Carl von Ossietzky
Universität
Oldenburg

On simple polarized abelian varieties of dimension 3 with CM by non-maximal orders

Herr Marco Melles,
geboren am 15. Mai 1991 in Norderney

Von der Fakultät für Mathematik und Naturwissenschaften der Carl von Ossietzky Universität Oldenburg zur Erlangung des Grades und Titels eines Doktors der Naturwissenschaften (Dr. rer. nat.) angenommene Dissertation

Tag der Disputation: 17.10.2023

Erstgutachter: Prof. Dr. Andreas Stein
Zweitgutachterin: Prof. Dr. Anne Frühbis-Krüger
Weiteres Mitglied der Prüfungskommision: Prof. Dr. Florian Hess

Acknowledgements

I want to thank my supervisor Prof. Dr. Andreas Stein for giving me the chance to grow as a person and as a mathematician during the process of working on this thesis and for the hints such as the regular discussions. I also thank Prof. Dr. Marco Streng and Prof. Dr. Jeroen Sijsling for the correspondence, especially for helping me to better understand the algorithmic aspects. Additionally, I want to thank Dr. Pınar Kılıçer for the first discussions on this topic and helping me find my way into complex multiplication theory. Last but not least, I want to thank my good friend Dr. Ingo Schoolmann for being a big support during this journey.

Abstract

This thesis discusses simple polarized abelian varieties with complex multiplication by an arbitrary order S in a CM field K, especially the case in which the field of moduli k_0 is contained in the reflex field K^r of a CM type (K, Φ). From Shimuras third main theorem, we deduce necessary conditions on the orders S and apply them to the dimension 3 case, focusing on field of moduli $\mathbb{Q}$. We construct explicit bounds on the primes dividing the index $[\,\mathcal{O}_K : S\,]$ and their exponents. In some interesting special cases, the results allow constructing a certain minimal order, which is contained in every possible order S appearing as the endomorphism ring of a simple polarized abelian variety with complex multiplication and field of moduli $\mathbb{Q}$. This allows to apply our results to simple genus 3 CM curves and algorithmically analyze $\bar{\mathbb{Q}}$-isomorphism classes of their Jacobians. In the end, we are able to show that there are no simple genus 3 hyperelliptic or Picard curves of a certain kind, which have complex multiplication by a non-maximal order S and field of moduli $\mathbb{Q}$. Additionally, this thesis includes an algorithmic analysis of orders in cubic number fields and their property of being Gorenstein.

Zusammenfassung

In dieser Arbeit besprechen wir einfache polarisierte abelsche Varietäten mit komplexer Multiplikation bezüglich einer Ordnung S in einem CM Körper K, insbesondere in dem Fall, dass der Modulkörper k_0 in dem Reflexkörper K^r von einem CM Typ (K, Φ) liegt. Ausgehend von Shimuras drittem Hauptsatz folgern wir notwendige Bedingungen an die Ordnungen S und wenden diese auf den Dimension 3 Fall mit Fokus auf die Modulkörper $\mathbb{Q}$ Situation an. Wir bestimmen explizite Schranken an die Primzahlen, die den Index $[\,\mathcal{O}_K : S\,]$ der auftretenden Ordnungen teilen und an deren Exponenten. In einigen interessanten Situationen erlauben es unsere Resultate eine bestimmte minimale Ordnung zu konstruieren, die in allen Ordnungen S enthalten sein muss, welche als Endomorphismenringe von einfachen polarisierten abelschen Varietäten mit komplexer Multiplikation und Modulkörper $\mathbb{Q}$ auftreten können. Dies erlaubt eine algorithmische Analyse der $\bar{\mathbb{Q}}$-Isomorphieklassen der Jacobischen von einfachen Kurven vom Geschlecht 3 mit komplexer Multiplikation. Am Ende können wir zeigen, dass es keine einfachen hyperelliptischen oder Picard Kurven vom Geschlecht 3 einer bestimmten Art gibt, die komplexe Multiplikation bezüglich einer nicht maximalen Ordnung S und Modulkörper $\mathbb{Q}$ haben. Zusätzlich enthält diese Arbeit eine algorithmische Analyse von Ordnungen in kubischen Zahlkörpern und ihrer Eigenschaft, Gorenstein zu sein.

Contents

Introduction

Background

In the year 1853, Kronecker ([Kro53]) stated the subsequent famous theorem, today known as the *Kronecker-Weber Theorem*.

Theorem.
Every finite abelian extension of $\mathbb{Q}$ *is contained in some cyclotomic field.*

In the following years, mathematicians like Weber ([Web86]) and Hilbert ([Hil96]) completed the proof. The natural generalization of this theorem asks for finite abelian extensions of arbitrary number fields. This is known as *Kronecker's Jugendtraum* or *Hilbert's 12th problem*. One approach to describe finite abelian extensions of arbitrary number fields is class field theory, which connects class groups and Galois groups of abelian extensions via the *Artin map*. However, this is not explicit and does not answer the question in the spirit of Kronecker, which asks for a single function, like the exponential function $z \mapsto \exp(2\,\pi\,z\,/\,2)$ for ground field $\mathbb{Q}$, that parametrizes the generators of the abelian extensions.

For imaginary quadratic number fields, complex multiplication (CM) theory of elliptic curves and their j-invariants provided a complete answer to *Kronecker's Jugendtraum*. This is due to Fueter ([Fue14]), Takagi ([Tak20]) and Hasse ([Has27]). The generalization of the complex multiplication theory from elliptic curves to multidimensional abelian varieties was then developed by Weil ([Wei55]), Taniyama ([Tan55]) and Shimura ([Shi55]) and answers *Kronecker's Jugendtraum* for so-called complex multiplication fields (CM fields), which are totally imaginary quadratic extensions of totally real number fields. A first summary of this theory is given in [ST61].

Now consider *Gauss' class number one problem*, which seeks to identify all imaginary quadratic number fields K of class number one. As the j-invariant of an elliptic curve with complex multiplication is actually an algebraic number that generates the maximal order of a quadratic CM field, the theory of complex multiplication of elliptic curves allows a reformulation of this number theoretical

problem in terms of algebraic geometry: Find all elliptic curves with complex multiplication by the maximal order $\mathcal{O}_K$ of a quadratic number field K and which have field of moduli K. This problem has been solved by Heegner ([Hee52]), Baker ([Bak68]) and Stark ([Sta+67]) and the arising fields are $K = \mathbb{Q}(\sqrt{-d})$ for $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$. Due to Shimuras and Taniyamas multidimensional theory on abelian varieties with complex multiplication ([ST61]), the natural generalization of this question is to ask for the following:

Find all simple principally polarized abelian varieties, which have complex multiplication by a maximal order and field of moduli contained in the reflex field K^r of a CM type (K, Φ).

In the cases of dimensions 2 and 3, we can think of simple principally polarized abelian varieties over the complex numbers $\mathbb{C}$ as Jacobians of simple curves. Specifically, these are curves of genus 2 or 3, depending on the dimension. Hence, restricting to abelian varieties over $\mathbb{C}$, this allows us to express the same question, but in the language of curves instead of abelian varieties:

Find all simple curves over the complex numbers $\mathbb{C}$, whose Jacobians have complex multiplication by a maximal order and field of moduli contained in the reflex field K^r of a CM type (K, Φ).

Much research has been performed around this question. For genus 2 curves, the problem has been entirely solved thanks to several mathematicians. Spallek ([Spa94]) described an explicit construction of such curves, van Wamelen ([VW99]) computed examples over the rationals, Murabayashi and Umegaki ([MU01]) determined all rational CM points in the moduli space of principally polarized abelian surfaces, Bouyer and Streng ([BS15]) focused on examples over the reflex field, and Kilicer ([Kıl16]) listed all quartic CM fields appearing as the corresponding CM fields of these curves.

However, the situation is more complex for genus 3 curves. This is mainly because the corresponding CM fields are of degree six over $\mathbb{Q}$, not of degree four, and genus 3 curves may not be hyperelliptic, which complicates explicit construction. There has still significant progress been made. Weng ([Wen01b]) gives a detailed method for constructing hyperelliptic CM curves of genus 3. Koike and Weng ([KW05]) explain how to construct genus 3 Picard curves with CM. More-

over, in [Kıl16], Kilicer lists all sextic CM fields that have an imaginary quadratic subfield and provides a complete list of CM fields for curves with field of moduli $\mathbb{Q}$. Summarizing, Table 1 gives an overview of the advantages in the construction of low genus curves over subfields of $\mathbb{C}$ with complex multiplication by maximal orders.

Genus	Current status	Researchers
1	Problem solved	Heegner, Baker, Stark
2	Problem solved	Spallek, van Wamelen, Murabayashi & Umegaki, Bouyer & Streng, Kilicer
3	Progress made, examples constructed for hyperelliptic and Picard curves, CM pairs completely classified for sextic CM fields containing an imaginary quadratic subfield	Weng, Koike, Kilicer
≥ 4	open	

Table 1: Overview of the research on simple low genus curves with complex multiplication by maximal orders

In this thesis, we want to consider a closely related question arising from the previous work together with Shimuras third main theorem ([ST61]). Instead of focusing on maximal orders, we will consider arbitrary orders and especially address the case in which these orders are non-maximal:

Find all simple curves over the complex numbers $\mathbb{C}$, whose Jacobians have complex multiplication by a non-maximal order and field of moduli contained in the reflex field K^r of a CM type (K, Φ).

One of the main problems is determining how to narrow down the many different orders that could appear as the endomorphism rings of the CM curves. To make things more manageable, researchers often investigate special cases with extra constraints, for example, assuming the field of moduli to be $\mathbb{Q}$ or assuming the CM field K to contain specific subfields. In the case of elliptic curves, considering isomorphism classes over an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$, it is well known that the list of nine isomorphism classes of elliptic curves over $\mathbb{Q}$ with complex multiplication by a maximal order can be extended by four isomorphism classes with complex multiplication by a non-maximal order (see [Sil09][Appendix C.11]). For genus 2

curves, Bisson and Streng ([BS17]) were able to expand van Wamelen's ([VW99]) list of curves with complex multiplication by maximal orders. They added two isomorphism classes of rational curves with complex multiplication by a non-maximal order and demonstrated a complete classification of all rational genus 2 curves with complex multiplication by an arbitrary order $S \subseteq \mathcal{O}_K$ up to isomorphism.

One natural next step is to see how far we can generalize these principles to genus 3 curves. However, the complexity increases notably for several reasons. On the one hand, we have to deal with the same issues as when considering maximal orders in sextic CM fields. On the other hand, non-maximal orders usually do not come with a classical ideal factorization into prime ideals unless they are integrally closed and thus Dedekind. Moreover, for non-maximal orders in sextic CM fields, unlike in quartic CM fields, their restrictions to the maximal totally real subfield do not always have an invertible trace dual which is crucial in the approach of Bisson and Streng in [BS17]. This thesis aims to present some partial solutions to the presented challenges.

Application

Elliptic and hyperelliptic curves are fundamental in modern cryptography, especially in public-key cryptography. Our main reference on this topic is [Coh+05]. Introduced by Diffie and Hellman in the late 1970s, as explained in [DH76], public-key cryptography relies on specific one-way functions that are computationally easy to evaluate but difficult to reverse within a reasonable amount of time. When these functions are selected carefully, it becomes nearly impossible for attackers to decrypt the encrypted messages, even if they are familiar with the function.

A main task in public-key cryptography is choosing suitable cryptosystems. Among the numerous methods developed over time, two have been particularly stood out. The first group of methods, including the famous RSA cryptosystem, is based on the challenge of factoring products of large prime numbers. The second approach builds on the discrete logarithm problem (DLP) in cyclic groups of prime order, which is defined to be the following.

Let $(G, \cdot)$ be a cyclic group of prime order together with a generator $g \in G$. Given any element $h \in G$ with $h = g^k$ for some $k \in \mathbb{N}$, determine the integer k.

The group G can be chosen as the set of points on an elliptic curve over a finite

field or, more generally, as the set of elements in the Jacobian of small genus curves over finite fields. In certain groups, the DLP can be attacked with subexponential methods, making their security comparable to RSA. However, when using specific elliptic or hyperelliptic curves of genus $g \leq 3$, the DLP seems to be resistant to such strategies as no subexponential attack has been discovered yet.

A resistance to subexponential attacks is of great significance to cryptographers. It is suggested that elliptic curves can provide security comparable to RSA, but with much shorter key lengths. For instance, in order to match the security of a 3200-bit RSA, an elliptic curve over a finite field is estimated to require a group size of only about 256 bits (see [IS23]). While operations on elliptic curves or Jacobians are more complex than in other groups, such as $(\mathbb{Z}/n\mathbb{Z})^\times$, they have efficient addition rules. The smaller key size compensates for this slightly more complex group operation. This feature is especially beneficial in environments such as smart cards, where computational resources are limited.

In order to benefit from these considerations, a main task is the identification of suitable elliptic curves over finite fields that provide a large prime factor in their group order. In the early 1990s, Atkin and Morain proposed a method to address this challenge by considering elliptic curves with complex multiplication, as described in [AM93]. This method is called CM method. Over the years, this approach has been extended to Jacobians of small genus curves. For curves of genus 2 and 3, we refer to [Wen01b] and [KW05]. The CM method especially requires the identification of suitable CM fields and involves determining isomorphism classes of the curves over $\mathbb{C}$, a task that is specifically addressed in this thesis with a special focus on endomorphism rings which are non-maximal orders in the CM fields.

Overview

In Chapter 1, we give basic definitions and statements on fractional ideals of orders, global class field theory, complex multiplication theory and abelian varieties, especially over $\mathbb{C}$. Within Chapter 2, we discuss orders in cubic number fields, with a special focus on diagonal orders.The orders in cubic number fields play an important role in the discussion on abelian varieties of dimension 3 having CM by a non-maximal order S in a sextic CM field K. To be more precise, they appear when we intersect the endomorphism ring S of the abelian variety with the totally real cubic subfield K_0 of K. We provide explicit representations of the $\mathbb{Z}$-bases for both diagonal Gorenstein orders and diagonal orders that are not Gorenstein. For diagonal orders, we prove the following result, that completely describes the $\mathbb{Z}$-basis of a diagonal order in a cubic number field.

Proposition.
Let L be a cubic number field with ring of integers $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$. Let $\lambda_{ij} \in \mathbb{Z}$ with $1 \leq i \leq 2$ and $0 \leq j \leq 2$ such that

$$\omega_1^2 = \lambda_{10} + \lambda_{11}\,\omega_1 + \lambda_{12}\,\omega_2 \quad \textit{and}$$
$$\omega_2^2 = \lambda_{20} + \lambda_{21}\,\omega_1 + \lambda_{22}\,\omega_2\,.$$

A sublattice $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ of $\mathcal{O}_L$ with $a, c \in \mathbb{N}$ is an order in L if and only if

$$a \mid \lambda_{21}\,c^2 \quad \textit{and} \quad c \mid \lambda_{12}\,a^2\,.$$

This proposition about the structure of the $\mathbb{Z}$-bases of diagonal orders in cubic number fields enables us to provide explicit descriptions of diagonal Gorenstein orders in cubic number fields. We have computationally verified this for a defined bound on the index $[\,\mathcal{O}_K : S\,]$ and a specific list of cubic number fields, which are of relevance in our discussion about sextic CM fields and their totally real cubic subfields. Those fields are presented in Table 2.1. The subsequent theorem extends the known types of Gorenstein orders in cubic number fields, as documented in [JT15].

Theorem.
Let L be a cubic number field from Table 2.1 with ring of integers $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$. Let $\lambda_{21}, \lambda_{12} \geq 1$ be integers such that $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is an order if and only if $a \mid \lambda_{21}\,c^2$ and $c \mid \lambda_{12}\,a^2$. Let D_1 and D_2 be the set of divisors of λ_{21} and λ_{12}, respectively.

(a) *Let $x, y \geq 1$ with $\gcd(x, y) = 1$. For all $r \in D_1$ and $s \in D_2$ such that*

  (i) $1 = \gcd(x, s) = \gcd(r, y) = \gcd(r, s)$,
  (ii) $\forall\, p \mid x$ *prime*: $v_p(r) = v_p(\lambda_{21})$,
  (iii) $\forall\, p \mid y$ *prime*: $v_p(s) = v_p(\lambda_{12})$ *and*
  (iv) $(r\,x^2\,y)\,(s\,x\,y^2) \leq 10^5$

  the lattice $S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2 \rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein.

(b) *If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is a Gorenstein order in L with $[\,\mathcal{O}_L : S\,] \leq 10^5$, then exist $x, y \geq 1$, $r \in D_1$ and $s \in D_2$ with*

  (i) $1 = \gcd(x, y) = \gcd(x, s) = \gcd(r, y) = \gcd(r, s)$,
  (ii) $\forall\, p \mid x$ *prime*: $v_p(r) = v_p(\lambda_{21})$ *and*
  (iii) $\forall\, p \mid y$ *prime*: $v_p(s) = v_p(\lambda_{12})$

  such that $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Additionally, we give a corresponding result for non-Gorenstein orders in cubic number fields, as presented below. Together with the previous theorem, this provides a complete characterization of both Gorenstein and non-Gorenstein diagonal orders in the considered list of cubic number fields with special relevance.

Theorem.
Let L be a cubic number field from Table 2.1 with ring of integers $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$. Let $\lambda_{21}, \lambda_{12} \geq 1$ be integers such that $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is an order if and only if $a \mid \lambda_{21}\,c^2$ and $c \mid \lambda_{12}\,a^2$. Let D_1 and D_2 be the set of divisors of λ_{21} and λ_{12}, respectively.

(a) *Let $x > 1$. Then for all $e, d \mid x$ with $\gcd(e, d) = 1$ and $e\,d \neq x$ and for all $r \in D_1$, $s \in D_2$ with $(r\,e\,x)\,(s\,d\,x) \leq 10^5$ the lattice $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2 \rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.*

(b) *If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is an order in L with $[\,\mathcal{O}_L : S\,] \leq 10^5$ which is not Gorenstein, then exist $x > 1$, $e, d \mid x$ with $\gcd(e, d) = 1$ and $e\,d \neq x$ such as $r \in D_1$, $s \in D_2$ with $a = r\,e\,x$ and $c = s\,d\,x$.*

Afterwards, in Chapter 3, we summarize the construction of polarized abelian varieties over $\mathbb{C}$ with complex multiplication by arbitrary orders and discuss the computation of the so-called ideal class monoid.

Furthermore, in Chapter 4.1, we present Shimuras third main theorem, both, in the classical way and in a modern formulation in terms of the polarized class group and the type norm. This theorem lays the foundation for the whole discussion on curves with CM by non-maximal orders.

Theorem (Shimuras Third Main Theorem - Modern Formulation)**.**
Let (K^r, Φ^r) be a primitive CM-type and (K, Φ) its reflex. Let $S \subseteq \mathcal{O}_K$ be an order of K, $f := [\,\mathcal{O}_K : S\,]$ and (A, ι) be an abelian variety of type (K, Φ) with CM by S. Let $\mathscr{C}$ be a polarization of A and k_0 be the field of moduli of $(A, \mathscr{C})$. Then $k_0 \cdot K^r$ is the class field over K^r corresponding to $\Omega_S = \Omega_S(f)$.

In particular, Shimuras third main theorem for arbitrary orders provides necessary conditions on the orders, which may appear as endomorphism rings of simple polarized abelian varieties with CM and field of moduli contained in the reflex field. To be more precise, those orders are CM class number one orders in CM class number one fields. Due to the Rosati involution, the orders additionally have to be stable under complex conjugation.

In Chapter 4.2, we revisit results from [Kıl16] and discuss the possible appearing CM fields in the field of moduli $\mathbb{Q}$ situation. We show that, analogue to the case of maximal orders, even for arbitrary orders, the CM fields are cyclic sextic CM

class number one fields containing an imaginary quadratic subfield. In Chapter 4.3, we extend results from [Wen01b] and [KW05], originally demonstrated for maximal orders, to arbitrary orders. In particular, on the one hand, we will show that if an order S is isomorphic to the endomorphism ring of a simple CM curve C over $\mathbb{C}$ and $\mathbb{Z}[i] \subseteq S$, then it is hyperelliptic. On the other hand, considering simple CM curves of genus 3 over $\mathbb{C}$, this curve is a Picard curve if and only if $\mathbb{Z}[\zeta_3] \subseteq S$.

From now, we focus on bounding the index of the orders which might appear as endomorphism rings of principally polarized abelian varieties over $\mathbb{C}$ with complex multiplication and field of moduli $\mathbb{Q}$. This generalizes an approach from Bisson and Streng ([BS17]) from quartic CM fields to sextic CM fields. In a first step, in Chapter 5, we take a closer look at CM class number one orders in cyclic and non-normal sextic CM fields, and we show that the kernel of the relative norm is of exponent at most two. In Chapter 6, we give relations between the index of an order and the index of its restriction to a subfield. We present two different approaches, one using Minkowskis convex body theorem and the other one generalizes a result from [BS17].

Definition.
Let S be an order in a number field K and $\mathfrak{a}$ be a fractional ideal of S. We define

$$\delta(\mathfrak{a}) := \frac{[\,\mathcal{O}_K \,:\, \mathfrak{a}\mathcal{O}_K\,]}{[\,S \,:\, \mathfrak{a}\,]}.$$

Let $K_0 \subseteq K$ be a number field with $m = [\,K \,:\, K_0\,]$ and $S_0 := S \cap K_0$, then, for S_0^* denoting the trace dual of S_0, we define

$$\delta_S := \frac{\delta(S_0^*)^m}{\delta(S_0^* S)}\,.$$

The main result of Chapter 6 is the following theorem.

Theorem.
Let $\mathbb{Q} \subseteq K_0 \subseteq K$ be number fields, where K_0 is of degree n over $\mathbb{Q}$ and K is a degree m Galois extension of K_0. Let $S \subseteq \mathcal{O}_K$ be an order of K, which is stable under the Galois group $\mathrm{Gal}(K/K_0)$, and let $S_0 := S \cap K_0$. Then $[\,S^* \,:\, S_0^* S\,]$ is an integer and there exists $\delta_S \in \mathbb{Q}$ such that

$$[\,S^* \,:\, S_0^* S\,]\,[\,\mathcal{O}_{K_0} \,:\, S_0\,]^{2m} \;=\; \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,[\,\mathcal{O}_K \,:\, S\,]^2\,\delta_S\,.$$

We give two classes of orders S in which the parameter δ_S is equal to 1. In particular, this is the case whenever S_0 is Gorenstein.

Within Chapter 7, we delve deeper into the situation of cyclic sextic CM fields and, under the assumption that the kernel of the relative norm is of exponent at most 2, prove another divisibility criterion for the indices of relative orders, inspired by a similar result for quartic CM fields in [BS17].

Theorem.
Let K be a cyclic sextic CM field with maximal totally real subfield K_0 and $S \subseteq R$ be orders in K with $f := [\,\mathcal{O}_K : S\,]$. Let $S_0 := S \cap K_0$ and $R_0 := R \cap K_0$. Let the kernel of the relative norm

$$\psi : \left(R/f\mathcal{O}_K\right)^\times / \left(S/f\mathcal{O}_K\right)^\times \mu_R \longrightarrow \left(R_0/f\mathcal{O}_{K_0}\right)^\times / \left(S_0/f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most 2. Then

$$\frac{[\,R : S\,]}{[\,R_0 : S_0\,]} \,\Big|\, B\,,$$

where B is an integer depending only on the number of elements in the group of roots of unity μ_R.

This result requires decomposing ideals into so-called $\mathfrak{q}$-primary parts, some results on the decomposition of unit groups of finite rings and the decomposition of the indices. In addition, we make use of the specific splitting behavior of primes in cyclic sextic CM fields. Applying this theorem for $R = \mathcal{O}_K$ to the main result of Chapter 6, we will then deduce the following theorem.

Theorem.
Let K be a cyclic sextic CM field and let K_0 be the totally real cubic subfield of K. Let $S \subseteq \mathcal{O}_K$ be an order of K stable under complex conjugation and let the kernel of the relative norm

$$\psi : \left(\mathcal{O}_K/f\mathcal{O}_K\right)^\times / \left(S/f\mathcal{O}_K\right)^\times \mu_K \longrightarrow \left(\mathcal{O}_{K_0}/f\mathcal{O}_{K_0}\right)^\times / \left(S_0/f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most 2, where $f := [\,\mathcal{O}_K : S\,]$. Then we have

$$f^2 = [\,\mathcal{O}_K : S\,]^2 \,\Big|\, B^4 \,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,\delta_S,$$

where B is an integer, depending only on the number of elements in the group of roots of unity μ_K and $\delta_S \in \mathbb{Q}$.

Combing the results from Chapter 4.1 and Chapter 7, in Chapter 8 we give explicit bounds on the index of the orders that can appear as endomorphism rings of simple polarized abelian varieties over $\mathbb{C}$ with complex multiplication and field of moduli $\mathbb{Q}$. This is the main theoretical result of this work and combines most of the previous considerations in this thesis.

Theorem.
Let (K, Φ) be a sextic CM type, (K^r, Φ^r) be its reflex and let K_0 denote the totally real cubic subfield such as $S \subseteq \mathcal{O}_K$ be an order of index $f = [\mathcal{O}_K : S]$. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a simple polarized abelian variety over $\mathbb{C}$ of type (K, Φ) with complex multiplication by S and field of moduli $\mathbb{Q}$. Then K is a cyclic sextic CM class number one field containing an imaginary quadratic subfield, $\Omega_S = I_{K^r}(f)$ and

$$f^2 = [\mathcal{O}_K : S]^2 \,\Big|\, B^4 \, \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\, \delta_S,$$

where B is an integer depending only on the number of elements in the group of roots of unity μ_K and $\delta_S \in \mathbb{Q}$.

The provided bound on the index depends on δ_S, and, as we will demonstrate, there does not exist a general upper bound for δ_S. However, in the case of orders S with $\delta_S = 1$, such as those where the reduction S_0 of S to K_0 is Gorenstein, this theorem offers an explicit divisibility criterion. In order to find a comprehensive list of potential endomorphism rings, a straightforward search for all orders with an index satisfying this criterion is not realistic in a reasonable amount of time due to the large number of possibilities. In the two scenarios addressed in Chapter 4.3, we will be able to construct certain minimal orders which allow to only consider their overorders during our search.

In the last chapter (Chapter 9), we apply our results to the computation of simple genus 3 curves over $\mathbb{C}$ with complex multiplication by arbitrary orders and field of moduli $\mathbb{Q}$. Under the condition that $\delta_S = 1$, we computationally prove that there are no Picard curves having field of moduli $\mathbb{Q}$ and complex multiplication by an order $S \subsetneq \mathcal{O}_K$ for all CM fields with a group of roots of unity satisfying $|\mu_K| = 6$.

Corollary.
Let K be a sextic CM field with $|\mu_K| = 6$ and totally real cubic subfield K_0. There is no simple Picard curve $C/\mathbb{C}$ having field of moduli $\mathbb{Q}$ and complex multiplication by a non-maximal order S in K such that $\delta_S = 1$.

If we omit the condition that $\delta_S = 1$, then, assuming that the index is only divisible by primes up to a certain bound, we show an analogue result. This gives us reason to believe that there might be no Picard curves with field of moduli $\mathbb{Q}$ and CM by a non-maximal order at all.

Corollary.
Let K be a sextic CM field with $|\mu_K| \neq 18$ and totally real cubic subfield K_0. There is no simple Picard curve $C/\mathbb{C}$ having field of moduli $\mathbb{Q}$ and complex multiplication by a non-maximal order S in K such that $[\,\mathcal{O}_K : S\,]$ is only divisible by prime numbers $p \leq 10^5$.

We also computationally show that there are no such hyperelliptic curves with $\mathbb{Z}[i] \subseteq S \subsetneq \mathcal{O}_K$, but we find some curves defined over K_0. This requires computing period matrices and Shioda invariants, such as models of the curves over its field of moduli. Some examples of the received models over K_0 are given in Appendix E.

Corollary.
Let K be a sextic CM field with totally real cubic subfield K_0. There is no simple hyperelliptic curve $C/\mathbb{C}$ having field of moduli $\mathbb{Q}$ and complex multiplication by a non-maximal order $S \supseteq \mathbb{Z}[i]$ in K such that $\delta_S = 1$.

Additionally, omitting the condition that $\delta_S = 1$, we prove a similar result for orders up to a certain bound on the primes dividing the index $[\,\mathcal{O}_K : S\,]$. Again, this gives us reason to believe that there might be no hyperelliptic curve having field of moduli $\mathbb{Q}$ and CM by a non-maximal order $S \supseteq \mathbb{Z}[i]$.

Corollary.
Let K be a sextic CM field with totally real cubic subfield K_0. There is no simple hyperelliptic curve $C/\mathbb{C}$ having field of moduli $\mathbb{Q}$ and complex multiplication by a non-maximal order $S \supseteq \mathbb{Z}[i]$ in K such that $[\,\mathcal{O}_K : S\,]$ is only divisible by primes $p \leq 10^5$.

Notations

μ_K	Group of roots of unity of a number field K
$\Delta_{K/L}$	Relative discriminant of number fields $K \supseteq L$
$\mathrm{Tr}_{K/L}$	Trace of number fields $K \supseteq L$
$\mathrm{N}_{K/L}$	Norm of number fields $K \supseteq L$
$\mathcal{O}_K$	Maximal order of a number field K
I_K	Group of fractional ideals of $\mathcal{O}_K$
$I_K(\mathfrak{a})$	Subgroup of I_K of fractional ideals coprime to the integral ideal $\mathfrak{a}$ of $\mathcal{O}_K$
P_K	Subgroup of I_K of principal fractional ideals
$P_K(\mathfrak{a})$	Intersection of $I_K(\mathfrak{a})$ and P_K
$\mathcal{C}\ell_K$	Quotient of I_K by P_K, the class group of K
$I_K(\mathfrak{m})$	Group $I_K(\mathfrak{m}_0)$ for a modulus $\mathfrak{m} = \mathfrak{m}_0\,\mathfrak{m}_\infty$ of a number field K
$P_{K,1}(\mathfrak{m})$	Subgroup of $I_K(\mathfrak{m})$ of principal ideals $\alpha\,\mathcal{O}_K$ with $\alpha \equiv 1 \pmod{\mathfrak{m}_0}$ and $\sigma(\alpha) > 0$ for all infinite places σ dividing $\mathfrak{m}_\infty$ for a modulus $\mathfrak{m} = \mathfrak{m}_0\,\mathfrak{m}_\infty$ of a number field K.
$\mathcal{C}\ell_K(\mathfrak{m})$	Quotient of $I_K(\mathfrak{m})$ by $P_{K,1}(\mathfrak{m})$, the Ray class group of K modulo $\mathfrak{m}$
$r(\mathfrak{a})$	Multiplier ring of a lattice $\mathfrak{a}$ in a number field K
$\mathfrak{a}^*$	Trace dual of a lattice $\mathfrak{a}$ in a number field K
J_S	Set of fractional ideals of an order S
I_S	Group of invertible fractional ideals of an order S
$I_S(\mathfrak{a})$	Subgroup of I_S of invertible ideals coprime to the integral ideal $\mathfrak{a}$ of S
P_S	Subgroup of I_S of principal invertible ideals
$P_S(\mathfrak{a})$	Intersection of $I_S(\mathfrak{a})$ and P_S
$\mathrm{ICM}(S)$	Quotient of J_S by P_S, the ideal class monoid of S
$\mathcal{C}\ell(S)$	Quotient of I_S by P_S, the class group of S
$\mathrm{Pic}(S)$	Picard group of S
$\mathfrak{f}_S$	Conductor of an order S in $\mathcal{O}_K$
$\mathrm{Spec}(S)$	Set of prime ideals of an order S, the spectrum of S
K_0	Maximal totally real subfield of a CM field K
S_0	Intersection of an order S in a CM field K with K_0

$\mathcal{I}_S$	Group of tuples $(\mathfrak{a}, \alpha) \in (I_S, K_0)$, where α is totally positive and $\mathfrak{a}\,\bar{\mathfrak{a}} = \alpha\, S$
$\mathcal{P}_S$	Subgroup of $\mathcal{I}_S$ consisting of tuples $(xS, x\bar{x}) \in (I_S, K_0)$ with $x \in K^*$
$\mathfrak{C}(S)$	Quotient of $\mathcal{I}_S$ by $\mathcal{P}_S$
Φ	CM type of a CM field K
(K^r, Φ^r)	Reflex type of a CM type (K, Φ)
N_Φ	Type norm of a CM type Φ
Ψ	Map $I_{K^r}(f) \to \mathfrak{C}(S)$, $\mathfrak{a} \mapsto (\mathrm{N}_{\Phi^r}(\mathfrak{a}), \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a})$, where $S \subseteq \mathcal{O}_K$ is an order of index f.
Ω_S	Kernel of Ψ
ψ	Relative norm
$\mathscr{C}$	Polarization of an abelian variety
$\mathcal{P}$	Polarized abelian variety $(A, \mathscr{C})$
$\mathrm{Hom}(A, B)$	Set of homomorphisms between two abelian varieties A and B
$\mathrm{End}(A)$	Group $\mathrm{Hom}(A, A)$
$\mathrm{Hom}_\mathbb{Q}(A, B)$	Set $\mathrm{Hom}(A, B) \otimes_\mathbb{Z} \mathbb{Q}$
$\mathrm{End}_\mathbb{Q}(A)$	Algebra $\mathrm{Hom}_\mathbb{Q}(A, A)$
A^*	Picard variety of A
k_0	Field of moduli of a polarized abelian variety $\mathcal{P} = (A, \mathscr{C})$
$\mathbb{H}_g$	g-dimensional Siegel upper half-space
J_C	Jacobian of a curve C

Chapter 1

Preliminaries

This chapter contains some fundamental definitions and results on orders in number fields, class field theory, complex multiplication and abelian varieties. While the first four sections focus on number theoretical aspects, in the last section, we will turn our attention to algebraic geometry and the relation between both fields provided by complex multiplication theory.

1.1 Fractional ideals and orders

Fractional ideals of orders in number fields play an important role in constructing abelian varieties with complex multiplication. We collect some basic terminologies and results, mainly following [Neu99], [Ste08] and [AK13].

1.1.1 Fractional ideals of noetherian domains

Definition 1.1.
Let R be a noetherian domain with field of fractions K. A finitely generated non-zero R-submodule $\mathfrak{a}$ of K is called a *fractional ideal* of R (also called a fractional R-ideal). If $\mathfrak{a}$ is contained in R, then we say that $\mathfrak{a}$ is an *integral ideal* of R and denote it as $\mathfrak{a} \leq R$.

A non-zero R-submodule $\mathfrak{a}$ of a noetherian domain R with field of fractions K is a fractional R-ideal if and only if there exists $x \in R$ with $x\mathfrak{a} \subseteq R$. Hence, fractional R-ideals are precisely the R-submodules $\mathfrak{a} \neq \{0\}$ such that there exists $x \in R$ with $x\mathfrak{a} \subseteq R$.

Definition 1.2.
Let R be a noetherian domain with field of fractions K, and let $\mathfrak{a}$ such as $\mathfrak{b}$ be fractional ideals of R. We define the *intersection* $\mathfrak{a} \cap \mathfrak{b}$, the *sum* $\mathfrak{a} + \mathfrak{b}$, the *product* $\mathfrak{a}\,\mathfrak{b}$ and the *quotient (colon ideal)* $(\mathfrak{a} : \mathfrak{b})$ as

$$\begin{aligned} \mathfrak{a} \cap \mathfrak{b} &:= \{x \in K \mid x \in \mathfrak{a}\,, x \in \mathfrak{b}\}\,, \\ \mathfrak{a} + \mathfrak{b} &:= \{a + b \mid a \in \mathfrak{a}\,,\, b \in \mathfrak{b}\}\,, \\ \mathfrak{a}\,\mathfrak{b} &:= \langle \{a\,b \mid a \in \mathfrak{a}\,,\, b \in \mathfrak{b}\} \rangle\,, \qquad \text{and} \\ (\mathfrak{a} : \mathfrak{b}) &:= \{x \in K \mid x\mathfrak{b} \subseteq \mathfrak{a}\}\,. \end{aligned}$$

All four objects are in particular fractional R-ideals.

Definition 1.3.
Let R be a noetherian domain with field of fractions K, and let $\mathfrak{a}$ be a fractional ideal of R. Then $\mathfrak{a}$ is said to be *principal* if there exists $y \in K^\times$ with $\mathfrak{a} = yR$.

We may consider a fractional R-ideal as a quotient of an integral R-ideal divided by a principal integral R-ideal.

Definition 1.4.
Let R be a noetherian domain with field of fractions K, and let $\mathfrak{a}$ be a fractional ideal of R. We define $\mathfrak{a}^{-1} := (R : \mathfrak{a})$ and we say that $\mathfrak{a}$ is *invertible*, if $\mathfrak{a}\,\mathfrak{a}^{-1} = R$.

Note that $\mathfrak{a}\,\mathfrak{a}^{-1} \subseteq R$ is true for every fractional ideal $\mathfrak{a}$ of a noetherian domain R. Being invertible is equivalent to the property that there exists a fractional R-ideal $\mathfrak{b}$ such that $\mathfrak{a}\,\mathfrak{b}$ is a non-zero principal R-ideal. By J_R we denote the set of fractional ideals of R. The set I_R of invertible fractional R-ideals forms a group under ideal multiplication and contains a subgroup P_R formed by the principal fractional ideals. P_R is then isomorphic to the quotient $K^\times/R^\times$.

Definition 1.5.
Let R be a noetherian domain with field of fractions K. Let I_R be the group of invertible fractional ideals of R, and let P_R be its subgroup consisting of principal fractional ideals. We define the *ideal class group* of R to be

$$\mathcal{C}\ell(R) := {}^{I_R}\!\diagup_{P_R}.$$

In noetherian domains, the ideal class group of R is canonically isomorphic to the *Picard group* $\mathrm{Pic}(R)$, which is defined to be the group of isomorphism classes of R-modules which are invertible under the tensor product. For more details on this, see [AK13][Chapter 25]. In this situation, we will use the term Picard group as a

synonym of the term ideal class group. As already indicated above, the following sequence is exact and summarizes the relations between the introduced objects:

$$0 \longrightarrow R^\times \longrightarrow K^\times \longrightarrow I_R \longrightarrow \mathrm{Pic}(R) \longrightarrow 0.$$

1.1.2 Number fields and orders

Throughout this thesis, we will discuss orders in number fields, their fractional ideals, and their specific properties. This section summarizes the basic knowledge on these objects.

Definition 1.6.
A finite field extension K of the rational numbers $\mathbb{Q}$ is said to be a *number field*. For two number fields K and L such that L can be embedded into K, we may write $L \subseteq K$ and define the *degree of K over L* to be the dimension of K as a L - vector space. If this is the case, we say K is *normal* over L if every irreducible polynomial in $L[x]$ that has a root in K splits completely in K.

Especially during our discussions on the construction of abelian varieties, we frequently refer to the terms outlined below.

Definition 1.7.
Let K be a number field. A free $\mathbb{Z}$-module of full rank in K is defined as a *lattice* in K. For any lattice $\mathfrak{a}$ in K, we define the *multiplier ring* of $\mathfrak{a}$ to be

$$r(\mathfrak{a}) := \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\}.$$

If $\mathfrak{b}$ is a lattice in K and $\mathfrak{b}$ is contained in $\mathfrak{a}$, then $\mathfrak{b}$ said to be *sublattice* of $\mathfrak{a}$.

Definition 1.8.
Let $\mathfrak{a}$ and $\mathfrak{b}$ be lattices in a number field K with bases $(a_1, \ldots, a_r)$ and $(b_1, \ldots, b_r)$, respectively. Let $P \in \mathbb{Q}^{r\times r}$ be a transformation matrix such that

$$(b_1, \ldots, b_r) \;=\; (a_1, \ldots, a_r) \cdot P\,.$$

Then the *index of $\mathfrak{b}$ in $\mathfrak{a}$* is defined to be $[\,\mathfrak{a} \,:\, \mathfrak{b}\,] := |\det(P)|$.

For every $c \in \mathbb{Q}^\times$ we have $[\,\mathfrak{a} \,:\, c\mathfrak{b}\,] = c^r\,[\,A \,:\, B\,]$ and if $\mathfrak{b}$ is contained in $\mathfrak{a}$, then $[\,\mathfrak{a} \,:\, \mathfrak{b}\,] \in \mathbb{Z}$. We also mention that $[\,\mathfrak{a} \,:\, \mathfrak{b}\,]^{-1} = [\,\mathfrak{b} \,:\, \mathfrak{a}\,]$ and whenever $\mathfrak{c}$ is another lattice in K, then $[\,\mathfrak{a} \,:\, \mathfrak{b}\,] = [\,\mathfrak{a} \,:\, \mathfrak{c}\,]\,[\,\mathfrak{c} \,:\, \mathfrak{b}\,]$.

As one of the main objects of interest in this thesis, we consider the following specific type of subrings of number fields, which also provide the structure of a lattice.

Definition 1.9.
Let K be a number field. A subring $R \subseteq K$ that is also a lattice in K is called an *order* of K. For any order $\tilde{R}$ of K contained in an order R, we say that $\tilde{R}$ is a *suborder* of R, and say that R is an *overorder* of $\tilde{R}$.

For two orders $\tilde{R} \subseteq R$ in a number field K, the index of $\tilde{R}$ in R can be expressed as

$$[\, R : \tilde{R}\,] = \left|{}^{R}\!/_{\tilde{R}}\right| .$$

Every order R of a number field K is a subring of the *ring of integers of K:*

$$\mathcal{O}_K := \{x \in K \mid f_{x,\mathbb{Q}} \in \mathbb{Z}[t]\},$$

which is itself an order of K and hence called the *maximal order* of K. The following result can be found in [Neu99][Chapter 1.12] and [Ste08][Chapter 2+6] summarizing some of the most basic knowledge on orders.

Proposition 1.10.
Let R be an order in a number field K. Then:

(a) *The field of fractions of R is K.*
(b) *R is a one-dimensional noetherian integral domain. Especially, every non-zero prime ideal $\mathfrak{p}$ of R is maximal and $R/\mathfrak{p}$ is a field.*
(c) *R is integrally closed if and only if it is a Dedekind domain. In particular, the maximal order $\mathcal{O}_K$ of K is Dedekind.*
(d) *For every suborder $\tilde{R} \subseteq R$, the index $[\, R : \tilde{R}\,]$ is finite and for every non-zero ideal $\mathfrak{a} \leq R$, the ideal norm $\mathrm{N}(\mathfrak{a}) := |\, R/\mathfrak{a}\,|$ is finite.*

Based on these considerations, we can relate the terms lattices and fractional ideals of orders. For any lattice $\mathfrak{a}$ in a number field K, the multiplier ring $r(\mathfrak{a})$ of $\mathfrak{a}$ is an order in K but not necessarily equal to $\mathcal{O}_K$. We will now present the relationship between fractional ideals and lattices.

Proposition 1.11.
Let K be a number field, and let S be an order in K.

(a) *Every lattice $\mathfrak{a}$ in K is a fractional ideal of its multiplier ring $r(\mathfrak{a})$.*
(b) *Every fractional ideal $\mathfrak{a}$ of S is a lattice in K.*

Proof. Firstly, let $\mathfrak{a}$ be a lattice in K, and let $r(\mathfrak{a})$ be its multiplier ring. Then we have $r(\mathfrak{a})\mathfrak{a} \subseteq r(\mathfrak{a})$ and $\mathfrak{a}$ is a $r(\mathfrak{a})$-submodule of K. Since $\mathfrak{a}$ is free and has full rank as a $\mathbb{Z}$-module, $\mathfrak{a}$ is non-zero and finitely generated as a $r(\mathfrak{a})$-submodule of K. Hence $\mathfrak{a}$ is a fractional ideal of $r(\mathfrak{a})$. Secondly, let S be an order in K and $\mathfrak{a}$ be a fractional S-ideal. Then $\mathfrak{a}$ is finitely generated as a S-submodule of K, and since S is a lattice in K, the fractional ideal $\mathfrak{a}$ is also a lattice in K. □

Definition 1.12.
Let K be a number field, and let S be an order in K. A fractional S-ideal $\mathfrak{a}$ is said to be *proper* if its multiplier ring equals S:

$$r(\mathfrak{a}) = \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\} = S\,.$$

According to Proposition 1.11, every lattice in a number field K is a proper fractional ideal of some order S in K. For any fractional ideal $\mathfrak{a}$ of an order $S \subseteq \mathcal{O}_K$, the order S is contained in the multiplier ring $r(\mathfrak{a})$. Furthermore, every invertible fractional ideal is proper because for every x in $r(\mathfrak{a})$, x is contained in $\mathfrak{a}\mathfrak{a}^{-1} = S$.

The following definitions and discussions are based on [Neu99][Chapter 3.2] as well as the considerations in [Ste08][Chapter 7].

Definition 1.13.
Let $L \subseteq K$ be number fields with $r = [\,K : L\,]$. For any basis $(\alpha_1, \ldots, \alpha_r)$ of L as a vector space over K, we define the *discriminant of* $(\alpha_1, \ldots, \alpha_r)$ to be

$$\operatorname{disc}(\alpha_1, \ldots, \alpha_r) := \det(\operatorname{Tr}_{K/L}(\alpha_i\,\alpha_j)_{i,j})\,.$$

Additionally, we define the *discriminant of* K *over* L to be the following integral ideal of $\mathcal{O}_L$:

$$\Delta_{K/L} := \langle\{\operatorname{disc}(\alpha_1, \ldots, \alpha_r) \mid (\alpha_1, \ldots, \alpha_r) \text{ is a } K\text{-basis of } L \text{ lying in } \mathcal{O}_L\}\rangle\,.$$

We may also define a similar object for orders.

Definition 1.14.
Let S be an order in a number field K. Let $(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i \in S$ be a basis of S as a lattice. We define the *discriminant of* S, denoted as $\Delta(S)$, as

$$\Delta(S) := \det(\operatorname{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j))_{i,j} \in \mathbb{Z}\,.$$

The following statement summarized considerations from [Ste08][Chapter 7].

Proposition 1.15.
Let K be a number field, and let S be an order in K. If $\sigma_1, \ldots, \sigma_r$ denote the different embeddings of K into $\mathbb{C}$ and $(\alpha_1, \ldots, \alpha_r)$ with $\alpha_i \in S$ is a basis of S as a lattice, then

$$\Delta(S) = (\det(\sigma_i(\alpha_j))_{i,j})^2 \in \mathbb{Z}\,.$$

The discriminant of $\mathcal{O}_K$ is the discriminant of K over $\mathbb{Q}$: $\Delta(\mathcal{O}_K) = \Delta_{K/\mathbb{Q}}$. Moreover, for any suborder $S' \subseteq S$, we have

$$\Delta(S') = [\, S \,:\, S' \,]^2\, \Delta(S)\,.$$

Note that whenever K is totally real and S is an order in K, then $\sigma_1, \ldots, \sigma_r$ have values in $\mathbb{R}$ and $\Delta(S)$ is positive.

Definition 1.16.
Let S be an order in a number field K. We define the *trace dual of S* to be the following fractional ideal of S:

$$S^* := \{\alpha \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(\alpha\, S) \subseteq \mathbb{Z}\}\,.$$

The inverse $\mathfrak{D}_{K/\mathbb{Q}} := (\mathcal{O}_K^*)^{-1} \leq \mathcal{O}_K$ of the trace dual of $\mathcal{O}_K$ is said to be the *different of K*.

In the following proposition, we give relations between the objects mentioned above, partially following [Neu99][Chapter 3].

Proposition 1.17.
Let K_0 be a number field contained in a number field K.Let $n := [\, K_0 \,:\, \mathbb{Q}\,]$ such as $m := [\, K \,:\, K_0\,]$. Let S be an order in K and $S_0 := S \cap K_0$. Then

(a) $\Delta(S) = [\, S^* \,:\, S\,]$,
(b) $\Delta_{K/\mathbb{Q}} = \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{D}_{K/\mathbb{Q}})$,
(c) $\Delta_{K/\mathbb{Q}} = \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0}) \cdot \Delta_{K_0/\mathbb{Q}}^m$,
(d) $[\, S^* \,:\, S\,] = [\, \mathcal{O}_K \,:\, S\,]^2\, \Delta_{K/\mathbb{Q}}$, *and*
(e) *if K is Galois over K_0 and S is stable under* $\mathrm{Gal}(K/K_0)$, *then*

$$\mathrm{Tr}_{K/K_0}(S) \subseteq S_0\,.$$

Especially, $\mathrm{Tr}_{K/\mathbb{Q}}(S) \subseteq \mathrm{Tr}_{K_0/\mathbb{Q}}(S_0)$ *and* $S_0^* S \subseteq S^*$.

Proof. Let $r := nm$ be the degree of K over $\mathbb{Q}$, and let $(\alpha_1, \dots, \alpha_r)$ be a basis of S as a lattice. Then $(\alpha_1^*, \dots, \alpha_r^*)$, uniquely determined by the relation $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i^* \alpha_j) = \delta_{ij}$, defines a basis of S^* as a lattice and the transformation matrix of S^* into S is given by $P = (\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i \alpha_j))_{ij}$. It follows that $[\, S^* : S \,] = |\det(P)| = \Delta(S)$, which proves (a). The results (b) and (c) can be found in [Neu99][Theorem 2.9 + Corollary 2.10, Chapter 3]. Result (d) follows from (a) together with the properties of the index. If K is additionally Galois over K_0 and S stable under $\mathrm{Gal}(K/K_0)$, then $\mathrm{Tr}_{K/K_0}(S) \subseteq S \cap K_0 = S_0$ and by the transitivity of the trace it is

$$\mathrm{Tr}_{K/\mathbb{Q}}(S) = \mathrm{Tr}_{K_0/\mathbb{Q}}(\mathrm{Tr}_{K/K_0}(S)) \subseteq \mathrm{Tr}_{K_0/\mathbb{Q}}(S_0).$$

Now let $x \in S_0^*$, then

$$\mathrm{Tr}_{K/\mathbb{Q}}(xS) = \mathrm{Tr}_{K_0/\mathbb{Q}}(x \,\mathrm{Tr}_{K/K_0}(S)) \subseteq \mathrm{Tr}_{K_0/\mathbb{Q}}(xS_0) \in \mathbb{Z}\,.$$

□

In order to prepare for our discussion on the decomposition of indices in Chapter 7, we summarize some fundamental definitions and results on localizing orders as it can be found in [Ste08][Chapter 3]. Beginning with arbitrary multiplicative subsets S of an order R, we will not only apply this to $S = R \setminus \mathfrak{p}$ for prime ideals $\mathfrak{p}$ of R, but also to $S = \mathbb{Z} \setminus p\mathbb{Z}$.

Proposition 1.18.
Let R be an order in a number field K, and let S be a multiplicative subset of R. Then:

(a) $S^{-1}R = \{r/s \mid r \in R \text{ and } s \in S\}$ *is a subring of* K.

(b) *The fractional ideals of $S^{-1}R$ are of the form*

$$S^{-1}\mathfrak{a} = \{a/s \mid a \in \mathfrak{a} \text{ and } s \in S\}\,,$$

where $\mathfrak{a}$ is a fractional ideal of R. If $S \cap \mathfrak{a} \neq \emptyset$, then $S^{-1}\mathfrak{a} = S^{-1}R$.

(c) *The prime ideals of $S^{-1}R$ are of the form $S^{-1}\mathfrak{q}$, where $\mathfrak{q}$ is a prime ideal of R with $S \cap \mathfrak{q} = \emptyset$.*

(d) *If $\tilde{R}$ is a suborder of R with $[\, R : \tilde{R} \,] \in S$, then $S^{-1}R = S^{-1}\tilde{R}$.*

We will primarily focus on the case where $S = R \setminus \mathfrak{p}$ for prime ideals $\mathfrak{p}$ of R, defined as *localizations* $R_{\mathfrak{p}} := (R \setminus \mathfrak{p})^{-1} R$ *at* $\mathfrak{p}$. The localizations of fractional ideals $\mathfrak{a}$ of R at $\mathfrak{p}$ in the sense of Proposition 1.18 (b) will classically be denoted by $\mathfrak{a}_{\mathfrak{p}}$.

The ring $R_\mathfrak{p}$ is local with the unique maximal ideal

$$\mathfrak{p}R_\mathfrak{p} = \{r/s \mid r \in \mathfrak{p}\,,\ s \notin \mathfrak{p}\}.$$

For every fractional ideal $\mathfrak{a}$ of R we have $\mathfrak{a} = \bigcap_\mathfrak{p} \mathfrak{a}_\mathfrak{p}$, which means that we can recover $\mathfrak{a}$ from its localizations at the primes $\mathfrak{p}$ of R. For more information, see [Ste08][Chapter 4].

Additionally, we have special interest in the case $S = \mathbb{Z} \setminus p\mathbb{Z}$, where $p \in \mathbb{Z}$ is a prime number. In this scenario,

$$R_{(p)} := S^{-1}R = \{r/s \in K \mid r, s \in R \text{ and } p \nmid s\}$$

is a semi-local ring having only finitely many primes which all contain p. Those primes correspond to the primes of R lying above p.

Definition 1.19.
Let R be an order in a number field K, and let $\mathfrak{a}$ such as $\mathfrak{b}$ be integral ideals of R. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are *coprime*, if $\mathfrak{a} + \mathfrak{b} = R$. Sometimes we may also say that $\mathfrak{a}$ is *prime to* $\mathfrak{b}$.

Locally, and since R is a noetherian domain, this is equivalent to the property that $\mathfrak{a}_\mathfrak{p} + \mathfrak{b}_\mathfrak{p} = R_\mathfrak{p}$ for all primes $\mathfrak{p}$ of R. Recall that $\mathfrak{p}\,R_\mathfrak{p}$ is the unique maximal ideal of $R_\mathfrak{p}$. On the one hand, if $\mathfrak{p}$ does not contain $\mathfrak{b}$, then $\mathfrak{b}_\mathfrak{p} = R_\mathfrak{p}$ and we have $\mathfrak{a}_\mathfrak{p} + \mathfrak{b}_\mathfrak{p} = R_\mathfrak{p}$. On the other hand, if $\mathfrak{p}$ contains $\mathfrak{b}$, then $\mathfrak{p}\,R_\mathfrak{p}$ contains $\mathfrak{b}_\mathfrak{p}$ and $\mathfrak{a}_\mathfrak{p} + \mathfrak{b}_\mathfrak{p} = R_\mathfrak{p}$ holds if and only if $\mathfrak{a}_\mathfrak{p} \not\subseteq \mathfrak{p}\,R_\mathfrak{p}$. In this case we have $\mathfrak{a}_\mathfrak{p} = R_\mathfrak{p}$, respectively, $\mathfrak{a}\,R_\mathfrak{p} = R_\mathfrak{p}$. This motivates the following generalization of the previous definition from integral ideals to fractional ideals.

Definition 1.20.
Let R be an order in a number field K. A fractional R-ideal $\mathfrak{a}$ is said to be *prime to* an integral R-ideal $\mathfrak{b}$ if $\mathfrak{a}\,R_\mathfrak{p} = R_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of R containing $\mathfrak{b}$.

The set $I_R(\mathfrak{b})$ of all invertible fractional ideals of R prime to a fixed integral ideal $\mathfrak{b}$ of R forms a subgroup of I_R. We denote by $P_R(\mathfrak{b})$ the intersection of $I_R(\mathfrak{b})$ and P_R.

Definition 1.21.
Let R be an order in a number field K. We define the *conductor* of R in $\mathcal{O}_K$ as

$$\mathfrak{f}_R := \{\, x \in \mathcal{O}_K \mid x\,\mathcal{O}_K \subseteq R \,\}.$$

The conductor of R in $\mathcal{O}_K$ is the largest $\mathcal{O}_K$-ideal contained in R, and hence also an R-ideal. The index $f := [\,\mathcal{O}_K : R\,]$ is contained in $\mathfrak{f}_R$ and $f\mathcal{O}_K \subseteq \mathfrak{f}_R$. There are only finitely many prime ideals $\mathfrak{p}$ of R, which contain $\mathfrak{f}_R$. Following [Neu99][Theorem 12.10, Chapter 1], for every prime ideal $\mathfrak{q}$ of R not containing $\mathfrak{f}_R$, the ideal $\mathfrak{p} := \mathfrak{q}\,\mathcal{O}_K$ of $\mathcal{O}_K$ is a prime ideal. This leads to the following proposition, in which we denote by $\mathrm{Spec}(R)$ the set of prime ideals of R, the so-called *spectrum* of R.

Proposition 1.22.
Let R be an order in a number field K. The map

$$\begin{aligned} \mathrm{Spec}(\mathcal{O}_K) &\longrightarrow \mathrm{Spec}(R) \\ \mathfrak{p} &\longmapsto \mathfrak{p} \cap R \end{aligned}$$

is well-defined, surjective and becomes a bijection if we restrict to primes, which do not contain the conductor $\mathfrak{f}_R$. In this case, the inverse map is then given by $\mathfrak{q} \longmapsto \mathfrak{q}\,\mathcal{O}_K$.

Having introduced localizations and the conductor $\mathfrak{f}_R$ of an order R in $\mathcal{O}_K$, we can give some equivalent descriptions of invertible prime ideals $\mathfrak{p}$ of R. The following theorem summarizes results from [Neu99][Chapter 1.12].

Theorem 1.23.
Let R be an order in a number field K. Let $\mathfrak{f}_R$ be the conductor of R in $\mathcal{O}_K$, and let $\mathfrak{p}$ be a prime ideal of R. The following conditions are equivalent:

(a) *$\mathfrak{p}$ is invertible,*
(b) *$\mathfrak{p}$ does not contain $\mathfrak{f}_R$,*
(c) *$R_\mathfrak{p}$ is a discrete valuation ring (DVR),*
(d) *$R_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{p}$,*
(e) *$\mathfrak{p}\,R_\mathfrak{p}$ is principal.*

Now let $\mathfrak{a}$ be fractional R-ideal. For every invertible prime ideal $\mathfrak{p}$ of R, there exists a uniformizer $\pi_\mathfrak{p}$, such that $\mathfrak{a}\,R_\mathfrak{p} = \pi^{v_\mathfrak{p}(\mathfrak{a})}\,R_\mathfrak{p}$ for some $v_\mathfrak{p}(\mathfrak{a}) \in \mathbb{Z}$. Recalling Definition 1.20, $\mathfrak{a}$ being prime to the invertible prime $\mathfrak{p}$ is equivalent to $v_\mathfrak{p}(\mathfrak{a}) = 0$. Assuming the nominator $\mathfrak{c} \subseteq R$ and denominator $y \in R$ of $\mathfrak{a}$ not to be divisible by the same prime ideal, $v_\mathfrak{p}(\mathfrak{a}) = 0$ if and only if $v_\mathfrak{p}(\mathfrak{c}) = 0$ and $v_\mathfrak{p}(yR) = 0$. Now let $\mathfrak{b}$ be an arbitrary invertible integral R-ideal. Then $\mathfrak{b}$ is not contained in any non-invertible prime ideal $\mathfrak{p}$. Thus, we have

Proposition 1.24.
Let R be an order in a number field K. Let $\mathfrak{a} = \frac{1}{y}\mathfrak{c}$ be a fractional R-ideal with integral nominator $\mathfrak{c} \subseteq R$ and denominator $y \in R$, both not divisible by the same prime ideal. Let $\mathfrak{b}$ be an invertible integral R-ideal. Then $\mathfrak{a}$ is prime to $\mathfrak{b}$ if and only if $v_\mathfrak{p}(\mathfrak{c}) = 0$ and $v_\mathfrak{p}(yR) = 0$ holds for every $\mathfrak{p}$ containing $\mathfrak{b}$.

