FIELDS OF MODULI FOR QM ABELIAN SURFACES WITH CM

A Thesis

Submitted to the Faculty

in partial fulfillment of the requirements for the

degree of

Bachelor of Arts

in

Mathematics

by

Jacob Swenberg

Advisor

John Voight

DARTMOUTH COLLEGE

Hanover, New Hampshire

May 2021

Abstract

Motivated by the class number 1 problem of Gauss, we provide a complete description of the Galois action on the set of principally polarized abelian surfaces with QM by a maximal quaternion order O and CM by an imaginary quadratic order S. The set $\mathcal{A}$ of such abelian surfaces is in bijection with a set of classes of optimal embeddings of S into O. We describe an action of the absolute Galois group on these optimal embeddings and show that the action agrees with the action on abelian surfaces. By completely describing the action on optimal embeddings, we describe the action on abelian surfaces. As a consequence, we determine various fields of moduli of abelian surfaces. Using recent progress on finding rational points on curves using the technique of quadratic Chabauty, we apply the results to give a new solution to the Gauss class number 1 problem.

Preface

The construction of this thesis has been an incredible voyage. We started in 2019 with the goal of solving the Gauss class number 1 problem for CM extensions of totally real fields using Shimura curves. It was my first exposure to math research, and I loved it so much that I decided I wanted to do math for a living. Eventually, we ran into problems having to deal with the difference between fields of moduli versus fields of definition. These problems were coupled with computational issues we had with Magma, the computer algebra system that we have been using for the project. We ended up setting our sights on a different goal: to understand fields of moduli better for CM points on Shimura curves. By the time this thesis started to come together, the project had been ongoing for about 2 years, half of my time in college. I am extremely grateful to be able to share the product of all of that work in this thesis.

I could not have done any of this without the support of my advisor, John Voight. Dr. Voight gave me the chance to try my hand at math research. Through his positive energy, excellent teaching, personal support, and deep insight, I have grown as a person in ways I never could have expected. I am honored to have worked with him.

I also want to acknowledge the support I have had from the entire Department of Mathematics at Dartmouth. Numerous professors have helped get me to where I am today, providing the guidance I needed to pursue this mathematical journey.

Much thanks are due to Vanessa Pinney for talking with me about my mathematical struggles and successes when I needed it the most, and to all of the friends and family who have supported me through my undergraduate experience. I am so grateful for the kindness of these people.

Contents

Chapter 1

Introduction

Section 1.1

Motivation

One of the famous problems in number theory is Gauss's class number 1 problem for binary quadratic forms [7]: how many discriminants D (negative integers congruent to 0 or 1 mod 4) of positive-definite binary quadratic forms over $\mathbb{Z}$ have exactly one primitive binary quadratic form of discriminant D up to an invertible change of variables? The question can be translated into a question about imaginary quadratic orders: how many imaginary quadratic orders have class number 1? Equivalently, when are all invertible fractional ideals of $\mathbb{Z}[\nu]$ principal, assuming ν is a root of a monic integer quadratic polynomial with negative discriminant? When $\mathbb{Z}[\nu]$ is maximal (i.e. the ring of integers in an imaginary quadratic field), this is the same as asking when $\mathbb{Z}[\nu]$ is a PID, or equivalently, a UFD.

A *binary quadratic form* over $\mathbb{Z}$ is a function

$$f : \mathbb{Z}^2 \to \mathbb{Z}$$

$$f(x, y) = ax^2 + bxy + cy^2,$$

where $a, b, c \in \mathbb{Z}$. We define the *discriminant* of f to be $b^2 - 4ac$, and say that f is *positive-definite* if $D < 0$. We say f is *primitive* if a, b, c have no factors in common. For example, we have a form $x^2 + y^2$ with discriminant $0^2 - 4(1)(1) = -4$. This form is primitive and positive-definite. A basic question we might ask about such forms is when they *represent* certain numbers. That is, given an integer m, when are there integers $x, y \in \mathbb{Z}$ such that $ax^2 + bxy + cy^2 = m$? What if m is prime? We could change variables and get a form which represents the same primes. For example, we could replace x with $x + y$. With the form $x^2 + y^2$, this gives the form $(x + y)^2 + y^2 = x^2 + 2xy + 2y^2$. We check that this form has the same discriminant: $2^2 - 4(1)(2) = 4 - 8 = -4$. The class number 1 problem asks: if f and f' are primitive positive-definite binary quadratic forms of discriminant D, can we get from f to f' with a change of variables?

The answer for $D = -4$ (corresponding to the form $x^2 + y^2$) turns out to be yes, that any other primitive positive-definite binary quadratic form of discriminant -4 comes from $x^2 + y^2$ by an invertible change of variables. Which other discriminants give the same answer?

Various mathematicians had proven results showing that as D grows in magnitude, the class number $h(D)$ grows as well [7]. However, the proof that there were only finitely many discriminants with class number 1 remained elusive. In 1952, Heegner [11] published a proof using modular forms, but at the time, the proof was believed to be incorrect. Over a decade later, in 1966, Baker [3] provided an analytic proof. Then, in 1967, Stark [18] patched the supposed "gap" in Heegner's argument. Heegner, Baker, and Stark all proved the following theorem.

Theorem 1.1.1 (Heegner–Baker–Stark)**.** *If $D < 0$ is a discriminant, then*

$$h(D) = 1 \iff D \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}.$$

A proof of this theorem can also be found in Cox [7], who follows Heegner's idea.

A sketch of a modern reinterpretation of Heegner's original proof is as follows (from [16]): given an imaginary quadratic order S of class number 1, there is an elliptic curve with CM (complex multiplication) by S. Assuming S satisfies some conditions (that only finitely many S fail to satisfy), this elliptic curve gives rise to an integral point on a modular curve of level 24. An explicit computation shows that this modular curve has only finitely many integral points, and they correspond to a subset of the known class number 1 discriminants.

Modular curves naturally arise as spaces that parametrize *elliptic curves*, which are a kind of projective non-singular algebraic curve that admit a group structure. Elliptic curves are generalized by *abelian surfaces*, and the analogues of modular curves in the general case are *Shimura curves*. The Shimura curves we are interested in come from quotients of the complex upper half-plane $\mathfrak{H}$ by an action by *quaternionic unit groups*. These units come from *quaternion algebras*, which also make many appearances in modern number theory (see [20]).

A natural question comes from these observations: *could Shimura curves be used to solve class number 1 problems*? Starting in the spring of 2019, we set out to answer this question. Unfortunately, there were significant obstacles. Foremost among the obstructions was a misunderstanding of the difference between *fields of moduli* and *fields of definition*. We needed to have a better understanding of fields of moduli.

A large body of work has gone into understanding fields of moduli (see [14], for example). The goal of this thesis is to answer basic questions about fields of moduli for abelian surfaces with QM by a maximal quaternion order O. Specifically, we look at abelian surfaces with *CM (complex multiplication)*.

Section 1.2

Main result

In this thesis, we answer questions about fields of moduli by relating CM points on Shimura curves with classes of optimal embeddings of imaginary quadratic orders. A *field of moduli* for an object is, loosely speaking, the largest field fixed by all automorphisms of algebraic numbers that take the given object to something that is isomorphic (under suitable definition of isomorphism). Intuitively, fields of moduli measure a kind of symmetry of objects: a larger field of moduli indicates something that is not as symmetric or controlled, whereas a small field of moduli ($\mathbb{Q}$ being the smallest) indicates an object that is highly symmetric.

In this thesis, we are concerned with abelian surfaces with some extra structure—namely, *QM (quaternionic multiplication)* by a maximal quaternion order O in an indefinite quaternion algebra B of discriminant Δ, and *CM (complex multiplication)* by an imaginary quadratic order $S = \mathbb{Z}[\nu]$ of discriminant D that embeds optimally in O. To understand fields of moduli, we must understand how the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ acts on such abelian surfaces. The Main Theorem (Theorem 3.4.8) completely describes this action.

Let n be the number of primes dividing Δ, and let r primes dividing Δ be ramified in S. Let K be the field of fractions of S, and let H be the ring class field of K associated to S. We denote the Atkin-Lehner group of O by $\mathrm{AL}(O)$. We denote by $h(S)$ the size of the *Picard group* as defined in Definition 2.1.17. For an invertible fractional S-ideal $\mathfrak{c}$, we denote by $\mathrm{Frob}_{\mathfrak{c}}$ the image of the ideal class of $\mathfrak{c}$ under the *Artin isomorphism* (see Theorem 2.1.19).

Theorem 1.2.1 (Main Theorem 3.4.8)**.** *Let $\mathcal{A}$ be the set of isomorphism classes of principally polarized abelian surfaces with QM by O and CM by S. Then the following statements hold:*

(a) *There are commuting actions of $\mathrm{AL}(O)$ and $\mathrm{Gal}(H \mid \mathbb{Q})$ on $\mathcal{A}$, and*

$$\#\mathcal{A} = h(S)2^{n-r}.$$

(b) *The group* $\mathrm{Gal}(H \mid K)$ *acts freely on* $\mathcal{A}$ *with* 2^{n-r} *orbits of size* $h(S)$.

(c) *The group* $\mathrm{AL}(O)$ *acts transitively on the set of* $\mathrm{Gal}(H \mid K)$*-orbits.*

(d) *Each element of* $\mathrm{AL}(O)$ *acts either trivially or without fixed points on* $\mathcal{A}$. *Given* $[\omega_d] \in \mathrm{AL}(O)$ *represented by* $\omega_d \in N_{B^\times}(O) \cap O$ *with* $\mathrm{nrd}(\omega_d) = d \mid \Delta$ *and* $d > 0$, $[\omega_d]$ *acts trivially on* $\mathcal{A}$ *if and only if* S *has an element of norm* d. *If* S *has an ideal* $\mathfrak{a}$ *of norm* $d \mid \Delta$, *then* $[\omega_d]$ *acts identically to* $\mathrm{Frob}_{\mathfrak{a}} \in \mathrm{Gal}(H \mid K)$. *If* $[\omega_d]$ *acts as some* $\sigma \in \mathrm{Gal}(H \mid K)$ *on some* $A \in \mathcal{A}$, *then there exists an invertible ideal* $\mathfrak{a} \subseteq S$ *of norm* d *such that* $\sigma = \mathrm{Frob}_{\mathfrak{a}}$. *So each element of* $\mathrm{AL}(O)$ *acts either trivially or without fixed points on the set of* $\mathrm{Gal}(H \mid K)$*-orbits.*

(e) *There exists* $b \in \mathbb{Z}_{>0}$ *such that* $B \cong \left(\dfrac{D, b}{\mathbb{Q}}\right)$. *Furthermore, there exists* $\sigma_C \in \mathrm{Gal}(H \mid \mathbb{Q})$ *in the conjugacy class of complex conjugation such that for all* $A \in \mathcal{A}$, *there exists an invertible fractional* S*-ideal* $\mathfrak{c}$ *of norm* $b\Delta$ *such that*

$$\sigma_C(A) = \mathrm{Frob}_{\mathfrak{c}}(A^{[\omega_\Delta]}).$$

(f) *If* S *is maximal, then for all fractional* S*-ideals* $\mathfrak{c}$ *of norm* $b\Delta$, *there exists* $A \in \mathcal{A}$ *such that*

$$\sigma_C(A) = \mathrm{Frob}_{\mathfrak{c}}(A^{[\omega_\Delta]}).$$

Most of the thesis is concerned with describing an action of $\mathrm{Gal}(H \mid \mathbb{Q})$ on optimal embeddings, then establishing a bijection between classes of optimal embeddings and the relevant abelian surfaces. This bijection respects the actions of all groups involved, so understanding the action on embeddings gives us an understanding of the action on abelian surfaces. One group action we are interested in is that of the *Atkin-Lehner group* $\mathrm{AL}(O)$. Taking quotients by Atkin-Lehner elements proves to have useful interpretations (see [2]).

This theorem allows us to understand fields of moduli, as shown in the Main Corollary:

Corollary 1.2.2 (Main Corollary 3.4.9)**.** *Keep all of the conditions and notation of Theorem 1.2.1. Let $\Gamma \leq \mathrm{AL}(O)$ be a subgroup, and let k_Γ be the field of moduli of an element of $\mathcal{A}/\Gamma$.*

(a) *Let $\mathfrak{a} \subseteq S$ be an ideal of norm d. Then k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}$ if and only if $[\omega_d] \in \Gamma$.*

(b) *If k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}\, \sigma_C$, then $[\mathfrak{a}]$ can be represented by a fractional S-ideal $\mathfrak{a}$ of norm db for some $d \mid \Delta$ with $[\omega_d] \in \Gamma$. Conversely, if S is maximal and $\mathfrak{a}$ is a fractional S-ideal of norm db and $\mathfrak{c}$ is a fractional ideal of norm $b\Delta$ such that $(db)^{-1}\mathfrak{a}\mathfrak{c}$ is integral, then there is some $A \in \mathcal{A}$ such that k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}\, \sigma_C$.*

As an application, we prove the Heegner-Baker-Stark Theorem, Theorem 1.1.1, concerning imaginary quadratic orders with class number 1. Let B be the quaternion algebra over $\mathbb{Q}$ with discriminant $91 = 7 \cdot 13$. We show that only finitely many CM orders S have 7 or 13 not inert, and we determine all such S. For each class number 1 CM order S with 7 and 13 each ramified or inert, there are rational points on some curve corresponding to $[\omega_{91}]$-equivalence classes in $\mathcal{A}$. Using recent results on finding rational points on curves by the technique of *quadratic Chabauty*, we determine all rational points on this curve and show that we have identified all CM orders with class number 1. See the proof of Theorem 3.4.11 in Subsection 3.4.5 for details.

Section 1.3

Overview of structure

In Chapter 2, we give a brief survey of some of the concepts involved in the thesis. There are entire books to read about the objects and ideas involved in this thesis, but we provide hopefully enough for the reader to follow the main ideas. We walk through some basic concepts in algebraic number theory, quaternion algebras, and QM abelian surfaces.

In Chapter 3, we develop the ideas needed for the Main Theorem and its corollary. We begin in Sections 3.2 and 3.3 by describing a few group actions on a set of classes of optimal embeddings. We then, in Section 3.4, establish a bijection between these classes of optimal embeddings and the abelian surfaces we are concerned with. Finally, we state and prove the Main Theorem 3.4.8 and the Main Corollary 3.4.9.

Chapter 2

Background

Section 2.1

Algebraic Number Theory

2.1.1. Number Fields

Algebraic number theory is concerned with *number fields*.

Definition 2.1.1. A *number field* is a finite (hence algebraic) extension of the rational numbers.

Examples of number fields are $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt[3]{5})$, or $\mathbb{Q}(\sqrt{1+\sqrt{-1}}, \sqrt{3})$. or $\mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^5 + x^2 + 1$. Since the complex numbers $\mathbb{C}$ form an algebraically closed field over $\mathbb{Q}$, basic field theory says that every number field embeds into the complex numbers.

We will mostly be concerned with *imaginary quadratic fields* and their extensions.

Definition 2.1.2. An *imaginary quadratic field* is a field of the form $\mathbb{Q}(\sqrt{D})$, where $D < 0$.

In number fields, we will be interested in the numbers that behave like integers.

Definition 2.1.3. Let K be a number field. An element $\alpha \in K$ is said to be an *algebraic integer* (α is *integral*) if α is the root of a monic polynomial with coefficients in $\mathbb{Z}$. Equivalently, the minimal polynomial of α has coefficients in $\mathbb{Z}$.

Any integer n is integral, since n is the root of the degree 1 polynomial $x - n$. Other examples of algebraic integers are $\sqrt{2}$ (a root of $x^2 - 2$) or $(\sqrt{5}+1)/2$ (a root of $x^2 - x - 1$). However, $(\sqrt{3}+1)/2$ is not integral because its minimal polynomial is $x^2 - x - 1/2$, which does not have integer coefficients. Note that if α is integral, then all of its conjugates (roots of the same minimal polynomial in an algebraic closure) are integral as well.

Theorem 2.1.4. *Let K be a number field of degree n over $\mathbb{Q}$ (e.g. K is an n-dimensional $\mathbb{Q}$-vector space). The algebraic integers in K form a ring, denoted $\mathbb{Z}_K$, also called the ring of integers in K. This ring is a free abelian group of rank n, and its field of fractions is K.*

Proof. See [13]. □

Let K be an imaginary quadratic field. Then $K \supset \mathbb{Q}$ is a Galois extension, with $\mathrm{Gal}(K \mid \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Under an embedding $K \hookrightarrow \mathbb{C}$, the nontrivial element of $\mathrm{Gal}(K \mid \mathbb{Q})$ is the restriction of complex conjugation to K. Accordingly, we write $\alpha \mapsto \overline{\alpha}$ for the nontrivial automorphism in $\mathrm{Gal}(K \mid \mathbb{Q})$.

Definition 2.1.5. Let K be an imaginary quadratic field, and let $\alpha \in K$. The *norm* of α is $\mathrm{Nm}(\alpha) := \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha) := \alpha\overline{\alpha}$. The *trace* of α is $\mathrm{Tr}(\alpha) := \mathrm{Tr}_{\mathbb{Q}}^{K}(\alpha) := \alpha + \overline{\alpha}$.

Lemma 2.1.6. *Let K be an imaginary quadratic field, and let $\alpha \in K$. Then α is an algebraic integer if and only if $\mathrm{Nm}(\alpha), \mathrm{Tr}(\alpha) \in \mathbb{Z}$.*

Proof. We have $\alpha^2 - (\alpha + \overline{\alpha})\alpha + \alpha\overline{\alpha}$, so α is a root of $x^2 - \mathrm{Tr}(\alpha)x + \mathrm{Nm}(\alpha)$. If the trace and norm are both integers, then α is integral by definition. Suppose α is integral. If $\alpha \in \mathbb{Q}$, then the minimal polynomial of α is $x - \alpha$, so $\alpha \in \mathbb{Z}$, and $\mathrm{Nm}(\alpha) = \alpha^2 \in \mathbb{Z}$ and $\mathrm{Tr}(\alpha) = 2\alpha \in \mathbb{Z}$.

If $\alpha \notin \mathbb{Q}$, then $x^2 - \mathrm{Tr}(\alpha)x + \mathrm{Nm}(\alpha)$ is the minimal polynomial of α and α has integer trace and norm. □

Proposition 2.1.7. *Let $K := \mathbb{Q}(\sqrt{N})$, where N is a squarefree integer. Then we can write $\mathbb{Z}_K = \mathbb{Z}[\nu] = \mathbb{Z} + \mathbb{Z}\nu$, where*

$$\nu = \begin{cases} \sqrt{N}, & N \equiv 2, 3 \mod 4, \\ \dfrac{1+\sqrt{N}}{2}, & N \equiv 1 \mod 4. \end{cases}$$

Proof. See [13]. □

The ring of integers in a number field has many nice properties. Specifically, while we do not know that $\mathbb{Z}_K$ is a PID or a UFD, a result like prime factorization holds.

Theorem 2.1.8. *Let K be a number field. Then $\mathbb{Z}_K$ is a Dedekind domain, e.g. an a Noetherian integral domain where every nonzero prime ideal is maximal, and $\mathbb{Z}_K$ contains all integral elements of its field of fractions K. As a consequence, every ideal in $\mathbb{Z}_K$ can be written uniquely as a product of prime ideals, unique up to reordering. Furthermore, $\mathbb{Z}_K$ is a PID if and only if it is a UFD.*

Proof. See [13, Ch 2]. □

2.1.2. Orders

The ring of integers in an imaginary quadratic field has many nice properties. However, we would like to consider more general subrings of imaginary quadratic fields.

Definition 2.1.9. Let K be an imaginary quadratic field. An *order* (or *imaginary quadratic order* or *CM order*) is a subring $S \subset K$ (containing 1) that is a finitely generated $\mathbb{Z}$-module and contains a $\mathbb{Q}$-basis for K.

For example, $\mathbb{Z}_K$ is an order by Proposition 2.1.7. A basic result from commutative algebra says that a ring which is a finitely generated $\mathbb{Z}$-module must be integral (over $\mathbb{Z}$), i.e. every element is integral [8, §15.3, Prop 23]. It follows that if S is an order in K, then $S \subseteq \mathbb{Z}_K$. Consequently, we call $\mathbb{Z}_K$ the *maximal order* in K. We can say even more about the structure of S relative to that of $\mathbb{Z}_K$.

Lemma 2.1.10. *Let K be an imaginary quadratic field with $\mathbb{Z}_K = \mathbb{Z}[\nu_0]$, and S an order in K. Then*

$$S = \mathbb{Z}[f\nu_0] = \mathbb{Z} + \mathbb{Z}f\nu_0,$$

where $f = [\mathbb{Z}_K : S] < \infty$ is the index of S in $\mathbb{Z}_K$.

Proof. See [7, Lem 7.2]. □

Definition 2.1.11. Let S be an order in K. The *conductor* of S is the positive integer $f := [\mathbb{Z}_K : S]$.

Note that in some places, the *conductor* of S means something slightly different. Since we are only concerned with imaginary quadratic orders in this thesis, Definition 2.1.11 will suffice.

Let $\{\alpha, \beta\}$ be a $\mathbb{Z}$-basis for and order $S \subset K$. Then the quantity

$$D := \left(\det \begin{pmatrix} \alpha & \beta \\ \overline{\alpha} & \overline{\beta} \end{pmatrix} \right)^2$$

does not depend on the choice of $\{\alpha, \beta\}$. In particular, if $S = \mathbb{Z}[\nu]$, then we get

$$D = (\nu - \overline{\nu})^2 = (\nu + \overline{\nu})^2 - 4\nu\overline{\nu} = \operatorname{Tr}(\nu)^2 - 4\operatorname{Nm}(\nu).$$

Definition 2.1.12. Let $S = \mathbb{Z}[\nu]$ be an order in K. The *discriminant* of S is $D := \operatorname{Tr}(\nu)^2 - 4\operatorname{Nm}(\nu) \in \mathbb{Z}$. Any integer congruent to 0 or 1 mod 4 is called a *discriminant.* The *discriminant of* K is the discriminant of $\mathbb{Z}_K$.

Proposition 2.1.13. *Let $S = \mathbb{Z}[\nu]$ be an order in K, where $\mathbb{Z}_K = \mathbb{Z}[\nu_0]$ and $\nu = f\nu_0$. Let D be the discriminant of S, and let D_0 be the discriminant of $\mathbb{Z}_K$. Then*

(a) $D = f^2 D_0 < 0$,

(b) $D \equiv 0, 1 \mod 4$, *and*

(c) $K = \mathbb{Q}(\sqrt{D})$.

(d) *A prime p divides D if and only if p is ramified in S, i.e. there is a unique prime of S over p that is not equal to pS.*

Conversely, if $D < 0$ is an integer congruent to 0 or 1 mod 4, then D is the discriminant of some imaginary quadratic order S, and S is maximal if and only D is not equal to $f^2 D_0$, where D_0 is some smaller discriminant and $f \in \mathbb{Z}$.

Proof. See [7, §7.A]. □

The discriminant of a maximal order is called a *fundamental discriminant.*

We now turn to the ideal theory of orders.

Definition 2.1.14. Let S be an order in K. A *fractional ideal* of S (or a *fractional S-ideal*) is a finitely generated S-submodule of K. A fractional ideal $\mathfrak{a}$ is called *proper* if

$$S = \{\alpha \in K : \alpha\mathfrak{a} = \mathfrak{a}\}.$$

We define the *norm* $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})$ of a fractional ideal $\mathfrak{a}$ to be the $\mathbb{Z}$-submodule of $\mathbb{Q}$ generated by $\{\mathrm{Nm}(\alpha) : \alpha \in \mathfrak{a}\}$. By an abuse of notation, we will sometimes write $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})$ to denote the positive principal generator of $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})$, and refer to this principal generator as the norm of $\mathfrak{a}$.

Given two fractional S-ideals $\mathfrak{a}$ and $\mathfrak{b}$, we define their *product* $\mathfrak{a}\mathfrak{b}$ to be the S-submodule of K generated by $\{\alpha\beta : \alpha \in \mathfrak{a}, \beta \in \mathfrak{b}\}$. We say that a fractional S-ideal $\mathfrak{a}$ is invertible if and only if there exists a fractional S-ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = S$.

Proposition 2.1.15. *Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional S-ideals and let $\alpha \in K$. Then the following are true:*

(a) *There exists $n \in \mathbb{Z}$ such that $n\mathfrak{a} \subseteq S$ is an S-ideal.*

(b) *$\mathfrak{a}$ is invertible if and only if it is proper. The*

(c) $\mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha S) = \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha)\mathbb{Z}$.

(d) *If $\mathfrak{a}$ and $\mathfrak{b}$ are proper, then $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a}\mathfrak{b}) = \mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})\,\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{b})$.*

(e) *If $\mathfrak{a}$ is proper, then $\mathfrak{a}\bar{\mathfrak{a}} = \mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})S$.*

(f) *If $\mathfrak{a} \subseteq S$ is proper, then $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})$ is principally generated by $\#(S/\mathfrak{a})$, and $\mathfrak{a}$ is invertible if the order of $S/\mathfrak{a}$ is coprime to the conductor f.*

Proof. Let $\alpha_1, \ldots, \alpha_r$ generate $\mathfrak{a}$. Then by [8, §15.3,Thm 29], there exists $n \in \mathbb{Z}$ such that $n\alpha_1, \ldots, n\alpha_r \in \mathbb{Z}_K$. Then $n\mathfrak{a} \subseteq S$ and (a) follows. See [7, Prop 7.4] for a proof of (b). For all $z \in S$, $\mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha z) = \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha)\,\mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha) \in \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha)\mathbb{Z}$. Also, $\mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha) \in \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha S)$, so $\mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha S) = \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha)\mathbb{Z}$, which proves (d). For (d) and (e), see [20, Lem 16.3.7] and [20, 16.6.14]. The first part of (f) follows from [20, Lem 9.6.9] and [20, Prop 16.4.3]. See [7, Lem 7.18] for the second part of (f). □

The set of invertible fractional S-ideals has a rich structure.

Lemma 2.1.16. *The set $I(S)$ of invertible fractional S-ideals forms an abelian group with a subgroup $P(S)$ consisting of principal ideals.*

Proof. See [7, §7.A]. □

Definition 2.1.17. The *Picard group* of S is the quotient group $\mathrm{Pic}(S) := I(S)/P(S)$. Elements of $\mathrm{Pic}(S)$ are called ideal classes. If $\mathfrak{a}$ is a fractional S-ideal, its class is denoted $[\mathfrak{a}]$. We sometimes denote the trivial element of $\mathrm{Pic}(S)$ by $[1]$. The size of the Picard group is also called the *class number* of S, and is denoted $h(S)$, or $h(D)$.

