2017

Hilbert Class Fields of Imaginary Quadratic Fields and Reflex Fields of Certain Sextic CM Fields

Garvin Gaston
University of Vermont

Hilbert Class Fields of Imaginary Quadratic Fields and Reflex Fields of Certain Sextic CM Fields

A Thesis Presented

by

Garvin Gaston

to

The Faculty of the Graduate College

of

The University of Vermont

In Partial Fulfillment of the Requirements
for the Degree of Master of Science
Specializing in Mathematics

October, 2017

Defense Date: August 2, 2017
Thesis Examination Committee:

Christelle Vincent, Ph.D., Advisor
Christian Skalka, Ph.D., Chairperson
Richard Foote, Ph.D.
Cynthia J. Forehand, Ph.D., Dean of Graduate College

Abstract

In this thesis we look at particular details of class field theory for complex multiplication fields. We begin by giving some background on fields, abelian varieties, and complex multiplication. We then turn to the first task of this thesis and give an implementation in Sage of a classical algorithm to compute the Hilbert class field of a quadratic complex multiplication field using the j-invariant of elliptic curves with complex multiplication by the ring of integers of the field, and we include three explicit examples to illustrate the algorithm.

The second part of this thesis contains new results: Let K be a sextic complex multiplication field with Galois closure L such that the Galois group of L over $\mathbb{Q}$ is isomorphic to D_{12}, the dihedral group with twelve elements. For each complex multiplication type Φ of K, we compute the reflex field and reflex type of the pair (K, Φ) explicitly. We then illustrate our results with the case of $K = \mathbb{Q}[x]/(x^6 - 2x^5 + 2x^4 + 2x^3 + 4x^2 - 4x + 2)$.

Acknowledgements

First and foremost, I'd like to express my overwhelming gratitude to my advisor, Professor Christelle Vincent, for her unwavering guidance, her obvious love and enthusiasm for mathematics, her talent for teaching, and perhaps above all her sense of humor and her patience throughout this process. She has gone above and beyond what I expected from an advisor, and I will forever be grateful to her for her dedication.

I would also like to thank my family: my parents Gaynor and Tony Banham and John Gaston; my sister and brother-in-law Caroline and Noush Haghpeykar and my nephew Johnny; and my dogs Juno and Martin. I depended on their emotional support like I never have before over the past two years. Thank you.

Finally, I have been so fortunate to have incredible teachers throughout my life. I thank them all, and I hope to follow in their footsteps.

Table of Contents

Acknowledgements ii

1 Introduction **1**
1.1 Explicit class field theory 1
1.2 Overview of contents 4

2 Field preliminaries **7**
2.1 Field theory 7
2.1.1 Fields and field extensions 7
2.1.2 Finding the minimal polynomial 8
2.1.3 Number fields 10
2.1.4 Galois extensions 11
2.2 Rings of integers 13
2.2.1 Ideals in a ring 13
2.2.2 The ring of integers of a number field 14
2.2.3 Dirichlet's Unit Theorem 16
2.2.4 The different of a number field 17
2.3 Class field theory 17
2.4 Fixed fields 19

3 Abelian varieties **22**
3.1 Elliptic curves 22
3.1.1 Preliminaries 22
3.1.2 Analytic Theory 25
3.2 General case 29
3.2.1 Preliminaries 30
3.2.2 Analytic theory 31

4 Complex Multiplication **36**
4.1 Elliptic curves 36
4.2 Generating $f_K(x)$ 38
4.3 CM-types 39
4.4 Construction of dimension 3 abelian varieties 42

5 Elliptic curves and Sage **44**
5.1 Computing the j-invariant 44
5.2 Examples 45

6 Reflex fields **52**
6.1 Galois group preliminaries 52
6.2 Matching an embedding to a Galois element 53
6.3 Equivalence classes of CM-types 55
6.4 Finding reflex types 58
6.4.1 Reflex of Φ_1 59
6.4.2 Reflex of Φ_2 60
6.4.3 Reflex of Φ_3 61
6.4.4 Reflex of Φ_4 61
6.4.5 Reflex of $\overline{\Phi_1}$ 62
6.4.6 Reflex of $\overline{\Phi_2}$ 62
6.4.7 Reflex of $\overline{\Phi_3}$ 63
6.4.8 Reflex of $\overline{\Phi_4}$ 64

7 Example **65**
7.1 Preliminaries 65
7.2 Computation of Reflex Fields and Reflex Types 70
7.2.1 CM-types Φ_1 and $\overline{\Phi_1}$ 71
7.2.2 CM-types Φ_2 and $\overline{\Phi_2}$ 73
7.2.3 CM-types Φ_3 and $\overline{\Phi_3}$ 74
7.2.4 CM-types Φ_4 and $\overline{\Phi_4}$ 75

Bibliography **78**

A Sage code **80**

Chapter 1

Introduction

Given a number field K, it is of interest to consider its abelian field extensions, by which we mean the Galois extensions of K with abelian Galois group. The study of these extensions is called class field theory, which more generally is a branch of algebraic number theory that looks at abelian extensions of local and global fields, and the arithmetic properties of these extensions.

Of particular interest is the Hilbert class field, which is the maximal abelian unramified extension of a field. If K is a number field, its Hilbert class field exists and has finite degree over K, as shown by Furtwängler [6].

1.1 Explicit class field theory

In [4], Daberkow and Pohst give an algorithm to explicitly compute the Hilbert class field of arbitrary number fields. However, the algorithm is not practical, as it requires computing a large number of Kummer extensions of the base field. In any case, their algorithm shows that the problem is decidable.

If one is willing to restrict the class of number fields considered, much more can be said. If $K = \mathbb{Q}$, then all of the abelian Galois extensions of K are contained in some $\mathbb{Q}(\zeta_n)$, where ζ_n is a primitive n^{th} root of unity. In other words, for any extension $L/\mathbb{Q}$ that is abelian, there exists an n such that $L \subseteq \mathbb{Q}(\zeta_n)$. It is important to note that not every Galois extension of $\mathbb{Q}$ is contained in some $\mathbb{Q}(\zeta_n)$, just the abelian extensions. However, all of these extensions are ramified, as $\mathbb{Q}$ does not have any unramified extensions.

The next case for which we have an explicit construction of abelian extensions is that of K, an imaginary quadratic field, i.e., a quadratic CM field. For example, we can construct the Hilbert class field of K, which we denote H_K, explicitly:

Theorem 1.1.1. *Let K be an imaginary quadratic field. Then its Hilbert class field is $K(j)$ for j the j-invariant of an elliptic curve with endomorphism ring $\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K.*

In this thesis, we provide code that, given any imaginary quadratic field K, gives a monic polynomial f_K with integer coefficients such that $H_K = \mathbb{Q}[x]/(f_K(x))$. The algorithm that we give is not new, and is not an optimal implementation. It is merely a toy problem to grapple with the higher degree CM fields that form the real heart of this thesis. For an optimal implementation, we direct the reader to Cohen's book *A course in computational algebraic number theory* [2]. Although we won't consider this here, we note that more general abelian extensions of such K can be generated using the torsion points of the elliptic curves appearing in Theorem 1.1.1.

The next case for which we have partial explicit constructions is that of K, a general CM field. When K is of degree four or more over $\mathbb{Q}$, we must consider a few differences. First, instead of considering the field of moduli of the abelian variety

(which is generated by the j-invariant when the abelian variety has dimension 1), we must give the abelian variety a polarization, and consider the field of moduli of the polarized abelian variety. Secondly, given a polarized abelian variety with endomorphism ring isomorphic to $\mathcal{O}_K$, its field of moduli is an extension of the reflex field, which we denote K^R, and not necessarily of the field of complex multiplication. Thirdly, this field of moduli will be an unramified abelian extension of K^R, but in general it will not be the maximal such extension. In other words, the field of moduli of the polarized abelian variety will not necessarily give us the Hilbert class field of K^R.

In this thesis, we introduce the definitions and notions necessary to more fully explain the concepts of the previous paragraph. We then consider the situation of K a sextic CM field whose Galois closure L has Galois group isomorphic to D_{12}, the dihedral group with twelve elements. For this class of fields and any CM-type attached to K, we compute the corresponding reflex field and reflex type. In addition, we choose an explicit such field to carry out the computations, as an example of our results.

Finally, for completeness we mention the last case for which we have explicit constructions of unramified abelian extensions, which is that of real quadratic fields. Indeed, in 1999 Cohen and Roblot [3] gave an algorithm for computing the Hilbert class field of a real quadratic field using Stark units. This method is different from the CM method used for quadratic and higher degree CM fields which is mentioned above.

1.2 Overview of contents

We now delve into some more details about the contents of each Chapter of this thesis. We note that for all topics covered in the literature, specific references are offered within each Chapter. However, as many of these results are quite old, the references we offer are merely suggestions and do not reflect an exhaustive list. Producing such a list would be impossible given the wealth of work that has been done on some of these topics.

In Chapter 2 we review the basic properties of fields. We begin with a review of field theory, including Galois theory and facts about the ring of integers $\mathcal{O}_K$ of a number field K. We then introduce the notion of ramification of prime ideals to introduce class field theory and define unramified extensions. All of these results are well-known. We end with some new results which we will need about sextic CM subfields of a Galois CM field with Galois group D_{12}.

In Chapter 3 we turn our attention to the theory of abelian varieties. We begin by presenting in some detail the case of elliptic curves, which are abelian varieties of dimension 1, and then turn our attention to the general case, with a focus in particular on abelian varieties of dimension 3. Throughout, we particularly introduce the theory of abelian varieties defined over $\mathbb{C}$, the complex field, as these are the varieties that arise in the construction of explicit class fields. Again, all of these results are well-known and amply covered in the literature.

In Chapter 4 we tackle two tasks. We first explain the process for finding the Hilbert class polynomial $f_K(x)$ of an imaginary quadratic field K. We then define complex multiplication (CM) and define CM-types and various notions associated to

CM-types. In particular this is where reflex fields and reflex types are introduced. Finally, we end with the Main Theorem of Complex Multiplication, which precisely describes the unramified abelian extension generated by the field of moduli of a polarized abelian variety with CM by an order in a CM field. This is the last Chapter reviewing the literature necessary for the new results that follow.

As a toy problem in Chapter 5 we turn our attention to the classical computation of the Hilbert class field of an imaginary quadratic field K. We again note that algorithms that do so are well-known, and point the reader to Cohen's *A Course in Computational Algebraic Number Theory* [2] for a particularly efficient example. In this work we use the naïve algorithm given in Section 4.2 and its implementation given in Appendix A to explore three examples where we compute f_K, the monic polynomial such that $H_K = \mathbb{Q}[x]/(f_K(x))$, where we recall that H_K is the Hilbert class field of K.

Finally, Chapter 6 contains the bulk of the new results of this thesis. In it, we systematically study the case of K, a sextic CM field whose Galois closure L has Galois group isomorphic to D_{12}. Armed with these results, we then proceed to compute, for each CM-type Φ of K, the associated reflex field K^R and reflex type Φ^R of the pair (K, Φ). This is a new contribution to the field, which should be useful in future computational projects. In Chapter 7 we apply the theory of Chapter 6 to an explicit example, the case where

$$K = \mathbb{Q}[x]/(x^6 - 2x^5 + 2x^4 + 2x^3 + 4x^2 - 4x + 2).$$

The thesis ends with an Appendix containing the implementation of the algorithm given in Section 4.2 whose results are given for a few examples in Chapter 5. We note

here some implementation details. First, we used the software Sage for several reasons: it contains all of the libraries and packages necessary to perform the computations, as do Magma and Pari. We chose Sage among these three mathematical software libraries because it is based on the language Python, which is in wide use and therefore easy to learn. Furthermore, Sage is open source and has excellent documentation. Although the algorithm is correct for the three examples of Chapter 5, we note that for examples with larger class number the precision will need to be increased to produce numbers accurate enough to be rounded to integers.

Chapter 2

Field preliminaries

In this chapter we present the background on fields that we will need for the work of this thesis, notably our work in Chapter 6 on reflex fields.

Most of the definitions, theorems, etc. are standard and can be found, for example, in Dummit and Foote [5] or Milne [9] or [11]. Section 4 contains new results that we will need later, which are specific to the context of Chapter 6.

2.1 Field theory

Here we review some basic definitions and theorems related to field theory which will help us to build the structures we will need in the subsequent chapters. We are interested in particular in number fields that have complex multiplication.

2.1.1 Fields and field extensions

We begin with some basic information on fields and field extensions that we will use as we move forward.

Definition 2.1.1. *Let K and L be fields. Then a field homomorphism is a map $f\colon K \to L$ such that for all $a, b \in K$,*

1. $f(a+b) = f(a) + f(b)$,
2. $f(ab) = f(a)f(b)$,
3. $f(1_K) = 1_L$.

Definition 2.1.2. *Let F and K be fields. We say that K is a field extension of F if there exists an injective field homomorphism from F into K. Such a field extension is denoted K/F.*

Definition 2.1.3. *An extension K/F is said to be simple if $K = F(\alpha)$ for some $\alpha \in K$. In this case, α is called a primitive element.*

Example 2.1.4. *$\mathbb{Q}(\pi)$ and $\mathbb{Q}[i]$ are simple extensions of $\mathbb{Q}$.*

Definition 2.1.5. *Let K and K' be two field extensions of F and σ a field isomorphism from K to K'. One says that σ is an F-isomorphism if $\sigma(x) = x$ for all $x \in F$. If $K' = K$, the set of automorphisms of K fixing F is denoted $\mathrm{Aut}(K/F)$.*

Definition 2.1.6. *Let K/F be a field extension. Then K can be considered as an F-vector space. The dimension of K/F is called the degree of K/F and is denoted $[K : F]$. If $[K : F]$ is finite then we say that the extension K/F is finite.*

2.1.2 Finding the minimal polynomial

In Chapter 4 we will present a well-known algorithm to compute the so-called Hilbert class field (see Definition 2.3.5) of an imaginary quadratic field K, which we will

denote H_K. We will do so by giving the minimal polynomial of a primitive element of the extension H_K/K. To this end, we now give the definition of the minimal polynomial of an element of a field and give an example of how to compute the minimal polynomial of an element of an imaginary quadratic extension of $\mathbb{Q}$.