As already described in Chapter 1.1.1 in the more general situation of noetherian domains, we may define the *class group* (also called the *Picard group*) of an order R as $\mathrm{Pic}(R) = I_R/P_R$. Recall that, for a fixed integral ideal $\mathfrak{b}$ of R, we denote by $I_R(\mathfrak{b})$ the group of invertible fractional ideals of R, which are prime to $\mathfrak{b}$, and by $P_R(\mathfrak{b})$ the analogue subgroup consisting of the principal invertible ideals prime to $\mathfrak{b}$. If $\mathfrak{b} = xR$ is principal, we may just write $I_R(x)$ and $P_R(x)$. If $R = \mathcal{O}_K$, we often just write K in the index instead of $\mathcal{O}_K$.

We will now show that every class in the Picard group of an order R contains a representative, which is prime to a fixed arbitrary integral ideal of R. In the first step, we recall the result for $R = \mathcal{O}_K$, which is a well-known consequence of the following weak approximation theorem ([Coh12][Proposition 1.2.3]).

Theorem 1.25.
Let R be a Dedekind domain with field of fractions K. Let S be a set of prime ideals of R, let $(e_\mathfrak{p})_{\mathfrak{p}\in S}$ a set of integers, and let $(x_\mathfrak{p})_{\mathfrak{p}\in S}$ be a set of elements in K. Then there exists an element $x \in K$ such that:

(a) $v_\mathfrak{p}(x - x_\mathfrak{p}) = e_\mathfrak{p}$ *for all* $\mathfrak{p} \in S$,
(b) $v_\mathfrak{p}(x) \geq 0$ *for all* $\mathfrak{p} \notin S$.

The following lemma about the representation of classes in the class group can be found for example in [Coh12][Corollary 1.2.11].

Lemma 1.26.
Let K be a number field, and let $\mathfrak{a}$ be a non-zero integral ideal of $\mathcal{O}_K$. Every class in the ideal class group $\mathcal{C}\ell_K$ can be represented by an integral ideal $\mathfrak{b}$ prime to $\mathfrak{a}$.

Proof. Let K be a number field, and let $\mathfrak{a}$ be an integral ideal of $\mathcal{O}_K$. Consider a fractional ideal $\mathfrak{c}$ of O_K. We can apply the weak approximation theorem (as presented in Theorem 1.25) to the set S of those prime ideals $\mathfrak{p}$ that either divide $\mathfrak{c}$ or for which $v_\mathfrak{p}(\mathfrak{c}) < 0$. Setting $e_\mathfrak{p} = -v_\mathfrak{p}$, we can find an element $\alpha \in K$ that satisfies $v_\mathfrak{p}(\alpha) = e_\mathfrak{p}$ for these specific prime ideals $\mathfrak{p}$, and has non-negative valuation for all other prime ideals. As a result, the ideal $\mathfrak{b} = \alpha\mathfrak{c}$ is integral, is coprime to $\mathfrak{a}$, and represents the same class as $\mathfrak{c}$ in the ideal class group $\mathcal{C}\ell_K$. □

We now describe a group homomorphism between $I_K(\mathfrak{b})$ and $I_R(\mathfrak{b})$ for every integral $\mathcal{O}_K$-ideal $\mathfrak{b}$ contained in the conductor $\mathfrak{f}_R$.

Theorem 1.27.
Let R be an order in a number field K with conductor $\mathfrak{f}_R$. Let $\mathfrak{b}$ be an integral ideal of $\mathcal{O}_K$ contained in $\mathfrak{f}_R$. Then there exists a group isomorphism between $I_K(\mathfrak{b})$ and $I_R(\mathfrak{b})$ induced by $\mathfrak{p} \longmapsto \mathfrak{p} \cap R$. In particular, every fractional ideal $\mathfrak{a} \in I_R(\mathfrak{b})$ has a unique factorization into prime ideals $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}$ which matches the factorization in $\mathcal{O}_K$ in the sense that $\mathfrak{a}\,\mathcal{O}_K = \prod \mathfrak{q}_i^{e_i}$ with $\mathfrak{q}_i \cap R = \mathfrak{p}_i$.

Proof. It is $\mathfrak{b} \subseteq \mathfrak{f}_R \subseteq R \subseteq \mathcal{O}_K$ such that $\mathfrak{b}$ is also an ideal of R and $I_R(\mathfrak{b})$ is well-defined. Let $\mathfrak{p}$ be a prime ideal of $I_K(\mathfrak{b})$. Then $\mathfrak{p} \cap R$ is coprime to $\mathfrak{b}$ and Proposition 1.22 gives the isomorphism between the subgroups of the prime ideals coprime to $\mathfrak{b}$, which expands to an isomorphism between $I_K(\mathfrak{b})$ and $I_R(\mathfrak{b})$. Now every $\mathfrak{a} \in I_R(\mathfrak{b})$ has a unique image $\mathfrak{a}\,\mathcal{O}_K \in I_K(\mathfrak{b})$ with a prime ideal factorization $\mathfrak{a}\,\mathcal{O}_K = \prod \mathfrak{q}_i^{e_i}$ and $\mathfrak{a} = \prod \mathfrak{p}_i^{e_i}$ provides a unique factorization into primes $\mathfrak{p}_i = \mathfrak{q}_i \cap R$ of R. □

Combining Proposition 1.26 and Theorem 1.27, we can give a surjective homomorphism between the class groups of R and $\mathcal{O}_K$.

Theorem 1.28.
Let K be a number field, and let R be an order in K. The following group homomorphism is surjective:

$$\begin{aligned} \eta \,:\, \mathrm{Pic}(R) &\longrightarrow \mathcal{C}\ell_K \\ [\mathfrak{b}] &\longmapsto [\mathfrak{b}\,\mathcal{O}_K]\,. \end{aligned}$$

The kernel is given by $\ker\eta = \{[\alpha\,\mathcal{O}_K \cap R] \mid \alpha \in \mathcal{O}_K$ prime to $\mathfrak{f}_R\}$, where $\mathfrak{f}_R$ is the conductor of R.

Proof. Following Lemma 1.26, we can represent every class of $\mathcal{C}\ell_K$ by an integral ideal $\mathfrak{a}$ coprime to $\mathfrak{f}_R$ and $\mathfrak{a} \cap R$ is also coprime to $\mathfrak{f}_R$. Due to Theorem 1.27, we have $\mathfrak{a} = (\mathfrak{a} \cap R)\,\mathcal{O}_K$, so $\mathfrak{a} \cap R$ is an invertible ideal of R and $[\mathfrak{a} \cap R]$ is a preimage of $[\mathfrak{a}]$. It remains to determine the kernel. of η. On the one hand, a class $[\mathfrak{b}] \in \mathrm{Pic}(R)$ becomes trivial in $\mathcal{C}\ell_K$ if there exists $\alpha \in \mathcal{O}_K$ with $\mathfrak{b}\mathcal{O}_K = \alpha\mathcal{O}_K$. Since $\mathfrak{b}\mathcal{O}_K$ is coprime to $\mathfrak{f}_R$, α has to be coprime to $\mathfrak{f}_R$. Then $\mathfrak{b} = \mathfrak{b}\mathcal{O}_K \cap R = \alpha\mathcal{O}_K \cap R$. On the other hand, if $\alpha \in \mathcal{O}_K$ is coprime to $\mathfrak{f}_R$, then $\alpha\mathcal{O}_K \cap R$ is coprime to $\mathfrak{f}_R$. Hence $(\alpha\mathcal{O}_K \cap R)\,\mathcal{O}_K = \alpha\mathcal{O}_K$, which is trivial in $\mathcal{C}\ell_K$. □

In a first step, we now show that every class in the Picard group of an order R can be represented by an ideal coprime to the conductor $\mathfrak{f}_R$.

Lemma 1.29.
Let R be an order in a number field K with conductor $\mathfrak{f}_R$. Then every ideal class in $\mathrm{Pic}(R)$ *contains an ideal prime to $\mathfrak{f}_R$.*

Proof. Let $[\mathfrak{b}] \in \mathrm{Pic}(R)$. According to Theorem 1.28, there exists a class $[\mathfrak{a}] \in \mathcal{C}\ell_K$ such that $\eta([\mathfrak{b}]) = [\mathfrak{a}] \in \mathcal{C}\ell_K$ and by Lemma 1.26, we may assume, without loss of generality, that $\mathfrak{a} \in I_K(\mathfrak{f}_R)$ is integral. Now

$$\eta([\mathfrak{a} \cap R]) = [\mathfrak{a}] = \eta([\mathfrak{b}])$$

and since we know the kernel of η, there exists an $\alpha \in \mathcal{O}_K$ prime to $\mathfrak{f}_R$ such that

$$[\mathfrak{b}] = [(\mathfrak{a} \cap R)]\,[(\alpha\,\mathcal{O}_K \cap R)].$$

Applying the isomorphism of Theorem 1.27, the R-ideal $\mathfrak{a} \cap R$ is prime to $\mathfrak{f}_R$. On the other hand, since $\alpha\,\mathcal{O}_K$ is prime to $\mathfrak{f}_R$, the same holds for $\alpha\,\mathcal{O}_K \cap R$. It follows that every ideal class can be represented by an ideal prime to $\mathfrak{f}_R$. □

In the final lemma of this section, we generalize Lemma 1.26 to arbitrary orders R, and, respectively, Lemma 1.29 to arbitrary integral ideals $\mathfrak{b}$. Note that, due to Theorem 1.23, we can apply the idea of the weak approximation theorem for all primes that do not contain the conductor.

Lemma 1.30.
Let R be an order in a number field K. Let $\mathfrak{b}$ be an integral $\mathcal{O}_K$-ideal. Then every ideal class in $\mathrm{Pic}(R)$ *can be represented by an integral ideal prime to $\mathfrak{b}$.*

Proof. Let $\mathfrak{f}_R$ be the conductor of R in $\mathcal{O}_K$. Following Lemma 1.29, we can represent every class in $\mathrm{Pic}(R)$ by an ideal integral $\mathfrak{a}$, which is coprime to $\mathfrak{f}_R$. Hence, $\mathfrak{a}_\mathfrak{p} = R_\mathfrak{p}$ for all $\mathfrak{p} \supseteq \mathfrak{f}_R$. Now let P be the set of prime ideals of R, which lie above $\mathfrak{b}$, but do not lie above $\mathfrak{f}_R$. Following Theorem 1.23, every prime ideal $\mathfrak{p}$ in P is invertible, which means that $R_\mathfrak{p}$ is a DVR and $R_\mathfrak{p} = (\mathcal{O}_K)_\mathfrak{p}$. Hence, we can take a uniformizer $\pi_\mathfrak{p}$, which satisfies

$$\pi_\mathfrak{p} \equiv 1 \pmod{\mathfrak{f}_R} \quad \text{and} \quad \pi_\mathfrak{p} \equiv 1 \pmod{\mathfrak{q}} \text{ for all } \mathfrak{q} \in P \setminus \{\mathfrak{p}\}.$$

Now define

$$x := \prod_{\mathfrak{p} \in P} \pi_\mathfrak{p}^{-\operatorname{ord}_{\pi_\mathfrak{p}}(\mathfrak{a})}.$$

Then $\mathfrak{a}' := x\,\mathfrak{a}$ is a fractional ideal prime to $\mathfrak{b}$ representing the class of $\mathfrak{a}$. To be more precise, for every $\mathfrak{p} \in P$ we have

$$\mathfrak{a}'\,R_\mathfrak{p} = (x\,\mathfrak{a})_\mathfrak{p} = x_\mathfrak{p}\,\mathfrak{a}_\mathfrak{p} = \pi_\mathfrak{p}^{-\operatorname{ord}_{\pi_\mathfrak{p}}(\mathfrak{a})}\,\pi_\mathfrak{p}^{\operatorname{ord}_{\pi_\mathfrak{p}}(\mathfrak{a})}\,R_\mathfrak{p} = R_\mathfrak{p}.$$

For every $\mathfrak{p} \supseteq \mathfrak{b}$ with $\mathfrak{p} \notin P$ we have $\mathfrak{p} \supseteq \mathfrak{f}_R$ and since $\mathfrak{a}$ is prime to $\mathfrak{f}_R$ we get

$$\mathfrak{a}'\,R_\mathfrak{p} = (x\,\mathfrak{a})_\mathfrak{p} = x_\mathfrak{p}\,\mathfrak{a}_\mathfrak{p} = R_\mathfrak{p}.$$

If we multiply by the norm of the denominator of $\mathfrak{a}'$, we additionally receive an integral representative prime to $\mathfrak{b}$. □

1.1.3 Gorenstein orders

During this section, we follow [JT15] and [Mar20] starting with the definition of the term Gorenstein order in number fields.

Definition 1.31.
Let K be a number field, and let S be an order in K. We call S a *Gorenstein order* if its trace dual S^* is an invertible fractional ideal of S. Furthermore, S is called a *Bass order*, if every overorder $S' \supseteq S$ of S is also Gorenstein.

As pointed out in [JT15][Characterization 2.6], there are further equivalent descriptions of the term Gorenstein order, but we will focus on the above-mentioned view as orders with an invertible trace dual. For a number field $K = \mathbb{Q}(\alpha)$ with $\alpha \in \mathcal{O}_K$, classical examples of Gorenstein orders include $\mathbb{Z}[\alpha]$ and the ring of integers $\mathcal{O}_K$. Moreover, if K is a quadratic number field, every order S in K is Gorenstein. However, this is not true if the degree of K over $\mathbb{Q}$ is three or larger. In that case, K contains infinitely many orders that are Gorenstein, as well as infinitely many that are not. For instance, if $p \in \mathbb{Z}$ is a prime number, then, according to [JT15][Example 7.2], the lattice $\mathbb{Z}[p\alpha]$ is a Gorenstein order in K, while the lattice $\langle 1, p\alpha, p\alpha^2, \ldots, p\alpha^{n-1}\rangle_\mathbb{Z}$ is an order in K that is not Gorenstein. We can also consider the compositum of Gorenstein orders in different number fields. In order to do so, we introduce the following term.

Definition 1.32.
Let K and L be number fields. Then K and L are said to be *linearly disjoint over* $\mathbb{Q}$ if every $\mathbb{Q}$-basis of K is linear independent over L.

We can now formulate the following result, which is [JT15][Proposition 3.5].

Proposition 1.33.
If $S = S_1 \cdots S_r$ is the compositum of $r \geq 1$ Gorenstein orders S_i, and their fields of fractions $K_i := \mathrm{Quot}(S_i)$ are pairwise linearly disjoint over $\mathbb{Q}$, then S is also a Gorenstein order.

Consequently, for a number field K and $\alpha_1, \ldots, \alpha_r \in K$, the order $\mathbb{Z}[\alpha_1, \ldots, \alpha_r]$ in K is Gorenstein if the fields $\mathbb{Q}(\alpha_1), \ldots, \mathbb{Q}(\alpha_r)$ are linearly disjoint. It is clear that Proposition 1.33 can also be employed to construct many other Gorenstein and non-Gorenstein orders. In Chapter 2, we will explicitly analyze and partially classify Gorenstein and non-Gorenstein orders in cubic number fields.

1.2 Finite Rings

In this section, we consider R to be a finite ring and focus on the relationship between the cardinalities of finite rings and their unit groups. These considerations will later be applied in decomposing the index of relative orders. Our primary references are [McD74][Chapter 18] and [Ste08][Chapter 5].

Definition 1.34.
Let R be a finite ring, and let $\mathfrak{p}$ be a prime ideal of R. We define the *norm of* $\mathfrak{p}$ to be

$$N(\mathfrak{p}) := \left| \left({}^{R}\!/_{\mathfrak{p}} \right) \right| .$$

The following statement relates the cardinalities of finite rings with the cardinalities of their unit group and can be found in [Ste12][Exercise 44, Chapter 2] as an unproven exercise.

Proposition 1.35.
Let R be a finite ring, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideals of R. Then we have

$$\left| R^{\times} \right| = |R| \prod_{i=1}^{r} \left(1 - \frac{1}{N(\mathfrak{p}_i)} \right).$$

Proof. Firstly, we have $\{0\} = \cap_{i=1}^{r} \mathfrak{p}_i^{n_i}$ for some $n_i \geq 1$. All those prime ideals are coprime to each other such that the Chinese remainder theorem gives us

$$R \cong {}^{R}\!/_{\{0\}} \cong {}^{R}\!/_{\cap_{i=1}^{r} \mathfrak{p}_i^{n_i}} \cong {}^{R}\!/_{\prod_{i=1}^{r} \mathfrak{p}_i^{n_i}} \cong {}^{R}\!/_{\mathfrak{p}_1^{n_1}} \times \cdots \times {}^{R}\!/_{\mathfrak{p}_r^{n_r}}. \tag{1.1}$$

Considering the units on both sides gives us

$$R^\times \cong \left(R/\mathfrak{p}_1^{n_1}\right)^\times \times \cdots \times \left(R/\mathfrak{p}_r^{n_r}\right)^\times . \tag{1.2}$$

Combing (1.1) with (1.2) we get

$$\frac{|\,R^\times\,|}{|\,R\,|} = \prod_{i=1}^{r} \frac{\left|\left(R/\mathfrak{p}_i^{n_i}\right)^\times\right|}{\left|\left(R/\mathfrak{p}_i^{n_i}\right)\right|}. \tag{1.3}$$

For all $i \in \{1, \ldots, r\}$ it is $R/\mathfrak{p}_i^{n_i}$ a finite local ring with the unique maximal ideal $\mathfrak{m}_i = \mathfrak{p}_i/\mathfrak{p}_i^{n_i}$ such that

$$\left|\left(R/\mathfrak{p}_i^{n_i}\right)^\times\right| = \left|\left(R/\mathfrak{p}_i^{n_i}\right)\right| - \left|\left(\mathfrak{p}_i/\mathfrak{p}_i^{n_i}\right)\right| . \tag{1.4}$$

Hence, for each factor on the right-hand side of (1.3), we receive from (1.4) that

$$\frac{\left|\left(R/\mathfrak{p}_i^{n_i}\right)^\times\right|}{\left|\left(R/\mathfrak{p}_i^{n_i}\right)\right|} = 1 - \frac{\left|\left(\mathfrak{p}_i/\mathfrak{p}_i^{n_i}\right)\right|}{\left|\left(R/\mathfrak{p}_i^{n_i}\right)\right|}. \tag{1.5}$$

Finally, combining the fact that $(R/\mathfrak{p}_i^{n_1})/(\mathfrak{p}_i/\mathfrak{p}_i^{n_1}) \cong (R/\mathfrak{p}_i)$ with (1.5), we receive

$$\frac{\left|\left(R/\mathfrak{p}_i^{n_i}\right)^\times\right|}{\left|\left(R/\mathfrak{p}_i^{n_i}\right)\right|} = 1 - \frac{1}{\left|\left(R/\mathfrak{p}_i\right)\right|} = 1 - \frac{1}{N(\mathfrak{p}_i)}$$

and (1.3) becomes the following equation, which is equivalent to the claim

$$\frac{|\,R^\times\,|}{|\,R\,|} = \prod_{i=1}^{r} \left(1 - \frac{1}{N(\mathfrak{p}_i)}\right).$$

□

The following theorem is a result from [McD74][Theorem 2, Chapter 18] and describes the connection between unit groups and residue fields of finite local rings.

Theorem 1.36.
Let R be a finite local ring with unique maximal ideal $\mathfrak{m}$ and residue field $k := R/\mathfrak{m}$. The following sequence is exact:

$$1 \to 1 + \mathfrak{m} \to R^\times \to k^\times \to 1\,.$$

1.3 Global class field theory

This section presents some basic results of *global class field theory*. We specifically focus on Ray class groups, which will play a significant role in the discussion on the construction of certain minimal orders (see Chapter 8.1). One of the main results of global class field theory is *Artin's Reciprocity theorem*, which establishes a connection between the Galois group of an abelian extension of a global field and certain generalized ideal class groups. Note that Artin's Reciprocity Theorem is non-constructive. The complex multiplication theory of abelian varieties, which we will discuss later, provides partial answers to the question of constructing these abelian extensions. However, before delving into complex multiplication theory, it is valuable to review and state some essential principles of global class field theory and understand its limitations. In order to do so, we follow the ideal theoretic version of global class field theory, as presented in [Jan96], [Coh12], and [Cox13].

Definition 1.37.
Let K be a number field. We define a *modulus* of K to be a formal product $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$ over all places $\mathfrak{p}$ of K, where the integer exponents satisfy the following conditions:

(a) $m_{\mathfrak{p}} \geq 0$ and at most finitely many are non-zero,
(b) $m_{\mathfrak{p}} = 0$ if $\mathfrak{p}$ is a complex infinite place and
(c) $m_{\mathfrak{p}} \leq 1$ if $\mathfrak{p}$ is a real infinite place.

Now let $\mathfrak{m}$ be a modulus of a number field K. We will write $\mathfrak{m}$ as a formal product $\mathfrak{m} = \mathfrak{m}_0 \, \mathfrak{m}_\infty$, where $\mathfrak{m}_0$ collects the finite part, which is actually an integral $\mathcal{O}_K$-ideal, and $\mathfrak{m}_\infty$ consists of the infinite real part of $\mathfrak{m}$. We say that another modulus $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ of K divides $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{m_{\mathfrak{p}}}$, if $n_{\mathfrak{p}} \leq m_{\mathfrak{p}}$ for all places $\mathfrak{p}$ of K. Note that for number fields K without any real embedding, we may consider a modulus simply as an integral $\mathcal{O}_K$-ideal. Recall that the group of fractional ideals of K that are coprime to $\mathfrak{m}_0$ is

$$I_K(\mathfrak{m}) := \{\mathfrak{a} \in I_K \mid v_{\mathfrak{p}}(\mathfrak{a}) = 0 \,\text{for all}\, \mathfrak{p} \mid \mathfrak{m}_0\} \,.$$

Definition 1.38.
Let K be a number field and let $\mathfrak{m}$ be a modulus of K. We define the following groups:

(a) The group of units in K which generate ideals coprime to $\mathfrak{m}_0$ is denoted as

$$K(\mathfrak{m}) := \left\{\alpha \in K^\times \mid \alpha\mathcal{O}_K \in I_K(\mathfrak{m})\right\}.$$

(b) The subgroup $K_1(\mathfrak{m})$ of $K(\mathfrak{m})$ is defined as

$$K_1(\mathfrak{m}) := \left\{\alpha \in K(\mathfrak{m}) \;\middle|\; \begin{array}{l} v_\mathfrak{p}(\alpha - 1) \geq v_\mathfrak{p}(\mathfrak{m}_0) \text{ for all } \mathfrak{p} \mid \mathfrak{m}_0, \\ \alpha_v > 0 \text{ for all real places } v \in \mathfrak{m}_\infty \end{array}\right\}.$$

(c) The subgroup of $I_K(\mathfrak{m})$ containing the principal ideals generated by elements of $K_1(\mathfrak{m})$ is represented as

$$P_{K,1}(\mathfrak{m}) := \{\alpha\mathcal{O}_K \mid \alpha \in K_1(\mathfrak{m})\}.$$

(d) The *Ray class group* of K modulo $\mathfrak{m}$ is defined as:

$$\mathcal{C}\ell_K(\mathfrak{m}) := {}^{I_K(\mathfrak{m})}\!/_{P_{K,1}(\mathfrak{m})}.$$

Note that the Ray class group of K for the modulus $\mathfrak{m} = 1$ is the classical ideal class group $\mathcal{C}\ell_K$. We give a simple example for the introduced notation, in particular for a Ray class group, in order to better understand their definitions. The following example can be found in [Sut19][Example 21.6, Chapter 21.3].

Example 1.39.
Consider the rational number field $K = \mathbb{Q}$ with $\mathcal{O}_K = \mathbb{Z}$ and the modulus $\mathfrak{m} = 5\mathbb{Z}$. Now, the group of fractional ideals $(\alpha) = \alpha\mathbb{Z}$ coprime to $\mathfrak{m} = \mathfrak{m}_0$ is given by:

$$I_K(\mathfrak{m}) = \left\{(1), \left(\frac{1}{2}\right), (2), \left(\frac{1}{3}\right), \left(\frac{2}{3}\right), \left(\frac{3}{2}\right), (3), \left(\frac{1}{4}\right), \left(\frac{3}{4}\right), \left(\frac{4}{3}\right), (4), \left(\frac{1}{6}\right), (6), \ldots\right\}.$$

Among these, the subgroup $P_{K,1}(\mathfrak{m})$ consists of:

$$P_{K,1}(\mathfrak{m}) = \left\{(1), \left(\frac{2}{3}\right), \left(\frac{3}{2}\right), \left(\frac{1}{4}\right), (4), (6), \left(\frac{1}{6}\right), \left(\frac{2}{7}\right), \left(\frac{7}{2}\right), \ldots\right\}.$$

The occurrence of $\left(\frac{2}{3}\right)$ in $P_{K,1}(\mathfrak{m})$ might wonder since $\frac{2}{3}$ is not an element of $K_{\mathfrak{m},1}$. However, its negative counterpart $\frac{-2}{3}$ is an element of $K_{\mathfrak{m},1}$ and, in terms of ideal representation, $\left(\frac{-2}{3}\right)$ is equal to $\left(\frac{2}{3}\right)$. The Ray class group of K modulo $\mathfrak{m}$ is then

given by:

$$\mathcal{C}\ell_K(\mathfrak{m}) = {}^{I_K(\mathfrak{m})}\!/_{P_{K,1}(\mathfrak{m})} = \{[(1)], [(2)]\} \cong (\mathbb{Z}/5\mathbb{Z})^\times / \{\pm 1\}.$$

As pointed out in [Coh12][Lemma 3.3.1] and presented below, Theorem 1.26 generalizes to Ray class groups, which means that we can always take an integral representative of $\mathcal{C}\ell_K(\mathfrak{m})$ which is prime to a fixed integral ideal $\mathfrak{b}$ of $\mathcal{O}_K$.

Lemma 1.40.
Let $\mathfrak{m}$ be a modulus of a number field K, and let $\mathfrak{b}$ be an integral ideal of $\mathcal{O}_K$. Every class in the Ray class group $\mathcal{C}\ell_K(\mathfrak{m})$ can be represented by an integral ideal $\mathfrak{a}$ coprime to $\mathfrak{b}$.

Before we state the fundamental theorems of class field theory, we introduce some notation.

Definition 1.41.
Let L be a finite abelian extension of a number field K, and let $\mathfrak{m}$ be a modulus of K divisible by all places of K, which ramify in L. Via the *Artin symbol* we can define the *Artin map*, which is

$$\begin{aligned} \Phi_\mathfrak{m} \,:\, I_K(\mathfrak{m}) &\longrightarrow \mathrm{Gal}(L/K) \\ \mathfrak{a} &\longmapsto \left(\frac{L/K}{\mathfrak{a}}\right). \end{aligned}$$

Definition 1.42.
Given a number field K and a modulus $\mathfrak{m}$ of K, a subgroup $H \subseteq I_K(\mathfrak{m})$ is termed a *congruence subgroup* for $\mathfrak{m}$ if it contains $P_{K,1}(\mathfrak{m})$. When this condition is given, the quotient group $I_K(\mathfrak{m})/H$ is considered as a *generalized ideal class group* for $\mathfrak{m}$. When $H = P_{K,1}(\mathfrak{m})$, the congruence subgroup for $\mathfrak{m}$ is specifically defined as the *Ray class group of* $\mathfrak{m}$.

We can now recall the famous *Artin Reciprocity Theorem*, which can be found for example in [Jan96][Theorem 5.7, Chapter 5].

Theorem 1.43.
Let K be a number field and L be an abelian extension of K. Let $\mathfrak{m}$ be a modulus of K, which is divisible by all places of K that ramify in L. Then:

(a) *The Artin map is surjective.*
(b) *If the exponents of the places in $\mathfrak{m}_0$ are sufficiently large, then $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ and*

$$I_K(\mathfrak{m})/\ker(\Phi_{\mathfrak{m}}) \cong Gal(L/K).$$

Let $\mathfrak{m}$ be a modulus of a number field K as in Theorem 1.43 such that $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$ and let $\mathfrak{n}$ be another modulus divisible by $\mathfrak{m}$, then $\ker(\Phi_{\mathfrak{n}})$ is a congruence subgroup for $\mathfrak{n}$. Actually, following [Jan96][Theorem 12.7, Chapter V], for every finite abelian extension L over K there exists a minimal modulus $\mathfrak{f}$, called the *conductor* of L over K, which satisfies

$$I_K(\mathfrak{f})/\ker(\Phi_{\mathfrak{f}}) \cong \mathrm{Gal}(L/K).$$

Consider a place $\mathfrak{p}$ of K. It ramifies in L precisely when it divides $\mathfrak{f}$. Now, given a modulus $\mathfrak{m}$ that is divisible by all places that ramify, the kernel $\ker(\Phi_{\mathfrak{m}})$ becomes a congruence subgroup for $\mathfrak{m}$ only when $\mathfrak{m}$ itself is divisible by $\mathfrak{f}$. We say that a finite abelian extension L of K *admits* a modulus $\mathfrak{m}$ if, firstly, all places of K that ramify in L are included in $\mathfrak{m}$, and secondly, $\ker(\Phi_{\mathfrak{m}})$ is a congruence subgroup for $\mathfrak{m}$. This foundational idea is captured in what is known as the *Existence theorem*, which can be found in [Jan96][Theorem 9.16, Chapter V]:

Theorem 1.44.
Let K be a number field, and let $\mathfrak{m}$ be a modulus of K. Let H be a congruence subgroup for $\mathfrak{m}$. Then there exists a unique abelian extension L of K such that all places of K that ramify in L divide $\mathfrak{m}$ and if $\Phi_{\mathfrak{m}} : I_K(\mathfrak{m}) \to Gal(L/K)$ is the Artin map of L over K, then $H = \ker(\Phi_{\mathfrak{m}})$. In particular, the map $L \mapsto \ker(\Phi_{\mathfrak{m}})$ is an inclusion reversing bijection of the finite abelian extensions of K which admit $\mathfrak{m}$ and the congruence subgroups H for $\mathfrak{m}$.

Applying this theorem to the modulus $\mathfrak{m} = 1$, we obtain that there exists a unique finite abelian extension L of K, such that $\mathcal{C}\ell_K \cong \mathrm{Gal}(L/K)$.

Definition 1.45.
Let L be the finite abelian extension of a number field K such that $\mathcal{C}\ell_K \cong \mathrm{Gal}(L/K)$, then L is said to be the *Hilbert class field* of K.

Clearly, the Hilbert class field L of a number field K is unramified for the choice of $\mathfrak{m} = 1$ and maximal with this property, due to the choice of $H = P_{K,1}(\mathfrak{m})$. In other words, the Hilbert class field is the finite abelian extension of K, which corresponds to the Ray class group for the modulus $\mathfrak{m} = 1$. The Existence theorem also justifies the following term.

Definition 1.46.
Let $\mathfrak{m}$ be a modulus of a number field K. We define the finite abelian extension $K_\mathfrak{m}$ of K corresponding the congruence group $H = P_{K,1}(\mathfrak{m})$ as the *Ray class field* for the modulus $\mathfrak{m}$.

We may derive the Kronecker-Weber theorem from the Existence theorem, which is for example proven in [Cox13][Theorem 8.8, Chapter 2]. This theorem states that every abelian extension of $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_m)$ for some $m \in \mathbb{Z}$. In the following example, we present this result in the case where m is a prime number:

Example 1.47.
Consider the rational number field $K = \mathbb{Q}$ and a modulus $\mathfrak{m} = (p)$, where p is a prime number. Theorem 1.44 implies the existence of a unique maximal abelian extension L of K that ramifies precisely at the places of $\mathfrak{m}$ and nowhere else. In our case, this is the cyclotomic extension $L = K(\mathfrak{m}) = \mathbb{Q}(\zeta_p)$ generated by a p-th root of unity, ζ_p. The Galois group of L/K corresponds to the quotient of the ideal class group of K by the congruence subgroup defined by $\mathfrak{m}$.

While global class field theory offers a theoretical framework for the description of abelian extensions of number fields, it does not provide their explicit construction. This limitation is addressed by the complex multiplication theorem and solves this issue for a specific class of number fields. In the following section, we will introduce the basic terms of complex multiplication theory.

1.4 Complex multiplication fields and types

This section provides essential definitions and results on complex multiplication fields and types. This represents the number theoretical side of complex multiplication theory and is fundamental for the following discussions on abelian varieties with complex multiplication. Our primary references are [Lan83], [Spa94], [Shi16], [Str10], [Bis11], and [Kıl16]. We also refer to [Spa94] and [Wen01b].

Definition 1.48.
A number field K is said to be a *complex multiplication field (CM field)*, if it is a totally imaginary quadratic extension of a totally real number field K_0.

For every CM field K, there exists an automorphism ρ, which fixes K_0 and satisfies the condition that if $\iota : K \hookrightarrow \mathbb{C}$ is an embedding from K into $\mathbb{C}$ and $\bar{\cdot}$ denotes the complex conjugation of $\mathbb{C}$, then $\bar{\cdot} \circ \iota = \iota \circ \rho$.

Definition 1.49.
Let K be a CM field, and let K_0 be its maximal totally real subfield. The automorphism ρ of K is called the *complex multiplication on* K if it fixes K_0 and satisfies the condition that if $\iota : K \hookrightarrow \mathbb{C}$ is an embedding from K into $\mathbb{C}$, then $\bar{\cdot} \circ \iota = \iota \circ \rho$.

In order to simplify notation, we will admit both notations $\bar{\cdot}$ and ρ for the complex conjugation of K. Note that, due to the fact that K is a quadratic extension of a totally real number field K_0, we can always assume that there exists an $n \in \mathbb{N}$ with $[\, K : \mathbb{Q}\,] = 2n$.

Definition 1.50.
Let K be a CM field of degree $2n$ over $\mathbb{Q}$. Let N' be a number field, which contains a subfield that is isomorphic over $\mathbb{Q}$ to a normal closure of K over $\mathbb{Q}$. We call a set Φ of n different embeddings $\phi : K \hookrightarrow N'$, where none of these embeddings is a complex conjugated of one of the others, a *complex multiplication type (CM type) of K with values in N'*. We may also call such a tuple (K, Φ) a CM type.

Definition 1.51.
Let K be a CM field, and let $\tilde{K}$ be a strict CM subfield of K. If $\tilde{\Phi}$ is a CM type of $\tilde{K}$ with values in N', then we call

$$\Phi := \{\phi \in \mathrm{Hom}(K, N') \mid \phi|_{\tilde{K}} \in \tilde{\Phi}\}$$

the CM type of K *induced* by $\tilde{\Phi}$. If (K, Φ) is not induced by any CM type $(\tilde{K}, \tilde{\Phi})$, then we call (K, Φ) *primitive*.

If we fix a CM type (K, Φ), then the normal closure N of K over $\mathbb{Q}$ is also a CM field, and we may fix a CM type Φ_N of N with values in N', which is induced by Φ. As presented in [Shi16][Proposition 26], we have the following proposition.

Proposition 1.52.
Let (K, Φ) be a CM type, and let N be a normal closure of K over $\mathbb{Q}$. Then (K, Φ) is primitive if and only if

$$\mathit{Gal}(N/K) = \{\gamma \in \mathit{Gal}(K/\mathbb{Q}) \mid \Phi_N \circ \gamma = \Phi_N\}.$$

Applying this proposition to the case in which K is normal over $\mathbb{Q}$, we can immediately formulate the following corollary.

Corollary 1.53.
Let Φ be a CM type of a CM field K, which is normal over $\mathbb{Q}$. Then (K, Φ) is primitive if and only if there exists no non-trivial $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\Phi \circ \sigma = \Phi$.

Definition 1.54.
Let K be a CM field, and let Φ_1 such as Φ_2 be CM types of K. Then Φ_1 and Φ_2 of a CM field K are called *equivalent*, if there exists an automorphism σ of K with $\Phi_1 \circ \sigma = \Phi_2$.

Now let (K, Φ) be a CM type with values in N' and N be a normal closure of K over $\mathbb{Q}$. If we assume N' to be isomorphic to N, then Φ_N only contains isomorphisms, and we may take their inverse, which we collect in the set

$$\Phi_N^{-1} := \{\phi^{-1} : N' \hookrightarrow N \mid \phi \in \Phi_N\}.$$

The fixed field K^r of $\{\gamma \in \mathrm{Gal}(N'/\mathbb{Q}) \mid \Phi_N^{-1} \circ \gamma = \Phi_N^{-1}\}$ is a CM field and its CM type $\Phi^r := \Phi_N^{-1}|_{K^r}$ is primitive. This justifies the following definition.

Definition 1.55.
Let (K, Φ) be a CM type with values in a number field $N' \cong N$, where N is a normal closure of K over $\mathbb{Q}$. We define the *reflex field* K^r *of* (K, Φ) as the fixed field of

$$\{\gamma \in \mathrm{Gal}(N'/\mathbb{Q}) \mid \Phi_N^{-1} \circ \gamma = \Phi_N^{-1}\}.$$

Additionally, the CM type $\Phi^r = \Phi_N^{-1}|_{K^r}$ is identified as the *reflex type* of (K, Φ) and the pair (K^r, Φ^r) is said to be the *reflex* of (K, Φ).

Note that if a CM type (K, Φ) is induced by a CM type $(\tilde{K}, \tilde{\Phi})$, then they have the same reflex (K^r, Φ^r). If we take the reflex (K^{rr}, Φ^{rr}) of the reflex (K^r, Φ^r) of (K, Φ), then this is a primitive CM type and $K^{rr} \subseteq K$ (see [Str10][Lemma 7.2]). If (K, Φ) is primitive, then $K^{rr} = K$ and $\Phi^{rr} = \Phi$. The following lemma can be found in [Str10][Lemma 7.3] and is a direct consequence of the definition of the reflex field. We also refer to [Lan83][Chapter 3.3].

Lemma 1.56.
Let (K, Φ) be a CM type with values in N'. The reflex field K^r of (K, Φ) satisfies

$$\mathit{Gal}(N'/K^r) = \{\gamma \in \mathit{Gal}(N'/\mathbb{Q}) \mid \gamma \circ \Phi = \Phi\}.$$

This lemma justifies the following definition of the term *type norm* of Φ.

Definition 1.57.
Let (K, Φ) be a CM type with values in a number field $N' \cong N$, where N is a normal closure of K over $\mathbb{Q}$. We define the *type norm* of Φ as

$$\mathrm{N}_\Phi : K \longrightarrow K^r \subseteq N' \,,\, x \longmapsto \prod_{\phi \in \Phi} \phi(x)\,.$$

As presented in [Shi16][Proposition 28, Chapter 8.3] and [BS17][Chapter 2], the image of K under the type norm generates the reflex field over $\mathbb{Q}$:

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

Furthermore, this map defines a group homomorphism on the unit groups of K and K^r. As presented in [Shi16][Proposition 29, Chapter 8.3], for all fractional ideals $\mathfrak{a}$ of $\mathcal{O}_K$, there exists a unique fractional ideal $\mathfrak{b}$ of $\mathcal{O}_{K^r}$, such that

$$\mathfrak{b}\mathcal{O}_{N'} = \prod_{\phi \in \Phi} \phi(\mathfrak{a})\mathcal{O}_{N'}.$$

This enables us to extend the term type norm to the group of fractional ideals of K and to the class group of K. The following lemma is for example stated in [Lan83][Remark, Chapter 3.3] and [Str10][Lemma 8.3].

Lemma 1.58.
Let (K, Φ) be a CM type with values in N', and let K^r be the reflex field of (K, Φ). The type norm induces group homomorphisms $\mathrm{N}_\Phi : I_K \longrightarrow I_{K^r}$, $\mathfrak{a} \longmapsto \mathfrak{b} =: \mathrm{N}_\Phi(\mathfrak{a})$, where $\mathfrak{b}\mathcal{O}_{N'} = \prod_{\phi \in \Phi} \phi(\mathfrak{a})\mathcal{O}_{N'}$, and $\mathrm{N}_\Phi : \mathcal{C}\ell_K \longrightarrow \mathcal{C}\ell_{K^r}$.

Using the insights from the previous lemma, we find the following properties of the type norm. These are detailed further in [Str10][Chapter 1.8].

$$\begin{aligned} \mathrm{N}_\Phi(x)\,\overline{\mathrm{N}_\Phi(x)} &= \mathrm{N}_{K/\mathbb{Q}}(x) \qquad \forall x \in K^\times, \quad \text{and} \\ \mathrm{N}_\Phi(\mathfrak{a})\,\overline{\mathrm{N}_\Phi(\mathfrak{a})} &= \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a}) \qquad \forall \mathfrak{a} \in I_K. \end{aligned}$$

Note that all of these considerations also hold for the so-called *reflex type norm* N_{Φ^r}, which is defined to be the type norm of the reflex (K^r, Φ^r) of (K, Φ).

We state one further proposition in order to handle images of ideals prime to an integer under the type norm.

Proposition 1.59.
Let (K, Φ) be a CM type, and let (K^r, Φ^r) be its reflex. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_{K^r}$ prime to an integer $f \in \mathbb{Z}$. Then $\mathrm{N}_{\Phi^r}(\mathfrak{a})$ is prime to f.

Proof. Let N be a normal closure containing K and K^r. Since f is an integer, the ideal $f\,\mathcal{O}_N$ is Galois invariant, so for every $\sigma \in \mathrm{Gal}(N/\mathbb{Q})$ we have that $\sigma(\mathfrak{a})$ and $\sigma(f\,\mathcal{O}_N) = f\,\mathcal{O}_N$ are coprime. Consequently, $\mathrm{N}_{\Phi^r}(\mathfrak{a})\,\mathcal{O}_N = \prod_{\phi\in\Phi^r}\phi(\mathfrak{a})$ is coprime to $f\,\mathcal{O}_N$. This implies that $\mathrm{N}_{\Phi^r}(\mathfrak{a})$ is coprime to $f\,\mathcal{O}_K$. □

1.5 Abelian varieties with complex multiplication

In this section we turn our attention to the connection between algebraic geometry and complex multiplication, focusing specifically on abelian varieties with complex multiplication. On the geometrical side, abelian varieties can be thought of as an extension of elliptic curves, and they hold a significant place in modern mathematics, especially in cryptography. We will lay out the foundational definitions for abelian varieties over arbitrary fields. This is crucial as these varieties are of interest not just considered over $\mathbb{C}$, but also over finite fields and number fields. We introduce fundamental terms such as the Picard variety, polarization, and the field of moduli of polarized abelian varieties. However, our primary focus will be on the properties and behaviors of abelian varieties over $\mathbb{C}$. Additionally, we discuss the relationship between algebraic curves, their Jacobians, and abelian varieties, helping to provide a clearer understanding of the topic. Finally, combining the geometrical aspects with the number theoretical aspects from the previous sections, we will then explore what it means for an abelian variety to have complex multiplication.

1.5.1 Abelian varieties and polarizations

We begin with fundamental definitions related to abelian varieties, their homomorphisms, and dual varieties. Our discussion starts with abelian varieties over any field k. For our exploration, we mainly follow the works in [ST61], [Shi16], [Lan19], and [Liu02].

Abelian varieties and homomorphisms

Definition 1.60.
A *group variety* V over a field k is an algebraic variety together with a group structure such the operations $\circ : V \times V \to V$, $(a, b) \mapsto a \circ b$, and $\cdot^{-1} : V \to V$, $a \mapsto a^{-1}$ are rational and defined everywhere on V. If both V and the operations are defined over k, then the group variety is said to be *defined over* k. Furthermore, V is said to be *affine* or *projective* if it can be embedded into either an affine or projective space, respectively.

Example 1.61.
Now, to provide a more in-depth understanding of the given definition, we give some examples.

(a) A simple example of an algebraic variety that is not a group variety is the parabola given by the equation $y = x^2$ in $\mathbb{C}^2$. While it represents solutions to a polynomial equation, making it an algebraic variety, it does not have a group structure.

(b) Elliptic curves are algebraic varieties, but also come with a group structure thanks to a well-defined addition operation. Being non-singular, an elliptic curve can be embedded into projective space, making it a projective group variety.

(c) For a straightforward example of an affine group variety, consider the additive group $\mathbb{C}$ of complex numbers. The group operation $\circ$ is simply the standard addition of complex numbers, while the inverse $\cdot^{-1}$ corresponds to negation. This group variety exists over the field $\mathbb{C}$ and is affine, being naturally embedded into the affine space $\mathbb{C}$ via the identity map $z \mapsto z$. However, it does not have an embedding into a projective space.

Building on our understanding of group varieties, we introduce the following terminology and refer to [Shi16] as our primary reference.

Definition 1.62.
An *abelian variety* A is defined to be a projective non-singular group variety having a commutative group law. We use additive notation for the group law. A subvariety of an abelian variety A is called *abelian subvariety of* A, if it is a subgroup of A and A is said to be *simple* if the only abelian subvarieties are $\{0\}$ and A itself. We say a field k is a *field of definition* for an abelian variety A if A is definable over k.

Example 1.63.
By further examining our previous examples, we briefly present the distinction between group varieties and abelian varieties.

(a) Elliptic curves are projective group varieties and have a commutative group law. Therefore, they are abelian varieties.

(b) The additive group $\mathbb{C}$ of complex numbers, on the other hand, demonstrates a group variety that is not abelian. While it has a clear commutative group structure, it cannot be embedded into a projective space. Thus, the additive group $\mathbb{C}$ is a commutative affine group variety but not an abelian variety.

Continuing to follow [ST61] and [Shi16], we can now delve deeper into the structure of abelian varieties by considering homomorphisms.

Definition 1.64.
Let k be a field, and let A and B be abelian varieties defined over k. By a *homomorphism* of A into B, we define a rational mapping $\lambda : A \to B$ with

$$\lambda(P+Q) = \lambda(P) + \lambda(Q)$$

for all $P \in A$ and $Q \in B$. Such a homomorphism is called *endomorphism* if $A = B$.We denote by $\mathrm{Hom}(A, B)$ the set of all homomorphisms from A to B over any extension of k and define $\mathrm{End}(A) := \mathrm{Hom}(A, A)$.

The set $\mathrm{Hom}(A, B)$ forms a free $\mathbb{Z}$-module of finite rank. Each element in $\mathrm{Hom}(A, B)$ is defined over a separable algebraic extension of k. By extending the scalars to $\mathbb{Q}$, we can now define $\mathrm{Hom}_{\mathbb{Q}}(A, B) := \mathrm{Hom}(A, B) \otimes_{\mathbb{Z}} \mathbb{Q}$ such as $\mathrm{End}_{\mathbb{Q}}(A) := \mathrm{Hom}_{\mathbb{Q}}(A, A)$. We know that $\mathrm{End}_{\mathbb{Q}}(A)$ is an algebra over $\mathbb{Q}$.

Definition 1.65.
Let k be a field, and let A and B be abelian varieties defined over k. A surjective homomorphism $\lambda \in \mathrm{Hom}(A, B)$ is called *isogeny* if it has a finite kernel. The cardinality of the kernel is said to be the *degree* of λ. If such an isogeny exists between the two abelian varieties A and B, they are called *isogenous*.

The Picard variety and polarizations

Understanding the concepts of polarization and the dual space is essential when studying abelian varieties. We introduce these concepts following [ST61], [Shi16] and [Lan83]. For further details on equivalence classes of divisors we refer to [Lan19].

Definition 1.66.
Let A be an abelian variety over a field k with algebraic closure $\bar{k}$. A *divisor* D on A is a formal sum:

$$D = \sum_{P \in A(\bar{k})} n_P P,$$

where n_P are integers, and only a finite number of these are non-zero. We let $D_a(A)$ denote the group of divisors of A over $\bar{k}$, which are algebraically equivalent to 0 and $D_\ell(A)$ denotes the subgroup of all divisors which are linearly equivalent to 0. The *dual variety* (or *Picard variety*) A^* of A is an abelian variety isomorphic over $\bar{k}$ to

$$\mathrm{Pic}^0(A) := D_a(A)/D_\ell(A).$$

In order to introduce polarizations on abelian varieties following [Shi16], let X be a divisor of an abelian variety A over a field k. If we define X_a as the translation

of X by an element $a \in A$, then the mapping

$$\varphi_X : A \to A^*, \quad a \mapsto (X_a - X)'$$

is a homomorphism. The divisor X is called *non-degenerate* if φ_X is an isogeny. Two divisors X and Y on A satisfy $\varphi_X = \varphi_Y$ if and only if X is algebraically equivalent to Y. Let $\mathscr{C}(X)$ represent the set of divisors Y on A for which positive integers m and m_1 exist, such that mX and m_1Y are algebraically equivalent. When X is non-degenerate, $\mathscr{C}(X)$ corresponds to the isogeny $\varphi_{\mathscr{C}} = \varphi_X : A \to A^*$.

Definition 1.67.
Let A be an abelian variety over a field k, and let X be a non-degenerate divisor of A. Then $\mathscr{C} := \mathscr{C}(X)$, respectively $\varphi_{\mathscr{C}} := \varphi_X : A \to A^*$, is said to be a *polarization* on A. We say that a polarization on A is *principal* if φ is an isomorphism, which means that it has degree one. Moreover, we say that a pair (A, φ) (or $(A, \mathscr{C})$) is a *polarized abelian variety* over k, if a A is an abelian variety and φ is a fixed polarization on A, both defined over k.

The term *polarization* for abelian varieties was introduced by Weil during his discussion on abelian varieties with complex multiplication. He suggested an analogy to oriented manifolds in topology, as discussed in [Wei55]. Around the same period, Matsusaka expanded on this concept in [Mat58]. Both Weil's and Matsusaka's pioneering works on this topic are frequently cited, for example in Shimura's writings. The concept of polarization can be considered a generalization of the following well-known ideas related to elliptic curves, which is for example stated in [Sil09][Proposition 3.4, Chapter 3].

Example 1.68.
Let k be a field with an algebraic closure $\bar{k}$. Let E be an elliptic curve over k together with a point $\mathcal{O} \in E(\bar{k})$. Let $\mathrm{Pic}^0(E) := \mathrm{Pic}^0_{\bar{k}}(E)$ denote the Picard group of E. Then the following map is a bijection:

$$\begin{aligned} E(\bar{k}) &\longrightarrow \mathrm{Pic}^0(E) \\ P &\longmapsto [P] - [\mathcal{O}] \end{aligned}$$

Just as for elliptic curves, a polarization lets us view the Picard group $\mathrm{Pic}^0(A)$ of an abelian variety A as a geometric object. When the polarization is principal, the Picard group $\mathrm{Pic}^0(A)$ (or the dual variety A^*) can be identified with the polarized abelian variety A. Every abelian variety has a polarization over its field of definition, as outlined in [ST61][Proposition 11+12, Chapter 1].

Building on [Shi16], we will now discuss the concepts of the transpose and the Rosati involution for abelian varieties. These concepts are crucial for our later investigation of endomorphism rings of abelian varieties with complex multiplication.

Let A and B be abelian varieties over a field k. Let A^* and B^* represent their respective dual varieties. For a detailed elaboration, we refer the reader to [Shi16]. However, we give a short sketch of the idea. Given any $Z \in D_a(A)$, it corresponds to a point on A^*, represented as Z'. For a given homomorphism $\lambda \in \mathrm{Hom}(A, B)$, there exists a corresponding $\lambda^* \in \mathrm{Hom}(B^*, A^*)$ such that we have $\lambda^*(Z') = (\lambda^{-1}(Z))'$ whenever $\lambda^{-1}(Z)$ is defined for $Z \in D_a(A)$.

This establishes a map

$$\begin{aligned} \mathrm{Hom}(A, B) &\to \mathrm{Hom}(B^*, A^*) \\ \lambda &\mapsto \lambda^* \end{aligned}$$

which extends uniquely to an isomorphism

$$\cdot^t : \mathrm{Hom}_{\mathbb{Q}}(A, B) \to \mathrm{Hom}_{\mathbb{Q}}(B^*, A^*).$$

Definition 1.69.
Let k be a field, and let A such as B be abelian varieties over k. The unique extension $\cdot^t : \mathrm{Hom}_{\mathbb{Q}}(A, B) \to \mathrm{Hom}_{\mathbb{Q}}(B^*, A^*)$ of $\mathrm{Hom}(A, B) \to \mathrm{Hom}(B^*, A^*)$, $\lambda \mapsto \lambda^*$ is called *transpose* or *dual*.

Now, we may extend the term homomorphism to polarized abelian varieties and introduce the term Rosati involution.

Definition 1.70.
Let $(A, \mathscr{C}_A)$ and $(B, \mathscr{C}_B)$ be polarized abelian varieties over a field k. A homomorphism $\lambda \in \mathrm{Hom}(A, B)$ is called a *homomorphism from* $(A, \mathscr{C}_A)$ *to* $(B, \mathscr{C}_B)$ if

$$\lambda^t \circ \varphi_{\mathscr{C}_B} \circ \lambda = \varphi_{\mathscr{C}_A},$$

where λ^t denotes the transpose of λ.

Consider the case $A = B$ and $\mathscr{C}_A = \mathscr{C}_B$ with $\varphi : A \to A^*$. Then every $\lambda \in \mathrm{End}_{\mathbb{Q}}(A)$ has a transpose $\lambda^t \in \mathrm{End}_{\mathbb{Q}}(A^*)$ and the map $\lambda \mapsto \varphi^{-1} \circ \lambda^t \circ \varphi$ is an involution on $\mathrm{End}_{\mathbb{Q}}(A)$.

Definition 1.71.
Let k be field, and let $(A, \mathscr{C})$ be a polarized abelian variety with corresponding isogeny $\varphi : A \to A^*$. The map $\lambda \mapsto \varphi^{-1} \circ \lambda^t \circ \varphi$ is called *Rosati involution*.

In the context of abelian varieties with complex multiplication, which we will discuss later, the Rosati involution establishes a crucial link between polarizations and endomorphisms of the abelian variety. This involution acts as a conjugate transpose on the endomorphism algebra and, over the complex field $\mathbb{C}$, preserves the Riemann form induced by the polarization.

The field of moduli

The following construction follows [ST61], which we also refer to for further details. Consider a polarized abelian variety $(A, \mathscr{C})$ defined over a field k. For every isomorphism $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$, $(A^\sigma, \mathscr{C}^\sigma)$ is a polarized abelian variety. Based on [ST61][Theorem 2, Chapter 1], there exists a subfield k_0 of k such that $(A, \mathscr{C})$ is isomorphic to $(A^\sigma, \mathscr{C}^\sigma)$ if and only if $\sigma \in \mathrm{Gal}(k/k_0)$. Importantly, when the characteristic of k is zero, k_0 is uniquely determined, as outlined in [ST61][Proposition 14, Chapter 1].

Definition 1.72.
Let $(A, \mathscr{C})$ be a polarized abelian variety over a field k, and let k_0 be the subfield of k such that $(A, \mathscr{C})$ is isomorphic to $(A^\sigma, \mathscr{C}^\sigma)$ if and only if $\sigma \in \mathrm{Gal}(k/k_0)$. Then k_0 is called the *field of moduli* of $(A, \mathscr{C})$.

The field of moduli plays a foundational role in understanding isomorphism classes of polarized abelian varieties, and can be considered as the smallest field over which at least one polarized abelian variety in the isomorphism class can be defined.

1.5.2 Abelian varieties over $\mathbb{C}$

In this thesis, our main focus is on abelian varieties over $\mathbb{C}$. Firstly, we will see how they relate to complex tori and discuss Riemann forms. We will also show how theta functions let us connect polarizations on abelian varieties with Riemann forms on tori, and introduce period matrices. Most of what we discuss in this section comes from [Lan83][Chapter 3.4], [BL04], and [Spa94][Chapter 3]. At the end of this section, we will also take a brief look at theta characteristics using [Wen01b][Chapter 1.1.6]. These are important when we classify and construct models of hyperelliptic curves.

Complex tori and Riemann forms

It is well known that, as presented in [Sil09], elliptic curves over $\mathbb{C}$ are complex tori and that every torus of dimension one defines an elliptic curve. Moreover, every

abelian variety A over $\mathbb{C}$ is isomorphic to a torus $\mathbb{C}^g/\Lambda$ for some $g \in \mathbb{N}$ and lattice Λ in $\mathbb{C}^g$ via an analytic isomorphism $\theta : \mathbb{C}^g/\Lambda \longrightarrow A(\mathbb{C})$. The integer g is defined to be the *dimension* of A. However, if g is strictly greater than one, not every torus $\mathbb{C}^g/\Lambda$ arises from an abelian variety.

Definition 1.73.
A *(non-degenerated) Riemann form* E on a torus $\mathbb{C}^g/\Lambda$ with $g \in \mathbb{N}$ is an alternating (non-degenerated) form on $\mathbb{C}^g$ such that $E(v, w) \in \mathbb{Z}$ for all $v, w \in \Lambda$. A torus is said to be *polarizable* if it admits a Riemann form.

We receive the following crucial theorem, which can be found for example in [Mum99][Lecture 4].

Theorem 1.74.
Let g be a positive integer. A complex torus $\mathbb{C}^g/\Lambda$ with Λ being a lattice in $\mathbb{C}^g$ is isomorphic to an abelian variety A over $\mathbb{C}$ if and only if it is polarizable.

Theta functions

Next, we briefly look at how polarizations of abelian varieties over $\mathbb{C}$ relate to Riemann forms on complex tori. This correspondence will be important when we later talk about the construction of specific abelian varieties. We refer to [Lan83][Chapter 3.4] and [Spa94][Chapter 3] as our primary references.

Definition 1.75.
Let g be a positive integer and $\mathbb{C}^g/\Lambda$ be a complex torus, where Λ denotes a lattice in $\mathbb{C}^g$.

(a) A function $f : \mathbb{C}^g/\Lambda \to \mathbb{C}$ is said to be *holomorphic* if it is complex differentiable at every point of $\mathbb{C}^g/\Lambda$.

(b) A function $f : \mathbb{C}^g/\Lambda \to \mathbb{C} \cup \{\infty\}$ is termed *meromorphic* if it is holomorphic everywhere on $\mathbb{C}^g/\Lambda$ except possibly at a set of isolated points, where the function might not be defined or might take the value ∞.

(c) A meromorphic function f on $\mathbb{C}^g/\Lambda$ is said to be a *theta function* if there exists a $\mathbb{C}$-linear form L on $\mathbb{C}^g$ such that for all $u \in \Lambda$ it is

$$f(z + u) = f(z) \cdot e^{2\pi i(L(z,u)+c(u))}.$$

Let f be a theta function on a complex torus $\mathbb{C}^g/\Lambda$ with corresponding linear form L. Following [Spa94][Chapter 3], as $L(z, u_1 + u_2) = L(z, u_1) + L(z, u_2)$, we may extend L to a $\mathbb{R}$-bilinear function on $\mathbb{C}^g$. If f is holomorphic, we can define a

Riemann form on $\mathbb{C}^g/\Lambda$ via

$$E_f(u,v) := L(u,v) - L(v,u).$$

On the other hand, if E is a Riemann form on $\mathbb{C}^g/\Lambda$, there is always a holomorphic theta function f on $\mathbb{C}^g/\Lambda$ such that $E = E_f$.

The Riemann form E_f depends only on the divisor $X := (f)$ on $\mathbb{C}^g/\Lambda$, and two divisors X , Y on $\mathbb{C}^g/\Lambda$ are algebraically equivalent if and only if they correspond to the same Riemann form E.