One key property we will use is that complex conjugation in K corresponds to inversion in the class group.

Lemma 2.1.18. *Given* $[\mathfrak{a}] \in \mathrm{Pic}(S)$,

$$[\mathfrak{a}]^{-1} = [\overline{\mathfrak{a}}].$$

Proof. We have $\mathfrak{a}\overline{\mathfrak{a}} = \mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})S$ by Proposition 2.1.15. Then

$$[\mathfrak{a}][\overline{\mathfrak{a}}] = [\mathfrak{a}\overline{\mathfrak{a}}] = [\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{a})S] = [1]. \qquad \square$$

The group $\mathrm{Pic}(S)$ will be central to the main analysis of this thesis. Specifically, we are concerned with abelian extensions of K that are unramified away from some finite set of places.

Theorem 2.1.19. *Let S be an order in an imaginary quadratic field K. Then there is a maximal abelian extension H of K that is unramified at primes coprime to the conductor of S. The field extension $H \supset \mathbb{Q}$ is Galois. Furthermore, there is a canonical isomorphism*

$$\Phi : \mathrm{Pic}(S) \xrightarrow{\sim} \mathrm{Gal}(H \mid K).$$

Proof. See [7, §8.A]. □

Definition 2.1.20. In Theorem 2.1.19, the field H is called the *ring class field of K associated to S*, and the map Φ is called the *Artin isomorphism*. Given $[\mathfrak{a}] \in \mathrm{Pic}(S)$ represented by an ideal $\mathfrak{a} \subseteq S$ coprime to the conductor, we denote

$$\mathrm{Frob}_{\mathfrak{a}} := \left(\frac{H/K}{\mathfrak{a}}\right) := \Phi([\mathfrak{a}]).$$

2.1.3. Localizations, Completions, and Adeles

Given a prime $p \in \mathbb{Z}$, we denote by $\mathbb{Z}_{(p)}$ the localization of the integers away from p:

$$\mathbb{Z}_{(p)} := \{a/b \in \mathbb{Q} : p \nmid b\}.$$

Recall that this localization is a *local ring*: the ring $\mathbb{Z}_{(p)}$ has a unique maximal ideal $p\mathbb{Z}_{(p)}$ (see [1, Ch 3]).

We briefly introduce p-adic numbers. Given $a \in \mathbb{Z}$, we define $v_p(a)$ to be the number of times the prime p divides a. For $a/b \in \mathbb{Q}$, we define $v_p(a/b) := v_p(a) - v_p(b)$. By convention, we define $v_p(0) = \infty$. The function v_p is called the *p-adic valuation* of $\mathbb{Q}$. We define the *p-adic absolute value* $|\cdot|_p$ by $|0|_p = 0$ and $|q|_p = p^{-v_p(q)}$ for all $q \in \mathbb{Q}^\times$. One can check that this satisfies the properties of a *field norm* (or an *absolute value*) on $\mathbb{Q}$. We define the *p-adic numbers* $\mathbb{Q}_p$ to be the completion of $\mathbb{Q}$ with respect to this absolute value. It turns out that $\mathbb{Q}_p$ has the structure of a field, and the p-adic valuation and absolute value $|\cdot|_p$ extend to $\mathbb{Q}_p$. See [12, Ch 1] for more details.

Inside $\mathbb{Q}_p$, we are interested in the ring

$$\mathbb{Z}_p := \{x \in \mathbb{Q}_p : v_p(x) \geq 0\}.$$

The ring $\mathbb{Z}_p$ is an integral domain (in fact, a PID) called the ring of *p-adic integers*, and has many nice properties. For instance, $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$, and every other ideal is of the form $p^e\mathbb{Z}_p$ for e any integer greater than or equal to 1. As a consequence, $\mathbb{Z}_p$ is a *Dedekind domain*.

We will make use of more general completions.

Definition 2.1.21. Let K be an imaginary quadratic field. We define the *completion of* K *at* p as

$$K_p := K \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

Given a (finitely-generated) $\mathbb{Z}$-submodule M of K, we define the *completion of* M *at* p as

$$M_p := M \otimes_{\mathbb{Z}} \mathbb{Z}_p \subset K_p.$$

For example, given an order S in K, we get S_p for each integer prime p. Given a fractional S-ideal $\mathfrak{a}$, we have completions $\mathfrak{a}_p$ for each integer prime p.

Note that K_p and S_p are not necessarily even integral domains, but $\mathfrak{a}_p$ is still a finitely-generated $\mathbb{Z}_p$-submodule of S_p such that $\mathfrak{a}_p \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = K_p$.

Theorem 2.1.22. *Let K be an imaginary quadratic field, and let S be an order in K. Let $\mathfrak{a} \subset K$ be a fractional S-ideal. Then $\mathfrak{a}$ is invertible if and only if for all p, $\mathfrak{a}_p = a_p S_p$ for some $a_p \in K_p^\times$.*

Proof. Note that K is a $\mathbb{Q}$-algebra with a *standard involution* (see [20, Def 3.2.1] and [20, Def 3.2.4]). Then the theorem follows from [20, Thm 16.6.1]. □

When is S_p integrally closed?

Lemma 2.1.23. *The ring S_p is integrally closed in K_p if and only if p divides the conductor of S.*

Proof. Let $\mathbb{Z}_K = \mathbb{Z}[\nu]$ and write $S = \mathbb{Z}[f\nu]$, where f is the conductor of S. Then $S_p = \mathbb{Z}_p[f\nu]$. If p does not divide f, then f is a unit in $\mathbb{Z}_p$, so $S_p = \mathbb{Z}_p[\nu]$ is integrally closed. Conversely, suppose p divides f. Then $\mathbb{Z}_p[f\nu]$ does not contain ν, since f is not a unit in $\mathbb{Z}_p$. □

We would like a way to consider all completions simultaneously. Let K be an imaginary quadratic field, and let S be an order in K. We define the *adele ring of* K as

$$\widehat{K} := \{(a_p)_p \in \prod_p K_p : a_p \in S_p \text{ for all but finitely many } p\}.$$

In this definition, the product is taken over all integer primes p. Note that this ring is not an integral domain, so caution is warranted. Note that K embeds in $\widehat{K}$ diagonally: we identify $\alpha \in K$ with $(\alpha, \alpha, \dots) \in \widehat{K}$. This really is an element of $\widehat{K}$, because $\alpha = s/n$ for some $s \in S$ and some $n \in \mathbb{Z}$, and only finitely many primes divide n.

In the adele ring, we are concerned with two subsets. We have the *idele group* $\widehat{K}^\times$, and we have the *adele ring of* S

$$\widehat{S} := \{\widehat{\alpha} = (a_p)_p \in \widehat{K} : a_p \in S_p \text{ for all integer primes } p\} = \prod_p S_p \subset \widehat{K}.$$

Proposition 2.1.24. *There is a bijection*

$$\begin{aligned} \operatorname{Pic}(S) &\longleftrightarrow K^\times \backslash \widehat{K}^\times / \widehat{S}^\times \\ [\mathfrak{a}] &\mapsto K^\times \widehat{\alpha} \widehat{S}^\times \quad \textit{where } \widehat{\alpha} = (a_p)_p \in \widehat{K}^\times \textit{ is such that } \mathfrak{a}_p = a_p S_p \\ [\widehat{\alpha}\widehat{S} \cap K] &\hookleftarrow K^\times \widehat{\alpha} \widehat{S}^\times. \end{aligned}$$

Proof. See [20, 27.5.1]. □

Because of this proposition, we will frequently identify $\operatorname{Pic}(S)$ with the set of double-cosets $K^\times \backslash \widehat{K}^\times / \widehat{S}^\times$.

Section 2.2

Quaternion Algebras

2.2.1. Quaternion Algebras

Quaternion algebras appear frequently in number theory. For a thorough treatment of quaternion algebras, see Voight [20].

For this chapter, let F be a field with $\operatorname{char} F \neq 2$.

Definition 2.2.1. A *quaternion algebra* over F is an F-algebra B generated by elements $i, j \in B$ such that $\{1, i, j, ij\}$ is an F-basis for B and for some $a, b \in F^\times$,

$$i^2 = a, \quad j^2 = b, \quad ij = -ji.$$

Write $B = \left(\dfrac{a, b}{F}\right) = (a, b \mid F)$ for such a quaternion algebra.

Theorem 2.2.2. *A quaternion algebra B over F is a central simple algebra. That is, the center of B is $Z(B) = F$, and B has no nontrivial two-sided ideals.*

Proof. See [20, Cor 7.1.2]. □

For $\alpha = t + xi + yj + zij \in B$, define

$$\overline{\alpha} := t - xi - yj - zij.$$

Lemma 2.2.3. *For all $\alpha, \beta \in B$ and for all $x, y \in F$:*

(a) $\overline{x\alpha + y\beta} = x\overline{\alpha} + y\overline{\beta}$.

(b) $\overline{1} = 1$.

(c) $\overline{\overline{\alpha}} = \alpha$.

(d) $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$.

(e) $\alpha\overline{\alpha} = \overline{\alpha}\alpha \in F$.

(f) $\alpha + \overline{\alpha} \in F$.

Furthermore, the involution $\alpha \mapsto \overline{\alpha}$ is the unique such map satisfying (a)-(e).

Proof. See [20, 3.2.9]. □

This involution $\alpha \mapsto \overline{\alpha}$ is called a *standard involution*. Algebras with standard involutions have nice properties. For example, we can define trace and norm in the same way we did for imaginary quadratic fields.

Definition 2.2.4. Let $\alpha \in B$. The *reduced trace* of α is $\operatorname{trd}(\alpha) = \alpha + \overline{\alpha}$. The *reduced norm* of α is $\operatorname{nrd}(\alpha) = \alpha\overline{\alpha}$.

A few immediate observations can be made about the reduced trace and reduced norm. First of all, for any $\alpha \in B$,

$$0 = \alpha^2 - (\alpha + \overline{\alpha})\alpha + \alpha\overline{\alpha} = \alpha^2 - \operatorname{trd}(\alpha)\alpha + \operatorname{nrd}(\alpha).$$

So every $\alpha \in B$ satisfies a quadratic polynomial, and we say that the *degree* of B is 2. Note also that the reduced trace is F-linear, and the reduced norm is multiplicative: for all $\alpha, \beta \in B$,

$$\operatorname{nrd}(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\beta}\overline{\alpha} = \alpha \operatorname{nrd}(\beta)\overline{\alpha} = \alpha\overline{\alpha}\operatorname{nrd}(\beta) = \operatorname{nrd}(\alpha)\operatorname{nrd}(\beta).$$

Furthermore, we claim that the reduced norm identifies which elements of B are invertible. If $\alpha \in B$ has an inverse α^{-1}, then $\alpha\alpha^{-1} = 1$. But then $\operatorname{nrd}(\alpha)\operatorname{nrd}(\alpha^{-1}) = 1$ from which it follows that $\operatorname{nrd}(\alpha) \neq 0$. Conversely, if $\operatorname{nrd}(\alpha) \neq 0$, then $\operatorname{nrd}(\alpha)^{-1}\overline{\alpha}$ is a two-sided inverse for α.

2.2.2. Quaternion Orders

Just as we considered orders in imaginary quadratic fields, we want to consider analogous structures in quaternion algebras. Let $R \subset F$ be a Dedekind domain with field of fractions F.

Definition 2.2.5. Let V be a vector space over F. An *R-lattice* is a finitely-generated R-submodule $M \subset V$ such that $FM = V$. A $\mathbb{Z}$-lattice is also called a *lattice.*

Definition 2.2.6. Let B be a quaternion algebra over F. An *R-order* of B is lattice $O \subset B$ that is also a subring, i.e. closed under multiplication and contains 1. A $\mathbb{Z}$-order in a quaternion algebra over $\mathbb{Q}$ is also called an *order.* An R-order O is called *maximal* if it is maximal among all orders under containment. In other words, an order is maximal if and only if for all orders $O' \subset B$,

$$O \subseteq O' \implies O = O'.$$

It turns out that every element of an order O is integral [20, Cor 10.3.3]. However, the set of integral elements is in general not a subring of B: see [20, 10.1.1] for an explicit counterexample.

For notation, let

$$O^1 := \{\alpha \in O : \operatorname{nrd}(\alpha) = 1\}.$$

2.2.3. Localization and Completion in Quaternion Algebras

We define localizations and completions of lattices in B. Let B be a quaternion algebra over $\mathbb{Q}$ for the remainder of this section.

Definition 2.2.7. Let V be a $\mathbb{Q}$-vector space. The completion of V at p is

$$V_p := V \otimes_{\mathbb{Q}} \mathbb{Q}_p.$$

Let $M \subset V$ be a lattice, and let p be an integer prime. The *localization of M at p* is

$$M_{(p)} := \mathbb{Z}_{(p)} M \subset V.$$

The *completion of M at p* is

$$M_p := M_{(p)} \otimes_{\mathbb{Z}_{(p)}} \mathbb{Z}_p \subset V_p.$$

By extension of scalars, the completion $B_p := B \otimes_{\mathbb{Q}} \mathbb{Q}_p$ is naturally a quaternion algebra over $\mathbb{Q}_p$.

Lemma 2.2.8. *Suppose B_p is a division algebra. Then there is a valuation v_p on B_p extending the p-adic valuation on $\mathbb{Q}_p$, given by*

$$v_p(\alpha) = \frac{v_p(\operatorname{nrd}(\alpha))}{2}.$$

Furthermore, the valuation ring

$$O_p := \{\alpha \in B_p : v_p(\alpha) \geq 0\}$$

consists of all elements of B_p that are integral over $\mathbb{Z}_p$, and is thus the unique maximal $\mathbb{Z}_p$-order of B_p. The ring O_p has a unique maximal ideal $P \subset O_p$, which is two-sided and satisfies $P^2 = pO_p$.

Proof. See [20, Lem 13.3.2] and [20, Prop 13.3.4] for the first part. For the statement about the maximal ideal of O_p, see [20, Thm 13.3.11]. □

Definition 2.2.9. Let B be a quaternion algebra over $\mathbb{Q}$. Let p be an integer prime. We say B is *ramified* at p if B_p is a division algebra. Otherwise, we say B_p is *unramified* (or *split*) at p. We say B is *ramified at infinity* (or *definite* if $B \otimes_{\mathbb{Q}} \mathbb{R}$ is a division algebra. Otherwise, we say B is *indefinite*.

Theorem 2.2.10. *Let B be a quaternion algebra over $\mathbb{Q}$. The following are true:*

(a) *B is ramified at finitely many primes.*

(b) *B is ramified at an even number of primes if and only if B is indefinite.*

(c) *If B is split at p, then $B_p \cong \mathrm{M}_2(\mathbb{Q}_p)$.*

(d) *If B is definite, then $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$, where $\mathbb{H}$ is Hamilton's quaternions.*

(e) *If B is indefinite, then $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$.*

(f) *If B_p is a division algebra, then it is isomorphic to the unique division quaternion algebra over $\mathbb{Q}_p$.*

Proof. For (a), see [20, Lem 14.5.3]. For (b), see [20, Cor 14.6.2]. For (c) and (e), see [20, Prop 7.6.2]. For (d), see [20, Cor 3.5.8]. For (f), see [20, Thm 13.3.11]. □

Definition 2.2.11. Let B be a quaternion algebra over $\mathbb{Q}$. The *discriminant* of B is the product of all primes that are ramified in B.

Theorem 2.2.12. *Let Δ be a squarefree positive integer. Then there is a unique quaternion algebra B over $\mathbb{Q}$ with discriminant Δ.*

Proof. See [20, Thm 14.6.1]. □

Theorem 2.2.12 tells us that it is enough to look locally at each prime to determine a quaternion algebra's isomorphism class. The *Hilbert symbol* gives a quick way to compute what happens at each prime. For $a, b \in \mathbb{Z}$, we define $(a, b)_p$ to be 1 if $(a, b \mid \mathbb{Q})$ is split at p, and -1 if $(a, b \mid \mathbb{Q})$ is ramified at p. We also define $(a, b)_\infty$ to be 1 if $(a, b \mid \mathbb{Q})$ is indefinite, and -1 if $(a, b \mid \mathbb{Q})$ is definite. Some quick ways to calculate these symbols are given in [20, §12.4].

2.2.4. The Atkin-Lehner Group

Definition 2.2.13. Let O be an order of a quaternion algebra B over $\mathbb{Q}$. The *Atkin-Lehner group* of O is

$$\mathrm{AL}(O) := N_{B^\times}(O)/\mathbb{Q}^\times O^\times.$$

Proposition 2.2.14. *Suppose B is an indefinite quaternion algebra over $\mathbb{Q}$. Let Δ be the discriminant of B, and let n be the number of primes dividing Δ. Then*

$$\mathrm{AL}(O) \cong \prod_{r=1}^{n} \mathbb{Z}/2\mathbb{Z}.$$

Furthermore, any element of $\mathrm{AL}(O)$ can be represented by an element $\omega_d \in N_{B^\times}(O) \cap O$ such that $\mathrm{nrd}(\omega_d) = d \mid \Delta$.

Proof. See [15, Def 3.1], combined with the fact from [20, 43.7.1] that there exists $\epsilon \in O^\times$ such that $\mathrm{nrd}(\epsilon) = -1$. □

2.2.5. Adelic Quaternions

We will need some adelic technology for our quaternions. Let B be a quaternion algebra over $\mathbb{Q}$ and let $O \subset B$ be an order. We define the *adele ring* of B to be

$$\widehat{B} := \{(\alpha_p)_p \in \prod_p B_p : \alpha_p \in O_p \text{ for all but finitely many } p\}.$$

Just as before, we are concerned with the *idele group* $\widehat{B}^\times$ and the *adele ring of* O, defined as

$$\widehat{O} := \prod_p O_p \subset \widehat{B}.$$

We can recover O from $\widehat{O}$, as explained in the following lemma.

Lemma 2.2.15. *We have*

$$O = \widehat{O} \cap B.$$

Proof. This is a consequence of [20, Lem 9.5.2]. □

Just like with imaginary quadratic orders, adeles can be used to represent quaternionic ideals.

Proposition 2.2.16. *Suppose B is indefinite and O is a maximal order in B. Then every invertible right O-ideal is principal, and $\#(B^\times \backslash \widehat{B}^\times / \widehat{O}^\times) = 1$. We say that O has class number 1.*

Proof. Invertible right O-ideals are locally principal by [20, Thm 16.6.1]. In this setting, locally principal right-ideals are also principal by [20, Thm 28.2.11]. The statement about double cosets comes from [20, Lem 27.6.8]. □

2.2.6. Optimal Embeddings

Given an imaginary quadratic order S, we would like to consider embeddings of S into a maximal order $O \subset B$ that are well-behaved in terms of extension and restriction of scalars. We start more generally: suppose B is a quaternion algebra over a field F with $\operatorname{char} F \neq 2$, and suppose $R \subset F$ a Dedekind domain with field of fractions F. Let $O \subset B$ be a maximal R-order.

We need one basic fact about embeddings of quadratic algebras.

Lemma 2.2.17. *Suppose K is a separable quadratic F-algebra, and suppose there exists an embedding $K \hookrightarrow B$ under which we identify K as a subring of B. Then the following are true:*

(a) *The centralizer of K in B is $C_{B^\times}(K) = K^\times$.*

(b) *For all embeddings $\phi : K \hookrightarrow B$, there exists $\beta \in B^\times$ such that $\phi(\alpha) = \beta^{-1}\alpha\beta$ for all $\alpha \in K$.*

(c) *With the fixed embedding $K \hookrightarrow B$, the set of all embeddings of K into B is identified with $K^\times \backslash B^\times$, where $K^\times\beta$ is identified with the embedding $\alpha \mapsto \beta^{-1}\alpha\beta$.*

Proof. This is explained in [20, 30.3.1]. □

Let K be a quadratic field extension of F, and let $S \subset K$ be an R-order. Given an embedding $S \hookrightarrow O$, we get an embedding $K \hookrightarrow B$ by extending scalars (tensoring with F).

Definition 2.2.18. An embedding $\iota : S \hookrightarrow O$ is called *optimal* if

$$\iota(K) \cap O = \iota(S).$$

We denote the set of optimal embeddings $S \hookrightarrow O$ by $\mathrm{Emb}(S, O)$.

Suppose Γ is a group with $O^1 \leq \Gamma \leq N_{B^\times}(O)$. We say that two embeddings $\iota, \iota' : S \hookrightarrow O$ are Γ-*equivalent* if there exists $\gamma \in \Gamma$ such that

$$\iota'(\alpha) = \gamma^{-1}\iota(\alpha)\gamma$$

for all $\alpha \in K$. We denote the set of Γ-equivalence classes of optimal embeddings by $\mathrm{Emb}(S, O; \Gamma)$.

Lemma 2.2.19. *Any embedding that is Γ-equivalent to an optimal embedding is optimal.*

Proof. Suppose $\iota : S \hookrightarrow O$ is an optimal embedding, and suppose $\iota' : S \hookrightarrow O$ is a Γ-equivalent embedding. Then for some $\gamma \in N_{B^\times}(O)$ and some embeddings $\iota, \iota' : S \hookrightarrow O$,

$$\iota'(\alpha) = \gamma^{-1}\iota(\alpha)\gamma$$

for all $\alpha \in K$. We see that

$$\iota'(S) = \gamma^{-1}\iota(S)\gamma = \gamma^{-1}\iota(K)\gamma \cap \gamma^{-1}O\gamma = \iota'(K) \cap O. \qquad \square$$

For the remainder of the section, we suppose there is an optimal embedding $S \hookrightarrow O$ by which we identify S as a subring of O. Let

$$E := \{\beta \in B^\times : \beta^{-1}K\beta \cap O = \beta^{-1}S\beta\}.$$

Lemma 2.2.20. *Suppose $O^1 \leq \Gamma \leq N_{B^\times}(O)$. There is a bijection*

$$\mathrm{Emb}(S, O; \Gamma) \longleftrightarrow K^\times \backslash E / O^\times$$

that associates $K^\times\beta O^\times$ with the embedding $\alpha \mapsto \beta^{-1}\alpha\beta$.

Proof. See [20, 30.3.13]. □

Section 2.3

QM Abelian Surfaces

The objects which our main results are concerned with are abelian surfaces. Though there is a more general notion of a *complex abelian variety* at work, we restrict to complex tori of dimension 2.

Definition 2.3.1. A *(complex) abelian surface* A is a $A = \mathbb{C}^2/\Lambda$, where Λ is a lattice of rank 4 in $\mathbb{C}$, such that there exists a holomorphic embedding $A \hookrightarrow \mathbb{P}^n(\mathbb{C})$ for some $n \geq 1$.

An abelian surface A is said to be *polarized* if the lattice Λ is equipped with a *Riemann form*, and A is *principally polarized* if the Riemann form has a representing matrix of a certain form. An abelian surface also comes with an involution called the *Rosati involution.*

The details of principal polarization and the Rosati involution are not relevant to this thesis: see [20, §43.4] for details.

The abelian surfaces we want to consider are equipped with extra structure beyond just being abelian varieties. Specifically, they have a guaranteed amount of "symmetry," measured by quaternions. For the remainder of this section, let B be an indefinite quaternion algebra over $\mathbb{Q}$ with discriminant Δ, and let O be a maximal order in B. We fix a *polarization* of O, meaning a choice of $\mu \in O$ such that $\mu^2 + \Delta = 0$. Then O has an involution given by

$$\alpha \mapsto \mu^{-1}\overline{\alpha}\mu.$$

Definition 2.3.2. An abelian surface A is said to have *quaternionic multiplication* or *QM* if both of the following are true:

(a) $B \cong \mathrm{End}(A) \otimes \mathbb{Q}$ is an indefinite quaternion algebra over $\mathbb{Q}$.

(b) There exists an embedding $\iota : O \hookrightarrow \mathrm{End}(A)$ that respects the involutions of O and $\mathrm{End}(A)$, i.e. involuting O then passing to $\mathrm{End}(A)$ is the same as passing from O to $\mathrm{End}(A)$ then involuting.

We call ι a *QM structure* on A, and say that A is a *QM abelian surface*.

If we fix an embedding $\iota_\infty : B \hookrightarrow B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$ and a point $z \in \mathbb{C} \setminus \mathbb{R}$, we get a lattice

$$\Lambda_z := \iota_\infty(O)\begin{pmatrix} z \\ 1 \end{pmatrix} \subset \mathbb{C}^2.$$

We define $A_z := \mathbb{C}^2/\Lambda_z$. Then A_z is a principally polarized abelian surface, and ι_∞ induces an embedding $\iota : O \hookrightarrow \mathrm{End}(A)$ that is a QM structure on A [20, 43.6.12].

We will want to focus on A_z for certain values of z.

Lemma 2.3.3. *There is an action of $B^\times$ on complex numbers. Given $z \in \mathbb{C}\backslash\mathbb{R}$ and $\xi \in B^\times$,* *if* $\iota_\infty(\xi) = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix}$, *then the action is given by*

$$\xi \cdot z = \frac{a_0 z + b_0}{c_0 z + d_0}.$$

Furthermore, if $z \in \mathfrak{H}$ *and* $\operatorname{nrd}(\xi) > 0$*, then* $\xi \cdot z \in \mathfrak{H}$*. If* $\operatorname{Im}(z) < 0$ *and* $\operatorname{nrd}(\xi) < 0$*, then* $\xi \cdot z \in \mathfrak{H}$*.*

Proof. See [20, §33.3]. □

Definition 2.3.4. Suppose K is an imaginary quadratic field with an order $S = \mathbb{Z}[\nu]$ that is optimally embedded in O. By [20, 43.7.4], ν has a unique fixed point in $\mathfrak{H}$, called a *CM point* for S.

We will say that an abelian surface which arises as A_z for z a CM point for S has *CM by* S.

Chapter 3

Proof of Main Results

Section 3.1

Overview

Throughout this chapter, let O be a maximal order in an indefinite quaternion algebra B with discriminant Δ over $\mathbb{Q}$, and let $S = \mathbb{Z}[\nu]$ be an imaginary quadratic order over $\mathbb{Z}$ with discriminant D and field of fractions K. Let H be the ring class field of K associated to S. In this chapter, we precisely determine the fields of moduli of principally polarized abelian surfaces with QM by O and CM by S. We accomplish this by transforming questions about fields of moduli into problems about optimal embeddings of S into O. We propose that there is a bijection

$$\mathcal{A} := \begin{bmatrix} (A, \iota) \text{ principally polarized} \\ \text{abelian surfaces with QM by } O \\ \text{and CM by } S \\ \text{up to isomorphism preserving QM} \end{bmatrix} \longleftrightarrow \operatorname{Emb}(S, O; O^\times).$$

We will see that $\mathrm{Gal}(H \mid \mathbb{Q})$ acts on $\mathrm{Emb}(S, O; O^\times)$ in a way that agrees with the action of $\mathrm{Gal}(H \mid \mathbb{Q})$ on $\mathcal{A}$. There is also an action of $\mathrm{AL}(O)$ on $\mathrm{Emb}(S, O; O^\times)$, and the orbits of various subgroups correspond with "weak" isomorphism classes of abelian surfaces in $\mathcal{A}$. The "weak" isomorphisms being considered in this thesis are isomorphisms of principally polarized abelian surfaces that do not preserve the whole QM structure, but preserve endomorphisms by some subring of O.

