, B_j)]_{i,j}$ is equal to $\Omega_{\mathbb{Z}/2\mathbb{Z}}$, where Ω_R is the $2g \times 2g$ matrix of the form

$$\Omega_R = \begin{bmatrix}\mathbf{0} & \mathbf{I}_g\\ -\mathbf{I}_g & \mathbf{0}\end{bmatrix}$$

whose entries are in the ring R. The pair $(A, \mathcal{B})$ is called a *principally polarized abelian surface with level* 2 *structure*. Two principally polarized abelian surfaces with level 2 structures $(A, \mathcal{B})$ and $(A', \mathcal{B}')$ are said to be isomorphic if and only if there exists an isomorphism $a : A \to A'$ of principally polarized abelian surfaces such that $a(B_i) = B_i'$.

We define the following set of functions on $\mathbb{H}_2$.

(5.1)

$$\lambda_1(\boldsymbol{\tau}) = \left(\frac{\vartheta_0(\boldsymbol{\tau})\vartheta_1(\boldsymbol{\tau})}{\vartheta_2(\boldsymbol{\tau})\vartheta_3(\boldsymbol{\tau})}\right)^2,\ \lambda_2(\boldsymbol{\tau}) = \left(\frac{\vartheta_1(\boldsymbol{\tau})\vartheta_{12}(\boldsymbol{\tau})}{\vartheta_2(\boldsymbol{\tau})\vartheta_{15}(\boldsymbol{\tau})}\right)^2,\ \lambda_3(\boldsymbol{\tau}) = \left(\frac{\vartheta_0(\boldsymbol{\tau})\vartheta_{12}(\boldsymbol{\tau})}{\vartheta_3(\boldsymbol{\tau})\vartheta_{15}(\boldsymbol{\tau})}\right)^2.$$

Given $\boldsymbol{\tau} \in \mathbb{H}_2$, we say that $\boldsymbol{\lambda}(\boldsymbol{\tau}) := (\lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau}))$ is *a triple of Rosenhain invariants for* $\boldsymbol{\tau}$. There are other possible choices for defining the Rosenhain invariants but we fix the above choice in this article for the sake of simplicity. This choice is the same as Gaudry's 2007 article[Gau07]. The reader interested in learning more about Rosenhain invariants is referred to [Mum07a; Mum07b].

Let $\boldsymbol{\tau} \in \mathbb{H}_2$ and consider the complex hyperelliptic curve $C_{\boldsymbol{\tau}}$:

$$C_{\boldsymbol{\tau}} : y^2 = x(x-1)(x-\lambda_1(\boldsymbol{\tau}))(x-\lambda_2(\boldsymbol{\tau}))(x-\lambda_3(\boldsymbol{\tau})).$$

We denote its hyperelliptic involution map $(x, y) \mapsto (x, -y)$ by ι. For each $i \in \{0, 1\}$, we denote by P_i the point $(i, 0) \in C$ and for each $j \in \{1, 2, 3\}$, we denote by Q_j the point $(\lambda_j(\boldsymbol{\tau}), 0)$. The points fixed by ι, called the Weierstrass points of $C_{\boldsymbol{\tau}}$, are then P_0, P_1, Q_1, Q_2, Q_3 and the point ∞ at infinity.

The Jacobian $J(C)$ of $C_{\boldsymbol{\tau}}$ is a complex principally polarized abelian surface $A_{\boldsymbol{\tau}}$ isomorphic to the torus $\mathbb{C}^2/(\mathbb{Z}^2 + \boldsymbol{\tau}\mathbb{Z}^2)$. The Jacobian $J(C)$ is isomorphic to the quotient of the group of degree-zero divisors of C by its subgroup of principal divisors, and so elements of a Jacobian can be thought of as divisor classes. A basis $\mathcal{B}_{\boldsymbol{\tau}}$ for the 2 torsion subgroup $A_{\boldsymbol{\tau}}[2]$ of $A_{\boldsymbol{\tau}}$ is given by $\mathcal{B}_{\boldsymbol{\tau}} = \{B_1, B_2, B_3, B_4\}$ where

$$\begin{aligned} B_1 &= [Q_1 + Q_2 - 2\infty]\\ B_2 &= [P_0 + P_1 - 2\infty]\\ B_3 &= [Q_2 + Q_3 - 2\infty]\\ B_4 &= [P_0 - \infty]. \end{aligned} \tag{5.2}$$