Summarizing our considerations, for every polarization $\mathscr{C} = \mathscr{C}(X)$ on an abelian variety A over $\mathbb{C}$ we may associate a unique Riemann form E_X on the corresponding torus $\mathbb{C}^g/\Lambda$ via the theta function f_X. On the other hand, assuming that the torus $\mathbb{C}^g/\Lambda$ is polarizable, every Riemann form on $\mathbb{C}^g/\Lambda$ determines a holomorphic theta function f on $\mathbb{C}^g/\Lambda$ and an equivalence class of divisors, hence a polarization on A. Thus, we receive a one-to-one correspondence between Riemann forms and polarizations:

$$\mathscr{C} = \mathscr{C}_X \longleftrightarrow [X]_a \longleftrightarrow E = E_{\mathscr{C}} = E_X.$$

In the following we will see how this correspondence plays a role in categorizing isomorphism classes of polarized abelian varieties through the use of period matrices.

Period matrices and the Siegel upper half-space

Now let $(A, \mathscr{C})$ be a polarized abelian variety of dimension g over $\mathbb{C}$ such that $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ for some torus $\mathbb{C}^g/\Lambda$, and let E be the Riemann form corresponding to the polarization $\mathscr{C}$. We follow [Spa94][Chapter 3] and [Str10][Chapter 2.4]. There exists a basis $(b_1 , \dots , b_{2g})$ of Λ with

$$(E(b_i, b_j))_{i,j} = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix},$$

where $D = (d_{i\,j})_{i,j} \in \mathbb{Z}_+^{g\times g}$ is a diagonal matrix with positive integer entries such that $d_{11} \mid \cdots \mid d_{gg}$. The polarization $\mathscr{C}$ of A is principal if and only if $D = E_g$. This is equivalent to say that $\varphi_{\mathscr{C}}$ induces an isomorphism between A and the dual variety A^* of A.

Definition 1.76.
Let $(A, \mathscr{C})$ be a polarized abelian variety of dimension g over $\mathbb{C}$ such that A is isomorphic over $\mathbb{C}$ to a complex torus $\mathbb{C}^g/\Lambda$, and let E be the Riemann form corresponding to the polarization $\mathscr{C}$. A basis $(b_1, \ldots, b_{2g})$ of Λ with

$$(E(b_i, b_j))_{i,j} = \begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix},$$

where $D = (d_{i\,j})_{i,j} \in \mathbb{Z}_+^{g\times g}$ is a diagonal matrix with positive integer entries such that $d_{11} \mid \cdots \mid d_{gg}$ is called *symplectic with respect to* E.

Moreover, if we define $\Omega_1 := (b_1, \cdots, b_g)$ and $\Omega_2 := (b_{g+1}, \cdots, b_{2g})$, then $\mathscr{C}$ is a principal polarization of A if and only if $\Omega := \Omega_2^{-1}\Omega_1$ is symmetric and has positive definite imaginary part ($\mathrm{Im}(\Omega) > 0$).

Definition 1.77.
Let g be a positive integer. We define the *g-dimensional Siegel upper half-space* to be

$$\mathbb{H}_g := \{\Omega \in \mathrm{GL}(g, \mathbb{C}) \mid \Omega^T = \Omega \text{ and } \mathrm{Im}(\Omega) > 0\}$$

and call the elements of $\mathbb{H}_g$ *period matrices*.

There is an action of the *symplectic group*, defined to be

$$\mathrm{SP}_{2g}(\mathbb{Z}) = \left\{ M \in \mathrm{GL}(2g, \mathbb{Z}) \mid M^T \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix} M = \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix} \right\},$$

on the Siegel upper half-space via

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \Omega = (A\Omega + B)(C\Omega + D)^{-1}.$$

Definition 1.78.
Let g be a positive integer and $\mathbb{H}_g$ be the g-dimensional Siegel upper half-space. The set of orbits under the action of $\mathrm{SP}_{2g}(\mathbb{Z})$ on $\mathbb{H}_g$ is defined to be the *g-dimensional moduli space*.

The moduli space in a one-to-one correspondence to the set of isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$.

Theta characteristics

We now introduce theta characteristics, which are, for example, used in the construction of Rosenhain models and in the classification of hyperelliptic curves. For more information, see [Wen01b]. For a given positive integer g, we define the *Riemann theta function* to be

$$\begin{aligned}\Theta : \mathbb{C}^g \times \mathbb{H}_g &\longrightarrow \mathbb{C} \\ (z, \Omega) &\longmapsto \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i \left(n^T \Omega n + 2n^T z\right)\right).\end{aligned}$$

Such a function is always holomorphic and $\Theta(z, \Omega) = \Theta(-z, \Omega)$. If we fix a period matrix $\Omega \in \mathbb{H}_g$ of a principally polarized torus $\mathbb{C}^g/\Lambda$, we receive a function from $\mathbb{C}^g$ into $\mathbb{C}$ and we may define a *Riemann theta divisor* of Ω:

$$\Theta^{(\Omega)} := \{z + \Lambda \mid z \in \mathbb{C}^g \text{ and } \Theta(z, \Omega) = 0\}.$$

One can show that two period matrices $\Omega, \Omega_1 \in \mathbb{H}_g$ within in the same orbit do not necessarily induce the same theta divisor. However, the theta divisors are translations of each other in the sense that $\Theta^{(\Omega_1)} = \Theta_a^{(\Omega)}$ for some $a \in \Omega\left(\frac{1}{2}\mathbb{Z}^g\right) + \frac{1}{2}\mathbb{Z}^g$. This motivates the following definition.

Definition 1.79.
Let g be a positive integer, and let $\delta, \varepsilon \in (\mathbb{Z}/2\mathbb{Z})^g$. A *theta characteristic* is a function

$$\begin{aligned}\Theta[\delta, \varepsilon] : \mathbb{C}^g \times \mathbb{H}_g &\longrightarrow \mathbb{C} \\ (z, \Omega) &\longmapsto \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i \left((n + \frac{1}{2}\delta)^T \Omega (n + \frac{1}{2}\delta) + 2(n + \frac{1}{2}\delta)^T (z + \frac{1}{2}\varepsilon)\right)\right).\end{aligned}$$

Observe that $\Theta[\delta, \varepsilon](-z, \Omega) = (-1)^{\delta^T \varepsilon} \Theta[\delta, \varepsilon](z, \Omega)$. We introduce the concept of theta null values, which are determined by evaluating theta characteristics at zero.

Definition 1.80.
Let g be a positive integer, let $\delta, \varepsilon \in (\mathbb{Z}/2\mathbb{Z})^g$, and let $\Theta[\delta, \varepsilon]$ be a theta characteristic. The mapping

$$\begin{aligned}\Theta[\delta, \varepsilon] : \mathbb{H}_g &\longrightarrow \mathbb{C} \\ \Omega &\longmapsto \Theta[\delta, \varepsilon](0, \Omega)\end{aligned}$$

is called a *theta null value* or *theta constant*. A theta null value is said to be *even* if $\delta^T \varepsilon$ is even, and *odd* otherwise.

Note that, for $g \in \mathbb{N}$ and vectors $\delta, \varepsilon \in (\mathbb{Z}/2\mathbb{Z})^g$, if $\delta^T\varepsilon \equiv 1 \equiv \delta_1^T\varepsilon_1$, then $\Theta[\delta,\varepsilon](0,\Omega) = 0$ if and only if $\Theta[\delta_1,\varepsilon_1](0,\Omega) = 0$. Building on insights from [Wen01b], there are always $2^{g-1}(2^g+1)$ odd and $2^{g-1}(2^g-1)$ even theta null values. For instance, when $g = 2$, there are 10 even theta constants, and for $g = 3$, there are 36 odd theta constants.

1.5.3 Curves and Jacobians

Based on [Liu02] and [BL04], we briefly introduce the concepts of curves and their Jacobians.

Definition 1.81.
An *(algebraic) curve* over a field k is defined to be an algebraic variety whose irreducible components have dimension one.

In this thesis, we always assume that a curve is smooth, geometrically connected, and projective. We state that for every curve C over a field k, there exists a certain abelian variety J of dimension $g \in \mathbb{N}$ over k, such that $J(L)$ is isomorphic to Picard group $\mathrm{Pic}^0(C_L)$ of C for every field extension $L \supseteq k$. While we do not dive deep into the construction details, we refer the reader to [Liu02][Chapter 7.4] or [BL04][Chapter 11.1] for a comprehensive overview.

Definition 1.82.
Let C be a curve over a field k. The abelian variety J over k that satisfies

$$J(L) \cong \mathrm{Pic}^0(C_L)$$

for every field extension $L \supseteq k$ is said to be the *Jacobian of* C.

The *genus* of the curve C equals the dimension of its corresponding Jacobian J and we can think of the elements of J as equivalence classes of g-tuples of points on C. Jacobians come with a principal polarization, relating curves to principally polarized abelian varieties (see [BL04][Proposition 11.1.2]). While the Jacobian of an elliptic curve is isomorphic to the curve itself, this is not the case for curves of genus $g \geq 2$.

Definition 1.83.
Let C be a curve of a field k and J be its Jacobian. We say that C is *simple*, if J is simple as an abelian variety.

Over the complex numbers, we can state the following crucial theorems about Jacobians over $\mathbb{C}$. The following is known as *Torellis theorem* and can be found in [BL04][Theorem 11.1.7] or [Mum99][Lecture IV].

Theorem 1.84.
Let C and C_1 be curves over $\mathbb{C}$, and let $\mathcal{P} = (J_C, \mathscr{C})$ and $\mathcal{P}_1 = (J_{C_1}, \mathscr{C}_1)$ be their principally polarized Jacobians, respectively. If $\mathcal{P}$ and $\mathcal{P}_1$ are isomorphic, then C and C_1 are isomorphic.

Fortunately, we can characterize simple principally polarized abelian varieties of low dimension as Jacobians of curves, as summarized in [BL04][Corollary 11.8.2] and originally proved by Weil ($g = 2$) and Matsusaka-Ran ($g = 3$).

Theorem 1.85.
Every simple principally polarized abelian variety over $\mathbb{C}$ of dimension $g \in \{1, 2, 3\}$ is the Jacobian of a simple curve of genus g.

We have observed a deep connection between simple curves, their Jacobians, and simple principally polarized abelian varieties. Specifically, the isomorphism classes of simple curves and these structures are closely linked. To be precise, over the complex numbers $\mathbb{C}$, we can connect each isomorphism class of simple principally polarized abelian varieties with a dimension g to an isomorphism class of simple curves with the same genus g.

1.5.4 Abelian varieties with complex multiplication

In this section, following [ST61] and [Lan83], we discuss the concept of complex multiplication of abelian varieties, connecting the number theoretical and the geometrical aspects.

Definition 1.86.
Let A be an abelian variety of dimension g over a field k. If there is an embedding $\iota : F \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A) := \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ from a CM field F of degree $2g$ into the endomorphism algebra of A, then A is said to have *complex multiplication (CM) by* F. To be precise, there exists an order $R \subseteq \mathcal{O}_F$ of F such that

$$R = \iota^{-1}(\mathrm{End}(A) \cap \iota(F)) .$$

We say that A *has complex multiplication (CM) by* R. In addition, we say that a curve C over k has complex multiplication by R if its Jacobian has complex multiplication by R.

Now, let A be an abelian variety of dimension g over a field k with complex multiplication by F. Then there exists a simple abelian variety B such that A is isogenous to the product $B \times \cdots \times B$. Let K be the center of $\mathrm{End}_{\mathbb{Q}}(B)$, then K is a subfield of F. Whenever the characteristic of k is equal to zero, then K is a CM field isomorphic to $\mathrm{End}_{\mathbb{Q}}(B)$. Furthermore, (A, ι) is said to be defined over k, if k is a field of definition of A and every element of $\iota(R)$ is defined over k.

Definition 1.87.
Let (A, ι) and (A', ι') be abelian varieties with CM by F. We say that a homomorphism $\lambda : A \to A'$ is a *homomorphism from* (A, ι) *to* (A', ι'), if $\lambda\, \iota(\alpha) = \iota'(\alpha)\, \lambda$ for every $\alpha \in F$.

Consider an abelian variety (A, ι) of dimension g over $\mathbb{C}$ with CM by a CM field F of degree $2g$ over $\mathbb{Q}$. Let $\mathrm{Tgt}_0(A)$ denote the tangent space of A at the point zero, which is a g-dimensional $\mathbb{C}$-vector space. According to [Lan83][Chapter 1.4], there exists a CM type Φ of F consisting of embeddings $\phi : F \hookrightarrow \mathbb{C}$ where the representation of F on $\mathrm{End}(\mathrm{Tgt}_0(A))$ via ι is equivalent to $\oplus_{\phi \in \Phi} \phi$. This CM type Φ is uniquely defined by both A and ι.

Definition 1.88.
Let (A, ι) be an abelian variety of dimension g over $\mathbb{C}$ with CM by the CM field F. Let Φ be the CM type of F such that the representation of F on $\mathrm{End}(\mathrm{Tgt}_0(A))$ via ι is equivalent to $\oplus_{\phi \in \Phi} \phi$. The tuple (A, ι) is said to be an *abelian variety of type* (F, Φ).

The next proposition, presented in [Shi16][Chapter 8.2], links the term simple of an abelian variety on the geometric side with the term primitive of a CM type on the number theoretical side.

Proposition 1.89.
Let (F, Φ) be a CM type. An abelian variety (A, ι) over $\mathbb{C}$ of type (F, Φ) is simple if and only if Φ is primitive.

By including polarization, we introduce one more definition.

Definition 1.90.
Let (F, Φ) be a CM type. A triple $(A, \iota, \mathscr{C})$ is said to be a *polarized abelian variety of type* (F, Φ) if (A, ι) is an abelian variety over $\mathbb{C}$ of type (F, Φ) and $\mathscr{C}$ is a polarization of A. Two polarized abelian varieties $(A, \iota, \mathscr{C})$ and $(A_1, \iota_1, \mathscr{C}_1)$ of the same type (F, Φ) are called *isomorphic*, if there exists an isomorphism from (A, ι) to (A_1, ι_1), which maps $\mathscr{C}$ to $\mathscr{C}_1$.

Chapter 2

Orders in cubic number fields

In this chapter, we delve into orders in cubic number fields and provide concrete representations for both Gorenstein and non-Gorenstein orders. These orders will be fundamental in following discussions on the existence of certain simple CM curves of genus 3. Specifically, in order to determine the index of the endomorphism rings of the Jacobians of these curves, which are orders in sextic CM fields K, we need to ensure their reductions to the totally real cubic subfield K_0 of K are of a particular type. Gorenstein orders will be one of the main examples of these orders in cubic number fields, which justifies a detailed investigation of these objects. The opening section introduces orders in cubic number fields and outlines conditions on the $\mathbb{Z}$-bases of orders. The following sections provide detailed descriptions of Gorenstein and non-Gorenstein orders.

2.1 Representation of orders in cubic number fields

Throughout this section, let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle f \rangle$ be a cubic number field with monic irreducible polynomial $f \in \mathbb{Z}[x]$, and let $\beta \in \mathcal{O}_L$. Firstly, every order $S \subseteq \mathcal{O}_L$ is a lattice and a ring with field of fractions L. Thus, it contains the multiplicative unit $1 \in L$ and there exists a $\mathbb{Z}$-basis $(1, \omega_1, \omega_2)$ of $\mathcal{O}_L$ as a lattice for some integral $\omega_1, \omega_2 \in L$. In other words, we have

$$\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}},$$

where $\langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$ denotes the $\mathbb{Z}$-module contained in L generated by $1, \omega_1$ and ω_2. Since S is a subset of $\mathcal{O}_L$, a $\mathbb{Z}$-basis (s_0, s_1, s_2) of S can then be derived by multiplying the fixed $\mathbb{Z}$-basis of $\mathcal{O}_L$ with a transformation matrix U in Hermite normal form. Again, since $\mathbb{Z} \subseteq S$, we may assume $s_0 = 1$ such that there are

integers $a, c \in \mathbb{N}$ and $b \in \{0, \dots, a-1\}$ with

$$\begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix} = \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & b & c \end{pmatrix}}_{U} \begin{pmatrix} 1 \\ \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} 1 \\ a\,\omega_1 \\ b\,\omega_1 + c\,\omega_2 \end{pmatrix}.$$

As a consequence, without loss of generality, we assume that every suborder S of $\mathcal{O}_L$ can be described as a lattice via $S = \langle 1, a\,\omega_1, b\,\omega_1 + c\,\omega_2 \rangle_{\mathbb{Z}}$.

Note that while every combination of such a, b, c defines a sublattice of $\mathcal{O}_L$, only a few combinations actually define rings and, consequently, suborders of $\mathcal{O}_L$. For this to hold, S must be multiplicatively closed, which implies that

$$S^2 = \langle 1, a\,\omega_1, b\,\omega_1 + c\,\omega_2, a^2\,\omega_1^2, a\,\omega_1\,(b\,\omega_1 + c\,\omega_2), (b\,\omega_1 + c\,\omega_2)^2 \rangle_{\mathbb{Z}} \subseteq S.$$

The following theorem provides conditions on a, b, c to ensure this property. Given that $\mathcal{O}_L$ is multiplicatively closed, there exist integers $\lambda_{ij} \in \mathbb{Z}$ for $1 \leq i \leq 3$ and $0 \leq j \leq 2$ such that

$$\begin{aligned} \omega_1^2 &= \lambda_{10} + \lambda_{11}\,\omega_1 + \lambda_{12}\,\omega_2\,, \\ \omega_2^2 &= \lambda_{20} + \lambda_{21}\,\omega_1 + \lambda_{22}\,\omega_2 \quad \text{and} \\ \omega_1\,\omega_2 &= \lambda_{30} + \lambda_{31}\,\omega_1 + \lambda_{32}\,\omega_2\,. \end{aligned}$$

Theorem 2.1.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle f \rangle$ be a cubic number field with monic irreducible polynomial $f \in \mathbb{Z}[x]$ and $\beta \in \mathcal{O}_L$. Let $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$ for some integral $\omega_1, \omega_2 \in L$ and let $\lambda_{ij} \in \mathbb{Z}$ with $1 \leq i \leq 3$ and $0 \leq j \leq 2$ such that

$$\begin{aligned} \omega_1^2 &= \lambda_{10} + \lambda_{11}\,\omega_1 + \lambda_{12}\,\omega_2\,, \\ \omega_2^2 &= \lambda_{20} + \lambda_{21}\,\omega_1 + \lambda_{22}\,\omega_2 \quad \textit{and} \\ \omega_1\,\omega_2 &= \lambda_{30} + \lambda_{31}\,\omega_1 + \lambda_{32}\,\omega_2\,. \end{aligned}$$

Then $S = \langle 1, a\,\omega_1, b\,\omega_1 + c\,\omega_2 \rangle_{\mathbb{Z}}$ is an order in L if and only if the following conditions hold:

(a) $c \mid a^2\,\lambda_{12}$ *and* $c \mid a\,b\,\lambda_{12}$,

(b) $c \mid (a\,b\,\lambda_{12} + a\,c\,\lambda_{32})$ *and* $c \mid (b^2\,\lambda_{12} + b\,c\,\lambda_{32})$,

(c) $c \mid (b^2\,\lambda_{12} + 2\,b\,c\,\lambda_{32} + c^2\,\lambda_{22})$ *and*
$a \mid \left(b^2\,\lambda_{11} + 2\,b\,c\,\lambda_{31} + c^2\,\lambda_{21} - b\,\frac{b^2\,\lambda_{12} + 2\,b\,c\,\lambda_{32} + c^2\,\lambda_{22}}{c}\right)$.

Proof. In order to show that S is multiplicatively closed, we have to show that

$$S^2 = \langle 1, a\,\omega_1, b\,\omega_1 + c\,\omega_2, a^2\,\omega_1^2, a\,\omega_1\,(b\,\omega_1 + c\,\omega_2), (b\,\omega_1 + c\,\omega_2)^2 \rangle_{\mathbb{Z}} \subseteq S.$$

Given that these elements precisely generate S, the first three generators of S^2 belong to S. We now determine conditions on a, b, c ensuring that the next three generators are also contained in S.
Starting with the first remaining generator, we have

$$\begin{aligned} a^2\,\omega_1^2 &= a^2\,(\lambda_{10} + \lambda_{11}\,\omega_1 + \lambda_{12}\,\omega_2) \\ &= a^2\,\lambda_{10} + a^2\lambda_{11}\,\omega_1 + a^2\,\lambda_{12}\,\omega_2\,. \end{aligned}$$

We have $a^2\,\lambda_{10} \in S$ and receive that $a^2\,\omega_1^2 \in S$ if and only if

$$a^2\lambda_{11}\,\omega_1 + a^2\,\lambda_{12}\,\omega_2 \in S\,.$$

This is the case if and only if there exist $\mu_1, \mu_2 \in \mathbb{Z}$ with

$$a^2\lambda_{11}\,\omega_1 + a^2\,\lambda_{12}\,\omega_2 = \mu_1\,a\,\omega_1 + \mu_2\,(b\,\omega_1 + c\,\omega_2)\,.$$

Equating coefficients results in the following system of linear equations over $\mathbb{Z}$:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} \mu_1 \\ \mu_2 \end{pmatrix} = \begin{pmatrix} a^2\lambda_{11} \\ a^2\lambda_{12} \end{pmatrix}\,.$$

Now $a^2\,\omega_1^2 \in S$ if and only if this system of linear equations has a solution $\begin{pmatrix} \mu_1 & \mu_2 \end{pmatrix}^T$ over $\mathbb{Z}$. On the one hand, we receive the condition

$$c \mid a^2\,\lambda_{12}\,. \tag{2.1}$$

If condition (2.1) holds, then exists $\mu_2 \in \mathbb{Z}$ with $\mu_2\,c = a^2\,\lambda_{12}$. Now, on the other hand, the second condition becomes

$$a \mid (a^2\,\lambda_{11} - b\,\mu_2) = \left(a^2\,\lambda_{11} - \frac{a^2\,b\,\lambda_{12}}{c}\right)\,,$$

which is equivalent to

$$c \mid a\,b\,\lambda_{12}\,. \tag{2.2}$$

We follow the same argument for the other generators. For the second remaining

generator of S^2, we have

$$\begin{aligned} a\,\omega_1\,(b\,\omega_1 + c\,\omega_2) &= a\,b\,\omega_1^2 + a\,c\,\omega_1\,\omega_2 \\ &= a\,b(\lambda_{10} + \lambda_{11}\,\omega_1 + \lambda_{12}\,\omega_2) + a\,c\,(\lambda_{30} + \lambda_{31}\,\omega_1 + \lambda_{32}\,\omega_2) \\ &= (a\,b\,\lambda_{10} + a\,c\,\lambda_{30}) + (a\,b\,\lambda_{11} + a\,c\,\lambda_{31})\,\omega_1 + (a\,b\,\lambda_{12} + a\,c\,\lambda_{32})\,\omega_2\,. \end{aligned}$$

Again, $a\,\omega_1\,(b\,\omega_1 + c\,\omega_2) \in S$ if and only if

$$(a\,b\,\lambda_{11} + a\,c\,\lambda_{31})\,\omega_1 + (a\,b\,\lambda_{12} + a\,c\,\lambda_{32})\,\omega_2 \in S\,.$$

This is the case if and only if there exist $\eta_1, \eta_2 \in \mathbb{Z}$ such that

$$(a\,b\,\lambda_{11} + a\,c\,\lambda_{31})\,\omega_1 + (a\,b\,\lambda_{12} + a\,c\,\lambda_{32})\,\omega_2 = \eta_1\,a\,\omega_1 + \eta_2\,(b\,\omega_1 + c\,\omega_2)\,.$$

Equating coefficients gives the following system of linear equations over $\mathbb{Z}$:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} \eta_1 \\ \eta_2 \end{pmatrix} = \begin{pmatrix} a\,b\,\lambda_{11} + a\,c\,\lambda_{31} \\ a\,b\,\lambda_{12} + a\,c\,\lambda_{32} \end{pmatrix}\,.$$

Now $a\,\omega_1\,(b\,\omega_1 + c\,\omega_2) \in S$ if and only if this system of linear equations has a solution over $\mathbb{Z}$. Hence, on the one hand, we receive the condition

$$c \mid (a\,b\,\lambda_{12} + a\,c\,\lambda_{32})\,. \tag{2.3}$$

Assuming that condition (2.3) holds, there exists a $\eta_2 \in \mathbb{Z}$ with $\eta_2\,c = a\,b\,\lambda_{12} + a\,c\,\lambda_{32}$. Then, on the other hand, the second condition becomes

$$a \mid (a\,b\,\lambda_{11} + a\,c\,\lambda_{31} - b\,\eta_2)\,.$$

Again, substituting η_2, this condition is equivalent to

$$c \mid (b^2\,\lambda_{12} + b\,c\,\lambda_{32})\,. \tag{2.4}$$

It remains to find an analogous condition for the last generator of S^2. We have

$$\begin{aligned} (b\,\omega_1 + c\,\omega_2)^2 &= b^2\,\omega_1^2 + 2\,b\,c\,\omega_1\,\omega_2 + c^2\,\omega_2^2 \\ &= b^2\,(\lambda_{10} + \lambda_{11}\,\omega_1 + \lambda_{12}\,\omega_2) + 2\,b\,c(\lambda_{30} + \lambda_{31}\,\omega_1 + \lambda_{32}\,\omega_2) \\ &\quad + c^2\,(\lambda_{20} + \lambda_{21}\,\omega_1 + \lambda_{22}\,\omega_2)\,. \end{aligned}$$

For this generator, $(b\,\omega_1 + c\,\omega_2)^2 \in S$ if and only if there exist $\gamma_1, \gamma_2 \in \mathbb{Z}$ such that

$$(b^2\,\lambda_{11}+2\,b\,c\,\lambda_{31}+c^2\,\lambda_{21})\,\omega_1+(b^2\,\lambda_{12}+2\,b\,c\,\lambda_{32}+c^2\,\lambda_{22})\,\omega_2 = \gamma_1\,a\,\omega_1+\gamma_2\,(b\,\omega_1+c\,\omega_2)\,.$$

Equating coefficients, we obtain the next system of linear equations over $\mathbb{Z}$:

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \end{pmatrix} = \begin{pmatrix} b^2\,\lambda_{11} + 2\,b\,c\,\lambda_{31} + c^2\,\lambda_{21} \\ b^2\,\lambda_{12} + 2\,b\,c\,\lambda_{32} + c^2\,\lambda_{22} \end{pmatrix}\,.$$

Now, on the one hand, we obtain the condition

$$c \mid (b^2\,\lambda_{12} + 2\,b\,c\,\lambda_{32} + c^2\,\lambda_{22})\,. \tag{2.5}$$

Hence, there exists a $\gamma_2 \in \mathbb{Z}$ satisfying $\gamma_2\,c = b^2\,\lambda_{12} + 2\,b\,c\,\lambda_{32} + c^2\,\lambda_{22}$. Then, on the other hand, we have the following condition

$$a \mid (b^2\,\lambda_{11} + 2\,b\,c\,\lambda_{31} + c^2\,\lambda_{21} - b\,\gamma_2)\,.$$

Substituting γ_2 yields

$$a \mid \left(b^2\,\lambda_{11} + 2\,b\,c\,\lambda_{31} + c^2\,\lambda_{21} - b\,\frac{b^2\,\lambda_{12} + 2\,b\,c\,\lambda_{32} + c^2\,\lambda_{22}}{c}\right)\,. \tag{2.6}$$

□

This general description of the $\mathbb{Z}$-bases of orders $S \subseteq \mathcal{O}_L$ as a lattice still allows many different choices of the parameters $a, b, c \in \mathbb{N}$. In what follows, we want to give a more explicit representation for $\mathbb{Z}$-bases of Gorenstein orders, which is only possible if we add further constrains. We focus on orders in cubic number fields with diagonal transformation matrix U, meaning that $b = 0$. Those orders are called *diagonal*. Focusing on diagonal orders allows us to get a clear view on the structure of $\mathbb{Z}$-bases of those orders in cubic number field. Setting $b = 0$ into Theorem 2.1 directly delivers the following corollary.

Corollary 2.2.
Let L be a cubic number field with maximal order $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$. Let $\lambda_{ij} \in \mathbb{Z}$ with $1 \leq i \leq 2$ and $0 \leq j \leq 2$ such that

$$\omega_1^2 = \lambda_{10} + \lambda_{11}\,\omega_1 + \lambda_{12}\,\omega_2 \quad \textit{and}$$
$$\omega_2^2 = \lambda_{20} + \lambda_{21}\,\omega_1 + \lambda_{22}\,\omega_2\,.$$

A sublattice $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ of $\mathcal{O}_L$ with $a, c > 0$ is an order in L if and only if

$$a \mid \lambda_{21}\,c^2 \quad \textit{and} \quad c \mid \lambda_{12}\,a^2\,.$$

Recall that the parameters λ_{21} and λ_{12} depend only on the cubic number field

$$L = \mathbb{Q}(\beta) = {}^{\mathbb{Q}[x]}\!/_{\langle f \rangle},$$

where $f = x^3 + \alpha_2\,x^2 + \alpha_1\,x + \alpha_0 \in \mathbb{Z}[x]$ is irreducible. Especially, these parameters depend on the $\mathbb{Z}$-basis of the ring of integers $\mathcal{O}_L$. Whenever $\mathcal{O}_L$ is monogenic, meaning that $\omega_1 = \beta$ and $\omega_2 = \beta^2$, we receive the following corollary.

Corollary 2.3.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle f \rangle$ with irreducible $f = x^3 + \alpha_2\,x^2 + \alpha_1\,x + \alpha_0 \in \mathbb{Z}[x]$ be a cubic number field with a monogenic ring of integers $\mathcal{O}_L = \langle 1, \beta, \beta^2 \rangle_{\mathbb{Z}}$. Then a sublattice $S = \langle 1, a\,\beta, c\,\beta^2 \rangle_{\mathbb{Z}}$ of $\mathcal{O}_L$ is an order in L if and only if $a \mid (\alpha_2^2\,\alpha_1 - \alpha_0)\,c^2$ and $c \mid a^2$.

Proof. In the notation of Corollary 2.2, We have $\omega_1^2 = \omega_2$ and $\lambda_{12} = 1$. On the other hand, applying that $f(\beta) = 0$, we have

$$\begin{aligned}
\omega_2^2 = (\beta^2)^2 = \beta^3\,\beta &= -(\alpha_0 + \alpha_1\,\beta + \alpha_2^2\,\beta^2)\,\beta \\
&= -\alpha_0\,\beta - \alpha_1\,\beta^2 - \alpha_2^2\,\beta^3 \\
&= -\alpha_0\,\beta - \alpha_1\,\beta^2 - \alpha_2^2\,(-(\alpha_0 + \alpha_1\,\beta + \alpha_2^2\,\beta^2)) \\
&= \alpha_2^2\,\alpha_0 + (\alpha_2^2\,\alpha_1 - \alpha_0)\beta + (\alpha_2^4 - \alpha_1)\,\beta^2 \\
&= \alpha_2^2\,\alpha_0 + (\alpha_2^2\,\alpha_1 - \alpha_0)\,\omega_1 + (\alpha_2^4 - \alpha_1)\,\omega_2\,.
\end{aligned}$$

As a consequence, $\lambda_{21} = \alpha_2^2\,\alpha_1 - \alpha_0$. Substituting λ_{12} and λ_{21} into Corollary 2.2 proves the claim. □

We now present a list of examples of cubic number fields with their specific parameters λ_{21} and λ_{12} (see Table 2.1 below). In following chapters, we will consider a specific list of sextic CM fields. These fields appear as the CM fields of specific principally polarized abelian varieties with complex multiplication. The first eleven

cubic fields listed in Table 2.1 are totally real and serve as the cubic subfields of these sextic CM fields. The final five fields, in contrast, are randomly selected cubic number fields that are not totally real.

We denote $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle f \rangle$, where f is an irreducible monic polynomial defined as $f = x^3 + \alpha_2\, x^2 + \alpha_1\, x + \alpha_0 \in \mathbb{Z}[x]$. The coefficients of f are represented by the tuple $[\alpha_0, \alpha_1, \alpha_2]$. Additionally, we define $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$. With the above-mentioned considerations, it becomes straightforward to calculate both λ_{21} and λ_{12}, thus, all diagonal orders in L up to an arbitrary bound on the index.

Table 2.1: Examples of parameters λ_{21} and λ_{12}

No.	f	monogenic	ω_1	ω_2	λ_{21}	λ_{12}
1	$[-1,-3,0]$	yes	β	β^2	1	1
2	$[-1,-2,-1]$	yes	β	β^2	1	1
3	$[1,-5,2]$	yes	β	β^2	11	1
4	$[1,-4,1]$	yes	β	β^2	5	1
5	$[1,-9,6]$	yes	β	β^2	55	1
6	$[8,-14,1]$	no	β	$\frac{\beta+\beta^2}{2}$	2	2
7	$[-8,-10,1]$	no	β	$\frac{\beta+\beta^2}{2}$	2	2
8	$[8,-18,3]$	no	β	$\frac{\beta+\beta^2}{2}$	12	2
9	$[-27,-15,4]$	no	β	$\frac{\beta+\beta^2}{3}$	3	3
10	$[-27,-21,2]$	no	β	$\frac{2\beta+\beta^2}{3}$	3	3
11	$[-64,-36,3]$	no	β	$\frac{\beta+\beta^2}{4}$	4	4
12	$[-3,1,-1]$	yes	β	β^2	2	1
13	$[-7,0,0]$	yes	β	β^2	7	1
14	$[26,-12,-1]$	yes	β	β^2	14	1
15	$[-104,-16,-1]$	no	β	$\frac{\beta+\beta^2}{2}$	33	2
16	$[12,4,-1]$	no	β	$\frac{\beta+\beta^2}{2}$	6	2

2.2 Diagonal Gorenstein orders in cubic number fields

Based on the description of diagonal orders from the previous section, our focus now shifts to Gorenstein orders in cubic number fields. In the literature, only very few classes of Gorenstein orders in cubic number fields are documented. For a detailed overview, we refer to [JT15]. In our study, we performed a detailed investigation on Gorenstein orders in the cubic number fields L listed in Table 2.1. We computed all diagonal orders $S \subseteq \mathcal{O}_L$ up to an index of $[\,\mathcal{O}_L : S\,] \leq 10^5$ and observed a specific structure whenever S is Gorenstein, as presented in the following theorem. This structure not only aligns with the known classes of Gorenstein orders in cubic number fields, as described in [JT15][Example 7.2], but also produces numerous additional Gorenstein orders. Our findings offer valuable insights into the structure of $\mathbb{Z}$-bases of Gorenstein orders in these fields.

Theorem 2.4.
Let L be a cubic number field from Table 2.1 with ring of integers $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_\mathbb{Z}$. Let $\lambda_{21}, \lambda_{12} \geq 1$ be integers such that $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_\mathbb{Z}$ is an order if and only if $a \mid \lambda_{21}\,c^2$ and $c \mid \lambda_{12}\,a^2$. Let $D_1 \subseteq \mathbb{N}$ and $D_2 \subseteq \mathbb{N}$ be the set of divisors of λ_{21} and λ_{12}, respectively.

(a) *Let $x, y \geq 1$ with $\gcd(x, y) = 1$. For all $r \in D_1$ and $s \in D_2$ such that*

(i) $1 = \gcd(x, s) = \gcd(r, y) = \gcd(r, s)$,
(ii) $\forall\, p \mid x$ *prime*: $v_p(r) = v_p(\lambda_{21})$,
(iii) $\forall\, p \mid y$ *prime*: $v_p(s) = v_p(\lambda_{12})$ *and*
(iv) $(r\,x^2\,y)\,(s\,x\,y^2) \leq 10^5$,

the lattice $S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2 \rangle_\mathbb{Z}$ is an order of L which is Gorenstein.

(b) *If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_\mathbb{Z}$ is a Gorenstein order in L with $[\,\mathcal{O}_L : S\,] \leq 10^5$, then exist $x, y \geq 1$, $r \in D_1$ and $s \in D_2$ with*

(i) $1 = \gcd(x, y) = \gcd(x, s) = \gcd(r, y) = \gcd(r, s)$,
(ii) $\forall\, p \mid x$ *prime*: $v_p(r) = v_p(\lambda_{21})$ *and*
(iii) $\forall\, p \mid y$ *prime*: $v_p(s) = v_p(\lambda_{12})$,

such that $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Proof. Let L be one of the cubic number fields from Table 2.1 together with its corresponding parameters λ_{12} and λ_{21}. Firstly, determine the set of divisors $D_1 \subseteq \mathbb{N}$ for λ_{21} and $D_2 \subseteq \mathbb{N}$ for λ_{12}. Next, applying Corollary 2.2, we computed every diagonal order $S = \langle 1, a, \omega_1, c, \omega_2 \rangle_\mathbb{Z}$ in L with $[\,\mathcal{O}_L : S\,] \leq 10^5$ and filtered out those ones that are Gorenstein. For each of the identified Gorenstein orders, we find parameters

x, y, r, s that meet the criteria specified in (b). Conversely, by selecting parameters that fulfill the conditions in (a), the lattice $S = \langle 1, r, x^2, y, \omega_1, s, x, y^2, \omega_2 \rangle_{\mathbb{Z}}$ is a Gorenstein order of L. Combining these two observations, we have fully characterized all diagonal Gorenstein orders up to the stated index for each cubic number field in Table 2.1. □

Given that Table 2.1 includes randomly selected cubic fields, we conjecture that this theorem applies universally to all cubic number fields, without any constraints on the index. It is worth highlighting that Theorem 2.4 covers the Gorenstein orders previously identified in cubic number fields, as mentioned in [JT15][Example 7.2]. To verify this, consider $y \in \{1, p\}$ and set $x = r = s = 1$, with p being a prime number. A more detailed application of Theorem 2.4 to each of the totally real cubic number fields listed in Table 2.1 is presented in Appendix C. Two significant examples from our findings are presented below.

Example 2.5.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 - 3\,x - 1 \rangle$ or $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 - x^2 - 2\,x - 1 \rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$. Then $\omega_1 = \beta$ and $\omega_2 = \beta^2$. In the meaning of Corollary 2.2 and due to Table 2.1, the parameters $\lambda_{21}, \lambda_{12}$ are both equal to 1. Consequently, $D_1 = \{1\} = D_2$ and we only have to consider the case $r = 1 = s$. Now the conditions (i)-(iii) in Theorem 2.4 (a) are trivial, and we receive the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$. Then the lattice $S = \langle 1, x^2\,y\,\omega_1, x\,y^2\,\omega_2 \rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then there exist $x, y \geq 1$ with $\gcd(x, y) = 1$ such that $a = x^2\,y$ and $c = x\,y^2$.

Example 2.6.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 3\,x^2 - 36\,x - 64 \rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = (1/4)\,(\beta + \beta^2)$. Now, due to Table 2.1, $\lambda_{21} = 4 = \lambda_{12}$ such that we have $D_1 = \{1, 2, 4\} = D_2$ and Theorem 2.4 tells us the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $2 \nmid x$ such as $2 \nmid y$ or
(ii) if $r = 1$, $s = 2$ and $2 \nmid x$ such as $2 \nmid y$ or
(iii) if $r = 1$, $s = 4$ and $2 \nmid x$ or
(iv) if $r = 2$, $s = 1$ and $2 \nmid x$ such as $2 \nmid y$ or
(v) if $r = 4$, $s = 1$ and $2 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2 \rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein,

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

2.3 Diagonal non-Gorenstein orders in cubic number fields

Similar to our approach in Chapter 2.2, we can provide a description of the $\mathbb{Z}$-bases of all diagonal orders in a cubic number field from Table 2.1 that are not Gorenstein. This expands upon the known diagonal orders in cubic number fields that are not Gorenstein, as outlined in [JT15][Example 7.2]. Once more, we computed all diagonal orders S with an index $[\,\mathcal{O}_L \,:\, S\,] \leq 10^5$ and identified the following result on the structure.

Theorem 2.7.
Let L be a cubic number field from Table 2.1 with ring of integers $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$. Let $\lambda_{21}, \lambda_{12} \geq 1$ be integers such that $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is an order if and only if $a \mid \lambda_{21}\,c^2$ and $c \mid \lambda_{12}\,a^2$. Let $D_1 \subseteq \mathbb{N}$ and $D_2 \subseteq \mathbb{N}$ be the set of divisors of λ_{21} and λ_{12}, respectively.

(a) *Let $x > 1$. Then for all $e, d \mid x$ with $\gcd(e, d) = 1$ and $e\,d \neq x$ and for all $r \in D_1$, $s \in D_2$ with $(r\,e\,x)\,(s\,d\,x) \leq 10^5$ the lattice $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2 \rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.*

(b) *If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is an order in L with $[\,\mathcal{O}_L \,:\, S\,] \leq 10^5$ which is not Gorenstein, then exist $x > 1$, $e, d \mid x$ with $\gcd(e, d) = 1$ and $e\,d \neq x$ such as $r \in D_1$, $s \in D_2$ with $a = r\,e\,x$ and $c = s\,d\,x$.*

Proof. Let L be a cubic number field from Table 2.1. We fix the corresponding parameters λ_{12} and λ_{21} as presented in the table. We then determine the sets of divisors $D_1 \subseteq \mathbb{N}$ of λ_{21} and $D_2 \subseteq \mathbb{N}$ of λ_{12}. Applying Corollary 2.2, we compute every diagonal order $S = \langle 1, a, \omega_1, c, \omega_2 \rangle_{\mathbb{Z}}$ in L with index $[\,\mathcal{O}_L \,:\, S\,] \leq 10^5$, filtering out those ones that are not Gorenstein. For each resulting non-Gorenstein order, we identify parameters x, e, d, r, s that satisfy the conditions in (b). Conversely, with parameters meeting the conditions in (a), we find that the lattice $S = \langle 1, r, e, x, \omega_1, s, d, x, \omega_2 \rangle_{\mathbb{Z}}$ is an order in L that is not Gorenstein. By combining these two observations, we describe all non-Gorenstein diagonal orders up to the given index in the fields from Table 2.1. □

Again, we conjecture that this theorem applies to arbitrary cubic fields, without any limitations on the index. Theorem 2.7 covers the known diagonal non-Gorenstein orders from [JT15][Example 7.2] for cubic number fields. To see this, take $x = p$ as a prime and set $1 = e = d = r = s$. We will present a few illustrative examples below. A comprehensive list where Theorem 2.7 is applied to each of the totally real cubic number fields from Table 2.1 can be found in Appendix D.

Example 2.8.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 2\,x^2 - 5\,x + 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = \beta^2$. Then, due to Table 2.1, the parameters $\lambda_{21} = 11$ and $\lambda_{12} = 1$ such that $D_1 = \{1, 11\}$ and $D_2 = \{1\}$. Applying Theorem 2.7 gives the following.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for $r \in D_1 = \{1, 11\}$, the lattice $S = \langle 1, r\,e\,x\,\omega_1, d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then exist x, e, d, r as in (a) such that $a = r\,e\,x$ and $c = d\,x$.

Example 2.9.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 3\,x^2 - 18\,x + 8\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$ and $\omega_1 = \beta$ such as $\omega_2 = (1/2)\,(\beta + \beta^2)$. Here the parameters are $\lambda_{21} = 12$ and $\lambda_{12} = 2$ such that $D_1 = \{1, 2, 3, 4, 6, 12\}$ and $D_2 = \{1, 2\}$. We obtain the following from Theorem 2.7.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for $r \in D_1 = \{1, 2, 3, 4, 6, 12\}$ and $s \in D_2 = \{1, 2\}$, the lattice given by $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then there exist x, e, d, r, s as in (a) such that $a = r\,e\,x$ and $c = s\,d\,x$.

Chapter 3

Constructing isomorphism classes of abelian varieties

By Theorem 1.74, there is a one-to-one correspondence between abelian varieties over $\mathbb{C}$ and polarizable complex tori. The focus of this chapter is to present the construction of principally polarized abelian varieties A over $\mathbb{C}$ that have CM by an arbitrary order S in a CM field K, and to develop an algorithm from this construction. In order to do so, we will reinterpret some classical results from [ST61], [Lan83], and [Shi16] using the framework of proper fractional ideals rather than lattices. Furthermore, we will present how to identify representatives of the isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$ with CM by the specified order S. Additionally, as this is a significant part of the algorithm, we will outline how to find representatives of the ideal class monoid of a chosen order S, revisiting [Mar20]. At the end of this chapter, we will combine our discussions to present the final algorithm. Specifically, this algorithm will compute a representative for each isomorphism class of principally polarized abelian varieties over $\mathbb{C}$ with CM by a particular order S in a CM field K. The algorithm is inspired by a similar algorithm for quartic CM fields in [Str21], which itself extends the classical approach in [VW99] to arbitrary orders.

3.1 Constructing polarized abelian varieties over $\mathbb{C}$ with CM

The construction of polarized abelian varieties over $\mathbb{C}$ with CM by a CM field K, as given in [Lan83][Chapter 1.4], is expressed in terms of lattices in K. To compute these lattices more efficiently, it is helpful to view them as proper fractional ideals of an order S in K. The relationship between these two concepts was previously investigated in Chapter 1.1.2. We revisit [Lan83][Theorem 4.1, Chapter 1] using

the framework of proper fractional ideals.

Theorem 3.1.
Let (K, Φ) be a CM type with $2n = [K : \mathbb{Q}]$.

(a) *If S is an order in K and $\mathfrak{a}$ is a proper fractional S-ideal, then $\Phi(\mathfrak{a})$ is a lattice in $\mathbb{C}^n$ and $\mathbb{C}^n/\Phi(\mathfrak{a})$ is a complex torus with End$(\mathbb{C}^n/\Phi(\mathfrak{a})) \cong S$.*

(b) *If (A, ι) is an abelian variety over $\mathbb{C}$ of type (K, Φ), then there exists an order S in K and a proper fractional S-ideal $\mathfrak{a}$ such that $A(\mathbb{C}) \cong \mathbb{C}^n/\Phi(\mathfrak{a})$ and $\iota^{-1}(\mathrm{End}(A)) = S$.*

Proof. Firstly, let S be an order in K and $\mathfrak{a}$ be a fractional S-ideal. Due to Proposition 1.11, $\mathfrak{a}$ is also a lattice in K. Therefore, we can apply [Lan83][Theorem 4.1 (i), Chapter 1] and get that $\mathbb{C}^n/\Phi(\mathfrak{a})$ is a complex torus of type (K, Φ). Since $\mathfrak{a}$ is also proper, by using [Lan83][Theorem 4.1 (iii), Chapter 1], the endomorphism ring of $\mathbb{C}^n/\Phi(\mathfrak{a})$ is isomorphic to S.
Secondly, let (A, ι) be an abelian variety over $\mathbb{C}$ of type (K, Φ). Then, according to [Lan83][Theorem 4.1 (ii), Chapter 1], there exists a lattice $\mathfrak{a}$ in K such that A is isomorphic to $\mathbb{C}^n/\Phi(\mathfrak{a})$. From Proposition 1.11, $\mathfrak{a}$ is a fractional ideal of its multiplier ring $r(\mathfrak{a}) =: S$. Additionally, by applying [Lan83][Theorem 4.1 (iii), Chapter 1], we conclude that End(A) is isomorphic to $r(\mathfrak{a})$, which is an order in K. □

Note that it remains to show that the complex torus from Theorem 3.1 (a) is actually an abelian variety (A, ι) of type (K, Φ). That requires to show that it is polarizable, which will be done explicitly in Theorem 3.3. We will see that Riemann forms on complex tori of type (K, Φ) correspond to certain elements of K. We introduce some notation.

Definition 3.2.
Let (K, Φ) be a CM field with $[\, K : \mathbb{Q}\,] = 2n$. For every $\alpha \in K$ we define

$$S_\Phi(\alpha) := \begin{pmatrix} \phi_1(\alpha) & & 0 \\ & \ddots & \\ 0 & & \phi_n(\alpha) \end{pmatrix} \in \mathbb{C}^{n \times n}\,.$$

The upcoming theorem summarizes the results presented in [ST61][Chapter 6.2]. We will formulate it in the context of proper fractional ideals. As a further reference, see also [Lan83][Chapter 1, Theorem 4.5].

Theorem 3.3.
Let (K, Φ) be a CM type with $[K : \mathbb{Q}] = 2n$. Let $\mathfrak{a}$ be a proper fractional ideal of some order S of K.

(a) *There exists $\xi \in K$ such that*

$$K = K_0(\xi), \quad -\xi^2 \in K_0^{++}, \quad Im\,\phi(\xi) > 0 \quad \text{for all } \phi \in \Phi, \tag{3.1}$$

where K_0^{++} denotes the set of totally positive elements in K_0. Especially, for such an element $\xi \in K$, we have $\bar{\xi} = -\xi$.

(b) *Let $\xi \in K$ satisfy (3.1) and define $E_\xi(u, v) := \sum_{j=1}^n \phi_j(\xi)(u_j\bar{v_j} - \bar{u_j}v_j)$ for all $u, v \in \mathbb{C}^n$. There exists a positive integer $g \in \mathbb{Z}$ such that $g\,E$ is a non-degenerate Riemann form. Furthermore, we have $E_\xi(\Phi(\alpha), \Phi(\beta)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi\,\alpha\,\bar{\beta})$ for all $\alpha, \beta \in K$ and*

$$E_\xi(u, S_\Phi(\xi)v) = E_\xi(S_\Phi(\bar{\xi})u, v) \quad \text{for all} \quad u, v \in \mathbb{C}^n. \tag{3.2}$$

(c) *Every non-degenerate Riemann form on $\mathbb{C}^n/\Phi(\mathfrak{a})$ satisfying (3.2) is obtained by a $\xi \in K$ satisfying (3.1).*

(d) *If $\mathbb{C}^n/\Phi(\mathfrak{a})$ is simple, then every non-zero Riemann form on $\mathbb{C}^n/\Phi(\mathfrak{a})$ is non-degenerate and satisfies (3.2).*

We briefly outline the implications of this theorem. Given a CM type (K, Φ) and a proper fractional ideal $\mathfrak{a}$ of some order S in K, Theorem 3.3 (a)+(b) show that there is always a Riemann form on the torus $\mathbb{C}^n/\Phi(\mathfrak{a})$ given via a $\xi \in K$ satisfying (3.1). Consequently, the torus is polarizable and isomorphic to an abelian variety A. On the other hand, as presented in Theorem 3.3 (c)+(d), whenever (K, Φ) is primitive, every Riemann form on the torus $\mathbb{C}^n/\Phi(\mathfrak{a})$ is coming from a $\xi \in K$ satisfying the condition of (3.1). It's worth noting that for every $\alpha \in K$, the linear transformation given by $S_\Phi(\alpha)$ corresponds to an element in $\mathrm{End}_\mathbb{Q}(A)$. We will denote this element as $\iota(\alpha)$, allowing us to define an embedding ι such that (A, ι) corresponds to the type (K, Φ).

We have thus seen that an abelian variety (A, ι) of primitive type (K, Φ) with endomorphism ring isomorphic to an order S in K corresponds to a proper fractional ideal $\mathfrak{a}$ of S. Moreover, we can explicitly give a Riemann from on $\mathbb{C}^n/\Phi(\mathfrak{a})$ for every ξ satisfying (3.1) and hence a polarization of the abelian variety (A, ι). This determines all abelian varieties (A, ι) over $\mathbb{C}$ with primitive CM type (K, Φ). Recall from Proposition 1.89 that an abelian variety (A, ι) of type (K, Φ) is simple if and only if Φ is primitive.

In the following proposition, we demonstrate that it is not necessary to initially specify the CM type Φ. Instead, we can determine the CM type based on a suitable element $\xi \in K$. In order to justify the existence of such an element, we refer to Theorem 3.3. Although we have cited [ST61] and [Lan83] for a complete proof, we will provide a brief insight into why, in Theorem 3.3 (a), the condition $\xi^2 \in K_0$ results in $\bar{\xi} = -\xi$. Using an arbitrary embedding σ from K into $\mathbb{C}$, it follows that $\sigma(\xi) = a + i\,b$ for some $a, b \in \mathbb{R}$ and $\sigma(\xi^2) = (a + i\,b)^2 = a^2 + 2\,a\,b\,i + b^2$, which can only be contained in $\mathbb{R}$ if either $a = 0$ or $b = 0$. Given that ξ cannot be embedded into $\mathbb{R}$, we receive that b cannot be zero, leaving us with $a = 0$. As a direct consequence, $\sigma(\bar{\xi}) = -i\,b = \sigma(-\xi)$. Applying the injectivity of the embedding, we can conclude that $\bar{\xi} = -\xi$.

Proposition 3.4.
Let K be a CM field, and let $\xi \in K^\times$ with $\bar{\xi} = -\xi$ and $K = K_0(\xi)$. There exists a CM type Φ of K satisfying $Im(\phi(\xi)) > 0$ for all $\phi \in \Phi$.

Proof. Firstly, $\phi(\xi) \notin K_0$ for all $\phi \in \Phi$ because ξ generates K over K_0 and K can not be embedded into K_0. Thus, $\mathrm{Im}(\phi(\xi)) \neq 0$ for all $\phi \in \Phi$. If $\mathrm{Im}(\phi(\xi)) < 0$, there exists another CM Φ' of K, which differs by Φ only by replacing ϕ with $\phi' := \rho \circ \phi$, where ρ denotes the complex conjugation of K. Now $\mathrm{Im}(\phi'(\xi)) > 0$ and we can find a suitable CM type by repeating this procedure until $\mathrm{Im}(\phi'(\xi)) > 0$ for all $\phi' \in \Phi'$. □

Definition 3.5.
Let (A, ι) be an abelian variety of dimension n over $\mathbb{C}$ of type (K, Φ). We define (A, ι) as being *of type* $(K, \Phi, \mathfrak{a})$ if $A(\mathbb{C}) \cong \mathbb{C}^n/\Phi(\mathfrak{a})$. Furthermore, if (A, ι) is also polarized by $\mathscr{C}$ through an element $\xi \in K$ that satisfies (3.1), then $(A, \iota, \mathscr{C})$ is called a *polarized abelian variety of type* $(K, \Phi, \mathfrak{a}, \xi)$.

Summarizing the discussions from this section and applying the introduced notation, we can state the following. If $(A, \mathscr{C})$ is a simple polarized abelian variety of dimension n over $\mathbb{C}$ with complex multiplication, then, by definition, there exists a CM field K of degree $2n$ over $\mathbb{Q}$ and an isomorphism $\iota : K \hookrightarrow \mathrm{End}_{\mathbb{Q}}(A)$ such that $\iota^{-1}(\mathrm{End}(A)) =: S \subseteq \mathcal{O}_K$ is an order in K. Given the fixed isomorphism ι, a unique primitive CM type Φ of K exists such that $(A, \iota, \mathscr{C})$ is of type (K, Φ). Following Theorem 3.1 and Theorem 3.3, there exists a proper fractional ideal $\mathfrak{a}$ of S and an element $\xi \in K$ satisfying (3.1). In our notation, we say that $(A, \iota, \mathscr{C})$ is of type $(K, \Phi, \mathfrak{a}, \xi)$.

3.2 Isomorphism classes of abelian varieties with CM

This section collects results from [Lan83], [JT15] and [Mar20] in order to present how to determine isomorphism classes of polarized abelian varieties $(A, \iota, \mathscr{C})$ of type (K, Φ). As discussed in the previous section, each such polarized abelian variety can be represented by a tuple $(\mathfrak{a}, \xi)$, where ξ is a certain element in K and $\mathfrak{a}$ is a proper fractional ideal in some order S of K. In the first part of this section, mainly following [Lan83], we explain how to determine isomorphism classes of polarized abelian varieties and highlight the special case in which the polarization is principal. In the second half, we present results from [JT15] and [Mar20] in order to introduce and discuss the ideal class monoid. This allows to compute a representative of each class of proper fractions ideals which will then be helpful to compute the isomorphism classes of polarized abelian varieties explicitly, as presented in the next section.

3.2.1 Isomorphism classes and principal polarizations

Beginning with some basic knowledge about homomorphisms between abelian varieties over $\mathbb{C}$ with complex multiplication, we introduce the following theorem. It can be found in [Lan83][Theorem 4.2, Chapter 1] in terms of lattices. Again, we present it in terms of fractional ideals.

Theorem 3.6.
Let (A, ι) and (A_1, ι_1) be abelian varieties over $\mathbb{C}$ of the same type (K, Φ), say of type $(K, \Phi, \mathfrak{a})$ and $(K, \Phi, \mathfrak{a}_1)$, respectively, where $\mathfrak{a}, \mathfrak{a}_1$ are proper fractional ideals in the same order S of K. Then:

(a) *The homomorphisms from (A, ι) to (A_1, ι_1) correspond to*

$$S_\Phi((\mathfrak{a}_1 : \mathfrak{a})) = S_\Phi(\{\gamma \in K \mid \gamma\mathfrak{a} \subseteq \mathfrak{a}_1\}).$$

(b) *If Φ is primitive, then every homomorphism from A to A_1 is a homomorphism from (A, ι) to (A_1, ι_1).*

The following diagram shows the situation in Theorem 3.6 (a) for λ being a homomorphism from (A, ι) to (A_1, ι_1) corresponding to $\gamma \in K$ with $\gamma\mathfrak{a} \subseteq \mathfrak{a}_1$.

$$\begin{array}{ccc} A & \xrightarrow{\quad\lambda\quad} & A_1 \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta_1} \\ \mathbb{C}^n/\Phi(\mathfrak{a}) & \xrightarrow[S_\Phi(\gamma)]{} & \mathbb{C}^n/\Phi(\mathfrak{a}_1) \end{array}$$

We note that due to Theorem 3.6, if $(A, \iota, \mathscr{C})$ and $(A_1, \iota_1, \mathscr{C}_1)$ are polarized abelian varieties of the same primitive type (K, Φ), then every isomorphism from $(A, \mathscr{C})$ to $(A_1, \mathscr{C}_1)$ gives rise to an isomorphism from $(A, \iota, \mathscr{C})$ to $(A_1, \iota_1, \mathscr{C}_1)$. By applying Theorem 3.6, we can derive the following corollary on the representation of isomorphisms between abelian varieties with complex multiplication using elements of the CM field K and proper fractional ideals.

Corollary 3.7.
Let (A, ι) and (A_1, ι_1) be abelian varieties over $\mathbb{C}$ of the same type (K, Φ), say of type $(K, \Phi, \mathfrak{a})$ and $(K, \Phi, \mathfrak{a}_1)$, respectively, where $\mathfrak{a}, \mathfrak{a}_1$ are proper fractional ideals in the same order S of K. Then, the set of isomorphisms from (A, ι) to (A_1, ι_1) is represented by

$$S_\Phi(\{\gamma \in K \setminus \{0\} \mid \gamma\mathfrak{a} = \mathfrak{a}_1\}).$$

If Φ is primitive, this even holds for the isomorphisms from A to A_1.

Proof. Let λ be a non-zero homomorphism from (A, ι) to (A_1, ι_1). Then, due to Theorem 3.6, the homomorphism λ is represented by $S_\Phi(\gamma)$ for some $\gamma \in K \setminus \{0\}$ with $\gamma\,\mathfrak{a} \subseteq \mathfrak{a}_1$. Now $S_\Phi(\gamma^{-1})$ is an inverse of $S_\Phi(\gamma)$ in $\mathrm{Hom}_{\mathbb{Q}}(\mathbb{C}^n/\Phi(\mathfrak{a}), \mathbb{C}^n/\Phi(\mathfrak{a}_1))$. It remains to show that $S_\Phi(\gamma^{-1}) \in \mathrm{Hom}(\mathbb{C}^n/\Phi(\mathfrak{a}_1), \mathbb{C}^n/\Phi(\mathfrak{a}))$ if and only if $\gamma\,\mathfrak{a} = \mathfrak{a}_1$. Theorem 3.6 also tells us that $S_\Phi(\gamma^{-1}) \in \mathrm{Hom}(\mathbb{C}^n/\Phi(\mathfrak{a}_1), \mathbb{C}^n/\Phi(\mathfrak{a}))$ if and only if $\gamma^{-1}\mathfrak{a}_1 \subseteq \mathfrak{a}$. Therefore, λ has an explicit inverse in $\mathrm{Hom}(\mathbb{C}^n/\Phi(\mathfrak{a}_1), \mathbb{C}^n/\Phi(\mathfrak{a}))$ if and only if

$$\mathfrak{a} = \gamma^{-1}\,\gamma\,\mathfrak{a} \subseteq \gamma^{-1}\mathfrak{a}_1 \subseteq \mathfrak{a}.$$

That means that λ is an isomorphism if and only if $\gamma^{-1}\mathfrak{a}_1 = \mathfrak{a}$, which is equivalent to saying that $\gamma\,\mathfrak{a} = \mathfrak{a}_1$. Whenever Φ is primitive, every isomorphism from A to A_1 also serves as an isomorphism from (A, ι) to (A_1, ι_1). □

In other words, according to Corollary 3.7, two abelian varieties (A, ι) and (A_1, ι_1) over $\mathbb{C}$ of the same type (K, Φ), denoted as $(K, \Phi, \mathfrak{a})$ and $(K, \Phi, \mathfrak{a}_1)$, respectively, are isomorphic if and only if there exists a $\gamma \in K$ such that $\gamma\mathfrak{a} = \mathfrak{a}_1$. We now turn our attention to including polarizations in our considerations.