The group $\mathrm{Gal}(H \mid \mathbb{Q})$ can be realized as a semidirect product:

$$\mathrm{Gal}(H \mid \mathbb{Q}) \cong \mathrm{Gal}(H \mid K) \rtimes \mathrm{Gal}(K \mid \mathbb{Q}).$$

This isomorphism can be arranged so that the nontrivial element of $\mathrm{Gal}(K \mid \mathbb{Q})$ corresponds to some $\sigma_C \in \mathrm{Gal}(H \mid \mathbb{Q})$ that represents "complex conjugation" to H. Furthermore, H is by definition the ring class field of K associated to S, so $\mathrm{Gal}(H \mid K) \cong \mathrm{Pic}(S)$. In Section 3.2, we will describe an action of $\mathrm{Pic}(S)$ on $\mathrm{Emb}(S, O; O^\times)$. In Section 3.3, we will describe an action of complex conjugation on $\mathrm{Emb}(S, O; O^\times)$. Finally, in Section 3.4, we will put these actions together to give an action of $\mathrm{Gal}(H \mid \mathbb{Q})$ on $\mathrm{Emb}(S, O; O^\times)$. We will show that this action agrees with the corresponding action on abelian surfaces, and draw conclusions about fields of moduli.

Section 3.2

The Action of $\mathrm{Pic}(S)$ on $\mathrm{Emb}(S, O; O^\times)$

3.2.1. Acting Locally, Then Globally

Recall from Lemma 2.2.20 that $\mathrm{Emb}(S, O; O^\times)$ is naturally identified with $K^\times \backslash E / O^\times$, where

$$E := \{\beta \in B^\times : \beta^{-1} K \beta \cap O = \beta^{-1} S \beta\}.$$

Sometimes, however, it is convenient to be able to consider the local behavior of embeddings simultaneously using adelic language. We define

$$\widehat{E} := \{\widehat{\beta} \in \widehat{B}^\times : \widehat{\beta}^{-1}\widehat{K}\widehat{\beta} \cap \widehat{O} = \widehat{\beta}^{-1}\widehat{S}\widehat{\beta}\}$$

and define $\mathrm{Emb}(\widehat{S}, \widehat{O}; \widehat{O}^\times) := \widehat{K}^\times\backslash\widehat{E}/\widehat{O}^\times$. These double cosets are well-defined in $\widehat{E}$ in the same way that $K^\times\backslash E/O^\times$ is well-defined (see [20, 30.4.5]).

In order to define an action of $\mathrm{Pic}(S)$ on $\mathrm{Emb}(S, O; O^\times)$, we first define an action of $\mathrm{Pic}(S)$ on a related set that is easier to manage. Recall from Proposition 2.1.24 that $\mathrm{Pic}(S)$ is naturally identified with $K^\times\backslash\widehat{K}/\widehat{S}^\times$.

Lemma 3.2.1. *There is a free action of* $\mathrm{Pic}(S)$ *on* $K^\times\backslash\widehat{E}/\widehat{O}^\times$ *given by left multiplication of coset representatives, i.e.*

$$\begin{aligned} K^\times\backslash\widehat{K}^\times/\widehat{S}^\times &\circlearrowleft K^\times\backslash\widehat{E}/\widehat{O}^\times \\ K^\times\widehat{\alpha}\widehat{S}^\times \cdot K^\times\widehat{\beta}\widehat{O}^\times &= K^\times\widehat{\alpha}\widehat{\beta}\widehat{O}^\times. \end{aligned}$$

See [20, Corollary 30.4.23] for a more general statement.

Proof. This action is well-defined: for $\alpha_1, \alpha_2 \in K^\times$, $\widehat{\alpha} \in \widehat{K}^\times$, $\widehat{u} \in \widehat{S}^\times$, $\widehat{\beta} \in \widehat{E}$, and $\widehat{\epsilon} \in \widehat{O}^\times$,

$$(\alpha_1\widehat{\alpha}\widehat{u})(\alpha_2\widehat{\beta}\widehat{\epsilon}) = \alpha_1\alpha_2\widehat{\alpha}\widehat{u}\widehat{\beta}\widehat{\epsilon} = \alpha_1\alpha_2\widehat{\alpha}\widehat{\beta}(\widehat{\beta}^{-1}\widehat{u}\widehat{\beta})\widehat{\epsilon},$$

where $\alpha_1\alpha_2 \in K^\times$ and $\widehat{\beta}^{-1}\widehat{u}\widehat{\beta} \in \widehat{O}^\times$ by definition of $\widehat{E}$. We also have

$$\widehat{\beta}^{-1}\widehat{\alpha}^{-1}\widehat{K}\widehat{\alpha}\widehat{\beta} \cap \widehat{O} = \widehat{\beta}^{-1}\widehat{K}\widehat{\beta} \cap \widehat{O} = \widehat{\beta}^{-1}\widehat{S}\widehat{\beta} = \widehat{\beta}^{-1}\widehat{\alpha}^{-1}\widehat{S}\widehat{\alpha}\widehat{\beta},$$

so $\widehat{\alpha}\widehat{\beta} \in \widehat{E}$.

It remains to show that the action is free. Suppose that for some $\widehat{\alpha} \in \widehat{K}^\times$, $\widehat{\beta} \in \widehat{E}$,

$$K^\times \widehat{\alpha}\widehat{\beta}\widehat{O}^\times = K^\times \widehat{\beta}\widehat{O}^\times.$$

Then for some $\alpha \in K^\times$ and some $\widehat{\epsilon} \in \widehat{O}^\times$,

$$\widehat{\alpha}\widehat{\beta} = \alpha\widehat{\beta}\widehat{\epsilon}.$$

Then, since $\widehat{\beta} \in \widehat{E}$, we have

$$\alpha^{-1}\widehat{\alpha} = \widehat{\beta}\widehat{\epsilon}\widehat{\beta}^{-1} \in \widehat{K}^\times \cap \widehat{\beta}\widehat{O}^\times\widehat{\beta}^{-1} = \widehat{S}^\times.$$

But then $K^\times\widehat{\alpha}\widehat{S}^\times = K^\times\alpha\widehat{S}^\times = K^\times 1\widehat{S}^\times$ corresponds to the trivial element in $\mathrm{Pic}(S)$, so the action is free. $\square$

We now want to lift this to a global action on $\mathrm{Emb}(S, O; O^\times)$. We are already not too far away, since the sets $K^\times\backslash E/O^\times$ and $K^\times\backslash\widehat{E}/\widehat{O}^\times$ are naturally in bijection.

Lemma 3.2.2. *There is a bijection*

$$G : K^\times\backslash E/O^\times \longleftrightarrow K^\times\backslash\widehat{E}/\widehat{O}^\times$$
$$K^\times\beta O^\times \mapsto K^\times\beta\widehat{O}^\times.$$

Proof. Since O has class number 1, we have $\#(B^\times\backslash\widehat{B}^\times/\widehat{O}^\times) = 1$. In other words, for all $\widehat{\beta} \in \widehat{B}^\times$, we have $\widehat{\beta} = \beta\widehat{\epsilon}$ for some $\beta \in B^\times$ and $\widehat{\epsilon} \in \widehat{O}^\times$. Concretely, if $\widehat{\beta}\widehat{O}^\times$ gives a right ideal $I \subseteq O$, then $\widehat{\beta}\widehat{O} = \beta\widehat{O}$, so $I = \widehat{\beta}\widehat{O} \cap B = \beta O$, so β is well-defined up to right multiplication by $O^\times$. This establishes a bijection

$$\widehat{B}^\times/\widehat{O}^\times \leftrightarrow B^\times/O^\times.$$

Let $\widehat{\beta} = \beta\widehat{\epsilon}$ for some $\beta \in E$ and $\widehat{\epsilon} \in \widehat{O}^\times$. We have $\widehat{\beta} \in \widehat{E}$ if and only if

$$\widehat{K} \cap \beta\widehat{O}\beta^{-1} = \widehat{K} \cap \beta\widehat{\epsilon}\widehat{O}\widehat{\epsilon}^{-1}\beta^{-1} = \widehat{K} \cap \widehat{\beta}\widehat{O}\widehat{\beta}^{-1} = \widehat{S}.$$

By intersecting the above equation with B, we see that

$$K \cap \beta O \beta^{-1} = S,$$

so $\beta \in E$. Conversely, if $\beta \in E$, then $\beta \in \widehat{E}$ by looking at completions in the equation $K \cap \beta O \beta^{-1} = S$.

At this point we have shown that the inclusion $E \hookrightarrow \widehat{E}$ induces a surjection

$$E/O^\times \to \widehat{E}/\widehat{O}^\times.$$

Then there is a surjection

$$K^\times \backslash E/O^\times \to K^\times \backslash \widehat{E}/\widehat{O}^\times.$$

We claim that this map is injective. Given $\beta_1, \beta_2 \in E$, suppose that $K^\times\beta_1\widehat{O}^\times = K^\times\beta_2\widehat{O}^\times$. Then for some $\alpha \in K^\times$,

$$\alpha\beta_1 \in \beta_2\widehat{O}^\times.$$

Then by Lemma 2.2.15,

$$\beta_2^{-1}\alpha\beta_1 \in \widehat{O}^\times \cap B = O^\times.$$

So

$$\alpha\beta_1 O^\times = \beta_2 O^\times,$$

and hence

$$K^\times\beta_1 O^\times = K^\times\beta_2 O^\times. \qquad \square$$

Corollary 3.2.3. *There exists a free action of* $\mathrm{Pic}(S)$ *on* $\mathrm{Emb}(S, O; O^\times)$*.*

Proof. This follows from the fact that $\mathrm{Emb}(S, O; O^\times)$ is identified with $K^\times\backslash E/O^\times$ which is identified with $K^\times\backslash\widehat{E}/\widehat{O}^\times$ by the bijection in Lemma 3.2.2. Since $\mathrm{Pic}(S)$ acts on $K^\times\backslash\widehat{E}/\widehat{O}^\times$ freely, the bijection gives a free action on $\mathrm{Emb}(S, O; O^\times)$.

What does this action actually look like globally? Take an ideal $\mathfrak{a} \subseteq S$ defining an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(S)$, and take some $\beta \in E$. What is $[\mathfrak{a}] \cdot K^\times\beta O^\times$? We know that $K^\times\beta O^\times$ corresponds to $K^\times\beta\widehat{O}^\times$. Adelically, $\mathfrak{a}$ is locally principal, so $\mathfrak{a} = \widehat{\alpha}\widehat{S} \cap K$ for some $\widehat{\alpha} \in \widehat{K}^\times$. We represent $[\mathfrak{a}]$ as $K^\times\widehat{\alpha}\widehat{S}^\times$. Then $[\mathfrak{a}]$ acts on $K^\times\beta O^\times$ to give $K^\times\widehat{\alpha}\beta\widehat{O}^\times \in K^\times\backslash\widehat{E}/\widehat{O}^\times$. What element does this correspond to in $K^\times\backslash E/O^\times$? Since O has class number 1, there exists $\xi \in O$ such that $\beta^{-1}\mathfrak{a}\beta O = \xi O$. Completing at every prime gives $\beta^{-1}\widehat{\alpha}\beta\widehat{O} = \xi\widehat{O}$: we have $\mathfrak{a}\widehat{S} = \widehat{\alpha}\widehat{S}$, and $\beta^{-1}\widehat{S}\beta \subset \widehat{O}$, so

$$\xi\widehat{O} = \beta^{-1}\mathfrak{a}\beta\widehat{O} = \beta^{-1}\mathfrak{a}\widehat{S}\beta\widehat{O} = \beta^{-1}\widehat{\alpha}\widehat{S}\beta\widehat{O} = \beta^{-1}\widehat{\alpha}\beta\widehat{O}.$$

Then $\widehat{\alpha}\beta\widehat{O}^\times = \beta\xi\widehat{O}^\times$. In particular, $\beta\xi \in \widehat{E} \cap B^\times = E$. Then $K^\times\beta\xi O^\times$ corresponds with $K^\times\beta\xi\widehat{O}^\times = K^\times\widehat{\alpha}\beta\widehat{O}^\times$.

Putting all of the above together, we have that $\mathrm{Pic}(S)$ acts freely on $\mathrm{Emb}(S, O; O^\times)$ as

$$[\mathfrak{a}] \cdot K^\times\beta O^\times = K^\times\beta\xi O^\times,$$

where $[\mathfrak{a}] \in \mathrm{Pic}(S)$, $\beta \in E$, and $\xi \in O$ is such that $\beta^{-1}\mathfrak{a}\beta O = \xi O$. □

We will see in Section 3.4 that this action agrees with the action of $\mathrm{Pic}(S)$ on $\mathcal{A}$ described by Shimura Reciprocity.

If we look at the global description of that action of $\mathrm{Pic}(S)$ above, it might look like a right action: we are multiplying an element $\beta \in E$ on the right by an element $\xi \in O$. However, the element $\xi \in O$ depends not just on $\mathfrak{a}$, but β as well. Let $\beta \in E$, $[\mathfrak{a}] \in \mathrm{Pic}(S)$, and $\xi \in O$ such that $\xi O = \beta^{-1}\mathfrak{a}\beta O$. Consider $[\mathfrak{b}] \in \mathrm{Pic}(S)$, and suppose we principalize ideals to get $\xi \in O$ such that

$$(\xi^{-1}\beta^{-1}\mathfrak{b}\beta\xi)O = \xi' O.$$

Then $\mathfrak{b}$ acts on $K^\times\beta\xi O^\times$ to give $K^\times\beta\xi\xi' O^\times$. On the other hand, if we look at the right ideal $(\beta^{-1}\mathfrak{b}\mathfrak{a}\beta)O$, we have

$$(\beta^{-1}\mathfrak{b}\mathfrak{a}\beta)O = (\beta^{-1}\mathfrak{b}\beta\beta^{-1}\mathfrak{a}\beta)O = (\beta^{-1}\mathfrak{b}\beta\xi)O = \xi\xi' O.$$

So $\mathfrak{b}\mathfrak{a}$ acts on $K^\times\beta O^\times$ to give $K^\times\beta\xi\xi' O^\times$.

Although we know from Lemma 3.2.1 that the action is free, we might want to check this from the explicit global description. Suppose that $[\mathfrak{a}] \cdot K^\times\beta O^\times = K^\times\beta O^\times$. Then $K^\times\beta\xi O^\times = K^\times\beta O^\times$. Then $\beta\xi = \alpha\beta\epsilon$ for some $\alpha \in K^\times$ and $\epsilon \in O^\times$. Then $\xi = \beta^{-1}\alpha\beta\epsilon$, so

$$(\beta^{-1}\mathfrak{a}\beta)O = \xi O = (\beta^{-1}\alpha\beta)O.$$

Then for all $x \in \mathfrak{a}$, there exists $y \in O$ such that

$$\beta^{-1}x\beta = \beta^{-1}\alpha\beta y \implies x = \alpha\beta y\beta^{-1}.$$

So

$$\alpha^{-1}x = \beta y\beta^{-1} \in \beta O\beta^{-1} \cap K = S$$

and $x \in \alpha S$. Conversely, $\beta^{-1}\alpha\beta = \beta^{-1}x\beta y$ for some $x \in \mathfrak{a}$ and $y \in O$. Then

$$\beta y\beta^{-1} = x^{-1}\alpha \in \beta O\beta^{-1} \cap K = S,$$

and

$$\alpha \in xS \subseteq \mathfrak{a}.$$

So $\mathfrak{a} = \alpha S$ is principal, and $[\mathfrak{a}] = [S] \in \mathrm{Pic}(S)$ is trivial.

3.2.2. The Action of $\mathrm{Pic}(S)$ Versus the Action of $\mathrm{AL}(O)$

Recall from Definition 2.2.13 that we have the *Atkin-Lehner group of O* given by

$$\mathrm{AL}(O) := N_{B^\times}(O)/\mathbb{Q}^\times O^\times.$$

For $\omega \in N_{B^\times}(O)$, we write $[\omega] := \omega\mathbb{Q}^\times O^\times$ for short.

Lemma 3.2.4. *The Atkin-Lehner group acts on* $\mathrm{Emb}(S, O; O^\times)$ *on the right: for $\beta \in E$ and $\omega \in N_{B^\times}(O)$,*

$$(K^\times \beta O^\times)^{[\omega]} := K^\times \beta\omega O^\times.$$

Proof. First, we show the action is well-defined. Let $\beta \in E$ and $[\omega] \in \mathrm{AL}(O)$. Given any $\alpha \in K^\times$, $\epsilon_1, \epsilon_2 \in O^\times$, and $q \in \mathbb{Q}^\times$,

$$(K^\times \alpha\beta\epsilon_1 O^\times)^{[\omega q \epsilon_2]} = K^\times \alpha\beta\epsilon_1\omega q\epsilon_2 O^\times.$$

The rational number q commutes with everything, and $\epsilon_1\omega = \omega\epsilon_1'$ for some $\epsilon_1' \in O^\times$ since $\omega^{-1}O^\times\omega = O^\times$, so

$$(K^\times \alpha\beta\epsilon_1 O^\times)^{[\omega q \epsilon_2]} = K^\times q\alpha\beta\omega\epsilon_1'\epsilon_2 O^\times = K^\times \beta\omega O^\times = (K^\times \beta O^\times)^{[\omega]}.$$

Furthermore, this really is a right action: for $[\omega'] \in \mathrm{AL}(O)$, we have

$$((K^\times \beta O^\times)^{[\omega]})^{[\omega']} = (K^\times \beta\omega O^\times)^{[\omega']} = K^\times \beta\omega\omega' O^\times = (K^\times \beta O^\times)^{[\omega\omega']},$$

and

$$(K^\times \beta O^\times)^{[1]} = K^\times \beta 1 O^\times = K^\times \beta O^\times.$$

$\square$

We care how the action of $\mathrm{AL}(O)$ interacts with the action of $\mathrm{Pic}(S)$. A basic fact we will need is that the two actions commute.

Lemma 3.2.5. *The (left) action of* $\mathrm{Pic}(S)$ *is compatible with the (right) action of* $\mathrm{AL}(O)$ *on* $\mathrm{Emb}(S, O; O^\times)$*. That is, for all* $[e] \in \mathrm{Emb}(S, O; O^\times)$*,* $[\omega] \in \mathrm{AL}(O)$*, and* $[\mathfrak{a}] \in \mathrm{Pic}(S)$*,*

$$[\mathfrak{a}] \cdot \big((K^\times \beta O^\times)^{[\omega]}\big) = ([\mathfrak{a}] \cdot K^\times \beta O^\times)^{[\omega]}.$$

Proof. If we act first by $[\mathfrak{a}] \in \mathrm{Pic}(S)$ then by $[\omega] \in \mathrm{AL}(O)$, we get $K^\times \beta\xi\omega O^\times$, where $\xi \in O$ is such that $(\beta^{-1}\mathfrak{a}\beta)O = \xi O$. If we act first by $[\omega]$, we get $K^\times \beta\omega O^\times$. Consider the right ideal $(\omega^{-1}\beta^{-1}\mathfrak{a}\beta\omega)O$. We have

$$(\omega^{-1}\beta^{-1}\mathfrak{a}\beta\omega)O = \omega^{-1}((\beta^{-1}\mathfrak{a}\beta)O)\omega = \omega^{-1}(\xi O)\omega = \omega^{-1}\xi\omega O.$$

So

$$[\mathfrak{a}] \cdot K^\times \beta\omega O^\times = K^\times \beta\omega\omega^{-1}\xi\omega O^\times = K^\times \beta\xi\omega O^\times = (K^\times \beta\xi O^\times)^{[\omega]}.$$

But the left hand side of this equation is $[\mathfrak{a}] \cdot \big((K^\times \beta O^\times)^{[\omega]}\big)$ and the right hand side is $([\mathfrak{a}] \cdot K^\times \beta O^\times)^{[\omega]}$, so the two actions are compatible. $\square$

To completely understand how the action of $\mathrm{Pic}(S)$ relates to the action of $\mathrm{AL}(O)$, we need to know when an Atkin-Lehner element acts the same as an ideal class on embeddings. First, we need a lemma.

Lemma 3.2.6. *Let d be a positive integer dividing Δ, the discriminant of B. Then there exists a unique right ideal $I \subseteq O$ with $\operatorname{nrd}(I) = d\mathbb{Z}$. In fact, I is a two-sided ideal.*

Proof. Recall from Proposition 2.2.14 that there exists $\omega_d \in N_{B^\times}(O)$ such that $\operatorname{nrd}(\omega_d) = d$. Then $\operatorname{nrd}(\omega_d O) = d\mathbb{Z}$, so a right ideal of norm d exists, and since $\omega_d O = O\omega_d$, this ideal happens to be two-sided. The main content of this proof is to show that there are no other right ideals with the same norm.

Suppose $I \subseteq O$ is a right ideal with $\operatorname{nrd}(I) = d\mathbb{Z}$. Note that since O is maximal, the right order of I is O. Then I is a lattice in B (a sublattice of O, since $I\mathbb{Q} = O\mathbb{Q} = B$). By the local-global dictionary for lattices (see [20, Lem 9.4.9]), it suffices to show that $I_{(p)}$ is uniquely determined for every prime p. By [20, Lem 9.5.2], we can equivalently show that I_p is uniquely determined. We know that $d \in I$, so that $d \in I_{(p)}$ for every prime p. But $I_{(p)}$ is a right ideal of $O_{(p)}$ in which d is a unit if $p \nmid d$. So $I_{(p)} = O_{(p)}$ for $p \nmid d$. For $p \mid d$, since $I_{(p)} = \mathbb{Z}_{(p)} I$, we have that $\operatorname{nrd}(I_{(p)}) = \operatorname{nrd}(I)\mathbb{Z}_{(p)} = d\mathbb{Z}_{(p)} = p\mathbb{Z}_{(p)}$ since every other prime dividing d is a unit in $\mathbb{Z}_{(p)}$ and d is squarefree. Furthermore, $p \mid \Delta$ since $d \mid \Delta$.

The $\mathbb{Z}_{(p)}$-order $O_{(p)}$ is maximal. We know that B is ramified at p, so B_p is a division algebra over $\mathbb{Q}_p$. We know that $\mathbb{Z}_p$ is a complete DVR with field of fractions $\mathbb{Q}_p$ and uniformizer p. Extending the valuation on $\mathbb{Q}_p$ to B_p makes B_p into a DVR with some valuation ring O_p that is the unique maximal $\mathbb{Z}_p$-order in B_p. The unique maximal ideal $\mathfrak{m}$ of O_p satisfies $\mathfrak{m}^2 = pO_p$. We claim that $\mathfrak{m} = I_p$ really is the completion of I at p. We know that $I_p \subsetneq \mathfrak{m}$ because $\mathfrak{m}$ is the unique maximal ideal of O_p. By [20, 13.3.10], both $\mathfrak{m}$ and I_p are principally generated two-sided ideals, say $I_p = \alpha_p O_p$ and $\mathfrak{m} = \pi_p O_p$ for some $\alpha_p, \pi_p \in O_p$. So $\alpha_p = \pi_p x$ for some $x \in O_p$. But

$$p = \operatorname{nrd}(\alpha_p) = \operatorname{nrd}(\pi_p)\operatorname{nrd}(x) = p \operatorname{nrd}(x).$$

So $\operatorname{nrd}(x) = 1$, $x \in O_p^\times$, and $I_p = \alpha_p O_p = \pi_p O_p = \mathfrak{m}$. This shows that I_p was uniquely determined, which shows that $I_{(p)}$ was uniquely determined. Since we have shown this for all rational primes p, $I \subseteq O$ is uniquely determined by its norm. $\square$

With this lemma in hand, we can understand more about how the action of $\operatorname{AL}(O)$ is related to the action of $\operatorname{Pic}(S)$. For example, for a given Atkin-Lehner element, either everything is a fixed point or nothing is a fixed point.

Proposition 3.2.7. *If there exists $\alpha \in S$ such that $\operatorname{Nm}_{\mathbb{Q}}^{K}(\alpha) = d$, then $[\omega_d]$ acts trivially on $\operatorname{Emb}(S, O; O^\times)$. If no such α exists, then $[\omega_d]$ acts freely on $\operatorname{Emb}(S, O; O^\times)$.*

Proof. Suppose such an $\alpha \in S$ exists. Consider $\beta \in E$. We have $(\beta^{-1}\alpha\beta)O = \omega_d O$ by Lemma 3.2.6. Then

$$K^\times \beta O^\times = K^\times \alpha\beta O^\times = K^\times \beta\omega_d O^\times = (K^\times \beta O^\times)^{[\omega_d]}.$$

Now suppose $[\omega_d]$ has a fixed point $K^\times \beta O^\times$. So

$$K^\times \beta\omega_d O^\times = K^\times \beta O^\times.$$

Then $\beta\omega_d O^\times = \alpha\beta O^\times$ for some $\alpha \in K^\times$, so $\omega_d O^\times = \beta^{-1}\alpha\beta O^\times$. Comparing norms, we get that $\operatorname{Nm}_{\mathbb{Q}}^{K}(\alpha) = |\operatorname{nrd}(\omega_d)| = d$. We also have $\beta^{-1}\alpha\beta \in O \cap \beta^{-1}K\beta = \beta^{-1}S\beta$, so $\alpha \in S$. $\square$

Proposition 3.2.7 tells us when Atkin-Lehner elements act trivially. When do Atkin-Lehner elements act the same as an ideal class in $\operatorname{Pic}(S)$?