Definition 2.1.7. *Let K/F be a field extension and α be an element of K. The minimal polynomial of α over F, if it exists, is the monic polynomial of least degree among all polynomials belonging to $F[x]$ having α as a root. If the minimal polynomial of α over F exists, we say that α is algebraic over F.*

Example 2.1.8. *Let $K = \mathbb{Q}(i)$. Then any $\tau \in K$ is of the form $\tau = a + bi$ with $a, b \in \mathbb{Q}$.*

Suppose first that $\tau \in \mathbb{Q}$, so $b = 0$. Then the minimal polynomial of τ over $\mathbb{Q}$ is $x - \tau$. Suppose now that $\tau \notin \mathbb{Q}$, so $b \neq 0$. To find the minimal polynomial of τ over $\mathbb{Q}$, we first square τ:

$$\tau^2 = (a + bi)^2 = a^2 + 2abi - b^2$$

If $a^2 + 2abi - b^2 \in \mathbb{Q}$, i.e., $2ab = 0$, then necessarily $a = 0$. In that case $x^2 + b^2$ is the minimal polynomial of $\tau = ib$ over $\mathbb{Q}$. On the other hand, if $ab \neq 0$, then

$$2a\tau = 2a^2 + 2abi$$

and

$$\tau^2 - 2a\tau = a^2 - b^2 - 2a^2 = -a^2 - b^2.$$

So,

$$\tau^2 - 2a\tau + a^2 + b^2 = 0.$$

Since $a, b \in \mathbb{Q}$, we get a polynomial over $\mathbb{Q}$, and the minimal polynomial of τ over $\mathbb{Q}$ is

$$m_\tau(x) = x^2 - 2ax + a^2 + b^2.$$

2.1.3 Number fields

A goal of this thesis is to compute reflex fields specifically of certain number fields, so we provide some definitions on number fields, a particular kind of field extension.

Definition 2.1.9. *A number field is a finite degree field extension of the field $\mathbb{Q}$ of rational numbers.*

Definition 2.1.10. *Let K be a number field. A complex embedding of K is an injective field homomorphism $\varphi\colon K \hookrightarrow \mathbb{C}$ such that $\mathrm{Im}\sigma \not\subseteq \mathbb{R}$, and a real embedding of K is an injection $\sigma\colon K \hookrightarrow \mathbb{R}$.*

Definition 2.1.11. *A number field K is a CM-field if it is a totally imaginary extension K/K_0 of degree 2 of a totally real field K_0.*

In our work, we will often need a different characterization of CM fields, due to Lang:

Proposition 2.1.12 (Characterization of CM-fields from Lang [7])**.** *Either one of the following two conditions characterize a CM-field:*

1. *K is a totally imaginary quadratic extension of a totally real field.*
2. *Complex conjugation $\bar{\cdot}$ commutes with every embedding of K in $\overline{\mathbb{Q}}$, and K is not real. In particular, if $K/\mathbb{Q}$ is Galois, then $\bar{\cdot}$ is in the center of $\mathrm{Gal}(K/\mathbb{Q})$.*

Theorem 2.1.13. *Let K be a number field. Then its complex embeddings come in conjugate pairs, where we define the complex conjugate of φ, denoted $\overline{\varphi}$, to be the composition of first φ and then complex conjugation. Furthermore, if $[K : \mathbb{Q}] = n$, r_1 is the number of distinct real embeddings of K and r_2 is the number of conjugate pairs of complex embeddings of K, we have*

$$n = r_1 + 2r_2.$$

2.1.4 Galois extensions

We are particularly interested in a certain special kind of field extension called a Galois extension. Before we define a Galois extension, we define two specific types of field extensions.

Definition 2.1.14. *A field extension K/F is said to be normal over F if every irreducible polynomial in $F[x]$ either has no root in K or splits into linear factors in K.*

Definition 2.1.15. *A separable extension is an algebraic field extension K/F such that for every $\alpha \in K$, the minimal polynomial of α over F is a separable polynomial, i.e., its roots are distinct.*

Theorem 2.1.16 (Primitive Element Theorem from [5])**.** *If K/F is finite and separable, then K/F is simple, i.e. $K = F(\alpha)$ for a single element $\alpha \in K$. In this case $K \cong F[x]/(m_\alpha(x))$. In particular, any finite extension of fields of characteristic 0 is simple.*

Definition 2.1.17. *A Galois extension is a finite algebraic field extension K/F that is normal and separable.*

Definition 2.1.18. *Let K/F be a Galois extension. The group of automorphisms* $\mathrm{Aut}(K/F)$ *is called the Galois group of K/F, denoted* $\mathrm{Gal}(K/F)$.

Definition 2.1.19. *The Galois closure of an extension K/F in a fixed algebraic closure $\overline{F}$ is a field which is minimal among all Galois extensions of F containing K. In particular, if K is a number field we adopt the convention that the Galois closure of K is the Galois closure of $K/\mathbb{Q}$.*

The following proposition and theorem are used in Chapter 6 to prove Proposition 6.3.1, which gives information about the automorphism group of a certain field K of interest in this work.

Definition 2.1.20. *Let $K/\mathbb{Q}$ be a finite Galois extension. The fixed field K^H of a subgroup $H \leq \mathrm{Gal}(K/\mathbb{Q})$ is the set of elements of K that are fixed by H. This set is a subfield of K and $[K : K^H] = |H|$ with $H \cong \mathrm{Gal}(K/K^H)$.*

Theorem 2.1.21 (Theorem 9 from page 570 of [5])**.** *Let K be a field and let $G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_n\}$ be a subgroup. Let F be the fixed field of* $\mathrm{Aut}(K)$. *Then*

$$[K\colon F] = n = |G|.$$

Proposition 2.1.22 (Corollary 10 from page 572 of [5])**.** *Let K/F be any finite field extension. Then*

$$|\mathrm{Aut}(K/F)| \leq [K\colon F]$$

with equality if and only if F is the fixed field of $\mathrm{Aut}(K/F)$*. Put another way, K/F is Galois if and only if F is the fixed field of* $\mathrm{Aut}(K/F)$*.*

2.2 Rings of integers

We now turn our attention to the so-called ring of integers of a number field, which plays for the number field the role played by the integers $\mathbb{Z}$ for the rational field $\mathbb{Q}$.

2.2.1 Ideals in a ring

We begin with some background on ideals in general rings.

Definition 2.2.1. *Let R be a ring, let I be a subset of R, and let $r \in R$.*

1. *We define the sets $rI = \{ra \mid a \in I\}$ and $Ir = \{ar \mid a \in I\}$.*
2. *A subset I of R is a left ideal of R if*
   (a) *I is a subring of R, and*
   (b) *I is closed under left multiplication by elements from R, i.e., $rI \subseteq I$ for all $r \in R$.*

   Similarly I is a right ideal if (a) holds and in place of (b) one has
   (c) *I is closed under right multiplication by elements from R, i.e., $Ir \subseteq I$ for all $r \in R$.*
3. *A subset I that is both a left ideal and a right ideal is called an ideal (or, for added emphasis, a two-sided ideal) of R.*

Definition 2.2.2. *Let R be a ring. We say an ideal I is generated by $a_1, \ldots, a_n \in R$ and write $I = (a_1, \ldots, a_n)$ if*

$$I = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_i \in R\}.$$

Example 2.2.3. *If $R = \mathbb{Z}[\sqrt{-5}]$, then $I = (2, 1 + \sqrt{-5}) = \{2a + (1 + \sqrt{-5})b \mid a, b \in \mathbb{Z}[\sqrt{-5}]\}$.*

Definition 2.2.4. *An ideal generated by a single element is called a principal ideal.*

Definition 2.2.5. *Let I and J both be ideals. Then IJ is the ideal generated by all elements of the form ij where $i \in I$ and $j \in J$.*

Example 2.2.6. *If $I = (a, b)$ and $J = (c, d)$, then $IJ = (ac, ad, bc, bd)$.*

Definition 2.2.7. *Let I be an ideal of a commutative ring R. Then I is a prime ideal of R if the following two properties hold:*

1. *Let $a, b \in R$ such that $ab \in I$. Then $a \in I$ or $b \in I$.*
2. *$I \neq R$.*

2.2.2 The ring of integers of a number field

We can now define the ring of integers of a number field, and along with it the ideal class group of a number field K.

Definition 2.2.8. *Let K be a number field. Then the ring of integers of K, denoted $\mathcal{O}_K$, is the set of all algebraic integers in K,*

$$\mathcal{O}_K = \{\tau \in K : \text{the minimal polynomial of } \tau \text{ has coefficients in } \mathbb{Z}\}.$$

We note that $\mathcal{O}_K$ is a ring, and it is of rank n over $\mathbb{Z}$, where $n = [K : \mathbb{Q}]$.

Example 2.2.9. *The Gaussian integers $\mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z}\}$ is the ring of integers of $K = \mathbb{Q}(i)$, and the Eisenstein integers $\mathbb{Z}[\omega] = \{a + b\omega \colon a, b \in \mathbb{Z}\}$, is the ring of integers of $\mathbb{Q}(\omega)$, where $\omega = (-1 + \sqrt{-3})/2$ is a primitive cube root of unity.*

Theorem 2.2.10. *$\mathcal{O}_K$ has unique factorization into primes for ideals.*

We now give a different characterization of the relationship between a number field K and its ring of integers $\mathcal{O}_K$.

Definition 2.2.11. *A commutative ring with identity $1 \neq 0$ is called an integral domain if it has no zero divisors.*

Definition 2.2.12. *Let K be a field and let $A \subset K$ be an integral domain. If every $c \in K$ can be written in the form $c = ab^{-1}$, where $a, b \in A$ and $b \neq 0$, then K is called the field of fractions of A.*

Example 2.2.13. *The field of fractions of $\mathbb{Z}$, the ring of integers, is $\mathbb{Q}$, i.e.,* $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$. *If we let $R = \mathbb{Z}[i] = \{a + bi \colon a, b \in \mathbb{Z}\}$, then* $\mathrm{Quot}(R) = \mathbb{Q}(i) = \{c + di \colon c, d \in \mathbb{Q}\}$.

Theorem 2.2.14. *Let K be a number field and $\mathcal{O}_K$ be its ring of integers. Then $\mathcal{O}_K$ is an integral domain, and K is its field of fractions.*

We are finally in a position to define the ideal class group of a number field K.

Definition 2.2.15. *Let R be an integral domain and let K be its field of fractions. A fractional ideal of R is an R-submodule I of K such that there exists $0 \neq r \in R$ with $rI \subseteq R$. The element r can be thought of as clearing out the denominators in I.*

Example 2.2.16. *Consider* $\mathbb{Z} \subset \mathbb{Q}$. *Then* $I = \{\frac{a}{2^n} \mid a \in \mathbb{Z}, n \in \mathbb{Z}^+\}$ *is not a fractional ideal because there is no largest denominator to clear. However,* $I = \frac{1}{3}\mathbb{Z}$ *is a fractional ideal because we can clear the denominator of 3, i.e.,* $3I \subseteq \mathbb{Z}$.

Definition 2.2.17. *The ideal class group of a number field* K *is a certain group of equivalence classes of ideals, given by* $\{I\}/\sim$ *where* $I \sim J$ *if there exists* $\alpha \in K$ *such that* $(\alpha)I = J$.

2.2.3 Dirichlet's Unit Theorem

Dirichlet's Unit Theorem is a fundamental result in algebraic number theory that we give here because of its significance.

Theorem 2.2.18. *(Dirichlet's Unit Theorem) Let* K *be a number field with* r_1 *real embeddings and* r_2 *conjugate pairs of complex embeddings. Then the group of units of the ring of integers, denoted* $\mathcal{O}_K^\times$, *is finitely generated with rank* $d = r_1 + r_2 - 1$.

Definition 2.2.19. *Let* $\mathcal{O}_K^\times \cong \mathcal{O}_{K,tors}^\times \times \mathbb{Z}^d$. *A set* $\epsilon_1, \ldots, \epsilon_d$ *of units that generates* $\mathcal{O}_K^\times/\mathcal{O}_{K,tors}^\times$ *is called a set of fundamental units.*

Example 2.2.20. *Let* K *be a sextic CM field. Since* $[K : \mathbb{Q}] = 6$ *and* K *is totally imaginary, the field* K *has 3 conjugate pairs of complex embeddings. Its totally real subfield* K_0 *has degree 3 over* $\mathbb{Q}$ *and therefore has 3 real embeddings and no complex embeddings.* K_0 *has* $r_1 = 3$, $r_2 = 0$, *so has* $3 + 0 - 1 = 2$ *fundamental units.* K *also has 2 fundamental units. By Dirichlet's Unit Theorem we have*

$$\mathcal{O}_K^\times \cong \mathcal{O}_{K,tors}^\times \times \epsilon_1^{\mathbb{Z}} \times \epsilon_2^{\mathbb{Z}}$$

and

$$\mathcal{O}_{K_0}^{\times} = \{\pm 1\} \times \epsilon_1^{\mathbb{Z}} \times \epsilon_2^{\mathbb{Z}}.$$

Therefore it follows that the fundamental units of K belong to K_0. We note that $\mathcal{O}_{K,tors}^{\times}$ possibly contains more complex roots of unity.

2.2.4 The different of a number field

We now end this Section by introducing a distinguished fractional ideal of a number field K, called the different, which we will need to verify if a certain construction of an abelian variety is principally polarizable.

Definition 2.2.21. *Let $K/\mathbb{Q}$ be a finite field extension. The trace of $\alpha \in K$ is*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = [K : \mathbb{Q}(\alpha)] \sum_{j=1}^{n} \alpha_j$$

where α_j ranges over all Galois conjugates of α.

Definition 2.2.22. *Let $I \subseteq K$ be the set*

$$I = \{x \in K : \mathrm{Tr}_{K/\mathbb{Q}}(xy) \in \mathbb{Z} \text{ for all } y \in \mathcal{O}_K\}.$$

I is a fractional ideal of K. $\delta_{K/\mathbb{Q}} = I^{-1}$ is an ideal of $\mathcal{O}_K$ called the different of K.

2.3 Class field theory

As mentioned in the introduction, class field theory is the study of the arithmetic properties of the abelian field extensions of a number field K. We are particularly

interested in H_K, the Hilbert class field of K, which we define in this section.

The first notion we need is that of the ramification of primes in a Galois extension of number fields.

Proposition 2.3.1. *Let L be an extension of a number field K, and let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_K$, the ring of integers of K. Then $\mathfrak{p}\mathcal{O}_L$ is an ideal of $\mathcal{O}_L$.*

Proposition 2.3.2. *Let L be a Galois extension of a field K, with $[L : K] = n$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$, and consider the ideal $\mathfrak{p}\mathcal{O}_L$ of $\mathcal{O}_L$. Then we have*

$$\mathfrak{p}\mathcal{O}_L = (\mathfrak{P}_1 \cdots \mathfrak{P}_r)^e, \tag{2.1}$$

where the $\mathfrak{P}_i$s are distinct prime ideals of $\mathcal{O}_L$, and

$$erf = n,$$

where f is such that

$$f = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}].$$

(We note that this quantity is independent of the choice of ideal $\mathfrak{P}_i$ among the factors of $\mathfrak{p}$.)

Definition 2.3.3. *Let L be a Galois extension of a field K and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$. If $e > 1$ in the decomposition into prime factors of $\mathfrak{p}\mathcal{O}_L$ of equation 2.1, then we say that the extension L/K is ramified at the finite prime $\mathfrak{p}$.*

Definition 2.3.4. *Let L be a Galois extension of a field K, and let φ be a real*

embedding of K. Consider the following sets of embeddings of L:

$$\{\psi\colon L \to \mathbb{C} : \psi|_K = \varphi\}.$$

If the embeddings contained in this set are real embeddings of L, we say that the infinite prime φ is unramified. If the embeddings are complex (in other words, if they do not factor through the real numbers), then the infinite prime φ is ramified. If φ is a complex embedding of K that does not factor through the real numbers, then φ is always unramified in any extension of K.