Definition 3.8.
Let S be an order in a number field K, and let $\mathfrak{a}$ be a fractional ideal of S. The *trace dual of* $\mathfrak{a}$ is defined to be

$$\mathfrak{a}^* := \{x \in K \mid \mathrm{Tr}_{K/\mathbb{Q}}(x\bar{\mathfrak{a}}) \subseteq \mathbb{Z}\}\,.$$

Following the discussions in [ST61][Chapter 6.3], let (K, Φ) be a CM type where $[\,K\,:\,\mathbb{Q}\,] = 2n$. Let $(A, \iota, \mathscr{C})$ be a polarized abelian variety over $\mathbb{C}$ of type $(K, \Phi, \mathfrak{a}, \xi)$ together with an isomorphism $\theta : A/\mathbb{C} \to \mathbb{C}^n/\Phi(\mathfrak{a})$ such that $\iota \in \mathrm{End}_{\mathbb{Q}}(A)$ is defined for every $\alpha \in K$ via

$$\iota(\alpha) = \theta^{-1}(S_\Phi(\alpha) \cdot \theta(\alpha)).$$

Based on [ST61][Chapter 14.2], there exists an isomorphism

$$\theta^* \,:\, A^*(\mathbb{C}) \to \mathbb{C}^n/\Phi(\mathfrak{a}^*)\,,$$

where A^* denotes the Picard variety of A. Furthermore, as highlighted in [ST61][Chapter 6.2], we can define an isomorphism ι^* from K to $\mathrm{End}_{\mathbb{Q}}(A^*)$ by

$$\iota^*(\alpha) := (\iota(\rho(\alpha))^t\,,$$

where $\cdot^t$ represents the transpose, as defined in Chapter 1.5.1. Consequently, (A^*, ι^*) shares the same type (K, Φ) as (A, ι).

Definition 3.9.
Let $(A, \iota, \mathscr{C})$ be a polarized abelian variety over $\mathbb{C}$ of type $(K, \Phi, \mathfrak{a}, \xi)$, and let A^* be the Picard variety of A. Let

$$\begin{aligned} \iota^* \,:\, K &\longrightarrow \mathrm{End}_{\mathbb{Q}}(A^*) \\ \alpha &\longmapsto (\iota(\rho(\alpha))^t\,, \end{aligned}$$

where we denote by ρ the complex conjugation and by $\cdot^t$ the transpose. Then we call (A^*, ι^*) the *dual* of (A, ι).

Building further on the discussion from [ST61][Chapter 6.3], we consider the implications to the polarization. As we have pointed out in Theorem 3.3, the polarization $\varphi_\xi \,:\, A \to A^*$ can be represented by the diagonal matrix $S_\Phi(\xi)$.

We summarize this setup in the following two commutative diagrams, providing an overview of the relationships:

$$\begin{array}{ccc} A(\mathbb{C}) & \xrightarrow{\varphi_\xi} & A^*(\mathbb{C}) \\ {\scriptstyle\theta}\downarrow & & \downarrow{\scriptstyle\theta^*} \\ \mathbb{C}^n/\Phi(\mathfrak{a}) & \xrightarrow[S_\Phi(\xi)]{} & \mathbb{C}^n/\Phi(\mathfrak{a}^*) \end{array} \qquad \begin{array}{ccc} K & \xrightarrow{\iota^*} & \mathrm{End}_{\mathbb{Q}}(A^*) \\ {\scriptstyle\rho}\downarrow & & \uparrow{\scriptstyle .t} \\ K & \xrightarrow[\iota]{} & \mathrm{End}_{\mathbb{Q}}(A) \end{array}$$

Additionally, simply by adapting the definitions and using that we can commute diagonal matrices, we can state that, for each $\alpha \in K$ and for each point $P \in A(\mathbb{C})$, we have

$$\begin{aligned} \varphi_\xi(\iota(\alpha)(P)) &= \varphi_\xi\left(\theta^{-1}(S_\Phi(\alpha)) \cdot \theta(P)\right) \\ &= (\theta^*)^{-1}\left(S_\Phi(\xi) \cdot \theta\left(\theta^{-1}(S_\Phi(\alpha)) \cdot \theta(P)\right)\right) \\ &= (\theta^*)^{-1}\left(S_\Phi(\xi) \cdot S_\Phi(\alpha) \cdot \theta(P)\right) \\ &= (\theta^*)^{-1}\left(S_\Phi(\alpha) \cdot S_\Phi(\xi) \cdot \theta(P)\right) \\ &= (\theta^*)^{-1}\left(S_\Phi(\alpha) \cdot \theta^*\left((\theta^*)^{-1}\left(S_\Phi(\xi)\right) \cdot \theta(P)\right)\right) \\ &= (\theta^*)^{-1}\left(S_\Phi(\alpha) \cdot \theta^*(\varphi_\xi(P))\right) \\ &= \iota^*(\alpha)(\varphi_\xi(P))\,. \end{aligned}$$

Consequently, we can state that, for every $\alpha \in K$, we have

$$\varphi_\xi \iota(\alpha) = \iota^*(\alpha)\varphi_\xi\,.$$

As a consequence of the previous considerations, we can now determine whether a polarization is principal.

Corollary 3.10.
Let (K, Φ) be a CM type with $[K : \mathbb{Q}] = 2n$, and let $(A, \iota, \mathscr{C})$ be a polarized abelian variety over $\mathbb{C}$ of type $(K, \Phi, \mathfrak{a}, \xi)$. The polarization $\mathscr{C}$ on A corresponding to ξ is principal if and only if

$$\xi\mathfrak{a} = \mathfrak{a}^*.$$

Proof. Let (A^*, ι^*) be the dual of (A, ι). The polarization on A coming from ξ is principal if and only if φ_ξ is an isomorphism. Since (A, ι) and (A^*, ι^*) are of the same type (K, Φ), Corollary 3.7 shows that φ_ξ is an isomorphism if and only if $\xi\mathfrak{a} = \mathfrak{a}^*$. □

The next theorem identifies the isomorphism classes of polarized abelian varieties of a specified type, as defined in Definition 1.70. The argument can be viewed as

a combination of Corollary 3.7 and the discussion in [Lan83][Chapter 3.5.2]. The result can be found in [Spa94][Theorem 3.19].

Theorem 3.11.
Let (K, Φ) be a CM type with $[K : \mathbb{Q}] = 2n$. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ and $\mathcal{P}_1 = (A_1, \iota_1, \mathscr{C}_1)$ be principally polarized abelian varieties of the same type (K, Φ), say $(K, \Phi, \mathfrak{a}, \xi)$ and $(K, \Phi, \mathfrak{a}_1, \xi_1)$, respectively. Then $\mathcal{P}$ and $\mathcal{P}_1$ are isomorphic if and only if there exists $\gamma \in K^\times$ with $\mathfrak{a} = \gamma\mathfrak{a}_1$ and $\xi = \gamma\bar{\gamma}\xi_1$.

Proof. Let $\theta : A(\mathbb{C}) \to \mathbb{C}^n/\Phi(\mathfrak{a})$ such as $\theta_1 : A_1(\mathbb{C}) \to \mathbb{C}^n/\Phi(\mathfrak{a}_1)$ be fixed isomorphisms and let λ be an isomorphism from $\mathcal{P}$ to $\mathcal{P}_1$, implying an isomorphism from (A, ι) to (A_1, ι_1) that fulfills

$$\lambda^t \circ \varphi \circ \lambda = \varphi_1.$$

Firstly, based on Corollary 3.7, there exists a $\gamma \in K^\times$ such that $\gamma\,\mathfrak{a} = \mathfrak{a}_1$. Secondly, the map from $\mathbb{C}^n/\Phi(\mathfrak{a})$ to $\mathbb{C}^n/\Phi(\mathfrak{a}_1)$ given by the matrix multiplication with $S_\Phi(\gamma)$ satisfies $\theta_1 \circ \lambda = S_\Phi(\gamma) \circ \theta$. Now, let E and E_1 denote the Riemann forms on $\mathbb{C}^n/\Phi(\mathfrak{a})$ and $\mathbb{C}^n/\Phi(\mathfrak{a}_1) = \mathbb{C}^n/\Phi(\gamma\mathfrak{a})$, corresponding to ξ and ξ_1, respectively. Then we have

$$E_1(S_\Phi(\gamma)\,u, S_\Phi(\gamma)\,v) = E(u, v)$$

and for every $\alpha, \beta \in K$,

$$E(\Phi(\alpha), \Phi(\beta)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi\,\alpha\,\bar{\beta})$$

and

$$E_1(\Phi(\alpha), \Phi(\beta)) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi_1\,\alpha\,\bar{\beta}).$$

From this, it follows that

$$\mathrm{Tr}_{K/\mathbb{Q}}(\xi\,\alpha\,\bar{\beta}) = \mathrm{Tr}_{K/\mathbb{Q}}(\xi_1\,\gamma\alpha\,\bar{\gamma}\bar{\beta}) = \mathrm{Tr}_{K/\mathbb{Q}}(\gamma\bar{\gamma}\xi_1\,\alpha\,\bar{\beta})$$

for all $\alpha, \beta \in K$. This implies $\xi = \gamma\bar{\gamma}\xi_1$. The reverse argument establishes the converse. □

Definition 3.12.
Let (K, Φ) be a CM type with $[K : \mathbb{Q}] = 2n$. Moreover, let $\mathcal{P} = (A, \iota, \mathscr{C})$ and $\mathcal{P}_1 = (A_1, \iota_1, \mathscr{C}_1)$ be polarized abelian varieties of the same type (K, Φ), say $(K, \Phi, \mathfrak{a}, \xi)$ and $(K, \Phi, \mathfrak{a}_1, \xi_1)$, respectively. We say that two tuples $(\mathfrak{a}, \xi)$ and $(\mathfrak{a}_1, \xi_1)$ are equivalent if there exists $\gamma \in K^\times$ with $\mathfrak{a} = \gamma\mathfrak{a}_1$ and $\xi = \gamma\bar{\gamma}\xi_1$. Such an equivalence class is called a *polarized ideal class*. In order to simplify notation, the polarized ideal classes will also be denoted by $(\mathfrak{a}, \xi)$.

Building on Theorem 3.11, we present an additional corollary that highlights the implications of fixing $\mathfrak{a}$.

Corollary 3.13.
Let (K, Φ) be a CM type. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ and $\mathcal{P}_1 = (A_1, \iota_1, \mathscr{C}_1)$ be principally polarized abelian varieties of the same type $(K, \Phi, \mathfrak{a})$, say $(K, \Phi, \mathfrak{a}, \xi)$ and $(K, \Phi, \mathfrak{a}, \xi_1)$, respectively. Let S be the multiplier ring of $\mathfrak{a}$. Then $\mathcal{P}$ and $\mathcal{P}_1$ are isomorphic if and only if there exists $\gamma \in S^\times$ with $\xi = \gamma\bar{\gamma}\xi_1$.

Proof. Let $\mathcal{P}$ and $\mathcal{P}_1$ be isomorphic. Due to Theorem 3.11, there exists $\gamma \in K$ with $\mathfrak{a} = \gamma\mathfrak{a}$ and $\xi = \gamma\bar{\gamma}\xi_1$. As $\mathfrak{a}$ is a proper fractional ideal of its multiplier ring S, we have $\mathfrak{a} = \gamma\mathfrak{a}$ if and only if $\gamma \in S^\times$. On the other hand, if there exists $\gamma \in S^\times$ with $\xi = \gamma\bar{\gamma}\xi_1$, then $\gamma \in K$ and Theorem 3.11 shows that $\mathcal{P}$ and $\mathcal{P}_1$ are isomorphic. □

The following proposition can be found in [Str10][Chapter 1.5.2]. We provide a brief sketch of the proof.

Proposition 3.14.
Let (K, Φ) and (K, Φ') be CM types, and let Φ' be primitive. Let $\mathcal{P}$ be a principally polarized abelian variety of type $(K, \Phi, \mathfrak{a}, \xi)$, and let $\mathcal{P}'$ be a principally polarized abelian variety of type $(K, \Phi', \mathfrak{a}', \xi')$. Then $\mathcal{P}$ and $\mathcal{P}'$ are isomorphic, if and only if Φ and Φ' are equivalent, meaning that there exists $\sigma \in \mathrm{Aut}(K)$ with $\Phi' = \Phi \circ \sigma$, and there exists an element $\gamma \in K^\times$ such that $\sigma(\mathfrak{a}') = \gamma\,\mathfrak{a}$ and $\sigma(\xi') = \gamma\bar{\gamma}\xi$.

Proof. Let $\mathcal{P}$ be isomorphic to $\mathcal{P}'$, which implies they are also isogenous. Given the primitiveness of Φ', according to [Str10][Lemma 5.6, Chapter 1], Φ and Φ' are equivalent. There exists an automorphism $\sigma \in \mathrm{Aut}(K)$ such that $\Phi = \Phi' \circ \sigma^{-1}$. Referring to [Str10][Lemma 5.4, Chapter 1], $\mathcal{P}'$ is isomorphic to a principally polarized abelian variety $\mathcal{P}_1$ characterized by the type $(K, \Phi, \sigma(\mathfrak{a}), \sigma(\xi))$. Consequently, $\mathcal{P}$ is isomorphic to $\mathcal{P}_1$. By invoking Theorem 3.11, this holds if and only if there exists an element $\gamma \in K^\times$ such that $\sigma(\mathfrak{a}) = \gamma\mathfrak{a}$ and $\sigma(\xi) = \gamma\bar{\gamma}\xi$. The reverse reasoning applies analogously. □

Hence, when it comes to determining isomorphism classes of simple polarized abelian varieties, it is sufficient to only consider equivalence classes of primitive CM types.

3.2.2 The ideal class monoid

Recall that we want to construct isomorphism classes of abelian varieties (A, ι) over $\mathbb{C}$ of type (K, Φ) with CM by an arbitrary order S. In Chapter 3.2.1 we explained that this comes down to determine proper fractional S-ideals up to a certain equivalence. To be more precise, this equivalence is characterized by $\mathfrak{a} \sim \mathfrak{b}$ if and only if there exists $\gamma \in K^\times$ with $\gamma\mathfrak{a} = \mathfrak{b}$. This section follows [JT15] and [Mar20].

In order to put the upcoming definition into context, let us revisit a fundamental concept. In quadratic number fields, every order S is Gorenstein, which implies that every proper fractional ideal of S is invertible, as for example pointed out in [Lan87][Chapter 8.1] or [JT15]. This property does not universally hold for number fields of higher degree over $\mathbb{Q}$. We illustrate this in the following example found in [San91][Chapter 2], originally due to Dade, Taussky and Zassenhaus ([DTZ61]).

Example 3.15.
Let ω be an algebraic integer, and let $K = \mathbb{Q}(\omega)$ be a number field of degree $[\, K : \mathbb{Q}\,] = n$. Let $S := \mathbb{Z} + 2\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$. Then S is an order in K. Furthermore, $\mathfrak{a} = \mathbb{Z} + \omega\mathbb{Z} + 2\mathbb{Z}[\omega]$ is a proper fractional S-ideal which is not invertible and the fractional ideal $\mathfrak{a}^{n-1}$ is not even proper, which shows that the set of proper fractional S-ideals is not multiplicatively closed.

Following [JT15], the set of fractional S-ideals is a commutative monoid and the group of principal fractional S-ideals acts on this set by multiplication. The received set of orbits is a monoid. This motivates the following definition.

Definition 3.16.
Let S be an order in a number field K. We denote by J_S the set of fractional S-ideals is a commutative monoid and by P_S of group of principal fractional S-ideals. The set of orbits $\mathrm{ICM}(S) := J_S/P_S$ is called *ideal class monoid* of S. The elements of $\mathrm{ICM}(S)$ will be denoted as $\{\mathfrak{a}\}$.

As presented in [Mar20], the ideal class monoid of an order S can be partitioned into classes of fractional S-ideals with the same multiplier ring. Note that $\mathrm{ICM}(S)$ contains the Picard group $\mathrm{Pic}(S)$ of S and that both are equal if and only if $S = \mathcal{O}_K$. We give the following results, which are [Mar20][Lemma 3.6] and [Mar20][Proposition 3.7].

Lemma 3.17.
Let S be an order in a number field K. Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional S-ideals. If $\mathfrak{a}$ and $\mathfrak{b}$ lie in the same class of $\mathrm{ICM}(S)$*, then they have the same multiplier ring.*

Proposition 3.18.
Let S be an order in a number field K. Then

$$\mathrm{ICM}(S) \supseteq \dot{\bigcup}_{S \subseteq S' \subseteq \mathcal{O}_K} Pic(S')$$

and the inclusion is an equality if and only if S is Bass.

Definition 3.19.
Let $\mathfrak{a}$ and $\mathfrak{b}$ be fractional ideals of an order S in a number field K. We say that $\mathfrak{a}$ and $\mathfrak{b}$ are *weakly equivalent* if they have the same multiplier ring S' and there exists an invertible fractional ideal $\mathfrak{c}$ of S' such that $\mathfrak{a} = \mathfrak{c}\,\mathfrak{b}$. The set of weak equivalence classes of fractional ideals of S is denoted by $\mathscr{W}(S)$, and a class in $\mathscr{W}(S)$ will be denoted by $[\mathfrak{a}]$.

Note that, as pointed out in [Mar20][Proposition 4.1], to say that $\mathfrak{a}$ is weakly equivalent to $\mathfrak{b}$ is equivalent to saying that $1 \in (\mathfrak{a} : \mathfrak{b})(\mathfrak{b} : \mathfrak{a})$.

Definition 3.20.
Let S be an order in a number field K, and let S' be an overorder of S. Then we set

$$\overline{\mathscr{W}}(S') := \{[\mathfrak{a}] \in \mathscr{W}(S) \mid (\mathfrak{a} : \mathfrak{a}) = S'\}.$$

As highlighted in [Mar20], the set of weak equivalence classes, denoted as $\mathscr{W}(S)$, for S, inherits the structure of a commutative monoid from J_S. It can be partitioned as

$$\mathscr{W}(S) = \dot{\bigcup}_{S \subseteq S' \subseteq \mathcal{O}_K} \overline{\mathscr{W}}(S').$$

A fractional ideal is invertible if and only if it is weakly equivalent to its multiplier ring. Thus, we deduce that $\overline{\mathscr{W}}(S') = \{[S']\}$ if and only if S' is Gorenstein. If this is not the case, we do always have at least two different weak equivalent classes in $\overline{\mathscr{W}}(S')$, namely $\{[S']\}$ and $\{[S'^*]\}$, where S'^* denotes the trace dual of S'. The proposition that follows is [Mar20][Corollary 4.5].

Proposition 3.21.
Let S be an order in a number field K. Let $\mathfrak{a}$ and $\mathfrak{b}$ be weakly equivalent fractional S-ideals with the same multiplier ring S'. Then $\mathfrak{a} \sim \mathfrak{b}$ if and only if $(\mathfrak{a} : \mathfrak{b})$ is a principal fractional S'-ideal.

Definition 3.22.
Let S be an order in a number field K. For any overorder S' of S we define

$$\overline{\mathrm{ICM}}(S') := \{\{\mathfrak{a}\} \in \mathrm{ICM}(S) \mid (\mathfrak{a} : \mathfrak{a}) = S'\}.$$

Using the previously introduced notation and Proposition 3.21, we obtain a partition of the ideal class monoid $\mathrm{ICM}(S)$ of an order S in a number field K given by

$$\mathrm{ICM}(S) = \dot{\bigcup}_{S \subseteq S' \subseteq \mathcal{O}_K} \overline{\mathrm{ICM}}(S').$$

The next theorem, as presented in [Mar20][Theorem 4.6], establishes the connection between the Picard group, the commutative monoid of weak equivalence classes and the ideal class monoid of an order. This provides a full set of representatives for the ideal class monoid.

Theorem 3.23.
Let S be an order in a number field K. For every overorder S' of S, the action of $Pic(S')$ on $\overline{\mathrm{ICM}}(S')$, induced by ideal multiplication, is free and

$$\overline{\mathscr{W}}(S') = {\overline{\mathrm{ICM}}(S')}\big/_{Pic(S')}.$$

To be more precise, if we have complete sets of representatives

$$\overline{\mathscr{W}}(S') = \{[\mathfrak{a}_1], \ldots, [\mathfrak{a}_r]\} \qquad \text{and} \qquad Pic(S') = \{\{\mathfrak{b}_1\}, \ldots, \{\mathfrak{b}_s\}\},$$

then

$$\overline{\mathrm{ICM}}(S') = \{\{\mathfrak{a}_i\, \mathfrak{b}_j\} \mid 1 \leq i \leq r,\, 1 \leq j \leq s\}.$$

Combining Proposition 3.18 and Theorem 3.23 allows finding representatives of the ideal class monoid $\mathrm{ICM}(S)$ of an order S by computing all overorders S' of S, their Picard groups $\mathrm{Pic}(S')$ and $\overline{\mathscr{W}}(S')$.

Recall from the beginning of this section that we are interested in identifying all proper fractional S-ideals up to the equivalence $\sim$ for a given order S in a particular number field K. These are specifically represented by $\overline{\mathrm{ICM}}(S)$. Based on Theorem 3.23, $\overline{\mathrm{ICM}}(S)$ can be found by determining the weak equivalence classes $\overline{\mathscr{W}}(S)$ and the Picard group $\mathrm{Pic}(S)$.

3.3 Computing polarized ideal classes

At the end of this chapter, we summarize the considerations from Chapter 3.1 and Chapter 3.2 in an explicit algorithm to compute representatives for every isomorphism class of simple principally polarized abelian varieties A over $\mathbb{C}$ with CM by a given order S in a CM field K. This algorithm is based on an algorithm for quartic CM fields used in [Str21]. In order to compute representatives of $\overline{\mathrm{ICM}}(S)$, we apply the MAGMA implementation from [Mar21] called `ICM_bar`.

Note that, according to Proposition 3.14, it is generally sufficient to consider representatives from the equivalence classes of primitive CM types to identify all isomorphism classes of simple principally polarized abelian varieties over $\mathbb{C}$ with CM by S. Our following algorithm is formulated specifically for a single, fixed primitive CM type. Moreover, we point out that a generator of the ideal $\mathfrak{c}$ in the algorithm is unique only up to multiplication by $\mathcal{O}_K^\times$. This is precisely why we initially compute representatives of $\mathcal{O}_K^\times / \mathrm{N}_{K/K_0}(S^\times)$, where N_{K/K_0} denotes the norm from K into the maximal totally real subfield K_0 of K. The correctness directly follows from the considerations in Chapter 3.1 and Chapter 3.2.

Algorithm 1: Polarized Ideal Classes

input : A primitive CM type (K, Φ) and an order S in K.

output: All tuples $(\mathfrak{a}, \xi)$ representing the isomorphism classes of simple principally polarized abelian varieties $(A, \iota, \mathscr{C})$ over $\mathbb{C}$ of type (K, Φ) with CM by S.

```
1  Initialize an empty sequence Ret.
2  Compute a list of representatives of the proper part ICM-bar(S) of the ideal
     class monoid ICM(S). Save them in ICMbar.
3  Compute representatives of O_K^× / N_{K/K_0}(S^×) and save them in UnitsMod.
4  for a in ICMbar do
5      Compute the complex conjugate b of the trace dual of a.
6      Compute the fractional O_K-ideal c = b O_K · (a O_K)^{-1}.
7      if c is principal then
8          Compute a generator ξ ∈ K of c.
9          for u in UnitsMod do
10             Compute the fractional S-ideal e = u ξ a.
11             if e equals b then
12                 if conj(u ξ) equals −u ξ then
13                     if Φ maps ξ to the positive imaginary axis then
14                         Add (a, ξ) to Ret.
15                     end
16                 end
17             end
18         end
19     end
20 end
21 return Ret
```

Chapter 4

Shimuras third main theorem

This chapter introduces the famous third main theorem of Shimura as outlined in [ST61]. We will present this theorem in its original form and in its modern interpretation found in [BS17]. Shimuras third main theorem provides an explicit description of class fields of complex multiplication fields. This enlarges the results from global class field theory as we revisited in Chapter 1.3. Furthermore, these findings specify certain conditions for principally polarized abelian varieties $\mathcal{P}$ of CM type (K, Φ), especially when their field of moduli is contained in the reflex field of (K, Φ). Our final goal is to deduce specific conditions helping to reduce the amount of possible endomorphism rings of our aimed principally polarized abelian varieties allowing to explicitly classify and construct them. To do so, we further focus on the situation in which this field of moduli equals $\mathbb{Q}$. We will then apply our results to Jacobians of simple curves of genus 3.

4.1 Shimuras third main theorem

In this section, our focus is on Shimura's third main theorem, as originally presented in [ST61][Chapter 17]. While the first main theorem of [ST61] is well-known and can be viewed as a special case of the third main theorem, the third is clearly much more general. Afterwards, we introduce so called polarized ideal classes and apply these objects in order to reformulate Shimuras third main theorem in its modern formulation.

4.1.1 Classical formulation of Shimuras third main theorem

The following theorem is known as Shimuras third main theorem and can be found in [ST61][Chapter 17].

Theorem 4.1.
Let (K^r, Φ^r) be a primitive CM-type, and let (K, Φ) be its reflex. Let S be an order in K of conductor $\mathfrak{f}$, and let (A, ι) be an abelian variety of type (K, Φ) with CM by S. Let u be a point on A of finite order, and let

$$\mathfrak{m} := \{\xi \in S \mid \iota(\xi)u = 0\} \leq S.$$

Let $\mathscr{C}$ be a polarization of A, and let k_0 be the field of moduli of $(A, \mathscr{C})$. Let s be the smallest positive integer in $\mathfrak{f} \cap \mathfrak{m}$. Let $H(S; \mathfrak{m}) \subseteq I_{K^r}(s)$ be the subgroup of ideals $\mathfrak{a}$ such that there exists $x \in K^\times$ with

$$\mathrm{N}_{\Phi^r}(\mathfrak{a}) = x\mathcal{O}_K, \qquad \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a}) = x\bar{x} \quad \textit{and} \quad x \equiv 1 \ \textit{mod}\ (S; \mathfrak{m}),$$

where $x \equiv 1 \ mod\ (S; \mathfrak{m})$ means that there exists $\alpha, \beta \in S$, both prime to $\mathfrak{f}$, satisfying $x = \frac{\alpha}{\beta}$ and $\alpha \equiv \beta \equiv 1 \ mod\, \mathfrak{m}$. Then $k_0(F(u)) \cdot K^r$ is the class field over K^r corresponding to $H(S; \mathfrak{m})$.

In order to obtain practical necessary conditions on the endomorphism rings of simple polarized abelian varieties with a given field of moduli, we deduce some consequences of Theorem 4.1. Before doing so, we introduce some notation.

Definition 4.2.
Let (K^r, Φ^r) be a primitive CM-type, and let (K, Φ) be its reflex. Let $(A, \mathscr{C})$ be a polarized abelian variety of type (K, Φ), and let k_0 be the field of moduli of $(A, \mathscr{C})$. Then we define

$$k_0^* := k_0 \cdot K^r.$$

Firstly, choosing the point of finite order u in Theorem 4.1 to be zero, the module $\mathfrak{m}$ becomes the whole order S and we receive the analogue of the first main theorem of Shimura for arbitrary orders.

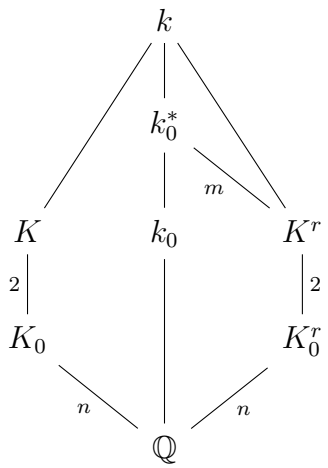
Corollary 4.3.
Let (K^r, Φ^r) be a primitive CM-type, and let (K, Φ) be its reflex. Let S be an order in K of conductor $\mathfrak{f}$, let s be the smallest positive integer in $\mathfrak{f}$, and let (A, ι) be an abelian variety of type (K, Φ) with CM by S. Let $\mathscr{C}$ be a polarization of A, and let k_0 be the field of moduli of $(A, \mathscr{C})$. Let $H(S) \subseteq I_{K^r}(s)$ be the subgroup of ideals $\mathfrak{a}$ such that there exists $x \in K^\times$ with $\mathrm{N}_{\Phi^r}(\mathfrak{a}) = x\mathcal{O}_K$ and $\mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a}) = x\bar{x}$. Then k_0^* is the class field over K^r corresponding to $H(S)$.

Proof. Let $u = 0$, the additive identity element on A. This u is a point of finite order on A. Using the notation from Theorem 4.1, we have

$$\mathfrak{m} = \{\xi \in S \mid \iota(\xi)\, 0 = 0\} = S\,.$$

Consequently, since $\mathfrak{m} = S$, the group $H(S;\mathfrak{m})$ from Theorem 4.1 consists of all ideals $\mathfrak{a}$ in $I_{K^r}(s)$ for which there exists an element $x \in K^\times$ such that $\mathrm{N}_{\Phi^r}(\mathfrak{a}) = x\mathcal{O}_K$ and $\mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a}) = x\bar{x}$. Therefore, given our choice of u, it follows that $H(S;\mathfrak{m})$ is equal to $H(S)$. By applying Theorem 4.1, we derive that k_0^* is the class field over K^r corresponding to $H(S)$. □

We can summarize the situation from Corollary 4.3 in the following diagram. Here, k is a certain suitable number field as presented in [ST61][Chapter 17.3], $[\,K\,:\,\mathbb{Q}\,] =: 2n$, and $[\,k_0^*\,:\,K^r\,] =: m$.



If the polarized abelian variety has its field of moduli k_0 contained in the reflex field K^r (implying that $m = 1$), we can immediately deduce the following result.

Corollary 4.4.
Let (K^r, Φ^r) be a primitive CM-type, and let (K, Φ) be its reflex. Let S be an order in K of conductor $\mathfrak{f}$, let s be the smallest positive integer in $\mathfrak{f}$, and let (A, ι) be an abelian variety which is of type (K, Φ) with CM by S. Let $\mathscr{C}$ be polarization of A, and let the field of moduli k_0 of $(A, \mathscr{C})$ be contained in the reflex field K^r. Then, for every $\mathfrak{a} \in I_{K^r}(s)$, there ex. $x \in K^\times$ with $\mathrm{N}_{\Phi^r}(\mathfrak{a}) = x\mathcal{O}_K$ and $\mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a}) = x\bar{x}$.

Proof. Firstly, as indicated by Corollary 4.3, we have k_0^* as the class field over K^r corresponding to $H(S)$. Given that the field of moduli k_0 is selected to be contained in the reflex field K^r, it follows that $k_0^* = K^r$. Therefore, the field extension of k_0^* over K^r becomes trivial. Consequently, the group $H(S)$ is trivial, implying $H(S) = I_{K^r}(s)$. Based on the definition of $H(S)$, for each $\mathfrak{a}$ in $I_{K^r}(s)$, there exists an element $x \in K^\times$ such that $\mathrm{N}_{\Phi^r}(\mathfrak{a}) = x\mathcal{O}_K$ and $\mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a}) = x\bar{x}$. □

Note that, if we assume A to be defined over a number field $\ell \subseteq K^r$ and do not fix a polarization in the first place, then we can always choose a polarization $\mathscr{C}$ of A, which is also defined over ℓ (see [ST61][Proposition 11, Chapter 1]) such that ℓ is a field of definition of $(A, \mathscr{C})$. The field of moduli k_0 of $(A, \mathscr{C})$ is then contained in ℓ, which means it is contained in K^r and we get the same necessary condition as in Corollary 4.4.

4.1.2 The polarized class group

We introduce the following notation as it can be found in [BGL11], [Bis11], [BS17] and [JW19].

Definition 4.5.
The *polarized class group* (or *Shimura class group*) $\mathfrak{C}(S)$ of an order S in K is defined to be the quotient $\mathcal{I}_S/\mathcal{P}_S$, where

$$\mathcal{I}_S := \{(\mathfrak{a}, \alpha) \in (I_S, K_0) \mid \mathfrak{a}\bar{\mathfrak{a}} = \alpha S \text{ and } \alpha \text{ is totally positive}\}$$
$$\mathcal{P}_S := \{(xS, x\bar{x}) \in \mathcal{I}_S \mid x \in K^\times\}.$$

This definition naturally generalizes a similar group in the well-known case of maximal orders of CM fields as given in [ST61][Chapter 14]. In order to simplify notation, whenever the situation is clear, we will also denote the classes of $\mathfrak{C}(S)$ by $(\mathfrak{a}, \alpha)$. The group operation is given as component-wise multiplication. In the same way as in Lemma 1.30, every class in $\mathfrak{C}(S)$ can be represented by an element $(\mathfrak{a}, \alpha)$, where $\mathfrak{a}$ is prime to a fixed integral ideal $\mathfrak{c}$.

If we fix a primitive CM type (K, Φ), as we have seen in Chapter 3, a principally polarized abelian variety $\mathcal{P} = (A, \mathscr{C})$ over $\mathbb{C}$ of type (K, Φ) with complex multiplication by an order S in K is simple. It is completely determined by a pair $(\mathfrak{a}, \xi)$, where $\mathfrak{a}$ is a proper fractional ideal of S and ξ is a certain element in K corresponding to the polarization of A. As pointed out in [JW19], the polarized class group acts on the set of such pairs in the following way. For $(\mathfrak{b}, \beta) \in \mathfrak{C}(S)$, the pair $\mathcal{P}_1 = (\mathfrak{b}^{-1}\mathfrak{a}, \beta\,\xi)$ determines a principally polarized abelian variety with CM by S that is isogenous to A. This action is free on the set of isomorphism classes of principally polarized abelian varieties with CM by S, or in other words, on the principally polarized ideal classes of S.

Definition 4.6.
Let K be a number field, and let K_0 be a subfield contained in K. For every order S in K, we set $S_0 := S \cap K_0$. The group $\mathrm{Pic}^+(S_0)$ is defined to be the quotient of invertible ideals of S_0 by the principal ideals that have a totally positive generator. Furthermore, we use $(S_0^\times)^+$ to represent the totally positive units of S_0.

Applying this notation, as described in [Bis11][Chapter 3.4] and [JW19][Chapter 2.3], we may also describe the polarized class group by the following exact sequence.

$$1 \to {(S_0^\times)^+}\big/{\mathrm{N}_{K/K_0}(S^\times)} \xrightarrow{u\mapsto(S,u)} \mathfrak{C}(S) \xrightarrow{(\mathfrak{a},\alpha)\mapsto\mathfrak{a}} \mathrm{Pic}(S) \xrightarrow{\mathfrak{a}\mapsto \mathrm{N}_{K/K_0}(\mathfrak{a})} \mathrm{Pic}^+(S_0)\,.$$

Note that the first non-trivial map $u \mapsto (S,u)$ has a trivial kernel because $(S,u) \in \mathcal{P}_S$ if and only if $u = x\,\bar{x}$ for some $x \in K^\times$ with $x\,S = S$. This is the case if and only if $x \in S^\times$ which is equivalent to $u \in \mathrm{N}_{K/K_0}(S^\times)$. The kernel of the second map $(\mathfrak{a},\alpha) \mapsto \mathfrak{a}$ consists of all classes $(\mathfrak{a},\alpha) \in \mathfrak{C}(S)$ with $\mathfrak{a}$ being an invertible principal ideal of S. Therefore, for every class $(\mathfrak{a},\alpha)$ in the kernel, there exists a $x \in K^\times$ with $\mathfrak{a} = xS$. In particular, it is $x^{-1}\,\mathfrak{a} = S$ and by defining $u := x^{-1}\,\overline{x^{-1}}\alpha \in (S_0^\times)^+$ we conclude that $(S,u) = (\mathfrak{a},\alpha)$ in $\mathfrak{C}(S)$. The kernel of the third map $\mathfrak{a} \mapsto \mathrm{N}_{K/K_0}(\mathfrak{a})$ in the sequence consists of all classes in $\mathrm{Pic}(S)$ such that their image under the norm N_{K/K_0} is a principal invertible ideal of S_0 having a totally positive generator. This equals, by definition, the image of the second map.

4.1.3 Modern formulation of Shimuras third main theorem

We are now ready to reformulate Shimuras third main theorem in the framework of polarized class groups.We follow the notation from [BS17]. Let (K,Φ) be a fixed CM type with reflex (K^r,Φ^r). Let $S \subseteq R \subseteq \mathcal{O}_K$ be orders in K and $f := [\,\mathcal{O}_K\,:\,S\,]$. If $\mathfrak{a} \in I_{K^r}(f)$ then $\mathrm{N}_{\Phi^r}(\mathfrak{a}) \in I_K(f)$ (see Proposition 1.59), especially

$$\mathrm{N}_{\Phi^r}(\mathfrak{a}) \in I_K([\,\mathcal{O}_K\,:\,R\,]) \subseteq I_K(\mathfrak{f}_R)\,.$$

If we restrict this ideal to R, then it is still coprime to $\mathfrak{f}_R$ and hence invertible as we have seen in Theorem 1.23. Consequently, the following map is well-defined.

$$\begin{aligned}\Psi : I_{K^r}(f) &\longrightarrow \mathfrak{C}(R)\\ \mathfrak{a} &\longmapsto (\mathrm{N}_{\Phi^r}(\mathfrak{a}), \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a})).\end{aligned}$$

The kernel of Ψ will be denoted as $\Omega_R(f) := \ker\Psi$. Since $\mathfrak{C}(R)$ does not depend on the integer f, the image isomorphic to $I_{K^r}(f)/\Omega_R(f)$ does not depend on f. As a consequence and in order to simplify notation, we can now just write $\Omega_R := \Omega_R(f)$.

We consider two important special cases. Firstly, if $R = \mathcal{O}_K$, then Ψ is a map from $I_{K^r}(f)$ to $\mathfrak{C}(\mathcal{O}_K)$ and we denote the kernel by $\Omega_{\mathcal{O}_K} := \Omega_{\mathcal{O}_K}(f)$. Secondly, whenever $R = S$, then Ψ is a map from $I_{K^r}(f)$ to $\mathfrak{C}(S)$ and we denote the kernel by $\Omega_S := \Omega_S(f)$. We can now reformulate Shimuras third main theorem for arbitrary orders in terms of this modern notation.

Theorem 4.7.
Let (K^r, Φ^r) be a primitive CM-type, and let (K, Φ) be its reflex. Let S be an order in K of index $f := [\,\mathcal{O}_K : S\,]$, and let (A, ι) be an abelian variety of type (K, Φ) with CM by S. Let $\mathscr{C}$ be a polarization of A, and let k_0 be the field of moduli of $(A, \mathscr{C})$. Then k_0^* is the class field over K^r corresponding to $\Omega_S = \Omega_S(f)$.

Proof. Due to Corollary 4.3, we know that $H(S) \subseteq I_{K^r}(s)$ corresponds to the class field k_0^* over K^r, where s is the smallest positive integer in the conductor $\mathfrak{f}$ of S in $\mathcal{O}_K$. The image of an ideal $\mathfrak{a} \in I_{K^r}(s)$ under N_{Φ^r} lies in $I_K(s) \subseteq I_K(\mathfrak{f})$, and is hence actually an ideal in $I_S(\mathfrak{f})$. In the definition of Ψ, we may also replace f by s and Ψ is still well-defined by the same argument. In this sense, it follows that $H(S) = \Omega_S(s)$ and

$$I_{K^r}(s) \big/ \Omega_S(s) = I_{K^r}(f) \big/ \Omega_S(f).$$

Consequently, we know that Ω_S corresponds to the class field k_0^* over K^r. □

This motivates the following definition.

Definition 4.8.
Let K be a CM field, and let S be an order in K of index $f := [\,\mathcal{O}_K : S\,]$. We say that S is a *CM class number one order*, if there exists a primitive CM type Φ of K with $\Omega_S = I_{K^r}(f)$, where K^r is the reflex field of (K, Φ). If the maximal order $\mathcal{O}_K$ of K is a CM class number one order, then K is said to be a *CM class number one field*.

We should mention at this point that $\Omega_S \subseteq \Omega_{\mathcal{O}_K} \subseteq I_{K^r}(f)$. Due to Theorem 4.7, we know that $\Omega_S = I_{K^r}(f)$ whenever the field of moduli is contained in the reflex field $k_0 \subseteq K^r$. Especially, $\Omega_{\mathcal{O}_K} = I_{K^r}(f)$, which means that K has to be CM class number one field. Analog to Corollary 4.4, we obtain the following corollary in the framework of polarized class groups.

Corollary 4.9.
Let (K^r, Φ^r) be a primitive CM-type, and let (K, Φ) be its reflex. Let S be an order in K of index $f := [\mathcal{O}_K : S]$, and let (A, ι) be an abelian variety of type (K, Φ) with CM by S. Let $\mathscr{C}$ be a polarization of A, and let k_0 be the field of moduli of $(A, \mathscr{C})$ contained in K^r. Then S is a CM class number one order and K is a CM class number one field.

Proof. As a consequence of Theorem 4.7, $k_0^* = k_0 \cdot K^r$ is the class field over K^r corresponding to $\Omega_S = \Omega_S(f)$. Since we chose k_0 to be contained in K^r, the field extension k_0^* over K^r is trivial, and we receive that $\Omega_S = I_{K^r}(f)$, which, by definition, means that S is a CM class number one field. □

Summarizing the latest results of this section, we see that every simple polarized abelian variety $\mathcal{P} = (A, \iota, \mathscr{C})$ of a CM type (K, Φ) with field of moduli k_0 contained in the reflex field K^r of (K, Φ) must have an endomorphism ring isomorphic to a CM class number one order S, and K has to be a CM class number one field. The upcoming section will now focus on the case $k_0 = \mathbb{Q}$ concluding further conditions on K.

4.2 Simple polarized abelian varieties with CM and field of moduli $\mathbb{Q}$

In this section we revisit [Shi71][Chapter 5.5] and generalize results on the field of moduli of simple polarized abelian varieties with complex multiplication by maximal orders from [Kıl16][Chapter 4] to arbitrary orders. We start with some notation following [Shi71].

Definition 4.10.
Let (K, Φ) be a primitive CM type, let (K^r, Φ^r) be its reflex, and let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a polarized abelian variety over $\mathbb{C}$ of type (K, Φ). For any subfield L of K, we define the *field of moduli* $k_{0,L}$ of $(A, \iota|_L, \mathscr{C})$ to be the unique subfield of $\mathbb{C}$ such that an automorphism σ of $\mathbb{C}$ is the identity on $k_{0,L}$ if and only if there exists an isomorphism $\eta : A \to A^\sigma$ with $\eta(\mathscr{C}) = \mathscr{C}^\sigma$ and $\eta \circ \iota|_L(\alpha) = \iota|_L^\sigma(\alpha) \circ \eta$ for all $\alpha \in L$.

Note that, in the situation of this definition, the field of moduli of $(A, \iota|_{\mathbb{Q}}, \mathscr{C})$ is the field of moduli of $(A, \mathscr{C})$. The following proposition is [Shi71][Proposition 5.17].

Proposition 4.11.
Let (K, Φ) be a primitive CM type, and let (K^r, Φ^r) be its reflex. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a polarized abelian variety over $\mathbb{C}$ of type (K, Φ) and let L be a subfield of K. Then

(a) *$k_{0,L} \cdot K^r$ is the field of moduli of $(A, \iota|_L, \mathscr{C})$*
(b) *K^r is normal over $k_{0,L} \cap K^r$,*
(c) *$k_{0,L} \cdot K^r$ is normal over K^r,*
(d) *$\mathrm{Gal}(k_{0,L} \cdot K^r / k_{0,L})$ is isomorphic to $\mathrm{Aut}(K/L)$,*
(e) *$k_{0,L}$ contains the smallest subfield of K^r over which K^r is normal.*

We obtain the following proposition, which can be found in [Kıl16][Proposition 4.2.3], and we provide a brief sketch of the proof.

Proposition 4.12.
Let (K, Φ) be a primitive CM type, and let (K^r, Φ^r) be its reflex. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a polarized abelian variety over $\mathbb{C}$ of type (K, Φ). If L is a subfield of K and $k_{0,L} = \mathbb{Q}$, then $L = \mathbb{Q}$ and $K \cong K^r$ is Galois over $\mathbb{Q}$.

Proof. Let L be a subfield of K, and let $k_{0,L} = \mathbb{Q}$. Proposition 4.11 (b) tells us that K^r is normal over $\mathbb{Q}$ and by (d) the Galois group of K^r over $\mathbb{Q}$ is isomorphic to a subgroup of $\mathrm{Aut}(K/L)$, which means that $[\,K^r : \mathbb{Q}\,] \mid [\,K : L\,]$. Since Φ is primitive, we have $K^{rr} = K$, and because K^r is normal over $\mathbb{Q}$, the reflex K^{rr} is isomorphic to a subfield of K^r. Especially $[\,K : L\,] \leq [\,K^r : \mathbb{Q}\,]$ and together with the previous considerations on the degrees we have $L = \mathbb{Q}$ and $K^r \cong K$. □

We can now formulate the following generalization of [Kıl16][Lemma 4.3.2], which extends to arbitrary orders. The initial part of the proof mirrors the one given in [Kıl16]. It is presented for the sake of completeness and a more in-depth understanding. In the latter part of the proof, we apply Shimura's third main theorem in instead of the first main theorem.

Lemma 4.13.
Let (K, Φ) be a CM type with $[\,K : \mathbb{Q}\,] = 2n$ for some prime number $g \neq 2$. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a n-dimensional polarized abelian variety over $\mathbb{C}$ of type (K, Φ) and $\iota^{-1}(\mathrm{End}(A)) = S$, where S is an order in K. If A is simple and the field of moduli $k_0 = k_{0,\mathbb{Q}}$ of $(A, \mathscr{C})$ is $\mathbb{Q}$, then Φ is primitive and S is CM class number one order in a cyclic Galois CM class number one field K containing an imaginary quadratic subfield k.

Proof. Let A be simple, and let the field of moduli $k_0 = k_{0,\mathbb{Q}}$ of $(A, \mathscr{C})$ be equal to $\mathbb{Q}$. Due to Proposition 1.89, the CM type Φ is primitive. Then, together with Lemma

4.12, the CM field K is Galois over $\mathbb{Q}$ and contains a maximal totally real subfield K_0 of odd prime degree n, which implies that $\mathrm{Gal}(K_0/\mathbb{Q})$ is cyclic. Moreover, $\mathrm{Gal}(K/K_0)$ contains the complex conjugation ρ on K and $|\mathrm{Gal}(K/K_0)| = 2$. If k is the subfield of K fixed by the cyclic subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ of order n, then, as $n \neq 2$, we have $\mathrm{Gal}(K/F) = 2$. Therefore, the subfield k of K is imaginary quadratic over $\mathbb{Q}$. As ρ commutes with every element in $\mathrm{Gal}(K/k)$, the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ is abelian and K is cyclic over $\mathbb{Q}$. We may now apply Corollary 4.9 and since $k_0 = \mathbb{Q}$, we receive that S a CM class number one order and K is a CM class number one field. □

In the following discussions, we consider the case $n = 3$. We are asking for simple polarized abelian varieties $(A, \mathscr{C})$ with field of moduli $\mathbb{Q}$ and complex multiplication by an arbitrary order S in a sextic CM field K. Relying on Corollary 4.9 and Lemma 4.13, it is sufficient to focus on CM class number one fields K that are cyclic Galois over $\mathbb{Q}$ and contain an imaginary quadratic subfield. These 37 fields are already presented in [Kıl16][Table 3.1], which we present below.

The table presents the cyclic sextic CM field K, which contains an imaginary quadratic subfield denoted as k. Additionally, F represents the totally real cubic subfield of K, defined by a monic, irreducible polynomial $p(X)$. The value d_k denotes the absolute value of the discriminant of k, and h_F denotes the class number of F. In column C, a '$*$' indicates the availability of a rational model of a corresponding curve with CM by the maximal order $\mathcal{O}_K$ of K.

[Kıl16][Table 3.1]: All CM class number one cyclic sextic CM fields

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

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

4.3 Simple genus 3 curves over $\mathbb{C}$ with CM by arbitrary orders

We remind the reader that every simple principally polarized abelian variety of dimension 3 over $\mathbb{C}$ corresponds to the Jacobian of a simple genus 3 curve over $\mathbb{C}$ (see Theorem 1.85). Additionally, the Jacobian of a simple genus 3 curve over $\mathbb{C}$ can be described as a principally polarized simple abelian variety over $\mathbb{C}$. Consequently, considering simple genus 3 curves over $\mathbb{C}$ with complex multiplication is equivalent to consider simple principally polarized abelian varieties over $\mathbb{C}$ with complex multiplication. We expand the results from [Wen01b] and [KW05] on two specific types of curves with complex multiplication by maximal orders. To be more precise, we will also investigate non-maximal orders. This generalization will be very helpful in explicitly computing isomorphism classes of simple genus 3 CM curves.

4.3.1 Simple hyperelliptic genus 3 curves with CM

Definition 4.14.
Let g be an integer. A *hyperelliptic curve* of genus g over a subfield k of $\mathbb{C}$ is a curve given by an affine equation $y^2 = f(x)$, where $f \in k[x]$, $\deg f \in \{2g+1, 2g+2\}$ and f has no multiple roots in $\bar{k}$. The subspace of g-dimensional Jacobians of hyperelliptic curves of genus g in the g-dimensional moduli space is defined to be the *moduli space of hyperelliptic curves of genus g*.

It is well-known that every genus 2 curve over $\mathbb{C}$ is hyperelliptic. This is not the case for genus $g \geq 3$. As outlined in [Wen01b], the moduli space of hyperelliptic curves of genus 3 has codimension 1 in the moduli space of genus 3 curves. Thus, the chance of a randomly chosen genus 3 curve being hyperelliptic is quite small. Unfortunately, as all simple principally polarized abelian varieties over $\mathbb{C}$ are Jacobians of simple genus 3 curves, this observation extends to the construction of abelian varieties with complex multiplication by an order S in a CM field K, as discussed in Chapter 3. In [Wen01b], Weng introduced a strategy to circumvent this complication for the case $S = \mathcal{O}_K$ by further assuming that K contains $\mathbb{Q}(i)$. The goal of this section is to generalize this approach to arbitrary orders S.

The next theorem extends the findings of [Wen01b][Theorem 4.4.2], and its argument is largely analogous to the original. We provide a brief outline of the proof and direct the reader to [Wen01b] for details on the part that is entirely the same.

Theorem 4.15.
Let C be a simple genus g curve over $\mathbb{C}$ with CM by an order $S \subseteq \mathcal{O}_K$ in a CM field K. If $\mathbb{Z}[i] \subseteq S$, then C is hyperelliptic.

Proof. Let $(J, \mathscr{C})$ be the principally polarized Jacobian of C. As a corollary of Torellis theorem (see [Wen01b][Theorem 1.1.1 and Corollary 1.1.2]) we have

$$\mathrm{Aut}(C) \cong \begin{cases} \mathrm{Aut}(J,\mathscr{C}), & \text{if C is hyperelliptic} \\ \mathrm{Aut}(J,\mathscr{C})/\{\pm 1\}, & \text{if C is not hyperelliptic.} \end{cases}$$

Following [Wen01b][Chapter 4.4], every automorphism on $(J, \mathscr{C})$ is a root of unity in S. Let $\mathbb{Z}[\,i\,] \subseteq S$. Since $\mathrm{End}(J) \cong S$, the automorphism group $\mathrm{Aut}(J, \mathscr{C})$ has order 4, and the automorphisms correspond to $\{\pm 1\,,\, \pm i\}$. Accordingly, there exists an automorphism $\alpha \in \mathrm{Aut}(C)$ of order 2. Since J is simple, $C/\langle\alpha\rangle$ has genus 0. It follows that C is a degree 2 cover of $\mathbb{P}_1$, which is equivalent to C being hyperelliptic. □

Using Theorem 4.15, we narrow our search for simple hyperelliptic genus 3 CM curves to those with complex multiplication by an order S that contains $\mathbb{Z}[i]$. Specifically, we concentrate on sextic CM fields that contain $\mathbb{Q}(i)$.

Building on our considerations from Chapter 4.2, by assuming that the Jacobian of the hyperelliptic genus 3 curves have field of moduli $\mathbb{Q}$, we can further narrow our search to those sextic CM fields, which are cyclic Galois over $\mathbb{Q}$ and have CM class number one. Summarizing these considerations, we finally present the following theorem.

Theorem 4.16.
Let C be a genus 3 curves over a subfield k of $\mathbb{C}$ with complex multiplication by an order S in a CM field K such that $\mathbb{Z}[i] \subseteq S$. Let J denote the Jacobian of C having field of moduli $\mathbb{Q}$. Then

(a) *C is hyperelliptic,*
(b) *K is a cyclic sextic CM class number one field containing $\mathbb{Q}(i)$, and*
(c) *S is a CM class number one order.*

Proof. By applying Theorem 4.15 to C and noting that $\mathbb{Z}[i] \subseteq S$, we deduce that C is hyperelliptic. Furthermore, given that J is assumed to have a field of moduli $\mathbb{Q}$, the application of Lemma 4.13 confirms that K is a sextic cyclic Galois CM field with a CM class number of one, which includes $\mathbb{Q}(i)$, and S is an order with a CM class number of one. □

As highlighted at the very end of the previous section, [Kıl16][Table 3.1] provides a complete list of cyclic sextic CM class number one fields containing an imaginary quadratic subfield. Of the 37 fields listed, six contain the quadratic subfield $\mathbb{Q}(i)$. Table 4.1 collects these six fields from [Kıl16][Table 3.1].

In the following table, we define K as $\mathbb{Q}[x]/\langle f\rangle$, where the irreducible polynomial f is given by $f = \sum_{i=0}^{6} \alpha_i x^i$ with $\alpha_i \in \mathbb{Z}[x]$. Similarly, K_0 is defined as $\mathbb{Q}[x]/\langle g\rangle$, where $g = \sum_{i=0}^{3} \beta_i x^i$ with $\beta_i \in \mathbb{Z}[x]$. K_0 is the totally real cubic subfield of K such that $K = \mathbb{Q}(i)K_0$. We take both f and g to be monic, implying $\alpha_6 = 1$ and $\beta_3 = 1$. Consequently, we represent the polynomials, and thus the fields, as tuples $[\alpha_0, \ldots, \alpha_5]$ and $[\beta_0, \beta_1, \beta_2]$.

Table 4.1: CM class number one fields $K = \mathbb{Q}(i)\, K_0$

No.	g	f
1	$[1, -5, 2]$	$[37, -32, 40, -10, -3, 4]$
2	$[-1, -3, 0]$	$[17, 12, 12, -2, -3, 0]$
3	$[-1, -2, 1]$	$[13, 8, 7, -2, 0, 2]$
4	$[8, -14, 1]$	$[274, -298, 217, -8, -24, 2]$
4	$[-8, -10, 1]$	$[202, 190, 89, -32, -16, 2]$
6	$[8, -18, 3]$	$[386, -438, 393, -80, -24, 6]$

Summarizing the discussions in this section, when seeking hyperelliptic genus 3 curves over $\mathbb{C}$ with CM by an order S in a CM field K, it is beneficial to focus on those where $\mathbb{Z}[i]$ is a subset of S. Furthermore, when assuming that the Jacobian of such a curve has field of moduli $\mathbb{Q}$, the CM field must be among those listed in Table 4.1. In order to provide a complete list of potential endomorphism rings for these curves, we will deduce further conditions in the following chapters.

4.3.2 Simple Picard genus 3 curves with CM

Definition 4.17.
A *Picard curve* over a subfield k of $\mathbb{C}$ is a cyclic trigonal curve of genus 3 given by an affine equation $y^3 = f(x)$ with $f \in k[x]$ being a polynomial of degree 4 having no multiple roots in $\bar{k}$.

In [KW05], Koike and Weng present an explicit method for constructing Picard curves with complex multiplication by the maximal order $\mathcal{O}_K$ in a sextic CM field K. Specifically, as illustrated in [KW05][Lemma 1], they demonstrate that if K includes $\mathbb{Q}(\zeta_3)$, where ζ_3 represents a third root of unity, the curve is Picard. Conversely, if a curve is a Picard curve, then K must contain $\mathbb{Q}(\zeta_3)$.

The theorem below extends the findings of [KW05][Lemma 1]. Again, its argument largely follows the original. We provide a brief outline of the proof, and we direct the reader to [KW05] for details on the part that is entirely analogous.

Theorem 4.18.
Let C be a simple genus 3 curve over $\mathbb{C}$ with CM by an order $S \subseteq \mathcal{O}_K$ in a sextic CM field K. Then C is Picard if and only if $\mathbb{Z}[\zeta_3] \subseteq S$. If this is the case, then $K = \mathbb{Q}(\zeta_3)K_0$, where K_0 denotes the maximal totally real subfield of K.

Proof. On the one hand, if C is Picard, then C can be represented by an affine equation $y^3 = f(x)$ with $f \in \mathbb{C}[x]$, $\deg f = 4$ and f has no multiple roots. Hence, C has an automorphism of order 3 and $\mathbb{Z}[\zeta_3] \subseteq S$. On the other hand, if $\mathbb{Z}[\zeta_3] \subseteq S$ we can apply Torellis theorem (see [Wen01b][Theorem 1.1.1 and Corollary 1.1.2]) and receive that C has an automorphism α of order 3. Now let $\mathbb{C}(C) = \mathbb{C}(x, y)$ be the function field of C and let $\mathbb{C}(\tilde{C})$ be the function field of C factored by α. As the Jacobian J of C is simple, $\mathbb{C}(\tilde{C})$ must be the rational field and $\mathbb{C}(C)/\mathbb{C}(\tilde{C})$ is a Kummer extension of degree 3. Accordingly, C can be given by an affine equation $y^3 = f(x)$. The Riemann-Hurwitz formula tells us that $C \to \mathbb{P}_1$ is branched at five points. If we choose the point at infinity to be a ramification point, then f has degree 4 and C is Picard. □

As a consequence of Theorem 4.18, for every Picard curve with complex multiplication by an order S in a CM field K, we know that S contains $\mathbb{Z}[\zeta_3]$ and K is a sextic CM field that contains $\mathbb{Q}(\zeta_3)$.

Following the argument of Chapter 4.2, by assuming that the Jacobian of the Picard curve has field of moduli $\mathbb{Q}$, we can further narrow our search to sextic CM fields, which are cyclic Galois over $\mathbb{Q}$ and have CM class number one. Summarizing these considerations, we receive the following theorem.