Proposition 3.2.8. *Suppose $d \mid \Delta$. If S has an ideal $\mathfrak{a}$ of norm d, then $\mathfrak{a}$ is invertible and $[\omega_d] \in \operatorname{AL}(O)$ acts as $[\mathfrak{a}] \in \operatorname{Pic}(S)$ on all of $\operatorname{Emb}(S, O; O^\times)$. That is, for all $\beta \in E$,*

$$(K^\times \beta O^\times)^{[\omega_d]} = [\mathfrak{a}] \cdot (K^\times \beta O^\times).$$

Conversely, if $(K^\times \beta O^\times)^{[\omega_d]} = [\mathfrak{a}] \cdot (K^\times \beta O^\times)$ *for some* $\beta \in E$ *and some* $[\mathfrak{a}] \in \operatorname{Pic}(S)$*, then* $[\mathfrak{a}]$ *can be represented by an ideal* $\mathfrak{b} \subseteq S$ *of norm* d*.*

Proof. Suppose an ideal $\mathfrak{a} \subseteq S$ has norm $d \mid \Delta$. Since S embeds optimally into O, by [20, Prop 30.5.3], for every prime p dividing Δ, we have S_p is integrally closed. Then p does not divide the conductor of S by Lemma 2.1.23. It follows that $\mathfrak{a}$ is relatively prime to the conductor of S, so is invertible, giving a well-defined ideal class $[\mathfrak{a}] \in \operatorname{Pic}(S)$. For all $\beta \in E$, $\beta^{-1}\mathfrak{a}\beta O = \omega_d O$ by Lemma 3.2.6. Then

$$(K^\times \beta O^\times)^{[\omega_d]} = K^\times \beta \omega_d O^\times = [\mathfrak{a}] \cdot (K^\times \beta O^\times).$$

For the second part of the proposition, suppose that for some $\beta \in E$ and some $[\mathfrak{a}] \in \operatorname{Pic}(S)$ we have

$$(K^\times \beta O^\times)^{[\omega_d]} = [\mathfrak{a}] \cdot (K^\times \beta O^\times).$$

Let $\xi \in O$ be such that $\beta^{-1}\mathfrak{a}\beta O = \xi O$. Then

$$K^\times \beta \omega_d O^\times = K^\times \beta \xi O^\times.$$

Then $\beta \omega_d O^\times = \alpha \beta \xi O^\times$ for some $\alpha \in K^\times$. Then

$$\omega_d O = \beta^{-1} \alpha \beta \xi O = (\beta^{-1} \alpha \mathfrak{a} \beta) O.$$

Then $d\mathbb{Z} = \operatorname{nrd}(\omega_d O) = \operatorname{nrd}(\beta^{-1}\alpha\mathfrak{a}\beta)\mathbb{Z} = \operatorname{nrd}(\alpha\mathfrak{a})\mathbb{Z}$, so $\operatorname{Nm}^K_{\mathbb{Q}}(\alpha\mathfrak{a}) = d$. All that remains is to show that $\mathfrak{b} := \alpha\mathfrak{a} \subseteq S$. But

$$\beta^{-1}\mathfrak{b}\beta \subset \omega_d O \subset O,$$

$$\beta^{-1}\mathfrak{b}\beta \subseteq \beta^{-1} K \beta \cap O = \beta^{-1} S \beta.$$

So $\mathfrak{b} \subseteq S$ and $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{b}) = d$. □

3.2.3. Counting Embeddings with Orbits

We have answered almost all questions about how the actions of $\mathrm{Pic}(S)$ and $\mathrm{AL}(O)$ interact on $\mathrm{Emb}(S, O; O^\times)$. We know that $\mathrm{Pic}(S)$ acts freely, so $\mathrm{Emb}(S, O; O^\times)$ is a disjoint union of $\mathrm{Pic}(S)$-orbits, each of size $\#\,\mathrm{Pic}(S)$. We also know when elements of $\mathrm{AL}(O)$ have fixed points or act within a $\mathrm{Pic}(S)$-orbit. The only question remaining is whether or not the action of $\mathrm{AL}(O)$ acts transitively on $\mathrm{Pic}(S)$-orbits. We will show that it does, and that the $\mathrm{Pic}(S)$-orbits are naturally labelled by adelic embeddings.

Let

$$\Omega(S, O) := \mathrm{Pic}(S) \backslash \mathrm{Emb}(S, O; O^\times)$$

be the set of $\mathrm{Pic}(S)$-orbits in $\mathrm{Emb}(S, O; O^\times)$.

Lemma 3.2.9. *The group* $\mathrm{AL}(O)$ *acts on* $\Omega(S, O)$ *on the right: for* $e \in \mathrm{Emb}(S, O; O^\times)$ *and* $[\omega] \in \mathrm{AL}(O)$, *the action is given by*

$$(\mathrm{Pic}(S) \cdot e)^{[\omega]} := \mathrm{Pic}(S) \cdot (e^{[\omega]}).$$

Proof. First, this is well-defined. Suppose $e \in \mathrm{Emb}(S, O; O^\times)$, $[\omega] \in \mathrm{AL}(O)$, and $[\mathfrak{a}] \in \mathrm{Pic}(S)$. Then by Lemma 3.2.5,

$$\mathrm{Pic}(S) \cdot ([\mathfrak{a}] \cdot e)^{[\omega]} = \mathrm{Pic}(S) \cdot ([\mathfrak{a}] \cdot e^{[\omega]}) = \mathrm{Pic}(S) \cdot e^{[\omega]}.$$

This really is an action because it is defined in terms of an action of $\mathrm{AL}(O)$ on $\mathrm{Emb}(S, O; O^\times)$: for $[\omega'] \in \mathrm{AL}(O)$,

$$((\mathrm{Pic}(S) \cdot e)^{[\omega]})^{[\omega']} = (\mathrm{Pic}(S) \cdot e^{[\omega]})^{[\omega']} = \mathrm{Pic}(S) \cdot (e^{[\omega]})^{[\omega']} = \mathrm{Pic}(S) \cdot e^{[\omega][\omega']}$$

$$= (\mathrm{Pic}(S) \cdot e)^{[\omega][\omega']},$$

and

$$(\mathrm{Pic}(S) \cdot e)^{[1]} = \mathrm{Pic}(S) \cdot e^{[1]} = \mathrm{Pic}(S) \cdot e. \qquad \square$$

We also already know that the fixed points of this action are.

Lemma 3.2.10. *Let t primes dividing Δ be ramified in S. Let $e \in \mathrm{Emb}(S, O; O^\times)$. Then*

$$\mathrm{Stab}_{\mathrm{AL}(O)}(\mathrm{Pic}(S) \cdot e) = \langle \omega_p : p \text{ divides } \Delta \text{ and is ramified in } S \rangle,$$

and this stabilizer has order 2^t.

Proof. By Proposition 2.2.14, an arbitrary element of $\mathrm{AL}(O)$ is represented by $\omega_d \in N_{B^\times}(O)$, where $\mathrm{nrd}(\omega_d) = d \mid \Delta$. Suppose that $[\omega_d] \in \mathrm{Stab}_{\mathrm{AL}(O)}(\mathrm{Pic}(S) \cdot e)$. In other words, $e^{[\omega_d]} = [\mathfrak{a}] \cdot e$ for some $[\mathfrak{a}] \in \mathrm{Pic}(S)$. By Proposition 3.2.8, we can take $\mathfrak{a}$ to be an ideal in S of norm d. By [7, Exc 7.26], $\mathfrak{a}$ is a product of prime ideals of S, and since d is squarefree, all of these primes must be ramified in S. Then

$$\omega_d = \prod_{p \mid \mathrm{Nm}^K_{\mathbb{Q}}(\mathfrak{a})} \omega_p.$$

Conversely, suppose $p \mid \Delta$ is ramified in S, and consider $\omega_p \in N_{B^\times}(O)$ such that $\mathrm{nrd}(\omega_p) = p$. Since p is ramified in S, S has an ideal of norm p. Then by Proposition 3.2.8, $e^{[\omega_p]} = [\mathfrak{a}] \cdot e$ for some $[\mathfrak{a}] \in \mathrm{Pic}(S)$. Then $[\omega_p] \in \mathrm{Stab}_{\mathrm{AL}(O)}(\mathrm{Pic}(S) \cdot e)$.

We have thus shown the first part of the lemma. For the second part, we recall from Proposition 2.2.14 that $\mathrm{AL}(O)$ is a vector space over $\mathbb{Z}/2\mathbb{Z}$ with a basis consisting of $[\omega_p] \in \mathrm{AL}(O)$ for $p \mid \Delta$. Then the subspace generated by $[\omega_p]$ for p ramified in S has dimension t, so has 2^t elements. $\square$

To get a better handle on embeddings, we consider their local behavior.

Lemma 3.2.11. *There is a well-defined surjective map*

$$L : K^\times \backslash E / O^\times \to \widehat{K}^\times \backslash \widehat{E} / \widehat{O}^\times,$$
$$K^\times \beta O^\times \mapsto \widehat{K}^\times \beta \widehat{O}^\times.$$

Proof. This map is well-defined because $K^\times \subset \widehat{K}^\times$ and $O^\times \subset \widehat{O}^\times$. This map is also surjective by the same proof in 3.2.2. □

How is this map related to the local embeddings? We have previously identified $K^\times \backslash E / O^\times$ with $\operatorname{Emb}(S, O; O^\times)$. We have also previously identified $\widehat{K}^\times \backslash \widehat{E} / \widehat{O}^\times$ with $\operatorname{Emb}(\widehat{S}, \widehat{O}; \widehat{O}^\times$, which is in turn identified with

$$\prod_{p \text{ prime}} \operatorname{Emb}(S_p, O_p; O_p^\times).$$

Given $\beta \in E$, we have an embedding $\phi : S = \mathbb{Z}[\nu] \hookrightarrow O$ given on generators by $\phi(\nu) = \beta^{-1}\nu\beta$. By extension of scalars, we get optimal embeddings $\phi_p : S_p \to O_p$ for each prime p, and these are still given on generators by $\phi_p(\nu) = \beta^{-1}\nu\beta$. So the product of the local embeddings is given by $\widehat{K}^\times \beta \widehat{O}^\times = L(K^\times \beta O^\times)$. This shows that the map L is just localization of global embeddings at every prime.

What are the fibers of the map L? It turns out they are exactly the $\operatorname{Pic}(S)$-orbits.

Lemma 3.2.12. *Let $L : K^\times \backslash E / O^\times \to \widehat{K}^\times \backslash \widehat{E} / \widehat{O}^\times$ be the map from Lemma 3.2.11, and let $\beta \in E$. Then the fibers of L are exactly the* Pic(S)*-orbits:*

$$L^{-1}(\widehat{K}^\times \beta \widehat{O}^\times) = \operatorname{Pic}(S) \cdot (K^\times \beta O^\times).$$

Proof. Recall the bijection G from Lemma 3.2.2. Let $\beta \in E$, and suppose that for some

$\beta' \in E$,

$$K^\times \beta' O^\times \in L^{-1}(\widehat{K}^\times \beta \widehat{O}^\times).$$

Then $\widehat{K}^\times \beta' \widehat{O}^\times = \widehat{K}^\times \beta \widehat{O}^\times$, so for some $\widehat{\alpha} \in \widehat{K}$, we have

$$K^\times \beta' \widehat{O}^\times = K^\times \widehat{\alpha} \beta \widehat{O}^\times \in K^\times \backslash \widehat{E} / \widehat{O}^\times.$$

Using the action from Lemma 3.2.1, we have shown that

$$K^\times \beta' \widehat{O}^\times = K^\times \widehat{\alpha} \widehat{S}^\times \cdot K^\times \beta \widehat{O}^\times.$$

Let $K^\times \widehat{\alpha} \widehat{S}^\times$ correspond to the ideal class $[\mathfrak{a}] \in \mathrm{Pic}(S)$. By Corollary 3.2.3,

$$K^\times \beta' O^\times = [\mathfrak{a}] \cdot K^\times \beta O^\times.$$

This shows the inclusion $L^{-1}(\widehat{K}^\times \beta \widehat{O}^\times) \subseteq \mathrm{Pic}(S) \cdot K^\times \beta O^\times$.

For the other inclusion, suppose $\beta \in E$ and $[\mathfrak{a}] \in \mathrm{Pic}(S)$. For some $\beta' \in E$,

$$[\mathfrak{a}] \cdot K \times \beta O^\times = K^\times \beta' O^\times.$$

Also, for some $\widehat{\alpha} \in \widehat{K}^\times$,

$$G([\mathfrak{a}] \cdot K^\times \beta O^\times) = K^\times \widehat{\alpha} \beta \widehat{O}^\times,$$

so

$$K^\times \widehat{\alpha} \beta \widehat{O}^\times = K^\times \beta' \widehat{O}^\times.$$

Then

$$\widehat{K}^\times \beta \widehat{O}^\times = \widehat{K}^\times \beta' \widehat{O}^\times = L(K^\times \beta' O^\times),$$

so $K^\times \beta' O^\times \in L^{-1}(\widehat{K}^\times \beta \widehat{O}^\times)$. We have thus shown that

$$L^{-1}(\widehat{K}^\times \beta \widehat{O}^\times) = \mathrm{Pic}(S) \cdot (K^\times \beta O^\times). \qquad \square$$

Corollary 3.2.13. *There is a bijection*

$$\begin{aligned} \Omega(S,O) &\longleftrightarrow \prod_{p \text{ prime}} \mathrm{Emb}(S_p, O_p; O_p^\times), \\ \mathrm{Pic}(S) \cdot \phi &\longmapsto (\phi_p)_p, \end{aligned}$$

where $\phi \in \mathrm{Emb}(S, O; O^\times)$.

Proof. The desired bijection is induced by L following Lemma 3.2.12. □

We still have to see that $\mathrm{AL}(O)$ acts transitively on $\Omega(S,O)$.

Proposition 3.2.14. *The action of* $\mathrm{AL}(O)$ *on* $\Omega(S,O)$ *described in Lemma 3.2.9 is transitive.*

Proof. First, we count the number of elements in $\Omega(S,O)$. By Corollary 3.2.13,

$$\#\Omega(S,O) = \prod_{p \text{ prime}} \mathrm{Emb}(S_p, O_p; O_p^\times).$$

This product is finite because for all primes p not dividing Δ, $B_p \cong \mathrm{M}_2(\mathbb{Q}_p)$, $O_p \cong \mathrm{M}_2(\mathbb{Z}_p)$, and $\#\,\mathrm{Emb}(S_p, O_p; O_p^\times) = 1$ by [20, Prop 30.5.3]. So we have

$$\#\Omega(S,O) = \prod_{p \mid \Delta} \mathrm{Emb}(S_p, O_p; O_p^\times).$$

Also, by [20, Prop 30.5.3], we have that $\mathrm{Emb}(S_p, O_p; O_p^\times) = 2$ if $K_p \supset \mathbb{Q}_p$ is an unramified field extension, which occurs if p is inert in K. Similarly, $\mathrm{Emb}(S_p, O_p; O_p^\times) = 1$ if p is ramified in K, and the same proposition say that this is all possible cases (we cannot have p split in K). Let Δ be a product of n primes, t of which are ramified in K. Then we have shown that

$$\#\Omega(S, O) = 2^{n-t}.$$

On the other hand, we can use the Orbit-Stabilizer Theorem to calculate the size of an $\mathrm{AL}(O)$ orbit in $\Omega(S, O)$. Note that if p is ramified in K, then it is ramified in S: the discriminant of S is a multiple of the discriminant of K (see Proposition 2.1.13). On the other hand, if p divides Δ and p is ramified in S, then p does not divide the conductor of S, so p is ramified in K as well. So t primes dividing Δ are ramified in S. By Lemma 3.2.10, there are 2^t elements in the stabilizer of an element of $\Omega(S, O)$. By the Orbit-Stabilizer Theorem, the size of an $\mathrm{AL}(O)$-orbit in $\Omega(S, O)$ is $\#\,\mathrm{AL}(O)$ divided by the size of the stabilizer of an element of the orbit. This gives orbits with size $2^n/2^t = 2^{n-t}$. But this is the size of all of $\Omega(S, O)$, so $\mathrm{AL}(O)$ must act transitively on $\Omega(S, O)$. □

Corollary 3.2.15. *For all $e, e' \in \mathrm{Emb}(S, O; O^\times)$, there exists $[\mathfrak{a}] \in \mathrm{Pic}(S)$ and $[\omega] \in \mathrm{AL}(O)$ such that*

$$e' = [\mathfrak{a}] \cdot e^{[\omega]}.$$

Proof. We know that there exists some $[\omega] \in \mathrm{AL}(O)$ such that

$$\mathrm{Pic}(S) \cdot e' = (\mathrm{Pic}(S) \cdot e)^{[\omega]} = \mathrm{Pic}(S) \cdot e^{[\omega]}.$$

Then there exists $[\mathfrak{a}] \in \mathrm{Pic}(S)$ such that

$$e' = [\mathfrak{a}] \cdot e^{[\omega]}.$$

□

3.2.4. Examples

At this point we have given a complete description of the set $\mathrm{Emb}(S, O; O^\times)$ with respect to the actions of $\mathrm{Pic}(S)$ and $\mathrm{AL}(O)$. We pause to calculate with some examples. For these examples, B is the quaternion algebra over $\mathbb{Q}$ with discriminant $6 = 2 \cdot 3$. Then

$$\mathrm{AL}(O) = \{[1], [\omega_2], [\omega_3], [\omega_6]\}.$$

Example 3.2.16. Suppose $D = -3$. Then $h(S) = \#\,\mathrm{Pic}(S) = 1$, so $\mathrm{Pic}(S)$ orbits are singletons, and $\mathrm{AL}(O)$ must act transitively on $\mathrm{Emb}(S, O; O^\times)$. Also, 2 is inert and 3 is ramified in S. Then $[\omega_3] \in \mathrm{AL}(O)$ acts trivially, while $[\omega_2]$ acts freely on $\mathrm{Emb}(S, O; O^\times)$. Thus, $\#\,\mathrm{Emb}(S, O; O^\times) = 2$ and these embeddings are swapped by $[\omega_2]$ (equivalently, $[\omega_6]$).

Example 3.2.17. Suppose $D = -19$. Then $h(S) = 1$, but both 2 and 3 are inert in S. So $[\omega_2]$, $[\omega_3]$, and $[\omega_6]$ all act freely on $\Omega(S, O)$, and thus on $\mathrm{Emb}(S, O; O^\times)$. So the action of $\mathrm{AL}(O)$ is free and transitive, and $\#\,\mathrm{Emb}(S, O; O^\times) = 4$.

What about CM orders with other class numbers?

Example 3.2.18. Consider $D = -24$. In this case, $h(S) = 2$. Both 2 and 3 are ramified in S, so there are S-ideals of norm 2, 3, and 6. On the other hand, there is an element of norm 6, but not 2 or 3, in S. So $[\omega_6]$ acts trivially on $\mathrm{Emb}(S, O; O^\times)$, and $[\omega_2]$ and $[\omega_3]$ act in the same way, as the nontrivial ideal class in $\mathrm{Pic}(S)$. Then $\#\,\mathrm{Emb}(S, O; O^\times) = 2$.

Example 3.2.19. Suppose $D = -148 = -4 \cdot 37$. In this case, $h(S) = 2$, but both 2 and 3 are inert in S, so there are no ideals of norm 2 or 3. It follows that $\mathrm{AL}(O)$ acts freely on $\mathrm{Emb}(S, O; O^\times)$ and $\Omega(S, O)$. Then $\#\Omega(S, O) = 4$ and $\#\,\mathrm{Emb}(S, O; O^\times) = 2 \cdot 4 = 8$.

More examples are given in the tables in Section 4.2.

Section 3.3

Complex Conjugation

3.3.1. What is Complex Conjugation?

We want to find an action of $\mathrm{Gal}(H \mid \mathbb{Q})$ on $\mathrm{Emb}(S, O; O^\times)$. At this point, we have a thorough understanding of an action of $\mathrm{Pic}(S)$ on embeddings. The Artin isomorphism identifies $\mathrm{Pic}(S)$ with $\mathrm{Gal}(H \mid K)$, as described in Theorem 2.1.19. But $\mathrm{Gal}(H \mid K)$ is a normal subgroup of $\mathrm{Gal}(H \mid \mathbb{Q})$ of index $2 = [K : \mathbb{Q}]$ by Galois theory, so the rest of $\mathrm{Gal}(H \mid \mathbb{Q})$ is a single coset. If we fixed an embedding $H \hookrightarrow \mathbb{C}$, then complex conjugation on $\mathbb{C}$ restricts to an element of $\mathrm{Gal}(H \mid \mathbb{Q})$ that does not fix K. But a priori, we do not have a preferred embedding of H into $\mathbb{C}$, and this might not always give the same automorphism of H. Because of this, "complex conjugation" is not well-defined on H, in general.

On the other hand, we can make some choice. There is a split exact sequence

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{Gal}(H \mid K) \arrow[r, hook] & \mathrm{Gal}(H \mid \mathbb{Q}) \arrow[r, shift left, "\rho"] & \mathrm{Gal}(K \mid \mathbb{Q}) \arrow[l, shift left, "s"] \arrow[r] & 1 \end{tikzcd},$$

where $\rho : \mathrm{Gal}(H \mid \mathbb{Q}) \to \mathrm{Gal}(K \mid \mathbb{Q})$ is the restriction of automorphisms of H to automorphisms of K (which exists because $K \supset \mathbb{Q}$ is a normal extension of fields). The sequence is exact because the automorphisms of H that restrict to the trivial automorphism of K are exactly the automorphisms of H fixing K. Moreover, the sequence splits by mapping the nontrivial automorphism of K to some choice of complex conjugation, which will restrict back to a nontrivial automorphism of K. It follows that

$$\mathrm{Gal}(H \mid \mathbb{Q}) \cong \mathrm{Gal}(H \mid K) \rtimes \mathrm{Gal}(K \mid \mathbb{Q}).$$

It is important to note that we made a choice of splitting for this exact sequence that might not be unique. The lack of uniqueness will add some subtlety to Section 3.4.

3.3.2. Complex Conjugation on Embeddings

Suppose that there is a fixed embedding $H \hookrightarrow \mathbb{C}$, and we take $\sigma_C \in \mathrm{Gal}(H \mid \mathbb{Q})$ to be the restriction of complex conjugation to H. Since K is imaginary quadratic, σ_C restricts further to the nontrivial element of $\mathrm{Gal}(K \mid \mathbb{Q})$. Since have fixed an embedding $K \hookrightarrow B$, the standard involution on B restricts to a nontrivial automorphism of K. It then makes some sense to try to define an action on $\mathrm{Emb}(S, O; O^\times)$ that comes from the standard involution on B.

Given an embedding $\phi : S \hookrightarrow O$, there is an embedding $\overline{\phi} : S \hookrightarrow O$ given by $\alpha \mapsto \overline{\phi(\alpha)}$. This embedding really is an embedding: $\phi(S)$ is commutative, so the standard involution is a homomorphism on $\phi(S)$.

Lemma 3.3.1. *Given an optimal embedding $\phi : S \hookrightarrow O$, there is an optimal embedding $\overline{\phi} : S \hookrightarrow O$ given by $\overline{\phi}(\alpha) = \overline{\phi(\alpha)}$.*

Proof. Given ϕ, the map $\overline{\phi}$ really is a ring homomorphism, and extends to a $\mathbb{Q}$-algebra homomorphism $K \hookrightarrow B$: both the standard involution and ϕ are $\mathbb{Q}$-linear, so $\overline{\phi}$ is $\mathbb{Q}$-linear. Given $\alpha_1, \alpha_2 \in S$,

$$\overline{\phi}(\alpha_1\alpha_2) = \overline{\phi}(\alpha_2\alpha_1) = \overline{\phi(\alpha_2)\phi(\alpha_1)} = (\overline{\phi(\alpha_1)})(\overline{\phi(\alpha_2)}) = \overline{\phi}(\alpha_1)\overline{\phi}(\alpha_2).$$

Since ϕ and the standard involution are injective, $\overline{\phi}$ is injective. Finally, $\overline{\phi}$ is optimal: $\overline{\phi}(S) = \overline{\phi(S)} = \phi(S)$ and after extending scalars, $\overline{\phi}(K) = \overline{\phi(K)} = \phi(K)$, so

$$\overline{\phi}(S) = \phi(S) = O \cap \phi(K) = O \cap \overline{\phi}(K). \qquad \square$$

Definition 3.3.2. Given an optimal embedding $\phi : S \hookrightarrow O$, we call $\overline{\phi}$ from Lemma 3.3.1 the *conjugate embedding* of ϕ.

In particular, since we have fixed an optimal embedding $S \hookrightarrow O$, there is an optimal embedding given by $\nu \mapsto \overline{\nu}$.

We would like to start understanding conjugate embeddings in terms of double cosets as we have done with optimal embeddings before.

Lemma 3.3.3. *There exists some $j \in B^\times$ such that $j\nu j^{-1} = \overline{\nu}$. The set of all such j is given by $K^\times j$. Furthermore, j satisfies the following properties:*

(i) *for all $\alpha \in K$, $j\alpha j^{-1} = j^{-1}\alpha j = \overline{\alpha}$;*

(ii) $\operatorname{trd}(j) = 0$, *and $j^2 = b \in \mathbb{Q}^\times_{>0}$ such that $B \cong \left(\dfrac{D, b}{\mathbb{Q}}\right)$.*

Proof. By Lemma 2.2.17, there exists some $j \in B^\times$ such that $j\nu = \overline{\nu}j$. Then $j\alpha = \overline{\alpha}j$ for all $\alpha \in K$. Furthermore,

$$\alpha j = (\operatorname{trd}(\alpha) - \overline{\alpha})j = \operatorname{trd}(\alpha)j - \overline{\alpha}j = j\operatorname{trd}(\alpha) - j\alpha = j(\operatorname{trd}(\alpha) - \alpha) = j\overline{\alpha},$$

so $j^{-1}\alpha j = \overline{\alpha}$ for all $\alpha \in K$, proving (i). Note that for all $\alpha \in K^\times$, $j\alpha\nu = j\nu\alpha = \overline{\nu}j\alpha$, so αj satisfies the same defining property as j. If $j' \in B^\times$ also satisfies this property, then

$$(j')^{-1}j\nu j^{-1}j' = \nu \implies j^{-1}j' \in K^\times.$$

So j is well-defined up to right multiplication by elements of $K^\times$, and $j\alpha = \overline{\alpha}j$, so j is well-defined up to left multiplication by elements of $K^\times$ as well.

Note that $j^2\nu = j\overline{\nu}j = \nu j^2$, so $j^2 \in K^\times$. In fact, $j^2 = \operatorname{trd}(j)j - \operatorname{nrd}(j)$, so $\operatorname{trd}(j)j \in K$. But since $j \notin K$, we must have $\operatorname{trd}(j) = 0$, and $j^2 = -\operatorname{nrd}(j) \in \mathbb{Q}^\times$. Define

$$b := j^2 \in \mathbb{Q}.$$

Let $i := \nu - \overline{\nu} \in S$. Then

$$i^2 = \nu^2 - \nu\overline{\nu} + \overline{\nu}^2 = (\nu + \overline{\nu})^2 - 4\nu\overline{\nu} = \operatorname{trd}(\nu)^2 - 4\operatorname{nrd}(\nu) = D.$$

Furthermore,

$$ij = \nu j - \overline{\nu} j = j\overline{\nu} - j\nu = -ji.$$

At this point, we have 1 and j are linearly independent over K, so $1, i, j, ij$ are linearly independent over $\mathbb{Q}$. So we have shown that $B = \mathbb{Q}(i,j) = \left(\dfrac{D, b}{\mathbb{Q}}\right)$. But B is indefinite, so $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathrm{M}_2(\mathbb{R})$. If it was true that $b < 0$, then $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}$ would be a division algebra, a contradiction. So $b > 0$. □

For notational purposes, we will continue to use j and b as defined in Lemma 3.3.3. By rescaling j by an element of $\mathbb{Q}^\times$, we can ensure that $b \in \mathbb{Z}$. The following lemma gives a way to calculate b.