One can verify that not only is this a basis for $A_{\boldsymbol{\tau}}[2]$, but it is also symplectic with respect to the Weil pairing μ_2. Just like the choice of Rosenhain invariants, one could use other choices to associate a different symplectic basis to the hyperelliptic curve $C_{\boldsymbol{\tau}}$ but we use this choice for the rest of the article. Hence the pair $(A_{\boldsymbol{\tau}}, \mathcal{B}_{\boldsymbol{\tau}})$ is a principally polarized abelian surface with level 2 structure.

Example 4.11 (continuing from p. 18)**.** We continue with the CM field

$$K = \mathbb{Q}[\alpha] \,/\, (\alpha^4 \;+\; 53\;\alpha^2 \;+\; 500).$$

This CM field has two pairs of CM types up to equivalence. They are:

$$\Phi = \{\, \alpha \mapsto 6.3813\ldots i \;,\; \alpha \mapsto 3.5041\ldots i \,\} \quad \Phi' = \{\, \alpha \mapsto 6.3813\ldots i \;,\; \alpha \mapsto -3.5041\ldots i \,\}$$

We consider a complex principally polarized abelian surface A with complex multiplication by $\mathcal{O}_K$ isomorphic to $\mathbb{C}^2/(\Phi(\mathfrak{o}))$ where $\mathfrak{o}$ is the ideal $(49, \alpha + 5)$ of $\mathcal{O}_K$. Our principally polarized abelian surface A is isomorphic to $A_{\boldsymbol{\tau}}$ where

$$\boldsymbol{\tau} \approx \begin{bmatrix} 1.5852i & -1.6036 \\ -1.6036 & 1/2 + 1.7723i \end{bmatrix}.$$

Defining $\mathcal{B}_{\boldsymbol{\tau}}$ as in (5.2), we find that $(A_{\boldsymbol{\tau}}, \mathcal{B}_{\boldsymbol{\tau}})$ is a principally polarized abelian surface with level 2 structure over $\mathbb{C}$. ▲

If $A_{\boldsymbol{\tau}}$ has complex multiplication by $\mathcal{O}_K$, that is $\operatorname{End} A \cong \mathcal{O}_K$, then the set $\boldsymbol{\lambda}(\boldsymbol{\tau})$ consists only of algebraic numbers. The field of moduli of $(A_{\boldsymbol{\tau}}, \mathcal{B}_{\boldsymbol{\tau}})$ is $\mathbb{Q}(\boldsymbol{\lambda}(\boldsymbol{\tau}))$. This fact, combined with [Shi98b, Corollary 18.9] gives the following equality of fields:

$$\mathrm{CM}_{K^r,\Phi^r}(2) = K^r(\,\boldsymbol{\lambda}(\boldsymbol{\tau})\,). \tag{5.3}$$

5.2. **The algorithm and implementation.** Let (K, Φ) be a primitive quartic CM pair and let (K^r, Φ^r) be its reflex pair.

We discuss how to obtain $H_{K^r}(1)$ assuming $(\star_2)$ holds. Recall that we may use Algorithm 4.15 to determine whether or not $(\star_2)$ holds, which in turn lets us know if we can use this method or not. Under Stark's conjectures, for any positive integer m, the field $H_{K_0^r}(m)$ can be obtained complex-analytically using Stark units [Rob00]. In practice, this works. If we encounter a case where it fails, then this case is a contradiction to Stark's conjectures and we would fallback to Kummer-theory based algorithms. Once we have computed a set of defining polynomials for the compositum, we may then use Galois theory via the technique described in [EM03, Section 6] to determine a set of defining polynomials for to obtain $H_{K^r}(1)$.