We can now define the Hilbert class field of a number field.

Definition 2.3.5. *The Hilbert class field H_K of a number field K is the maximal abelian unramified extension of K, by which we mean that H_K is unramified at all finite and infinite primes of K.*

Example 2.3.6. *The Hilbert class field of $\mathbb{Q}$ is $\mathbb{Q}$ itself. $\mathbb{Q}(\zeta_n)$ is ramified at each $p|n$.*

Theorem 2.3.7. *Let K be a number field and H_K be the Hilbert class field of K. Then $[H_K : K] = h_K$, where h_K is the size of the ideal class group of K, which we call the class number of K.*

2.4 Fixed fields

We finally turn our attention to the particular situation we consider in this thesis. We will be concerned with the case of K a sextic CM field with Galois closure L and

such that $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$. (Here D_{12} is the group with presentation $\langle r, s \mid r^6 = s^2 = 1, srs = r^{-1} \rangle$.) We are interested in this Section in proving some results about certain subfields of L.

By direct computation, one can see that D_{12} has seven subgroups of order 2, which are $\langle r^3 \rangle$, $\langle s \rangle$, $\langle rs \rangle$, $\langle r^2 s \rangle$, $\langle r^3 s \rangle$, $\langle r^4 s \rangle$, and $\langle r^5 s \rangle$. Taking the fixed field of these subgroups yields seven subfields of L of degree 6 over $\mathbb{Q}$.

One of these subgroups is generated by r^3, which we will see in Proposition 6.1.2 is complex conjugation and therefore its fixed field $L^{\langle r^3 \rangle}$ is totally real. In fact, L is a degree 12 CM field, and $L^{\langle r^3 \rangle}$ is its totally real subfield of index 2. The other six subgroups all give rise to sextic CM fields.

Proposition 2.4.1. *We have that $L^{\langle s \rangle} \cong L^{\langle r^2 s \rangle} \cong L^{\langle r^4 s \rangle}$ and that $L^{\langle rs \rangle} \cong L^{\langle r^3 s \rangle} \cong L^{\langle r^5 s \rangle}$, where $\cong$ denotes field isomorphism.*

Proof. First we show that $L^{\langle s \rangle} \cong L^{\langle r^2 s \rangle}$. We claim that $r \colon L^{\langle s \rangle} \to L^{\langle r^2 s \rangle}$ is well-defined, where $r \in D_{12}$ is restriced to $L^{\langle s \rangle}$. Let $l \in L^{\langle s \rangle}$, then by definition $s(l) = l$. We want to show that $r(l) \in L^{\langle r^2 s \rangle}$, i.e., $r^2 s(r(l)) = r(l)$. Indeed:

$$r^2 s(r(l)) = r^2 sr(l) = r^2 r^{-1} s^{-1} = rs(l) = r(l).$$

Thus the map is well-defined. Since r is an automorphism of L, it is invertible. Thus $L^{\langle s \rangle} \cong L^{\langle r^2 s \rangle}$.

Next we show that $L^{\langle s \rangle} \cong L^{\langle r^4 s \rangle}$. We claim that $r^2 \colon L^{\langle s \rangle} \to L^{\langle r^4 s \rangle}$. Let $l \in L^{\langle s \rangle}$, then again $s(l) = l$. We will show that $r^4 s(r^2(l)) = r^2(l)$, so $r^2(l) \in L^{\langle r^4 s \rangle}$:

$$r^4 s(r^2(l)) = r^4 sr^2(l) = r^4 r^{-2} s^{-1}(l) = r^2 s(l) = r^2(l).$$

Thus r^2 is well-defined. Again, r^2 is an automorphism of L and therefore invertible. Thus $L^{\langle s\rangle} \cong L^{\langle r^2 s\rangle} \cong L^{\langle r^4 s\rangle}$.

The case of $L^{\langle rs\rangle} \cong L^{\langle r^3 s\rangle} \cong L^{\langle r^5 s\rangle}$ is similar with the maps

$$r\colon L^{\langle rs\rangle} \to L^{\langle r^3 s\rangle},$$

and

$$r^2\colon L^{\langle rs\rangle} \cong L^{\langle r^2 s\rangle}$$

giving the isomorphisms. □

Chapter 3

Abelian varieties

In this Chapter we provide the basics of the theory of elliptic curves and abelian varieties. We focus in particular on the case of elliptic curves and abelian varieties of dimension 3 defined over the field $\mathbb{C}$, as these are the abelian varieties connected to the work of Chapters 5 and 6.

3.1 Elliptic curves

3.1.1 Preliminaries

All of these facts are standard and can be found in Silverman [13] and [14].

Definition 3.1.1. *Let k be a field of characteristic different from 2 or 3. An elliptic curve E defined over k (we will write E/k) has a Weierstrass equation of the form*

$$E : y^2 = x^3 + Ax + B$$

with $A, B \in k$ and such that $\Delta = 4A^3 + 27B^2 \neq 0$.

Definition 3.1.2. *If an elliptic curve E has a Weierstrass equation as in Definition 3.1.1, then the j-invariant of E is defined as*

$$j = -1728\frac{(4A)^3}{-16(4A^3 + 27B^2)}. \tag{3.1}$$

Remark 3.1.3. *Two elliptic curves are isomorphic (see Definition 3.1.6) over an algebraically closed field if and only if they have the same j-invariant.*

Theorem 3.1.4. *An elliptic curve as in Definition 3.1.1 is a one-dimensional abelian variety with identity O, the unique point at infinity of the Weierstrass equation.*

Our interest in this work is in what are called CM elliptic curves.

Definition 3.1.5. *Let E_1 and E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism defined over $\overline{k}$, the algebraic closure of k,*

$$\varphi\colon E_1 \to E_2 \quad \text{satisfying} \quad \varphi(O) = O. \tag{3.2}$$

Two elliptic curves E_1 and E_2 are isogenous if there is an isogeny from E_1 to E_2 with $\varphi(E_1) \neq \{O\}$.

Elliptic curves are abelian groups, so the set of maps between them forms a group. Indeed, we denote the set of isogenies from E_1 to E_2 by

$$\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\}. \tag{3.3}$$

The sum of two isogenies φ, ψ is defined by

$$(\varphi + \psi)(P) = \varphi(P) + \psi(P), \tag{3.4}$$

and $\varphi + \psi$ is a morphism, so it is an isogeny or the zero map. Hence $\mathrm{Hom}(E_1, E_2)$ is an abelian group.

Definition 3.1.6. *An endomorphism of an elliptic curve defined over a field k is an isogeny $\varphi\colon E \to E$ defined over $\overline{k}$, the algebraic closure of k.*

Since endomorphisms have two operations, composition and addition, the abelian group $\mathrm{Hom}(E, E)$ is in fact a ring.

Definition 3.1.7. *The endomorphism ring of an elliptic curve E, denoted* $\mathrm{End}(E)$*, is the ring of all endomorphisms of E. The set* $\mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$*, the ring of endomorphisms tensored up to $\mathbb{Q}$ over $\mathbb{Z}$, is called the endomorphism algebra of E.*

Theorem 3.1.8 (Corollary 9.4 from [14])**.** *Let k be a field of characteristic 0 (e.g., $k = \mathbb{C}$). The endomorphism ring of an elliptic curve E/k is either isomorphic to $\mathbb{Z}$ or to an order in an imaginary quadratic field.*

Definition 3.1.9. *An elliptic curve defined over a field of characteristic 0 whose endomorphism ring is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field K is said to have complex multiplication (CM) by $\mathcal{O}$.*

Example 3.1.10. *Let E have complex multiplication by an order $\mathcal{O}$ in a number field K. Then the curve E is not necessarily defined over the field K. Indeed, consider for example*

$$E : y^2 = x^3 - x.$$

The field of definition is $k = \mathbb{Q}$*, but* $K = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q} = \mathbb{Q}(i)$*. In fact,* $\mathrm{End}(E) \cong \mathbb{Z}[i]$ *with*

$$[i] \colon (x, y) \to (-x, iy) \tag{3.5}$$

We see that this is well-defined as a map from E *to itself because* $(iy)^2 = (-x)^3 - (-x)$*.*

3.1.2 Analytic Theory

We now turn our attention to the case of elliptic curves defined specifically over the field $\mathbb{C}$. We develop in this case a correspondence between isomorphism classes of elliptic curves defined over $\mathbb{C}$, and homothety classes of lattices $\Lambda \subset \mathbb{C}$. This correspondence will be crucial to the computations of Chapter 5.

Definition 3.1.11. *A lattice* Λ *(of rank* 2*) is a discrete subgroup of* $\mathbb{C}$ *that contains an* $\mathbb{R}$*-basis for* $\mathbb{C}$*, i.e.,* $\Lambda = \{n_1\omega_1 + n_2\omega_2 \colon n_1, n_2 \in \mathbb{Z}\}$*, where* ω_1 *and* ω_2 *are complex numbers that are linearly independent over* $\mathbb{R}$*.*

To give the correspondence, we first need some functions.

Definition 3.1.12. *Let* $\Lambda \subseteq \mathbb{C}$ *be a lattice and let* $z \in \mathbb{C}$*. The Weierstrass* $\wp$*-function (relative to* Λ*) is defined by the series*

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{0 \neq \omega \in \Lambda} \left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right). \tag{3.6}$$

Definition 3.1.13. *Let $\Lambda \subseteq \mathbb{C}$ be a lattice and let $z \in \mathbb{C}$. Define g_2 and g_3 as follows:*

$$g_2 = g_2(\Lambda) = 60 \sum_{0 \neq \omega \in \Lambda} \omega^{-4}, \tag{3.7}$$

$$g_3 = g_3(\Lambda) = 140 \sum_{0 \neq \omega \in \Lambda} \omega^{-6} \tag{3.8}$$

We can now give the correspondence.

Theorem 3.1.14. *Let $g_2 = g_2(\Lambda)$ and $g_3 = g_3(\Lambda)$ be the quantities associated to a lattice $\Lambda \subseteq \mathbb{C}$.*

1. *Then the polynomial*

$$f_\Lambda(x) = 4x^3 - g_2 x - g_3 \tag{3.9}$$

has distinct roots, so its discriminant

$$\Delta(\Lambda) = g_2^3 - 27 g_3^2 \tag{3.10}$$

is nonzero.

2. *Let $E/\mathbb{C}$ be the curve*

$$E \colon y^2 = 4x^2 - g_2 x - g_3, \tag{3.11}$$

which from (1) is an elliptic curve. Then the map

$$\varphi \colon \mathbb{C}/\Lambda \to E(\mathbb{C}) \subset \mathbb{P}^2(\mathbb{C}), \quad z \mapsto [\wp(z), \wp'(z), 1], \tag{3.12}$$

is an isomorphism of Riemann surfaces that is also a group homomorphism.

Conversely, let $E/\mathbb{C}$ be an elliptic curve. There exists a lattice $\Lambda \in \mathbb{C}$, unique up to

homothety, and a complex analytic isomorphism

$$\varphi\colon \mathbb{C}/\Lambda \to E \cong E(\mathbb{C}), \quad \varphi(z) = [\wp(z,\Lambda), \wp'(z,\Lambda), 1]. \tag{3.13}$$

Remark 3.1.15. *Theorem 3.1.14 contains Proposition VI.3.6 from Silverman [14], and his typos have been corrected here.*

As a consequence, every elliptic curve corresponds to a lattice of the form

$$\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}. \tag{3.14}$$

We now show that isogenies can also be given in terms of the lattice:

Theorem 3.1.16. *Let E_1 and E_2 be elliptic curves corresponding to the lattices Λ_1 and Λ_2, respectively. Then we have a bijection of sets*

$$\{\varphi\colon E_1 \to E_2 \ \mid \varphi \text{ an isogeny}\} \leftrightarrow \{\alpha \in \mathbb{C}^\times : \alpha\Lambda_1 \subseteq \Lambda_2\}. \tag{3.15}$$

Corollary 3.1.17. *Let $E_1/\mathbb{C}$ and $E_2/\mathbb{C}$ be elliptic curves corresponding under Theorem 3.1.14 to lattices Λ_1 and Λ_2, respectively. Then E_1 and E_2 are isomorphic over $\mathbb{C}$ if and only if Λ_1 and Λ_2 are homothetic, i.e., there exists some $\alpha \in \mathbb{C}^\times$ such that $\Lambda_1 = \alpha\Lambda_2$.*

We now show the connection between the lattice and the endomorphism ring.

Theorem 3.1.18. *Let $E/\mathbb{C}$ be an elliptic curve, and let ω_1 and ω_2 be generators for the lattice Λ associated to E by Theorem 3.1.14. Then one of the following is true:*

1. $\mathrm{End}(E) = \mathbb{Z}$.

2. *The field* $\mathbb{Q}(\omega_1/\omega_2)$ *is an imaginary quadratic extension of* $\mathbb{Q}$*, and* $\mathrm{End}(E)$ *is isomorphic to an order in* $\mathbb{Q}(\omega_1/\omega_2)$*.*

For the purposes of Chapter 5, we will need to identify an elliptic curve $E/\mathbb{C}$ to an element $\tau \in \mathbb{H}$, where $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

Proposition 3.1.19. *(a) Let* $\Lambda \subset \mathbb{C}$ *be a lattice, and let* ω_1, ω_2 *and* ω_1', ω_2' *be two bases for* Λ *such that* $\mathrm{Im}(\omega_1/\omega_2) > 0$ *and* $\mathrm{Im}(\omega_1'/\omega_2') > 0$*. Then*

$$\omega_1' = a\omega_1 + b\omega_2$$

$$\omega_2' = c\omega_1 + d\omega_2$$

for some matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{3.16}$$

such that $a, b, c, d \in \mathbb{Z}$ *and* $ad - bc = 1$*. We say such a matrix belongs to the group* $\mathrm{SL}_2(\mathbb{Z})$*.*

(b) Let $\tau_1, \tau_2 \in \mathbb{H}$*, the complex upper half-plane. Then* $\Lambda_{\tau_1} = \mathbb{Z}\tau_1 + \mathbb{Z}$ *is homothetic to* $\Lambda_{\tau_2} = \mathbb{Z}\tau_2 + \mathbb{Z}$ *if and only if there is a matrix*

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

such that

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}.$$

(c) Let $\Lambda \subset \mathbb{C}$ be a lattice. Then there is $\tau \in \mathbb{H}$ such that Λ is homothetic to $\Lambda_\tau = \mathbb{Z}\tau + \mathbb{Z}$.