Lemma 3.3.4. *Let $b \in \mathbb{Q}$. If $(D, b')_v = (D, b)_v$ for all places v of $\mathbb{Q}$, then $b^{-1}b' \in \operatorname{Nm}_{\mathbb{Q}}^{K}(K^\times)$.*

Proof. If $(D, b')_v = (D, b)_v$ for all places v of $\mathbb{Q}$, then $\left(\dfrac{D, b'}{\mathbb{R}}\right) \cong \left(\dfrac{D, b}{\mathbb{R}}\right)$ and $\left(\dfrac{D, b'}{\mathbb{Q}_p}\right) \cong \left(\dfrac{D, b}{\mathbb{Q}_p}\right)$ for all primes p. Then by Hasse-Minkowski [20, Thm 14.3.1], $\left(\dfrac{D, b'}{\mathbb{Q}}\right) \cong \left(\dfrac{D, b}{\mathbb{Q}}\right)$. The result then follows from [20, Cor 7.7.6]. □

In fact, j can be used to get the conjugate embedding of any embedding, not just the fixed embedding.

Lemma 3.3.5. *If an embedding $S \hookrightarrow O$ is given by $\nu \mapsto \beta^{-1}\nu\beta$ for some $\beta \in E$, then the conjugate embedding is given by $(j\beta)^{-1}\nu(j\beta)$. In fact, $O^\times$-equivalent embeddings have $O^\times$-equivalent conjugate embeddings. For $\beta \in E$, the conjugate embedding of $K^\times\beta O^\times$ is $K^\times j\beta O^\times$.*

Proof. For $\beta \in E$, we have the optimal embedding $\nu \mapsto \beta^{-1}\nu\beta$. By definition, the conjugate embedding is given by

$$\nu \mapsto \overline{\beta^{-1}\nu\beta} = \overline{\beta}\overline{\nu}\overline{\beta}^{-1}.$$

But $\beta\overline{\beta} = \operatorname{nrd}(\beta) \in \mathbb{Q}$, so $\overline{\beta} = \operatorname{nrd}(\beta)\beta^{-1}$ and the conjugate embedding is given by

$$\nu \mapsto \beta^{-1}\overline{\nu}\beta = \beta^{-1}j^{-1}\nu j\beta.$$

For $\epsilon \in O^{\times}$, the conjugate embedding of $\nu \mapsto \epsilon^{-1}\beta^{-1}\nu\beta\epsilon$ is then $\nu \mapsto \epsilon^{-1}\beta^{-1}j^{-1}\nu j\beta\epsilon$. This means that $O^{\times}$-equivalent embeddings have $O^{\times}$-equivalent conjugate embeddings. In other words, there is a well-defined action of complex conjugation on $\operatorname{Emb}(S, O; O^{\times})$. We have also shown that the conjugate embedding of $K^{\times}\beta O^{\times}$ is $K^{\times}j\beta O^{\times}$. □

Lemma 3.3.5 tells us that there is a well-defined "action" of complex conjugation on $\operatorname{Emb}(S, O; O^{\times})$, which we will also call *complex conjugation* when the meaning is clear. Calling it an "action" is justified: given an embedding ϕ, $\overline{\overline{\phi}} = \phi$, so we have really defined an action of $\mathbb{Z}/2\mathbb{Z} \cong \operatorname{Gal}(K \mid \mathbb{Q})$. For notational purposes, we write

$$j(K^{\times}\beta O^{\times}) := K^{\times}j\beta O^{\times}.$$

If $e \in \operatorname{Emb}(S, O; O^{\times})$, we write $j(e)$ for the conjugate embedding since e is not strictly an embedding, but an $O^{\times}$-equivalence class of embeddings.

The goal of the rest of this section is to understand how this action interacts with the actions of $\operatorname{Pic}(S)$ and $\operatorname{AL}(O)$ described in Section 3.2. Specifically, we have effectively labeled elements of $\operatorname{Emb}(S, O; O^{\times})$ using the free action of $\operatorname{Pic}(S)$ and the identification of $\operatorname{Pic}(S)$-orbits with local (adelic) embeddings. We want to know, for example, what $j(e)$ is in terms of these local actions.

3.3.3. Complex Conjugation Versus Other Actions

The most basic question we can ask about complex conjugation is whether it commutes with the actions of $\mathrm{Pic}(S)$ and $\mathrm{AL}(O)$.

Lemma 3.3.6. *The action of complex conjugation on* $\mathrm{Emb}(S, O; O^\times)$ *commutes with the action of* $\mathrm{AL}(O)$*. That is, for any* $e \in \mathrm{Emb}(S, O; O^\times)$ *and any* $[\omega] \in \mathrm{AL}(O)$*,*

$$j(e^{[\omega]}) = j(e)^{[\omega]}.$$

Proof. Let $e = K^\times \beta O^\times$ for some $\beta \in E$. Then

$$j(e^{[\omega]}) = j(K^\times \beta\omega O^\times) = K^\times j\beta\omega O^\times = (K^\times j\beta O^\times)^{[\omega]} = j(e)^{[\omega]}. \qquad \square$$

Lemma 3.3.7. *The action of complex conjugation on* $\mathrm{Emb}(S, O; O^\times)$ *skew-commutes with the action of* $\mathrm{Pic}(S)$*. That is, for any* $e \in \mathrm{Emb}(S, O; O^\times)$ *and any* $[\mathfrak{a}] \in \mathrm{Pic}(S)$*,*

$$j([\mathfrak{a}] \cdot e) = [\mathfrak{a}]^{-1} \cdot j(e).$$

Proof. Suppose $e = K^\times \beta O^\times$ for some $\beta \in E$. We can assume without loss of generality that $\mathfrak{a} \subset S$ is an proper ideal. For some $\xi \in O$, we have $\beta^{-1}\mathfrak{a}\beta O = \xi O$ and $[\mathfrak{a}] \cdot e = K^\times \beta\xi O^\times$. Then

$$j([\mathfrak{a}] \cdot e) = K^\times j\beta\xi O^\times.$$

Now consider $j(e) = K^\times j\beta O^\times$. Then with $\xi \in O$ as above,

$$\xi O = \beta^{-1}\mathfrak{a}\beta O = \beta^{-1}j^{-1}\overline{\mathfrak{a}}j\beta O.$$

Then

$$[\mathfrak{a}]^{-1} \cdot j(e) = [\overline{\mathfrak{a}}] \cdot (K^\times j\beta O^\times) = K^\times j\beta\xi O^\times = j([\mathfrak{a}] \cdot e). \qquad \square$$

Corollary 3.3.8. *The action of complex conjugation is well-defined on* $\mathrm{Pic}(S)$*-orbits of* $\mathrm{Emb}(S, O; O^\times)$ *as*

$$j(\mathrm{Pic}(S) \cdot e) = \mathrm{Pic}(S) \cdot j(e)$$

for all $e \in \mathrm{Emb}(S, O; O^\times)$*. In other words, complex conjugation acts on* $\Omega(S, O)$*.*

Proof. Given $e \in \mathrm{Emb}(S, O; O^\times)$ and $[\mathfrak{a}] \in \mathrm{Pic}(S)$,

$$\mathrm{Pic}(S) \cdot j([\mathfrak{a}] \cdot e) = \mathrm{Pic}(S) \cdot ([\mathfrak{a}]^{-1} \cdot j(e)) = \mathrm{Pic}(S) \cdot j(e).$$

This shows that the action is well-defined. □

As a consequence of Lemmas 3.3.6 and 3.3.7 and Corollary 3.2.15, it suffices to see how complex conjugation acts on a single embedding in order to know how complex conjugation acts on all embeddings. To do this, we will have to look locally.

3.3.4. Local Action of Complex Conjugation

We now look at how complex conjugation acts on local embeddings. Specifically, we saw in Corollary 3.3.8 that complex conjugation acts in a natural way on $\Omega(S, O)$. Let us recall this action. Given an embedding $e \in \mathrm{Emb}(S, O; O^\times)$, complex conjugation acts on $\mathrm{Pic}(S) \cdot e$ to give $\mathrm{Pic}(S) \cdot j(e)$. By Lemma 3.2.12 and the bijection in Corollary 3.2.13, if we represent e by $\beta \in E$, then complex conjugation is acting $\widehat{K}^\times \beta \widehat{O}^\times$ to give $\widehat{K}^\times j\beta \widehat{O}^\times$. On the other hand, if we represent e by an actual embedding $\phi : S \hookrightarrow O$, then complex conjugation is acting on $(\phi_p)_p$ to give $(\overline{\phi}_p)_p$. We note here that $\overline{\phi}_p = \overline{\phi_p}$, that is the localization of the conjugate embedding is the conjugate local embedding. This is because the standard involution on B_p restricts to the standard involution on B by uniqueness. How else can we realize this action?

Recall that Δ is the discriminant of the quaternion algebra B.

Lemma 3.3.9. *Complex conjugation acts as* $[\omega_\Delta]$ *on* $\Omega(S, O)$. *That is, for all* $e \in \operatorname{Emb}(S, O; O^\times)$,

$$j(\operatorname{Pic}(S) \cdot e) = (\operatorname{Pic}(S) \cdot e)^{[\omega_\Delta]}.$$

Proof. Since complex conjugation commutes with the transitive action of $\operatorname{AL}(O)$, it is sufficient to show that complex conjugation and $[\omega_\Delta]$ act the same on the fixed $\operatorname{Pic}(S)$-orbit in $\Omega(S, O)$. By the above remarks, it suffices to show that ω_Δ gives the complex conjugation local embedding at p for all primes p. By [20, Prop 30.5.3], $\# \operatorname{Emb}(S_p, O_p; O_p^\times) = 1$ for all p not dividing Δ, since $B_p \cong \mathrm{M}_2(\mathbb{Q}_p)$ in this case. If p is ramified in K, then $K_p \supset \mathbb{Q}_p$ is a ramified extension and $\# \operatorname{Emb}(S_p, O_p; O_p^\times) = 1$ as well by [20, Prop 30.5.3]. Otherwise p is inert in K. Then $K_p \supset \mathbb{Q}_p$ is an unramified extension, and $\# \operatorname{Emb}(S_p, O_p; O_p^\times) = 2$. We note that $v_p(\operatorname{nrd}(\omega_\Delta)) = 1$, so $\omega_\Delta \notin \mathbb{Q}_p^\times O_p^\times$. But by the proof of [20, Prop 30.5.3], this means that ω_Δ represents the nontrivial element of $N_{B_p^\times}(O_p)/\mathbb{Q}_p^\times O_p^\times \cong \mathbb{Z}/2\mathbb{Z}$ that normalizes K_p but does not centralize K_p. Then ω_Δ must act as the nontrivial automorphism on K_p. □

Corollary 3.3.10. *For all* $e \in \operatorname{Emb}(S, O; O^\times)$, *there exists* $[\mathfrak{c}] \in \operatorname{Pic}(S)$ *such that*

$$j(e) = [\mathfrak{c}] \cdot e^{[\omega_\Delta]}.$$

Proof. By Lemma 3.3.9,

$$\operatorname{Pic}(S) \cdot j(e) = j(\operatorname{Pic}(S) \cdot e) = (\operatorname{Pic}(S) \cdot e)^{[\omega_\Delta]} = \operatorname{Pic}(S) \cdot e^{[\omega_\Delta]}.$$

This means that for some $[\mathfrak{c}] \in \operatorname{Pic}(S)$, we have $j(e) = [\mathfrak{c}] \cdot e^{[\omega_\Delta]}$. □

Getting control on the ideal class $[\mathfrak{c}]$ might be tricky in general, but we can make do with norms.

3.3.5. Global Action of Complex Conjugation

Let $e \in \mathrm{Emb}(S, O; O^\times)$ be an embedding given by $K^\times \beta O^\times$ for some $\beta \in E$. Suppose that $[\mathfrak{c}] \in \mathrm{Pic}(S)$ is such that $j(e) = [\mathfrak{c}] \cdot e^{[\omega_\Delta]}$. Then

$$[\mathfrak{c}] \cdot e = ([\mathfrak{c}] \cdot e^{[\omega_\Delta]})^{[\omega_\Delta]} = j(e)^{[\omega_\Delta]}.$$

We know that for some $\xi \in O$, $\beta^{-1}\mathfrak{c}\beta O = \xi O$, and $[\mathfrak{c}] \cdot e = K^\times \xi \beta O^\times$. Then

$$K^\times \xi \beta O^\times = K^\times j \beta \omega_\Delta O^\times.$$

For some $\alpha \in K^\times$, we must have

$$\alpha \xi \beta O^\times = j \beta \omega_\Delta O^\times,$$

so

$$\mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha \mathfrak{c}) = |\,\mathrm{nrd}(\alpha)\,\mathrm{nrd}(\xi)| = |\,\mathrm{nrd}(j\omega_\Delta)| = b\Delta.$$

In other words, we have proved the following lemma:

Lemma 3.3.11. *The ideal class $[\mathfrak{c}] \in \mathrm{Pic}(S)$ from Corollary 3.3.10 can be represented by a fractional ideal of norm $b\Delta$. In other words, for all $e \in \mathrm{Emb}(S, O; O^\times)$, there exists a fractional S-ideal $\mathfrak{c}$ of norm $b\Delta$ such that*

$$j(e) = [\mathfrak{c}] \cdot e^{[\omega_\Delta]}.$$

Proof. See above. □

It is suggestive that $\mathfrak{c}$ can be taken to have norm $b\Delta$ regardless of which embedding we are looking at. How different can ideals of the same norm be?

Lemma 3.3.12. *Suppose S is maximal. Suppose $\mathfrak{c}$ and $\mathfrak{c}'$ are invertible fractional S-ideals such that $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{c}) = \mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{c}')$. Then*

$$[\mathfrak{c}]\,\mathrm{Pic}(S)^2 = [\mathfrak{c}']\,\mathrm{Pic}(S)^2.$$

In other words, there exists $[\mathfrak{a}] \in \mathrm{Pic}(S)$ such that $[\mathfrak{c}'] = [\mathfrak{a}]^2[\mathfrak{c}]$.

Proof. It suffices to assume that $\mathfrak{c}$ and $\mathfrak{c}'$ are actual S-ideals, since both can simultaneously be rescaled by an element of $K^\times$ to make it so.

Suppose first that $\mathfrak{c}$ and $\mathfrak{c}'$ are prime and let $p \mid \mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{c}) = \mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{c}')$. If $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{c}) = p^2$, then p is inert and $\mathfrak{c} = \mathfrak{c}' = pS$. If $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{c}) = p$, then $\mathfrak{c}$ and $\mathfrak{c}'$ are primes over p. If $\mathfrak{c} \neq \mathfrak{c}'$, then

$$\mathfrak{c}' = \bar{\mathfrak{c}} = p^{-1}\bar{\mathfrak{c}}^2\mathfrak{c},$$

so

$$[\mathfrak{c}'] = [\bar{\mathfrak{c}}]^2[\mathfrak{c}].$$

Now suppose that $\mathfrak{c}$ and $\mathfrak{c}'$ are not prime. Then by Theorem 2.1.8, they each decompose uniquely into a product of prime ideals. Comparing norms shows that the primes dividing $\mathfrak{c}$ can be paired with the primes dividing $\mathfrak{c}'$ such that primes in each pair have the same norm. The result follows from the prime case. □

For the previous result, we needed S to be maximal to guarantee unique factorization of ideals. If we assume this, we get nice results. For example, every fractional S-ideal of norm $b\Delta$ gives part of complex conjugation for some embedding.

Lemma 3.3.13. *Let S be maximal. Let $\mathfrak{c}$ be a fractional S-ideal of norm $b\Delta$. Then there exists some $e \in \mathrm{Emb}(S, O; O^\times)$ such that*

$$j(e) = [\mathfrak{c}] \cdot e^{[\omega_\Delta]}.$$

Proof. Consider a fixed embedding $e_0 \in \mathrm{Emb}(S, O; O^\times)$. By Lemma 3.3.11, for some fractional S-ideal $\mathfrak{c}_0$ of norm $b\Delta$,

$$j(e_0) = [\mathfrak{c}_0] \cdot e^{[\omega_\Delta]}.$$

By Lemma 3.3.12, there exists $[\mathfrak{a}] \in \mathrm{Pic}(S)$ such that $[\mathfrak{c}_0] = [\mathfrak{a}]^2[\mathfrak{c}]$. Let $e = [\mathfrak{a}] \cdot e_0$. Then

$$j(e) = j([\mathfrak{a}] \cdot e_0) = [\mathfrak{a}]^{-1} \cdot j(e_0) = [\mathfrak{a}]^{-1}[\mathfrak{c}_0] \cdot e_0^{[\omega_\Delta]} = [\mathfrak{c}][\mathfrak{a}] \cdot e_0^{[\omega_\Delta]} = [\mathfrak{c}] \cdot e^{[\omega_\Delta]}. \qquad \square$$

With these tools in hand, we can answer one basic question about complex conjugation.

Proposition 3.3.14. *Suppose B is a division algebra. The action of complex conjugation on $\mathrm{Emb}(S, O; O^\times)$ is free, and the action of complex conjugation on $\Omega(S, O)$ is free if and only if $\#\Omega(S, O) > 1$.*

Proof. Fix $e \in \mathrm{Emb}(S, O; O^\times)$ and suppose for the sake of contradiction that $j(e) = e$. Then by Lemma 3.3.11, for some fraction S-ideal $\mathfrak{c}$ of norm $b\Delta$,

$$[\mathfrak{c}] \cdot e^{[\omega_\Delta]} = e.$$

So

$$e^{[\omega_\Delta]} = ([\mathfrak{c}] \cdot e^{[\omega_\Delta]})^{[\omega_\Delta]} = [\mathfrak{c}] \cdot e.$$

By Proposition 3.2.8, there exists and ideal $\mathfrak{a} \subseteq S$ of norm Δ such that $[\mathfrak{a}] = [\mathfrak{c}]$. In other words, for some $\alpha \in K^\times$, $\mathfrak{c} = \alpha\mathfrak{a}$. This implies that $b\Delta = \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha)\Delta$, so $b \in \mathrm{Nm}_{\mathbb{Q}}^{K}(K^\times)$. By [20, Thm 5.4.4], we have a contradiction since B is a division algebra. It follows that complex conjugation acts freely on $\mathrm{Emb}(S, O; O^\times)$.

Now suppose that j has a fixed point in $\Omega(S, O)$, i.e. $j(\mathrm{Pic}(S) \cdot e) = \mathrm{Pic}(S) \cdot e$ for some

$e \in \mathrm{Emb}(S, O; O^\times)$. Then for some $[\mathfrak{a}], [\mathfrak{c}] \in \mathrm{Pic}(S)$ with $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{c}) = b\Delta$,

$$e = [\mathfrak{a}] \cdot j(e) = [\mathfrak{a}][\mathfrak{c}] \cdot e^{[\omega_\Delta]}.$$

Then $[\omega_\Delta]$ acts trivially on $\Omega(S, O)$. By Lemma 3.2.10, $[\omega_p]$ is in the stabilizer of $\mathrm{Pic}(S) \cdot e$ for all primes p dividing Δ. But then all of $\mathrm{AL}(O)$ stabilizes $\mathrm{Pic}(S) \cdot e$, so $\Omega(S, O)$, which is the $\mathrm{AL}(O)$-orbit of $\mathrm{Pic}(S) \cdot e$, has just one element. □

3.3.6. Examples

In the following examples, we still work with B with discriminant 6 as in Section 3.2.

Example 3.3.15. Suppose $D = -4$. Then $h(S) = 1$, so $\Omega(S, O)$ is in bijection with $\mathrm{Emb}(S, O; O^\times)$. Also, 3 is inert and 2 is ramified, and there is an element of norm 2. So $[\omega_3]$ has no fixed points, $[\omega_2]$ acts trivially, and $\#\,\mathrm{Emb}(S, O; O^\times) = 2$. Since $\mathrm{Pic}(S)$ is trivial, complex conjugation acts as $[\omega_6]$, or equivalently $[\omega_3]$. This makes sense because complex conjugation should swap the two local embeddings at 3. In general, if $h(S) = 1$, then complex conjugation will act the same $[\omega_6]$.

What about larger class numbers? If $\mathrm{Pic}(S)$ has exponent 2 (i.e. every nontrivial ideal class has order 2), then by Lemma 3.3.12, the norm of a fractional ideal uniquely defines its ideal class. Then complex conjugation acts the same on every embedding.

Example 3.3.16. Suppose $D = -51$. Then $h(S) = 2$, 3 is ramified), 2 is inert, and no elements of S have norm 2, 3, or 6. Then $[\omega_3]$ acts as the nontrivial ideal class $[\mathfrak{p}_3] \in \mathrm{Pic}(S)$, and $[\omega_2]$ acts freely and transitively on $\Omega(S, O)$. If we fix an embedding $e \in \mathrm{Emb}(S, O; O^\times)$, then $\mathrm{Emb}(S, O; O^\times) = \{e, [\mathfrak{p}_3] \cdot e = e^{[\omega_3]}, e^{[\omega_2]}, [\mathfrak{p}_3] \cdot e^{[\omega_2]} = e^{[\omega_6]}\}$. How does complex conjugation act? We calculate with Magma [6] that one possible value for b is $b = 2$. An ideal of norm $2 \cdot 6 = 12$ is $2\mathfrak{p}_3$. It follows that complex conjugation acts as $j(e) = [\mathfrak{p}_3] \cdot e^{[\omega_6]} = e^{[\omega_2]}$.

Diagrammatically, $[\mathfrak{p}_3]$ and $[\omega_3]$ act as

$$\begin{tikzcd}
e \arrow[r, leftrightarrow] & e^{[\omega_3]} \\
e^{[\omega_2]} \arrow[r, leftrightarrow] & e^{[\omega_6]},
\end{tikzcd}$$

whereas $[\omega_2]$ and complex conjugation both act as

$$\begin{tikzcd}
e \arrow[d, leftrightarrow] & e^{[\omega_3]} \arrow[d, leftrightarrow] \\
e^{[\omega_2]} & e^{[\omega_6]},
\end{tikzcd}$$

and $[\omega_6]$ acts as

$$\begin{tikzcd}
e \arrow[dr, leftrightarrow] & e^{[\omega_3]} \arrow[dl, leftrightarrow] \\
e^{[\omega_2]} & e^{[\omega_6]}.
\end{tikzcd}$$

In these diagrams, note that the rows are $\mathrm{Pic}(S)$-orbits.

Example 3.3.17. Suppose $D = -84$. Then $h(S) = 4$, $\mathrm{Pic}(S)$ has exponent 2, 2 and 3 are ramified with no elements of norm 2, 3, or 6. Then $\#\Omega(S, O) = 1$ and $\mathrm{Pic}(S)$ acts transitively on $\mathrm{Emb}(S, O; O^\times)$, which has 4 elements. Furthermore, $[\omega_2]$ acts as $[\mathfrak{p}_2]$, the prime over 2, and $[\omega_3]$ acts as $[\mathfrak{p}_3]$, the prime over 3, and these two primes generate $\mathrm{Pic}(S)$. It follows that $\mathrm{AL}(O)$ acts transitively on $\mathrm{Emb}(S, O; O^\times)$. How does complex conjugation act? We calculate that a possible value of b is $b = 2$. An ideal of norm $2 \cdot 6 = 12$ is $2\mathfrak{p}_3$, so complex conjugation acts as $j(e) = [\mathfrak{p}_3] \cdot e^{[\omega_6]} = e^{[\omega_2]}$ again.

What about cases where $\mathrm{AL}(O)$ does not act transitively on all embeddings?

Example 3.3.18. Suppose $D = -91 = -7 \cdot 13$. Here, $h(S) = 2$. Both 2 and 3 are inert, so $\mathrm{AL}(O)$ acts freely on $\Omega(S, O)$ and $\#\,\mathrm{Emb}(S, O; O^\times) = 8$. Note that 7 is ramified in S, and the ideal $\mathfrak{p}_7$ over 7 represents the nontrivial ideal class in $\mathrm{Pic}(S)$. How does complex conjugation act? We calculate that a possible value for b is $b = 42 = 6 \cdot 7$. An ideal of norm $6^2 \cdot 7$ is $6\mathfrak{p}_7$, so $j(e) = [\mathfrak{p}_7] \cdot e^{[\omega_6]}$. Diagramatically, complex conjugation acts as:

$$\begin{tikzcd}
e \arrow[dddr, leftrightarrow] & {[\mathfrak{p}_7] \cdot e} \arrow[dddl, leftrightarrow] \\
e^{[\omega_2]} \arrow[dr, leftrightarrow] & {[\mathfrak{p}_7] \cdot e^{[\omega_2]}} \\
e^{[\omega_3]} \arrow[ur, leftrightarrow] & {[\mathfrak{p}_7] \cdot e^{[\omega_3]}} \\
e^{[\omega_6]} & {[\mathfrak{p}_7] \cdot e^{[\omega_6]}.}
\end{tikzcd}$$

Example 3.3.19. Another interesting case is $D = -136$. Here, $h(S) = 4$ and $\mathrm{Pic}(S)$ is cyclic, generated by $[\mathfrak{p}_5]$, where $\mathfrak{p}_5$ is a prime over 5. We have 2 is ramified but 3 is inert, and no elements of norm 2, 3, or 6 exist in S. Then $[\omega_2]$ acts as $[\mathfrak{p}_2]$ represented by the prime over 2, which has order 2 and is thus in the same ideal class as $[\mathfrak{p}_5]^2$. On the other hand, $[\omega_3]$ acts freely and transitively on $\Omega(S, O)$. How does complex conjugation act? A possible value for b is $b = 30 = 6 \cdot 5$. An ideal of norm $6^2 \cdot 5$ is $6\mathfrak{p}_5$, so there exists some $e \in \mathrm{Emb}(S, O; O^\times)$ such that

$$j(e) = [\mathfrak{p}_5] \cdot e^{[\omega_6]} = [\mathfrak{p}_5][\mathfrak{p}_2] \cdot e^{[\omega_3]} = [\mathfrak{p}_5]^3 \cdot e^{[\omega_3]}.$$

We then calculate the action of complex conjugation on all embeddings:

$$\begin{tikzcd}
e \arrow[drrr, leftrightarrow] & {[\mathfrak{p}_5] \cdot e} \arrow[dr, leftrightarrow] & {[\mathfrak{p}_5]^2 \cdot e} \arrow[dl, leftrightarrow] & {[\mathfrak{p}_5]^3 \cdot e} \arrow[dlll, leftrightarrow] \\
e^{[\omega_3]} & {[\mathfrak{p}_5] \cdot e^{[\omega_3]}} & {[\mathfrak{p}_5]^2 \cdot e^{[\omega_3]}} & {[\mathfrak{p}_5]^3 \cdot e^{[\omega_3]}.}
\end{tikzcd}$$

In the diagram above, $[\mathfrak{p}_5]$ cycles the columns horizontally and $[\omega_3]$ swaps the rows vertically.