The author has written a partial implementation of the above algorithm. The implementation is meant to show, as a proof-of-concept, that CM theory algorithms can compute Hilbert class fields of various examples of quartic CM fields which the current implementations of the known algorithms cannot. We elaborate more on this in Section 5.3. This implementation uses SageMath to interface with the PARI/GP `fgag.gp` script (see page 17) in order to find $\mathfrak{C}_K(\mathfrak{m})$ and the group $I_{K^r,\Phi^r}(m)$. In order to compute period matrices of the relevant principally polarized abelian surfaces and to compute the action of $\mathrm{Cl}_{K^r}(m)$ on the Rosenhain invariants using explicit Shimura reciprocity [Str12], we use Streng's SageMath Recip package. Finally, SageMath interfaces with PARI/GP to approximate the needed theta constants, using the algorithm in [ET14], for the Rosenhain invariant computations.

Example 4.11 (continuing from p. 21)**.** Take

$$G = \ker \eta = \ker(\mathrm{Cl}_{K^r}(2) \to \mathfrak{C}_K(2))$$

and

$$H = \ker \pi_2 = \ker(\mathrm{Cl}_{K^r}(2) \to \mathrm{Cl}_{K^r}(1)).$$

By applying explicit Shimura reciprocity, we find, for each $[\mathfrak{g}] \in G$, a set of integers i_0, i_1, i_2, i_3, a root of unity μ, and a period matrix $\boldsymbol{\tau}'$ such that

$$\lambda_1(\boldsymbol{\tau})^{[\mathfrak{g}]} = \left(\frac{\vartheta_{i_0}(\boldsymbol{\tau}')\vartheta_{i_1}(\boldsymbol{\tau}')}{\vartheta_{i_2}(\boldsymbol{\tau}')\vartheta_{i_3}(\boldsymbol{\tau})} \right)^2.$$

For each period matrix encountered in the previous step, we may then compute approximations of the squares of the relevant theta constants.

Consider the polynomial

$$p_1(X) = \prod_{[\mathfrak{a}] \in G/H} \left(X - \sum_{h \in H} \widetilde{\lambda}_1(\boldsymbol{\tau})^{[\mathfrak{h}][\mathfrak{a}]} \right)$$

where for each $[\mathfrak{g}] \in G$, the value $\widetilde{\lambda}_1(\boldsymbol{\tau})^{[\mathfrak{g}]}$ is an approximation of $\lambda_1(\boldsymbol{\tau})^{[\mathfrak{g}]}$ with a sufficiently high precision for the next steps. Using the approximating polynomial $\widetilde{p}_1(X)$ and the methods in [Str10, Section II.10] to recover a polynomial with coefficients in K^r from this approximation, we find a defining polynomial $p_1(X)$ of the extension $K^r(\lambda_1(\boldsymbol{\tau}))/K^r$ as follows:

$$\begin{aligned} d \cdot p_1(X) = dX^8 + (&-30122040343136935304570011105514912 5{\alpha_r}^2 \\ &- 29438063764199719491190907374578941125)X^7 + \dots \end{aligned}$$

with $d = 5^5 \cdot 11^4 \cdot 71^2 \cdot 251^4 \cdot 311^2 \cdot 431^2$. Observe that this polynomial satisfies

$$p_1(X) \ \in \ \frac{1}{d}\, \mathcal{O}_{K^r}[X] \ \subseteq \ K^r[X].$$

Finally, one may verify that the extension of K^r defined by this polynomial is unramified and cyclic of degree 8. This means that

$$H_{K^r}(1) \cong K^r[X]/(p_1(X)).$$

▲

5.3. **Comparison to the existing Kummer theory algorithm.** Other methods are known for computing abelian extensions, and in particular Hilbert class fields.

One approach is an algorithm based on Kummer theory [Fie01]. This algorithm can find abelian extensions L/K, say of degree d, of a general number field K. However, this algorithm requires that the base field K has sufficiently many roots of unity or that we consider the larger field $K' = K(\zeta_d)$ to find abelian extensions of the original base field K. Such an algorithm is at a disadvantage when K is a quartic CM field and the required extension L has a large prime power degree, since working with a larger field $K' = K(\zeta_d)$ is required to use the algorithm.