Theorem 4.19.
Let C be a genus 3 curve over a subfield k of $\mathbb{C}$ with complex multiplication by an order S in a CM field K. Let J be the Jacobian of C. Then C is a Picard curve if and only if $\mathbb{Z}[\zeta_3] \subseteq S$. If this is the case and if J has field of moduli $\mathbb{Q}$, then S is a CM class number one order in a cyclic sextic CM class number one field K containing $\mathbb{Q}(\zeta_3)$.

Proof. By applying Theorem 4.18, we deduce that C is a Picard curve if and only if $\mathbb{Z}[\zeta_3] \subseteq S$. Given that C is a Picard curve and its Jacobian has a field of moduli $\mathbb{Q}$, Lemma 4.13 implies that S is a CM class number one order in a cyclic Galois sextic CM field which includes an imaginary quadratic subfield. Since $\mathbb{Z}[\zeta_3] \subseteq S$, this specific subfield is $\mathbb{Q}(\zeta_3)$. □

Similar to the argument in Chapter 4.3.1, [Kıl16][Table 3.1] provides a complete list of all 37 cyclic sextic CM class number fields K containing an imaginary quadratic subfield. Of these 37 fields, ten contain the subfield $\mathbb{Q}(\zeta_3)$.

In the following table, we define K as $\mathbb{Q}[x]/\langle f\rangle$, where the irreducible polynomial f is given by $f = \sum_{i=0}^{6} \alpha_i x^i$ with $\alpha_i \in \mathbb{Z}[x]$. Similarly, K_0 is defined as $\mathbb{Q}[x]/\langle g\rangle$, where $g = \sum_{i=0}^{3} \beta_i x^i$ with $\beta_i \in \mathbb{Z}[x]$. K_0 is the totally real cubic subfield of K such that $K = \mathbb{Q}(\zeta_3)K_0$. We let both f and g be monic, implying $\alpha_6 = 1$ and $\beta_3 = 1$. Consequently, we represent the polynomials, and thus the fields, as tuples $[\alpha_0, \ldots, \alpha_5]$ and $[\beta_0, \beta_1, \beta_2]$.

Table 4.2: CM class number one fields $K = \mathbb{Q}(\zeta_3)\, K_0$

No.	g	f
7	$[1, -4, 1]$	$[151, -32, 51, 6, 2, 2]$
8	$[-1, -2, 1]$	$[91, 28, 35, 6, 6, 2]$
9	$[-8, -10, 1]$	$[628, 262, 117, -24, -10, 2]$
10	$[8, -14, 1]$	$[892, -434, 245, 0, -18, 2]$
11	$[8, -18, 3]$	$[1324, -702, 453, -56, -18, -18, 6]$
12	$[1, -9, 6]$	$[721, -252, 336, -34, 27, 12]$
13	$[-64, -36, 3]$	$[9892, 5166, 993, -308, -54, 6]$
14	$[-27, -15, 4]$	$[2493, 1008, 132, -126, -5, 8]$
15	$[-27, -21, 2]$	$[2817, 1404, 384, -114, -29, 4]$
16	$[-1, -3, 0]$	$[109, 24, 36, -2, 3, 0]$

We note that the first nine fields in Table 4.2 have $|\mu_K| = 6$, whereas the last field has $|\mu_K| = 18$. This will play a role in later chapters on the existence of certain Picard curves with CM.

Summarizing the discussions from this section, we have found that for Picard curves over $\mathbb{C}$ with CM by an order S in a CM field K, it is sufficient to narrow our focus to those where $\mathbb{Z}[\zeta_3]$ is contained in S. Moreover, if we assume their Jacobian to have a field of moduli $\mathbb{Q}$, the CM field is contained in those outlined in Table 4.2. An open challenge is finding further constrains of the orders S to provide a complete list of potential endomorphism rings for these curves. We will explore this in the following chapters, especially in Chapter 7.

Chapter 5

The relative norm of CM class number one orders

During this chapter, (K, Φ) is a primitive CM type, where K a cyclic Galois or non-normal sextic CM field containing an imaginary quadratic subfield k. We let S and R be orders in K such that S is contained in R. As in the previous chapters, we denote by K_0 the totally real cubic subfield of K, and let S_0 and R_0 be the restrictions of S and R to K_0, respectively. Additionally, define $f := [\,\mathcal{O}_K\,:\,S\,]$ to be the index of S in the maximal order $\mathcal{O}_K$ of K.

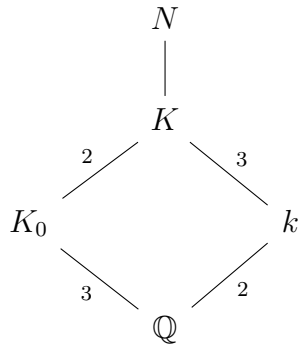
The goal of this chapter is to establish a relationship between the orders S and R as well as their restrictions S_0 and R_0, in the context, where S is a CM class number one order. We will do this by examining the following map with a special focus on its kernel. The approach is inspired by [BS17] in which Bisson and Streng considered quartic instead of sextic CM fields, and we will use the same notation.

Definition 5.1.
Let R and S be orders in a CM field K with $S \subseteq R$, and let μ_R be the group of roots of unity of R. Let K_0 the maximal totally real subfield of K, and let R_0 and S_0 be the restrictions of R and S to K_0, respectively. We define the *relative norm* to be the following map induced by the relative norm N_{K/K_0}:

$$\psi : {(R/f\mathcal{O}_K)^\times}\big/{(S/f\mathcal{O}_K)^\times \mu_R} \longrightarrow {(R_0/f\mathcal{O}_{K_0})^\times}\big/{(S_0/f\mathcal{O}_{K_0})^\times}.$$

As discussed in the previous chapters, the above-mentioned situation in this chapter applies to several situations when asking for curves with complex multiplication. For example, simple polarized abelian varieties of dimension 3 with CM and field of moduli $\mathbb{Q}$ (see Lemma 4.13), hyperelliptic genus 3 CM curves $C/\mathbb{C}$ with $\mathbb{Z}[i] \subseteq S$, which means that $\mathbb{Q}(i) \subseteq K$ (see Theorem 4.15) and Picard CM curves $C/\mathbb{C}$ with $\mathbb{Z}[\zeta_3] \subseteq S$, implying that $\mathbb{Q}(\zeta_3) \subseteq K$ (see Theorem 4.18).

Due to the fact that K contains an imaginary quadratic subfield, we can characterize the primitive CM types as detailed in [Kıl16][Chapter 3]. We provide a brief summary. Since K_0 is a totally real cubic field and k is imaginary quadratic, we conclude that $k \cap K_0 = \mathbb{Q}$ and $K = K_0 k$. Let N represent the normal closure of K. In this context, K can either be Galois with $\mathrm{Gal}(N/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q}) \cong C_6$ or non-normal with $\mathrm{Gal}(N/\mathbb{Q}) \cong S_3 \times C_2 \cong D_6$. The diagram below summarizes the situation.



As pointed out in [Kıl16][Proposition 3.3.2] and [Kıl16][Proposition 3.4.2], in both cases, whether K is Galois or non-normal, there is only one equivalence class of primitive CM types. Furthermore, we can give an explicit description of a representative for this class.

(a) (K cyclic Galois): The Galois group is given by $\mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle$, where τ is an automorphism such that $\tau^3 = \rho$, which represents the complex conjugation. Without loss of generality, we state that a primitive CM type Φ of K takes the form $\Phi = \{1, \tau, \tau^{-1}\}$. This ensures that $K^r = K$ and $\Phi^r = \Phi$.

(b) (K non-normal): In this case, the corresponding Galois group is given by $\mathrm{Gal}(N/\mathbb{Q}) = \langle \tau, \sigma \mid \tau^6 = \sigma^2 = 1,\ (\tau\sigma)^2 = 1 \rangle$. Here, the second automorphism, σ, leaves K invariant, and once more $\tau^3 = \rho$ represents the complex conjugation. Without a loss of generality, we state that a primitive CM type Φ of K has the form $\Phi = \{1, \tau|_K, \tau^{-1}|_K\}$. We also have $K^r = K$ and $\Phi^r = \Phi$.

In order to simplify our notation, and as the argument is completely analogue, we will denote the CM type of our CM field K by $\Phi = \{1, \tau, \tau^{-1}\}$ in both cases. In the non-normal case, this actually means the restriction of τ to K. Furthermore, for the rest of this chapter, we will assume that $K^r = K$ and $\Phi^r = \Phi$.

We return to the map Ψ from Chapter 4.1.3, examining it in this particular context, which now takes the form:

$$\begin{aligned}\Psi : I_K(f) &\longrightarrow \mathfrak{C}(S)\\ \mathfrak{a} &\longmapsto (\mathrm{N}_\Phi(\mathfrak{a}), \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{a})).\end{aligned}$$

The kernel of Ψ is denoted by $\Omega_S := \Omega_S(f)$.

The aim of this section is to show that when S is a CM class number one order, i.e. $\Omega_S = I_K(f)$, the kernel of the relative norm of the two orders $S \subseteq R$ has an exponent of at most two. The argument is inspired by [BS17], which handles non-biquadratic quartic CM fields.

Before proving the first proposition of this section, it is important to note that for $\Phi = \{1, \tau, \tau^{-1}\}$, we get $\rho \circ \tau = \tau^{-2}$ and $\rho \circ \tau^{-1} = \tau^2$, with ρ representing the complex conjugation in K.

Proposition 5.2.
Let (K, Φ) be a primitive sextic CM type, let K contain an imaginary quadratic subfield, and let K be cyclic Galois or non-normal. Let $\Phi = \{1, \tau, \tau^{-1}\}$, and let S be an order in K. Then, for every $(\mathfrak{a}, \alpha) \in \mathcal{I}_S$, we have

$$\begin{aligned}\mathrm{N}_\Phi(\mathrm{N}_\Phi(\mathfrak{a})) &= \mathfrak{a}^2 \left(\tau(\alpha)\tau^{-1}(\alpha)\,\mathrm{N}_\Phi(\mathfrak{a})\right) \qquad \textit{and}\\ \mathrm{N}_{K/\mathbb{Q}}\left(\mathrm{N}_\Phi(\mathfrak{a})\right) &= \alpha^2 \left(\tau(\alpha\bar{\alpha})\tau^{-1}(\alpha\bar{\alpha})\,\mathrm{N}_\Phi(\mathfrak{a}\bar{\mathfrak{a}})\right).\end{aligned}$$

Proof. Let $(\mathfrak{a}, \alpha) \in \mathcal{I}_S$, then $\mathfrak{a}\bar{\mathfrak{a}} = \alpha S$. Applying the type norm twice, we receive

$$\begin{aligned}\mathrm{N}_\Phi(\mathrm{N}_\Phi(\mathfrak{a})) &= \mathrm{N}_\Phi(\mathfrak{a}\tau(\mathfrak{a})\tau^{-1}(\mathfrak{a}))\\ &= \left(\mathfrak{a}\tau(\mathfrak{a})\tau^{-1}(\mathfrak{a})\right)\left(\tau(\mathfrak{a})\tau^2(\mathfrak{a})\mathfrak{a}\right)\left(\tau^{-1}(\mathfrak{a})\mathfrak{a}\tau^{-2}(\mathfrak{a})\right)\\ &= \mathfrak{a}^2\left(\tau(\mathfrak{a})\tau^{-2}(\mathfrak{a})\tau^{-1}(\mathfrak{a})\tau^2(\mathfrak{a})\right)\left(\mathfrak{a}\tau(\mathfrak{a})\tau^{-1}(\mathfrak{a})\right).\end{aligned}$$

Together with $\rho \circ \tau = \tau^{-2}$ and $\rho \circ \tau^{-1} = \tau^2$ we can further say that

$$\begin{aligned}\mathrm{N}_\Phi(\mathrm{N}_\Phi(\mathfrak{a})) &= \mathfrak{a}^2\left(\tau(\mathfrak{a})(\tau\circ\rho)(\mathfrak{a})\tau^{-1}(\mathfrak{a})(\tau^{-1}\circ\rho)(\mathfrak{a})\right)\left(\mathfrak{a}\tau(\mathfrak{a})\tau^{-1}(\mathfrak{a})\right)\\ &= \mathfrak{a}^2\left(\tau(\mathfrak{a})\tau(\bar{\mathfrak{a}})\tau^{-1}(\mathfrak{a})\tau^{-1}(\bar{\mathfrak{a}})\right)\left(\mathfrak{a}\tau(\mathfrak{a})\tau^{-1}(\mathfrak{a})\right)\\ &= \mathfrak{a}^2\left(\tau(\mathfrak{a}\bar{\mathfrak{a}})\tau^{-1}(\mathfrak{a}\bar{\mathfrak{a}})\right)\left(\mathfrak{a}\tau(\mathfrak{a})\tau^{-1}(\mathfrak{a})\right)\\ &= \mathfrak{a}^2\left(\tau(\alpha)\tau^{-1}(\alpha)\,\mathrm{N}_\Phi(\mathfrak{a})\right).\end{aligned}$$

Since $\mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_\Phi(\mathfrak{a})) = \mathrm{N}_\Phi(\mathrm{N}_\Phi(\mathfrak{a})) \cdot \overline{\mathrm{N}_\Phi(\mathrm{N}_\Phi(\mathfrak{a}))}$ and $\mathfrak{a}\bar{\mathfrak{a}} = \alpha S$, we receive that

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_\Phi(\mathfrak{a})) &= \mathfrak{a}^2(\tau(\alpha)\tau^{-1}(\alpha)\,\mathrm{N}_\Phi(\mathfrak{a}))\,\overline{\mathfrak{a}^2\,(\tau(\alpha)\tau^{-1}(\alpha)\,\mathrm{N}_\Phi(\mathfrak{a}))} \\ &= \alpha^2\left(\tau(\alpha\bar{\alpha})\tau^{-1}(\alpha\bar{\alpha})\,\mathrm{N}_\Phi(\mathfrak{a}\bar{\mathfrak{a}})\right).\end{aligned}$$

□

We are now in a position to state the following lemma, which provides a necessary condition for CM class number orders S. Specifically, it establishes that every element in $\mathfrak{C}(S)$ has an order of at most 2.

Lemma 5.3.
Let (K, Φ) be a primitive sextic CM type, let K contain an imaginary quadratic subfield, and let K be cyclic Galois or non-normal. Let $\Phi = \{1, \tau, \tau^{-1}\}$, and let S be an order in K of index $f = [\mathcal{O}_K : S]$. If $\Omega_S = I_K(f)$, then, for every $(\mathfrak{a}, \alpha) \in \mathfrak{C}(S)$, we have

$$(\mathfrak{a}, \alpha)^2 = \Psi(\mathrm{N}_\Phi(\mathfrak{a})) = (S, 1).$$

Proof. Let $(\mathfrak{a}, \alpha) \in \mathcal{I}_S \in \mathfrak{C}(S)$ and $\Omega_S = I_K(f)$. Then $\mathrm{N}_\Phi(\mathfrak{a}) \in P_S$ and

$$\left(\tau(\alpha)\tau^{-1}(\alpha)\,\mathrm{N}_\Phi(\mathfrak{a}), \tau(\alpha\bar{\alpha})\tau^{-1}(\alpha\bar{\alpha})\,\mathrm{N}_\Phi(\mathfrak{a}\bar{\mathfrak{a}})\right) = (S, 1),$$

hence it is trivial in $\mathfrak{C}(S)$. Applying Proposition 5.2 we receive

$$\begin{aligned}(\mathfrak{a}, \alpha)^2 &= \left(\mathfrak{a}^2\left(\tau(\alpha)\tau^{-1}(\alpha)\,\mathrm{N}_\Phi(\mathfrak{a})\right), \alpha^2\left(\tau(\alpha\bar{\alpha})\tau^{-1}(\alpha\bar{\alpha})\,\mathrm{N}_\Phi(\mathfrak{a}\bar{\mathfrak{a}})\right)\right) \\ &= \left(\mathrm{N}_\Phi(\mathrm{N}_\Phi(\mathfrak{a})), \mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_\Phi(\mathfrak{a}))\right) \\ &= \Psi(\mathrm{N}_\Phi(\mathfrak{a})).\end{aligned}$$

Now $(\mathfrak{a}, \alpha)^2$ is in the image of Ψ and since $\Omega_S = I_K(f)$, we get that $(\mathfrak{a}, \alpha)^2 = (S, 1)$ is trivial in $\mathfrak{C}(S)$. □

We will now rephrase this theorem in terms of elements rather than ideals by using the relative norm introduced at the beginning of this section. The following lemma can be found in [BS17][Lemma 7]. It is of significant generality in order to be applicable to our situation. We will sketch the proof to better illustrate the links between the various parts. For a more detailed view, we refer to [BS17].

Lemma 5.4.
Let S and R be orders in a CM field K, and let $S \subseteq R$. Let K_0 be the maximal totally real subfield of K, and let $S_0 := S \cap K_0$ such as $R_0 := R \cap K_0$. Let $\eta : \mathfrak{C}(S) \longrightarrow \mathfrak{C}(R)$ be the natural homomorphism, $f := [\, \mathcal{O}_K \,:\, S \,]$. We consider the relative norm

$$\psi : {(R/f\mathcal{O}_K)^\times}\big/{(S/f\mathcal{O}_K)^\times \mu_R} \longrightarrow {(R_0/f\mathcal{O}_{K_0})^\times}\big/{(S_0/f\mathcal{O}_{K_0})^\times}.$$

Then

$$\ker \eta \cong \ker \psi \qquad \textit{and} \qquad \textit{coker}\, \eta \cong \textit{coker}\, \psi.$$

Proof. The diagram below describes the relationships among the groups $\mathcal{I}_S$, $\mathcal{P}_S$, and the polarized class group $\mathfrak{C}(S)$ of the order S as defined in Definition 4.5, together with the corresponding objects for the order R.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{P}_S & \longrightarrow & \mathcal{I}_S & \longrightarrow & \mathfrak{C}(S) & \longrightarrow & 1 \\ & & \big\downarrow & & \big\downarrow & & \big\downarrow & & \\ 1 & \longrightarrow & \mathcal{P}_R & \longrightarrow & \mathcal{I}_R & \longrightarrow & \mathfrak{C}(R) & \longrightarrow & 1 \end{array}$$

The snake lemma (see [Lan12][Lemma 9.1, Chapter 3]) tells us that

$$\text{(co-)}\ker \eta \cong \text{(co-)}\ker \left({\mathcal{P}_R}\big/{\mathcal{P}_S} \to {\mathcal{I}_R}\big/{\mathcal{I}_S} \right).$$

It remains to give an isomorphism between $\mathcal{P}_R/\mathcal{P}_S$ and $(R/f\mathcal{O}_K)^\times/(S/f\mathcal{O}_K)^\times\mu_R$ and an embedding from $\mathcal{I}_S/\mathcal{I}_R$ into $(R_0/f\mathcal{O}_{K_0})^\times/(S_0/f\mathcal{O}_{K_0})^\times$ such that the induced map is ψ. For the first map we take

$$\begin{aligned} {\mathcal{P}_R}\big/{\mathcal{P}_S} &\longrightarrow {(R/f\mathcal{O}_K)^\times}\big/{(S/f\mathcal{O}_K)^\times \mu_R} \\ (xR, x\bar{x}) &\longmapsto x, \end{aligned}$$

and for the second map we take

$$\begin{aligned} {\mathcal{I}_S}\big/{\mathcal{I}_R} &\longrightarrow {(R_0/f\mathcal{O}_{K_0})^\times}\big/{(S_0/f\mathcal{O}_{K_0})^\times} \\ (\mathfrak{a}, \alpha) &\longmapsto \alpha\,, \end{aligned}$$

each defined on the integral representatives.

The initial map is defined on $\mathcal{P}_R$ since the pair $(xR, x\bar{x})$ uniquely determines x up to roots of unity in R. Looking at the kernel, it includes those pairs $(xR, x\bar{x})$ for which x is invertible modulo f. This means that xS does not share any common factor with f. In other words, the kernel is $\mathcal{P}_S$. Therefore, the map is indeed well-defined, surjective, and injective when factoring its kernel $\mathcal{P}_S$.

Let the pair $(\mathfrak{a}, \alpha)$ belong to the kernel of the second map, $\mathfrak{a}$ being integral. It follows that αS_0 does not share any common factor with f, which means αS is also coprime to f. Let $\mathfrak{b}$ denote the unique S-ideal that is coprime to f and satisfies $\mathfrak{a} = \mathfrak{b}R$. From this, we get $\mathfrak{b}\bar{\mathfrak{b}}R = \alpha R$ and, given that both αS and $\mathfrak{b}$ are coprime to f, it follows that $(\mathfrak{b}, \alpha)$ belongs to $\mathcal{I}_S$. This suggests $(\mathfrak{a}, \alpha)$ is also in $\mathcal{I}_S$, proving injectivity. □

Combining this result with Lemma 5.3, we obtain the final proposition of this section.

Proposition 5.5.
Let (K, Φ) be a primitive sextic CM type, where K contains an imaginary quadratic subfield. Let K be cyclic Galois or non-normal. Let $\Phi = \{1, \tau, \tau^{-1}\}$, let S and R be orders in K with $S \subseteq R$, and let $f = [\,\mathcal{O}_K : S\,]$. If $\Omega_S = I_K(f)$, then the kernel of the relative norm

$$\psi : {(R/f\mathcal{O}_K)^\times}\big/{(S/f\mathcal{O}_K)^\times \mu_R} \longrightarrow {(R_0/f\mathcal{O}_{K_0})^\times}\big/{(S_0/f\mathcal{O}_{K_0})^\times}$$

is of exponent at most 2.

Proof. By applying Lemma 5.4, we deduce that $\ker\psi \cong \ker\eta$. More specifically, we have

$$(\ker\psi)^2 \cong (\ker\eta)^2 \subseteq \mathfrak{C}(S)^2\,.$$

Now, following Lemma 5.3, the square of any class within $\mathfrak{C}(S)$ is trivial. This leads to the conclusion that $\mathfrak{C}(S)^2 = \{(S, 1)\}$. Merging these observations, we see that $(\ker\psi)^2$ is trivial, and every element in $\ker\psi$ has an order not exceeding 2.

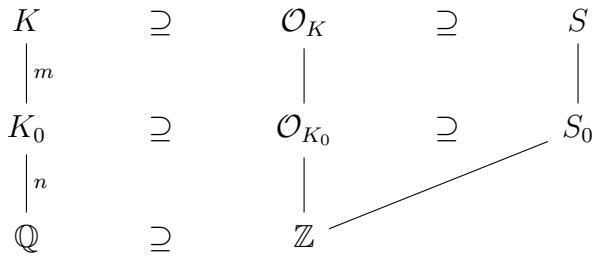
□

We have discussed that CM class number one orders come with a unique property for the associated relative norm. This property will be important in the next chapters, providing additional constrains on CM class number one orders. Specifically, Proposition 5.5 will be employed in Theorem 8.1 in order to establish bounds for the index of the endomorphism rings of certain simple principally polarized abelian varieties of dimension 3 that have complex multiplication.

Chapter 6

Relating the index of orders and their restrictions

Throughout this chapter, we consider towers of number fields $\mathbb{Q} \subseteq K_0 \subseteq K$ and orders $S \subseteq \mathcal{O}_K$, as well as their restriction $S_0 := S \cap \mathcal{O}_{K_0}$ to K_0. We aim to develop upper bounds on $[\,\mathcal{O}_{K_0} : S_0\,]$ which depend only on $[\,\mathcal{O}_K : S\,]$ and the number fields. In the initial section, we adopt a lattice-based approach, building on Minkowski's convex body theorem. In the following section, we expand on a result from [BS17], which not just proved an upper bound but also a divisibility criterion. The diagram that follows shows the considered situation.



6.1 Minkowski's convex body theorem

Before discussing useful consequences of Minkowski's convex body theorem, we first introduce some notation.

Definition 6.1.
Let $(V, \langle\cdot,\cdot\rangle)$ be an Euclidean vector space, and let $\mathfrak{a}$ be lattice in V of full rank n. Let $(\alpha_1, \ldots, \alpha_n)$ be a basis of $\mathfrak{a}$. The *fundamental domain* of $\mathfrak{a}$ is defined to be the set of vectors $v \in V$ such that there exist $\lambda_1, \ldots, \lambda_n \in [\,0, 1)$ with $v = \sum_{i=1}^{n} \lambda_i \alpha_i$. The *covolume* of $\mathfrak{a}$, denoted as $\mathrm{covol}(\mathfrak{a})$, is defined as the volume of the fundamental domain, which is

$$\mathrm{covol}(\mathfrak{a}) = |\det(\langle \alpha_i, \alpha_j \rangle)_{i,j})|^{1/2}\,.$$

The next theorem is known as *Minkowskis convex body theorem*, and can be for example in [Neu99][Theorem 4.4, Chapter 1].

Theorem 6.2.
Let $(V, \langle \cdot, \cdot \rangle)$ be an Euclidean vector space of dimension n, and let $\mathfrak{a}$ be a complete lattice in V. Let $X \subseteq V$ be a bounded, convex, symmetric subset with

$$\mathrm{vol}(X) > 2^n \,\mathrm{covol}(\mathfrak{a}) \,.$$

Then $X \cap \mathfrak{a}$ contains an element different from zero.

In order to apply Theorem 6.2, we consider number fields as Euclidean vector spaces in the following way, as it can be found in [Ste08][Chapter 10].

Definition 6.3.
Let K be a number field with $[\,K \,:\, \mathbb{Q}\,] = n$. Let $\sigma_1, \ldots, \sigma_n \,:\, K \hookrightarrow \mathbb{C}$ denote the embeddings of K into $\mathbb{C}$. The base extension from K as a $\mathbb{Q}$-vector space to a $\mathbb{C}$-vector space, denoted $K_{\mathbb{C}} := K \otimes_{\mathbb{Q}} \mathbb{C}$, delivers a ring homomorphism

$$\begin{aligned} j_K \,:\, K &\longrightarrow K_{\mathbb{C}} \cong \mathbb{C}^{n\times 1} \\ x &\longmapsto (\sigma_i(x))_i \,. \end{aligned}$$

We let $K_{\mathbb{R}}$ be the subring of $K_{\mathbb{C}}$ consisting of the elements, which are invariant under the involution $F \,:\, (z_{\sigma_i})_i \mapsto (\bar{z}_{\bar{\sigma}_i})_i$.

Now let K be a number field, then $j_K(K) \subseteq K_{\mathbb{R}}$ and $K_{\mathbb{R}}$ is an Euclidean vector space inheriting the scalar product from $K_{\mathbb{C}} \cong \mathbb{C}^n$. If we denote by r the number of real embeddings and by $2s$ the number of complex embeddings of K, then

$$K_{\mathbb{R}} \cong \mathbb{R}^r \times \mathbb{C}^s \,.$$

The volume in $K_{\mathbb{R}}$ is by a factor of 2^s larger than the canonical volume on $\mathbb{R}^r \times \mathbb{C}^s$. Note that whenever K is totally real then $K_{\mathbb{R}} \cong \mathbb{R}^n$, and then the volumes coincide. The following proposition can be found in [Ste08][Lemma 10.3]. It can be used to determine the covolume of orders and ideals.

Proposition 6.4.
Let S be an order in a number field K. Then the covolume of $j_K(S)$ in $K_{\mathbb{R}}$ is equal to $|\Delta(S)|^{1/2}$. Furthermore, for every integral ideal $\mathfrak{a}$ in S we have

$$\mathrm{covol}(j_K(\mathfrak{a})) = [\,S \,:\, \mathfrak{a}\,]\,|\Delta(S)|^{1/2}.$$

By merging Theorem 6.2 with Proposition 6.4, we can identify a non-zero element with a minimal norm in the trace dual of an order. This approach is inspired by the discussions on the finiteness of Picard groups found in [Ste08][Chapter 10].

Theorem 6.5.
Let K be a totally real number field of degree n over $\mathbb{Q}$, and let S be an order in K. Then the trace dual S^* of S contains a non-zero element $\alpha \in S^*$ with

$$0 < \mathrm{N}_{K/\mathbb{Q}}(\alpha) \leq [\, S \,:\, S^* \,]\, \Delta(S)^{1/2} = [\, \mathcal{O}_K \,:\, S \,]^{-1}\, \Delta_{K/\mathbb{Q}}^{-1/2}\,.$$

Proof. Let $\sigma_1, \ldots, \sigma_n$ denote the embeddings from K into $\mathbb{R}$ and $j_K : K \to K_{\mathbb{R}}$ be the map from Definition 6.3, where $K_{\mathbb{R}} \cong \mathbb{R}^{n\times 1}$. We know that S^* is a fractional ideal of S with $S \subseteq S^*$ and if $c := [\, S^* \,:\, S \,]$, then $\mathfrak{a} := c\, S^*$ is an integral ideal in S. Now $j_K(\mathfrak{a})$ is a lattice in $K_{\mathbb{R}} \cong \mathbb{R}^{n\times 1}$ with $\mathrm{covol}(j_K(\mathfrak{a})) = [\, S \,:\, \mathfrak{a} \,]\, \Delta(S)^{1/2}$ (see Proposition 6.4). In order to apply Theorem 6.2 we define bounded, convex, symmetric subsets X of $K_{\mathbb{R}}$ with

$$\mathrm{vol}(X) > 2^n\, \mathrm{covol}(j_K(\mathfrak{a}))\,.$$

For any $\varepsilon > 0$ let $R(\varepsilon) := [\, S \,:\, \mathfrak{a} \,]^{1/(n-1)}\, \Delta(S)^{1/2(n-1)} + \varepsilon$ and

$$X_{R(\varepsilon)} := \left\{ \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix}^T \mid |x_1| < 1\,,\ |x_j| < R(\varepsilon) \ \text{ for all } \ j = 2, \ldots, n \right\}.$$

Then $\mathrm{vol}(X_{R(\varepsilon)}) = 2^n\, R(\varepsilon)^{n-1}$, which implies that

$$\begin{aligned} \mathrm{vol}(X_{R(\varepsilon)}) = 2^n\, R(\varepsilon)^{n-1} &= 2^n\, (\, [\, S \,:\, \mathfrak{a} \,]^{1/(n-1)}\, \Delta(S)^{1/2(n-1)} + \varepsilon \,)^{n-1} \\ &> 2^n [\, S \,:\, \mathfrak{a} \,]\, \Delta(S)^{1/2} = 2^n\, \mathrm{covol}(\mathfrak{a})\,. \end{aligned}$$

Now Theorem 6.2 tells us that, for every $\varepsilon > 0$, $j_K(\mathfrak{a})$ contains a non-zero element $b = \begin{pmatrix} b_1 & \cdots & b_n \end{pmatrix}^T$ with

$$|b_1| < 1 \quad \text{and} \quad |b_j| < R(\varepsilon) = [\, S \,:\, \mathfrak{a} \,]^{1/2}\, \Delta(S)^{1/4} + \varepsilon \ \text{ for all } \ j = 2, \ldots, n\,.$$

Hence, there exists $\beta \in \mathfrak{a} \setminus \{0\}$ with

$$0 < \mathrm{N}_{K/\mathbb{Q}}(\beta) = \prod_{i=1}^{n} \sigma_i(\beta) < 1 \cdot R(\varepsilon)^{n-1}\,.$$

Note that $\beta \notin \mathbb{Z}$ as $|b_1| < 1$. Especially, for $\varepsilon \to 0$, we receive that

$$0 < \mathrm{N}_{K/\mathbb{Q}}(\beta) \leq [\, S \,:\, \mathfrak{a} \,]\, \Delta(S)^{1/2}\,.$$

Now we have

$$[\,S\,:\,\mathfrak{a}\,] = [\,S\,:\,cS^*\,] = c^n\,[\,S\,:\,S^*\,],$$

and there exists $\alpha \in S^* \setminus \{0\}$ with $\beta = c\,\alpha$. It follows that

$$0 < c^n\ \mathrm{N}_{K/\mathbb{Q}}(\alpha) = \mathrm{N}_{K/\mathbb{Q}}(\beta) \le c^n\,[\,S\,:\,S^*\,]\,\Delta(S)^{1/2},$$

which is equivalent to

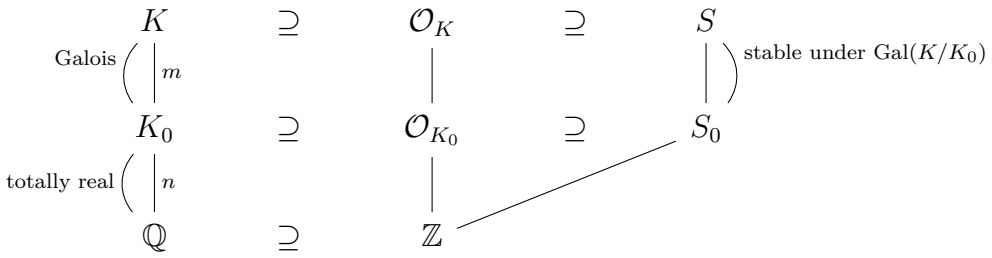
$$0 < a := \mathrm{N}_{K/\mathbb{Q}}(\alpha) \le [\,S\,:\,S^*\,]\,\Delta(S)^{1/2}\,. \tag{6.1}$$

Additionally, applying Proposition 1.17, we get that

$$[\,S\,:\,S^*\,] = [\,S^*\,:\,S\,]^{-1} = (\Delta_{K/\mathbb{Q}}\,[\,\mathcal{O}_K\,:\,S\,]^2)^{-1} = \Delta_{K/\mathbb{Q}}^{-1}\,[\,\mathcal{O}_K\,:\,S\,]^{-2}.$$

Also $\Delta(S) = [\,\mathcal{O}_K\,:\,S\,]^2\,\Delta_{K/\mathbb{Q}}$. This implies $\Delta(S)^{1/2} = [\,\mathcal{O}_K\,:\,S\,]\,\Delta_{K/\mathbb{Q}}^{1/2}$. Consequently, the right-hand side of (6.1) is equal to $[\,\mathcal{O}_K\,:\,S\,]^{-1}\,\Delta_{K/\mathbb{Q}}^{-1/2}$. □

We are now in the position to present the main result of this section, which is based on Theorem 6.5. The following diagram provides an overview of the situation.



Theorem 6.6.
Let K_0 be a totally real number field of degree n over $\mathbb{Q}$, and let K be a Galois extension of K_0 of degree m. Let S be an order in K stable under $\mathrm{Gal}(K/K_0)$*, and let S_0 denote the restriction of S to K_0. Then*

$$[\,\mathcal{O}_{K_0}\,:\,S_0\,]^m \le [\,\mathcal{O}_K\,:\,S\,]^2 \Delta_{K/\mathbb{Q}}\,\Delta_{K_0/\mathbb{Q}}^{-m/2}\,.$$

Proof. Due to Theorem 6.5, there exists $\alpha \in S_0^* \setminus \{0\}$ with

$$0 < a := \mathrm{N}_{K_0/\mathbb{Q}}(\alpha) \le [\,\mathcal{O}_{K_0}\,:\,S_0\,]^{-1}\,\Delta_{K_0/\mathbb{Q}}^{-1/2}\,.$$

Since S is stable under $\mathrm{Gal}(K/K_0)$, we know that $S_0^* S \subseteq S^*$ such that the following is a positive integer:

$$[\,S^*\,:\,\alpha S\,] = a^m [\,S^*\,:\,S\,]\,.$$

Now

$$[\,\mathcal{O}_{K_0} \,:\, S_0\,]^m\,\Delta_{K_0/\mathbb{Q}}^{m/2} \leq a^{-m} = \frac{[\,S^* \,:\, S\,]}{[\,S^* \,:\, \alpha S\,]} \leq [\,S^* \,:\, S\,] = [\,\mathcal{O}_K \,:\, S\,]^2 \Delta_{K/\mathbb{Q}}\,.$$

□

Summarizing the discussions of this section within the context of Theorem 6.6, we have identified an upper bound for the index $[\,\mathcal{O}_{K_0} \,:\, S_0\,]$ that depends only on the number fields and $[\,\mathcal{O}_K \,:\, S\,]$. Importantly, the scenario that we have considered covers the cases where K is a CM field because a CM field is a totally real quadratic extension of a totally real subfield K_0. Especially, K is Galois over K_0.

6.2 Divisibility criterion

In this section, we consider a tower of number fields $\mathbb{Q} \subseteq K_0 \subseteq K$ and an order S of K, as well as its restriction $S_0 := S \cap \mathcal{O}_{K_0}$ to K_0. Our goal is to extend [BS17][Lemma 13] and to eliminate the constraint $[\,K_0 \,:\, \mathbb{Q}\,] = 2$. Additionally, we apply our results to specific scenarios, especially to the case in which S_0 is Gorenstein. The following proposition on the index can be found in [DCD00][Theorem 1].

Proposition 6.7.
Let S be an order in a number field K. Let $\mathfrak{a}$ be a fractional ideal of S. Then, as fractional ideals of $\mathbb{Z}$, we have

(a) $[\,\mathcal{O}_K \,:\, \mathfrak{a}\mathcal{O}_K\,] \subseteq [\,S \,:\, \mathfrak{a}\,]$
(b) $[\,\mathcal{O}_K \,:\, \mathfrak{a}^{-1}\mathcal{O}_K\,] \subseteq [\,\mathfrak{a} \,:\, S\,]$
(c) $[\,S \,:\, \mathfrak{a}^{-1}\,] \subseteq [\,\mathfrak{a}\mathcal{O}_K \,:\, \mathcal{O}_K\,]$.

The inclusions are equations if and only if $\mathfrak{a}$ is invertible ($\mathfrak{a}\,\mathfrak{a}^{-1} = S$).

Definition 6.8.
Let S be an order in a number field K, and let $\mathfrak{a}$ be a fractional ideal of S. We define

$$\delta(\mathfrak{a}) := \frac{[\,\mathcal{O}_K \,:\, \mathfrak{a}\mathcal{O}_K\,]}{[\,S \,:\, \mathfrak{a}\,]} \geq 1\,.$$

According to Proposition 6.7, for a fractional ideal $\mathfrak{a}$ of the order S in the number field K, we have $\delta(\mathfrak{a}) = 1$ if and only if $\mathfrak{a}$ is invertible. Specifically, if $\mathfrak{a} = S^*$, being the trace dual of S, then $\delta(S^*) = 1$ if and only if S^* is invertible. This is true if and only if S is Gorenstein. The following proposition provides bounds on $\delta(\mathfrak{a})$ which are independent of the fractional ideal, but depend on the conductor and the index of the considered order.

Proposition 6.9.
Let $S \subseteq \mathcal{O}_K$ be an order in a number field K of conductor $\mathfrak{f}_S$. Let $\mathfrak{a}$ be a fractional ideal of S. Then

$$1 \leq \delta(\mathfrak{a}) \leq [\,\mathcal{O}_K \,:\, S\,]\, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}_S)\,.$$

Proof. In a first step, we show that there exists another fractional ideal $\mathfrak{b}$ of S, which is locally isomorphic to $\mathfrak{a}$ satisfying $\mathfrak{f}_S \subseteq \mathfrak{b} \subseteq \mathcal{O}_K$. Let $\mathfrak{p}$ be a prime ideal of S and $\bar{S}_\mathfrak{p}$ be the integral closure of $S_\mathfrak{p}$, then $\bar{S}_\mathfrak{p} = (S\setminus\mathfrak{p})^{-1}\mathcal{O}_K$ as integral closure commutes with localization. Now $\bar{S}_\mathfrak{p}$ is Dedekind (see [Neu99][Theorem 11.4, Chapter 1]) and local, hence a discrete valuation ring. In fact, there exists $\alpha \in K$ with

$$\mathfrak{a}_\mathfrak{p}\, \bar{S}_\mathfrak{p} \;=\; \alpha\, \bar{S}_\mathfrak{p}\,.$$

Now let $\mathfrak{b}_\mathfrak{p} := \alpha^{-1}\,\mathfrak{a}_\mathfrak{p}$. Then $\mathfrak{b}_\mathfrak{p} \subseteq \mathfrak{b}_\mathfrak{p}\,\bar{S}_\mathfrak{p} = \bar{S}_\mathfrak{p}$ and on the other hand, due to the fact that $\mathfrak{f}_S$ is an ideal of both S and $\mathcal{O}_K$, we have

$$(\mathfrak{f}_S)_\mathfrak{p} = (\mathfrak{f}_S)_\mathfrak{p}\,\bar{S}_\mathfrak{p} = (\mathfrak{f}_S)_\mathfrak{p}\,\mathfrak{b}_\mathfrak{p}\,\bar{S}_\mathfrak{p} = (\mathfrak{f}_S)_\mathfrak{p}\,\bar{S}_\mathfrak{p}\mathfrak{b}_\mathfrak{p} \;=\; (\mathfrak{f}_S)_\mathfrak{p}\,\mathfrak{b}_\mathfrak{p} \subseteq \mathfrak{b}_\mathfrak{p}\,.$$

Accordingly, for every prime $\mathfrak{p}$ of S we get a $\mathfrak{b}_\mathfrak{p}$ with $(\mathfrak{f}_S)_\mathfrak{p} \subseteq \mathfrak{b}_\mathfrak{p} \subseteq \bar{S}_\mathfrak{p}$ and there exists a fractional ideal $\mathfrak{b}$ of S locally isomorphic to $\mathfrak{a}$ such that $\mathfrak{f}_S \subseteq \mathfrak{b} \subseteq \mathcal{O}_K$. Since $\mathfrak{b}$ is locally isomorphic to $\mathfrak{a}$, they differ only by an invertible ideal of S which is locally principal. Thus, locally $\delta(\mathfrak{a})$ equals $\delta(\mathfrak{b})$ at every prime, and we receive $\delta(\mathfrak{a}) = \delta(\mathfrak{b})$. Applying Proposition 6.7 and the fact that $\mathfrak{f}_S \subseteq \mathfrak{b}\mathcal{O}_K \subseteq \mathcal{O}_K$ we receive that

$$[\,S \,:\, \mathfrak{b}\,] \leq [\,\mathcal{O}_K \,:\, \mathfrak{b}\,\mathcal{O}_K\,] \leq [\,\mathcal{O}_K \,:\, \mathfrak{f}_S\,]\,.$$

This comes down to

$$1 \leq \delta(\mathfrak{a}) = \delta(\mathfrak{b}) = \frac{[\,\mathcal{O}_K \,:\, \mathfrak{b}\,\mathcal{O}_K\,]}{[\,S \,:\, \mathfrak{b}\,]} \leq \frac{[\,\mathcal{O}_K \,:\, \mathfrak{f}_S\,]}{[\,S \,:\, \mathfrak{b}\,]}\,.$$

Now, as $\mathfrak{f}_S \subseteq \mathfrak{b} \subseteq \mathcal{O}_K$, we get that

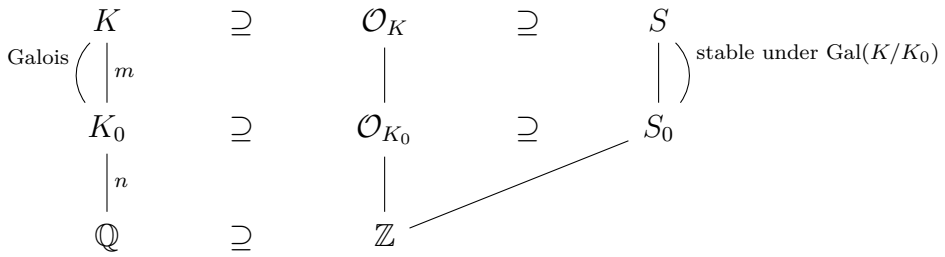
$$\frac{[\,\mathcal{O}_K \,:\, \mathfrak{f}_S\,]}{[\,S \,:\, \mathfrak{b}\,]} = \frac{[\,\mathcal{O}_K \,:\, \mathfrak{f}_S\,]}{[\,S \,:\, \mathfrak{f}_S\,]}\,[\,\mathfrak{b} \,:\, \mathfrak{f}_S\,] = [\,\mathcal{O}_K \,:\, S\,]\,[\,\mathfrak{b} \,:\, \mathfrak{f}_S\,] \leq [\,\mathcal{O}_K \,:\, S\,]\,[\,\mathcal{O}_K \,:\, \mathfrak{f}_S\,]\,.$$

Combining the last two inequalities with the definition of the norm, we receive

$$1 \leq \delta(\mathfrak{a}) \leq [\,\mathcal{O}_K \,:\, S\,]\, \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}_S)\,.$$

□

We now turn our attention to generalizing [BS17][Lemma 13]. While this lemma was originally formulated for quadratic extensions K_0 of $\mathbb{Q}$, we aim to extend it to any degree $n = [\, K_0 \,:\, \mathbb{Q} \,]$. The following diagram illustrates the situation.



In order to simplify notation, we introduce one more definition.

Definition 6.10.
Let $\mathbb{Q} \subseteq K_0 \subseteq K$ be number fields with $n = [\, K_0 \,:\, \mathbb{Q} \,]$ and $m = [\, K \,:\, K_0 \,]$. Let S be an order in K, and let $S_0 := S \cap K_0$. Then we define

$$\delta_S := \frac{\delta(S_0^*)^m}{\delta(S_0^* S)} \in \mathbb{Q}\,.$$

The following theorem generalized [BS17][Lemma 13] and it contains the aimed divisibility criterion.

Theorem 6.11.
Let $\mathbb{Q} \subseteq K_0 \subseteq K$ be number fields, where K_0 is of degree n over $\mathbb{Q}$. Let K be a degree m Galois extension of K_0. Let S be an order of K which is stable under the Galois group $\mathrm{Gal}(K/K_0)$*, and let $S_0 := S \cap K_0$. Then $[\, S^* \,:\, S_0^* S \,]$ is an integer, and*

$$[\, S^* \,:\, S_0^* S \,]\, [\, \mathcal{O}_{K_0} \,:\, S_0 \,]^{2m} \;=\; \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\, [\, \mathcal{O}_K \,:\, S \,]^2\, \delta_S\,.$$

Proof. We consider the trace dual S_0^* of S_0 as a fractional ideal of S_0. Following Proposition 1.17 (e) we know that $S_0^* S \subseteq S^*$ and $[\, S^* \,:\, S_0^* S \,]$ is an integer. On the other hand,

$$[\, S^* \,:\, S_0^* S \,] = [\, S^* \,:\, S \,][\, S \,:\, S_0^* S \,]\,. \tag{6.2}$$

The first factor on the right-hand side of (6.2), as described in Proposition 1.17 (d), decomposes into

$$[\, S^* \,:\, S \,] = \Delta_{K/\mathbb{Q}} [\, \mathcal{O}_K \,:\, S \,]^2\,. \tag{6.3}$$

For the second factor on the right-hand side of (6.2), applying Definition 6.10, the

usual properties of the norm and Proposition 1.17 (d) together deliver that

$$\begin{aligned}
[\, S \,:\, S_0^* S \,] &= [\, \mathcal{O}_K \,:\, S_0^* \mathcal{O}_K \,]\, \delta(S_0^* S)^{-1} \\
&= \mathrm{N}_{K/\mathbb{Q}}(S_0^* \mathcal{O}_K)\, \delta(S_0^* S)^{-1} \\
&= \mathrm{N}_{K/\mathbb{Q}}((S_0^* \mathcal{O}_{K_0}) \mathcal{O}_K)\, \delta(S_0^* S)^{-1} \\
&= \mathrm{N}_{K_0/\mathbb{Q}}((S_0^* \mathcal{O}_{K_0})^m)\, \delta(S_0^* S)^{-1} \\
&= [\, \mathcal{O}_{K_0} \,:\, S_0^* \mathcal{O}_{K_0} \,]^m\, \delta(S_0^* S)^{-1} \\
&= [\, S_0 \,:\, S_0^* \,]^m\, \delta(S_0^*)^m\, \delta(S_0^* S)^{-1} \\
&= [\, S_0^* \,:\, S_0 \,]^{-m}\, \delta(S_0^*)^m\, \delta(S_0^* S)^{-1} \\
&= \Delta_{K_0/\mathbb{Q}}^{-m} [\, \mathcal{O}_{K_0} \,:\, S_0 \,]^{-2m}\, \underbrace{\delta(S_0^*)^m\, \delta(S_0^* S)^{-1}}_{=\delta_S} \,.
\end{aligned}$$

Combining this with (6.3) we receive

$$[\, S^* \,:\, S_0^* S \,] = \left(\Delta_{K/\mathbb{Q}} [\, \mathcal{O}_K \,:\, S \,]^2\right) \left(\Delta_{K_0/\mathbb{Q}}^{-m} [\, \mathcal{O}_{K_0} \,:\, S_0 \,]^{-2m}\, \delta_S\right) ,$$

which is equivalent to

$$[\, S^* \,:\, S_0^* S \,]\, [\, \mathcal{O}_{K_0} \,:\, S_0 \,]^{2m} \;=\; \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\, [\, \mathcal{O}_K \,:\, S \,]^2\, \delta_S \,.$$

□

Note that both sides of the equation in Theorem 6.11 are integers. Furthermore, we have special interest in the case, in which we can control the quotient

$$\delta_S = \frac{\delta(S_0^*)^m}{\delta(S_0^* S)}.$$

In this case, the theorem can be used to provide an explicit divisibility criterion for the indices of the considered orders. The simplest situation is, of course, the case when $\delta_S = 1$. In this situation, we receive the following corollary.

Corollary 6.12.
Let $\mathbb{Q} \subseteq K_0 \subseteq K$ be number fields, where K_0 is of degree n over $\mathbb{Q}$ and K is a degree m Galois extension of K_0. Let S be an order of K which is stable under the Galois group $\mathrm{Gal}(K/K_0)$*, and let $S_0 := S \cap K_0$. Then $[\, S^* \,:\, S_0^* S \,]$ is an integer and if $\delta_S = 1$, then*

$$[\, S^* \,:\, S_0^* S \,]\, [\, \mathcal{O}_{K_0} \,:\, S_0 \,]^{2m} \;=\; \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\, [\, \mathcal{O}_K \,:\, S \,]^2 \,.$$

There are two explicit situations in which we know that $\delta_S = 1$ and where Corollary 6.12 can be applied. These are stated in the next two theorems.

Theorem 6.13.
Let $\mathbb{Q} \subseteq K_0 \subseteq K$ be number fields, where K_0 is of degree n over $\mathbb{Q}$ and K is a degree m Galois extension of K_0. Let S be an order in K, and let $S_0 := S \cap \mathcal{O}_{K_0}$. If S_0 is Gorenstein, then $\delta_S = 1$.

Proof. Let S_0 be Gorenstein. Then S_0^* is invertible as a fractional ideal of S_0 and also $S_0^*\, S$ is invertible as a fractional ideal of S. This implies that $\delta(S_0^*) = 1 = \delta(S_0^* S)$ and hence

$$\delta_S = \frac{\delta(S_0^*)^m}{\delta(S_0^* S)} = \frac{1^m}{1} = 1\,.$$

□

It is worth mentioning that, in the situation of Theorem 6.11, if $n = 2$, as in the original result [BS17][Lemma 13], every order S_0 in K_0 is Gorenstein and comes with an invertible trace dual S_0^*. Consequently, $\delta_S = 1$. This is not true if $n \geq 3$.

Note that since $(S_0^* \mathcal{O}_{K_0})\mathcal{O}_K = S_0^* \mathcal{O}_K$ we have

$$[\,\mathcal{O}_K \,:\, S_0^* \mathcal{O}_K\,] = [\,\mathcal{O}_{K_0} \,:\, S_0^* \mathcal{O}_{K_0}\,]^m\,,$$

which implies that

$$\delta_S := \frac{\delta(S_0^*)^m}{\delta(S_0^* S)} = \frac{[\,S \,:\, S_0^* S\,]}{[\,S_0 \,:\, S_0^*\,]^m}\,.$$

If we assume in addition that K is a CM field containing an imaginary quadratic subfield k such that $K = k\, K_0$, we obtain the following result.

Theorem 6.14.
Let K be a CM field of degree $2n$ containing an imaginary quadratic subfield k such that $K = k\, K_0$, where $K_0 = \mathbb{Q}(\beta)$ denotes the maximal totally real subfield of K. Let S_k be an order in k, and let S_0 be an order in K_0. If $S = S_k\, S_0$, then $\delta_S = 1$.

Proof. Let S_0^* be the trace dual of S_0, which is a fractional ideal of S_0 and, consequently, we have $S_0^* S_0 = S_0^*$. Then $S_0^* S = S_0^*(S_0\, S_k) = S_0^*\, S_k$. We let $\mathcal{O}_k = \langle 1, \zeta \rangle_{\mathbb{Z}}$ for some integral $\zeta \in k$ and without loss of generality, we assume that $S_k = \langle 1, \ell\, \zeta \rangle_{\mathbb{Z}}$ for some $\ell > 0$. Additionally, we may also assume that

$$S_0 = \langle 1, s_{0,1}, \ldots, s_{0,n-1} \rangle_{\mathbb{Z}}$$

for some $s_{0,1}, \ldots, s_{0,n-1} \in \mathcal{O}_{K_0}$. Combining both sets of generators, we receive that

$$S = S_0\, S_k = \langle 1, s_{0,1}, \ldots, s_{0,n-1}, \ell\, \zeta, \ell\, \zeta\, s_{0,1}, \ldots, \ell\, \zeta\, s_{0,n-1} \rangle_{\mathbb{Z}}\,.$$

On the other hand, if $S_0^* = \langle s_{0,0}^*, s_{0,1}^*, \ldots, s_{0,n-1}^* \rangle_{\mathbb{Z}}$, then

$$S_0^* S = S_0^* S_k = \langle s_{0,0}^*, s_{0,1}^*, \ldots, s_{0,n-1}^*, \ell\,\zeta\, s_{0,0}^*, \ell\,\zeta\, s_{0,1}^*, \ldots, \ell\,\zeta\, s_{0,n-1}^* \rangle_{\mathbb{Z}}\,.$$

Moreover, those generators of $S_0^* S$ form a $\mathbb{Z}$-basis of $S_0^* S$. Let M denote the transformation matrix of S_0 with respect to $(1, \beta, \beta^2, \ldots, \beta^{n-1})$, where β was chosen to be a primitive element of K_0 over $\mathbb{Q}$, and let $T := (\mathrm{Tr}_{K_0/\mathbb{Q}}\, \beta^{i+j})_{i,j=0}^{n-1}$. Then $[\, S_0 \,:\, S_0^* \,]$ is the absolute value of the determinant of the matrix P such that $M\,P = (M\,T)^{-1}$. As M is invertible, the last equation is equivalent to $P = M^{-1}\,T^{-1}\,M^{-1}$. Hence,

$$[\, S_0 \,:\, S_0^* \,] = |\det(M)^{-2}\, \det(T)^{-1}|\,.$$

Now the transformation matrix of the basis of S into the basis of $S_0^* S$ is the following block matrix:

$$\begin{pmatrix} (M^2 T)^{-1} & 0 \\ 0 & (M^2 T)^{-1} \end{pmatrix}.$$

The index $[\, S \,:\, S_0^* S \,]$ is now the absolute value of the determinant of this block matrix, which is

$$[\, S \,:\, S_0^* S \,] = |\det((M^2 T)^{-1})|^2 = |\det(M)^{-2} \det(T)^{-1}|^2 = [\, S_0 \,:\, S_0^* \,]^2\,.$$

Therefore, we receive that

$$\delta_S = \frac{\delta(S_0^*)^2}{\delta(S_0^* S)} = 1\,.$$

□

We have thus given two different situations in which we find that $\delta_S = 1$ and, combining this with Corollary 6.12, we receive the following two theorems starting with the consequences of Theorem 6.13.

Theorem 6.15.
Let $\mathbb{Q} \subseteq K_0 \subseteq K$ be number fields, where K_0 is of degree n over $\mathbb{Q}$, and K is a degree m Galois extension of K_0. Let S be an order of K stable under the Galois group $\mathrm{Gal}(K/K_0)$ *and such that $S_0 := S \cap K_0$ is Gorenstein. Then $[\, S^* \,:\, S_0^* S \,]$ is an integer, and*

$$[\, S^* \,:\, S_0^* S \,]\, [\, \mathcal{O}_{K_0} \,:\, S_0 \,]^{2m} \;=\; \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\, [\, \mathcal{O}_K \,:\, S \,]^2\,.$$

As every order in a quadratic number field is Gorenstein, this generalizes the result of [BS17][Lemma 13]. On the other hand, we receive the following theorem combining Theorem 6.14 with Corollary 6.12.

Theorem 6.16.
Let K be a sextic CM field with totally real cubic subfield K_0 containing an imaginary quadratic subfield $k = \mathbb{Q}(\zeta)$. Let S_0 be an order in K_0, let S_k be an order in k, and let $S := S_0\, S_k \subseteq \mathcal{O}_K$ be stable under complex conjugation. Then $S \cap K_0 = S_0$, and $[\, S^* \,:\, S_0^* S\,]$ is an integer such as

$$[\, S^* \,:\, S_0^* S\,]\,[\, \mathcal{O}_{K_0} \,:\, S_0\,]^{2m} \;=\; \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,[\, \mathcal{O}_K \,:\, S\,]^2\,.$$

We give a significant explicit class of examples for Theorem 6.16 in which S_0 is not Gorenstein, but we still have $\delta_S = 1$.

Example 6.17.
Let K be a cyclic sextic CM class number one field containing an imaginary quadratic subfield $k = \mathbb{Q}(\zeta) \in \{\mathbb{Q}(i), \mathbb{Q}(\zeta_3)\}$, and let $K_0 = \mathbb{Q}(\beta)$ be the totally real cubic subfield of K such that $K = k\, K_0$. Let p be a prime number and

$$S \;=\; \langle 1, p\,\beta, p\,\beta^2, \zeta, \zeta\,p\,\beta, \zeta\,p\,\beta^2 \rangle_{\mathbb{Z}}\,.$$

Then, due to [JT15][Example 7.2] (see also Theorem 2.7), $S_0 = S \cap K_0 = \langle 1, p\,\beta, p\,\beta^2 \rangle_{\mathbb{Z}}$ is an order in K_0 which is not Gorenstein. Additionally, S is stable under complex conjugation and, due to Theorem 6.16, we obtain

$$\delta_S = \frac{\delta(S_0^*)^2}{\delta(S_0^* S)} = 1.$$

Hence, $[\, S^* \,:\, S_0^* S\,]$ is an integer and

$$[\, S^* \,:\, S_0^* S\,]\,[\, \mathcal{O}_{K_0} \,:\, S_0\,]^{2m} \;=\; \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,[\, \mathcal{O}_K \,:\, S\,]^2\,.$$

It remains to give some examples for δ_S in situations where one can neither apply Theorem 6.13 nor Theorem 6.14. We let K be a cyclic sextic CM field containing an imaginary quadratic subfield k and let K_0 be the totally real cubic subfield of K. Let S_0 be an order of K_0 and let S_k be an order of k. Then, since k is a quadratic extension of $\mathbb{Q}$, S_k is Gorenstein, and if S_0 is Gorenstein, then $S = S_0\, S_k$ is a Gorenstein order in K (see Proposition 1.33). Equivalently, if $S = S_0\, S_k$ is not Gorenstein, then S_0 is not Gorenstein. We make use of the examples in Chapter 1.1.3 and computed δ_S for every prime $p \leq 10^4$. The results are presented in the following examples.