We now use the Propositions and Theorems above to show how to attach $\tau \in \mathbb{H}$ to $E/\mathbb{C}$. By Theorem 3.1.14, every elliptic curve over $\mathbb{C}$ corresponds to a lattice $\Lambda = \omega_1\mathbb{Z} + \omega_2\mathbb{Z}$. Then, by Proposition 3.1.19 part (c), there is a $\tau \in \mathbb{H}$ such that Λ is homothetic to Λ_τ. By Corollary 3.1.17, if the lattices are homothetic, the elliptic curves are isomorphic. In fact, in practice we can choose τ to be ω_1/ω_2 or ω_2/ω_1, whichever is in $\mathbb{H}$.

Therefore each isomorphism class of elliptic curves can be associated to some values $\tau \in \mathbb{H}$. In fact, by Theorem 3.1.19, E_{τ_1} is isomorphic to E_{τ_2} if and only if

$$\Lambda_{\tau_1} = \mathbb{Z} + \tau_1\mathbb{Z}, \quad \Lambda_{\tau_2} = \mathbb{Z} + \tau_2\mathbb{Z}, \tag{3.17}$$

where E_{τ_i} is the elliptic curve that arises from τ_i, and there exists a matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \tag{3.18}$$

such that

$$\tau_2 = \frac{a\tau_1 + b}{c\tau_1 + d}. \tag{3.19}$$

3.2 General case

Until now we have only considered the case of elliptic curves, which are abelian varieties of dimension 1. We now turn our attention to higher dimensional abelian

varieties. The information given below is widely known and can be found in Milne [9] and Birkenhake and Lange [1].

3.2.1 Preliminaries

Definition 3.2.1. *An abelian variety defined over a field k is a smooth connected projective variety equipped with the structure of an algebraic group. The group law is automatically commutative.*

Example 3.2.2. *An elliptic curve is an abelian variety of dimension 1.*

In this work we will focus our attention on so-called simple abelian varieties with CM (see the Main Theorem of CM (Theorem 4.3.9) for justification).

Definition 3.2.3. *Let A_1 and A_2 be abelian varieties. An isogeny from A_1 to A_2 is a morphism*

$$\varphi\colon A_1 \to A_2 \quad \text{satisfying} \quad \varphi(O_{A_1}) = O_{A_2}. \tag{3.20}$$

Two abelian varieties A_1 and A_2 are isogenous if there is an isogeny from A_1 to A_2 with finite kernel.

Since abelian varieties are abelian groups, as for elliptic curves their endomorphism set has the structure of a ring.

Definition 3.2.4. *We write* $\mathrm{End}(A) = \mathrm{Hom}(A, A)$*, and the ring* $\mathrm{End}(A)$ *is called the endomorphism ring of A. The set* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$*, the ring of endomorphisms tensored up to $\mathbb{Q}$ over $\mathbb{Z}$, is called the endomorphism algebra of A.*

Definition 3.2.5. *An abelian variety A is said to be simple if there does not exist an abelian variety $B \subset A$, with $0 \neq B \neq A$.*

Definition 3.2.6. *A simple abelian variety of dimension g is said to have complex multiplication if its endomorphism ring is isomorphic to an order in the ring of integers of a CM field of degree $2g$.*

Proposition 3.2.7. *If A is a simple abelian variety of dimension 3 defined over a field of characteristic 0, then*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}, \tag{3.21}$$

the endomorphism algebra, is isomorphic to either

1. $\mathbb{Q}$,
2. K_0, *a totally real field of degree 3 over* $\mathbb{Q}$,
3. F, *an imaginary quadratic field, or*
4. K, *a sextic CM field.*

In this work we focus on the case where $\mathrm{End}(A) \cong \mathcal{O}_K$ for K a sextic CM field, in which case $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \cong K$. We will say that A has CM by $\mathcal{O}_K$.

3.2.2 Analytic theory

As we saw in Section 3.1.2, an elliptic curve $E/\mathbb{C}$ and a lattic Λ of rank 1 have special properties that tie them together. We have a similar relationship between a lattice of higher rank and an abelian variety of dimension 2 or higher.

Definition 3.2.8. *A lattice Λ of rank $2g$ is a discrete subgroup of $\mathbb{C}^g$ that contains an $\mathbb{R}$-basis for $\mathbb{C}^g$.*

Example 3.2.9. *When $g = 3$, this means that $\Lambda = \{n_1\omega_1 + \ldots + n_6\omega_6 \colon n_i \in \mathbb{Z}\}$ where the ω_i's are linearly independent over $\mathbb{R}$ and each $\omega_i \in \mathbb{C}^3$.*

Definition 3.2.10. *Given Λ a lattice of rank $2g$, the quotient space $\mathbb{C}^g/\Lambda$ is called a complex torus of dimension g.*

Contrary to the case of $g = 1$, not every complex torus gives rise to an abelian variety. For that to be the case, the torus must be polarizable.

Definition 3.2.11. *A complex torus $\mathbb{C}^g/\Lambda$ is polarizable if there exists a skew-symmetric form*

$$E \colon \Lambda \times \Lambda \to \mathbb{Z} \tag{3.22}$$

such that its extension

$$E_{\mathbb{R}} \colon \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \times \Lambda \otimes_{\mathbb{Z}} \mathbb{R} \to \mathbb{R} \tag{3.23}$$

is such that

1. *$E_{\mathbb{R}}(iv, iw) = E_{\mathbb{R}}(v, w)$*
2. *the associated Hermitian form $H(v, w) = E(iv, w) + iE(v, w)$ is positive definite, i.e., all of its eigenvalues are positive.*

The form E is called a Riemann form.

We will further say

Theorem 3.2.12. *Every abelian variety $A/\mathbb{C}$ has $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ for some Λ.*

Definition 3.2.13. *A complex torus is principally polarizable if there exists a basis*

of Λ such that the Riemann form E from Definition 3.2.11 is given by the matrix

$$\begin{pmatrix} 0 & id_g \\ -id_g & 0 \end{pmatrix}, \tag{3.24}$$

where id_g is the $g \times g$ identity matrix.

In this work, principally polarizable abelian varieties will play the role of elliptic curves. Accordingly, we wish to give an analyic space similar to $\mathbb{H}$ for elliptic curves. We focus on the case of $g = 3$. Let $\dim A = 3$ and $A(\mathbb{C}) \cong \mathbb{C}^3/\Lambda$, where $\Lambda = \{n_1\omega_1 + \ldots + n_6\omega_6 \colon n_i \in \mathbb{Z}\}$.

Let Ω_1 be the 3×3 matrix with columns ω_1, ω_2, and ω_3, and let Ω_2 be the 3×3 matrix with columns ω_4, ω_5, and ω_6 where each ω_i is a column vector with three entries. Then $\tau = \Omega_1^{-1}\Omega_2$ has the property that $\mathrm{Im}(\tau)$, the matrix where we take the imaginary part of each entry, has only positive eigenvalues. Furthermore, this τ will be a symmetric matrix.

We define the space of all such matrices:

Definition 3.2.14. *$\mathbb{H}_g$, the Siegel upper half-space is the set*

$$\mathbb{H}_g = \{M \in M_{g\times g}(\mathbb{C}) \colon \mathrm{Im}(M) \text{ is positive definite and } M \text{ is symmetric}\}. \tag{3.25}$$

By the procedure we just outlined, each principally polarizable complex torus corresponds to $\tau \in \mathbb{H}_g$.

Conversely, for every $\tau \in \mathbb{H}_g$ we can construct a principally polarizable abelian variety in the following way:

Let $\tau \in M_{g\times g}(\mathbb{C})$ and let $\omega_i \in \mathbb{C}^g$ be the columns of τ for $i = 1, 2, \ldots, g$. Now let

$$\omega_{g+1} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \omega_{g+2} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \cdots, \omega_{2g} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}, \tag{3.26}$$

i.e., $\omega_{g+i} = e_i$ where $\{e_i\}$ is the standard basis of $\mathbb{C}^g$. Then $\{\omega_1, \ldots, \omega_{2g}\}$ generates a lattice Λ of rank $2g$ and $\mathbb{C}^g/\Lambda$ is a principally polarizable abelian variety.

We now investigate when two abelian varieties corresponding to τ_1 and $\tau_2 \in \mathbb{H}_g$ are isomorphic.

Definition 3.2.15. *Let* $\mathrm{Sp}_{2g}(\mathbb{Z})$ *be the group containing the matrices* M *such that*

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{3.27}$$

with $A, B, C, D \in M_{g\times g}(\mathbb{Z})$*, and*

$$M^T \begin{pmatrix} 0 & id_g \\ -id_g & 0 \end{pmatrix} M = \begin{pmatrix} 0 & id_g \\ -id_g & 0 \end{pmatrix}, \tag{3.28}$$

where again id_g *is the* $g \times g$ *identity matrix, and* M^T *is the transpose of* M*.*

Example 3.2.16. *Note that* $\mathrm{Sp}_2(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})$*. Indeed let*

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_2(\mathbb{Z}). \tag{3.29}$$

Then,

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} -c & a \\ -d & b \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 0 & ad-bc \\ -ad+bc & 0 \end{pmatrix}. \tag{3.30}$$

So $ad - bc = 1$*, by definition. Therefore,* $M \in \mathrm{SL}_2(\mathbb{Z})$*. By the same argument, we see that if* $M \in \mathrm{SL}_2(\mathbb{Z})$*, then we also get that* $M \in \mathrm{Sp}_2(\mathbb{Z})$*.*

The significance of the group $Sp_{2g}(\mathbb{Z})$ is the following: two elements τ_1 and $\tau_2 \in \mathbb{H}_g$ give isomorphic principally polarizable abelian varieties if and only if there exists an $M \in \mathrm{Sp}_{2g}(\mathbb{Z})$ with

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \tag{3.31}$$

and

$$\tau_2 = (C\tau_1 + D)^{-1}(A\tau_1 + B). \tag{3.32}$$

As a consequence, we have

Theorem 3.2.17. *There is a one-to-one correspondence between* $\mathbb{H}_g/\mathrm{Sp}_{2g}(\mathbb{Z})$ *and isomorphism classes of principally polarizable abelian varieties.*

Chapter 4

Complex Multiplication

In this Chapter we tackle two tasks. We first outline the process for finding the Hilbert class polynomial f_K of an imaginary quadratic field K. We then introduce the theory of complex multipication that we need to define the so-called reflex field and reflex type which we compute in Chapter 6. Finally, to explain the significance of the reflex field and reflex type, we give the Main Theorem of Complex Multiplication, and end with a short account of the algorithm that can be used to apply this theorem.

4.1 Elliptic curves

By Theorem 3.1.18, if we want an elliptic curve E with $\mathrm{End}(E)$ an order in an imaginary quadratic field K, then we should take

$$\Lambda_\tau = \mathbb{Z} + \tau\mathbb{Z}, \quad \tau \in K. \tag{4.1}$$

Furthermore, if we would like for $\mathrm{End}(E) = \mathcal{O}_K$ we need that for all $\alpha \in \mathcal{O}_K$, α gives an endomorphism of E, i.e.,

$$\alpha\Lambda_\tau \subseteq \Lambda_\tau. \tag{4.2}$$

By Definition 2.2.15, Λ_τ is therefore a fractional ideal of K. Conversely, every fractional ideal of K gives an elliptic curve with CM by $\mathcal{O}_K$.

We now investigate when two such elliptic curves are isomorphic. By Corollary 3.1.17, E_1 corresponding to Λ_1 and E_2 corresponding to Λ_2 are isomorphic if and only if there is an $\alpha \in \mathbb{C}^\times$ such that $\Lambda_1 = \alpha\Lambda_2$. This corresponds exactly to the statement that Λ_1 and Λ_2 differ by multiplication by the principal ideal (α), since α may be taken to belong to K (see [13] Chapter II). By Definition 2.2.17, it follows that Λ_1 and Λ_2 are equal in $\mathrm{Cl}(K)$, the ideal class group of K.

Proposition 4.1.1. *There is a one-to-one correspondence between the isomorphism classes of elliptic curves with* $\mathrm{End}(E) \cong \mathcal{O}_K$ *and elements of the ideal class group of* K.

We now give the connection between elliptic curves with CM by $\mathcal{O}_K$, for K an imaginary quadratic field, and the Hilbert class field of K.

Theorem 4.1.2 (Theorem II.4.3 from Silverman [13])**.** *Let E be an elliptic curve representing an isomorphism class in $\mathcal{ELL}(\mathcal{O}_K)$, where $\mathcal{ELL}(\mathcal{O}_K)$ is the set of isomorphism classes of elliptic curves over $\mathbb{C}$ that have CM by $\mathcal{O}_K$.*

1. *$K(j(E))$ is the Hilbert class field H_K of K.*
2. *$[\mathbb{Q}(j(E)) : \mathbb{Q}] = [K(j(E)) : K] = h_K$, where $h_K = \#\mathrm{Cl}(K)$ is the class number of K.*

3. *Let* $E_1, \ldots, E_{h_K}$ *be a complete set of representatives for* $\mathcal{ELL}(R_K)$. *Then* $j(E_1)$, $\ldots$, $j(E_{h_K})$ *is a complete set of* $\mathrm{Gal}(\overline{K}/K)$ *conjugates for* $j(E)$.

Theorem 4.1.3 (Theorem II.6.1 from Silverman [13])**.** *Let* $E/\mathbb{C}$ *be an elliptic curve with complex multiplication. Then* $j(E)$ *is an algebraic integer.*

4.2 Generating $f_K(x)$

In this section we give a procedure to, given an imaginary quadratic field K, computationally generate $f_K(x)$, a monic polynomial with integer coefficients such that $K[x]/(f_K(x))$ is the Hilbert class field of K:

First, generate a representative for each ideal class of K: $I_1, I_2, \ldots, I_{h_k}$. For each ideal, we will first compute a basis $a_{i,1}, a_{i,2}$ for $i = 1, 2, \ldots, h_k$, then fix an embedding $\varphi\colon K \hookrightarrow \mathbb{C}$, and form the complex numbers

$$\omega_{i,1} = \varphi(a_{i,1}) \tag{4.3}$$

$$\omega_{i,2} = \varphi(a_{i,2}). \tag{4.4}$$

Then $\Lambda_i = \mathbb{Z}\omega_{i,1} + \mathbb{Z}\omega_{i,2}$ is a lattice in $\mathbb{C}$ such that an elliptic curve E_i corresponding to Λ_i has $\mathrm{End}(E_i) \cong \mathcal{O}_K$. Next we compute $\tau_i = \omega_{i,1}/\omega_{i,2}$ or $\omega_{i,2}/\omega_{i,1}$, whichever has positive imaginary part, and compute $j(\tau_i)$, the j-invariant of E_i, to some fixed suitable precision. Once this is done for each ideal class, we can form the polynomial

$$\tilde{f_K}(x) = \prod_{i=1}^{h_k} (x - j(\tau_i)). \tag{4.5}$$

This polynomial is an approximation of a polynomial that is known to have integer

coefficients. If the j-invariants in the product are computed to high enough precision, we can round the coefficients of $\tilde{f_K}$ to obtain $f_K(x) \in \mathbb{Z}[x]$.