Example 3.3.20. What happens when not everything in $\operatorname{Pic}(S)$ has even order? The first example of this is $D = -139$. Here, $h(S) = 3$. We note that 139 is prime, and both 2 and 3 are inert in S. Then $\operatorname{AL}(O)$ acts freely and transitively on $\Omega(S, O)$, and $\#\operatorname{Emb}(S, O; O^\times) = 12$. How does complex conjugation act? We calculate $b = 6$. An ideal of norm $6 \cdot 6 = 36$ is just $6S$, so there exists an embedding $e \in \operatorname{Emb}(S, O; O^\times)$ such that $j(e) = e^{[\omega_6]}$. If $[\mathfrak{a}]$ generates $\operatorname{Pic}(S)$ (for instance, $\operatorname{Nm}^K_{\mathbb{Q}}(\mathfrak{a}) = 5$), then $j([\mathfrak{a}] \cdot e) = [\mathfrak{a}]^{-1} \cdot j(e) = [\mathfrak{a}]^2 \cdot e^{[\omega_6]}$, and similarly for $[\mathfrak{a}]^2 \cdot e$. Then the action of complex conjugation on all embeddings is

$$\begin{tikzcd}
e \arrow[d, leftrightarrow] & {[\mathfrak{a}] \cdot e} \arrow[dr, leftrightarrow] & {[\mathfrak{a}]^2 \cdot e} \arrow[dl, leftrightarrow] \\
e^{[\omega_6]} & {[\mathfrak{a}] \cdot e^{[\omega_6]}} & {[\mathfrak{a}]^2 \cdot e^{[\omega_6]}}
\end{tikzcd}$$

$$\begin{tikzcd}
e^{[\omega_2]} \arrow[d, leftrightarrow] & {[\mathfrak{a}] \cdot e^{[\omega_2]}} \arrow[dr, leftrightarrow] & {[\mathfrak{a}]^2 \cdot e^{[\omega_2]}} \arrow[dl, leftrightarrow] \\
e^{[\omega_3]} & {[\mathfrak{a}] \cdot e^{[\omega_3]}} & {[\mathfrak{a}]^2 \cdot e^{[\omega_3]}.}
\end{tikzcd}$$

The ideal class $[\mathfrak{a}]$ cycles the columns horizontally to the right, $[\omega_2]$ does the permutation (1 3)(2 4) to the rows (in each column), $[\omega_3]$ does the permutation (1 4)(2 3) to the rows (in each column), and $[\omega_6]$ does the permutation (1 2)(3 4) to the rows (in each column).

Section 3.4

Fields of Moduli of Abelian Surfaces

3.4.1. Establishing a Bijection

In Section 3.1, we claimed that there is a bijection

$$\mathcal{A} := \left\{ \begin{array}{c} (A,\iota) \text{ principally polarized} \\ \text{abelian surfaces with QM by } O \\ \text{an CM by } S \\ \text{up to isomorphism preserving QM} \end{array} \right\} \longleftrightarrow \operatorname{Emb}(S,O;O^\times)$$

such that actions of $\operatorname{Gal}(H \mid \mathbb{Q})$ on both sides agree. The careful reader will notice that we still have not described an action of $\operatorname{Gal}(H \mid \mathbb{Q})$ on $\operatorname{Emb}(S,O;O^\times)$. We have described an action of $\operatorname{Gal}(H \mid K)$ and an action of "complex conjugation" which is some representative of the nontrivial coset of $\operatorname{Gal}(H \mid K)$ in $\operatorname{Gal}(H \mid \mathbb{Q})$. But we do not yet know which representative it is. In this chapter, we first describe the bijection above. Then we show that the actions of $\operatorname{Gal}(H \mid K)$ and complex conjugation agree on both sides. Finally we will choose complex conjugation $\sigma_C \in \operatorname{Gal}(H \mid \mathbb{Q})$ so that the resulting actions of $\operatorname{Gal}(H \mid \mathbb{Q})$ agree.

Throughout this section, we fix an embedding $\iota_\infty : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$, which exists because B is indefinite. Through this section, we will identify B with its image in $\mathrm{M}_2(\mathbb{R})$ via ι_∞. Let $\Gamma^1 = \iota_\infty(O^1)/\{\pm 1\}$.

Proposition 3.4.1. *There exists a bijection*

$$\mathcal{A} := \left\{ \begin{array}{c} (A,\iota) \textit{ principally polarized} \\ \textit{abelian surfaces with QM by } O \\ \textit{an CM by } S \\ \textit{up to isomorphism preserving QM} \end{array} \right\} \longleftrightarrow \mathrm{Emb}(S, O; O^{\times}).$$

Proof. By [20, Thm 43.1.4] and [20, 43.7.4], there is a bijection

$$\{\Gamma^1 \cdot z \in \Gamma^1 \backslash \mathfrak{H} : z \text{ is a CM point of } S\} \longleftrightarrow \mathcal{A}.$$

The forward map works as follows: given a CM point $z \in \mathfrak{H}$, we get a lattice

$$\Lambda_\tau := \iota_\infty(O) \cdot \begin{pmatrix} z \\ 1 \end{pmatrix}$$

giving rise to a principally polarized abelian surface $A_z := \mathbb{C}^2/\Lambda_z$ with QM structure $\iota_z : O \hookrightarrow \mathrm{End}(A_z)$. For details, see [20, Ch 43] and [2]. It then suffices to find a bijection between CM points on $\Gamma^1 \backslash \mathfrak{H}$ and classes of embeddings in $\mathrm{Emb}(S, O; O^{\times})$.

Given an optimal embedding $S \hookrightarrow O$, we get a CM point $z \in \mathfrak{H}$, and all such CM points arise this way. This gives a surjective map

$$\mathrm{Emb}(S, O) \to \mathcal{A}.$$

It remains to show that two embeddings give rise to the same O^1-orbit of a CM point if and only if they are $O^{\times}$-equivalent.

Fix an embedding $S \hookrightarrow O$ and identify S with its image under this embedding. We have a CM point z such that $\nu \cdot z = z$. We need the following lemma.

Lemma 3.4.2. *Let* $z \in \mathfrak{H}$ *be the unique fixed point of* $\nu = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in O \subset \mathrm{M}_2(\mathbb{R})$*, where* $S = \mathbb{Z}[\nu] \subset O$ *is an optimally embedding CM order. Then*

$$\mathrm{Stab}_{B^\times \cap O}(z) = \mathbb{Z}[\nu] \setminus \{0\}.$$

Proof of the lemma. It suffices to show that

$$\mathrm{Stab}_{B^\times}(z) = \mathbb{Q}[\nu]^\times,$$

since $\mathbb{Q}[\nu] \cap O = \mathbb{Z}[\nu]$ is optimally embedded. First, note that $\mathbb{Q}^\times \subseteq \mathrm{Stab}_{B^\times}(z)$. It follows that $\mathbb{Q}^\times \nu \subseteq \mathrm{Stab}_{B^\times}(z)$. We show that if $M_1, M_2 \in \mathrm{Stab}_{B^\times}(z)$ and $M_1 + M_2 \in B^\times$, then $M_1 + M_2 \in \mathrm{Stab}_{B^\times}(z)$. Let

$$M_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \text{ and } M_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix}.$$

Then for $r \in \{1, 2\}$,

$$\frac{a_r z + b_r}{c_r z + d_r} = z,$$

so $c_r z^2 + (d_r - a_r)z - b_r = 0$. Then

$$(c_1 + c_2)z^2 + (d_1 + d_2 - a_1 - a_2)z - (b_1 + b_2) = 0.$$

Since $M_1 + M_2 \in B^\times$, we have $(c_1 + c_2)z + d_1 + d_2 \neq 0$, and we can rearrange to get

$$z = \frac{(a_1 + a_2)z + (b_1 + b_2)}{(c_1 + c_2)z + (d_1 + d_2)} = (M_1 + M_2) \cdot z.$$

As a consequence, we have shown that $\mathbb{Q}[\nu]^\times \subseteq \mathrm{Stab}_{B^\times}(z)$.

In fact, the above work shows that $K' := \mathrm{Stab}_{B^\times}(z) \cup \{0\}$ is a $\mathbb{Q}$-subalgebra of B. By linear algebra, $\dim_{\mathbb{Q}}(K')$ divides $\dim_{\mathbb{Q}}(B) = 4$. But the dimension of K' is strictly greater than 1, and strictly less than 4 because not every quaternion fixes z. It follows that $\dim_{\mathbb{Q}}(K') = 2 = \dim_{\mathbb{Q}}(\mathbb{Q}[\nu])$, so $K' = \mathbb{Q}[\nu]$, and the claim of the lemma follows. □

Now suppose that another embedding $\nu \mapsto \beta^{-1}\nu\beta$ for some $\beta \in E$. By the convention explained in [ref], we take the fixed point of $\beta^{-1}\nu\beta$ to be $\beta^{-1} \cdot z$, even if this might be in the lower half-plane if $\mathrm{nrd}(\beta) < 0$ (we come back to this in Lemma 3.4.5). If $\beta^{-1} \cdot z = \epsilon \cdot z$, Lemma 3.4.2 tells us that $\beta\epsilon \in K^\times$, so $\beta \in K^\times \epsilon^{-1}$ and the two embeddings are $O^\times$-equivalent.

If we have an $O^\times$-equivalent embedding $\nu \mapsto \epsilon^{-1}\nu\epsilon$, then the fixed point of $\epsilon^{-1}\nu\epsilon$ is $\epsilon^{-1} \cdot z$ by convention. By [20, 43.6.29], this CM point gives rise to an isomorphic abelian surface. □

Under this bijection, we get an action of $\mathrm{AL}(O)$ on $\mathcal{A}$ (equivalently, CM points on $\Gamma^\pm \backslash \mathfrak{H}^\pm$). Given a CM point $z \in \mathfrak{H}^\pm$ corresponding to an embedding $\nu \mapsto \beta^{-1}\nu\beta$, we have $K^\times \beta O^\times \in \mathrm{Emb}(S, O; O^\times)$. $[\omega] \in \mathrm{AL}(O)$ acts to give $K^\times \beta\omega O^\times = K^\times \beta\omega^{-1} O^\times$. On embedding representing this class is $\nu \mapsto \omega\beta^{-1}\nu\beta\omega^{-1}$, and the designated fixed point of this embedding is $\omega \cdot z$. So $[\omega] \in \mathrm{AL}(O)$ sends $\Gamma^\pm \cdot z \mapsto \Gamma^\pm \cdot (\omega \cdot z)$.

3.4.2. Shimura Reciprocity

By [20, Thm 43.8.1], there exists a projective nonsingular curve X defined over $\mathbb{Q}$ and an analytic isomorphism

$$\varphi : \Gamma^1 \backslash \mathfrak{H} \to X(\mathbb{C})$$

that respects the natural Galois action on CM points on $\Gamma^1 \backslash \mathfrak{H}$, which correspond to $\overline{\mathbb{Q}}$-points on $X(\overline{\mathbb{Q}})$.

Let $z \in \mathfrak{H}$ be a CM point corresponding to an optimal embedding $\iota_K : S \hookrightarrow O$ (extending to an embedding $\iota_K : K \hookrightarrow B$). We have the Artin isomorphism $\mathrm{Gal}(H \mid K) \cong \mathrm{Pic}(S)$. Lett $\sigma \in \mathrm{Gal}(H \mid K)$ and suppose $\sigma = \mathrm{Frob}_{\mathfrak{a}}$ for some invertible ideal $\mathfrak{a} \subseteq S$. Under the embedding ι_K, we have $\iota_K(\mathfrak{a})O = \xi O$ for some $\xi \in O$.

Theorem 3.4.3 (Shimura Reciprocity)**.** *With the notation as above, the object (A_z, ι_z) is defined over H. In other words, $\varphi(z) \in X(H)$. Furthermore,*

$$\sigma(\varphi(z)) = \varphi(\xi^{-1} \cdot z).$$

Proof. See [20, 43.8.2] and [19, Thm 5.1]. □

This theorem tells us that σ acts by sending z to $\xi^{-1} \cdot z$.

Proposition 3.4.4. *The action of* $\mathrm{Gal}(H \mid K) \cong \mathrm{Pic}(S)$ *agrees on both* $\mathcal{A}$ *and* $\mathrm{Emb}(S, O; O^\times)$.

Proof. Suppose we have an embedding $\nu \mapsto \beta^{-1}\nu\beta$. On one hand, this gives $K^\times \beta O^\times \in \mathrm{Emb}(S, O; O^\times)$. On the other hand, the fixed point of the embedding is some $z \in \mathfrak{H}^\pm$.

Let $\sigma \in \mathrm{Gal}(H \mid K)$ be $\sigma = \mathrm{Frob}_{\mathfrak{a}}$ for some ideal $\mathfrak{a} \subseteq S$. The embedding we are working from sends $\nu \mapsto \beta^{-1}\nu\beta$. For some $\xi \in O$, $\beta^{-1}\mathfrak{a}\beta O = \xi O$. Then σ (equivalently, $[\mathfrak{a}] \in \mathrm{Pic}(S)$) acts on $K^\times \beta O^\times$ to give $K^\times \beta \xi O$. One embedding in this class sends $\nu \mapsto \xi^{-1}\beta^{-1}\nu\beta\xi$. The fixed point of this new embedding is $\xi^{-1} \cdot z$. On the other hand, this is exactly what Shimura Reciprocity says it should be. □

3.4.3. Complex Conjugation

In the proof of Proposition 3.4.1, we brushed over the fact that fixed points of some embeddings might end up in the lower half-plane by convention. We would like to justify working with points in the upper and lower half-plane $\mathfrak{H}^\pm := \mathbb{C} \setminus \mathbb{R}$ so that we can talk about complex conjugation more naturally. To do this, we take as given from [20, 28.6.5] that there exists $\epsilon_0 \in O^\times$ with $\mathrm{nrd}(\epsilon_0) = -1$.

Let $\Gamma^\pm = \iota_\infty(O^\times)/\{\pm 1\}$.

Lemma 3.4.5. . *There is a bijection*

$$\Gamma^{\pm}\backslash\mathfrak{H}^{\pm} \longleftrightarrow \mathcal{A}$$

$$\Gamma^{\pm}\cdot\tau \mapsto [A_\tau, \iota_\tau].$$

Proof. From the proof of [20, 43.6.14], $A_{\epsilon_0\cdot z} \cong A_z$ as principally polarized abelian surfaces with QM by O. We will use this fact.

There we have an inclusion $\mathfrak{H} \hookrightarrow \mathfrak{H}^{\pm}$ that induces a map $\mathfrak{H} \to \Gamma^{\pm}\backslash\mathfrak{H}^{\pm}$. Since $\Gamma^1 \subset \Gamma^{\pm}$, we have an induced map

$$\Gamma^1\backslash\mathfrak{H} \to \Gamma^{\pm}\backslash\mathfrak{H}^{\pm}, \qquad \Gamma^1\cdot z \mapsto \Gamma^{\pm}\cdot z.$$

Given $z \in \mathfrak{H}^{\pm} \setminus \mathfrak{H}$, we know that $\epsilon_0 \cdot z \in \mathfrak{H}$, so

$$\Gamma^1\cdot(\epsilon_0\cdot z) \mapsto \Gamma^{\pm}\cdot(\epsilon_0\cdot z) = \Gamma^{\pm}\cdot z,$$

so the map is surjective. It is also injective: given $z, z' \in \mathfrak{H}$ with $z = \epsilon\cdot z'$ for some $\epsilon \in O^\times$, we must have $\mathrm{nrd}(\epsilon) < 0$, so$\epsilon \in O^1$ and $\Gamma^1\cdot z = \Gamma^1\cdot z'$. So we actually have a bijection

$$\Gamma^1\backslash\mathfrak{H} \longleftrightarrow \Gamma^{\pm}\backslash\mathfrak{H}^{\pm}, \qquad \Gamma^1\cdot z \mapsto \Gamma^{\pm}\cdot z.$$

The inverse of this map takes $\Gamma^{\pm}\cdot z$ to $\Gamma^1\cdot z$ if $z \in \mathfrak{H}$, or to $\Gamma^1\cdot(\epsilon_0\cdot z)$ if $z \notin \mathfrak{H}$. In either case, since $\Gamma^1\backslash\mathfrak{H}$ parametrizes principally polarized abelian surfaces with QM by O and $\epsilon_0\cdot z$ gives an isomorphic abelian surface, the result follows. □

How does complex conjugation act on CM points? According to [20, 43.7.1], complex conjugation acts naturally on $\Gamma^1\backslash\mathfrak{H}$ as

$$\Gamma^1 \cdot z \mapsto \Gamma^1 \cdot (\epsilon_0 \cdot z).$$

By the bijection above, this means the action on $\Gamma^{\pm}\backslash\mathfrak{H}^{\pm}$ is

$$\Gamma^{\pm} \cdot z \mapsto \Gamma^{\pm} \cdot \overline{z}.$$

This makes sense for a few reasons. First, if we have an analytic isomorphism $\varphi : \Gamma^1\backslash\mathfrak{H} \to X$ to some complex projective curve X defined over $\mathbb{Q}$ that respects Galois actions on both sides, we could hope to extend the map to the closure of the upper half-plane (including the real line) in such a way that the extension takes non-singular real values on the real axis. Then the *Schwarz reflection principle* would tell us that the analytic extension of φ to $\Gamma^{\pm}\backslash\mathfrak{H}^{\pm}$ must take $\varphi(\overline{z}) = \overline{\varphi(z)}$. Then the action of complex conjugation on $X(\mathbb{C})$ shows that the corresponding action on $\Gamma^{\pm}\backslash\mathfrak{H}^{\pm}$ should also send $z \mapsto \overline{z}$.

The other reason this makes sense is that it is *expected* that we could always construct an analytic isomorphism $\varphi : \Gamma^{\pm}\backslash\mathbb{C} \to X$, where X is a complex projective curve defined over $\mathbb{Q}$, and we further expect the power series representation of φ to have $\mathbb{Q}$-rational coefficients. This is the case of the j-function from $\mathrm{PSL}_2(\mathbb{Z})\backslash\mathfrak{H} \to \mathbb{C}$, which comes up when looking at elliptic curves (see [7, Thm 11.2]). With this isomorphism, complex conjugation on X can be pulled back to be exactly complex conjugation on $\mathfrak{H}^{\pm}$.

Proposition 3.4.6. *The action of complex conjugation on* $\mathrm{Emb}(S, O; O^{\times})$ *agrees with the action of complex conjugation on* $\mathcal{A}$.

Proof. Given an embedding $\nu \mapsto \beta^{-1}\nu\beta$, its class in $\mathrm{Emb}(S, O; O^{\times})$ is given by $K^{\times}\beta O^{\times}$. Complex conjugation then gives $K^{\times}j\beta O^{\times}$. This is represented by the embedding $\nu \mapsto \beta^{-1}j^{-1}\nu j\beta = \beta^{-1}j\nu j^{-1}\beta$.

Suppose that $z \in \mathfrak{H}^{\pm}$ is the fixed point of $\beta^{-1}\nu\beta$. Then by our convention, the designated fixed point of ν is $z_0 := \beta \cdot z$. Note that

$$\nu \cdot (j \cdot z_0) = \nu j \cdot z_0 = j\overline{\nu} \cdot z_0 = j \cdot (\overline{\nu} \cdot z_0) = j \cdot z_0.$$

So ν fixes $j \cdot z_0$. But $j \cdot z_0$ cannot be z_0 since $j \notin K^{\times}$, so $j \cdot z_0 = \overline{z_0}$. But $\beta \in \mathrm{M}_2(\mathbb{R})$, so

$$\beta^{-1} j \beta \cdot z = \beta^{-1} \cdot (j \cdot (\beta \cdot z)) = \beta^{-1} \cdot \overline{\beta \cdot z} = \beta^{-1} \cdot (\beta \cdot \overline{z}) = \overline{z}.$$

By our convention, this means that $\overline{z}$ is the designated fixed point of

$$(\beta^{-1} j \beta)(\beta^{-1} \nu \beta)(\beta^{-1} j \beta)^{-1} = \beta^{-1} j \nu j^{-1} \beta = \beta^{-1} j^{-1} \nu j \beta.$$

But this comes from the complex conjugate embedding of the embedding we started with. This shows that the actions agree. □

3.4.4. Putting It All Together

We are finally ready to put it all together. First, we need to resolve the choice of complex conjugation.

The action of complex conjugation on $\mathcal{A}$ that we have described comes from the actual automorphism of $\mathbb{C}$ that we call complex conjugation. By Shimura Reciprocity, we know that CM points corresponding to embeddings $S \hookrightarrow O$ are defined over H. Since we have some embedding of H into $\mathbb{C}$, complex conjugation restricts to some automorphism of H because $H \supset \mathbb{Q}$ is a Galois extension. We call this element $\sigma_C \in \mathrm{Gal}(H \mid \mathbb{Q})$.

The element σ_C is only well-defined up to conjugation by $\mathrm{Gal}(H \mid \mathbb{Q})$. In other words, if $\sigma \in \mathrm{Gal}(H \mid \mathbb{Q})$, then $\sigma^{-1}\sigma_C\sigma$ also comes from complex conjugation on $\mathbb{C}$ when the embedding of H into $\mathbb{C}$ is pre-composed with σ. Without loss of generality, we can take

$\sigma \in \mathrm{Gal}(H \mid K)$, since otherwise we have $\sigma = \sigma' \sigma_C$ for some $\sigma' \in \mathrm{Gal}(H \mid K)$, and

$$\sigma^{-1} \sigma_C \sigma = \sigma' \sigma_C \sigma'^{-1}.$$

Let σ_K be the nontrivial element of $\mathrm{Gal}(K \mid \mathbb{Q})$. Recall from Section 3.3 that we have an isomorphism

$$\begin{aligned} \mathrm{Gal}(H \mid K) \rtimes \mathrm{Gal}(K \mid \mathbb{Q}) &\cong \mathrm{Gal}(H \mid \mathbb{Q}), \\ (\sigma, \mathrm{Id}) &\mapsto \sigma \\ (\sigma, \sigma_K) &\mapsto \sigma \sigma_C. \end{aligned}$$

Then a different choice of σ_C is equivalent to post-composing this isomorphism with conjugation by some element of $\mathrm{Gal}(H \mid K)$. All we know, without more information, is that some choice of σ_C makes the action of σ_C on $\mathcal{A}$ agree with the action of complex conjugation on $\mathrm{Emb}(S, O; O^\times)$, and a different choice of σ_C will have the effect of applying some automorphism of H that fixes K.

What is the action of $\mathrm{Gal}(K \mid \mathbb{Q})$ on $\mathrm{Gal}(H \mid K)$ on the semidirect product? For a fractional S-ideal $\mathfrak{a}$, by [7, Cor 5.21],

$$\sigma_C \operatorname{Frob}_{\mathfrak{a}} \sigma_C^{-1} = \operatorname{Frob}_{\sigma_C(\mathfrak{a})} = \operatorname{Frob}_{\overline{\mathfrak{a}}} = \operatorname{Frob}_{\mathfrak{a}}^{-1}.$$

So $\mathrm{Gal}(K \mid \mathbb{Q})$ acts by inversion on $\mathrm{Gal}(H \mid K) \cong \mathrm{Pic}(S)$.

We return to the motivating question: what are the fields of moduli for various abelian surfaces?

Definition 3.4.7. Let $\sim$ be an equivalence relation on a set Θ of objects, and suppose $\mathrm{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ acts on Θ. Let $X = \Theta / \sim$ be the set of equivalence classes of objects in Θ. The *field of moduli* of an object $A \in \Theta$ is the fixed field of $\overline{\mathbb{Q}}$ by the subgroup of $\operatorname{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ generated by all σ such that $\sigma(A) \sim A$.

For our purposes, the equivalence relations we will look at are various notions of isomorphism, and the set of objects we will look at are principally polarized abelian surfaces with QM by O and CM by S. Accordingly, we will let Θ be the set of all such abelian surfaces equipped with a QM structure by O and CM by S. We know that $\operatorname{Gal}(\overline{\mathbb{Q}} \mid H)$ fixes every element of Θ by Shimura reciprocity, so it is equivalent to consider the action of $\operatorname{Gal}(H \mid \mathbb{Q})$ instead of all of $\operatorname{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$.

We are now ready to state our main theorem and its corollary about fields of moduli. Let O be a maximal order in an indefinite quaternion algebra B with discriminant Δ. Let $S = \mathbb{Z}[\nu]$ be an imaginary quadratic order of discriminant D that embeds optimally in O. Let n be the number of primes dividing Δ, and let r primes dividing Δ be ramified in S. Let $K = \mathbb{Q}(\nu)$ be the field of fractions of S, and let H be the ring class field of K associated to S.