Using current implementations of the Kummer algorithm on fields whose ideal class groups are cyclic with order a power of 2, we are able to find defining polynomials for the Hilbert class fields of primitive quartic CM fields whose class groups are cyclic of order up to 16.

For primitive quartic CM fields whose class groups are cyclic of order 32, there are examples for which our implementation of the CM theory algorithm outdoes current implementations of the Kummer theory algorithm. For example, computing the cyclic degree 32 extension H_{K^r} of

$$K^r = \mathbb{Q}[\alpha] \,/\, (\alpha^4 \,+\, 104\,\alpha^2 \,+\, 796),$$

which satisfies $(\star_2)$, takes less than 10 minutes using our implementation while the `bnrclassfield` function of PARI and the `HilbertClassField` function of MAGMA do not finish within twenty-four hours [4].

Acknowledgments. I would like to thank my supervisors, Andreas Enge and Marco Streng, for the careful reading and the invaluable suggestions and comments they gave.

References

[BCP97] Wieb Bosma, John Cannon and Catherine Playoust. 'The Magma algebra system. I. The user language'. *J. Symbolic Comput.* 24.3-4 (1997). Computational algebra and number theory (London, 1993), pp. 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125.

[Bel04] Karim Belabas. 'Topics in computational algebraic number theory'. *J. Théor. Nombres Bordeaux* 16.1 (2004), pp. 19–63. DOI: 10.5802/jtnb.433.

[BGL11] Reinier Bröker, David Gruenewald and Kristin Lauter. 'Explicit CM theory for level 2-structures on abelian surfaces'. *Algebra Number Theory* 5.4 (2011), pp. 495–528. ISSN: 1937-0652. DOI: 10.2140/ant.2011.5.495.

[CDO01] Henri Cohen, Francisco Diaz y Diaz and Michel Olivier. 'Algorithmic methods for finitely generated abelian groups'. In: vol. 31. 1-2. Computational algebra and number theory (Milwaukee, WI, 1996). 2001, pp. 133–147. DOI: 10.1006/jsco.2000.1014.

[Coh00] Henri Cohen. *Advanced topics in computational number theory.* Vol. 193. Graduate Texts in Mathematics. Springer-Verlag, New York, 2000, pp. xvi+578. ISBN: 0-387-98727-4. DOI: 10.1007/978-1-4419-8489-0.

[Coh93] Henri Cohen. *A course in computational algebraic number theory.* Vol. 138. Graduate Texts in Mathematics. Springer-Verlag, Berlin, 1993, pp. xii+534. ISBN: 3-540-55640-0. DOI: 10.1007/978-3-662-02945-9.

[Cos11] Romain Cosset. 'Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques.' Theses. Université Henri Poincaré - Nancy I, Nov. 2011.

[Cre89] Teresa Crespo. 'Embedding problems with ramification conditions'. *Arch. Math. (Basel)* 53.3 (1989), pp. 270–276. ISSN: 0003-889X. DOI: 10.1007/BF01277064.

[Dup06] Régis Dupont. 'Moyenne arithmético-géométrique, suites de Borchardt et applications.' PhD thesis. École polytechnique, 2006.

[EM03] Andreas Enge and François Morain. 'Fast decomposition of polynomials with known Galois group'. In: *Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 2003).* Vol. 2643. Lecture Notes in Comput. Sci. Springer, Berlin, 2003, pp. 254–264. DOI: 10.1007/3-540-44828-4_27.

[ET14] Andreas Enge and Emmanuel Thomé. 'Computing class polynomials for abelian surfaces'. *Exp. Math.* 23.2 (2014), pp. 129–145. ISSN: 1058-6458. DOI: 10.1080/10586458.2013.878675.

[Fie01] Claus Fieker. 'Computing class fields via the Artin map'. *Math. Comp.* 70.235 (2001), pp. 1293–1303. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-00-01255-2.

[4] The machine used is a laptop with 16 GB of RAM. Its processor was an *AMD Ryzen 7 2700U*.

[Gau07] P. Gaudry. 'Fast genus 2 arithmetic based on theta functions'. *J. Math. Cryptol.* 1.3 (2007), pp. 243–265. ISSN: 1862-2976. DOI: 10.1515/JMC.2007.012.