4.3 CM-types

The main work of this thesis is to compute the reflex field and reflex type of a pair (K, Φ), where K is a sextic CM field with a given Galois group, and Φ is a so-called CM-type of K. In this Section we introduce all of the notions we will need for our computation. In addition, this Section ends with the Main Theorem of Complex Multiplication (Theorem 4.3.9), which explains the significance of the reflex field and type of a pair (K, Φ).

Definition 4.3.1. *Let K be a CM field with $[K : \mathbb{Q}] = 2g$. A CM-type Φ of K is an unordered tuple of g complex embeddings of K, no two of which are complex conjugates.*

Example 4.3.2. *Let K be a sextic CM field. Then there are six embeddings of K into $\mathbb{C}$. To create a CM-type, we choose three embeddings, no two of which are complex conjugates. Denoting the complex embeddings of K by φ_1, φ_2, φ_3, $\overline{\varphi_1}$, $\overline{\varphi_2}$, and $\overline{\varphi_3}$, we*

have the following CM-types:

$$\Phi_1 = \{\varphi_1, \varphi_2, \varphi_3\}$$

$$\Phi_2 = \{\varphi_1, \varphi_2, \overline{\varphi_3}\}$$

$$\Phi_3 = \{\varphi_1, \overline{\varphi_2}, \varphi_3\}$$

$$\Phi_4 = \{\varphi_1, \overline{\varphi_2}, \overline{\varphi_3}\}$$

$$\overline{\Phi_1} = \{\overline{\varphi_1}, \overline{\varphi_2}, \overline{\varphi_3}\}$$

$$\overline{\Phi_2} = \{\overline{\varphi_1}, \overline{\varphi_2}, \varphi_3\}$$

$$\overline{\Phi_3} = \{\overline{\varphi_1}, \varphi_2, \overline{\varphi_3}\}$$

$$\overline{\Phi_4} = \{\overline{\varphi_1}, \varphi_2, \varphi_3\}.$$

Definition 4.3.3. *The CM-types Φ and Φ' are equivalent if there exists an automorphism τ of K such that $\Phi' = \Phi \circ \tau$.*

Example 4.3.4. *If complex conjugation is the only automorphism, then*

$$\{\varphi_1, \varphi_2, \varphi_3\} \sim \{\overline{\varphi_1}, \overline{\varphi_2}, \overline{\varphi_3}\}. \tag{4.6}$$

In that case there are 2^{g-1} equivalence classes of CM-types.

Let K be a CM field of degree $2g$ over $\mathbb{Q}$ and let $L/\mathbb{Q}$ be a field that contains a Galois closure of K over $\mathbb{Q}$.

Definition 4.3.5. *[15] Let K_2/K_1 be an extension of CM fields and let Φ be a CM-type of K_1. The CM-type of K_2 induced by Φ is*

$$\Phi^{K_2} = \{\varphi \colon K_2 \to \mathbb{C} \mid \varphi|_{K_1} \in \Phi\}.$$

We say that a CM-type is primitive if it is not induced from a CM-type of a strict CM subfield.

Proposition 4.3.6. *[15] Let K be a CM field with Galois closure L, let Φ be a CM-type of K, and let Φ^L be the CM-type of L induced by Φ. By fixing an embedding of L into $\mathbb{C}$, one may consider the elements of Φ^L as automorphisms of L, since L is a Galois field. Let $(\Phi^L)^{-1}$ be the set of their inverses, which is also a set of automorphisms of L. Again using the fixed embedding of L into $\mathbb{C}$, we may consider elements of $(\Phi^L)^{-1}$ as complex embeddings of L, and $(\Phi^L)^{-1}$ is a CM-type of L. Then there is a unique primitive pair (K^R, Φ^R), where K^R is a subfield of L, that induces $(L, (\Phi^L)^{-1})$.*

Definition 4.3.7. *The pair (K^R, Φ^R) is called the reflex of (K, Φ), the field K^R is called the reflex field of (K, Φ), and the CM-type Φ^R is called the reflex type of (K, Φ).*

Lemma 4.3.8. *[15] The CM-type Φ^R is a primitive CM-type of K^R. If we denote the reflex of (K^R, Φ^R) by (K^{RR}, Φ^{RR}), then K^{RR} is a subfield of K and Φ is induced by Φ^{RR}. If Φ is primitive, then we have $K^{RR} = K$ and $\Phi^{RR} = \Phi$.*

Now we give the main theorem of complex multiplication.

Theorem 4.3.9. *[12] Let (K^R, Φ^R) be a primitive CM-type and (K, Φ) the reflex of (K^R, Φ^R). Let H_0 be the group of all ideals $\mathfrak{a}$ of K^R such that there exists an element $\mu \in K$ for which we have*

$$g(\mathfrak{a}) = (\mu), \quad N(\mathfrak{a}) = \mu\overline{\mu},$$

where g is defined by

$$\mathcal{O}_L g(\mathfrak{a}) = \mathcal{O}_L \prod_{\alpha} \mathfrak{a}^{\psi_\alpha}$$

and $\overline{\mu}$ denotes the complex conjugate of μ. Let $(A, \mathcal{C})$ be such that A is an abelian variety of type (K, Φ) and $\mathcal{C}$ is a polarization of A. Let k_0 be the field of moduli $(A, \mathcal{C})$. Then H_0 is an ideal group of K^R defined modulo $\mathcal{O}_L g(\mathfrak{a})$; and the composite k_0^R of the fields k_0 and K^R is the unramified class field over K^R corresponding to the ideal-group H_0.

The significance of this theorem is the following: If one can construct a polarized abelian variety of type (K, Φ), then its field of moduli will generate an unramified abelian extension of the reflex field K^R of the pair (K, Φ). In general, this unramified abelian extension will not be maximal if the dimension of the abelian variety is greater than 1. Furthermore, the theorem gives the Galois group of the unramified abelian extension (it is the group H_0). This gives a sense of how far this unramified abelain extension is from being maximal, as the maximal unramified abelian extension will have Galois group $\mathrm{Cl}(K)$, the ideal class group of K.

4.4 Construction of dimension 3 abelian varieties

We now turn our attention to the construction of an abelian variety A of dimension 3 such that $\mathrm{End}(A) \cong \mathcal{O}_K$, where K is a sextic CM field. As we have seen, when equipped with a polarization, the field of moduli of such an abelian variety will give an unramified extension of a certain field associated to K.

To do so we begin with I, a fractional ideal of K, as defined in Definiton 2.2.15, and compute a $\mathbb{Z}$ basis a_1, a_2, a_3, a_4, a_5, a_6 of I. We then fix a CM-type $\Phi = \{\varphi_1, \varphi_2, \varphi_3\}$

of K and compute:

$$\omega_i = \begin{pmatrix} \varphi_1(a_i) \\ \varphi_2(a_i) \\ \varphi_3(a_i) \end{pmatrix} \in \mathbb{C}^3, \tag{4.7}$$

for $i = 1, 2, \ldots 6$. Armed with these elements, we may form the matrix Ω_1 whose columns are the vectors ω_1, ω_2 and ω_3 and the matrix Ω_2 whose columns are the vectors ω_4, ω_5 and ω_6. Then it is a theorem that $\Omega_1^{-1}\Omega_2$ belongs to the Siegel upper half-space $\mathbb{H}_3$. Therefore this matrix corresponds to a polarizable abelian variety.

To see if the abelian variety we have constructed is principally polarizable, we first check if

$$(I\overline{I}\delta_{K/\mathbb{Q}})^{-1} \tag{4.8}$$

is a principal ideal, where $\delta_{K/\mathbb{Q}}$ is the different of K. If so, we then determine if the ideal has a generator ξ such that

1. $\varphi_i(\xi)$ is imaginary for $\varphi_i \in \Phi$, and
2. $\mathrm{Im}(\varphi_i(\xi)) > 0$ for $\varphi_i \in \Phi$.

If this is the case, then

$$E_\xi(x, y) = \sum_{i=1}^{3} \varphi_i(\xi)(\overline{x}_i y_i - x_i \overline{y}_i) \tag{4.9}$$

is a Riemann form giving a principally polarizable abelian variety on $\mathbb{C}^3/\Phi(I)$ and this abelian variety has endomorphism ring $\mathcal{O}_K$.

Chapter 5

Elliptic curves and Sage

As an application of the algorithm given in Section 4.2 and implemented in the Appendix, we find the minimal polynomial for three number fields.

5.1 Computing the j-invariant

We previously defined the j-invariant of an elliptic curve in Definition 3.1.2. Here we introduce a new expression for the j-invariant which is based on the theta function given in Definition 5.1.1. This new expression is the one we use in the algorithm given in the Appendix.

Definition 5.1.1. *Let $a, b \in \frac{1}{2}\mathbb{Z}$. Then the theta function with characteristic (a, b) is the function given by the formula*

$$\theta(a, b, \tau) = \sum_{n \in \mathbb{Z}} \exp(\pi i \tau (n + a)^2 + 2\pi i (n + a) b)$$

where $\tau \in \mathbb{H}$, the upper half-plane.

Theorem 5.1.2. *The j-invariant of an elliptic curve E defined over a field K is given by the formula:*

$$j(\tau) = 32\frac{(\theta(\frac{1}{2},0,\tau)^8 + \theta(0,0,\tau)^8 + \theta(0,\frac{1}{2},\tau)^8)^3}{(\theta(\frac{1}{2},0,\tau)\theta(0,0,\tau)\theta(0,\frac{1}{2},\tau))^8},$$

where $\tau \in \mathbb{H}$ is an element identified with an elliptic curve $E/\mathbb{C}$.

5.2 Examples

In Section 4.2 we gave an algorithm for computing the Hilbert class field of a number field K. This algorithm was implemented in Sage and is given in the Appendix. Here we present the results we obtained for three imaginary quadratic fields.

Example 5.2.1. *Consider the case of $K = \mathbb{Q}[x]/(x^2 + 67)$. Here, $h_K = 1$, so $H_K = K$. We find our τ value to be*

$$\tau = \frac{-1}{34}\alpha - \frac{1}{34},$$

where α is a root of the defining polynomial of K. Then the j-invariant is approximately

$$\begin{aligned} &-1.4719795200000000000000000000000000000000000000000000000001 \times 10^{11} \\ &-6.1473588332120499861232338744484083212749528242416120053125 \times 10^{-48}i \end{aligned} \tag{5.1}$$

which, since we know it is an integer, must be the integer -147197952000. We note that since this j-invariant is an integer, indeed $H_K = K(j) = K$.

Example 5.2.2. *We now consider the case where* $K = \mathbb{Q}[x]/(x^2 + 23)$. *This time* $h_K = 3$, *so* $[H_K : K] = 3$. *We find that our* τ *values are:*

$$\tau_1 = \frac{-1}{6}\alpha + \frac{1}{6},$$
$$\tau_2 = \frac{-1}{6}\alpha - \frac{1}{6},$$
$$\tau_3 = \frac{-1}{12}\alpha - \frac{1}{12},$$

where α *is a root of the defining polynomial of* K. *Then the* j*-invariants are approximately:*

$$j_1 = -3.4932256999699333682055047385473297033961841797256116567546 \times 10^6$$
$$- 1.044048714879763924273647057481047608912186281291034647641 4 \times 10^{-53} i$$

$$j_2 = 737.84998496668410275236927366485169809208986280582837732196$$
$$- 1764.01893861274614164378642718096511601480642288450549887 13i$$

$$j_3 = 737.84998496668410275236927366485169809208986280582837732196$$
$$+ 1764.01893861274614164378642718096511601480642288450549887 13i$$

and the approximate polynomial $\tilde{f_K}(x)$, which is given by $(x-j_1)(x-j_2)(x-j_3)$, is:

$$x^3 + (3.491750000000000000000000000000000000000000000000000000000000 \times 10^6$$
$$+ 1.045068293702888693730945540935618944467764588206357923664 5 \times 10^{-53}i)x^2$$
$$- (5.151296875000000000000000000000000000000000000000000000000000 \times 10^9$$
$$- 2.672764710092195646140536467151481878815196880105048697961 9 \times 10^{-50}i)x$$
$$+ 1.277188085937500000000000000000000000000000000000000000000000 \times 10^{13}$$
$$- 1.094764425253763336659163736945246977562704642091027946685 2 \times 10^{-47}i.$$

Since we know that the coefficients of $f_K(x)$ are integers, we can see that a defining polynomial for H_K over $\mathbb{Q}$ is

$$f_K(x) = x^3 + 3491750x^2 - 5151296875x + 12771880859375. \tag{5.2}$$

Example 5.2.3. *Finally, we consider the case where $K = \mathbb{Q}[x]/(x^2+71)$. In this case, $h_K = 7$, so $[H_K : K] = 7$. We find our τ values to be:*

$$\tau_1 = \frac{-1}{36}\alpha - \frac{1}{36}$$
$$\tau_2 = \frac{-1}{18}\alpha - \frac{1}{18}$$
$$\tau_3 = \frac{-1}{10}\alpha + \frac{3}{10}$$
$$\tau_4 = \frac{-1}{12}\alpha - \frac{1}{12}$$

$$\tau_5 = \frac{-1}{12}\alpha + \frac{1}{12}$$
$$\tau_6 = \frac{-1}{12}\alpha + \frac{5}{12}$$
$$\tau_7 = \frac{-1}{18}\alpha + \frac{1}{18}$$

where α is a root of the defining polynomial of K over $\mathbb{Q}$. Then our j-invariants are approximately:

$$j_1 = -3.136458195742222701273140878636976013771003907116119205083 8 \times 10^{11}$$
$$- 4.190895065424562773148361180493523585982228708004716358404 3 \times 10^{-48} i$$

$$j_2 = 743.999931471237481683758606168583593443771635607891063257 35$$
$$- 560040.557951253536033890438591765761108144509563640906792 62 i$$

$$j_3 = 30.193974692298505402948948670453194673728189051084472057 093$$
$$+ 380.060172538012409230126097093617484410009243919257713260 62 i$$

$$j_4 = 4155.417228900121056845141245849513407238306135595223407273 1$$
$$- 5858.561905738502206662096744013906789500258407194017934831 1 i$$

$$j_5 = 4155.417228900121056845141245849513407238306135595223407273 2$$
$$+ 5858.561905738502206662096744013906789500258407194017934831 1i$$

$$j_6 = 30.193974692298505402948948670453194673728189051084472057101$$
$$- 380.060172538012409230126097093617484410009243919257713260 62i$$

$$j_7 = 743.999931471237481683758606168583593443771635607891063263 31$$
$$+ 560040.557951253536033890438591765761108144509563640906792 60i.$$

We get the polynomial:

$$\tilde{f_K}(x) = x^7 + (3.13645809714999999999999999999999999999999999998 \times 10^{11}$$
$$+ 4.19087423064993060071099174138990550029369282642112263829 73 \times 10^{-48}i)x^6$$
$$- (3.09199013860456999999999999999999999999999999999999979 \times 10^{15}$$
$$- 6.35296175032459879316659353204274602067547754623991881573 21 \times 10^{-42}i)x^5$$
$$+ (9.83940388100478120493019999999999999999999999999999994 \times 10^{22}$$
$$- 2.41882212992389874318870120228153630183791922006918345781 77 \times 10^{-36}i)x^4$$
$$- (8.23534263439730779968091388999999999999999999999999995 \times 10^{26}$$
$$- 2.37611606888775223370781278666415407924638290848573518587 73 \times 10^{-32}i)x^3$$
$$+ (5.13880036645397678032372632944599999999999999999999999998 \times 10^{30}$$
$$- 1.91495984742400615763697109222396357253170862122715334407 99 \times 10^{-28}i)x^2$$
$$- (4.25319473946139603274605151187658999999999999999999999993 \times 10^{32}$$
$$- 1.61558713389263217748322010169914619837072677910327911376 95 \times 10^{-26}i)x$$
$$+ 7.37707086760731113357714241006081262999999999999999999999998 \times 10^{35}$$
$$- 1.09601431163276166920461651699270078097470104694366455078 12 \times 10^{-23}i$$

and again, since we know that the coefficients of $f_K(x)$ are integers, we have that a

defining polynomial for H_K over $\mathbb{Q}$ is

$$f_K(x) = x^7 + 313645809715x^6 - 3091990138604570x^5 + 98394038810047812049302x^4$$
$$- 82353426343973077996809138 9x^3 + 513880036645397678032372632944 6x^2$$
$$- 42531947394613960327460515118765 9x$$
$$+ 737707086760731113357714241006081263.$$

Chapter 6

Reflex fields

In this Chapter, we assume throughout that K is a sextic CM field with Galois closure L over $\mathbb{Q}$ such that $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$. Here D_{12} is the dihedral group of order 12 such that $D_{12} = \langle r, s \rangle$ and $1 = r^6 = s^2$. In this situation, we compute the reflex field and reflex type of each pair (K, Φ), as Φ ranges over the CM-types of K.