Example 6.18.
Let $K = \mathbb{Q}(\alpha)$ be a cyclic sextic CM class number one field containing an imaginary quadratic subfield $k = \mathbb{Q}(i)$, and let K_0 be the totally real cubic subfield of K such that $K = k\,K_0$. Let $p \leq 10^4$ be a prime number, and let

$$S \;=\; \langle 1, p\,\alpha, p\,\alpha^2, p\,\alpha^3, p\,\alpha^4, p\,\alpha^5 \rangle_{\mathbb{Z}}\,.$$

Then S and $S_0 = S \cap K_0$ are not Gorenstein and

$$\delta_S = \frac{\delta(S_0^*)^2}{\delta(S_0^* S)} = p\,.$$

Example 6.19.
Let $K = \mathbb{Q}(\alpha)$ be a cyclic sextic CM class number one field containing an imaginary quadratic subfield $k = \mathbb{Q}(\zeta_3)$, and let K_0 be the totally real cubic subfield of K such that $K = k\,K_0$. Let $p \leq 10^4$ be a prime number, and let

$$S \;=\; \langle 1, p\,\alpha, p\,\alpha^2, p\,\alpha^3, p\,\alpha^4, p\,\alpha^5 \rangle_{\mathbb{Z}}\,.$$

Then S and $S_0 = S \cap K_0$ are not Gorenstein and

$$\delta_S = \frac{\delta(S_0^*)^2}{\delta(S_0^* S)} \in \left\{ p\,,\, \frac{p}{3} \right\}\,.$$

If we want to make sure that S is also stable under complex conjugation, we may take a look at the following example. Again, we computationally verified the correctness of this example for all $p \leq 10^4$.

Example 6.20.
Let $K = \mathbb{Q}(\alpha)$ be a cyclic sextic CM class number one field containing an imaginary quadratic subfield $k = \mathbb{Q}(i)$, and let K_0 be the totally real cubic subfield of K such that $K = k\,K_0$. Let $p \leq 10^4$ be a prime number, and let

$$S' \;=\; \langle 1, p\,\alpha, p\,\alpha^2, p\,\alpha^3, p\,\alpha^4, p\,\alpha^5 \rangle_{\mathbb{Z}}\,.$$

Then $S := S' + \bar{S}'$ and $S_0 = S \cap K_0$ are not Gorenstein, S is stable under complex conjugation and

$$\delta_S = \frac{\delta(S_0^*)^2}{\delta(S_0^* S)} = p\,.$$

Observe that, due to their construction, the orders S in Example 6.17 and Example 6.20 are stable under complex conjugation, making them applicable to Theorem 6.11. This demonstrates that even when $\delta_S \neq 1$, given a certain structure of S, we

can still derive divisibility conditions. Generally, beside the cases from Theorem 6.15 and Theorem 6.16 which are manageable, the parameter δ_S in Theorem 6.11 remains unbounded. Thus, in order to achieve a divisibility criterion as in Corollary 6.12, additional constraints on S are necessary, such as setting a specific δ_S or assuming that S_0 is Gorenstein.

Chapter 7

Bounding the index of relative orders

In this chapter, following the notation from Chapter 6, we concentrate on decomposing the indices $[\,R\,:\,S\,]$ and $[\,R_0\,:\,S_0\,]$, where $S \subseteq R$ are orders in a complex multiplication field K, and R_0 as well as S_0 are their restrictions to the largest totally real subfield K_0 of K. Initially, we delve into the primary decomposition of ideals within orders. Afterwards, we will establish bounds on both the domain and codomain of the relative norm at prime numbers p, as highlighted in Definition 5.1. We then deduce constraints on the indices of relative orders under the assumption that the kernel of the relative norm has an exponent smaller or equal to two. This is a condition that is satisfied by CM class number one orders as discussed in Chapter 5. Concluding this chapter, we apply our results to situations where K is a cyclic sextic CM field, presenting explicit bounds on the quotient of the indices $[\,R\,:\,S\,]$ and $[\,R_0\,:\,S_0\,]$, as well as on the index $[\,R\,:\,S\,]$ directly. The basic ideas are due to the findings in [Ste08] and [BS17]. They are also inspired by [Ste12].

7.1 Primary decomposition

Within this section, we let R be an order in a number field K, and we let I be an integral R-ideal. The ideas mainly follow the considerations in [Ste08][Chapter 5].

Definition 7.1.
Let R be an order in a number field K, and let I be an integral R-ideal. For any prime ideal $\mathfrak{q}$ of R we define the $\mathfrak{q}$-*primary part of* I to be the restriction of the localization of I at a prime ideal $\mathfrak{q}$:

$$I_{(\mathfrak{q})} := I_{\mathfrak{q}} \cap R.$$

Recall that an order R in a number field is a Dedekind domain if it is maximal. Consequently, an arbitrary order in a number field does not necessarily have a unique factorization into prime ideals. However, being a Noetherian domain, it will yield a factorization into $\mathfrak{q}$-primary components, as highlighted in the following lemma, which is sourced from [Ste08][Lemma 5.1]. It is noteworthy that $I_{(\mathfrak{q})} = R$ for all prime ideals $\mathfrak{q}$ not containing I.

Lemma 7.2.
Let K be a number field and $R_\mathfrak{q}$ be a localization of an order $R \subseteq \mathcal{O}_K$ at a prime ideal $\mathfrak{q} \leq R$. Then every non-zero ideal $I_\mathfrak{q}$ of $R_\mathfrak{q}$ contains some power of the unique maximal ideal $\mathfrak{q}\, R_\mathfrak{q}$.

In particular, this lemma shows that the $\mathfrak{q}$-primary part $I_{(\mathfrak{q})}$ of an ideal $I \subsetneq R$ contains some power or $\mathfrak{q}$. There are no inclusion between different prime ideals in orders. Hence, $\mathfrak{q}$-primary parts at different prime ideals $\mathfrak{q}$ are coprime. This brings us to the following result, which can be found in [Ste08][Theorem 5.2].

Theorem 7.3.
Let K be a number field, let $R \subseteq \mathcal{O}_K$ be an order, and let $I \lneq R$ be a non-zero ideal of R. Then I has a decomposition in $\mathfrak{q}$-primary parts as follows:

$$I = \prod_{\substack{\mathfrak{q} \supseteq I \\ \mathfrak{q} \leq R \text{ prime}}} I_{(\mathfrak{q})} \quad \text{and} \quad R/I \cong \prod_{\substack{\mathfrak{q} \supseteq I \\ \mathfrak{q} \leq R \text{ prime}}} R/I_{(\mathfrak{q})} \cong \prod_{\substack{\mathfrak{q} \supseteq I \\ \mathfrak{q} \leq R \text{ prime}}} R_\mathfrak{q}/I_\mathfrak{q}\,.$$

For some positive integers $n \in \mathbb{Z}$ sufficiently large, we have

$$I_{(\mathfrak{q})} := I_\mathfrak{q} \cap R = (I \cdot R_\mathfrak{q}) \cap R = I + \mathfrak{q}^n.$$

Definition 7.4.
Let R be an order in a number field K, and let I be an integral ideal of R. A decomposition of I into $\mathfrak{q}$-primary parts is called *primary decomposition of I*.

This primary decomposition extends the unique factorization of an ideal into powers of prime ideals, covering a larger class of rings beyond unique factorization domains or Dedekind rings. By grouping the $\mathfrak{q}$-primary parts of the prime ideals $\mathfrak{q}$ that lie over the same prime number, we introduce the following notation.

Definition 7.5.
Let K be a number field, let R be an order in K, and let I be an integral ideal of R. For any prime number $p \in \mathbb{Z}$, we define

$$I_{(p)} := \prod_{\substack{\mathfrak{q} \leq R \text{ prime} \\ \mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}}} I_{(\mathfrak{q})}.$$

It is crucial to note that, under the conditions of Theorem 7.3, the ring R/I is finite, and $R/I_{(\mathfrak{q})}$ is a finite local ring with the unique maximal ideal $\mathfrak{q} + I_{(\mathfrak{q})}$. Building on the discussions on finite rings in Chapter 1.2, we arrive at the following crucial consequences.

Corollary 7.6.
Let R be an order in a number field K, and let I be an integral ideal of R. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideal of R lying above I. Then

$$\left| \left(R \diagup I \right)^\times \right| = \left| \left(R \diagup I \right) \right| \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{N(\mathfrak{p}_i)} \right) .$$

Proof. We have that $\tilde{R} := R/I$ is a finite ring, and the prime ideals of $\tilde{R}$ are precisely the images of the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ under the canonical projection $R \to R/I$. Applying Proposition 1.2 proves the claim. □

Theorem 7.7.
Let R be an order in a number field K, and let I be an integral ideal of R. For any prime number $p \in \mathbb{Z}$ and prime ideal $\mathfrak{q} \leq R$ containing I such that $\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$, we have

$$\left(R \diagup I_{(\mathfrak{q})} \right)^\times \cong \left(R \diagup \mathfrak{q} \right)^\times \times \left(1 + \mathfrak{q} \right) \diagup \left(1 + I_{(\mathfrak{q})} \right) .$$

Moreover,

$$\left| \left(R \diagup \mathfrak{q} \right)^\times \right| = p^r - 1 \quad \text{and} \quad \left| \left(1 + \mathfrak{q} \right) \diagup \left(1 + I_{(\mathfrak{q})} \right) \right| = p^s$$

for some $r, s \in \mathbb{Z}_{\geq 0}$.

Proof. Let $p \in \mathbb{Z}$ be a prime number and $\mathfrak{q}$ be a prime ideal of R with $\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$. We aim to apply Theorem 1.36 in order to show the existence of the following exact sequence

$$1 \longrightarrow \left(1 + \mathfrak{q} \right) \diagup \left(1 + I_{(\mathfrak{q})} \right) \longrightarrow \left(R \diagup I_{(\mathfrak{q})} \right)^\times \longrightarrow \left(R \diagup \mathfrak{q} \right)^\times \longrightarrow 1 . \tag{7.1}$$

On the one hand, the unique maximal ideal of $R/I_{(\mathfrak{q})}$ is given by $\mathfrak{m} := \mathfrak{q} + I_{(\mathfrak{q})}$ since

it corresponds to the maximal ideal $\mathfrak{q}R_\mathfrak{q} + I_\mathfrak{q}$ of $R_\mathfrak{q}/I_\mathfrak{q}$. On the other hand,

$$(1+\mathfrak{q})\big/(1+I_{(\mathfrak{q})}) \cong 1+\mathfrak{q}+I_{(\mathfrak{q})} = 1+\mathfrak{m},$$

because $1+I_{(\mathfrak{q})}$ is the kernel of the epimorphism $1+\mathfrak{q} \longrightarrow 1+\mathfrak{q}+I_{(\mathfrak{q})}$. Furthermore,

$$R\big/\mathfrak{q} \cong \left(R\big/I_{(\mathfrak{q})}\right)\Big/(\mathfrak{q}+I_{(\mathfrak{q})})\,.$$

Applying Theorem 1.36 leads to the exactness of the sequence in (7.1). The group $(R/\mathfrak{q})^\times$ is the multiplicative cyclic group of the finite field $R/\mathfrak{q}$. Since $\mathfrak{m}$ is the maximal ideal of a finite local ring of characteristic p, it is a p-group. Consequently,

$$1+\mathfrak{m} \cong (1+\mathfrak{q})\big/(1+I_{(\mathfrak{q})}),$$

and it is also a p-group. □

7.2 Decomposing the index of relative orders

We can now decompose the index of relative orders $S \subseteq R$ in a number field K, applying the primary decomposition of a specific integral ideal.

Corollary 7.8.
Let $S \subseteq R$ be orders in a number field K, and let $I \subsetneq S$ be an integral ideal of R. Then I is also an integral ideal of S, and I provides a primary decomposition in both R and S such that

$$I = \prod_{p\in\mathbb{Z}\ prime} I_{(p)} = \prod_{p\in\mathbb{Z}\ prime} \prod_{\substack{\mathfrak{p}\leq R\ prime\\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} I_{(\mathfrak{p})} \quad \textit{and}$$
$$I = \prod_{q\in\mathbb{Z}\ prime} I_{(q)} = \prod_{q\in\mathbb{Z}\ prime} \prod_{\substack{\mathfrak{q}\leq S\ prime\\ \mathfrak{q}\cap\mathbb{Z}=q\mathbb{Z}}} I_{(\mathfrak{q})}\,.$$

Furthermore, we have

$$R\big/I \cong \prod_{p\in\mathbb{Z}\ prime} R\big/I_{(p)} \cong \prod_{p\in\mathbb{Z}\ prime} \prod_{\substack{\mathfrak{p}\leq R\ prime\\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} R\big/I_{(\mathfrak{p})} \quad \textit{and}$$
$$S\big/I \cong \prod_{q\in\mathbb{Z}\ prime} S\big/I_{(q)} \cong \prod_{q\in\mathbb{Z}\ prime} \prod_{\substack{\mathfrak{q}\leq S\ prime\\ \mathfrak{q}\cap\mathbb{Z}=q\mathbb{Z}}} S\big/I_{(\mathfrak{q})}\,.$$

Proof. Given that $I \subsetneq S \subseteq R$ and that I is an integral ideal of R, it is especially an integral ideal of S. According to Theorem 7.3, I provides a primary decomposition

in both R and S such that

$$I = \prod_{p\in\mathbb{Z} \text{ prime}} I_{(p)} = \prod_{p\in\mathbb{Z} \text{ prime}} \prod_{\substack{\mathfrak{p}\leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} I_{(\mathfrak{p})} \quad \text{and}$$
$$I = \prod_{q\in\mathbb{Z} \text{ prime}} I_{(q)} = \prod_{q\in\mathbb{Z} \text{ prime}} \prod_{\substack{\mathfrak{q}\leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z}=q\mathbb{Z}}} I_{(\mathfrak{q})}\,.$$

Consequently, by factoring the orders with I, we derive the following decompositions of finite rings:

$$R/I \cong \prod_{p\in\mathbb{Z} \text{ prime}} R/I_{(p)} \cong \prod_{p\in\mathbb{Z} \text{ prime}} \prod_{\substack{\mathfrak{p}\leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} R/I_{(\mathfrak{p})} \quad \text{and}$$
$$S/I \cong \prod_{q\in\mathbb{Z} \text{ prime}} S/I_{(q)} \cong \prod_{q\in\mathbb{Z} \text{ prime}} \prod_{\substack{\mathfrak{q}\leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z}=q\mathbb{Z}}} S/I_{(\mathfrak{q})}\,.$$

□

Definition 7.9.
For any $a \in \mathbb{Q}$, we define the p-part of a as $a_p := p^{v_p(a)}$, where $v_p(a)$ denotes the p-valuation of a. Especially, if we let S and R be orders in a number field K satisfying $S \subseteq R$, then we define the *p-part of the index* $[\,R : S\,] \in \mathbb{Z}$ to be

$$[\,R : S\,]_p := p^{v_p([\,R:S\,])}.$$

Thus, due to Corollary 7.8, we can express the index $[\,R : S\,]$ as follows.

Proposition 7.10.
Let $S \subseteq R$ be orders in a number field K, and let $I \subsetneq S$ be an integral ideal of R. Then, for every prime $p \in \mathbb{Z}$, we have

$$[\,R : S\,]_p = \left|R/I_{(p)}\right| \cdot \left|S/I_{(p)}\right|^{-1},$$

and the index can be decomposed in p-parts as

$$[\,R : S\,] = \prod_{p\in\mathbb{Z}\ prime} [\,R : S\,]_p\,.$$

Proof. As a consequence of Corollary 7.8, it is

$$[\,R : S\,] = \left|R/S\right| = \left|\left(R/I\right)/\left(S/I\right)\right| = \left|\left(\prod_{p\in\mathbb{Z} \text{ prime}} R/I_{(p)}\right)/\left(\prod_{q\in\mathbb{Z} \text{ prime}} S/I_{(q)}\right)\right|.$$

Given a prime $p \in \mathbb{Z}$ and any prime ideal $\mathfrak{p}$ of R satisfying $\mathfrak{p} \supseteq I$ and $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, there exists a prime ideal $\mathfrak{q}$ of S such that $\mathfrak{q} \supseteq I$, $\mathfrak{q} \cap \mathbb{Z} = p\mathbb{Z}$, and $I_{(\mathfrak{p})} \cap S = I_{(\mathfrak{q})}$. This allows us to express the index of S in R as:

$$[\,R\,:\,S\,] = \prod_{p\in\mathbb{Z} \text{ prime}} \left| \Big(R\big/I_{(p)}\Big) \Big/ \Big(S\big/I_{(p)}\Big) \right| = \prod_{p\in\mathbb{Z} \text{ prime}} \left(\left|R\big/I_{(p)}\right| \cdot \left|S\big/I_{(p)}\right|^{-1} \right) .$$

Applying the definition of the p-part of the index, we find that

$$[\,R\,:\,S\,]_p = \left|R\big/I_{(p)}\right| \cdot \left|S\big/I_{(p)}\right|^{-1}$$

and, consequently, it is

$$[\,R\,:\,S\,] = \prod_{p\in\mathbb{Z} \text{ prime}} [\,R\,:\,S\,]_p \,.$$

□

By further investigating the p-part of an index, we can conclude the following lemma.

Lemma 7.11.
Let $S \subseteq R$ be orders in a number field K, and let $I \subsetneq S$ be an integral ideal of R. Let $p \in \mathbb{Z}$ be a prime number. Then

$$[\,R\,:\,S\,]_p = \left|\Big(R\big/I_{(p)}\Big)\right|_p \left|\Big(S\big/I_{(p)}\Big)\right|_p^{-1} \prod_{\substack{\mathfrak{p}\leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} N(\mathfrak{p}) \prod_{\substack{\mathfrak{q}\leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z}=p\mathbb{Z}}} N(\mathfrak{q})^{-1}$$

Proof. As shown in Proposition 7.10 it is

$$[\,R\,:\,S\,]_p = \left|R\big/I_{(p)}\right| \cdot \left|S\big/I_{(p)}\right|^{-1} .$$

Applying Corollary 7.6 to both factors on the right-hand side, we receive that

$$\left|R\big/I_{(p)}\right| = \left|\Big(R\big/I_{(p)}\Big)^{\times}\right| \prod_{\substack{\mathfrak{p}\leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} \left(1 - \frac{1}{N(\mathfrak{p})}\right)^{-1} = \left|\Big(R\big/I_{(p)}\Big)^{\times}\right| \prod_{\substack{\mathfrak{p}\leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} \frac{N(\mathfrak{p})}{N(\mathfrak{p})-1} \quad \text{and}$$

$$\left|S\big/I_{(p)}\right| = \left|\Big(S\big/I_{(p)}\Big)^{\times}\right| \prod_{\substack{\mathfrak{q}\leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z}=p\mathbb{Z}}} \left(1 - \frac{1}{N(\mathfrak{q})}\right)^{-1} = \left|\Big(S\big/I_{(p)}\Big)^{\times}\right| \prod_{\substack{\mathfrak{q}\leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z}=p\mathbb{Z}}} \frac{N(\mathfrak{q})}{N(\mathfrak{q})-1} \,.$$

For all the prime ideals $\mathfrak{p} \leq R$ and $\mathfrak{q} \leq S$ lying above p, we have that $N(\mathfrak{p}) - 1$

and $N(\mathfrak{q}) - 1$ are not divisible by p. Thus, considering only the p-parts, delivers

$$\left|R/I_{(p)}\right|_p = \left|\left(R/I_{(p)}\right)^\times\right|_p \prod_{\substack{\mathfrak{p}\leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}}} N(\mathfrak{p}) \quad \text{and}$$
$$\left|S/I_{(p)}\right|_p = \left|\left(S/I_{(p)}\right)^\times\right|_p \prod_{\substack{\mathfrak{q}\leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z}=p\mathbb{Z}}} N(\mathfrak{q})\,.$$

□

After establishing our results for an arbitrary integral ideal I, we can now make these considerations explicit. This leads us to the main result of this section, which is inspired by [BS17][Proposition 10].

Lemma 7.12.
Let K be a number field of degree n over $\mathbb{Q}$, and let $S \subseteq R \subseteq T$ be orders in K. Let f be a multiple of $[\,T : S\,]$, and let $I := fT$. For every $p \mid f$ we have

$$[\,R : S\,]_p \left(1 - \frac{1}{p}\right)^n \leq \left|\left(R/I_{(p)}\right)^\times \Big/ \left(S/I_{(p)}\right)^\times\right| \leq [\,R : S\,]_p \left(1 - \frac{1}{p}\right)^{-n}.$$

Proof. Firstly, by definition, $I = fT$ is an integral ideal of T that is contained in both R and S. Let $p \in \mathbb{Z}$ be a prime number that divides f. Then we can apply Corollary 7.6 to obtain

$$\left|\left(R/I_{(p)}\right)^\times \Big/ \left(S/I_{(p)}\right)^\times\right| = \frac{\left|\left(R/I_{(p)}\right)\right|}{\left|\left(S/I_{(p)}\right)\right|} \cdot \frac{\prod_{\mathfrak{p}}(1 - \frac{1}{N(\mathfrak{p})})}{\prod_{\mathfrak{q}}(1 - \frac{1}{N(\mathfrak{q})})}, \tag{7.2}$$

where $\mathfrak{p}$ ranges overall prime ideals of R containing the integral ideal $I_{(p)}$ of R and $\mathfrak{q}$ ranges over all prime ideals of S containing the integral ideal $I_{(p)}$ of S.

There are at most n such primes each, and we can deduce the following bounds:

$$\left(1 - \frac{1}{p}\right)^n \leq \frac{\prod_{\mathfrak{p}}(1 - \frac{1}{N(\mathfrak{p})})}{\prod_{\mathfrak{q}}(1 - \frac{1}{N(\mathfrak{q})})} \leq \left(1 - \frac{1}{p}\right)^{-n}. \tag{7.3}$$

Multiplying this inequality by $[\,R : S\,]_p$ and applying Proposition 7.10 gives us

$$[\,R : S\,]_p \left(1 - \frac{1}{p}\right)^n \leq \frac{\left|\left(R/I_{(p)}\right)\right|}{\left|\left(S/I_{(p)}\right)\right|} \cdot \frac{\prod_{\mathfrak{p}}(1 - \frac{1}{N(\mathfrak{p})})}{\prod_{\mathfrak{q}}(1 - \frac{1}{N(\mathfrak{q})})} \leq [\,R : S\,]_p \left(1 - \frac{1}{p}\right)^{-n}.$$

Finally, by using equation (7.2), we obtain

$$[\,R\,:\,S\,]_p\left(1-\frac{1}{p}\right)^n \leq \left|\left(R/I_{(p)}\right)^\times / \left(S/I_{(p)}\right)^\times\right| \leq [\,R\,:\,S\,]_p\left(1-\frac{1}{p}\right)^{-n}.$$

□

It is noteworthy that we have presented this result for arbitrary orders T. In our application during the next sections, we will focus on the case where $T = \mathcal{O}_K$. Then f is the index of S in the maximal order $\mathcal{O}_K$ of K.

7.3 Bounding quotients of indices in CM fields

Let K be a CM field, and let $S \subseteq R$ be orders in K together with their restrictions S_0 and R_0 to the maximal totally real subfield K_0 of K. Let $f := [\,\mathcal{O}_K\,:\,S\,]$, and let $I := f\mathcal{O}_K$ such as $I_0 := f\mathcal{O}_{K_0}$.

In this section, we will apply the results from Section 7.2 to the domain and codomain of the relative norm, as outlined in Definition 5.1. Within the given framework, the relative norm is specified as:

$$\psi : \left(R/I\right)^\times / \left(S/I\right)^\times \mu_R \longrightarrow \left(R_0/I_0\right)^\times / \left(S_0/I_0\right)^\times.$$

In order to improve notation, we introduce two closely related maps.

Definition 7.13.
Let K be a CM field, and let $S \subseteq R$ be orders in K. Let S_0 and R_0 denote the restrictions of S and R to the maximal totally real subfield K_0 of K, respectively. Let $f := [\,\mathcal{O}_K\,:\,S\,]$, and let $I := f\mathcal{O}_K$ such as $I_0 := f\mathcal{O}_{K_0}$. Let $p \in \mathbb{Z}$ be a prime dividing f and $I_{(p)}$ such as $I_{0(p)}$ denote the p-parts of I and I_0, respectively. We define the following maps induced by the relative norm ψ:

$$\psi' : \left(R/I\right)^\times / \left(S/I\right)^\times \longrightarrow \left(R_0/I_0\right)^\times / \left(S_0/I_0\right)^\times,$$
$$\psi_p : \left(R/I_{(p)}\right)^\times / \left(S/I_{(p)}\right)^\times \longrightarrow \left(R_0/I_{0(p)}\right)^\times / \left(S_0/I_{0(p)}\right)^\times.$$

We let D and C represent the domain and the codomain of ψ', respectively. Additionally, we denote the domain of ψ_p as D_p and the codomain of ψ_p as C_p.

The p-parts of D and C are given by the domain D_p and the codomain C_p of ψ_p, respectively. Using these definitions, ψ' can be expressed as $\psi_{p_1} \times \cdots \times \psi_{p_r}$, where $p_1, \ldots, p_r$ are the primes dividing f. As a consequence, $\ker \psi'$ is isomorphic to $\prod_{p|f} \ker \psi_p$ and $\ker \psi$ is isomorphic to $\ker \psi'/(\mu_R/\{\pm 1\})$. Using this notation, we can now reformulate Lemma 7.12 to conclude initial bounds for D_p and C_p.

Corollary 7.14.
Let K be a CM field of degree $2n$ over $\mathbb{Q}$, and let $S \subseteq R$ be orders in K. Let S_0 and R_0 denote the restrictions of S and R to the maximal totally real subfield K_0 of K, respectively. Let $p \in \mathbb{Z}$ be a prime dividing f. Then

$$[\,R\,:\,S\,]_p \left(1-\frac{1}{p}\right)^{2n} \leq |D_p| \leq [\,R\,:\,S\,]_p \left(1-\frac{1}{p}\right)^{-2n}, \text{ and}$$
$$[\,R_0\,:\,S_0\,]_p \left(1-\frac{1}{p}\right)^{n} \leq |C_p| \leq [\,R_0\,:\,S_0\,]_p \left(1-\frac{1}{p}\right)^{-n}.$$

Proof. Let $f := [\,\mathcal{O}_K\,:\,S\,]$. By applying Lemma 7.12 to $I := f\mathcal{O}_K$, we deduce that

$$[\,R\,:\,S\,]_p \left(1-\frac{1}{p}\right)^{2n} \leq \left| \left(R/I_{(p)}\right)^{\times} \Big/ \left(S/I_{(p)}\right)^{\times} \right| \leq [\,R\,:\,S\,]_p \left(1-\frac{1}{p}\right)^{-2n}$$

The term in the center of this inequality represents the size of D_p. If we apply Lemma 7.12 to K_0, S_0, and R_0 with $I_0 := f\mathcal{O}_{K_0}$, we obtain the analogous result for C_p.

□

We are now in a position to state bounds on the primes that divide the quotient of the indices $[\,R\,:\,S\,]$ and $[\,R_0\,:\,S_0\,]$, given a certain constraint on the relative norm. This result generalized a similar result for quartic CM fields, which can be found in [BS17][Lemma 11].

Lemma 7.15.
Let K be a CM field of degree $2n$ over $\mathbb{Q}$, and let $S \subseteq R$ be orders in K. Let S_0 and R_0 denote the restrictions of S and R to the maximal totally real subfield K_0 of K, respectively. Let $f := [\,\mathcal{O}_K\,:\,S\,]$, and let $I := f\mathcal{O}_K$ such as $I_0 := f\mathcal{O}_{K_0}$. Let $p \in \mathbb{Z}$ be a prime dividing f and the kernel of ψ_p be of exponent at most two. If we denote by v_p the p-valuation of $[\,R\,:\,S\,]/[\,R_0\,:\,S_0\,]$, then

$$p^{v_p - 3n} \cdot (p-1)^{3n} \leq 2^{2n}.$$

Proof. As ψ_p is surjective, it is $|\ker \psi_p| \cdot |C_p| = |D_p|$. We apply Corollary 7.14, and we get

$$|\ker \psi_p| \geq \frac{[\,R\,:\,S\,]_p}{[\,R_0\,:\,S_0\,]_p} \cdot \frac{\left(1-\frac{1}{p}\right)^{2n}}{\left(1-\frac{1}{p}\right)^{-n}} = \frac{[\,R\,:\,S\,]_p}{[\,R_0\,:\,S_0\,]_p} \cdot \left(1-\frac{1}{p}\right)^{3n} . \tag{7.4}$$

Now $\ker \psi_p$ is generated by at most $2n$ elements of exponent at most two. Combining this with (7.4), we receive the following inequality:

$$2^{2n} \geq \frac{[\,R\,:\,S\,]_p}{[\,R_0\,:\,S_0\,]_p} \cdot \left(1-\frac{1}{p}\right)^{3n} = p^{v_p} \cdot \left(1-\frac{1}{p}\right)^{3n} . \tag{7.5}$$

By expanding the right hand side, inequality (7.5) is equivalent to our claim. □

Note that assuming the kernel of the relative norm ψ to be of exponent two does not imply that the kernel of ψ_p is of exponent at most two. But we do have the following lemma.

Lemma 7.16.
Let K be a CM field of degree $2n$ over $\mathbb{Q}$, and let $S \subseteq R$ be orders in K. Let S_0 and R_0 denote the restrictions of S and R to the maximal totally real subfield K_0 of K, respectively. Let $f := [\,\mathcal{O}_K\,:\,S\,]$ and $I := f\mathcal{O}_K$ such as $I_0 := f\mathcal{O}_{K_0}$. Let $p \in \mathbb{Z}$ be a prime dividing f and the kernel of ψ be of exponent at most two. If we denote by v_p the p-valuation of $[\,R\,:\,S\,]/[\,R_0\,:\,S_0\,]$, then

$$p^{v_p-3n} \cdot (p-1)^{3n} \leq 2^{2n-1} \cdot |\mu_R| .$$

Proof. As in the proof of Lemma 7.15, we have

$$|\ker \psi_p| \geq p^{v_p} \cdot \left(1-\frac{1}{p}\right)^{3n} . \tag{7.6}$$

As the kernel of ψ has an exponent of at most two, so has the group $\ker \psi_p/(\mu_R/\{\pm 1\})$. Now $\ker \psi_p/(\mu_R/\{\pm 1\})$ is generated by at most $2n$ elements of exponent at most two, such that

$$2^{2n} \geq \left| \ker \psi_p \Big/ \left(\mu_R \Big/ \{\pm 1\}\right) \right| = |\ker \psi_p| \cdot 2\,|\mu_R|^{-1} . \tag{7.7}$$

Now, combining (7.6) with (7.7) proves our claim:

$$p^{v_p} \cdot \left(1 - \frac{1}{p}\right)^{3n} \leq 2^{2n-1} \cdot |\mu_R| \ .$$

□

In other words, under the condition that the kernel of the relative norm ψ is of exponent at most two, then there are only finitely many primes p at which

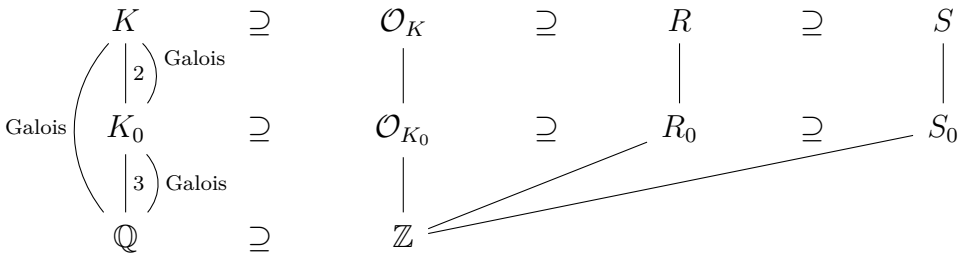
$$[\, R \,:\, S \,]_p \neq [\, R_0 \,:\, S_0 \,]_p \,,$$

and we do have an explicit bound on those primes and their multiplicities.

7.4 Bounding the index of orders in cyclic sextic CM fields

Until now, we have considered arbitrary CM fields. In this section, we will delve into a specific scenario. We let K be a cyclic sextic CM field with its totally real cubic subfield K_0, and let $S \subseteq R$ be orders in K. As before, we use S_0 and R_0 to denote their restrictions to K_0. We describe the prime splitting behavior in this context, and we apply our previous findings to provide bounds on the primes potentially dividing the index $[\, R \,:\, S \,]$ as well as their exponents.

Now, since K is a cyclic sextic CM field, its subfield K_0 is also cyclic and Galois over $\mathbb{Q}$. This property simplifies our investigation of the explicit splitting behavior of primes. The following diagram provides an overview of the situation.



7.4.1 Splitting behavior of primes

We assume the situation to be as defined at the beginning of Section 7.4. Now, we let $p \in \mathbb{Z}$ be a prime number, and let $\mathfrak{P} \leq \mathcal{O}_K$ be a prime ideal such that $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Its restrictions to R and S are denoted as $\mathfrak{p}$ and $\mathfrak{q}$, respectively. Both $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals. Thus, the corresponding residue fields satisfy:

$$\mathcal{O}_K/\mathfrak{P} \supseteq R/\mathfrak{p} \supseteq S/\mathfrak{q} \,.$$

Similarly, for the residue fields associated with the prime ideals $\mathfrak{P}_0 := \mathfrak{P} \cap \mathcal{O}_{K_0}$ of $\mathcal{O}_{K_0}$, $\mathfrak{p}_0 := \mathfrak{p} \cap R_0$ of R_0, and $\mathfrak{q}_0 := \mathfrak{q} \cap S_0$ of S_0, we have:

$$\mathcal{O}_K \big/ \mathfrak{P} \supseteq \mathcal{O}_{K_0} \big/ \mathfrak{P}_0, \quad R \big/ \mathfrak{p} \supseteq R_0 \big/ \mathfrak{p}_0, \quad \text{and} \quad S \big/ \mathfrak{q} \supseteq S_0 \big/ \mathfrak{q}_0 \,.$$

Considering the unit groups of the respective fields, we observe the following relationships:

$$\left(\mathcal{O}_K \big/ \mathfrak{P}\right)^\times \supseteq \left(R \big/ \mathfrak{p}\right)^\times \supseteq \left(S \big/ \mathfrak{q}\right)^\times .$$

Furthermore,

$$\left(\mathcal{O}_K \big/ \mathfrak{P}\right)^\times \supseteq \left(\mathcal{O}_{K_0} \big/ \mathfrak{P}_0\right)^\times, \quad \left(R \big/ \mathfrak{p}\right)^\times \supseteq \left(R_0 \big/ \mathfrak{p}_0\right)^\times, \quad \text{and} \quad \left(S \big/ \mathfrak{q}\right)^\times \supseteq \left(S_0 \big/ \mathfrak{q}_0\right)^\times .$$

On the one hand, all the above-mentioned fields are of cardinality p^s for some $s \in \mathbb{N}$, and their corresponding unit groups have a cardinality $p^s - 1$. This provides several conditions on the divisibility of the cardinalities.

On the other hand, the well-known fundamental equation for Galois extensions (see [Neu99][Theorem 8.2, Chapter 1]) gives additional conditions on the splitting behavior of prime ideals in maximal orders.

Proposition 7.17.
Let K be a cyclic sextic CM field, and let K_0 be its totally real cubic subfield. Let $p \in \mathbb{Z}$ be a prime number, and let $p\mathcal{O}_{K_0} = \prod_{i=1}^{r_0} \mathfrak{P}_{0,i}^{e_{0,i}}$ be the unique prime ideal factorization in $\mathcal{O}_{K_0}$, such as $f_{0,i} := [\,\mathcal{O}_{K_0}/\mathfrak{P}_{0,i} : \mathbb{Z}/p\mathbb{Z}\,]$. Then we have $e_{0,1} = \ldots = e_{0,r_0} =: e_0$ such as $f_{0,1} = \ldots = f_{0,r_0} =: f_0$, and $3 = r_0\, e_0\, f_0$. Furthermore, p splits in $\mathcal{O}_{K_0}$ in one of the following three ways:

(a) *If $r_0 = 3$, then $e_0 = 1 = f_0$ and $p\,\mathcal{O}_{K_0} = \prod_{i=1}^{3} \mathfrak{P}_{0,i}$ for some prime ideals $\mathfrak{P}_{0,i}$ of $\mathcal{O}_{K_0}$ lying above p. For all three residue fields, we receive that $|\mathcal{O}_{K_0}/\mathfrak{P}_{0,i}| = p$ and $\left|(\mathcal{O}_{K_0}/\mathfrak{P}_{0,i})^\times\right| = p - 1$.*

(b) *If $e_0 = 3$ then $r_0 = 1 = f_0$ and $p\,\mathcal{O}_{K_0} = \mathfrak{P}_0^3$ for a prime ideal $\mathfrak{P}_0$ of $\mathcal{O}_{K_0}$ lying above p. Accordingly, for the residue field, we get $|\mathcal{O}_{K_0}/\mathfrak{P}_0| = p$ and $\left|(\mathcal{O}_{K_0}/\mathfrak{P}_0)^\times\right| = p - 1$.*

(c) *If $f_0 = 3$ then $r_0 = 1 = e_0$ and $p\,\mathcal{O}_{K_0} = \mathfrak{P}_0$ for some prime ideal $\mathfrak{P}_0$ of $\mathcal{O}_{K_0}$ lying above p. Considering the residue field, we receive $|\mathcal{O}_{K_0}/\mathfrak{P}_0| = p^3$ and $\left|(\mathcal{O}_{K_0}/\mathfrak{P}_0)^\times\right| = p^3 - 1$.*

Proof. Given that K_0 is a Galois extension of $\mathbb{Q}$, we can apply the fundamental equation for Galois extensions. This implies $e_{0,1} = \ldots = e_{0,r_0} =: e_0$ such as $f_{0,1} = \ldots = f_{0,r_0} =: f_0$, and we have the relationship $3 = r_0\, e_0\, f_0$. Evaluating the remaining possible combinations of r_0, e_0, and f_0, we have proved the stated claim. □

Building on this, we can explore the possibilities for a prime ideal $\mathfrak{P}_0$ of $\mathcal{O}_{K_0}$ that lies above p when it is lifted to $\mathcal{O}_K$. Again, there are three different ways in which this can happen. These three ways are similar to our previous considerations, as we are once again considering a Galois extension. The only difference now is that the extension is of degree two, not three.

Proposition 7.18.
Let K be a cyclic sextic CM field, and let K_0 be its totally real cubic subfield. Let $p \in \mathbb{Z}$ be a prime number, and let $\mathfrak{P}_0 \leq \mathcal{O}_{K_0}$ be a prime ideal above p. Let $\mathfrak{P}_0\mathcal{O}_K = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ be the unique prime ideal factorization in $\mathcal{O}_K$ such as $f_i := [\,\mathcal{O}_K/\mathfrak{P}_i \,:\, \mathcal{O}_{K_0}/\mathfrak{P}_0\,]$. Then $e_1 = \ldots = e_r =: e$ and $f_1 = \ldots = f_r =: f$ such as $2 = r\,e\,f$. Furthermore, $\mathfrak{P}_0\mathcal{O}_K$ splits in $\mathcal{O}_K$ in one of the following ways:

(a) *If $r = 2$, then $e = 1 = f$, and $\mathfrak{P}_0\,\mathcal{O}_K = \prod_{i=1}^{2} \mathfrak{P}_i$ for prime ideals $\mathfrak{P}_i$ of $\mathcal{O}_K$ lying above $\mathfrak{P}_0$. For both residue fields, we have $|\mathcal{O}_K/\mathfrak{P}_i| = |\mathcal{O}_{K_0}/\mathfrak{P}_0|$ and $\left|(\mathcal{O}_K/\mathfrak{P}_i)^\times\right| = \left|(\mathcal{O}_{K_0}/\mathfrak{P}_0)^\times\right|$.*

(b) *If $e = 2$, then $r = 1 = f$, and $\mathfrak{P}_0\,\mathcal{O}_K = \mathfrak{P}^2$ for a prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying above $\mathfrak{P}_0$. For the residue field, we get $|\mathcal{O}_K/\mathfrak{P}| = |\mathcal{O}_{K_0}/\mathfrak{P}_0|$ and $\left|(\mathcal{O}_K/\mathfrak{P})^\times\right| = \left|(\mathcal{O}_{K_0}/\mathfrak{P}_0)^\times\right|$.*

(c) *If $f = 2$, then $r = 1 = e$, and $\mathfrak{P}_0\,\mathcal{O}_K = \mathfrak{P}$ for some prime ideal $\mathfrak{P}$ of $\mathcal{O}_K$ lying above $\mathfrak{P}_0$. Additionally, the residue field fulfills $|\mathcal{O}_K/\mathfrak{P}| = |\mathcal{O}_{K_0}/\mathfrak{P}_0|^2$ and $\left|(\mathcal{O}_K/\mathfrak{P})^\times\right| = |\mathcal{O}_{K_0}/\mathfrak{P}_0|^2 - 1$.*

Proof. Given that K is a Galois extension of K_0, we can use the fundamental equation for Galois extensions. This implies the equalities $e_1 = \ldots = e_r =: e$ such as $f_1 = \ldots = f_r =: f$, and we have the relationship $2 = r\,e\,f$. By evaluating the remaining potential combinations of r, e, and f, we have proved the claim. □

7.4.2 Bound quotients of indices

We are now prepared to prove the main results of this chapter. Initially, we will consider a trivial group of roots of unity, followed by a discussion on arbitrary groups of roots of unity. By the end of this section, we will provide explicit bounds on the index of relative orders. The following lemma is inspired by [BS17][Proposition 12], which handles quartic CM fields.

Lemma 7.19.
Let K be a cyclic sextic CM field with maximal totally real subfield K_0 together with orders $S \subseteq R \subseteq \mathcal{O}_K$ in K such that $\mu_R = \{\pm 1\}$. Let $f := [\,\mathcal{O}_K : S\,]$, $S_0 := S \cap K_0$ and $R_0 := R \cap K_0$. Let the kernel of the relative norm

$$\psi : \left(R/f\mathcal{O}_K\right)^\times / \left(S/f\mathcal{O}_K\right)^\times \longrightarrow \left(R_0/f\mathcal{O}_{K_0}\right)^\times / \left(S_0/f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most two. Then, for all prime numbers $p > 7$, we have

$$v_p([\,R : S\,]) = v_p([\,R_0 : S_0\,]).$$

Proof. Let $p > 7$ be a prime number. If $v_p([\,R : S\,]) = 0$, then $v_p([\,R_0 : S_0\,]) = 0$. So let p divide $[\,R : S\,]$, which means that p also divides f. Let $I := f\mathcal{O}_K$, $I_0 := f\mathcal{O}_{K_0}$ and consider the map

$$\psi_p : \left(R/I_{(p)}\right)^\times / \left(S/I_{(p)}\right)^\times \longrightarrow \left(R_0/I_{0(p)}\right)^\times / \left(S_0/I_{0(p)}\right)^\times.$$

Recall that, in the terminology as we defined in Chapter 7.3, $\psi = \psi'$ because μ_R is trivial. We denote the domain of ψ_p by D_p and the codomain of ψ_p by C_p. As a consequence of Theorem 7.7, we obtain

$$\left(R/I_{(p)}\right)^\times \cong \prod_{\substack{\mathfrak{p} \leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}}} \left(R/\mathfrak{p}\right)^\times \times (1+\mathfrak{p})/(1+I_{(\mathfrak{p})}) \quad \text{and}$$
$$\left(S/I_{(p)}\right)^\times \cong \prod_{\substack{\mathfrak{q} \leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z} = p\mathbb{Z}}} \left(S/\mathfrak{q}\right)^\times \times (1+\mathfrak{q})/(1+I_{(\mathfrak{q})}).$$

Thus, we can decompose the p-part of the domain of ψ, or equivalently, the domain of ψ_p, as

$$D_p := \left(R/I_{(p)}\right)^\times / \left(S/I_{(p)}\right)^\times \cong \underbrace{\left(\prod_{\substack{\mathfrak{p} \leq R \text{ prime} \\ \mathfrak{p}\cap\mathbb{Z} = p\mathbb{Z}}} \left(R/\mathfrak{p}\right)^\times / \prod_{\substack{\mathfrak{q} \leq S \text{ prime} \\ \mathfrak{q}\cap\mathbb{Z} = p\mathbb{Z}}} \left(S/\mathfrak{q}\right)^\times \right)}_{=:\tilde{D}_p} \times A_p$$

for some p-group A_p.

Decomposing the p-part of the codomain of ψ, respectively the codomain of ψ_p, results in

$$C_p := \left(R_0/I_{0(p)}\right)^\times \Big/ \left(S_0/I_{0(p)}\right)^\times \cong \underbrace{\left(\prod_{\substack{\mathfrak{p}_0 \le R_0 \text{ prime} \\ \mathfrak{p}_0 \cap \mathbb{Z} = p\mathbb{Z}}} \left(R_0/\mathfrak{p}_0\right)^\times \Big/ \prod_{\substack{\mathfrak{q}_0 \le S_0 \text{ prime} \\ \mathfrak{q}_0 \cap \mathbb{Z} = p\mathbb{Z}}} \left(S_0/\mathfrak{q}_0\right)^\times \right)}_{=:\tilde{C}_p} \times A_{0,p}$$

for some p-group $A_{0,p} \subseteq A_p$.

Given that the kernel of the relative norm ψ has an exponent of at most two, the same holds for the kernel of ψ_p. Since p is odd, we can embed A_p into $A_{0,p}$ through ψ_p, implying that $A_p = A_{0,p}$. The p-valuations of $\tilde{D}_p$ and $\tilde{C}_p$ are trivial, but the decompositions into prime ideals also appear in the decomposition of the indices, as observed in Lemma 7.11:

$$\begin{aligned}
[\,R\,:\,S\,]_p &= \left|\tilde{D}_p\right|_p \, |A_p|_p \prod_{\substack{\mathfrak{p} \le R \text{ prime} \\ \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{p}) \prod_{\substack{\mathfrak{q} \le S \text{ prime} \\ \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{q})^{-1} \\
&= |A_p|_p \prod_{\substack{\mathfrak{p} \le R \text{ prime} \\ \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{p}) \prod_{\substack{\mathfrak{q} \le S \text{ prime} \\ \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{q})^{-1} .
\end{aligned}$$

On the other hand, we have

$$\begin{aligned}
[\,R_0\,:\,S_0\,]_p &= \left|\tilde{C}_p\right|_p \, |A_{0,p}|_p \prod_{\substack{\mathfrak{p}_0 \le R_0 \text{ prime} \\ \mathfrak{p}_0 \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{p}_0) \prod_{\substack{\mathfrak{q}_0 \le S_0 \text{ prime} \\ \mathfrak{q}_0 \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{q}_0)^{-1} \\
&= |A_{0,p}|_p \prod_{\substack{\mathfrak{p}_0 \le R_0 \text{ prime} \\ \mathfrak{p}_0 \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{p}_0) \prod_{\substack{\mathfrak{q}_0 \le S_0 \text{ prime} \\ \mathfrak{q}_0 \cap \mathbb{Z} = p\mathbb{Z}}} N(\mathfrak{q}_0)^{-1} .
\end{aligned}$$

The p-part of the index $[\,R_0\,:\,S_0\,]$ is now in correspondence with $\tilde{C}_p$ in the following sense. If we consider $|\tilde{C}_p|$ as a polynomial in p, then the sum of its degree and the p-valuation of $|A_{0,p}|$ equals the p-valuation of the index $[\,R_0\,:\,S_0\,]$. The same holds for $\tilde{D}_p$ and for $[\,R\,:\,S\,]$, if we replace $|A_{0,p}|$ by $|A_p|$.

It remains to show that $|\tilde{C}_p| = |\tilde{D}_p|$ for all $p > 7$. If this is the case, then $[\,R_0\,:\,S_0\,]_p = [\,R\,:\,S\,]_p$ for all $p > 7$. Based on the splitting behavior of p in $\mathcal{O}_{K_0}$ and the insights from Proposition 7.17, we derive the following possibilities for the cyclic factors of $\tilde{C}_p$:

(a) If $p\mathcal{O}_{K_0} = \prod_{i=1}^{3} \mathfrak{P}_{0,i}$, then $|\mathcal{O}_{K_0}/\mathfrak{P}_{0,i}| = p$, and there are at most two (non-trivial) cyclic factors in $\tilde{C}_p$, each of cardinality $p-1$. Consequently, the cardinality of $|\tilde{C}_p|$ is contained in $\{(p-1)^2, (p-1), 1\}$.

(b) If $p\mathcal{O}_{K_0} = \mathfrak{P}_0^3$, there is no (non-trivial) cyclic factor in $\tilde{C}_p$, and $|\tilde{C}_p| = 1$.

(c) If $p\mathcal{O}_{K_0} = \mathfrak{P}_0$, there is at most one (non-trivial) cyclic factor in $\tilde{C}_p$ of cardinality $(p^3-1)/(p-1) = p^2+p+1$ or $(p^2-1)/(p-1) = p+1$. Accordingly, we obtain that $|\tilde{C}_p| \in \{(p^2+p+1, p+1, 1\}$.

Given that the kernel of ψ has an exponent of at most two and it is generated by no more than six elements, it follows that the cardinality of $\ker \psi_p$ divides 2^m, where m in the set $\{1, \ldots, 6\}$ represents the number of cyclic factors of $\tilde{D}_p$. Therefore,

$$|\tilde{D}_p| = |\ker \psi_p| \cdot |\mathrm{Im}(\psi_p)| = |\ker \psi_p| \cdot |\tilde{C}_p| \;\Big|\; 2^m \cdot |\tilde{C}_p|$$

Each cyclic factor of $\tilde{D}_p$ contains at most two elements from the kernel. From this, we deduce that the cardinality of a cyclic factor of $\tilde{D}_p$ divides $2 \cdot |\tilde{C}_p|$.

We observe that $\tilde{D}_p$ has at least as many cyclic factors as $\tilde{C}_p$. Each cyclic factor of $\tilde{D}_p$ has a cardinality either of the form $p^\ell - 1$ or $\frac{p^g-1}{p^h-1}$, where ℓ, g, h belong to the set $\{1, 2, 3, 6\}$, and h divides g (because otherwise $\frac{p^g-1}{p^h-1}$ would not be an integer). We will explore all potential values for $|\tilde{C}_p|$, keeping in mind the associated splitting behavior of p in each case, as discussed in Proposition 7.17 and Proposition 7.18. We will conclude that $|\tilde{D}_p| = |\tilde{C}_p|$ for all $p > 7$. Specifically, we have $[\, R : S \,]_p = [\, R_0 : S_0 \,]_p$ for all $p > 7$, by evaluating each case, step by step.

(a) ($|\tilde{C}_p| = 1$): Every cyclic factor of $\tilde{D}_p$ has a cardinality dividing 2, which is only possible if this factor has cardinality 1 or $(p-1)$ for $p = 3$. Hence, for $p > 3$, every factor is trivial and $|\tilde{D}_p| = 1 = |\tilde{C}_p|$.

(b) ($|\tilde{C}_p| = (p-1)$): Every cyclic factor of $\tilde{D}_p$ has a cardinality dividing $2 \cdot (p-1)$, which is only possible if this factor has order $(p-1)$ or $(p+1)$ for $p = 3$. Assume that $\tilde{D}_p$ is the product of $2 \leq m \leq 6$ cyclic groups of order $(p-1)$ satisfying $(p-1)^m \mid 2^m \cdot (p-1)$. Then $p \in \{2, 3, 5\}$. It follows that $|\tilde{D}_p| = (p-1) = |\tilde{C}_p|$ for all $p > 5$.

(c) ($|\tilde{C}_p| = (p+1)$): Every cyclic factor of $\tilde{D}_p$ has a cardinality dividing $2 \cdot (p+1)$, which is only possible if this factor has order $(p+1)$ or $(p-1)$ for $p = 3$. Assume that $\tilde{D}_p$ is the product of $2 \leq m \leq 6$ cyclic groups of order $(p+1)$ satisfying $(p+1)^m \mid 2^m \cdot (p+1)$. Then $p = 3$ and we have $|\tilde{D}_p| = (p+1) = |\tilde{C}_p|$ for all $p > 3$.

(d) ($|\tilde{C}_p| = (p-1)^2$): This is the first case, where $\tilde{C}_p$ has two non-trivial cyclic factors instead of one, both of order $(p-1)$. Now $\tilde{D}_p$ has at least two cyclic factors and every cyclic factor has cardinality divided by $(p-1)$. On the

other hand, every cyclic factor of $\tilde{D}_p$ has a cardinality dividing $2 \cdot (p-1)^2$, which is only possible if this factor has order $(p-1)$, $(p-1)^2$ or (p^2-1) if $p = 3$. Assume there are $2 \leq m \leq 5$ factors with cardinality $(p-1)$ or $(p-1)^2$ such that $(p-1)^{m_1} \cdot (p-1)^{2m_2} \mid 2^m \cdot (p-1)^2$ for some $m_1 \in \{0, \ldots, 5\}$ and $m_2 \in \{1, \ldots, 5\}$ with $m_1 + m_2 = m$. Then $p \in \{2, 3, 5\}$. Hence, there will be no factor of cardinality $(p-1)^2$ if $p > 5$. On the other hand, if $\tilde{D}_p$ consists of more than 2 non-trivial factors of cardinality $(p-1)$, it follows that $p \in \{2, 3, 5\}$. Jointly, we receive that $|\tilde{D}_p| = (p-1)^2 = |\tilde{C}_p|$ for all $p > 5$.

(e) ($|\tilde{C}_p| = (p^2+p+1)$): Every cyclic factor of $\tilde{D}_p$ has a cardinality dividing $2 \cdot (p^2+p+1)$, which is only possible if this factor has order (p^2+p+1) or $p \leq 7$. There can be at most two cyclic factors in $\tilde{D}_p$ because $r = 1$. But for all prime numbers $(p^2+p+1)^2 \nmid 2^2 \cdot (p^2+p+1)$. Consequently, for all $p > 7$, we have $|\tilde{D}_p| = (p^2+p+1) = |\tilde{C}_p|$.

In total, we have shown that $|\tilde{D}_p|$ equals $|\tilde{C}_p|$ for all $p > 7$, which means that $[\, R_0 \,:\, S_0 \,]_p = [\, R \,:\, S \,]_p$ for all $p > 7$. □

In a next step, the following theorem generalizes Lemma 7.19 to arbitrary cardinalities of μ_R. This requires a comparison of the maps ψ and ψ'. For $\mu_R = \{\pm 1\}$ we have $\psi = \psi'$, but this is not true in general. Note that for any degree six number field K it is $|\mu_K| \in \{2, 4, 6, 14, 18\}$, which implies that $|\mu_R| \in \{2, 4, 6, 14, 18\}$ for all orders $R \subseteq \mathcal{O}_K$.

Theorem 7.20.
Let K be a cyclic sextic CM field with maximal totally real subfield K_0. Let $S \subseteq R$ be orders in K, and let $f := [\, \mathcal{O}_K \,:\, S \,]$. Let $S_0 := S \cap K_0$ and $R_0 := R \cap K_0$. Let the kernel of the relative norm

$$\psi : \left(R \big/ f\mathcal{O}_K\right)^\times \Big/ \left(S \big/ f\mathcal{O}_K\right)^\times \mu_R \longrightarrow \left(R_0 \big/ f\mathcal{O}_{K_0}\right)^\times \Big/ \left(S_0 \big/ f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most two and let B be defined as in the following table, depending on the size of μ_R:

$\lvert\mu_R\rvert$	2	4	6	14	18
B	7	17	19	43	73

Then for every prime $p > B$, we have

$$v_p([\, R \,:\, S \,]) = v_p([\, R_0 \,:\, S_0 \,]).$$

Proof. Let $I = f\mathcal{O}_K$. We obtain the following relation of the cardinalities of the domains of ψ and ψ' depending on the intersection of $S^\times$ and μ_R:

$$\left|\frac{\left(R/I\right)^\times}{\left(S/I\right)^\times \mu_R}\right| = \frac{\left|\left(R/I\right)^\times\right|}{\left|\left(S/I\right)^\times\right|} \cdot \frac{|S^\times \cap \mu_R|}{|\mu_R|} \in \left\{ x \cdot \frac{\left|\left(R/I\right)^\times\right|}{\left|\left(S/I\right)^\times\right|} \;\middle|\; x \in \left\{1, \frac{2}{|\mu_R|}\right\} \right\}.$$

Consequently, the cardinality of the domain of ψ divides the cardinality of the domain of ψ'. In order to generalize Lemma 7.19, we can mainly follow the same argument, but when relating $\tilde{D}_p$, and its cyclic factors with $\tilde{C}_p$, we get an additional factor. Recall that, in the proof of Theorem 7.19, we stated

$$|\tilde{D}_p| = |\ker \psi_p| \cdot |\mathrm{Im}(\psi_p)| = |\ker \psi_p| \cdot |\tilde{C}_p|\,.$$

We have $\ker \psi = \ker \psi'/(\mu_R/\{\pm 1\})$, which is generated by at most six elements of exponent at most two, and we have

$$|\ker \psi_p| \;\Big|\; 2^6 \, \frac{|\mu_R|}{2}\,.$$

Consequently,

$$|\tilde{D}_p| = |\ker \psi_p| \cdot |\tilde{C}_p| \;\Big|\; 2^6 \, \frac{|\mu_R|}{2} \, |\tilde{C}_p|\,.$$

Now, the cyclic factors of $\tilde{D}_p$ contain at most two elements of the kernel and their cardinalities divide $2\,\frac{\mu_R}{2}\,|\tilde{C}_p| = |\mu_R|\,|\tilde{C}_p|$. Having these two conditions, we can now follow the same argument as in the proof of Lemma 7.19 and receive the following relations of $|\tilde{D}_p|$ and $|\tilde{C}_p|$ depending on the size of μ_R.

(a) ($|\tilde{C}_p| = 1$): We have $|\tilde{D}_p| = 1 = |\tilde{C}_p|$ for all $p > B$ where

$\lvert\mu_R\rvert$	2	4	6	14	18
B	3	5	7	13	19

(b) ($|\tilde{C}_p| = p - 1$): For all $p > B$ every cyclic factor of $\tilde{D}_p$ has order $(p-1)$ where

$\lvert\mu_R\rvert$	2	4	6	14	18
B	3	7	11	13	17

Now assume that $\tilde{D}_p$ is the product of $2 \le m \le 6$ factors of order $(p-1)$. Then $(p-1)^m \mid |\mu_K| \cdot 2^{m-1} \cdot (p-1)$, which is impossible for all $p > B$ where

$\lvert\mu_R\rvert$	2	4	6	14	18
B	5	5	13	29	37

As a consequence, for these bounds B depending on μ_R and every $p > B$, we receive that $|\tilde{D_p}| = p - 1 = |\tilde{C_p}|$.

(c) ($|\tilde{C_p}| = p + 1$): For all $p > B$ every cyclic factor of $\tilde{D_p}$ has order $(p + 1)$ where

$\lvert\mu_R\rvert$	2	4	6	14	18
B	5	5	13	29	37

Now assume that $\tilde{D_p}$ is the product of $2 \leq m \leq 6$ factors of order $(p + 1)$. Then $(p + 1)^m \mid |\mu_K| \cdot 2^{m-1} \cdot (p + 1)$, which is impossible for all $p > B$ if

$\lvert\mu_R\rvert$	2	4	6	14	18
B	3	7	11	13	17

Accordingly, for the following bounds B depending on μ_R and every $p > B$, we receive that $|\tilde{D_p}| = p - 1 = |\tilde{C_p}|$:

$\lvert\mu_R\rvert$	2	4	6	14	18
B	5	7	13	29	37

(d) ($|\tilde{C_p}| = (p - 1)^2$): The cardinality of every cyclic factor of $\tilde{D_p}$ has to divide $|\mu_K| \cdot |\tilde{C_p}|$ and contains a cyclic factor of $\tilde{C_p}$ with cardinality $(p-1)$. Hence, its order is of the form $(p - 1)$ for all $p > B$ where

$\lvert\mu_R\rvert$	2	4	6	14	18
B	3	7	11	13	17

We know that $\tilde{D_p}$ has at least two and at most four factors of order $(p - 1)$. Hence, $|\tilde{D_p}| = (p - 1)^2 = |\tilde{C_p}|$ for all $p > B$, if

$\lvert\mu_R\rvert$	2	4	6	14	18
B	5	17	13	29	73

(e) ($|\tilde{C_p}| = p^2 + p + 1$): For $p > B$ every cyclic factor of $\tilde{D_p}$ has cardinality $(p^2 + p + 1)$, if

$\lvert\mu_R\rvert$	2	4	6	14	18
B	7	13	19	43	19

Now assume that $\tilde{D_p}$ is the product of $2 \leq m \leq 6$ factors of order (p^2+p+1). Then $(p^2 + p + 1)^m \mid |\mu_K| \cdot 2^{m-1} \cdot (p^2 + p + 1)$, which is impossible for all primes p except for $p = 2$, if $|\mu_R| = 14$.