[Igu67] Jun-ichi Igusa. 'Modular forms and projective invariants'. *Amer. J. Math.* 89 (1967), pp. 817–855. ISSN: 0002-9327. DOI: 10.2307/2373243.

[Lan83] Serge Lang. *Complex multiplication*. Vol. 255. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, New York, 1983, pp. viii+184. ISBN: 0-387-90786-6. DOI: 10.1007/978-1-4612-5485-0.

[Mum07a] David Mumford. *Tata lectures on theta. I.* Modern Birkhäuser Classics. With the collaboration of C. Musili, M. Nori, E. Previato and M. Stillman, Reprint of the 1983 edition. Birkhäuser Boston, Inc., Boston, MA, 2007, pp. xiv+235. ISBN: 978-0-8176-4572-4. DOI: 10.1007/978-0-8176-4578-6.

[Mum07b] David Mumford. *Tata lectures on theta. II.* Modern Birkhäuser Classics. Jacobian theta functions and differential equations, With the collaboration of C. Musili, M. Nori, E. Previato, M. Stillman and H. Umemura, Reprint of the 1984 original. Birkhäuser Boston, Inc., Boston, MA, 2007, pp. xiv+272. ISBN: 978-0-8176-4569-4. DOI: 10.1007/978-0-8176-4578-6.

[Neu99] Jürgen Neukirch. *Algebraic number theory*. Vol. 322. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. Springer-Verlag, Berlin, 1999, pp. xviii+571. ISBN: 3-540-65399-6. DOI: 10.1007/978-3-662-03983-0.

[Par19] *PARI/GP version 2.11.2*. available from http://pari.math.u-bordeaux.fr/. The PARI Group. Univ. Bordeaux, 2019.

[Ric36a] Hans Richter. 'Über die Lösbarkeit des Einbettungsproblems für Abelsche Zahlkörper'. *Math. Ann.* 112.1 (1936), pp. 700–726. ISSN: 0025-5831. DOI: 10.1007/BF01565438.

[Ric36b] Hans Richter. 'Über die Lösbarkeit einiger nicht-Abelscher Einbettungsprobleme'. *Math. Ann.* 112.1 (1936), pp. 69–84. ISSN: 0025-5831. DOI: 10.1007/BF01565404.

[Rob00] Xavier-François Roblot. 'Stark's conjectures and Hilbert's twelfth problem'. *Experiment. Math.* 9.2 (2000), pp. 251–260. ISSN: 1058-6458.

[Shi62] Goro Shimura. 'On the class-fields obtained by complex multiplication of abelian varieties'. *Osaka Math. J.* 14 (1962), pp. 33–44. ISSN: 0388-0699.

[Shi94] Goro Shimura. *Introduction to the arithmetic theory of automorphic functions*. Vol. 11. Publications of the Mathematical Society of Japan. Reprint of the 1971 original, Kanô Memorial Lectures, 1. Princeton University Press, Princeton, NJ, 1994, pp. xiv+271. ISBN: 0-691-08092-5.

[Shi98a] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998, pp. xvi+218. ISBN: 0-691-01656-9. DOI: 10.1515/9781400883943.

[Shi98b] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*. Vol. 46. Princeton Mathematical Series. Princeton University Press, Princeton, NJ, 1998, pp. xvi+218. ISBN: 0-691-01656-9. DOI: 10.1515/9781400883943.

[Spa94] Anne-Monika Spallek. 'Kurven vom Geschlecht 2 und ihre Anwendung in Public-Key-Kryptosystemen'. PhD thesis. Universität Gesamthochschule Essen, 1994.

[Str10] Marco Streng. 'Complex multiplication of abelian surfaces'. PhD thesis. Universiteit Leiden, 2010.

[Str12] Marco Streng. *An explicit version of Shimura's reciprocity law for Siegel modular functions*. 2012. arXiv: 1201.0020 [math.NT].

[Wam99] Paul van Wamelen. 'Examples of genus two CM curves defined over the rationals'. *Math. Comp.* 68.225 (1999), pp. 307–320. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-99-01020-0.