6.1 Galois group preliminaries

We begin by proving two propositions tying the structure of K as a subfield of L and as a CM field to the abstract structure of $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$.

Proposition 6.1.1. *Let K be a sextic CM field with Galois closure L such that $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$. Then the Galois group $\mathrm{Gal}(L/K)$ is generated by a reflection of D_{12}, which without loss of generality we may choose to be denoted s.*

Proof. Since K is not Galois, the subgroup $\mathrm{Gal}(L/\mathbb{Q})$ must be non-normal, and since $[L : K] = 2$, its generator must be of order 2. The size 2 subgroups of D_{12} are $\langle r^3 \rangle, \langle s \rangle, \langle rs \rangle, \langle r^2 s \rangle, \langle r^3 s \rangle, \langle r^4 s \rangle$, and $\langle r^5 s \rangle$. Of these subgroups, only $\langle r^3 \rangle$ is normal.

The other six subgroups are non-normal and are generated by the six reflections of D_{12}. Relabelling if necessary, we may choose for s to fix K. □

Proposition 6.1.2. *The complex conjugation automorphism, indicated by $\bar{\cdot}$, is r^3.*

Proof. By Lang's characterization of a CM field given in Proposition 2.1.12, complex conjugation must commute with any complex embedding of L, and therefore with any element of $\mathrm{Gal}(L/\mathbb{Q})$. Furthermore, complex conjugation is of order 2. As we saw before, the order 2 elements of D_{12} are r^3, s, rs, r^2s, r^3s, r^4s, and r^5s. For any element $r^is^j \in D_{12}$, we have

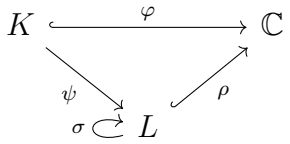
$$(r^is^j)r^3(r^is^j)^{-1} = r^is^jr^3s^{-j}r^{-i} = s^{-j}r^{-i}r^3r^is^j = s^{-j}r^3s^j = r^{-3}s^js^j = r^3.$$

Since $(r^js)r(r^js)^{-1} \neq r$, r^3 is the only element of order 2 that is in the center of D_{12} and must be the complex conjugation automorphism. □

6.2 Matching an embedding to a Galois element

We now turn our attention to the embeddings of K into $\mathbb{C}$. Since $[K\colon \mathbb{Q}] = 6$, there are 6 embeddings of K into $\mathbb{C}$. All of these embeddings are complex since K is a CM field. Let φ_1, φ_2, φ_3, $\overline{\varphi_1}$, $\overline{\varphi_2}$, and $\overline{\varphi_3}$ be the embeddings of K into $\mathbb{C}$.

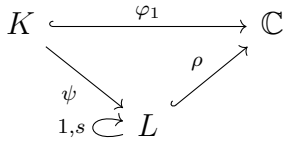
After choosing an arbitrary $\psi\colon K \hookrightarrow L$ and an arbitrary $\rho\colon L \hookrightarrow \mathbb{C}$, we can set up a bijection between the complex embeddings of K and the cosets of $\mathrm{Gal}(L/K)$ in $\mathrm{Gal}(L/\mathbb{Q})$. Indeed, for each $\varphi\colon K \hookrightarrow \mathbb{C}$ there are exactly two elements σ of $\mathrm{Gal}(L/\mathbb{Q})$ such that the diagram below commutes:

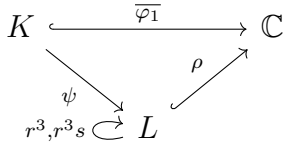


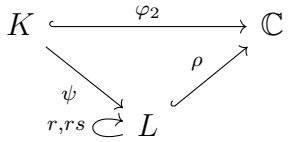
Also, since s fixes K by Proposition 6.1.1, it must be the case that if σ makes the diagram above commute, then so does $\sigma \circ s$.

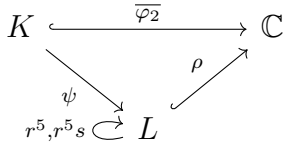
Without loss of generality, let $\varphi_1 \colon K \hookrightarrow \mathbb{C}$ be such that $\varphi = \rho \circ \psi$. Since s fixes K, it follows that $\varphi = \rho \circ s \circ \psi$ as well. Therefore, φ_1 corresponds to the coset $\{1, s\}$. Since r^3 is complex conjugation, $\overline{\varphi_1}$ must then correspond to $\{r^3, r^3 s\}$. Then without loss of generality, let φ_2 correspond to $\{r, rs\}$, since, if $\varphi_2 = \rho \circ r \circ \psi$, then $\varphi_2 = \rho \circ rs \circ \psi$ as well since s fixes K. Then $\overline{\varphi_2}$ will correspond to $\{r^4, r^4 s\}$. Finally, let φ_3 correspond to $\{r^2, r^2 s\}$, so $\overline{\varphi_3}$ corresponds to $\{r^5, r^5 s\}$.

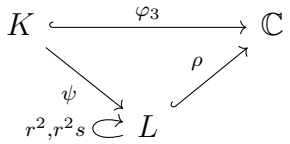
In conclusion, we have the following commutative diagrams:

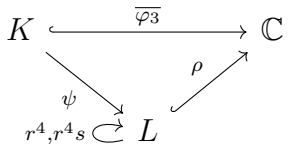












As a result, the correspondence between embeddings of K into $\mathbb{C}$ and cosets of $\mathrm{Gal}(L/K)$ is the following:

$$\varphi_1 \leftrightarrow \{1, s\} \tag{6.1}$$

$$\varphi_2 \leftrightarrow \{r, rs\} \tag{6.2}$$

$$\varphi_3 \leftrightarrow \{r^2, r^2s\} \tag{6.3}$$

$$\overline{\varphi_1} \leftrightarrow \{r^3, r^3s\} \tag{6.4}$$

$$\overline{\varphi_2} \leftrightarrow \{r^4, r^4s\} \tag{6.5}$$

$$\overline{\varphi_3} \leftrightarrow \{r^5, r^5s\}. \tag{6.6}$$

In what follows we will only need one Galois element corresponding to each embedding. In that case we will say that φ_1 corresponds to 1, φ_2 to r, φ_3 to r^2, $\overline{\varphi_1}$ to r^3, $\overline{\varphi_2}$ to r^4, and $\overline{\varphi_3}$ to r^5.

6.3 Equivalence classes of CM-types

We now turn our attention to the CM-types of K.

Proposition 6.3.1. *Let K be a sextic CM field with Galois closure L such that*

$\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$. *The identity automorphism and the complex conjugation automorphism are the only field automorphisms of* K.

Proof. Since K is a CM field, it has the identity automorphism (which is of order 1) and the complex conjugation automorphism (which is of order 2). Any automorphism of K fixes $\mathbb{Q}$ since $\mathbb{Q}$ is its prime field, and since $[K\colon \mathbb{Q}] = 6$, we know by Proposition 2.1.22 that

$$2 \leq |\mathrm{Aut}(K/\mathbb{Q})| \leq 6.$$

Since $\mathrm{Aut}(K/\mathbb{Q})$ is a group, we consider the possibilities. There are exactly seven groups of order between 2 and 6, inclusive: C_2, C_3, C_4, $C_2 \times C_2$, C_5, C_6, and S_3, where C_n is the cyclic group of order n and S_n is the symmetric group on n letters. $\mathrm{Aut}(K/\mathbb{Q})$ cannot be isomorphic to C_3 or C_5 because neither C_3 nor C_5 contains an element of order 2. $\mathrm{Aut}(K/\mathbb{Q})$ cannot be isomorphic to a group of order 6 because then $K/\mathbb{Q}$ would be Galois, but we know $K/\mathbb{Q}$ is not Galois. In the case where $\mathrm{Aut}(K/\mathbb{Q})$ has order 4, consider the field $F = K^{\mathrm{Aut}(K/\mathbb{Q})}$, the fixed field of the automorphism group of $K/\mathbb{Q}$. By Theorem 2.1.21, $[K\colon F] = 4$, but since $[K\colon F][F\colon \mathbb{Q}] = [K\colon \mathbb{Q}]$ we get a contradiction because $4 \nmid 6$. This leaves us with the group C_2, which contains only two elements, one of order 1 and the other of order 2. Thus, $\mathrm{Aut}(K/\mathbb{Q}) \cong C_2$, so the identity automorphism and the complex conjugation automorphism are the only automorphisms of $K/\mathbb{Q}$, and therefore of K. □

As an immediate corollary, we have

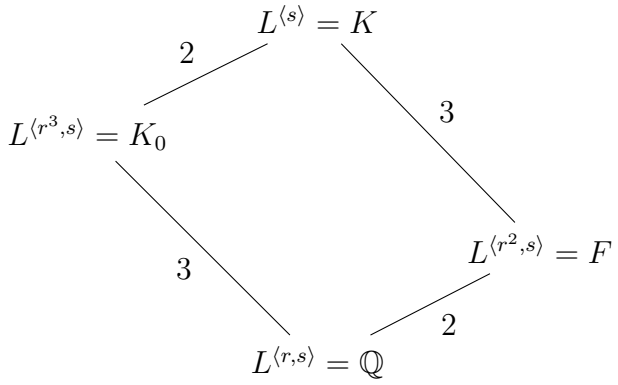
Corollary 6.3.2. *Let* K *be a sextic CM field with Galois closure* L *such that* $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$. *Let* φ_1, φ_2, φ_3, $\overline{\varphi_1}$, $\overline{\varphi}$, *and* $\overline{\varphi_3}$ *denote the six complex embeddings of* K. *Then repesentatives for each of the four equivalence classes of CM-types of* K

are $\Phi_1 = \{\varphi_1, \varphi_2, \varphi_3\}$, $\Phi_2 = \{\varphi_1, \overline{\varphi_2}, \varphi_3\}$, $\Phi_3 = \{\varphi_1, \varphi_2, \overline{\varphi_3}\}$, $\Phi_4 = \{\varphi_1, \overline{\varphi_2}, \overline{\varphi_3}\}$.

Proof. Since K has 3 pairs of complex conjugate embeddings, it has 8 CM-types in total (see Example 4.3.2). Because the only non-trivial automorphism of K is complex conjugation, each CM-type is equivalent to its complex conjugate and to no other. □

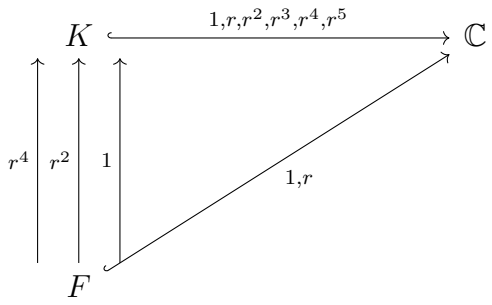
Proposition 6.3.3. *Let K be a sextic CM field with Galois closure L such that* $\mathrm{Gal}(L/\mathbb{Q}) \cong D_{12}$. *Then exactly three of the four equivalence classes of CM-types of K are primitive.*

Proof. Going back to the equivalence established in Section 2, we may write, by abuse of notation, our four CM-types as $\Phi_1 = \{1, r, r^2\}$, $\Phi_2 = \{1, r, r^5\}$, $\Phi_3 = \{1, r^2, r^4\}$, and $\Phi_4 = \{1, r^4, r^5\}$. Recall from Definition 4.3.5 that a CM-type is primitive if it is not induced from a CM-type of a strict CM subfield. Thus a CM-type is not primitive if it is induced. In the lattice of subfields of K below, the only subfields of $K = L^{\langle s \rangle}$ are $L^{\langle r^2, s \rangle}$, $L^{\langle r^3, s \rangle}$, and $\mathbb{Q} = L^{\langle r, s \rangle}$.



$L^{\langle r^3, s \rangle}$ is totally real since r^3 is complex conjugation. (In fact it is K_0, the totally real subfield of K). But $F = L^{\langle r^2, s \rangle}$ satisfies the property that r^3, complex conjugation,

commutes with all of the elements of its Galois group, $\mathrm{Gal}(F/\mathbb{Q})$, and therefore all of its complex embeddings. Therefore by Lang's characterization of CM fields from Proposition 2.1.12, $F = L^{\langle r^2, s\rangle}$ is a CM field. By a process similar to that of Section 6.2, the complex embeddings of F correspond to 1 and r, and the embeddings of F into K correspond to 1, r^2, and r^4 as below:



Therefore, the CM-type $\{1\}$ of F induces the CM-type $\Phi_3 = \{1, r^2, r^4\}$ on K, and the CM-type $\{r\}$ of F induces $\overline{\Phi_3} = \{r, r^3, r^5\}$ on K. Since F is the only CM subfield of K, the other CM-types are primitive. □

6.4 Finding reflex types

Recall that the definition of the reflex (K^R, Φ^R) of (K, Φ) from Definition 4.3.7. Guided by the definition, for each primitive CM-type of K, we may compute the reflex in the following manner: We first find the induced CM-type Φ^L, and then compute its inverse $(\Phi^L)^{-1}$. We then consider whether we can "factor out" a Galois subgroup to write $(\Phi^L)^{-1} = \{\sigma_1, \sigma_2, \sigma_3\}H$, for H a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$. Then $K^R = L^H$, the fixed field of H in L, and Φ^R is the CM-type of K^R induced by restricting σ_1, σ_2, and σ_3 to K^R. We apply a similar process to the non-primitive

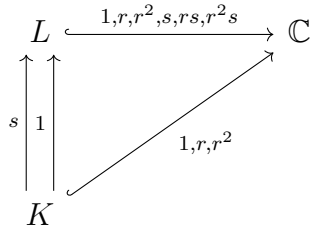
CM-types.