Summarizing these considerations, we find that $|\tilde{D}_p| = |\tilde{C}_p|$ for all $p > B$ with

$\lvert\mu_R\rvert$	2	4	6	14	18
B	7	17	19	43	73

.

Thus, for each such $p > B$, we have $v_p([\,R\,:\,S\,]) = v_p([\,R_0\,:\,S_0\,])$. □

Combining Theorem 7.20 with Lemma 7.15, we can now deduce the first main theorem of this chapter.

Theorem 7.21.
Let K be a cyclic sextic CM field with maximal totally real subfield K_0, and let $S \subseteq R \subseteq \mathcal{O}_K$ be orders in K with $f := [\,\mathcal{O}_K\,:\,S\,]$. Let $S_0 := S \cap K_0$, and let $R_0 := R \cap K_0$. Let the kernel of the relative norm

$$\psi : \left(R/f\mathcal{O}_K\right)^\times \Big/ \left(S/f\mathcal{O}_K\right)^\times \mu_R \longrightarrow \left(R_0/f\mathcal{O}_{K_0}\right)^\times \Big/ \left(S_0/f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most two. Then

$$\frac{[\,R\,:\,S\,]}{[\,R_0\,:\,S_0\,]} \,\Big|\, B\,,$$

where B is given by the following table depending on the number of elements in the group of roots of unity μ_R.

$\lvert\mu_R\rvert$	B
2	$2^{15}3^7 5^3 7^2$
4	$2^{16}3^7 5^4 7^3 11^2 13^2 17$
6	$2^{16}3^8 5^4 7^3 11^2 13^2$
14	$2^{17}3^8 5^5 7^3 11^2 13^2 \cdots 23^2 29$
18	$2^{18}3^9 5^5 7^3 11^3 13^2 \cdots 23^2 29 \cdots 73$

Proof. As the kernel of the relative norm is of exponent at most two, using Theorem 7.20, we receive that there are no primes greater than B in the quotient of $[\,R\,:\,S\,]$ by $[\,R_0\,:\,S_0\,]$. On the other hand, Lemma 7.15 gives us the bounds on the exponents to the remaining primes and proves the claim. □

7.4.3 Explicit bounds on the index

Combining Theorem 7.21 with Theorem 6.11, we receive the following second main theorem of this chapter.

Theorem 7.22.
Let K be a cyclic sextic CM field, and let K_0 be the totally real cubic subfield of K. Let $S \subseteq \mathcal{O}_K$ be an order of K stable under complex conjugation, and let the kernel of the relative norm

$$\psi : \left(\mathcal{O}_K \big/ f\mathcal{O}_K\right)^\times \Big/ \left(S \big/ f\mathcal{O}_K\right)^\times \mu_K \longrightarrow \left(\mathcal{O}_{K_0} \big/ f\mathcal{O}_{K_0}\right)^\times \Big/ \left(S_0 \big/ f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most two, where $f := [\,\mathcal{O}_K : S\,]$. Then we have

$$f^2 = [\,\mathcal{O}_K : S\,]^2 \,\Big|\, B^4 \,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,\delta_S,$$

where B is given by the following table depending on the number of elements in the group of roots of unity μ_K.

$\lvert\mu_K\rvert$	B
2	$2^{15}3^7 5^3 7^2$
4	$2^{16}3^7 5^4 7^3 11^2 13^2 17$
6	$2^{16}3^8 5^4 7^3 11^2 13^2$
14	$2^{17}3^8 5^5 7^3 11^2 13^2 \cdots 23^2 29$
18	$2^{18}3^9 5^5 7^3 11^3 13^2 \cdots 23^2 29 \cdots 73$

Proof. Applying Theorem 7.21 for the case $R = \mathcal{O}_K$, we receive that

$$[\,\mathcal{O}_K : S\,] \,\Big|\, B\,[\,\mathcal{O}_{K_0} : S_0\,],$$

where the bound B depends on the cardinality of μ_K. On the other hand, due to Theorem 6.11, we know that

$$[\,\mathcal{O}_{K_0} : S_0\,]^4 \,\Big|\, \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})[\,\mathcal{O}_K : S\,]^2\,\delta_S.$$

Combining this information, we obtain

$$[\,\mathcal{O}_K : S\,]^4 \,\Big|\, B^4\,[\,\mathcal{O}_{K_0} : S_0\,]^4 \,\Big|\, B^4 \,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,[\,\mathcal{O}_K : S\,]^2\,\delta_S,$$

which is equivalent to or claim. □

Now, whenever δ_S is known, Theorem 7.22 allows giving an explicit set of primes which can possibly divide the index $[\,\mathcal{O}_K : S\,]$. For example, if $\delta_S = 1$ we receive the following result.

Theorem 7.23.
Let K be a cyclic sextic CM field, and let K_0 be the totally real cubic subfield of K. Let $S \subseteq \mathcal{O}_K$ be an order of K stable under complex conjugation with $\delta_S = 1$, and let the kernel of the relative norm

$$\psi : \left(\mathcal{O}_K \big/ f\mathcal{O}_K\right)^\times \Big/ \left(S \big/ f\mathcal{O}_K\right)^\times \mu_K \longrightarrow \left(\mathcal{O}_{K_0} \big/ f\mathcal{O}_{K_0}\right)^\times \Big/ \left(S_0 \big/ f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most two, where $f := [\,\mathcal{O}_K : S\,]$. Then we have

$$f^2 = [\,\mathcal{O}_K : S\,]^2 \,\Big|\, B^4 \,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,,$$

where B is given by the following table depending on the number of elements in the group of roots of unity μ_K.

$\lvert\mu_K\rvert$	B
2	$2^{15}3^7 5^3 7^2$
4	$2^{16}3^7 5^4 7^3 11^2 13^2 17$
6	$2^{16}3^8 5^4 7^3 11^2 13^2$
14	$2^{17}3^8 5^5 7^3 11^2 13^2 \cdots 23^2 29$
18	$2^{18}3^9 5^5 7^3 11^3 13^2 \cdots 23^2 29 \cdots 73$

Proof. Using Theorem 7.22, we deduce

$$f^2 = [\,\mathcal{O}_K : S\,]^2 \,\Big|\, B^4 \,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,\delta_S,$$

with B defined as in Theorem 7.21. Given that $\delta_S = 1$, this confirms our claim. □

From what we observed in Theorem 6.15 and Theorem 6.16, Theorem 7.23 covers the cases where S_0 is Gorenstein and the case where S is composed of an order S_k in k and an order S_0 in K_0. Consequently, we can state the following two corollaries.

Corollary 7.24.
Let K be a cyclic sextic CM field and K_0 be the totally real cubic subfield of K. Let $S \subseteq \mathcal{O}_K$ be an order of K stable under complex conjugation such that $S_0 = S \cap K_0$ is Gorenstein and let the kernel of the relative norm

$$\psi : \left(\mathcal{O}_K \big/ f\mathcal{O}_K\right)^\times \Big/ \left(S \big/ f\mathcal{O}_K\right)^\times \mu_K \longrightarrow \left(\mathcal{O}_{K_0} \big/ f\mathcal{O}_{K_0}\right)^\times \Big/ \left(S_0 \big/ f\mathcal{O}_{K_0}\right)^\times$$

be of exponent at most two, where $f := [\,\mathcal{O}_K\,:\,S\,]$*. Then we have*

$$f^2 = [\,\mathcal{O}_K\,:\,S\,]^2 \;\Big|\; B^4\ \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0}),$$

where B *is given by the following table depending on the number of elements in the group of roots of unity* μ_K*.*

$\lvert\mu_K\rvert$	B
2	$2^{15}3^7 5^3 7^2$
4	$2^{16}3^7 5^4 7^3 11^2 13^2 17$
6	$2^{16}3^8 5^4 7^3 11^2 13^2$
14	$2^{17}3^8 5^5 7^3 11^2 13^2 \cdots 23^2 29$
18	$2^{18}3^9 5^5 7^3 11^3 13^2 \cdots 23^2 29 \cdots 73$

Proof. Given that S_0 is Gorenstein, Theorem 6.15 indicates that $\delta_S = 1$. By applying Theorem 7.23, we have proved our claim. □

Corollary 7.25.
Let K *be a cyclic sextic CM field containing an imaginary quadratic subfield* k*, and let* K_0 *be the totally real cubic subfield of* K*. Let* S_k *be an order in* k*, and let* S_0 *be an order in* K_0*. If* $S := S_k\, S_0$ *is stable under complex conjugation and if the kernel of the relative norm*

$$\psi : \Big(\mathcal{O}_K \big/ f\mathcal{O}_K\Big)^\times \Big/ \Big(S \big/ f\mathcal{O}_K\Big)^\times \mu_K \longrightarrow \Big(\mathcal{O}_{K_0} \big/ f\mathcal{O}_{K_0}\Big)^\times \Big/ \Big(S_0 \big/ f\mathcal{O}_{K_0}\Big)^\times$$

is of exponent at most two, where $f := [\,\mathcal{O}_K\,:\,S\,]$*, then we have*

$$f^2 = [\,\mathcal{O}_K\,:\,S\,]^2 \;\Big|\; B^4\ \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0}),$$

where B *is given by the following table depending on the number of elements in the group of roots of unity* μ_K*.*

$\lvert\mu_K\rvert$	B
2	$2^{15}3^7 5^3 7^2$
4	$2^{16}3^7 5^4 7^3 11^2 13^2 17$
6	$2^{16}3^8 5^4 7^3 11^2 13^2$
14	$2^{17}3^8 5^5 7^3 11^2 13^2 \cdots 23^2 29$
18	$2^{18}3^9 5^5 7^3 11^3 13^2 \cdots 23^2 29 \cdots 73$

Proof. Given $S = S_k\, S_0$, Theorem 6.16 suggests that $\delta_S = 1$. Using Theorem 7.23, we confirm our claim. □

In view of our later applications, Theorem 7.22 provides bounds on the index of orders that could serve as endomorphism rings for specific polarized abelian varieties over $\mathbb{C}$ with complex multiplication in a sextic CM field. This not only proves the finiteness of the number of potential endomorphism rings S with $\delta_S = 1$, but also allows the computation of all such endomorphism rings. We will discuss this in detail in the following chapters.

Even when $\delta_S \neq 1$, we can still give bounds on the index from Theorem 7.22 for specific classes of orders. We show this in the following example in which the value of δ_S was verified computationally.

Example 7.26.
Let K be a cyclic sextic CM field with $\mathcal{O}_K = \langle 1, \lambda_1, \ldots, \lambda_5 \rangle_{\mathbb{Z}}$ and totally real cubic subfield K_0. Let $a \in \mathbb{Z}$, and let $S = \langle 1, a\,\lambda_1, \ldots, a\lambda_5 \rangle_{\mathbb{Z}}$ be an order. Then $[\,\mathcal{O}_K : S\,] = a^5$, and $\delta_S = a$. If S is stable under complex conjugation and the kernel of the relative norm is of exponent at most two, Theorem 7.22 gives us

$$a^9 = a^{2\cdot 5\,-1} \,\Big|\, B^4\,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\,.$$

Since that the right-handed side does not depend on S, this provides a concrete bound on the primes dividing $[\,\mathcal{O}_K : S\,]$.

Chapter 8

Endomorphism rings of abelian varieties of dimension 3

We recall that, in Chapter 4.2, we discussed polarized abelian varieties over $\mathbb{C}$ with CM by an arbitrary order S in a CM field K that have field of moduli $\mathbb{Q}$. We identified all potential CM fields K in the dimension 3 case. Building on these results, in this chapter we aim to provide necessary conditions for the orders S in these CM fields, which potentially appear as endomorphism rings of such polarized abelian varieties. For the context of this chapter, we let (K, Φ) denote a sextic CM type, let (K^r, Φ^r) its reflex type, and let S an order in K. We let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a simple polarized abelian variety over $\mathbb{C}$ of type (K, Φ) with complex multiplication by S and field of moduli $\mathbb{Q}$. The goal of this chapter is to explicitly compute the possible endomorphism rings S of such polarized abelian varieties $\mathcal{P}$. The following first main result of this chapter is a consequence of Shimuras third main theorem (see Chapter 4.1) combined with our results from Chapter 7.

Theorem 8.1.
Let (K, Φ) be a sextic CM type and (K^r, Φ^r) be its reflex. Let K_0 denote the totally real cubic subfield of K, and let $S \subseteq \mathcal{O}_K$ be an order of index $f = [\mathcal{O}_K : S]$. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a simple polarized abelian variety over $\mathbb{C}$ of type (K, Φ) with complex multiplication by S and field of moduli $\mathbb{Q}$. Then

(a) *K is a cyclic sextic CM class number one field containing an imaginary quadratic subfield,*
(b) *$\Omega_S = I_{K^r}(f)$, and*
(c) *$f^2 = [\mathcal{O}_K : S]^2 \,\Big|\, B^4 \, \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})\, \delta_S$, where B is given by the following table depending on the number of elements in the group of roots of unity μ_K.*

$\lvert\mu_K\rvert$	B
2	$2^{15}3^7 5^3 7^2$
4	$2^{16}3^7 5^4 7^3 11^2 13^2 17$
6	$2^{16}3^8 5^4 7^3 11^2 13^2$
14	$2^{17}3^8 5^5 7^3 11^2 13^2 \cdots 23^2 29$
18	$2^{18}3^9 5^5 7^3 11^3 13^2 \cdots 23^2 29 \cdots 73$

Proof. Given that A is simple and by applying Proposition 1.89, the CM type (K, Φ) is primitive. Consequently, by definition, (K^r, Φ^r) is also primitive and thus $(K^{rr}, \Phi^{rr}) = (K, \Phi)$. Using Corollary 4.9 and noting that the field of moduli $\mathbb{Q}$ is a subfield of the reflex field K^r, we conclude $\Omega_S = \Omega_{\mathcal{O}_K} = I_{K^r}(f)$. As shown in Lemma 4.13, this means that K is a cyclic sextic CM class number one field containing an imaginary quadratic subfield. As we have pointed out in Chapter 5, in this situation all primitive CM types are equivalent. Therefore, without loss of generality, we can assume $\Phi = \{1, \tau, \tau^{-1}\}$, where τ is a generator of the automorphism group of K over $\mathbb{Q}$. Given $\Omega_S = I_{K^r}(f)$, the kernel of the relative norm has an exponent at most two, as presented in Proposition 5.5. Moreover, S is invariant under complex conjugation because of the Rosati involution. We can now apply Theorem 7.22 to receive the upper bounds for the primes $p \mid f$ and their multiplicities. □

Theorem 8.1 applies to Jacobians of simple genus 3 curves over $\mathbb{C}$ with CM by arbitrary orders, as these Jacobians are principally polarized abelian varieties. Again, as already discussed in Chapter 6 and Chapter 7, we are especially interested in situations where we can control δ_S, for example when $\delta_S = 1$. In this context, we can state the following corollary.

Corollary 8.2.
Let (K, Φ) be a sextic CM type and (K^r, Φ^r) be its reflex. Let K_0 denote the totally real cubic subfield of K and $S \subseteq \mathcal{O}_K$ be an order of index $f = [\mathcal{O}_K : S]$. Let $\mathcal{P} = (A, \iota, \mathscr{C})$ be a simple polarized abelian variety over $\mathbb{C}$ of type (K, Φ) with complex multiplication by S and field of moduli $\mathbb{Q}$. Then

(a) *K is a cyclic sextic CM class number one field containing an imaginary quadratic subfield,*
(b) *$\Omega_S = I_{K^r}(f)$, and*
(c) *if $\delta_S = 1$, then $f^2 = [\mathcal{O}_K : S]^2 \,\Big|\, B^4 \, \mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0})$, where B is given by the following table depending on the number of elements in the group of roots of unity μ_K.*

$\lvert\mu_K\rvert$	B
2	$2^{15}3^7 5^3 7^2$
4	$2^{16}3^7 5^4 7^3 11^2 13^2 17$
6	$2^{16}3^8 5^4 7^3 11^2 13^2$
14	$2^{17}3^8 5^5 7^3 11^2 13^2 \cdots 23^2 29$
18	$2^{18}3^9 5^5 7^3 11^3 13^2 \cdots 23^2 29 \cdots 73$

Proof. Applying Theorem 8.1 and inserting $\delta_S = 1$ proves the claim. □

Building on the notation of the last two statements, let k denote the imaginary quadratic subfield of K, $S_0 = S \cap K_0$ and $S_k = S \cap k$. Note that we can apply Corollary 8.2 to the case where $S_0 = S \cap K_0$ is Gorenstein (see Corollary 7.24) and to the case where $S = S_k \, S_0$ is the composition of orders S_k and S_0 (see Corollary 7.25). On the other hand, if we omit the condition $\delta_S = 1$, but have knowledge of δ_S and $[\mathcal{O}_K : S]$ in terms of a $\mathbb{Z}$-basis of S, we can still derive bounds on the index from Theorem 8.1. Such a class of orders was presented in Example 7.26.

Unfortunately, in practical applications, one might observe that the bounds on the prime powers dividing the indices as presented in Theorem 8.1 can be too large in order to compute all potential endomorphism rings within a feasible time. In order to circumvent this challenge, we will construct an explicit minimal order and narrow down our focus to the two important cases illustrated in Chapter 4.3.

8.1 Minimal orders

Let (A, ι) be an abelian variety of primitive CM type (K, Φ) with CM by an order $S \subseteq \mathcal{O}_K$ of index $f = [\mathcal{O}_K : S]$. Let $\mathscr{C}$ be a polarization of A such that the field of moduli k_0 of $(A, \mathscr{C})$ is contained in the reflex field K^r of (K, Φ). Then, due to

Shimura's third main theorem, we have $\Omega_S = I_{K^r}(f)$. Especially, for all $\alpha \in I_{K^r}(f)$, we have $\mathrm{N}_{\Phi^r}(\alpha) = x\mathcal{O}_K$ and $\mathrm{N}_{K^r/\mathbb{Q}}(\alpha) = x\bar{x} \in \mathbb{Q}$ for some $x \in K^\times$. Within this section, we aim to determine specific suborders of S.

Definition 8.3.
Let (K, Φ) be a CM type, (K^r, Φ^r) be its reflex and $\Omega_{K^r} = I_{K^r}$. Let f be an integer and $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ be integral generators of the ray class group $I_{K^r}(f)/P_{K^r,1}(f)$. Let $\alpha_j \in K^\times$ be generators of $\mathrm{N}_{\Phi^r}(\mathfrak{a}_j)$ with $\alpha_j\bar{\alpha_j} \in \mathbb{Q}$ for $j = 1, \ldots, s$. We define $S_{min,f}$ to be the order of K generated by $\alpha_1, \ldots, \alpha_s$, $f\mathcal{O}_K$ and μ_K.

The following statement generalizes [BS17][Lemma 18], which aims quartic CM fields.

Lemma 8.4.
Let (K, Φ) be a CM type and (K^r, Φ^r) be its reflex. Let $\Omega_{K^r} = I_{K^r}$. Let f be an integer, let S be an order of K such that $f\mathcal{O}_K \subseteq S$, and let the roots of unity μ_K of K be all contained in S. Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ be integral generators of the ray class group $I_{K^r}(f)/P_{K^r,1}(f)$, and let $\alpha_j \in K^\times$ be generators of $\mathrm{N}_{\Phi^r}(\mathfrak{a}_j)$ with $\alpha_j\bar{\alpha_j} \in \mathbb{Q}$ for $j = 1, \ldots, s$. Then

$$\Omega_S = I_{K^r}(f) \qquad \textit{if and only if} \qquad S_{min,f} \subseteq S.$$

Proof. On one hand, we can select integral generators for the Ray class group whose images under the type norm are integral. Since $\Omega_{K^r} = I_{K^r}$, there exists an element $\alpha_j \in \mathcal{O}_K$ such that

$$\mathrm{N}_{\Phi^r}(\mathfrak{a}_j) = \alpha_j\,\mathcal{O}_K \quad \text{and} \quad \mathrm{N}_{K^r/\mathbb{Q}}(\mathfrak{a}_j) = \alpha_j\bar{\alpha_j} \in \mathbb{Q}$$

for each index $j \in \{1, \ldots, s\}$. For every element $\zeta \in \mu_K$, the product $\zeta\,\alpha_j \in \mathcal{O}_K$ satisfies the same properties. Hence α_j is unique up to roots of unity of K.

As pointed out in Proposition 1.59, we deduce that $\mathrm{N}_{\Phi^r}(\mathfrak{a}_j) \in P_K(f) \subseteq P_K(\mathfrak{f}_S)$ and by applying Theorem 1.27, $\mathrm{N}_{\Phi^r}(\mathfrak{a}_j) \in P_S(f)$. Since $\mu_K = \mu_S \subseteq S$, it follows that $\alpha_j \in S$ for all $j \in \{1, \ldots, s\}$.On the other hand, both $f\mathcal{O}_K$ and μ_K are subsets of S. This implies that S includes $S_{\min,f}$.

Conversely, if S contains $S_{\min,f}$, then any $\mathfrak{a} \in I_{K^r}(f)$ can be integrally represented in the Ray class group of K^r modulo f. Let this representation be $\prod_{j=1}^s \mathfrak{a}_j^{\gamma_j}$ for some non-negative integers γ_j. Thus, we can write $\mathfrak{a} = \prod_{j=1}^s \mathfrak{a}_j^{\gamma_j}\, I$, where $I \in P_{K^r,1}(f)$. Given that $\alpha_j \in S$ for each $j \in \{1, \ldots, s\}$ and $\mu_K \subseteq S$, we get $\mathrm{N}_{\Phi^r}(\mathfrak{a}_j) \in P_S(f)$.

Furthermore, we can express I as $I = x\,\mathcal{O}_K$, where $x \equiv 1 \pmod{f\mathcal{O}_{K^r}}$ and $\mathrm{N}_{\Phi^r}(x) \equiv 1 \pmod{f\mathcal{O}_K}$. This leads to

$$\mathrm{N}_{\Phi^r}(I) = \mathrm{N}_{\Phi^r}(x)\,\mathcal{O}_K = (y+1)\,\mathcal{O}_K$$

for some $y \in f\mathcal{O}_K$. Given that S is a ring that includes $f\mathcal{O}_K$, we conclude that $y + 1 \in S$ and $\mathrm{N}_{\Phi^r}(I) \in P_S(f)$. Combining these observations, we receive that $\mathrm{N}_{\Phi^r}(\mathfrak{a}) \in P_S(f)$ which shows that $\Omega_S = I_{K^r}(f)$. □

Note that, in Lemma 8.4, we assume S to contain every root of unity in K. This is a crucial aspect. However, the lemma can still be applied to several interesting situations.

Firstly, consider the case where K has a trivial group of roots of unity, denoted by $\mu_K = \{\pm 1\}$. In such cases, S naturally contains μ_K. Additionally, our focus is on simple genus 3 CM curves with a field of moduli $\mathbb{Q}$. From Lemma 4.13, we know that the corresponding CM fields are cyclic sextic CM class number one fields containing an imaginary quadratic subfield. We can now deduce the following two theorems on potential endomorphism rings for the Jacobians of both specific hyperelliptic curves and Picard curves.

Theorem 8.5.
Let $C/\mathbb{C}$ be a simple genus 3 curve with CM by an order $S \subseteq \mathcal{O}_K$ in a CM field K and field of moduli $\mathbb{Q}$. Let f be the index of S in $\mathcal{O}_K$. If $\mathbb{Z}[i] \subseteq S$, then C is hyperelliptic, and S contains $S_{min,f}$.

Proof. Let $\mathbb{Z}[i] \subseteq S$. Given that C is simple over $\mathbb{C}$ and has a field of moduli $\mathbb{Q}$, Lemma 4.13 includes that K is a cyclic sextic CM field that contains an imaginary quadratic subfield. According to Theorem 4.15, the curve C is hyperelliptic, and the imaginary quadratic subfield is $\mathbb{Q}(i)$. Every such field K has a group of roots of unity $\mu_K = \{\pm 1, \pm i\}$. As S contains $\mathbb{Z}[i]$, we deduce $\mu_K \subseteq S$ and, by applying Lemma 8.4, it follows that S contains $S_{min,f}$. □

Note that every determined CM class number one field K containing $\mathbb{Q}(i)$ from Table 4.1 fulfills $\mu_K = \mu_{\mathbb{Q}(i)}$. This allows applying Theorem 8.5. A similar result can be formulated for curves such that the endomorphism ring of their Jacobian contains $\mathbb{Z}[\zeta_3]$.

Theorem 8.6.
Let $C/\mathbb{C}$ be a simple genus 3 curve with CM by an order $S \subseteq \mathcal{O}_K$ in a CM field K and field of moduli $\mathbb{Q}$. Let f be the index of S in $\mathcal{O}_K$ and $\mu_K = \{\zeta_3^k \mid k \in \{0, \ldots, 5\}\}$. If $\mathbb{Z}[\zeta_3] \subseteq S$, then C is Picard, and S contains $S_{min,f}$.

Proof. Let $\mathbb{Z}[\zeta_3] \subseteq S$. Given that C is simple over $\mathbb{C}$, and that C has a field of moduli $\mathbb{Q}$, Lemma 4.13 tells us that K is a cyclic sextic CM field, which includes an imaginary quadratic subfield. As presented in Theorem 4.18, the curve C is Picard. Given that $\mu_K = \{\zeta_3^k \mid k \in \{0, \dots, 5\}\}$, and that S is assumed to contain $\mathbb{Z}[\zeta_3]$, it follows that $\mu_K \subseteq S$. Applying Lemma 8.4, we deduce that S contains $S_{min,f}$. □

In contrast to the case $\mathbb{Q}(i) \subseteq K$ discussed above, not all CM class number one fields K that contain $\mathbb{Q}(\zeta_3)$, as of Table 4.2, satisfy the necessary condition $\mu_K = \{\zeta_3^k \mid k \in \{0, \dots, 5\}\}$ in Theorem 8.6. Specifically, there is one field with $|\mu_K| = 18$, which exceeds the size of $\mu_{\mathbb{Q}(\zeta_3)}$. Using the notation from Table 4.2, this particular CM field is denoted as $[-1, -3, 0]$. For the remaining 9 CM fields that contain $\mathbb{Q}(\zeta_3)$, they all satisfy $\mu_K = \mu_{\mathbb{Q}(\zeta_3)}$, allowing us to apply Theorem 8.6.

To conclude this section, we present how we can consider sequences of minimal orders and tell when such a sequence stabilizes. This will become powerful in order to determine possible endomorphism rings of the hyperelliptic and Picard curves.

Lemma 8.7.
Let (K, Φ) be a CM type, let (K^r, Φ^r) be its reflex, and let $\Omega_{K^r} = I_{K^r}$. Let f and f' be two positive integers with $f \mid f'$. Let $S_{min,f}$ and $S_{min,f'}$ be defined as in Lemma 8.4. Then $S_{min,f'} \subseteq S_{min,f}$.

Proof. Firstly, $f'\mathcal{O}_K \subseteq f\mathcal{O}_K$. Now let $\mathfrak{a}_1, \dots, \mathfrak{a}_r$ be generators of the Ray class group modulo f of the reflex field K^r, and $\mathfrak{b}_1, \dots, \mathfrak{b}_s$ be generators of the Ray class group modulo f' of K^r. The images of the generators under the reflex type norm N_{Φ^r} are principal, and we denote them as α_j and β_j, respectively. Since $I_{K^r}(f') \subseteq I_{K^r}(f)$, for all $j \in \{1, \dots, s\}$ there exist $\gamma_1, \dots, \gamma_r \in \mathbb{N}$ and $I \in P_{K^r,1}(f)$ such that

$$\mathfrak{b}_j = \prod_{i=1}^{r} \mathfrak{a}_i^{\gamma_i} I\,. \tag{8.1}$$

To be more precise, there is a totally positive $x \in K^r$ with $I = x\,\mathcal{O}_{K^r}$ and $x \equiv 1 \pmod{f\mathcal{O}_{K^r}}$. Now, applying the type norm and using (8.1), we receive that $\beta_j\,\mathcal{O}_K = (\prod_{i=1}^{r} \alpha_i^{\gamma_i})\,\mathrm{N}_{\Phi^r}(x)\,\mathcal{O}_K$ and $\mathrm{N}_{\Phi^r}(x) \equiv 1 \pmod{f\mathcal{O}_K}$, which means that there exists $y \in f\mathcal{O}_K$ with

$$\beta_j\,\mathcal{O}_K = (\prod_{i=1}^{r} \alpha_i^{\gamma_i})\,(y+1)\,\mathcal{O}_K.$$

The generator of the right-hand side differs from β_j only by a root of unity. Since all roots of unity of K are contained in $S_{min,f}$ and the generator on the right-hand side lies in $S_{min,f}$, we receive $\beta_j \in S_{min,f}$ for all $j \in \{1, \dots, s\}$.Consequently, we have $S_{min,f'} \subseteq S_{min,f}$. □

As a consequence of this lemma, we can define sequences $(S_{min,p^k})_{k\geq 0}$ for every prime number p. The following lemma is presented in [BS17][Lemma 19] up to the fact that we add the roots of unity of K to the minimal orders, which does not affect its correctness. It allows recognizing when such a sequence becomes stationary at some point.We sketch the proof and refer to [BS17] for details.

Lemma 8.8.
Let (K,Φ) be a CM type, let (K^r,Φ^r) be its reflex, and let $\Omega_{K^r} = I_{K^r}$. For any prime number $p \in \mathbb{Z}$, if $S_{min,p^k} = S_{min,p^{k+1}}$ for some $k \in \mathbb{Z}_{\geq 0}$, then $S_{min,p^\ell} = S_{min,p^k}$ for all $\ell \geq k$.

Proof. Let $p \in \mathbb{Z}$ be prime, let $k \in \mathbb{Z}_{\geq 0}$, and assume that $S_{\min,p^k} = S_{\min,p^{k+1}}$. We aim to show that $S_{\min,p^{k+2}} = S_{\min,p^{k+1}}$. For all $n \leq k+2$, we have the relation $S_{\min,p^n} = S_{\min,p^{k+1}} + p^n\mathcal{O}_K$. Specifically, this implies that

$$S_{\min,p^{k+2}} \subseteq S_{\min,p^{k+1}} = S_{\min,p^{k+2}} + p^k\mathcal{O}_K\,.$$

Multiplying the entire relation by p inverts this inclusion, leading to the fact that

$$S_{\min,p^{k+2}} \supseteq S_{\min,p^{k+2}} + p^k\mathcal{O}_K = S_{\min,p^{k+1}}\,.$$

Consequently, we deduce that $S_{\min,p^{k+2}} = S_{\min,p^{k+1}}$. □

We formulate one final corollary based on Lemma 8.4, which allows us to exclude certain primes from dividing the potential index of our considered orders.

Corollary 8.9.
Let (K,Φ) be a CM type, let (K^r,Φ^r) be its reflex, and let $\Omega_{K^r} = I_{K^r}$. Let $S \subsetneq \mathcal{O}_K$ be an order of index $f \in \mathbb{Z}$ containing μ_K and satisfying $\Omega_S = I_{K^r}(f)$. If p is a prime number such that $S_{min,p} = \mathcal{O}_K$, then $p \nmid f$.

Proof. Let p be a prime number with $S_{min,p} = \mathcal{O}_K$. If $p\mathcal{O}_K \subseteq S$, then, by Lemma 8.4, we have $\mathcal{O}_K = S_{min,p} \subseteq S \subseteq \mathcal{O}_K$. This implies $S = \mathcal{O}_K$, which is a contradiction. Thus, $p\mathcal{O}_K$ is not a subset of S. Furthermore, if p divides f, then $f\mathcal{O}_K \subseteq p\mathcal{O}_K \not\subseteq S$, which again contradicts the assumption $f\mathcal{O}_K \subseteq S$. Thus, p does not divide f. □

Let (K,Φ) be CM type and (K^r,Φ^r) be its reflex type. As a consequence of this corollary, if $\Omega_{K^r} = I_{K^r}$, and whenever $S_{\min,p} = \mathcal{O}_K$, the prime p cannot divide any index $f \in \mathbb{Z}$ of an order $S \subsetneq \mathcal{O}_K$ that includes μ_K and satisfies $\Omega_S = I_{K^r}(f)$.

Now, let $P = \{p_1,\ldots,p_r\}$ represent a complete set of primes that might divide the index f of such an order. If $S_{\min,p_i} = \mathcal{O}_K$ for every prime $p_i \in P$ except one

specific prime p_j, then according to Corollary 8.9, the index takes the form $f = p_j^\ell$ for some $\ell \in \mathbb{N}$. Let $k(p_j)$ denote the integer at which the sequence $(S_{\min,p_j^k})_k$ stabilizes. In that case, $S_{\min,f}$ provides an overorder of $S_{\min,p_j^{k(p_j)}}$.

Building on the considerations from this section, we present the following algorithms for computing the orders $S_{\min,f}$ as described in Lemma 8.4, and for determining the order $S_{\min,p^{k(p)}}$ for a particular prime p.

Algorithm 2: Computing the order $S_{min,f}$

input : A CM type (K, Φ) with $\Omega_{\mathcal{O}_K} = I_{K^r}$ and an integer f.
output: The order $S_{min,f}$ of K.

Compute the reflex (K^r, Φ^r) of (K, Φ).
Compute the degree n of K over $\mathbb{Q}$.
Compute the maximal order $\mathcal{O}_K$ of K.
Compute a generator ζ of the torsion unit group of $\mathcal{O}_K$.
Compute a basis $(\beta_1, \ldots, \beta_n)$ of $\mathcal{O}_K$ as a $\mathbb{Z}$-module.
Compute generators $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ of the Ray class group of K modulo f.
for $i = 1, \ldots, s$ **do**
    Compute a generator $\alpha_i \in K$ of the reflex type norm N_{Φ^r} of $\mathfrak{a}_i$.
end
Compute the order $S_{min,f}$ of K generated by $\alpha_1, \ldots, \alpha_s$, $f \cdot \beta_1, \ldots, f \cdot \beta_n$, and ζ.
return $S_{min,f}$

Algorithm 3: Computing the order $S_{min,p^{k(p)}}$

input : A CM type (K, Φ) with $\Omega_{\mathcal{O}_K} = I_{K^r}$ and a prime number p.
output: The order $S_{min,p^{k(p)}}$.

Initialize k_1 as 0 and k_2 as 1.
Define f_1 as p^{k_1} and f_2 as p^{k_2}.
Compute the minimal orders S_{min,f_1} and S_{min,f_2} with Algorithm 2.
while $S_{min,f_1} \neq S_{min,f_2}$ **do**
    Replace k_1 with k_2 and raise k_2 by 1.
    Define f_1 as f_2 and f_2 as p^{k_2}.
    Define S_{min,f_1} as S_{min,f_2}.
    Compute the minimal order S_{min,f_2} with Algorithm 2.
end
return S_{min,f_1}

8.2 Application to simple genus 3 curves with field of moduli $\mathbb{Q}$

Let $C/\mathbb{C}$ be a simple genus 3 curve with complex multiplication by an order S in a sextic CM field K. Then its Jacobian J is a simple principally polarized abelian variety of dimension 3 over $\mathbb{C}$ of a primitive CM type (K, Φ). Let the field of moduli of J be $\mathbb{Q}$. By Theorem 8.1, K is a cyclic CM class number one field that contains an imaginary quadratic subfield. Consequently, K is listed in [Kıl16][Table 3.1]. Let f denote the index of S in $\mathcal{O}_K$. Theorem 8.1 also tells us that $\Omega_S = I_{K^r}(f)$, where $(K^r, \Phi^r) = (K, \Phi)$ is the reflex of (K, Φ), and, under the assumption that $\delta_S = 1$, provides explicit bounds on the primes which might divide f. We will now discuss two scenarios, one where the endomorphism ring of the Jacobian J of C contains $\mathbb{Z}[i]$ and the other where it contains $\mathbb{Z}[\zeta_3]$. We begin with the case where $\mathbb{Z}[i] \subseteq S$.

Theorem 8.10.
Let $C/\mathbb{C}$ be a simple genus 3 curve with complex multiplication by an order $S \supseteq \mathbb{Z}[i]$ in a CM field K. Let the field of moduli of C be $\mathbb{Q}$. Let K_0 denote the totally real cubic subfield of K, let $S_0 := S \cap K_0$, and let $S_{\mathbb{Q}(i)} := S \cap \mathbb{Q}(i)$. Then C is hyperelliptic. Furthermore, if $\delta_S = 1$, then S is one of the orders whose indices are given in Table 8.2. If S_0 is Gorenstein, then S is one of the orders in Table 8.3. If $S = S_{\mathbb{Q}(i)}\, S_0$, then S is one of the orders in Table 8.4.

Proof. Let $\mathbb{Z}[i] \subseteq S$. By Theorem 8.1, we know that K is a cyclic CM class number one field, which includes the imaginary quadratic subfield $\mathbb{Q}(i)$. Using Theorem 8.5, we deduce that C is hyperelliptic, and S contains the order $S_{\min,f}$, where f represents the index of S in $\mathcal{O}_K$. Assuming $\delta_S = 1$, Corollary 8.2 implies that only primes less than or equal to 17 can divide f. Define P as the set of primes up to 17. Employing Algorithm 3, we compute $S_{\min,p^{k(p)}}$ for each prime in P. We observe that $S_{\min,p^{k(p)}} = \mathcal{O}_K$ for all primes $p \neq 2$ in all six sextic CM class number one fields K containing $\mathbb{Q}(i)$. Building on the conclusions of Chapter 8.1, and given that f is an integer not divided by any prime not contained in P, we receive:

$$S_{\min,2^{k(2)}} \subseteq S_{\min,f} \subseteq S.$$

Furthermore, given that S is stable under complex conjugation, S is an overorder of

$$S'_{\min,2^{k(2)}} := S_{\min,2^{k(2)}} + \overline{S_{\min,2^{k(2)}}}.$$

We apply the MAGMA algorithm `FindOverOrders` from [Mar21] in order to compute every overorder of $S'_{\min,2^{k(2)}}$ which is stable under complex conjugation. This computation results in 33 orders from which 6 are maximal and 27 are non-maximal. The computational results are detailed in Appendix A. Table 8.1 summarizes our findings, providing the indices of the orders in their corresponding maximal order. Furthermore, Table 8.2 filters the orders from Table 8.1 based on the constraint $\delta_S = 1$. In Table 8.3 and Table 8.4 we further filter the orders from Table 8.3 by applying the conditions that S_0 is Gorenstein and $S = S_{\mathbb{Q}(i)}S_0$, respectively. □

In the following tables, applying the notation from Table 4.1, the tuple $[\beta_0, \beta_1, \beta_2]$ represents the defining irreducible monic polynomial $g = \sum_{i=0}^{3} \beta_i x^i \in \mathbb{Z}[x]$ of the totally real cubic subfield K_0 contained in K. Here, K is assumed to be the composite $K = \mathbb{Q}(i)K_0$. The other columns present the amount of suitable orders corresponding to a specific index. Detailed descriptions of these orders are presented in Appendix A.

Table 8.1: Suitable orders for $K = \mathbb{Q}(i)\, K_0$

No.	g	Index 1	Index 2	Index 4	Index 8	Index 16
1	$[1, -5, 2]$	1	0	1	3	1
2	$[-1, -3, 0]$	1	0	1	3	1
3	$[-1, -2, 1]$	1	0	1	3	1
4	$[8, -14, 1]$	1	3	1	0	0
5	$[-8, -10, 1]$	1	3	1	0	0
6	$[8, -18, 3]$	1	3	1	0	0

Table 8.2: Suitable orders with $\delta_S = 1$ for $K = \mathbb{Q}(i)\, K_0$

No.	g	Index 1	Index 2	Index 4	Index 8	Index 16
1	$[1, -5, 2]$	1	0	0	3	1
2	$[-1, -3, 0]$	1	0	0	3	1
3	$[-1, -2, 1]$	1	0	0	3	1
4	$[8, -14, 1]$	1	3	0	0	0
5	$[-8, -10, 1]$	1	3	0	0	0
6	$[8, -18, 3]$	1	3	0	0	0

Table 8.3: Suitable orders with $S_0 = S \cap K_0$ is Gorenstein for $K = \mathbb{Q}(i)\, K_0$

No.	g	Index 1	Index 2
1	$[1, -5, 2]$	1	0
2	$[-1, -3, 0]$	1	0
3	$[-1, -2, 1]$	1	0
4	$[8, -14, 1]$	1	3
5	$[-8, -10, -1]$	1	3
6	$[8, -18, 3]$	1	3

Table 8.4: Suitable orders with $S = S_{\mathbb{Q}(i)}\, S_0$ for $K = \mathbb{Q}(i)\, K_0$

No.	g	Index 1	Index 16
1	$[1, -5, 2]$	1	1
2	$[-1, -3, 0]$	1	1
3	$[-1, -2, 1]$	1	1
4	$[8, -14, 1]$	1	0
5	$[-8, -10, 1]$	1	0
6	$[8, -18, 3]$	1	0

If we omit the condition that $\delta_S = 1$, then, in general, we do not get an explicit bound on the primes dividing the index $[\,\mathcal{O}_K : S\,]$, unless we are considering specific classes of examples.

In situations where we do not have a complete set of primes P as previously mentioned, we make the assumption that the index is not divisible by any prime larger than 10^5. We then replace P in the proof of Theorem 8.10 with the set of all primes below 10^5 and apply the same search for potential endomorphism rings. We get that there appear no new orders. Apart from using a different set of primes P, the proof of Theorem 8.11 is the same as the one of Theorem 8.10.

Theorem 8.11.
Let $C/\mathbb{C}$ be a simple genus 3 curve with complex multiplication by an order $S \supseteq \mathbb{Z}[i]$ in a CM field K and field of moduli $\mathbb{Q}$. Then C is hyperelliptic, and if $[\,\mathcal{O}_K : S\,]$ is not divisible by any prime $p \geq 10^5$, then S is one of the orders whose indices are given in Table 8.1.

Proof. We replace the set P in the proof of Theorem 8.10 by the set of primes below or equal 10^5. Applying the same computations for this set of primes does not yield any orders beyond the ones presented in Theorem 8.10. □

Theorem 8.11 might be an indicator that the orders listed in Table 8.1 represent the only potential endomorphism rings of simple genus 3 CM curves C with field of moduli $\mathbb{Q}$ and complex multiplication by orders S which include $\mathbb{Z}[i]$. Within Chapter 9, we will explicitly compute hyperelliptic curves based on the orders detailed in Table 8.1 and determine whether their respective fields of moduli are $\mathbb{Q}$ or not.

Similar to our previous discussions, we now focus on the second situation, considering orders S where $\mathbb{Z}[\zeta_3] \subseteq S$. In order to apply Theorem 8.6, we assume that K fulfills the condition $|\mu_K| = 6$. This condition is satisfied for all cyclic sextic CM class number one fields K that include $\mathbb{Q}(\zeta_3)$, as listed in Table 4.2, except for field No.16, where $|\mu_K| = 18$.

Theorem 8.12.
Let $C/\mathbb{C}$ be a simple genus 3 Picard curve field of moduli field of moduli $\mathbb{Q}$ and complex multiplication by an order S in a CM field K with $|\mu_K| = 6$. Let K_0 denote the totally real cubic subfield of K. Then $\mathbb{Z}[\zeta_3] \subseteq S$, and if $\delta_S = 1$, then S is maximal. Especially, for $S_0 = S \cap K_0$ and $S_{\mathbb{Q}(\zeta_3)} = S \cap \mathbb{Q}(\zeta_3)$, if S_0 is Gorenstein or if $S = S_{\mathbb{Q}(\zeta_3)} S_0$, then S is maximal.

Proof. Given that C is a Picard curve, Theorem 4.18 implies that $\mathbb{Z}[\zeta_3] \subseteq S$. By Theorem 8.1, we deduce that K is a cyclic CM class number one field that includes the imaginary quadratic subfield $\mathbb{Q}(\zeta_3)$. Since $|\mu_K| = 6$, when applying Theorem 8.6, we receive that S contains the order $S_{\min,f}$, where $f = [\,\mathcal{O}_K : S\,]$. Assuming $\delta_S = 1$, Corollary 8.2 provides that only primes up to 13 can divide f. Let P denote the set of such primes. Applying Algorithm 3, we compute $S_{\min,p^{k(p)}}$ for each prime within P and discover that $S_{\min,p^{k(p)}} = \mathcal{O}_K$ for all primes $p \neq 3$ in all the nine sextic CM fields. Following the considerations presented at the end of Chapter 8.1, and given that f is an integer not divided by any prime not contained in P, we conclude:

$$S_{\min,3^{k(3)}} \subseteq S_{\min,f} \subseteq S.$$

Now, given that S is stable under complex conjugation, it is an overorder of

$$S'_{\min,3^{k(3)}} := S_{\min,3^{k(3)}} + \overline{S_{\min,3^{k(3)}}}.$$

Once more, we apply the MAGMA algorithm `FindOverOrders` from [Mar21] to determine the overorders of $S'_{\min,3^{k(3)}}$ that are stable under complex conjugation in all nine fields.

This search produces 13 orders in total, of which 9 are maximal and 4 are non-maximal. The detailed results of these computations are outlined in Appendix B. The obtained indices are presented in Table 8.5. None of these non-maximal orders actually fulfills $\delta_S = 1$. □

Following the notation from Table 4.2, in Table 8.5, the tuple $[\beta_0, \beta_1, \beta_2]$ determines the defining irreducible monic polynomial $g = \sum_{i=0}^{3} \beta_i \, x^i \in \mathbb{Z}[x]$ of the totally real cubic subfield K_0 of K such that $K = \mathbb{Q}(\zeta_3) \, K_0$ and $|\mu_K| = 6$. The other columns give the amount of suitable orders for the specific index.

Table 8.5: Suitable orders for $K = \mathbb{Q}(\zeta_3) \, K_0$

No.	g	Index 1	Index 9
7	$[1, -4, 1]$	1	1
8	$[-1, -2, 1]$	1	1
9	$[-8, -10, 1]$	1	1
10	$[8, -14, 1]$	1	1
11	$[8, -18, 3]$	1	0
12	$[1, -9, 6]$	1	0
13	$[-64, -36, 3]$	1	0
14	$[-27, -15, 4]$	1	0
15	$[-27, -21, 2]$	1	0

Again, if we omit the condition $\delta_S = 1$, we can only provide a complete set of primes dividing the index $[\, \mathcal{O}_K : S \,]$ in specific classes of examples. Assuming that the index is divisible only by primes less than 10^5, we modify P in the previous proof of Theorem 8.12 to contain all primes below or equal 10^5. Once more, we observe that no orders appear apart from those with indices specified in Table 8.5. For further details, we refer to Appendix B. When replacing the set of primes P, the argument in the following theorem is precisely the one of Theorem 8.12.

Theorem 8.13.
Let $C/\mathbb{C}$ be a simple genus 3 Picard curve with field of moduli $\mathbb{Q}$ and complex multiplication by an order S in a CM field K with $|\mu_K| = 6$. Then $\mathbb{Z}[\zeta_3] \subseteq S$, and if $[\, \mathcal{O}_K : S \,]$ is not divisible by any prime $p \geq 10^5$, then S is one of the orders in Table 8.5.

Proof. Replacing the set P in the proof of Theorem 8.12 by the set of primes below 10^5 and applying the same computations for this set of primes does not yield any orders beside those presented in Table 8.5. □

Chapter 9

Computing genus 3 curves with CM by arbitrary orders

In this concluding chapter, we aim to show how to determine isomorphism classes of simple genus 3 curves $C/\mathbb{C}$ that have complex multiplication by arbitrary orders and field of moduli $\mathbb{Q}$. This combines the theoretical results and algorithms presented in the previous chapters.

We recall that on the one hand, the Jacobians of simple curves over $\mathbb{C}$ are principally polarized abelian varieties over $\mathbb{C}$. On the other hand, according to Theorem 1.85, every principally polarized abelian variety of dimension three over $\mathbb{C}$ is the Jacobian of a simple genus three curve over $\mathbb{C}$. Therefore, over $\mathbb{C}$, the principally polarized abelian varieties of dimension three correspond exactly to the Jacobian of simple genus three curves.

Moreover, as a consequence of Torelli's theorem (see Theorem 1.84), there exists a bijection between the isomorphism classes of genus three curves over $\mathbb{C}$ and the isomorphism classes of their Jacobians. Consequently, determining the isomorphism classes of simple genus three curves over $\mathbb{C}$ with complex multiplication by an arbitrary order S in a CM field K is equivalent to determining the isomorphism classes of simple principally polarized abelian varieties of dimension three over $\mathbb{C}$ with complex multiplication by an arbitrary order S in a CM field K.

As presented in [Kıl16][Theorem 4.1.1], there are precisely 37 isomorphism classes of principally polarized abelian varieties over $\mathbb{C}$ having complex multiplication by maximal orders and field of moduli $\mathbb{Q}$. Each isomorphism class corresponds to a sextic CM class number one field that contains an imaginary quadratic subfield, as listed in [Kıl16][Table 3.1]. Addressing this for non-maximal orders remains an open question. We give partial answers to this question in this chapter. For context, we refer to [BS17] in which the genus 2 case was discussed. This paper builds the foundation of our discussion on the genus 3 case.

We summarize the previous discussions. Firstly, as outlined in Chapter 3, in order to identify isomorphism classes of simple principally polarized abelian varieties of dimension 3 over $\mathbb{C}$ having complex multiplication by an arbitrary order S, we want to find certain quadruples $(K, \Phi, \mathfrak{a}, \xi)$.

Within such a quadruple, we let K be a sextic CM field, let Φ be a primitive CM type of K, and let $(\mathfrak{a}, \xi)$ be a principally polarized ideal class of an order S in K. Then, $\mathfrak{a}$ is a proper fractional ideal of S, and ξ is a specific element of K as defined in Chapter 3. We let (K^r, Φ^r) denote the reflex of (K, Φ).

Now, let $\mathcal{P}$ be a simple principally polarized abelian variety of type $(K, \Phi, \mathfrak{a}, \xi)$ and let the field of moduli of $\mathcal{P}$ be $\mathbb{Q}$. Then, due to Corollary 4.9, K is a cyclic sextic CM class number one field containing an imaginary quadratic subfield and $\Omega_S = I_{K^r}(f)$ for $f := [\,\mathcal{O}_K : S\,]$. As discussed in Chapter 5, this includes that $K^r = K$ and $\Phi^r = \Phi$.

Hence, our approach to determine all isomorphism classes of simple genus 3 curves having field of moduli $\mathbb{Q}$ can roughly be divided into the subsequent steps:

(a) Determine the cyclic sextic CM class number one fields K containing an imaginary quadratic subfield.
(b) Find all orders S in K, which are stable under complex conjugation and fulfill $\Omega_S = I_{K^r}(f)$.
(c) Compute representatives of all principally polarized ideal classes $(\mathfrak{a}, \xi)$, as in Chapter 3.
(d) Reconstruct models of the curves corresponding to the principally polarized abelian varieties.

The fields mentioned in (a) correspond directly to those listed in [Kıl16][Table 3.1]. The second point, (b), is the most challenging. We present results in Chapter 8 for the two cases $\mathbb{Z}[i] \subseteq S$ and $\mathbb{Z}[\zeta_3] \subseteq S$ (excluding the one field where $|\mu_K| = 18$). These cases yield either hyperelliptic or Picard curves. To be precise, in Chapter 8, we identify all such orders S with constraints on the primes dividing the index $[\,\mathcal{O}_K : S\,]$ and provide a complete description whenever $\delta_S = 1$. For these specific orders S, in both scenarios, we calculate all principally polarized ideal classes $(\mathfrak{a}, \xi)$ for (c) applying Algorithm 1. Further details and outcomes are presented in Chapter 9.1 and Chapter 9.2. In the following sections we do now aim to answer (d).

9.1 Picard curves with CM by an order $S \supseteq \mathbb{Z}[\zeta_3]$

Summarizing our results on Picard curves with complex multiplication and field of moduli $\mathbb{Q}$, we state two main theorems.

Theorem 9.1.
Let K be a sextic CM field with $|\mu_K| \neq 18$ and totally real cubic subfield K_0. There is no simple Picard curve $C/\mathbb{C}$ of genus 3 having field of moduli $\mathbb{Q}$ and complex multiplication by a non-maximal order S in K with $\delta_S = 1$. In particular, there is no such Picard curve satisfying either the condition that S_0 is Gorenstein or the condition that $S = S_{\mathbb{Q}(\zeta_3)}\, S_0$, where $S_{\mathbb{Q}(\zeta_3)} := S \cap \mathbb{Q}_{\zeta_3}$ and $S_0 := S \cap K_0$.

Proof. Let $C/\mathbb{C}$ be a simple Picard curve of genus 3 with CM by a non-maximal order S in K with $\delta_S = 1$ and field of moduli $\mathbb{Q}$. Then, due to Theorem 8.12, S is maximal. This contradicts the assumption that S is non-maximal. □

Additionally, when we omit the condition $\delta_S = 1$ and instead assume that the index $[\,\mathcal{O}_K : S\,]$ is divisible only by primes less than 10^5, we obtain at the following theorem, which was verified computationally using Algorithm 1.

Theorem 9.2.
Let K be a sextic CM field with $|\mu_K| \neq 18$ and totally real cubic subfield K_0. There is no simple Picard curve $C/\mathbb{C}$ having field of moduli $\mathbb{Q}$ and complex multiplication by a non-maximal order S in K such that $[\,\mathcal{O}_K : S\,]$ is only divisible by prime numbers $p \leq 10^5$.

Proof. Let $C/\mathbb{C}$ be a simple Picard curve of genus 3 with CM by a non-maximal order S in K. Let $[\,\mathcal{O}_K : S\,]$ be only divisible by prime numbers $p \leq 10^5$, and let C have field of moduli $\mathbb{Q}$. Then, due to Theorem 8.13, S is one of the orders in Appendix B whose indices are also presented in Table 8.5. None of these 4 non-maximal orders provides a principally polarized ideal class. This contradicts the assumption that C has CM by S. □

9.2 Hyperelliptic genus 3 curves with CM by an order $S \supseteq \mathbb{Z}[i]$

When considering simple hyperelliptic genus 3 curves with CM by a non-maximal order S that includes $\mathbb{Z}[i]$, a more in-depth understanding of the explicit construction of the curves is required. Generally, taking $(\mathfrak{a}, \xi)$ as a principally polarized ideal class that determines an isomorphism class, as described in Chapter 3 (computed using Algorithm 1), we describe the process of computing a model of the corresponding hyperelliptic curve. Finally, we will present an explicit reconstruction algorithm in Chapter 9.2.5. The computational results are given in Chapter 9.2.6 and Chapter 9.2.7. Our implementations in MAGMA ([Bos+22]) are based on the very useful packages [SCV21], [Sij22], and [Sij21].

9.2.1 Computing the period matrix

Building on the findings in Chapter 3, with a particular focus on Theorem 3.3, let g be a positive integer, and let (K, Φ) be a CM type where $[\, K : \mathbb{Q}\,] = 2g$. Given a principally polarized ideal class $(\mathfrak{a}, \xi)$ of an order S in K, our goal is to determine the associated period matrix Ω in the Siegel upper half-space $\mathbb{H}_g$. For a detailed exploration, we refer to [Lan83].

Revisiting Theorem 3.3, the CM type Φ and ξ are chosen such that

$$K = K_0(\xi)\,, \quad -\xi^2 \in K_0^{++}\,, \quad \text{and } \operatorname{Im}\phi(\xi) > 0 \quad \text{for all } \phi \in \Phi.$$

We represent the embeddings in Φ by $\phi_1, \ldots, \phi_g$. For two vectors in $\mathbb{C}^{g\times 1}$, namely $x = (x_1, \ldots, x_g)^T \in \mathbb{C}^{g\times 1}$ and $y = (y_1, \ldots, y_g)^T \in \mathbb{C}^{g\times 1}$, we introduce a Riemann form as

$$E_\xi(x, y) = \sum_{j=1}^{g} \phi_j(\xi)(\bar{x_j} y_j - x_j \bar{y_j}).$$

Given that $\phi_j(\xi)$ is purely imaginary with a positive imaginary part, this symmetric form E_ξ is positive definite. Moreover, for any $\alpha, \beta \in K$, we have

$$E_\xi(\Phi(\alpha), \Phi(\beta)) = \operatorname{Tr}_{K/\mathbb{Q}}(\xi \bar{\alpha} \beta).$$

For the computation, an initial step is determining a $\mathbb{Z}$-basis $\mathcal{A} = (a_1, \ldots, a_{2g})$ for $\mathfrak{a}$ such that $\Phi(\mathcal{A})$ is *symplectic with respect to* E_ξ. This means that

$$E_\xi(\Phi(a_i), \Phi(a_j))_{i,j} = \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix}.$$

We define the vectors $b_i := \Phi(a_i) \in \mathbb{C}^g$. Then, we let $\Omega_1 := (b_1 \cdots b_g) \in \mathbb{C}^{g\times g}$, and let $\Omega_2 := (b_{g+1} \cdots b_{2g}) \in \mathbb{C}^{g\times g}$. Then $\Phi(\mathfrak{a}) \approx \Omega_1\mathbb{Z}^g + \Omega_2\mathbb{Z}^g$, which is isomorphic to $\mathbb{Z}^g + \Omega\mathbb{Z}^g$. In this context, $\Omega := \Omega_2^{-1}\Omega_1$ is contained in $\mathbb{H}_g$ and represents the period matrix corresponding to $(\mathfrak{a}, \xi)$.

9.2.2 The Rosenhain model of a hyperelliptic curve

Definition 9.3.
Let C be a hyperelliptic genus g curve over $\mathbb{C}$. A complex model

$$C : y^2 = x\,(x-1)\,(x-a_3)\cdots(x-a_{2g+1})$$

where $a_3, \ldots, a_{2g+1} \in \mathbb{C}$, is called *Rosenhain model* of C.

We assume that a period matrix $\Omega \in \mathbb{H}_g$ is given.

Definition 9.4.
A period matrix $\Omega \in \mathbb{H}_g$ is called *hyperelliptic* if it represents the Jacobian of a hyperelliptic curve.

We provide a brief overview on how to determine whether Ω is hyperelliptic, following [Wen01a]. Recall the definitions of theta characteristics as discussed in Chapter 1.5.2.

Definition 9.5.
We call a set $\{\eta_i \mid i = 1, \ldots, 2g+1\}$ of distinct column vectors $\eta_i \in (\mathbb{Z}/2\mathbb{Z})^{2g} \setminus \{0\}$ such that for all $\eta_i = \begin{bmatrix}\delta_i \\ \varepsilon_i\end{bmatrix}$ and $\eta_j = \begin{bmatrix}\delta_j \\ \varepsilon_j\end{bmatrix}$ with $i \neq j$ we have $\eta_i^T\,\eta_j \equiv 0 \pmod 2$ an *azygetic fundamental system*.