Theorem 3.4.8 (Main Theorem)**.** *Let $\mathcal{A}$ be the set of isomorphism classes of principally polarized abelian surfaces with QM by O and CM by S.*

(a) *There are commuting actions of* $\operatorname{AL}(O)$ *and* $\operatorname{Gal}(H \mid \mathbb{Q})$ *on $\mathcal{A}$, and*

$$\#\mathcal{A} = h(S)2^{n-r}.$$

(b) *The group* $\operatorname{Gal}(H \mid K)$ *acts freely on $\mathcal{A}$ with 2^{n-r} orbits of size $h(S)$.*

(c) *The group* $\operatorname{AL}(O)$ *acts transitively on the set of* $\operatorname{Gal}(H \mid K)$*-orbits.*

(d) *Each element of* $\operatorname{AL}(O)$ *acts either trivially or without fixed points on $\mathcal{A}$. Given $[\omega_d] \in$* $\operatorname{AL}(O)$ *represented by $\omega_d \in N_{B^\times}(O) \cap O$ with* $\operatorname{nrd}(\omega_d) = d \mid \Delta$ *and $d > 0$, $[\omega_d]$ acts* *trivially on $\mathcal{A}$ if and only if S has an element of norm d. If S has an ideal $\mathfrak{a}$ of norm $d \mid \Delta$, then $[\omega_d]$ acts identically to $\mathrm{Frob}_{\mathfrak{a}} \in \mathrm{Gal}(H \mid K)$. If $[\omega_d]$ acts as some $\sigma \in \mathrm{Gal}(H \mid K)$ on some $A \in \mathcal{A}$, then there exists an invertible ideal $\mathfrak{a} \subseteq S$ of norm d such that $\sigma = \mathrm{Frob}_{\mathfrak{a}}$. So each element of $\mathrm{AL}(O)$ acts either trivially or without fixed points on the set of $\mathrm{Gal}(H \mid K)$-orbits.*

(e) *There exists $b \in \mathbb{Z}_{>0}$ such that $B \cong \left(\frac{D, b}{\mathbb{Q}}\right)$. Furthermore, there exists $\sigma_C \in \mathrm{Gal}(H \mid \mathbb{Q})$ in the conjugacy class of complex conjugation such that for all $A \in \mathcal{A}$, there exists an invertible fractional S-ideal $\mathfrak{c}$ of norm $b\Delta$ such that*

$$\sigma_C(A) = \mathrm{Frob}_{\mathfrak{c}}(A^{[\omega_\Delta]}).$$

(f) *If S is maximal, then for all fractional S-ideals $\mathfrak{c}$ of norm $b\Delta$, there exists $A \in \mathcal{A}$ such that*

$$\sigma_C(A) = \mathrm{Frob}_{\mathfrak{c}}(A^{[\omega_\Delta]}).$$

Proof. The action of $\mathrm{Gal}(H \mid \mathbb{Q})$ is described in the preceeding discussion as an action of $\mathrm{Gal}(H \mid K)$ and an action of complex conjugation. These actions together constitute an action of $\mathrm{Gal}(H \mid \mathbb{Q})$: we have $\mathrm{Gal}(H \mid \mathbb{Q})$ as a semidirect product of $\mathrm{Gal}(H \mid K)$ and $\mathrm{Gal}(K \mid \mathbb{Q})$, where $\mathrm{Gal}(K \mid \mathbb{Q})$ acts by inversion on $\mathrm{Gal}(H \mid K)$, and accordingly, the action of complex conjugation skew-commutes with the action of $\mathrm{Gal}(H \mid K)$ by Lemma 3.3.7. We use the bijection from Proposition 3.4.1 and looking at these actions on $\mathrm{Emb}(S, O; O^\times)$. By Lemma 3.2.5 and Lemma 3.3.6, the actions of $\mathrm{Gal}(H \mid K)$ and complex conjugation commute with the action of $\mathrm{AL}(O)$. By Proposition 3.2.14, there are 2^{n-r} orbits under the action of $\mathrm{Gal}(H \mid K)$, and since the action of $\mathrm{Gal}(H \mid K)$ is free, we get that $\#\mathrm{Emb}(S, O; O^\times) = 2^{n-r}h(S)$. This gives (a) and (b).

Proposition 3.2.14 gives (c). Propositions 3.2.7 and 3.2.8 give (d). Lemma 3.3.11 gives (e), and Lemma 3.3.13 gives (f). □

The main application of this theorem is to describe exactly what the fields of moduli of elements of $\mathcal{A}$ are up to equivalence by some subgroup $\Gamma \leq \mathrm{AL}(O)$. In other words, what are the fields of moduli of elements of $\mathcal{A}/\Gamma$?

Corollary 3.4.9 (Main Corollary)**.** *Keep all of the conditions and notation of Theorem 3.4.8. Let $\Gamma \leq \mathrm{AL}(O)$ be a subgroup, and let k_Γ be the field of moduli of an element of $\mathcal{A}/\Gamma$.*

(a) *Let $\mathfrak{a} \subseteq S$ be an ideal of norm d. Then k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}$ if and only if $[\omega_d] \in \Gamma$.*

(b) *If k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}\,\sigma_C$, then $[\mathfrak{a}]$ can be represented by a fractional S-ideal $\mathfrak{a}$ of norm db for some $d \mid \Delta$ with $[\omega_d] \in \Gamma$. Conversely, if S is maximal and $\mathfrak{a}$ is a fractional S-ideal of norm db and $\mathfrak{c}$ is a fractional ideal of norm $b\Delta$ such that $(db)^{-1}\mathfrak{a}\mathfrak{c}$ is integral, then there is some $A \in \mathcal{A}$ such that k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}\,\sigma_C$.*

Proof. We have that $\mathrm{Frob}_{\mathfrak{a}}$ acts as $[\omega_d]$ if and only if $[\mathfrak{a}]$ can be represented by an ideal in S of norm d, which gives the first statement.

Now suppose k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}\,\sigma_C$. Then $\mathrm{Frob}_{\mathfrak{a}}\,\sigma_C(A) = A^{[\omega_d]}$ for some $[\omega_d] \in \Gamma$. By the results of the preceeding section, for some $e \in \mathrm{Emb}(S, O; O^\times)$, and for some fractional S-ideal $\mathfrak{c}$ of norm $b\Delta$,

$$e^{[\omega_d]} = [\mathfrak{a}] \cdot j(e) = [\mathfrak{a}\mathfrak{c}] \cdot e^{[\omega_\Delta]}.$$

Then

$$[\mathfrak{a}\mathfrak{c}] \cdot e = e^{[\omega_{\Delta/d}]},$$

so we can rescale $\mathfrak{a}$ by $K^\times$ so that the norm of $\mathfrak{a}\mathfrak{c}$ is Δ/d. Rescaling again, we can make $\mathfrak{a}\mathfrak{c}$ have norm Δd. Then

$$\Delta d = \mathrm{Nm}^K_{\mathbb{Q}}(\mathfrak{a}\mathfrak{c}) = \mathrm{Nm}^K_{\mathbb{Q}}(\mathfrak{a}) b\Delta,$$

so $\mathrm{Nm}^K_{\mathbb{Q}}(\mathfrak{a}) = d/b$. We can rescale $\mathfrak{a}$ again by b to give it the norm db.

Conversely, suppose a fractional S-ideal $\mathfrak{a}$ of norm db exists, where $d \mid \Delta$ is such that $[\omega_d] \in \Gamma$. Suppose also that S is maximal. For any fractional S-ideal $\mathfrak{c}$ of norm $b\Delta$, so $\mathfrak{ac}$ has norm $db^2\Delta$. Then $\mathfrak{a}$ can be rescaled by $(db)^{-1}$ to give $\mathfrak{ac}$ the norm Δ/d. We suppose that $\mathfrak{ac}$ is integral at this point. Then for some $e \in \mathrm{Emb}(S, O; O^\times)$,

$$e^{[\omega_{\Delta/d}]} = [\mathfrak{ac}] \cdot e = [\mathfrak{a}] \cdot j(e)^{[\omega_\Delta]}.$$

Then

$$e^{[\omega_d]} = e^{[\omega_{\Delta/d}][\omega_\Delta]} = ([\mathfrak{a}] \cdot j(e)^{[\omega_\Delta]})^{[\omega_\Delta]} = \mathfrak{a} \cdot j(e).$$

In terms of abelian surfaces, this means that $\mathrm{Frob}_{\mathfrak{a}}\, \sigma_C(A) = A^{[\omega_d]}$ for some $A \in \mathcal{A}$, so k_Γ is fixed by $\mathrm{Frob}_{\mathfrak{a}}\, \sigma_C$. □

3.4.5. An Application: Solving Gauss's Class Number 1 Problem

Recall Gauss's Class Number 1 Problem from Section 1.1. We would like to determine all fundamental discriminants D of imaginary quadratic orders such that $h(D) = 1$. We need a "little" lemma first.

Lemma 3.4.10. *Let S be an imaginary quadratic order of discriminant D, and suppose $h(S) = 1$. If p is a prime less than $|D|/4$, then p is inert in S.*

Proof. Suppose p is not inert in S. Then there exists a prime $\mathfrak{p} \subset S$ of norm p. Since S has class number 1, $\mathfrak{p} = \alpha S$ for some $\alpha \in S$. We also have

$$p = \mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{p}) = \mathrm{Nm}_{\mathbb{Q}}^{K}(\alpha).$$

On the other hand, $\alpha = \frac{1}{2}(x + y\sqrt{D})$ for some $x, y \in \mathbb{Z}$, so

$$p = \frac{1}{4}(x^2 - Dy^2) \geq |D|/4.$$

This is a contradiction, so p must be inert in S. $\square$

Theorem 3.4.11. *There are exactly 9 imaginary quadratic orders S with class number 1. Their discriminants are*

$$D = -3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163.$$

Proof. We check with Magma [6] that these discriminants all have class number 1. We must show that there are no others.

Let B be the quaternion algebra over $\mathbb{Q}$ with discriminant $\Delta = 91 = 7 \cdot 13$. This is an indefinite division quaternion algebra. Let O be a maximal order. We have

$$\mathrm{AL}(O) = \{[1], [\omega_7], [\omega_{13}], [\omega_{91}]\}.$$

There exists a projective, genus 2 curve X that is a moduli space for $[\omega_{91}]$-equivalence classes of isomorphism classes of principally polarized abelian surfaces with QM by O [10, Table 4.1]. It has a defining equation given by

$$y^2 = -x^6 + 19x^4 - 3x^2 + 1.$$

The homogenization of this equation is

$$y^2z^4 + x^6 - 19x^4z^2 + 3x^2z^4 - z^6.$$

Since X is a moduli space for these classes, the Galois action is respected. In particular, if $A \in \mathcal{A}$ has field of moduli $\mathbb{Q}$, it will give a $\mathbb{Q}$-rational point on X. We want to show that the CM points corresponding to class number 1 maximal imaginary quadratic orders are rational. By Shimura reciprocity, the class number 1 CM points are at least K-rational.

Complex conjugation acts on CM points by $[\omega_{91}]$, so trivially on X. Then the class number 1 CM points are rational.

We calculate with Sage code from Francesca Bianchi [4] that there are 9 distinct rational points on X, counted with multiplicity. The code uses a technique called *quadratic Chabauty*, explained in more detail in [5, §6]. All of these points are nonsingular, except a point $[0 : 1 : 0]$ at infinity. Indeed, calculating the partials of the above equation for X, we get three expressions

$$6x^5 - 76x^3z^2 + 6xz^4, \qquad 2yz^4, \qquad 4y^2z^3 - 38x^4z + 12x^2z^3 - 6z^5.$$

These partials all vanish at $[0 : 1 : 0]$. Pulling back the 9 rational points on X, we then get 10 $[\omega_{91}]$-equivalence classes of isomorphism classes of principally polarized abelian surfaces with QM by O and CM.

Of the discriminants listed above, the ones for which S embeds optimally in O are

$$D = -7, -8, -11, -28, -67, -163.$$

For $D = -7, -28$, S has 7 ramified and 13 inert in S. Then $[\omega_7]$ acts trivially on $\operatorname{Emb}(S, O; O^\times)$, while $[\omega_{13}]$ and $[\omega_{91}]$ act the same, nontrivially. After modding out by $[\omega_{91}]$, we are left with only one CM point for each of these: $\# \operatorname{Emb}(S, O; \langle[\omega_{91}]\rangle) = 1$. For $D = -8, -11, -67, -163$, S has 7 and 13 inert. Then $\mathrm{AL}(O)$ acts freely and transitively on $\operatorname{Emb}(S, O; O^\times)$, and $\# \operatorname{Emb}(S, O; O^\times) = 4$. After modding out by $[\omega_{91}]$, $\# \operatorname{Emb}(S, O; \langle[\omega_{91}]\rangle) = 2$. In total, this would give us 10 points: 4 pairs, and 2 singles. It follows that if S is an class number 1 imaginary quadratic order with 7 and 13 either ramified or inert, and if S embeds optimally in O, then D must be one of $-7, -8, -11, -28, -67, -163$.

Now suppose S does not embed optimally in S. Then one or both of 7 or 13 is not inert in S. Then by Lemma 3.4.10, 7 or 13 is greater than or equal to $|D|/4$, so $D \leq 4 \cdot 13 = 52$.

We check with Magma [6] that we have already found all such discriminants D. □

Chapter 4

Examples and Data

Section 4.1

Further Consequences

In this section, we state some consequences of the theory we have developed.

For some applications, it is useful to know when $k_{\mathrm{AL}(O)} = \mathbb{Q}$ is as small as possible. For example, we need this to produce the tables of Baba and Granath [2].

Proposition 4.1.1. *If* $k_{\mathrm{AL}(O)} = \mathbb{Q}$*, then* $\mathrm{Pic}(S)$ *is isomorphic to a quotient of a subgroup of* $\mathrm{AL}(O)$*. Explicitly, if* $\Gamma_{\mathrm{Pic}} := \mathrm{Stab}_{\mathrm{AL}(O)}(\mathrm{Pic}(S) \cdot e)$ *for some* $e \in \mathrm{Emb}(S, O; O^\times)$ *and* $\Gamma_0 := \mathrm{Stab}_{\mathrm{AL}(O)}(e)$*, then*

$$\mathrm{Pic}(S) \cong \Gamma_{\mathrm{Pic}}/\Gamma_0.$$

Proof. Suppose $k_{\mathrm{AL}(O)} = \mathbb{Q}$ for some $A \in \mathcal{A}$. In particular, $k_{\mathrm{AL}(O)}$ is fixed by all elements of $\mathrm{Gal}(H \mid K)$. In terms of embeddings, for some embedding $e \in \mathrm{Emb}(S, O; O^\times)$, for all $[\mathfrak{a}] \in \mathrm{Pic}(S)$,

$$[\mathfrak{a}] \cdot e = e^{[\omega]}$$

for some $[\omega] \in \mathrm{AL}(O)$. It follows that $\mathrm{AL}(O)$ acts transitively on $\mathrm{Emb}(S, O; O^\times)$, e.g.

$\#\operatorname{Emb}(S, O; N_{B^\times}(O)) = 1$.

By definition, Γ_{Pic} acts on $\operatorname{Pic}(S) \cdot e$, and the action is transitive because the action of $\operatorname{AL}(O)$ is transitive on embeddings. Since the action of $\operatorname{Pic}(S)$ is free, each element of $\operatorname{Pic}(S) \cdot e$ can be written uniquely as $[\mathfrak{a}] \cdot e$ for some $[\mathfrak{a}] \in \operatorname{Pic}(S)$. Given $[\omega] \in \Gamma_{\text{Pic}}$, there exists a unique $[\mathfrak{a}] \in \operatorname{Pic}(S)$ such that $e^{[\omega]} = [\mathfrak{a}] \cdot e$. This defines a surjective map

$$\begin{aligned} \psi : \Gamma_{\text{Pic}} &\to \operatorname{Pic}(S) \\ [\omega] &\mapsto [\mathfrak{a}]. \end{aligned}$$

We claim that the map ψ is a group homomorphism. Let $[\omega], [\omega'] \in \Gamma_{\text{Pic}}$ and let $[\mathfrak{a}] = \psi([\omega])$ and $[\mathfrak{a}'] = \psi([\omega'])$. By definition,

$$[\mathfrak{a}] \cdot e = e^{[\omega]} \qquad \text{and} \qquad [\mathfrak{a}'] \cdot e = e^{[\omega']}.$$

Then

$$[\mathfrak{a}][\mathfrak{a}'] \cdot e = [\mathfrak{a}] \cdot e^{[\omega']} = ([\mathfrak{a}] \cdot e)^{[\omega']} = (e^{[\omega]})^{[\omega']} = e^{[\omega][\omega']}.$$

From the definition of ψ, this gives

$$\psi([\omega][\omega']) = [\mathfrak{a}][\mathfrak{a}'] = \psi([\omega])\psi([\omega']).$$

It remains to show that the kernel of ψ is Γ_0. We have $[\omega] \in \Gamma_0$ if and only if $e^{[\omega]} = e = [1] \cdot e$ if and only if $\psi([\omega]) = [1] \in \operatorname{Pic}(S)$, if and only if $[\omega] \in \ker \psi$. □

Corollary 4.1.2. *Let Δ be the product of n primes. If $k_{\operatorname{AL}(O)} = \mathbb{Q}$, then $\operatorname{Pic}(S)$ is an abelian group of exponent 2 and order at most 2^n. In other words, if $\operatorname{Pic}(S)$ is not trivial, then it is isomorphic to $\prod_{t=1}^{n} \mathbb{Z}/2\mathbb{Z}$.*

Proof. By Proposition 2.2.14, $\operatorname{AL}(O)$ is an abelian and has exponent 2, so any quotient of any subgroup must also be an abelian group with exponent 2 and order less than or equal to $\# \operatorname{AL}(O) = 2^n$. The result follows from Proposition 4.1.1. □

Corollary 4.1.3. *Suppose $k_{\operatorname{AL}(O)} = \mathbb{Q}$. Then complex conjugation acts as an Atkin-Lehner element, i.e. there exists $[\omega_C] \in \operatorname{AL}(O)$ such that for all $e \in \operatorname{Emb}(S, O; O^\times)$,*

$$j(e) = e^{[\omega_C]}.$$

Furthermore, j can be rescaled by an element of $K^\times$ so that b is an integer dividing Δ and j acts as $[\omega_b]$.

Proof. Since $k_{\operatorname{AL}(O)} = \mathbb{Q}$, we know that every element of $\operatorname{Pic}(S)$ has order at most 2, and $\operatorname{AL}(O)$ act transitively on embeddings. Let $e_0 \in \operatorname{Emb}(S, O; O^\times)$. Then there exists $[\omega_C] \in \operatorname{AL}(O)$ such that $j(e_0) = e_0^{[\omega_C]}$. Every other element of $\operatorname{Emb}(S, O; O^\times)$ is of the form $e_0^{[\omega]}$ for $[\omega] \in \operatorname{AL}(O)$. Then

$$j(e_0^{[\omega]}) = j(e_0)^{[\omega]} = (e_0^{[\omega_C]})^{[\omega]} = e_0^{[\omega][\omega_C]} = (e_0^{[\omega]})^{[\omega_C]}.$$

In terms of double-cosets, $K^\times j\beta O^\times = K^\times \beta\omega_C O^\times$ for all $\beta \in E$. Taking norms, $|\operatorname{nrd}(\alpha j)| = |\operatorname{nrd}(\omega_C)|$ for some $\alpha \in K^\times$. Then $\operatorname{nrd}(\alpha)b = |\operatorname{nrd}(\omega_C)|$. Since $\omega_C \in N_{B^\times}(O)$ could be chosen to have norm dividing Δ, and j can be rescaled by elements of $K^\times$, we can arrange so that $b = j^2 = -\operatorname{nrd}(j)$ divides Δ and is the norm of ω_C. □

We actually have necessary and sufficient conditions on $\operatorname{Pic}(S)$ that tell us when

$$k_{\operatorname{AL}(O)} = \mathbb{Q}.$$

Proposition 4.1.4. *We have $k_{\operatorname{AL}(O)} = \mathbb{Q}$ if and only if $\operatorname{Pic}(S)$ is generated by the primes of S lying over primes of Δ that are ramified in S.*

Proof. We know that $k_{\mathrm{AL}(O)} = \mathbb{Q}$ if and only if $\mathrm{AL}(O)$ acts transitively on $\mathrm{Emb}(S, O; O^\times)$. Suppose that $\mathrm{AL}(O)$ acts transitively. Let m be the product of all primes dividing Δ that are ramified in S. Suppose p is a prime dividing m. Then there is a prime $\mathfrak{p} \subset S$ with $\mathrm{Nm}_{\mathbb{Q}}^{K}(\mathfrak{p}) = p$. From Proposition 3.2.8, $[\mathfrak{p}] \cdot e = e^{[\omega_p]}$ for all $e \in \mathrm{Emb}(S, O; O^\times)$. By Lemma 3.2.10, Γ_{Pic} is generated by $\{[\omega_p] : p \mid m \text{ is prime}\}$. Via the isomorphism ψ in Proposition 4.1.1, $\mathrm{Pic}(S)$ is generated by $\{[\mathfrak{p}_p] \in \mathrm{Pic}(S) : p \mid m \text{ is prime}\}$, where $\mathfrak{p}_p$ is the prime of S lying over p.

Conversely, suppose $\mathrm{Pic}(S)$ is generated by $P := \{[\mathfrak{p}_p] \in \mathrm{Pic}(S) : p \mid m\}$. Since $\mathfrak{p}_p \subset S$ has norm p, the elements $[\omega_p] \in \Gamma_{\mathrm{Pic}}$ act as the elements of P on $\mathrm{Emb}(S, O; O^\times)$. But then Atkin-Lehner elements take any embedding to any other embedding, since $\mathrm{AL}(O)$ already acts transitively on $\Omega(S, O)$ by Proposition 3.2.14. □

Section 4.2

Examples and Tables

We extend some of the tables of Baba and Granath [2] with additional information, and we break the tables into cases based on the splitting behavior of primes dividing the discriminant of the quaternion algebra being considered. Computations regarding Picard groups, splitting of primes, and ring class fields are done in Magma [6]. For $d \mid \Delta$, we abbreviate

$$k_d := k_{\langle [\omega_d] \rangle}.$$

We also take $k_1 = k_{[1]}$ to be the field of moduli corresponding to the trivial subgroup of $\mathrm{AL}(O)$.

In the Baba–Granath tables [2, Table 1, Table 2] for $\Delta = p_1 p_2$, the fields of moduli $k_{\mathrm{AL}(O)}$ (which Baba and Granath call $k_{\mathbb{Z}}$) are all $k_{\mathrm{AL}(O)} = \mathbb{Q}$. By Corollary 4.1.2, the possible values of $h(S)$ are 1, 2, or 4. By Proposition 4.1.4, the primes of S over p_1 and p_2 must generate

D	$K = k_1 = k_2 = k_3$	k_6
-19	$\mathbb{Q}(\sqrt{-19})$	$\mathbb{Q}$
-43	$\mathbb{Q}(\sqrt{-43})$	$\mathbb{Q}$
-67	$\mathbb{Q}(\sqrt{-67})$	$\mathbb{Q}$
-163	$\mathbb{Q}(\sqrt{-163})$	$\mathbb{Q}$

Table 4.1: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 6$, and 2 and 3 inert in S.

D	$K = k_1 = k_2 = k_5$	k_{10}
-3	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$
-27	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$
-43	$\mathbb{Q}(\sqrt{-43})$	$\mathbb{Q}$
-67	$\mathbb{Q}(\sqrt{-67})$	$\mathbb{Q}$
-163	$\mathbb{Q}(\sqrt{-163})$	$\mathbb{Q}$

Table 4.2: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 10$, and 2 and 5 inert in S.

the class group. For example, if $h(S) = 4$, then we must have both p_1 and p_2 ramified in S, and if $h(S) = 2$, then at least one of p_1 or p_2 is ramified in S.

Example 4.2.1. Suppose $\Delta = p_1p_2$ and p_1 and p_2 are inert in S, and suppose $k_{\mathrm{AL}(O)} = \mathbb{Q}$. Then the preceding discussion shows that $h(S) = 1$. Furthermore, by Corollary 3.3.10, complex conjugation acts the same as $[\omega_\Delta]$ on embeddings, so $k_\Delta \subset K = H$ is fixed by complex conjugation and $k_\Delta = \mathbb{Q}$. On the other hand, since p_1 and p_2 are inert, $[\omega_{p_1}]$ and $[\omega_{p_2}]$ have no fixed points in $\mathrm{Emb}(S, O; O^\times)$, and neither acts the same as $[\omega_\Delta]$, so $k_{p_1} = k_{p_2} = K$. Similarly, $k_1 = K$. See Table 4.2 and Table 4.2, which agree with the data in [2, Tables 1 & 2].

When $h(S) > 1$, H is a nontrivial extension of K. If k_d is fixed by $\sigma \in \mathrm{Gal}(H \mid K)$, then so is the compositum Kk_d. Conversely, if Kk_d is fixed by $\sigma \in \mathrm{Gal}(H \mid K)$, then so is k_d. It is useful to think of Kk_d as the field of moduli before considering the action of complex conjugation.

Example 4.2.2. Suppose that $\Delta = 2p$, that 2 is ramified and p is inert in S, and that $k_{\mathrm{AL}(O)} = \mathbb{Q}$. Then $h(S) \in \{1, 2\}$: if the prime above 2 is principal, then $h(S) = 1$, and

$h(S) = 2$ otherwise. We know that $[\omega_2]$ acts as $[\mathfrak{p}_2] \in \operatorname{Pic}(S)$ and $[\omega_p]$ acts freely on $\Omega(S, O)$. It follows that $\#\operatorname{Emb}(S, O; O^\times) = 2$ if $h(S) = 1$ and $\#\operatorname{Emb}(S, O; O^\times) = 4$ if $h(S) = 2$. We can also conclude that k_2 is fixed by $\sigma_2 := \operatorname{Frob}_{\mathfrak{p}_2} \in \operatorname{Gal}(H \mid K)$. On the other hand, k_1 and k_p are not fixed by $\operatorname{Frob}_{\mathfrak{p}_2}$ by the Main Corollary 3.4.9. Is k_{2p} fixed by σ_2? We have k_{2p} fixed by σ_2 if and only if $[\mathfrak{p}_2] \cdot e = e^{[\omega_{2p}]} = [\mathfrak{p}_2] \cdot e^{[\omega_p]}$ for all $e \in \operatorname{Emb}(S, O; O^\times)$. This is true if and only if $[\omega_p]$ acts trivially on embeddings, which is true if and only if S has an element of norm p. Since p is inert in S, this cannot be true, so k_{2p} is not fixed by σ_2.

Suppose further that S is maximal. We know from Corollary 4.1.3 that j acts on $\operatorname{Emb}(S, O; O^\times)$ as an Atkin-Lehner element and since B is a division algebra, $b \neq 1$. Then we can arrange so that $b \in \{2, p, 2p\}$. Since p does not divide D, then p must divide b: otherwise $(D, b)_p = 1$, which contradicts $p \mid \Delta$. So $b \in \{p, 2p\}$.

From here, it is best to look on a case-by-case basis and apply the Main Theorem 3.4.8. The results of these calculations are given in Tables 4.2 and 4.2. We look at some specific cases to show how the calculations go.

Example 4.2.3. Suppose $\Delta = 6$ and $D = -4$. Then $h(S) = 1$, 2 is ramified, 3 is inert, and S has an element of norm 2. Then $[\omega_2]$ acts trivially on embeddings, and $[\omega_3]$ acts freely, and $\#\operatorname{Emb}(S, O; O^\times)$. Since $h(S) = 1$, complex conjugation acts on embeddings as $[\omega_6]$, equivalently $[\omega_3]$. So we could take $b = 3$ or $b = 6$. Then k_1 and k_2 are not fixed by complex conjugation, while k_3 and k_6 are.

Example 4.2.4. Suppose $\Delta = 6$ and $D = -40$. Then $h(S) = 2$, 2 is ramified, 3 is inert, and $\operatorname{AL}(O)$ acts freely on embeddings. We know that $[\omega_2]$ acts as σ_2. We calculate $b = 6$ is a possible value, but 3 is not. Then complex conjugation acts as $[\omega_6]$. So k_1 is not fixed by anything in $\operatorname{Gal}(H \mid \mathbb{Q})$. We have k_2 fixed by σ_2, but not σ_C or $\sigma_C\sigma_2$. We have k_3 fixed by $\sigma_2\sigma_C$, but not σ_2 or σ_C. Finally, we have k_6 fixed by σ_C but not σ_2 or $\sigma_2\sigma_C$.