As before, using the choices made in Section 6.2, we have that φ_1 corresponds to 1, φ_2 to r, and φ_3 to r^2, thus $\overline{\varphi_1}$ corresponds to r^3, $\overline{\varphi_2}$ to r^4, and $\overline{\varphi_3}$ to r^5.

Throughout, we use the notation of Example 4.3.2.

6.4.1 Reflex of Φ_1

Consider first $\Phi_1 = \{1, r, r^2\}$. We induce up to L using our two automorphisms, 1 and s, as below:



Therefore the induced CM-type, which we will denote Φ_1^L, is

$$\Phi_1^L = \{1, r, r^2, s, rs, r^2 s\}.$$

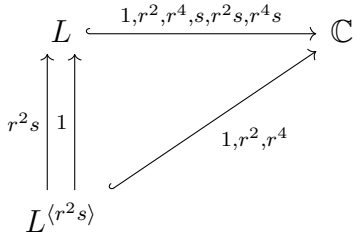
Next we find the inverse of each element of Φ_1^L in order to create $(\Phi_1^L)^{-1}$. For instance, the inverse of r^2 is r^4 since $r^2 r^4 = r^6 = 1$, and the inverse of $r^2 s$ is $r^2 s$ since

$$r^2 s r^2 s = r^2 s s^{-1} r^{-2} = r^2 r^{-2} = 1.$$

Thus

$$(\Phi_1^L)^{-1} = \{1, r^4, r^5, s, rs, r^2 s\}.$$

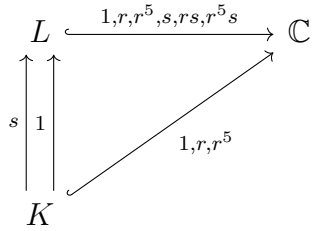
We notice that this is none other than the CM-type $\{1, r^2, r^4\}$ induced up from $L^{\langle r^2 s\rangle}$. Indeed we have



Therefore the reflex type is $\Phi_1^R = \{1, r^4, r^5\}$ and the reflex field $K_1^R = L^{\langle r^2 s\rangle}$, the fixed field of $\langle r^2 s\rangle$, a sextic CM field. We note that by Proposition 2.4.1, K_1^R is isomorphic to K.

6.4.2 Reflex of Φ_2

We consider now $\Phi_2 = \{1, r, r^5\}$. Again, we induce up to L using our two automorphisms, 1 and s, as below:



We get

$$\Phi_2^L = \{1, r, r^5, s, rs, r^5 s\}.$$

Then

$$(\Phi_2^L)^{-1} = \{1, r, r^5, s, rs, r^5 s\},$$

which is the CM-type $\{1, r, r^5\}$ induced from $L^{\langle s \rangle}$. We get our reflex type $\Phi_2^R = \{1, r, r^5\}$ and our reflex field $K_2^R = L^{\langle s \rangle}$. Thus (K, Φ_2) is its own reflex.

6.4.3 Reflex of Φ_3

Consider now $\Phi_3 = \{1, r^2, r^4\}$. Recall from Proposition 6.3.3 that Φ_3 is not primitive. It is the type $\{1\}$ induced up from $L^{\langle r^2, s \rangle}$. Nevertheless, we induce Φ_3 up to L and obtain

$$\Phi_3^L = \{1, r^2, r^4, s, r^2 s, r^4 s\}.$$

Therefore

$$(\Phi_3^L)^{-1} = \{1, r^2, r^4, s, r^2 s, r^4 s\} = \{1, r^2, r^4\}\langle r^2 s \rangle = \{1\}\langle r^2 \rangle \langle r^2 s \rangle = \{1\}\langle r^2, s \rangle$$

which is the CM-type $\{1\}$ induced up from $L^{\langle r^2, s \rangle}$. We see here that $\{1\}$ on $L^{\langle r^2, s \rangle}$ is its own reflex, which is to be expected since $L^{\langle r^2, s \rangle}$ is Galois.

6.4.4 Reflex of Φ_4

Next, we consider $\Phi_4 = \{1, r^4, r^5\}$. We have

$$\Phi_4^L = \{1, r^4, r^5, s, r^4 s, r^5 s\},$$

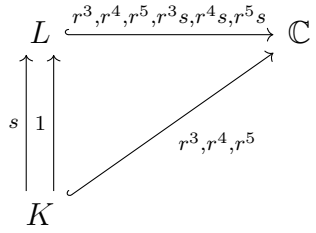
so that

$$(\Phi_4^L)^{-1} = \{1, r, r^2, s, r^4 s, r^5 s\}$$

which we see to be the CM-type $\{1, r, r^2\}$ induced from $L^{\langle r^4 s \rangle}$.

6.4.5 Reflex of $\overline{\Phi_1}$

We now turn our attention to $\overline{\Phi_1} = \{r^3, r^4, r^5\}$. We induce up to L using our two automorphisms, 1 and s, as below:



We get

$$\overline{\Phi_1}^L = \{r^3, r^4, r^5, r^3s, r^4s, r^5s\},$$

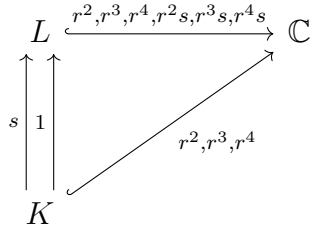
so that

$$(\overline{\Phi_1}^L)^{-1} = \{r, r^2, r^3, r^3s, r^4s, r^5s\}.$$

Thus we get reflex type $\overline{\Phi_1}^R = \{r, r^2, r^3\}$ and $\overline{K_1}^R = L^{\langle r^2 s \rangle}$. We note that $\overline{\Phi_1}^R = \overline{\Phi_1^R}$ and Φ_1 and $\overline{\Phi_1}$ have the same reflex field.

6.4.6 Reflex of $\overline{\Phi_2}$

Consider now $\overline{\Phi_2} = \{r^2, r^3, r^4\}$. We induce up to L using our two automorphisms, 1 and s, as below:



We get

$$\overline{\Phi_2}^L = \{r^2, r^3, r^4, r^2s, r^3s, r^4s\},$$

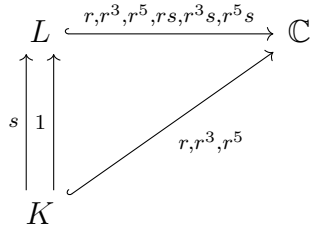
so that

$$(\overline{\Phi_2}^L)^{-1} = \{r^2, r^3, r^4, r^2s, r^3s, r^4s\}.$$

Thus we get reflex type $\overline{\Phi_2}^R = \{r^2, r^3, r^4\}$ and $\overline{K_2}^R = L^{\langle s \rangle}$. We see that $(K, \overline{\Phi_2})$ is its own reflex, as was (K, Φ_2).

6.4.7 Reflex of $\overline{\Phi_3}$

Consider the penultimate CM-type $\overline{\Phi_3} = \{r, r^3, r^5\}$. Again, from Proposition 6.3.3 we know that this CM-type is not primitive. It is the type $\{r\}$ induced up from $L^{\langle r^2, s \rangle}$. We induce up to L using our two automorphisms, 1 and s, as below:



We get

$$\overline{\Phi_3}^L = \{r, r^3, r^5, rs, r^3s, r^5s\},$$

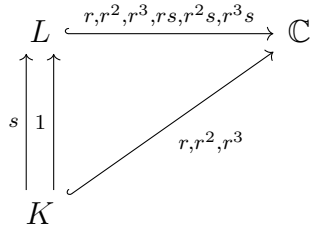
so that

$$(\overline{\Phi_3}^L)^{-1} = \{r, r^3, r^5, rs, r^3s, r^5s\} = \{r\}\langle r^2, s \rangle.$$

Again we see that $\{r\}$ on $L^{\langle r^2, s \rangle}$ is its own reflex, as we saw with $(\overline{\Phi_3}^L)^{-1}$, similarly to our conclusion for Φ_3.

6.4.8 Reflex of $\overline{\Phi_4}$

Finally we consider $\overline{\Phi_4} = \{r, r^2, r^3\}$. We induce up to L using our two automorphisms, 1 and s, as below:



We get

$$\overline{\Phi_4}^L = \{r, r^2, r^3, rs, r^2s, r^3s\},$$

so that

$$(\overline{\Phi_4}^L)^{-1} = \{r^3, r^4, r^5, r^3s, r^4s, r^5s\}.$$

Thus we get the reflex type $\overline{\Phi_4}^R = \{r^3, r^4, r^5\}$ and reflex field $\overline{K_4}^R = L^{\langle r^4 s \rangle}$. We notice that Φ_4 and $\overline{\Phi_4}$ have the same reflex field and that $\overline{\Phi_4}^R = \overline{\Phi_4^R}$.

Our conclusion that $\overline{\Phi_1}^R = \overline{\Phi_1^R}$ and $\overline{\Phi_4}^R = \overline{\Phi_4^R}$ leads us to conjecture that complex conjugation commutes with finding reflex types.

Chapter 7

Example

In this Chapter we give a concrete example of the computations described in Chapter 6.

We used the LMFDB [8] to find a sextic CM field whose Galois closure has Galois group D_{12}. We chose $K = \mathbb{Q}[x]/(x^6 - 2x^5 + 2x^4 + 2x^3 + 4x^2 - 4x + 2)$ and throughout we let α be a root of this polynomial. We then found the Galois closure of the field, $L = \mathbb{Q}[x]/(x^{12} + 128x^8 + 1728x^4 + 5476)$, and throughout we let β be a root of this polynomial.

7.1 Preliminaries

We know that the elements of D_{12} are 1, r, r^2, r^3, r^4, r^5, s, rs, r^2s, r^3s, r^4s, and r^5s, and we want to match these elements to our complex embeddings φ_1, φ_2, φ_3, $\overline{\varphi_1}$, $\overline{\varphi_2}$, and $\overline{\varphi_3}$ as in Section 6.2. To do this we first fix an arbitrary $\psi\colon K \hookrightarrow L$ and an arbitrary $\rho\colon L \hookrightarrow \mathbb{C}$. Using Sage, we choose ψ such that our primitive element $\alpha \in K$

maps to

$$\frac{109}{70300}\beta^{10} - \frac{2}{475}\beta^8 + \frac{6569}{35150}\beta^6 - \frac{483}{950}\beta^4 + \frac{22076}{17575}\beta^2 - \frac{1527}{475} \tag{7.1}$$

for $\beta \in L$, and (again using Sage) we choose ρ such that our primitive element $\beta \in L$ maps to

$$-2.30624364267427 - 2.30624364267424i. \tag{7.2}$$

Now we find the Galois element $1 \neq g \in D_{12}$ that fixes K. It suffices to find $g \neq 1$ such that

$$g(\psi(\alpha)) = \psi(\alpha) \tag{7.3}$$

and name this Galois element s. We see that

$$\psi(\alpha) = \frac{109}{70300}\beta^{10} - \frac{2}{475}\beta^8 + \frac{6569}{35150}\beta^6 - \frac{483}{950}\beta^4 + \frac{22076}{17575}\beta^2 - \frac{1527}{475} = s(\psi(\alpha)). \tag{7.4}$$

under the Galois element

$$s = (1,12)(2,11)(3,10)(4,9)(5,8)(6,7). \tag{7.5}$$

Next we find the Galois element $1 \neq g$ that corresponds to complex conjugation. So, we want to find g such that $\rho(g(\beta))$ is the complex conjugate of $\rho(\beta)$. We call this element r^3, and we find that

$$r^3 = (1,11)(2,12)(3,6)(4,5)(7,10)(8,9). \tag{7.6}$$

Finally we name the rest of the complex embeddings. As in Chapter 6, without loss

of generality, we choose φ_1 such that

$$\rho(\psi(\alpha)) = \varphi_1(\alpha) = 0.403031716762685 - 0.403031716762685i. \tag{7.7}$$

Thus $\overline{\varphi_1}$ is such that

$$\rho(r^3(\psi(\alpha))) = \overline{\varphi_1(\alpha)} = 0.403031716762685 + 0.403031716762685i. \tag{7.8}$$

Now (again without loss of generality), we choose φ_2 to correspond to r. To do this we must first fix r. Without loss of generality, we may choose r to be either one of the two elements of order 6 in $\mathrm{Gal}(L/\mathbb{Q})$ and we choose

$$r = (1, 4, 7, 11, 5, 10)(2, 6, 9, 12, 3, 8). \tag{7.9}$$

We get that

$$\rho(r(\psi(\alpha))) = \varphi_2(\alpha) = -0.854637679718466 - 0.854637679718459i. \tag{7.10}$$

Thus

$$\rho(r^4(\psi(\alpha))) = \overline{\varphi_2}(\alpha) = -0.854637679718466 + 0.854637679718459i. \tag{7.11}$$

determining for us that

$$r^4 = (1, 5, 7)(2, 3, 9)(4, 10, 11)(6, 8, 12). \tag{7.12}$$

Finally, since there is only one element of order 6 remaining, we know that

$$r^5 = (1, 10, 5, 11, 7, 4)(2, 8, 3, 12, 9, 6) \tag{7.13}$$

so that

$$\rho(r^5(\psi(\alpha))) = \overline{\varphi_3(\alpha)} = 1.45160596295577 + 1.45160596295574i, \tag{7.14}$$

and since there is only one element remaining of order 3, we have

$$r^2 = (1, 7, 5)(2, 9, 3)(4, 11, 10)(6, 12, 8), \tag{7.15}$$

so that

$$\rho(r^2(\psi(\alpha))) = \varphi_2(\alpha) = -0.854637679718466 - 0.854637679718459i. \tag{7.16}$$

By composing each of our Galois elements r^i with s, we may find the other Galois

elements. In summary, we find that

$$1 = () \tag{7.17}$$

$$r = (1,4,7,11,5,10)(2,6,9,12,3,8) \tag{7.18}$$

$$r^2 = (1,7,5)(2,9,3)(4,11,10)(6,12,8) \tag{7.19}$$

$$r^3 = (1,11)(2,12)(3,6)(4,5)(7,10)(8,9) \tag{7.20}$$

$$r^4 = (1,5,7)(2,3,9)(4,10,11)(6,8,12) \tag{7.21}$$

$$r^5 = (1,10,5,11,7,4)(2,8,3,12,9,6) \tag{7.22}$$

$$s = (1,12)(2,11)(3,10)(4,9)(5,8)(6,7) \tag{7.23}$$

$$rs = (1,3)(2,5)(4,12)(6,11)(7,9)(8,10) \tag{7.24}$$

$$r^2s = (1,8)(2,10)(3,4)(5,6)(7,12)(9,11) \tag{7.25}$$

$$r^3s = (1,2)(3,7)(4,8)(5,9)(6,10)(11,12) \tag{7.26}$$

$$r^4s = (1,6)(2,4)(3,11)(5,12)(7,8)(9,10) \tag{7.27}$$

$$r^5s = (1,9)(2,7)(3,5)(4,6)(8,11)(10,12). \tag{7.28}$$

and

$$\varphi_1(\alpha) = 0.403031716762685 - 0.403031716762685i, \tag{7.29}$$

$$\overline{\varphi_1}(\alpha) = 0.403031716762685 + 0.403031716762685i, \tag{7.30}$$

$$\varphi_2(\alpha) = -0.854637679718466 - 0.854637679718459i, \tag{7.31}$$

$$\overline{\varphi_2}(\alpha) = -0.854637679718466 + 0.854637679718459i, \tag{7.32}$$

$$\varphi_3(\alpha) = 1.45160596295577 - 1.45160596295574i, \tag{7.33}$$

$$\overline{\varphi_3}(\alpha) = 1.45160596295577 + 1.45160596295574i. \tag{7.34}$$

.

7.2 Computation of Reflex Fields and Reflex Types

With our Galois elements and complex embeddings fixed, we now apply the results of our computations from Chapter 6. Throughout we continue to fix ρ such that for a primitive element $\beta \in L$ we have

$$\rho(\beta) = -2.30624364267424 - 2.30624364267424i. \tag{7.35}$$

7.2.1 CM-types Φ_1 and $\overline{\Phi_1}$

Recall from Chapter 6 that

$$\Phi_1 = \{1, r, r^2\}, \tag{7.36}$$

$$\overline{\Phi_1} = \{r^3, r^4, r^5\}, \tag{7.37}$$

$$K_1^R = L^{\langle r^2 s \rangle}, \tag{7.38}$$

$$\Phi_1^R = \{1, r^4, r^5\}, \tag{7.39}$$

$$\overline{\Phi_1}^R = \{r, r^2, r^3\}. \tag{7.40}$$

We first compute $K_1^R = L^{\langle r^2 s \rangle}$, the reflex field shared by Φ_1 and $\overline{\Phi_1}$. We get

$$K_1^R = \mathbb{Q}[x]/(x^6 - 10x^3 + 576x^2 - 240x + 50) \tag{7.41}$$

with primitive element α_1. Once we have the reflex field, we recover complex embeddings from the Galois elements in the CM-type, as we did in Chapter 6. As before, we use our fixed embedding $\rho\colon L \hookrightarrow \mathbb{C}$ and an embedding $\psi_1\colon K_1^R \hookrightarrow L$, where ψ_1 sends the primitive element α_1 of K_1^R to

$$\frac{343}{140600}\beta^{10} + \frac{3}{475}\beta^8 + \frac{5192}{17575}\beta^6 + \frac{1449}{1900}\beta^4 + \frac{38346}{17575}\beta^2 + \frac{3}{2}\beta + \frac{2528}{475}, \tag{7.42}$$

For each Galois element σ in the CM-type we then compute the associated embedding

$$\varphi = \rho \circ \sigma \circ \psi_1 \tag{7.43}$$

and we get that the reflex type Φ_1^R is

$$\rho(\psi_1(\alpha_1)) = -3.56391303915539 - 3.56391303915538i \tag{7.44}$$

$$\rho(r^4(\psi_1(\alpha_1))) = 3.35481788886733 + 3.35481788886734i \tag{7.45}$$

$$\rho(r^5(\psi_1(\alpha_1))) = 0.209095150288055 - 0.209095150288037i \tag{7.46}$$

$$\tag{7.47}$$

and $\overline{\Phi_1}^R$ is

$$\rho(r(\psi_1(\delta))) = 3.35481788886733 - 3.35481788886727i \tag{7.48}$$

$$\rho(r^2(\psi_1(\delta))) = 0.209095150288055 + 0.209095150288037i \tag{7.49}$$

$$\rho(r^3(\psi_1(\delta))) = -3.56391303915540 + 3.56391303915538i. \tag{7.50}$$

We notice that

$$\rho(r(\psi_1(\delta))) = \overline{\rho(r^4(\psi(\delta)))}, \tag{7.51}$$

$$\rho(r^2(\psi_1(\delta))) = \overline{\rho(r^5(\psi_1(\delta)))}, \tag{7.52}$$

$$\rho(r^3(\psi_1(\delta))) = \overline{\rho(r^3(\psi(\delta)))}, \tag{7.53}$$

as expected.

7.2.2 CM-types Φ_2 and $\overline{\Phi_2}$

We recall from Chapter 6 that (K, Φ_2) and $(K, \overline{\Phi_2})$ are their own reflexes. We therefore only give the explicit CM-types. We compute Φ_2^R to be

$$\rho(\psi_2(\alpha_2)) = 0.403031716762694 - 0.403031716762712i, \tag{7.54}$$

$$\rho(r(\psi_2(\alpha_2))) = -0.854637679718466 - 0.854637679718459i, \tag{7.55}$$

$$\rho(r^5(\psi_2(\alpha_2))) = 1.45160596295577 + 1.45160596295578i, \tag{7.56}$$

$$\tag{7.57}$$

and $\overline{\Phi_2}^R$ to be

$$\rho(r^2(\psi_2(\alpha_2))) = 1.45160596295577 - 1.45160596295574i, \tag{7.58}$$

$$\rho(r^4(\psi_2(\alpha_2))) = -0.854637679718465 + 0.854637679718456, \tag{7.59}$$

$$\rho(r^3(\psi_2(\alpha_2))) = 0.403031716762694 + 0.403031716762712i. \tag{7.60}$$

7.2.3 CM-types Φ_3 and $\overline{\Phi_3}$

As before, we recall that

$$\Phi_3 = \{1, r^2, r^4\}, \tag{7.61}$$

$$\overline{\Phi_3} = \{r, r^3, r^5\}, \tag{7.62}$$

$$K_3^R = L^{\langle r^2, s\rangle}, \tag{7.63}$$

$$\Phi_3^R = \{1\}, \tag{7.64}$$

$$\overline{\Phi_3}^R = \{r\}. \tag{7.65}$$

We also note that Φ_3 and $\overline{\Phi_3}$, as we saw in 6.3.3, are not primitive. We compute $K_3^R = L^{\langle r^2, s\rangle}$, the reflex field shared by Φ_3 and $\overline{\Phi_3}$, which we find to be

$$K_3^R = \mathbb{Q}[x]/(x^2 + 1024) \tag{7.66}$$

with primitive element α_3. Then we recover the complex embeddings from the Galois elements in the CM-type. Next we use our fixed embedding $\rho\colon L \hookrightarrow \mathbb{C}$ and an embedding $\psi_3\colon K_3^R \hookrightarrow L$, where ψ_3 maps a primitive element α_3 of K_3^R as follows:

$$\alpha_1 \mapsto \frac{128}{17575}\beta^{10} + \frac{16976}{17575}\beta^6 + \frac{334848}{17575}\beta^2. \tag{7.67}$$

For each Galois element σ in the CM-type we compute the associated embedding

$$\varphi = \rho \circ \sigma \circ \psi_3 \tag{7.68}$$

and we get that the reflex type Φ_3^R is

$$\rho(\psi_3(\alpha_3)) = 32.0000000000000i, \tag{7.69}$$

and $\overline{\Phi_3}^R$ is

$$\rho(r(\psi_3(\alpha_3))) = -32.0000000000000i. \tag{7.70}$$

We clearly see that these two reflex types are complex conjugates. We note that each type contains only one embedding since the reflex field K_3^R is quadratic.

7.2.4 CM-types Φ_4 and $\overline{\Phi_4}$

Again we recall from Chapter 6 that

$$\Phi_4 = \{1, r^4, r^5\}, \tag{7.71}$$

$$\overline{\Phi_4} = \{r, r^2, r^3\}, \tag{7.72}$$

$$K_4^R = L^{\langle r^4 s \rangle}, \tag{7.73}$$

$$\Phi_4^R = \{1, r, r^2\}, \tag{7.74}$$

$$\overline{\Phi_4}^R = \{r^3, r^4, r^5\}. \tag{7.75}$$

As before, we first compute $K_4^R = L^{\langle r^4 s \rangle}$, the reflex field shared by Φ_4 and $\overline{\Phi_4}$. We get

$$K_4^R = \mathbb{Q}[x]/(x^6 + 10x^3 + 576x^2 + 240x + 50) \tag{7.76}$$

with primitive element α_4. We now recover the complex embeddings from the Galois elements in the CM-type. Next we use our fixed embedding $\rho\colon L \hookrightarrow \mathbb{C}$ and an embedding $\psi_4\colon K_4^R \hookrightarrow L$, where ψ_4 maps the primitive element α_4 of K_4^R as follows:

$$\alpha_4 \mapsto \frac{-343}{140600}\beta^{10} - \frac{3}{475}\beta^8 - \frac{5192}{17575}\beta^6 - \frac{1449}{1900}\beta^4 - \frac{38346}{17575}\beta^2 + \frac{3}{2}\beta - \frac{2528}{475}. \quad (7.77)$$

For each Galois element σ in the CM-type we then compute the associated embedding

$$\varphi = \rho \circ \sigma \circ \psi_4 \quad (7.78)$$

and we get that the reflex type Φ_4^R is

$$\rho(\psi_4(\alpha_4)) = -3.35481788886733 - 3.354817888867 34i, \quad (7.79)$$

$$\rho(r(\psi_4(\alpha_4))) = -0.209095150288055 + 0.209095150288037i, \quad (7.80)$$

$$\rho(r^2(\psi_4(\alpha_4))) = 3.56391303915539 + 3.56391303915538i, \quad (7.81)$$

and $\overline{\Phi_4}^R$ is

$$\rho(r^5(\psi_4(\alpha_4))) = 3.56391303915540 - 3.56391303915538i, \quad (7.82)$$

$$\rho(r^4(\psi_4(\alpha_4))) = -0.209095150288055 - 0.209095150288037i, \quad (7.83)$$

$$\rho(r^3(\psi_4(\alpha_4))) = -3.35481788886733 + 3.354817888867 27i. \quad (7.84)$$

We again note our pairs of complex conjugates:

$$\rho(\psi_4(\alpha_4)) = \overline{\rho(r^3(\psi_4(\alpha_4)))}, \tag{7.85}$$

$$\rho(r(\psi_4(\alpha_4))) = \overline{\rho(r^4(\psi_4(\alpha_4)))}, \tag{7.86}$$

$$\rho(r^5(\psi_4(\alpha_4))) = \overline{\rho(r^2(\psi_4(\alpha_4)))}. \tag{7.87}$$

Bibliography

[1] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*, volume 302. Springer Science & Business Media, 2013.

[2] Henri Cohen. *A course in computational algebraic number theory*, volume 138. Springer Science & Business Media, 2013.

[3] Henri Cohen and Xavier-François Roblot. Computing the hilbert class field of real quadratic fields. *Mathematics of Computation of the American Mathematical Society*, 69(231):1229–1244, 2000.

[4] Mario Daberkow and M Pohst. On the computation of hilbert class fields. *Journal of Number Theory*, 69(2):213–230, 1998.

[5] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, Inc., 3rd edition, 2004.

[6] Philipp Furtwängler. Allgemeiner existenzbeweis für den klassenkörper eines beliebigen algebraischen zahlkörpers. *Mathematische Annalen*, 63(1):1–37, 1906.

[7] Serge Lang. *Complex Multiplication*. Springer-Verlag, 1983.

[8] The LMFDB Collaboration. The l-functions and modular forms database. http://www.lmfdb.org, 2017. [Online; accessed January 2017].

[9] James S. Milne. Abelian varieties. www.jmilne.org/math/, 2008. [Online; accessed June 2017].

[10] James S. Milne. Algebraic number theory (v3.07), 2017. Available at www.jmilne.org/math/.

[11] James S. Milne. Fields and galois theory. www.jmilne.org/math/, 2017. [Online; accessed June 2017].

[12] Goro Shimura. *Abelian varieties with complex multiplication and modular functions*. Princeton University Press, 2016.

[13] Joseph H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, 1994.

[14] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 3rd edition, 2009.

[15] M. Streng. *Complex multiplication of abelian surfaces*. PhD thesis, Universiteit Leiden, 2010.

Appendix A

Sage code

```
def good_taus(K):
    good_taus = [] #empty list of good taus
    G = K.class_group() #G is the ideal class group
    phi = K.complex_embeddings(53)[0] #gets a complex
    embedding of K
    for L in G: #go through each element of the class
    group
        I_0 = L.ideal() #defines the ideal of L as I_0
        tau_) = I_0.basis()[0]/I_0.basis()[1] #computes tau
        for that L
        alpha = phi(tau_0) #defines alpha to be phi evaluated
        with tau
        if alpha.imag() > 0: #tests if tau is > 0
            #print ``positive"
            good_taus.append(alpha) #if tau > 0 adds tau to
            good tau list
        else: #only happens if tau <= 0
            #print ``not positive"
            #print 1/tau_0 #computes 1/tau
            good_taus.append(1/alpha) #adds 1/tau to good tau
            list
        return good_taus #returns good tau list

def theta(a,b,tau,B): #defines theta function with below
arguments
    #a is 0 or 1/2
    #b is 0 or 1/2
    #tau is the complex tau from before
    #B is a bound for the summation
```

```
30      from sage.symbolic.constants import pi
31      CC = ComplexField(53)
32      pi = CC(pi)
33      theta = 0 #starts theta sum at zero
34      for n in range(-B,B+1):
35          theta = theta + exp(pi * I * tau * (n + a)^2
36          + 2 * pi * I * (n + a) * b) #theta function
37      return theta #returns theta partial sums
38
39  def j_invariant(tau,D):
40      a_1 = theta(1/2,0,tau,D) #a value 10
41      b_1 = theta(0,0,tau,D) #b value 00
42      c_1 = theta(0,1/2,tau,D) #c value 01
43      j_invariant = 32 * ((a_1^8 + b_1^8 + c_1^8)^3
44      /(a_1 * b_1 * c_1)^8)
45      return j_invariant #j-invariant equation
46
47  def make_polynomial(J):
48      j_tau = good_taus(J)
49      j_inv_list = []
50      for number in j_tau:
51          inv = j_invariant(number,100) #arbitrary bound that works for our
52          #purposes
53          Ch. 5
54          j_inv_list.append(inv)
55      poly = 1
56      for inv in j_inv_list:
57          poly = poly * (y - inv)
58      return poly
```