Suppose $k_{\operatorname{AL}(O)} = \mathbb{Q}$ and $\Delta = 2p$. Since we can label elements of $\operatorname{Emb}(S, O; O^\times)$ by Atkin-

D	$h(S)$	H	b	k_1	k_2	k_3	k_6
-4	1	$\mathbb{Q}(\sqrt{-1})$	$\{3,6\}$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}$	$\mathbb{Q}$
-40	2	$\mathbb{Q}(\sqrt{-10},\sqrt{5})$	6	$\mathbb{Q}(\sqrt{-10},\sqrt{5})$	$\mathbb{Q}(\sqrt{-10})$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{5})$
-52	2	$\mathbb{Q}(\sqrt{-13},\sqrt{13})$	3	$\mathbb{Q}(\sqrt{-13},\sqrt{13})$	$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Q}(\sqrt{13})$	$\mathbb{Q}(\sqrt{-1})$
-88	2	$\mathbb{Q}(\sqrt{-22},\sqrt{2})$	3	$\mathbb{Q}(\sqrt{-22},\sqrt{2})$	$\mathbb{Q}(\sqrt{-22})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{-11})$
-148	2	$\mathbb{Q}(\sqrt{-37},\sqrt{37})$	3	$\mathbb{Q}(\sqrt{-37},\sqrt{37})$	$\mathbb{Q}(\sqrt{-37})$	$\mathbb{Q}(\sqrt{37})$	$\mathbb{Q}(\sqrt{-1})$
-232	2	$\mathbb{Q}(\sqrt{-58},\sqrt{29})$	6	$\mathbb{Q}(\sqrt{-58},\sqrt{29})$	$\mathbb{Q}(\sqrt{-58})$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{29})$

Table 4.3: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 6$, with 2 ramified and 3 inert in S and S maximal. When $h(S) = 2$, we write H as $\mathbb{Q}(\alpha, \beta)$, where $K = \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ is the fixed field of complex conjugation. We also choose $b \in \{3, 6\}$.

Lehner elements in the case where $k_{\mathrm{AL}(O)} = \mathbb{Q}$, we get the following diagram representing the previous example:

$$\begin{tikzcd}
1 \arrow[dr, <->] & 2 \arrow[dl, <->] \\
p & 2p.
\end{tikzcd}$$

In this diagram, the arrows show the action of complex conjugation, and the numbers indicate which Atkin-Lehner involution the embedding class is labeled by. Note that $[\omega_2]$ and σ_2 swap horizontally, while $[\omega_p]$ swaps vertically.

As the next example demonstrates, the other possibility for the action of complex conjugation looks like

$$\begin{tikzcd}
1 \arrow[d, <->] & 2 \arrow[d, <->] \\
p & 2p.
\end{tikzcd}$$

Example 4.2.5. Suppose $\Delta = 6$ and $D = -52$. Then $h(S) = 2$, 2 is ramified, 3 is inert, and $\mathrm{AL}(O)$ acts freely on embeddings. We know that $[\omega_2]$ acts as σ_2. We calculate $b = 3$ as a possible value, whereas 6 is not. Then complex conjugation acts as $[\omega_3]$. So k_1 is not fixed by anything in $\mathrm{Gal}(H \mid \mathbb{Q})$, k_2 is fixed by σ_2 but not the others, k_3 is fixed by σ_C but not the others, and k_6 is fixed by $\sigma_C\sigma_2$ but not the others.

Suppose $\Delta = 2p$, but 2 is inert and 3 is ramified in S. Using the same techniques that

D	$h(S)$	H	b	k_1	k_2	k_5	k_{10}
-8	1	$\mathbb{Q}(\sqrt{-2})$	$\{5,10\}$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}(\sqrt{-2})$	$\mathbb{Q}$	$\mathbb{Q}$
-52	2	$\mathbb{Q}(\sqrt{-13},\sqrt{13})$	10	$\mathbb{Q}(\sqrt{-13},\sqrt{13})$	$\mathbb{Q}(\sqrt{-13})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{13})$
-88	2	$\mathbb{Q}(\sqrt{-22},\sqrt{2})$	5	$\mathbb{Q}(\sqrt{-22},\sqrt{2})$	$\mathbb{Q}(\sqrt{-22})$	$\mathbb{Q}(\sqrt{2})$	$\mathbb{Q}(\sqrt{-11})$
-148	2	$\mathbb{Q}(\sqrt{-37},\sqrt{37})$	10	$\mathbb{Q}(\sqrt{-37},\sqrt{37})$	$\mathbb{Q}(\sqrt{-37})$	$\mathbb{Q}(\sqrt{-1})$	$\mathbb{Q}(\sqrt{37})$
-232	2	$\mathbb{Q}(\sqrt{-58},\sqrt{29})$	5	$\mathbb{Q}(\sqrt{-58},\sqrt{29})$	$\mathbb{Q}(\sqrt{-58})$	$\mathbb{Q}(\sqrt{29})$	$\mathbb{Q}(\sqrt{-2})$

Table 4.4: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 10$, with 2 ramified and 5 inert in S and S maximal. When $h(S) = 2$, we write H as $\mathbb{Q}(\alpha, \beta)$, where $K = \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ is the fixed field of complex conjugation. We also choose $b \in \{5, 10\}$.

D	$h(S)$	H	b	k_1	k_2	k_3	k_6
-3	1	$\mathbb{Q}(\sqrt{-3})$	$\{2,6\}$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$	$\mathbb{Q}(\sqrt{-3})$	$\mathbb{Q}$
-51	2	$\mathbb{Q}(\sqrt{-51},\sqrt{17})$	2	$\mathbb{Q}(\sqrt{-51},\sqrt{17})$	$\mathbb{Q}(\sqrt{17})$	$\mathbb{Q}(\sqrt{-51})$	$\mathbb{Q}(\sqrt{-3})$
-123	2	$\mathbb{Q}(\sqrt{-123},\sqrt{41})$	2	$\mathbb{Q}(\sqrt{-123},\sqrt{41})$	$\mathbb{Q}(\sqrt{41})$	$\mathbb{Q}(\sqrt{-123})$	$\mathbb{Q}(\sqrt{-3})$
-267	2	$\mathbb{Q}(\sqrt{-267},\sqrt{89})$	2	$\mathbb{Q}(\sqrt{-267},\sqrt{89})$	$\mathbb{Q}(\sqrt{89})$	$\mathbb{Q}(\sqrt{-267})$	$\mathbb{Q}(\sqrt{-3})$

Table 4.5: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 6$, with 2 inert and 3 ramified in S and S maximal. When $h(S) = 2$, we write H as $\mathbb{Q}(\alpha, \beta)$, where $K = \mathbb{Q}(\alpha)$ is the fixed field of σ_3 and $\mathbb{Q}(\beta)$ is the fixed field of complex conjugation. We also choose $b \in \{2, 6\}$.

generated Tables 4.2 and 4.2, we generate Tables 4.2 and 4.2 where S is maximal. When $h(S) = 2$, we have one nontrivial element $\sigma_p \in \mathrm{Gal}(H \mid K)$ corresponding to the ideal class generated by the prime in S over p. Now the two possible diagrams are

$$\begin{tikzcd}
1 \arrow[dr, leftrightarrow] & p \arrow[dl, leftrightarrow] \\
2 & 2p
\end{tikzcd}$$

when complex conjugation acts as $[\omega_\Delta]$, and

$$\begin{tikzcd}
1 \arrow[d, leftrightarrow] & p \arrow[d, leftrightarrow] \\
2 & 2p
\end{tikzcd}$$

when complex conjugation acts as $[\omega_2]$.

D	$h(S)$	H	b	k_1	k_2	k_5	k_{10}
-35	2	$\mathbb{Q}(\sqrt{-35}, \sqrt{5})$	2	$\mathbb{Q}(\sqrt{-35}, \sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-35})$	$\mathbb{Q}(\sqrt{-7})$
-115	2	$\mathbb{Q}(\sqrt{-115}, \sqrt{5})$	2	$\mathbb{Q}(\sqrt{-115}, \sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-115})$	$\mathbb{Q}(\sqrt{-23})$
-235	2	$\mathbb{Q}(\sqrt{-235}, \sqrt{5})$	2	$\mathbb{Q}(\sqrt{-235}, \sqrt{5})$	$\mathbb{Q}(\sqrt{5})$	$\mathbb{Q}(\sqrt{-235})$	$\mathbb{Q}(\sqrt{-47})$

Table 4.6: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 10$, with 2 inert and 5 ramified in S and S maximal. When $h(S) = 2$, we write H as $\mathbb{Q}(\alpha, \beta)$, where $K = \mathbb{Q}(\alpha)$ is the fixed field of σ_5 and $\mathbb{Q}(\beta)$ is the fixed field of complex conjugation. We also choose $b \in \{2, 10\}$.

What about when 2 and p are ramified but $h(S) = 2$?

Example 4.2.6. Suppose $\Delta = 2p$, 2 and p are ramified in S, and $h(S) = 2$. Assume that no element of norm 2 or p exists in S. Then $[\omega_2]$ and $[\omega_p]$ act as the ideal classes of the corresponding primes over 2 and p. Then $\#\Omega(S, O) = 1$, so $\#\operatorname{Emb}(S, O; O^\times) = 2$. We know from Proposition 3.3.14 that complex conjugation acts freely on these 2 elements.

Let $\sigma \in \operatorname{Gal}(H \mid K)$ be the nontrivial element. For all $d \mid \Delta$, we have k_d fixed by $\sigma_C \sigma$, since $\sigma \sigma_C$ acts trivially. On the other hand, k_Δ is not fixed by σ or σ_C, since these act nontrivially on embeddings while $[\omega_\Delta]$ acts trivially. We also have k_2 and k_p fixed by σ and σ_C, since σ, σ_C, $[\omega_2]$, and $[\omega_p]$ all act in the same nontrivial way. Then $k_2 = k_p = \mathbb{Q}$.

Example 4.2.7. Suppose $\Delta = 10$ and $D = -20$. Then $h(S) = 2$, the primes 2 and 5 are ramified in S, but an element of norm 5 exists. Then $[\omega_2]$ acts as σ_2, but $[\omega_5]$ acts trivially. Then $\mathrm{AL}(O)$ acts transitively and $\#\Omega(S, O) = 1$, so $\#\operatorname{Emb}(S, O; O^\times) = 2$. Complex conjugation acts freely on these two embedding classes in the same way that σ_2 and $[\omega_2]$ do. Then for all $d \mid \Delta$, the field of moduli k_d is fixed by $\sigma_2 \sigma_C$. On the other hand, k_2 and k_{10} are fixed by σ_2, since σ_2 acts as $[\omega_2]$, or equivalently, $[\omega_{10}]$.

We calculate that $H = \mathbb{Q}(\sqrt{-5}, \sqrt{5})$, so

$$\sigma_2 : \begin{cases} \sqrt{-5} & \mapsto \sqrt{-5} \\ \sqrt{5} & \mapsto -\sqrt{5} \end{cases}, \qquad \text{and} \qquad \sigma_2\sigma_C : \begin{cases} \sqrt{-5} & \mapsto -\sqrt{-5} \\ \sqrt{5} & \mapsto -\sqrt{5} \end{cases}.$$

Then all of the fields of moduli are contained in $\mathbb{Q}(\sqrt{-1})$, but $k_2 = k_{10} = \mathbb{Q}$.

For higher class number, the fields of moduli become slightly harder to compute by hand. The following examples show what goes into the calculations.

Example 4.2.8. Let $\Delta = 6$ and $D = -84$, so that $K = \mathbb{Q}(\sqrt{-21})$. Both 2 and 3 are inert, $h(S) = 4$, and the primes over 2 and 3 in S generate the class group. Since $\mathrm{AL}(O)$ acts transitively, there are at most 4 elements in $\mathrm{Emb}(S, O; O^\times)$. But $\#\operatorname{Pic}(S) = 4$, so $\#\operatorname{Emb}(S, O; O^\times) = 4$. We calculate a possible value of b is $b = 2$ (and not 3 or 6), so complex conjugation acts as $[\omega_2]$ (equivalently, σ_2). Then for all $d \mid \Delta$, we have k_d fixed by $\sigma_C\sigma_2$. Then k_1 is not fixed by any other automorphisms. On the other hand, k_2 is fixed by σ_2 (and σ_C). We have k_3 fixed by σ_3, and k_6 fixed by $\sigma_2\sigma_3$.

We have $H = \mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt{7})$. We calculate that

$$\sigma_2 : \begin{cases} \sqrt{-1} & \mapsto -\sqrt{-1} \\ \sqrt{3} & \mapsto \sqrt{3} \\ \sqrt{7} & \mapsto -\sqrt{7} \end{cases}, \qquad \sigma_3 : \begin{cases} \sqrt{-1} & \mapsto -\sqrt{-1} \\ \sqrt{3} & \mapsto -\sqrt{3} \\ \sqrt{7} & \mapsto \sqrt{7} \end{cases}.$$

So

$$\sigma_C\sigma_2 : \begin{cases} \sqrt{-1} & \mapsto \sqrt{-1} \\ \sqrt{3} & \mapsto \sqrt{3} \\ \sqrt{7} & \mapsto -\sqrt{7} \end{cases},$$

and every field of moduli is a subfield of $k_1 = \mathbb{Q}(\sqrt{-1}, \sqrt{3})$. From the above calculations, $k_2 = \mathbb{Q}(\sqrt{3})$, $k_3 = \mathbb{Q}(\sqrt{-3})$, and $k_6 = \mathbb{Q}(\sqrt{-1})$.

Example 4.2.9. More generally, suppose $\Delta = 2p$, $k_{\mathrm{AL}(O)} = \mathbb{Q}$, and $\#\operatorname{Pic}(S) = 4$. We also assume that S is maximal so that the action of complex conjugation is uniquely determined by any possible value of b. Then 2 and p are ramified in S, and the primes over

D	H	b	k_1	k_b
-84	$\mathbb{Q}(\sqrt{-1},\sqrt{3},\sqrt{7})$	2	$\mathbb{Q}(\sqrt{-1},\sqrt{3})$	$\mathbb{Q}(\sqrt{3})$
-120	$\mathbb{Q}(\sqrt{-3},\sqrt{5},\sqrt{2})$	6	$\mathbb{Q}(\sqrt{-3},\sqrt{5})$	$\mathbb{Q}(\sqrt{5})$
-132	$\mathbb{Q}(\sqrt{-1},\sqrt{3},\sqrt{11})$	3	$\mathbb{Q}(\sqrt{-1},\sqrt{3})$	$\mathbb{Q}(\sqrt{3})$
-168	$\mathbb{Q}(\sqrt{-2},\sqrt{-3},\sqrt{-7})$	2	$\mathbb{Q}(\sqrt{-2},\sqrt{-3})$	$\mathbb{Q}(\sqrt{6})$
-228	$\mathbb{Q}(\sqrt{-1},\sqrt{3},\sqrt{19})$	6	$\mathbb{Q}(\sqrt{-1},\sqrt{3})$	$\mathbb{Q}(\sqrt{3})$
-312	$\mathbb{Q}(\sqrt{-3},\sqrt{13},\sqrt{2})$	3	$\mathbb{Q}(\sqrt{-3},\sqrt{13})$	$\mathbb{Q}(\sqrt{13})$
-372	$\mathbb{Q}(\sqrt{-1},\sqrt{3},\sqrt{31})$	2	$\mathbb{Q}(\sqrt{-1},\sqrt{3})$	$\mathbb{Q}(\sqrt{3})$
-408	$\mathbb{Q}(\sqrt{-3},\sqrt{17},\sqrt{2})$	2	$\mathbb{Q}(\sqrt{-3},\sqrt{17})$	$\mathbb{Q}(\sqrt{17})$
-708	$\mathbb{Q}(\sqrt{-1},\sqrt{3},\sqrt{-59})$	3	$\mathbb{Q}(\sqrt{-1},\sqrt{3})$	$\mathbb{Q}(\sqrt{3})$

Table 4.7: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 6$, with 2 and 3 ramified in S and $\#\operatorname{Pic}(S) = 4$. We choose b such that $b \mid \Delta$ and complex conjugation acts as $[\omega_b]$.

2 and p generate $\operatorname{Pic}(S)$, which must have exponent 2. Since $\mathrm{AL}(O)$ acts transitively, the number of elements in $\operatorname{Emb}(S, O; O^\times)$ is at most 4. But $\operatorname{Pic}(S)$ acts freely on this set, so $\#\operatorname{Emb}(S, O; O^\times) = 4$, and both $\operatorname{Pic}(S)$ and $\mathrm{AL}(O)$ act transitively. Furthermore, complex conjugation σ_C acts as some $[\omega] \in \mathrm{AL}(O)$, which in turn must act as some $\sigma_0 \in \operatorname{Gal}(H \mid K)$ Then $\sigma_0\sigma_C = \sigma_C\sigma_0^{-1} = \sigma_C\sigma_0 \in \operatorname{Gal}(H \mid \mathbb{Q})$ acts trivially, so k_1 is fixed by $\sigma_0\sigma_C$. Since if $\sigma = \operatorname{Frob}_{\mathfrak{a}} \in \operatorname{Gal}(H \mid K)$ acted trivially, then $\mathfrak{a}$ would be principal and $\sigma = \operatorname{Id}$. If $\sigma\sigma_C$ acted trivially, then so would $\sigma\sigma_C(\sigma_0\sigma_C)^{-1} = \sigma\sigma_0^{-1}$. Then $\sigma = \sigma_0$. It follows that k_1 is exactly the fixed field of $\sigma_0\sigma_C$.

If complex conjugation acts as $[\omega_d]$, then $b = d$ is a possible value, and $\sigma_0 = \operatorname{Frob}_{\mathfrak{a}}$ where $\mathfrak{a} \subset S$ is an ideal of norm d. Then k_d is fixed by σ_0 and σ_C. If k_d was fixed by $\sigma \in \operatorname{Gal}(H \mid K)$, then $\sigma\sigma_0^{-1}$ acts trivially, and $\sigma = \sigma_0$. If k_d was fixed by $\sigma\sigma_C$, then possibly $\sigma = \sigma_0$ and k_d is fixed by $\sigma_0\sigma_C$. Otherwise, $\sigma\sigma_0^{-1}$ acts as $[\omega_d]$, which acts as σ_0, so σ acts as $\sigma_0^2 = \operatorname{Id}$, and $\sigma = \operatorname{Id}$. It follows that k_d is exactly the fixed field of σ_0 and σ_C. Tables 4.2 and 4.2 show some examples for $\Delta = 6$ and $\Delta = 10$.

What if $k_{\mathrm{AL}(O)}$ is not $\mathbb{Q}$ or $\operatorname{Pic}(S)$ does not have exponent 2? The answers we get are no longer as nice.

Example 4.2.10. Suppose $\Delta = 35 = 5 \cdot 7$ and $D = -23$. We check that 5 and 7 are inert in

D	H	b	k_1	k_b
-120	$\mathbb{Q}(\sqrt{-6}, \sqrt{10}, \sqrt{-3})$	10	$\mathbb{Q}(\sqrt{-6}, \sqrt{10})$	$\mathbb{Q}(\sqrt{10})$
-280	$\mathbb{Q}(\sqrt{10}, \sqrt{-14}, \sqrt{5})$	2	$\mathbb{Q}(\sqrt{10}, \sqrt{-14})$	$\mathbb{Q}(\sqrt{10})$
-340	$\mathbb{Q}(\sqrt{-1}, \sqrt{17}, \sqrt{-5})$	2	$\mathbb{Q}(\sqrt{-1}, \sqrt{17})$	$\mathbb{Q}(\sqrt{17})$
-520	$\mathbb{Q}(\sqrt{-2}, \sqrt{13}, \sqrt{5})$	10	$\mathbb{Q}(\sqrt{-2}, \sqrt{13})$	$\mathbb{Q}(\sqrt{13})$
-760	$\mathbb{Q}(\sqrt{10}, \sqrt{-38}, \sqrt{2})$	5	$\mathbb{Q}(\sqrt{10}, \sqrt{-38})$	$\mathbb{Q}(\sqrt{10})$

Table 4.8: $k_{\mathrm{AL}(O)} = \mathbb{Q}$, $\Delta = 10$, with 2 and 5 ramified in S and $\#\operatorname{Pic}(S) = 4$. We choose b such that $b \mid \Delta$ and complex conjugation acts as $[\omega_b]$.

S, so S embeds in O optimally. Also, $\operatorname{Pic}(S) \cong \mathbb{Z}/3\mathbb{Z}$ is generated by a prime $\mathfrak{p}_2$ over 2. So $k_{\mathrm{AL}(O)}$ cannot be $\mathbb{Q}$, since primes over 5 and 7 do not generate $\operatorname{Pic}(S)$. Furthermore, $\mathrm{AL}(O)$ acts freely on $\Omega(S, O)$, so $\#\Omega(S, O) = 4$ and $\#\operatorname{Emb}(S, O; O^\times) = 12$.

Different points will have different fields of moduli. A possible value for b is $b = 35$. An ideal of norm $b\Delta = 35^2$ is $35S$, so there is some $e \in \operatorname{Emb}(S, O; O^\times)$ such that $j(e) = e^{[\omega_{35}]}$.

$$j([\mathfrak{p}_2] \cdot e) = [\mathfrak{p}_2]^{-1} \cdot j(e) = [\mathfrak{p}_2]^2 \cdot e^{[\omega_{35}]} = [\mathfrak{p}_2] \cdot ([\mathfrak{p}_2] \cdot e)^{[\omega_{35}]}.$$

This tells us that k_{35} is fixed by complex conjugation for one embedding, but not for another embedding.

Section 4.3

Future work

4.3.1. Non-Maximal CM Orders

Most of what we have done applies when the CM order S is not maximal, but we assumed that S was maximal when determining exactly how complex conjugation acts on optimal embeddings. Concretely, recall that for $e \in \operatorname{Emb}(S, O; O^\times)$, there exists some $[\mathfrak{c}] \in \operatorname{Pic}(S)$ such that

$$j(e) = [\mathfrak{c}] \cdot e^{[\omega_\Delta]}.$$

We made no assumptions about S being maximal when computing possible norms of $\mathfrak{c}$. However, we did make use of the maximality of S in Lemma 3.3.12 and Lemma 3.3.13. These Lemmas help identify the action of complex conjugation when $\mathrm{Pic}(S)$ is nontrivial. Future work could work to prove similar results when S is not maximal.

4.3.2. Different Ground Fields

We worked with quaternion algebras over $\mathbb{Q}$ and orders over $\mathbb{Z}$. However, we only really needed $\mathbb{Q}$ to be a totally real field with a ring of integers that is a PID. Future work might generalize our results to different ground rings. This generalization also holds hope for new solutions to the class number 1 problem over other totally real fields.

Bibliography

[1] Atiyah, Michael Francis, and I. G. (Ian Grant) Macdonald. *Introduction to Commutative Algebra.* Addison-Wesley Series in Mathematics. Cambridge, Mass: Perseus Books, 2000.

[2] Srinath Baba, and Håkan Granath. "Genus 2 Curves with Quaternionic Multiplication." *Canadian journal of mathematics* 60, no. 4 (2008): 734–757.

[3] Baker, A. "Linear Forms in the Logarithms of Algebraic Numbers." *Mathematika* 13, no. 2 (1966): 204–16. https://doi.org/10.1112/S0025579300003971.

[4] F. Bianchi. Code for "Quadratic Chabauty for (bi)elliptic curves and Kim's conjecture", 2019, available at https://github.com/bianchifrancesca/quadratic_chabauty. Sage math code.

[5] Bianchi, Francesca. "Quadratic Chabauty for (Bi)Elliptic Curves and Kim's Conjecture." *Algebra & Number Theory* 14, no. 9 (2020): 2369–2416. https://doi.org/10.2140/ant.2020.14.2369.

[6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. 24 (1997), vol. 3–4, 235–265.

[7] David A. Cox, *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, second edition, John Wiley & Sons, Inc., Hoboken, NJ, 2013.

[8] Dummit, David Steven, and Richard M. Foote. *Abstract Algebra*. 3rd ed. Hoboken, NJ: Wiley, 2004.

[9] Fite, Francesc, and Xavier Guitart. “Endomorphism Algebras of Geometrically Split Abelian Surfaces over Q.” *Algebra & Number Theory* 14, no. 6 (2020): 1399–1421. https://doi.org/10.2140/ant.2020.14.1399.

[10] González, Josep, and Victor Rotger. “Equations of Shimura Curves of Genus Two.” *International Mathematics Research Notices* 2004, no. 14 (2004): 661–74. https://doi.org/10.1155/S1073792804131826.

[11] Heegner, Kurt. “Diophantische Analysis Und Modulfunktionen.” *Mathematische Zeitschrift* 56, no. 3 (1952): 227–53. https://doi.org/10.1007/BF01174749.

[12] Katok, Svetlana. *p-Adic Analysis Compared with Real*. Student Mathematical Library P-Adic Analysis Compared with Real. Providence, Rhode Island: American Mathematical Society, 2007.

[13] Marcus, Daniel A. *Number Fields*. Second edition. Universitext. Cham: Springer, 2018.

[14] Rotger, Victor. “The Field of Moduli of Quaternionic Multiplication On Abelian Varieties.” *International Journal of Mathematics and Mathematical Sciences* 2004, no. 52 (2004): 2795–2808. https://doi.org/10.1155/S0161171204302243.

[15] Rotger, Victor. “Modular Shimura Varieties and Forgetful Maps.” *Transactions of the American Mathematical Society* 356, no. 4 (2004): 1535–50. https://doi.org/10.1090/S0002-9947-03-03408-1.

[16] Serre, Jean-Pierre, Michel Waldschmidt, and Martin. Brown. *Lectures on the Mordell-Weil Theorem*. Aspects of Mathematics, Vol. E15 = Aspekte Der Mathematik. Braunschweig: F. Vieweg, 1989.

[17] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*. Publications of the Mathematical Society of Japan 11, Princeton University Press, Princeton, NJ, 1971.

[18] Stark, H.M. “On the ‘Gap’ in a Theorem of Heegner.” *Journal of Number Theory* 1, no. 1 (1969): 16–27. https://doi.org/10.1016/0022-314X(69)90023-7.

[19] Voight, John. “Computing CM Points on Shimura Curves Arising from Cocompact Arithmetic Triangle Groups” 4076 (2006): 406–20.

[20] Voight, John. *Quaternion Algebras*. Graduate Texts in Mathematics 288. Springer International Publishing, 2021.