For $\{\eta_i \mid i = 1, \ldots, 2g+1\}$, $B := \{1, \ldots, 2g+1\}$ and $T \subseteq B$, we define $\eta_T := \sum_{t\in T} \eta_t$ and for $U \subseteq B$ we define $T \circ U := (T \cup U) \setminus (T \cap U)$. We can now state the following theorem, which is [Wen01a][Theorem 4.2].

Theorem 9.6.
Let $\Omega \in \mathbb{H}_g$ be a period matrix. Then Ω is hyperelliptic if and only if there exists an azygetic fundamental system $\{\eta_i \mid i = 1, \ldots, 2g+1\}$ such that the theta constants $\Theta[\eta_T](\Omega)$ vanish in Ω for $T \subseteq B$ with $|T| \equiv 0 \pmod 2$ if and only if $|(T \circ U)| \neq g+1$, where $U = \{u \in B \mid u \equiv 1 \pmod 2\}$.

Note that by [Mum07] we can immediately provide such an azygetic fundamental system (see also citeWEHYP). Furthermore, $\mathrm{Sp}(2g, \mathbb{Z}/2\mathbb{Z})$ acts transitively on the set of azygetic fundamental systems.

Definition 9.7.
An azygetic fundamental system is called *admissible* if all even theta constants are contained in

$$M := \{\Theta[\eta_T] \mid |T| \equiv 0 \pmod 2 \text{ and } |(T \circ U)| \neq g+1\}.$$

In the case when $g = 3$, according to [Wen01a][Section 4.2], there are 29 subsets $T \subseteq B = \{1, \ldots, 7\}$ such that $|T| \equiv 0 \pmod 2$ and $|(T \circ U)| \neq 4$, where we have $U = \{1, 3, 5, 7\}$ for this scenario. Conversely, there are 28 odd theta constants. Therefore, when choosing any admissible fundamental system, there exists precisely one even theta constant $\Theta[\eta]$ where $\eta = \eta_T$ for a certain subset T that fulfills the conditions $|T| \equiv 0 \pmod 2$ and $|(T \circ U)| \neq 4$. Following this, the theorem given above can be reduced to the following criterion, which is [Wen01a][Theorem 4.3].

Theorem 9.8.
Let $\Omega \in \mathbb{H}_3$ be a period matrix. Then Ω is hyperelliptic if and only if exactly one even theta constant vanishes in Ω.

Let $\Omega \in \mathbb{H}_3$ be hyperelliptic. We are then able to compute a Rosenhain model of C using the vanishing theta constant and the azygetic fundamental system as outlined in [Web97], [Wen01a], and [Bal+16]. In our computational work, we applied the algorithms provided in the Magma package [Sij22], especially the fast theta computation algorithm `CalculTheta`, which is originally presented in [LT16].

9.2.3 The Shioda invariants of a hyperelliptic curve

We first provide a very brief introduction to Shioda invariants. Then we explain how to compute them when given a Rosenhain model of a hyperelliptic curve of genus three. For a more profound understanding and definitions related to this topic, we refer to [LR12] and [Wen01b], which are also the references for the following discussions.

Consider a field k together with its algebraic closure denoted as $\bar{k}$. Let V be a 2-dimensional vector space over k, together with a basis (X, Z). For a given positive integer $n \in \mathbb{Z}$, let $S^n(V)$ denote the vector space of dimension $n+1$ containing homogeneous forms of degree n in terms of (X, Z). Let G be a subset of $\mathrm{GL}(2, k)$ and M be contained in G. For any form $F \in S^n(V)$, we can define the action of M on F as $(M.F)(X, Z) = F(M^{-1}(X, Z))$, resulting in a projectively equivalent binary form $M.F$.

Definition 9.9.
Let $r \geq 0$ be an integer and $(n_1, \ldots, n_m)$ be positive integers. We call a multi-homogeneous polynomial function

$$C : \bigoplus_{i=1}^{m} S^{n_i}(V) \longrightarrow S^r(V)$$

of multi-degree $(d_1, \ldots, d_m)$ a *covariant* if there exists $\omega \in \mathbb{Z}$ such that

$$C(M.F_1, \ldots, M.F_m) = \det(M)^{-\omega}\, M.C(F_1, \ldots, F_m)$$

for all $M \in G$ and $(F_1, \ldots, F_m) \in \oplus_{i=1}^{m} S^{n_i}(V)$. The integer r is called the *order* of C and if $r = 0$, then C is called an *invariant*. The quotient of two invariants is called an *absolute invariant*.

We have special interest in the case $m = 1$, in which we set $n := n_1$ and $d := d_1$. Here r is called the *order* of the covariant and whenever $nd - r \equiv 0 \pmod 2$, we call ω the *weight* of the covariant. Otherwise, the covariant is zero. Note that $F(X, Z) \in S^n(V)$ is actually a covariant of degree n and of order 1.

Definition 9.10.
Let g_1 and g_2 be covariants of degree n and m and orders r and s, respectively. For any $h \in \mathbb{N}$, we define the *h-th ueberschiebung* of g_1 and g_2 as

$$(g_1\, g_2)_h := \frac{(m-h)!\,(n-h)!}{m!\,n!} \left(\frac{\partial g_1}{\partial x}\frac{\partial g_2}{\partial z} - \frac{\partial g_1}{\partial z}\frac{\partial g_2}{\partial x} \right)^h .$$

In the notation of the definition, the h-th ueberschiebung of g_1 and g_2 determines another covariant of degree $n + m$ and order $r + s - 2h$.

Let us revisit the scenario where $C : y^2 = f(x)$ and $\deg f \in \{2g + 1, 2g + 2\}$ defines a hyperelliptic curve of genus g. This could be represented by a Rosenhain model of $C/\mathbb{C}$. By homogenizing $f(x)$, we obtain $Y^2 = F(X, Z)$ where F is a binary form of degree $2g + 2$. Let $\mathcal{I}_{2g+2}$ denote the graded ring of invariants. The following proposition, presented in [LR12][Proposition 1.3], states that, up to a specific equivalence, the potential values of a generator set for $\mathcal{I}_{2g+2}$ correspond to the points in the coarse moduli space of hyperelliptic curves of genus g.

Proposition 9.11.
Let $\{I_i\}$ be a set of homogeneous generators of $\mathcal{I}_{2g+2}$ and $d_i := \deg I_i$. Then two hyperelliptic curves $C_1 : y^2 = f_1(x)$ and $C_2 : y^2 = f_2(x)$ of genus g are $\bar{k}$-isomorphic if and only there exists $\lambda \in \bar{k}^\times$, such that $I_i(f_2) = \lambda^{d_i} I_i(f_1)$ for all i.

Definition 9.12.
Let f be a binary octic. The following set of invariants is called *Shioda invariants*:

$$J_2 = (f\,f)_8, \quad J_3 = (f\,\mathfrak{g})_8, \quad J_4 = (\mathfrak{e}\,\mathfrak{e})_4, \quad J_5 = (\mathfrak{m}\,\mathfrak{e})_4, \quad J_6 = (\mathfrak{e}\,\mathfrak{h})_4,$$
$$J_7 = (\mathfrak{m}\,\mathfrak{h})_4, \quad J_8 = (\mathfrak{p}\,\mathfrak{h})_4, \quad J_9 = (\mathfrak{n}\,\mathfrak{h})_4, \quad J_{10} = (\mathfrak{q}\,\mathfrak{h})_4\,.$$

Here we let

$$\mathfrak{g} = (f\,f)_4, \quad \mathfrak{e} = (f\,f)_6, \quad \mathfrak{h} = (\mathfrak{e}\,\mathfrak{e})_2, \quad \mathfrak{m} = (f\,\mathfrak{e})_4,$$
$$\mathfrak{n} = (f\,\mathfrak{h})_4, \quad \mathfrak{p} = (\mathfrak{g}\,\mathfrak{e})_4, \quad \mathfrak{q} = (\mathfrak{g}\,\mathfrak{h})_4.$$

Now let $g = 3$, and let f be a binary octic. Then, as shown in [Shi67], the Shioda invariants are generators for $\mathcal{I}_8$ and provided due to the ueberschiebung of f. Note that, according to Proposition 9.11, the invariants $J_2, \ldots, J_{10}$ uniquely determine the isomorphism class. Furthermore, only the invariants $J_2, \ldots, J_7$ are algebraically independent, while J_8, J_9, and J_{10} can be expressed in terms of $J_2, \ldots, J_7$. For our specific situation, we present the subsequent lemma, which originally appears in [Wen01b][Corollary 4.4.5] and is also mentioned in [LR12][Lemma 3.4].

Lemma 9.13.
Let $C : x^2 = f(x)$ be a hyperelliptic curve over a subfield k of $\mathbb{C}$ with $Aut(C) \supseteq C_4$, then $J_i(f) = 0$ for all $i = 3, 5, 7, 9$ and the isomorphism class of C over $\bar{k}$ is uniquely determined by $(J_2, J_4, J_6, J_8, J_{10})$.

Note that Weng has used specific absolute invariants $j_1, \ldots, j_9$, which are formulated as products of $J_2, \ldots, J_{10}$ divided by the discriminant Δ of the binary form f. Specifically, she defined

$$j_1 := \frac{J_2^7}{\Delta}, \quad j_3 := \frac{J_2^5 J_4}{\Delta}, \quad j_5 := \frac{J_2^4 J_6}{\Delta}, \quad j_7 := \frac{J_2^3 J_8}{\Delta}, \quad j_9 := \frac{J_2^2 J_{10}}{\Delta}\,.$$

For our calculations, we applied [Sij22]. In order to reconstruct a model of the curve in the subsequent step, it is essential to recognize the Shioda invariants as algebraic elements. The package [SCV21] provides the algorithm `NumberFieldExtra`, which proved to be highly effective in identifying complex Shioda invariants as algebraic numbers.

9.2.4 From Shioda invariants to hyperelliptic curves

The remaining task is to reconstruct the curve from its Shioda invariants. A method for this is provided in [LR12]. This method depends on the automorphism group of the curve (see [LR12][Algorithm 3]). In the case where $\mathrm{Aut}(C) = C_4$, the hyper-

elliptic curve C can be defined over its field of moduli k_0 (see [LR12][Proposition 4.18]). To be precise, there exists $f \in k_0[x]$ such that $C : y^2 = f(x)$. For the reconstruction of a model of the curve over its field of moduli from the Shioda invariants, we apply the MAGMA function `HyperellipticCurveFromShiodaInvariants`.

Note that, if $C : y^2 = f(x)$ for some polynomial $f \in k[x]$, then its Shioda invariants $I_2(f), \ldots, I_{10}(f)$ are contained in k. Specifically, if C has a model over $\mathbb{Q}$, then the Shioda invariants are elements in $\mathbb{Q}$.

9.2.5 Hyperelliptic curve reconstruction algorithm

In order to summarize the discussions of this section, we present a final algorithm for reconstructing a hyperelliptic curve. Let $(\mathfrak{a}, \xi)$ be a principally polarized ideal class $(\mathfrak{a}, \xi)$, where the multiplier ring of $\mathfrak{a}$ is an order $S \supseteq \mathbb{Z}[i]$ in a sextic CM class number one field $K \supseteq \mathbb{Q}(i)$. The element $\xi \in K$ defines a primitive CM type Φ mapping ξ to the positive imaginary axis. If we define $f := [\,\mathcal{O}_K : S\,]$, then $\Omega_S = I_{K^r}(f)$, where K^r is the reflex field of (K, Φ). Then $(\mathfrak{a}, \xi)$ uniquely characterizes an isomorphism class of the Jacobian J of a hyperelliptic curve C with its field of moduli k_0 contained within the reflex field K^r.

The following Algorithm 4 computes a hyperelliptic model of C over k_0 by specifically applying the mentioned algorithms from [SCV21], [Sij22], and [Sij21]. In order to identify the Shioda invariants as algebraic numbers, we use of the function `NumberFieldExtra`. Note that, in our applications, we do not exceed a precision of 5400 digits in order to identify the Shioda invariants as algebraic integers. In most cases, a precision of 1000 digits is enough.

Algorithm 4: Principally Polarized Ideal Class To Curve

input : A principally polarized ideal class $(\mathfrak{a}, \xi)$ as above.

output: A hyperelliptic model of the curve over the field of moduli k_0.

Find the primitive CM type Φ that maps ξ to the positive imaginary axis.
Compute a $\mathbb{Z}$-basis $\mathscr{A}$ of $\mathfrak{a}$ such that $\Phi(\mathscr{A})$ is symplectic with respect to E_ξ.
Initialize a precision *prec*.
Compute the period matrix Ω with precision *prec*.
Reduce Ω with LLL algorithm.
Compute the theta values of Ω.
Construct a complex Rosenhain model C_{ros} from the theta values.
Compute complex Shioda invariants T from C_{ros}.
Try to algebraize T over the subfields of the reflex field K^r of (K, Φ).
while dind't find algebraic Shiodas **do**
    Raise the precision *prec*.
    Compute the period matrix Ω with precision *prec*.
    Reduce Ω with LLL algorithm.
    Compute the theta values of Ω.
    Construct a complex Rosenhain model C_{ros} from the theta values.
    Compute complex Shioda invariants T from C_{ros}.
    Try to algebraize T over the subfields of the reflex field K^r of (K, Φ).
end
Compute a model C/k_0 from the algebraized Shioda invariants.
return C

9.2.6 Results for hyperelliptic curves over $\mathbb{Q}$

Having discussed the construction of a simple genus three hyperelliptic curve over its field of moduli applying Algorithm 1 and Algorithm 4, we can now formulate the following theorems for these curves.

Theorem 9.14.
Let K be a sextic CM field with totally real cubic subfield K_0. There is no simple hyperelliptic curve C defined over $\mathbb{Q}$ having complex multiplication by a non-maximal order $S \supseteq \mathbb{Z}[i]$ in K such that $\delta_S = 1$.

Proof. Let $C/\mathbb{C}$ be a simple hyperelliptic curve of genus 3 with field of moduli $\mathbb{Q}$ and CM by a non-maximal order $S \supseteq \mathbb{Z}[i]$ satisfying $\delta_S = 1$. Given Theorem 8.10, S is one of the orders listed in Appendix A, with their respective indices presented in Table 8.2. Applying Algorithm 1, we calculate every principally polarized ideal class for each of the 21 non-maximal orders S. For every such class, we apply Algorithm 4 to compute the Shioda invariants and a model of C over its field of moduli k_0. Observing that none of these Shioda invariants are completely defined over $\mathbb{Q}$, it follows that none of these curves have field of moduli $\mathbb{Q}$, which contradicts our initial assumption. Hence, none of these curves can be represented over $\mathbb{Q}$. □

While performing the computations for the proof of Theorem 9.14, we observe that each set of Shioda invariants is defined over the totally real cubic subfield K_0 of K. Furthermore, we derive models of the curves over $k_0 = K_0$. Note that, due to Corollary 4.7 and the fact that $\Omega_S = I_K(f)$, we already know that a model should exist over a subfield of K. However, the precise field only becomes evident when computing the Shioda invariants.

We mention that not all considered orders deliver principally polarized ideal classes. The subsequent table presents the number of classes for each of the orders. The numbering of the orders corresponds to the convention in Appendix A.

Table 9.1: Non-maximal orders $\mathbb{Z}[i] \subsetneq S$ with principally polarized ideal classes

No.	1.2.	1.3.	1.4.	2.2.	2.3.	2.4.	3.2.	3.3.	3.4.
# ppics	2	3	2	2	2	2	2	2	2

On the other hand, omitting the condition that $\delta_S = 1$, but assuming that the index $[\,\mathcal{O}_K : S\,]$ is only divisible by primes smaller than 10^5, we find the subsequent theorem.

Theorem 9.15.
Let K be a sextic CM field with totally real cubic subfield K_0. There is no simple hyperelliptic curve C defined over $\mathbb{Q}$ having complex multiplication by a non-maximal order $S \supseteq \mathbb{Z}[i]$ in K such that $[\,\mathcal{O}_K : S\,]$ is only divisible by primes $p \leq 10^5$.

Proof. Let $C/\mathbb{C}$ be a simple hyperelliptic genus 3 curve with field of moduli $\mathbb{Q}$ and CM by a non-maximal order $S \supseteq \mathbb{Z}[i]$ such that $[\,\mathcal{O}_K : S\,]$ is divisible only by primes $p \leq 10^5$. Then, by Theorem 8.11, S corresponds to one of the orders listed in Appendix A, with their indices also shown in Table 8.1. By using Algorithm 1, we compute every principally polarized ideal class for each of the non-maximal orders S. For each of these classes, applying Algorithm 4, we observe that none of the resulting sets of Shioda invariants are entirely defined over $\mathbb{Q}$. Consequently, none of these curves has field of moduli $\mathbb{Q}$, contradicting our initial assumption. Specifically, none of these curves can be defined over $\mathbb{Q}$. □

9.2.7 Results for hyperelliptic curves over K_0

For 17 of the 19 computed principally polarized ideal classes in a non-maximal order $S \supseteq \mathbb{Z}[i]$, we are able to compute a model of the corresponding hyperelliptic curve over the totally real cubic subfield K_0 of the CM class number one field K using Algorithm 4. We provide a very brief summary of the reduction process of their models and refer to [BS15] for more details.

In general, following the notation in [BS15], if $H_n(k)$ denotes the set of separable binary forms of degree $n \geq 3$ in $k[X, Z]$ for some field k, then $\mathrm{GL}(n, k) \times k^*$ acts on $H_n(k)$ via

$$\left(F(X,Z), \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u\right)\right) \mapsto u\, F(aX + bZ, cX + dZ)\,.$$

If $f \in k[x]$ is a polynomial such that $f(x) = F(x, 1)$, then this action comes down to

$$\left(f(x) \times \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u\right)\right) \mapsto u\,(cx + d)^n\, f\left(\frac{ax + b}{cx + d}\right)\,.$$

Now let $n \geq 6$ be even, $F \in H_n(k)$ and $f \in k[x]$ define the hyperelliptic curve C of genus $g = (n - 2)/2$ meaning that $C : Y^2 = F(X, Z)$ in the weighted projective space $\mathbb{P}^{(1,g+1,1)}$ and $C : y^2 = f(x)$ is an affine model of C. The following proposition is [BS15][Proposition 4.1].

Proposition 9.16.
Let k be a field and $F, F_1 \in H_{2g+2}(k)$ for $g \geq 2$. If $\mathrm{Aut}(C)_{\bar{k}} = \{1, \iota\}$, where ι denotes the hyperelliptic involution, then C_F and C_{F_1} are isomorphic over $\bar{k}$ if and only if they lie in the same orbit of $\mathrm{GL}(n,k) \times k^*$.

Due to Proposition 9.16, we may find smaller models of the curves by searching for minimal representatives within a specific orbit. To be more precise, we aim to compute a binary form F within an orbit for which the valuation of the discriminant is minimal for all places of k. Generally, there does not always exists such a binary form (see [BS15][Chapter 4.2.2]). Fortunately, if k has class number one, then such a minimal binary form exists. This condition is met for all our considered totally real cubic number fields K_0. Moreover, we assume that $\mathbb{Z}[i] \subseteq S$. Hence, for each of our 19 principally polarized ideal classes the automorphism group of the curve over $\bar{K_0}$ is $\{1, \iota\}$. This justifies the application of the reduction algorithms `reduce_gcd` and `reduce_discriminant` from [BS22] (implemented in SageMath [The21]). For a more detailed discussion on the reduction of binary forms, we direct the reader to [SC03] and [BS15]. In order to verify the complex multiplication of the curves C/K_0, we use the function `HeuristicEndomorphismAlgebra` from [Sij21]. In Appendix E, we present some examples of the models (after applying both `reduce_gcd` and `reduce_discriminant`) of the resulting simple hyperelliptic curves C/K_0 that have complex multiplication by a non-maximal order $S \supseteq \mathbb{Z}[i]$.

9.3 Outlook

There are still various open questions that are worth considering for future research on these topics.

Firstly, in order to limit the number of CM types (K, Φ) to consider, we assumed our principally polarized abelian varieties of dimension 3 with complex multiplication by an order S in K to have field of moduli $\mathbb{Q}$. As highlighted in Chapter 8.2, the resulting CM fields are cyclic Galois. A potential generalization would be considering any field of moduli contained in the reflex field K^r. This would still result in CM class number one orders.

Secondly, it is of interest to explore cases where $\delta_S \neq 1$. This would make it quite challenging to follow the presented approach, as we could lose the divisibility criterion from Chapter 6.2. However, it would significantly expand the range of possible endomorphism rings.

Another research direction could be to seek smaller models of the curves over the totally real cubic subfield K_0 of $\mathbb{Q}$. Unfortunately, over number fields larger

than $\mathbb{Q}$, the reduction techniques for models are rare. Nevertheless, this presents an opportunity for future research.

We only briefly touched Gorenstein orders in number fields. These orders come with a lot of useful structure. They are certainly worth a detailed examination. We provided some computational insights and developed a foundation for better understanding these orders, especially in number fields of degree three or greater.

Lastly, but not less significant, the CM methods for hyperelliptic genus 3 and Picard curves, as presented in [Wen01b] and [KW05], require a more profound understanding of the invariants and the class polynomials of the isomorphism classes of the corresponding principally polarized abelian varieties over $\mathbb{C}$. We computed several such isomorphism classes for Jacobians of hyperelliptic genus 3 curves represented by polarized ideal classes and identified their Shioda invariants. Building on these findings, one might potentially be able to construct hyperelliptic genus 3 curves over finite fields with cryptographically useful properties.

Appendix A

Suitable orders I

In the following tables, we let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/\langle f \rangle$ with irreducible $f \in \mathbb{Z}[x]$ and $\alpha \in \mathcal{O}_K$ be a sextic CM class number one field containing $\mathbb{Q}(i)$. Let $K_0 = \mathbb{Q}[x]/\langle g \rangle$ with $g \in \mathbb{Z}[x]$ be the maximal totally real cubic subfield of K such that $K = K_0\mathbb{Q}(i)$. Moreover, we let $\lambda_1, \ldots, \lambda_5 \in K$ be integral such that $\mathcal{O}_K = \langle 1, \lambda_1, \ldots, \lambda_5 \rangle_{\mathbb{Z}}$. For each such CM field, we compute every non-maximal order $S \subsetneq \mathcal{O}_K$ containing $\mathbb{Z}[i]$, which has a CM class number one, is stable under complex conjugation, and fulfills

$$[\,\mathcal{O}_K \,:\, S\,] \,\Big|\, B^4 \,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0}),$$

where B is the parameter depending only on K given by Theorem 7.21. This delivers the computational results for Chapter 8.2 (the case $\mathbb{Z}[i] \subseteq S$). We give the order S via the transformation matrix $T \in \mathbb{Z}^{6\times 6}$ of $\mathcal{O}_K$ into S with respect to $(1, \lambda_1, \ldots, \lambda_5)$. Additionally, we provide the parameter δ_S and indicate whether $S_0 := S \cap K_0$ is Gorenstein or if $S = S_{\mathbb{Q}(i)}S_0$, where $S_{\mathbb{Q}(i)} := S \cap \mathbb{Q}(i)$.

Table A.1: Orders in sextic CM field $K \supseteq \mathbb{Q}(i)$ No. 1

$f = x^6 + 4\,x^5 - 3\,x^4 - 10\,x^3 + 40\,x^2 - 32\,x + 37$					
$g = x^3 + 2\,x^2 - 5\,x + 1$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = \alpha^3$, $\lambda_4 = \alpha^4$ $\lambda_5 = 1/2477\,(\alpha^5 + 44\,\alpha^4 + 1757\,\alpha^3 + 914\,\alpha^2 + 1922\,\alpha + 61)$					
No.	T	$[\,\mathcal{O}_K \,:\, S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(i)}\,S_0$
1.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	16	1	X	$\surd$

No.	T	$[\mathcal{O}_K : S]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(i)} S_0$
1.2	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$	8	1	X	X
1.3	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$	8	1	X	X
1.4	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	8	1	X	X
1.5	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$	4	2	X	X

Table A.2: Orders in sextic CM field $K \supseteq \mathbb{Q}(i)$ No. 2

$f = x^6 - 3\,x^4 - 2\,x^3 + 12\,x^2 + 12\,x + 17$					
$g = x^3 - 3\,x - 1$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = \alpha^3$, $\lambda_4 = \alpha^4$ $\lambda_5 = 1/757\,(\alpha^5 + 162\,\alpha^4 + 503\,\alpha^3 + 485\,\alpha^2 + 611\,\alpha + 584)$					
No.	T	$[\,\mathcal{O}_K\ :\ S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(i)}\,S_0$
2.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	16	1	X	$\surd$
2.2	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	8	1	X	X
2.3	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$	8	1	X	X
2.4	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	8	1	X	X
2.5	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	4	2	X	X

Table A.3: Orders in sextic CM field $K \supseteq \mathbb{Q}(i)$ No. 3

$f = x^6 + 2\,x^5 - 2\,x^3 + 7\,x^2 + 8\,x + 13$					
$g = x^3 + x^2 - 2\,x - 1$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = \alpha^3$, $\lambda_4 = \alpha^4$ $\lambda_5 = 1/533\,(\alpha^5 + 212\,\alpha^4 + 281\,\alpha^3 + 378\,\alpha^2 + 503\,\alpha + 104)$					
No.	T	$[\,\mathcal{O}_K\ :\ S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(i)}\,S_0$
3.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	16	1	X	$\surd$
3.2	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$	8	1	X	X
3.3	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	8	1	X	X
3.4	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$	8	1	X	X
3.5	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$	4	2	X	X

Table A.4: Orders in sextic CM field $K \supseteq \mathbb{Q}(i)$ No. 4

$f = x^6 + 2\,x^5 - 24\,x^4 - 8\,x^3 + 217\,x^2 - 298\,x + 274$					
$g = x^3 + x^2 - 14\,x + 8$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = \alpha^3$, $\lambda_4 = 1/4\,(\alpha^4 + 2\,\alpha^3 + 3\,\alpha^2 + 2\,\alpha + 2)$ $\lambda_5 = 1/16232\,(\alpha^5 + 1257\,\alpha^4 + 15181\,\alpha^3 + 3895\,\alpha^2 + 6668\,\alpha + 446)$					
No.	T	$[\,\mathcal{O}_K \,:\, S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(i)}\,S_0$
4.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	4	2	X	X
4.2	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$	2	1	$\surd$	X
4.3	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	2	1	$\surd$	X
4.4	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	2	1	$\surd$	X

Table A.5: Orders in sextic CM field $K \supseteq \mathbb{Q}(i)$ No. 5

$f = x^6 + 2\,x^5 - 16\,x^4 - 32\,x^3 + 89\,x^2 + 190\,x + 202$					
$g = x^3 + x^2 - 10\,x - 8$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = \alpha^3$, $\lambda_4 = 1/4\,(\alpha^4 + 2\,\alpha^3 + 3\,\alpha^2 + 2\,\alpha + 2)$ $\lambda_5 = 1/8744\,(\alpha^5 + 1933\,\alpha^4 + 5477\,\alpha^3 + 187\,\alpha^2 + 4868\,\alpha + 4870)$					
No.	T	$[\,\mathcal{O}_K : S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(i)}\,S_0$
5.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	4	2	X	X
5.2	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$	2	1	√	X
5.3	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	2	1	√	X
5.4	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	2	1	√	X

Table A.6: Orders in sextic CM field $K \supseteq \mathbb{Q}(i)$ No. 6

$f = x^6 + 6\,x^5 - 24\,x^4 - 80\,x^3 + 393\,x^2 - 438\,x + 386$					
$g = x^3 + 3\,x^2 - 18\,x + 8$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = \alpha^3$, $\lambda_4 = 1/4\,(\alpha^4 + 2\,\alpha^3 + 3\,\alpha^2 + 2\,\alpha + 2)$ $\lambda_5 = 1/33832\,(\alpha^5 + 345\,\alpha^4 + 6977\,\alpha^3 + 13799\,\alpha^2 + 17896\,\alpha + 27294)$					
No.	T	$[\,\mathcal{O}_K\ :\ S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(i)}\,S_0$
6.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	4	2	X	X
6.2	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$	2	1	$\surd$	X
6.3	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$	2	1	$\surd$	X
6.4	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 2 \end{pmatrix}$	2	1	$\surd$	X

Appendix B

Suitable orders II

In the following tables, we let $K = \mathbb{Q}(\alpha) = \mathbb{Q}[x]/\langle f \rangle$ with $f \in \mathbb{Z}[x]$, $\alpha \in \mathcal{O}_K$, and let $|\mu_K| = 6$ be a sextic CM class number one field containing $\mathbb{Q}(\zeta_3)$. Moreover, let $K_0 = \mathbb{Q}[x]/\langle g \rangle$ with $g \in \mathbb{Z}[x]$ be the maximal totally real cubic subfield of K such that $K = K_0\mathbb{Q}(\zeta_3)$. We let $\lambda_1, \dots, \lambda_5 \in K$ be integral with $\mathcal{O}_K = \langle 1, \lambda_1, \dots, \lambda_5 \rangle_{\mathbb{Z}}$. For each such CM field, we compute every non-maximal order $S \subsetneq \mathcal{O}_K$ containing $\mathbb{Z}[\zeta_3]$, which has a CM class number one, is stable under complex conjugation, and fulfills

$$[\,\mathcal{O}_K \,:\, S\,] \,\Big|\, B^4 \,\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_{K/K_0}),$$

where B is the parameter depending only on K given by Theorem 7.21. This provides the computational results for Chapter 8.2 (the case $\mathbb{Z}[\zeta_3] \subseteq S$). Again, we present the order S via the transformation matrix $T \in \mathbb{Z}^{6\times 6}$ with respect to the basis of $\mathcal{O}_K$. Additionally, we provide the parameter δ_S, and we indicate whether $S_0 := S \cap K_0$ is Gorenstein or if $S = S_{\mathbb{Q}(\zeta_3)}S_0$, where $S_{\mathbb{Q}(\zeta_3)} := S \cap \mathbb{Q}(\zeta_3)$. In the last table, which is Table B.5, we list the sextic CM fields $K \supseteq \mathbb{Q}(\zeta_3)$ that do not produce a non-maximal order satisfying the above-mentioned conditions.

Table B.1: Orders in sextic CM field $K \supseteq \mathbb{Q}(\zeta_3)$ No. 7

$f = x^6 + 2\,x^5 + 2\,x^4 + 6\,x^3 + 51\,x^2 - 32\,x + 151$					
$g = x^3 + x^2 - 4\,x + 1$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = 1/2\,(\alpha^3 + \alpha + 1)$, $\lambda_4 = 1/2\,(\alpha^4 + \alpha^2 + \alpha)$ $\lambda_5 = 1/15338\,(\alpha^5 + 5558\,\alpha^4 + 4856\,\alpha^3 + 8069\,\alpha^2 + 13779\,\alpha + 11803)$					
No.	T	$[\,\mathcal{O}_K : S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(\zeta_3)}\,S_0$
7.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$	9	3	X	X

Table B.2: Orders in sextic CM field $K \supseteq \mathbb{Q}(\zeta_3)$ No. 8

$f = x^6 + 2\,x^5 + 6\,x^4 + 6\,x^3 + 35\,x^2 + 28\,x + 91$					
$g = x^3 + x^2 - 2\,x - 1$					
$\lambda_1 = \alpha$, $\lambda_2 = \alpha^2$, $\lambda_3 = 1/2\,(\alpha^3 + \alpha + 1)$, $\lambda_4 = 1/2\,(\alpha^4 + \alpha^2 + \alpha)$ $\lambda_5 = 1/8762\,(\alpha^5 + 562\,\alpha^4 + 3675\,\alpha^3 + 3317\,\alpha^2 + 4392\,\alpha + 6188)$					
No.	T	$[\,\mathcal{O}_K : S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(\zeta_3)}\,S_0$
8.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$	9	3	X	X

Table B.3: Orders in sextic CM field $K \supseteq \mathbb{Q}(\zeta_3)$ No. 9

$f = x^6 + 2\,x^5 - 10\,x^4 - 24\,x^3 + 117\,x^2 + 262\,x + 628$					
$g = x^3 + x^2 - 10\,x - 8$					
$\lambda_1 = \alpha$, $\lambda_2 = 1/2\,(\alpha^2 + \alpha)$, $\lambda_3 = 1/2\,(\alpha^3 + \alpha)$, $\lambda_4 = 1/8\,(\alpha^4 + 2\,\alpha^3 + 3\,\alpha^2 + 2\,\alpha + 4)$ $\lambda_5 = 1/26032\,(\alpha^5 + 827\,\alpha^4 + 11941\,\alpha^3 + 11205\,\alpha^2 + 22406\,\alpha + 2492)$					
No.	T	$[\,\mathcal{O}_K\ :\ S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(\zeta_3)}\,S_0$
9.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \end{pmatrix}$	9	3	X	X

Table B.4: Orders in sextic CM field $K \supseteq \mathbb{Q}(\zeta_3)$ No. 10

$f = x^6 + 2\,x^5 - 18\,x^4 + 245\,x^2 - 434\,x + 892$					
$g = x^3 + x^2 - 14\,x + 8$					
$\lambda_1 = \alpha$, $\lambda_2 = 1/2\,(\alpha^2 + \alpha)$, $\lambda_3 = 1/2\,(\alpha^3 + \alpha)$, $\lambda_4 = 1/8\,(\alpha^4 + 2\,\alpha^3 + 3\,\alpha^2 + 2\,\alpha + 4)$ $\lambda_5 = 1/43696\,(\alpha^5 + 4773\,\alpha^4 + 17273\,\alpha^3 + 20675\,\alpha^2 + 7874\,\alpha + 9708)$					
No.	T	$[\,\mathcal{O}_K\ :\ S\,]$	δ_S	S_0 Gorenstein	$S = S_{\mathbb{Q}(\zeta_3)}\,S_0$
10.1	$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 2 & 0 & 1 & 0 \\ 0 & 0 & 2 & 0 & 0 & 1 \end{pmatrix}$	9	3	X	X

Table B.5: CM fields $K \supseteq \mathbb{Q}(\zeta_3)$ without suitable non-maximal orders

No.	f, g
11	$f = x^6 + 6\,x^5 - 18\,x^4 - 56\,x^3 + 453\,x^2 - 702\,x + 1324$ $g = x^3 + 3\,x^2 - 18\,x + 8$
12	$f = x^6 + 12\,x^5 + 27\,x^4 - 34\,x^3 + 336\,x^2 - 252\,x + 721$ $g = x^3 + 6\,x^2 - 9\,x + 1$
13	$f = x^6 + 6\,x^5 - 54\,x^4 - 308\,x^3 + 993\,x^2 + 5166\,x + 9892$ $g = x^3 + 3\,x^2 - 36\,x - 64$
14	$f = x^6 + 8\,x^5 - 5\,x^4 - 126\,x^3 + 132\,x^2 + 1008\,x + 2493$ $g = x^3 + 4\,x^2 - 15\,x - 27$
15	$f = x^6 + 4\,x^5 - 29\,x^4 - 114\,x^3 + 384\,x^2 + 1404\,x + 2817$ $g = x^3 + 2\,x^2 - 21\,x - 27,$

Appendix C

Examples of diagonal Gorenstein orders

We apply Theorem 2.4 to each totally real cubic number field listed in Table 2.1 to describe all diagonal Gorenstein orders within these fields.

Example C.1.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 - 3\,x - 1\rangle$ or $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 - x^2 - 2\,x - 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$. Then $\omega_1 = \beta$ and $\omega_2 = \beta^2$. In the meaning of Corollary 2.2 and due to Table 2.1, the parameters $\lambda_{21}, \lambda_{12}$ are both equal to 1. Consequently, $D_1 = \{1\} = D_2$ and we only have to consider the case $r = 1 = s$. Now the conditions (i)-(iii) in Theorem 2.4 (a) are trivial, and we receive the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$. Then the lattice $S = \langle 1, x^2\,y\,\omega_1, x\,y^2\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then there exist $x, y \geq 1$ with $\gcd(x, y) = 1$ such that $a = x^2\,y$ and $c = x\,y^2$.

Example C.2.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 2\,x^2 - 5\,x + 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$. Then $\omega_1 = \beta$ and $\omega_2 = \beta^2$. Due to Table 2.1, the parameters are $\lambda_{21} = 11$ and $\lambda_{12} = 1$ such that we receive $D_1 = \{1, 11\}$ and $D_2 = \{1\}$. Now Theorem 2.4 delivers the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $11 \nmid x$ or
(ii) if $r = 11$, $s = 1$ and $11 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Example C.3.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + x^2 - 4\,x + 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$. Then $\omega_1 = \beta$ and $\omega_2 = \beta^2$. In this case, we receive the same situation as in Example C.2 just by replacing 11 by 5. To be more precise because of Table 2.1, the parameters are $\lambda_{21} = 5$ and $\lambda_{12} = 1$ such that we receive $D_1 = \{1, 5\}$ and $D_2 = \{1\}$. Now Theorem 2.4 delivers the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $5 \nmid x$ or
(ii) if $r = 5$, $s = 1$ and $5 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Example C.4.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 6\,x^2 - 9\,x + 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$. Again, the ring of integers is monogenic, which means that $\omega_1 = \beta$ and $\omega_2 = \beta^2$. Now, due to Table 2.1, the parameters are $\lambda_{21} = 55$ and $\lambda_{12} = 1$ such that we receive $D_1 = \{1, 5, 11, 55\}$ and $D_2 = \{1\}$. Then Theorem 2.4 delivers the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $5, 11 \nmid x$ or
(ii) if $r = 5$, $s = 1$ and $11 \nmid x$ such as $5 \nmid y$ or
(iii) if $r = 11$, $s = 1$ and $5 \nmid x$ such as $11 \nmid y$ or
(iv) if $r = 55$, $s = 1$ and $5, 1 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Example C.5.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + x^2 - 14\,x + 8\rangle$ or $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + x^2 - 10\,x - 8\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$. For both fields, we consider $\omega_1 = \beta$ and $\omega_2 = (1/2)\,(\beta + \beta^2)$. Now, due to Table 2.1, $\lambda_{21} = 2 = \lambda_{12}$ such that $D_1 = \{1, 2\} = D_2$ and Theorem 2.4 tells us the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $2 \nmid x$ such as $2 \nmid y$ or
(ii) if $r = 1$, $s = 2$ and $2 \nmid x$ or
(iii) if $r = 2$, $s = 1$ and $2 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein,

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Example C.6.
Let $L = \mathbb{Q}[x]/\langle x^3 + 3\,x^2 - 18\,x + 8\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$. We consider $\omega_1 = \beta$ and $\omega_2 = (1/2)\,(\beta + \beta^2)$. Again, in the meaning of Corollary 2.2 and due to Table 2.1, $\lambda_{21} = 12$ and $\lambda_{12} = 2$ such that we get $D_1 = \{1, 2, 3, 4, 6, 12\}$ and $D_2 = \{1, 2\}$. Now Theorem 2.4 delivers the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and$2, 3 \nmid x$ such as $2 \nmid y$ or
(ii) if $r = 1$, $s = 2$ and $2, 3 \nmid x$ or
(iii) if $r = 2$, $s = 1$ and $2, 3 \nmid x$ such as $2 \nmid y$ or
(iv) if $r = 3$, $s = 1$ and $2 \nmid x$ such as $2, 3 \nmid y$ or
(v) if $r = 3$, $s = 2$ and $2 \nmid x$ such as $3 \nmid y$ or
(vi) if $r = 4$, $s = 1$ and $2, 3 \nmid x$ such as $2 \nmid y$ or
(vii) if $r = 6$, $s = 1$ and $2, 3 \nmid x$ such as $2 \nmid y$ or
(viii) if $r = 12$, $s = 1$ and $2, 3 \nmid x$ such as $2 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Example C.7.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 4\,x^2 - 15\,x + -27\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = (1/3)\,(\beta + \beta^2)$. Now, due to Table 2.1, $\lambda_{21} = 3 = \lambda_{12}$ and we receive the analogue situation as in Example C.5 by replacing the prime 2 by 3. To be more precise, we have $D_1 = \{1, 3\} = D_2$ and Theorem 2.4 tells us the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $3 \nmid x$ such as $3 \nmid y$ or
(ii) if $r = 1$, $s = 3$ and $3 \nmid x$ or
(iii) if $r = 3$, $s = 1$ and $3 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein,

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Example C.8.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 2\,x^2 - 21\,x - 8 - 27\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$ and $\omega_1 = \beta$ such as $\omega_2 = (1/3)\,(2\,\beta + \beta^2)$. Now, due to Table 2.1, $\lambda_{21} = 3 = \lambda_{12}$ and we receive the analogue situation as in Example C.7. To be more precise, we have $D_1 = \{1, 3\} = D_2$ and Theorem 2.4 tells us the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $3 \nmid x$ such as $3 \nmid y$ or
(ii) if $r = 1$, $s = 3$ and $3 \nmid x$ or
(iii) if $r = 3$, $s = 1$ and $3 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2 \rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein,

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Example C.9.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 3\,x^2 - 36\,x - 64 \rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2 \rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = (1/4)\,(\beta + \beta^2)$. Now, due to Table 2.1, $\lambda_{21} = 4 = \lambda_{12}$ such that $D_1 = \{1, 2, 4\} = D_2$ and Theorem 2.4 tells us the following.

(a) Let $x, y \geq 1$ with $\gcd(x, y) = 1$.

(i) If $r = 1$, $s = 1$ and $2 \nmid x$ such as $2 \nmid y$ or
(ii) if $r = 1$, $s = 2$ and $2 \nmid x$ such as $2 \nmid y$ or
(iii) if $r = 1$, $s = 4$ and $2 \nmid x$ or
(iv) if $r = 2$, $s = 1$ and $2 \nmid x$ such as $2 \nmid y$ or
(v) if $r = 4$, $s = 1$ and $2 \nmid y$, then

$S = \langle 1, r\,x^2\,y\,\omega_1, s\,x\,y^2\,\omega_2 \rangle_{\mathbb{Z}}$ is an order of L which is Gorenstein,

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2 \rangle_{\mathbb{Z}}$ is a Gorenstein order in L, then exist $x, y, r, s \in \mathbb{Z}$ as in (a) with $a = r\,x^2\,y$ and $c = s\,x\,y^2$.

Appendix D

Examples of diagonal non-Gorenstein orders

For each of the totally real cubic number fields listed in Table 2.1, we describe all non-Gorenstein orders by applying Theorem 2.7.

Example D.1.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 - 3\,x - 1\rangle$ or $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 - x^2 - 2\,x - 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, $\omega_1 = \beta$ and $\omega_2 = \beta^2$. Then, in the meaning of Corollary 2.2 and due to Table 2.1, the parameters $\lambda_{21}, \lambda_{12}$ are both equal to 1 and $D_1 = \{1\} = D_2$. We only have to consider the case $r = 1 = s$. Then Theorem 2.7 gives the following.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ such as $e\,d \neq x$. Then $S = \langle 1, e\,x\,\omega_1, d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then there exist x, e, d as in (a) such that $a = e\,x$ and $c = d\,x$.

Example D.2.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 2\,x^2 - 5\,x + 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = \beta^2$. Then, due to Table 2.1, the parameters $\lambda_{21} = 11$ and $\lambda_{12} = 1$ such that $D_1 = \{1, 11\}$ and $D_2 = \{1\}$. Applying Theorem 2.7 gives the following.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for $r \in D_1 = \{1, 11\}$, the lattice $S = \langle 1, r\,e\,x\,\omega_1, d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then exist x, e, d, r as in (a) such that $a = r\,e\,x$ and $c = d\,x$.

Example D.3.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + x^2 - 4\,x + 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = \beta^2$. Then, due to Table 2.1, the parameters $\lambda_{21} = 5$ and $\lambda_{12} = 1$ such that

$D_1 = \{1, 5\}$ and $D_2 = \{1\}$. Applying Theorem 2.7, we receive the analogue result as in Example D.2 by replacing the prime 11 by 5. To be more precise, we get the following.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for $r \in D_1 = \{1, 5\}$, the lattice $S = \langle 1, r\,e\,x\,\omega_1, d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then exist x, e, d, r as in (a) such that $a = r\,e\,x$ and $c = d\,x$.

Example D.4.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 6\,x^2 - 9\,x + 1\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$ and $\omega_1 = \beta$ such as $\omega_2 = \beta^2$. Due to Table 2.1 the parameters $\lambda_{21} = 55$ and $\lambda_{12} = 1$ such that $D_1 = \{1, 5, 11, 55\}$ and $D_2 = \{1\}$. Theorem 2.7 gives the following.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for $r \in D_1 = \{1, 5, 11, 55\}$, the lattice $S = \langle 1, r\,e\,x\,\omega_1, d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then exist x, e, d, r as in (a) such that $a = r\,e\,x$ and $c = d\,x$.

Example D.5.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + x^2 - 14\,x + 8\rangle$ or $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + x^2 - 10\,x - 8\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = (1/2)\,(\beta + \beta^2)$. Then, for both fields, Table 2.1 tells us that the parameters are $\lambda_{21} = 2 = \lambda_{12}$ and $D_1 = \{1, 2\} = D_2$. Now Theorem 2.7 delivers:

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for each $r \in D_1 = \{1, 2\}$ and $s \in D_2 = \{1, 2\}$, the lattice defined by $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then there exist x, e, d, r, s as in (a) such that $a = r\,e\,x$ and $c = s\,d\,x$.

Example D.6.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 3\,x^2 - 18\,x + 8\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$ and $\omega_1 = \beta$ such as $\omega_2 = (1/2)\,(\beta + \beta^2)$. Here the parameters are $\lambda_{21} = 12$ and $\lambda_{12} = 2$ such that $D_1 = \{1, 2, 3, 4, 6, 12\}$ and $D_2 = \{1, 2\}$. We obtain the following from Theorem 2.7.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for $r \in D_1 = \{1, 2, 3, 4, 6, 12\}$ and $s \in D_2 = \{1, 2\}$, the lattice given by $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.

(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then there exist x, e, d, r, s as in (a) such that $a = r\,e\,x$ and $c = s\,d\,x$.

Example D.7.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 4\,x^2 - 15\,x - 27\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = (1/3)\,(\beta + \beta^2)$. Table 2.1 tells us that the parameters are $\lambda_{21} = 3 = \lambda_{12}$ and $D_1 = \{1, 3\} = D_2$. We receive the analogue result as Example D.5 by replacing the prime 2 with 3. To be more precise, Theorem 2.7 delivers:

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for every $r \in D_1 = \{1, 3\}$ and $s \in D_2 = \{1, 3\}$, the lattice defined by $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.
(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then there exist x, e, d, r, s as in (a) such that $a = r\,e\,x$ and $c = s\,d\,x$.

Example D.8.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 2\,x^2 - 21\,x - 27\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = (1/3)\,(2\,\beta + \beta^2)$. As in Example D.7, Table 2.1 tells us that the parameters are $\lambda_{21} = 3 = \lambda_{12}$ and $D_1 = \{1, 3\} = D_2$. Again, Theorem 2.7 gives us the following.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for every $r \in D_1 = \{1, 3\}$ and $s \in D_2 = \{1, 3\}$, the lattice given by $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.
(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then there exist x, e, d, r, s as in (a) such that $a = r\,e\,x$ and $c = s\,d\,x$.

Example D.9.
Let $L = \mathbb{Q}(\beta) = \mathbb{Q}[x]/\langle x^3 + 3\,x^2 - 36\,x - 64\rangle$ with $\mathcal{O}_L = \langle 1, \omega_1, \omega_2\rangle_{\mathbb{Z}}$, where $\omega_1 = \beta$ and $\omega_2 = (1/4)\,(\beta + \beta^2)$. For this field, Table 2.1 tells us that the parameters are $\lambda_{21} = 4 = \lambda_{12}$ and $D_1 = \{1, 2, 4\} = D_2$ such that Theorem 2.7 gives us the following.

(a) Let $x > 0$ and e, d be positive divisors of x with $\gcd(e, d) = 1$ and $e\,d \neq x$. Then, for each $r \in D_1 = \{1, 2, 4\}$ and $s \in D_2 = \{1, 2, 4\}$, the lattice defined by $S = \langle 1, r\,e\,x\,\omega_1, s\,d\,x\,\omega_2\rangle_{\mathbb{Z}}$ is an order of L which is not Gorenstein.
(b) If $S = \langle 1, a\,\omega_1, c\,\omega_2\rangle_{\mathbb{Z}}$ is an order in L which is not Gorenstein, then there exist x, e, d, r, s as in (a) such that $a = r\,e\,x$ and $c = s\,d\,x$.

Appendix E

Models over the totally real cubic subfield

In the following examples, we let S be a non-maximal order from Appendix A in a sextic CM class number one field $K = \mathbb{Q}(\alpha)$. Let $K_0 = \mathbb{Q}(\beta)$ represent the totally real cubic subfield of K. The specific label of the order is provided in the header of each table. The curve $C : y^2 = f(x)$ offers an affine model of a simple hyperelliptic curve over K_0 with complex multiplication by S. Here, $f = \sum_{i=0}^{8} \lambda_i x^i \in \mathcal{O}_{K_0}[x]$ is detailed through its coefficients in a separate table. The second, third, and fourth columns present integral factors preceding β^2, β, and 1 for the coefficient λ_i, respectively. The table's last row provides the prime factorization of the norm of the discriminant of C. These models arise either from the reduction algorithm `reduce_gcd` or `reduce_discriminant` from [BS22], depending on which yielded smaller coefficients. The examples are organized based on the precision required to compute the Shioda invariants from the principally polarized ideal classes.

Table E.1: $C : y^2 = f(x)$ with CM by S No. 2.2.

coef	β^2	β	1
λ_0	- 2141386921139657387	743695861669812350	6165877918652417752
λ_1	-56104506150196692672	194848905044385650 16	1615464869932941217 20
λ_2	-1220679793833301925892	423937643430137923360	3514807383044508755346
λ_3	3348264465217338788832	- 1162840045463985671640	- 9640943286025920660384
λ_4	0	0	0
λ_5	-432548353451078323207944	150222466659222059619024	1245473345193224755793640
λ_6	203719018198287399992412 80	- 707508725324576548961010 2	- 5865855344276491014426730 6
λ_7	120960193286444609135150424	- 420090342688615381868244 24	348290995366662959702881008
λ_8	596423552747322594204325260	- 207135726104417756423107855	- 171733317550647066837370016 4
$N_{K_0/\mathbb{Q}}(\Delta_C)$	$2^{144} \cdot 3^{24} \cdot 3259^{21} \cdot 39039452414654723^{21}$		

Table E.2: $C : y^2 = f(x)$ with CM by S No. 3.3.

coef	β^2	β	1
λ_0	4445322355523152166120475907181390667549078481065213952	22473299873103740974556626005131667900018711119758622 72	- 1038432231139252454777627850476702266364252157870551859 2
λ_1	6623826879190028025076392709407012755496807935508480000	3644311463814629866173501586452285111913841518706688000	- 1494060842761160599115124881856485563425829267125043200 0
λ_2	6971955607672935303567707014924166760555268276224000000	3871200076665719502294648078324715300175839494144000000	- 1566213615514370094385095424100779986619836923904000000 0
λ_3	3133381994219412157219712799868990069533573120000000000	1739293125163943872922662755270309893130682368000000000	- 7039929510027337078861105517132579120187703296000000000
λ_4	0	0	0
λ_5	-303057332109867685642548919269971930496000000000000000000	- 1681856130441790366797466147147917932160000000000000000	6809609733536766045004065633486644910720000000000000000 0
λ_6	-652175519033331529107365522528966910937500000000000000	- 3619303940338743154513637050793339062500000000000000000	1465424573619201290275946973379364607187500000000000000 0
λ_7	-601120117002567326724959075367445678710937500000000000	- 3335963331048417768060775873678256103515625000000000	1350704938244346468868788028912027587890625000000000000
λ_8	-400474081161705071975725099229747235774993896484375	- 2222463052967349698364387336151501536369323730468 75	899857168575726248388071742449191510677337646484375
$N_{K_0/\mathbb{Q}}(\Delta_C)$	$2^{1152} \cdot 3^{504} \cdot 5^{504} \cdot 7^{168} \cdot 71^{56} \cdot 1637^{56} \cdot 1877^{56} \cdot 5039^{21} \cdot 5039^{21} \cdot 46271^{56} \cdot 14928913^{21}$		

Table E.3: $C : y^2 = f(x)$ with CM by S No. 2.2.

coef	β^2	β	1
λ_0	-46040442404066230	70538050012800345	30050764519660941
λ_1	335420959773819096	-513894724689939264	218930482922281920
λ_2	-2029281622597068612	3109039821222086764	1324519510759229134
λ_3	-1547777161337262792	2371332186519051312	1010239795724136648
λ_4	0	0	0
λ_5	15460358800783069392	-23686643947630313304	-10091032439954245800
λ_6	202471822877987718148	-310204830556553436246	-132154094951407685088
λ_7	-334290172574368588320	512162254684884462768	218192420583577744776
λ_8	4583360596266610062 09	-702211589961889878445	-299157603734370545077
$\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_C)$	$2^{144} \cdot 3^{24} \cdot 3259^{21} \cdot 3903945241465472 3^{21}$		

Table E.4: $C : y^2 = f(x)$ with CM by S No. 2.4.

coef	β^2	β	1
λ_0	-156949675735621	- 295965540798703	- 85038113962973
λ_1	-22315943108171736	- 41940267386888880	- 11874085625676888
λ_2	-2627453025605723902	- 4937996429617985962	- 1398038539285199630
λ_3	39000353556704688456	73296688890681707328	20751654687069616392
λ_4	0	0	0
λ_5	-147541646742082294016328	- 27728759340427198 4168400	- 78505270488708526988040
λ_6	37603400838190397043368614	70671276568204316488307818	20008351670752152115860710
λ_7	12082411096157309856666 79896	22707505096721605222842 95424	64289166632234649478474 1784
λ_8	32238995967239747777499927037	60589493223923699962636838863	17154011457638554684011003029
$\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_C)$	$2^{144} \cdot 3^{24} \cdot 3259^{21} \cdot 3903945241465472 3^{21}$		

Table E.5: $C : y^2 = f(x)$ with CM by S No. 3.2.

λ_0	β^2	13457628033573916897416725763111483453573851543995214204221343343327684568832540672
	β	- 10793373942788082443070683021068765314466714766592705990360356282730367238214254592
	1	- 7466817876682852644382966451727558973127426600564584500526511406459242905232998400
λ_1	β^2	-7193191314773829061628791698572572457316186298587973631189819622122988094095360000
	β	57727753131153864851088962550803847357133259654450473643646840992230965824716800
	1	39925383586496086547392578296202566168275989497897393547832961414870758273843200
λ_2	β^2	-32945201929182973678781309231800530921712694657617636642045050581060545413120000000
	β	26439711344496880831914250674013440904710501772288300475848483201364766228480000000
	1	18291712189416916860986165555948897749363206106965614761196482948541951508480000000
λ_3	β^2	21160072217281447326722315684956595371867307934488570715033726051837542400000000000
	β	- 16800675075361364297909790186005785195342852130750776148489060117328691200000000000
	1	- 11667899615611640817645553682415928069312252852217482576911194467703193600000000000
λ_4	β^2	0
	β	0
	1	0
λ_5	β^2	16400859733562122655932491821259486216475660730501436557063064384000000000000000000
	β	- 13427923748266400654532098594674314096816724025315438190300572736000000000000000000
	1	- 92243692763519453256500844273762143449251620253094335330659395200000000000000000000
λ_6	β^2	20102376183031995309536465009451142193244261085686641057747511468750000000000000000
	β	-16173133950998795913450204539780547628883140763287610945560074937500000000000000000
	1	- 11179241733699609564420135094348389445140705623157410808183877781250000000000000000
λ_7	β^2	-34377392964067433644181755655069042525973688418572242920656201171875000000000000
	β	27414531069418605720622345351843093800838846301556919831960327148437500000000000
	1	19009469112101511581972128693899514327594052276241461063834472656250000000000000
λ_8	β^2	-50175334785349726393013950238582313408784360179225539099414062500000000000000000
	β	40232716149000687907207609805039795688009697933791122264765024185180664062500 0
	1	27843082180354357946932706139801725412934975466328432552392417192459106445312 5
$N_{K_0/\mathbb{Q}}(\Delta_C)$		$2^{1152} \cdot 3^{504} \cdot 5^{504} \cdot 7^{201} \cdot 13^{56} \cdot 54^{56} \cdot 71^{56} \cdot 83^{56} \cdot 239^{112} \cdot 4088267^{21} \cdot 34990577^{56} \cdot 31164159504059723^{21}$

Table E.6: $C : y^2 = f(x)$ with CM by S No. 3.2.

λ_0	β^2	-22473299873103740974556626005131667900018711119758622 72
	β	219799236821277806866481330666822387754720736908935168 0
	1	753652386964153881920335910108925461457506495400771584
λ_1	β^2	-364431146381462986617350158645228511191384151870668800 0
	β	297951541537539815890289112295472764358296641680179200 0
	1	195135679458307992517503818670145498864916471847321600 0
λ_2	β^2	-387120007666571950229464807832471530017583949414400000 0
	β	310075553100721580127305893659945146037942878208000000 0
	1	215297513686788916557910786716524895508800680755200000 0
λ_3	β^2	-173929312516394387292266275527030989313068236800000000 0
	β	139408886905546828429705004459868017640289075200000000 0
	1	966127603575431108500982837875710912010125312000000000
λ_4	β^2	0
	β	0
	1	0
λ_5	β^2	16818561304417903667974661471479179321600000000000000 0
	β	- 13487171906568864896280230455518013728000000000000000 0
	1	- 93339303910237803464437889906071163136000000000000000 0
λ_6	β^2	36193039403387431545136370507933390625000000000000000 0
	β	- 29024512499945721365600181744963300468750000000000000 0
	1	- 20085685848133608339014777675790312093750000000000000 0
λ_7	β^2	33359633310484177680607758736782561035156250000000 0
	β	- 26752378389772554991888148799962006835937500000000 0
	1	- 18513162886562996138720770919068937988281250000000 0
λ_8	β^2	22224630529673496983643873361515015363693237304687 5
	β	- 17822777586497010213928636561459708213806152343750 0
	1	- 12333729904441886539981718962545311450958251953125 0
$N_{K_0/\mathbb{Q}}(\Delta_C)$		$2^{1152} \cdot 3^{504} \cdot 5^{504} \cdot 7^{168} \cdot 71^{56} \cdot 1637^{56} \cdot 1877^{56} \cdot 5039^{21} \cdot 5039^{21} \cdot 46271^{56} \cdot 14928913^{21}$

Table E.7: $C : y^2 = f(x)$ with CM by S No. 3.4.

λ_0	β^2	- 219799236821277806866481330666822387754720736908935168 0
	β	- 44453223555231521661204759071813906675490784810652139 52
	1	- 15430152194438162443261759842491842409990283594616012 80
λ_1	β^2	-29795154153753981589028911229547276435829664168017920 00
	β	- 66238268791900280250763927094070127554968079355084800 00
	1	- 23577507176707816482690738632483875915955519021383680 00
λ_2	β^2	-31007555310072158012730589365994514603794287820800000 00
	β	- 69719556076729353035677070149241667605552682762240000 00
	1	- 24886694854563340377371293528847301848842433986560000 00
λ_3	β^2	-13940888690554682842970500445986801764028907520000000 00
	β	- 31333819942194121572197127998689900695335731200000000 00
	1	- 11183697776969883530472926280662286978483486720000000 00
λ_4	β^2	0
	β	0
	1	0
λ_5	β^2	13487171906568864896280230455518013728000000000000000 00
	β	30305733210986768564254891926997193049600000000000000 00
	1	10816020311243162093225303496833228601600000000000000 00
λ_6	β^2	29024512499945721365600181744963300468750000000000000
	β	65217551903333152910736552252896691093750000000000000
	1	23275880458695533385657781595113168687500000000000000
λ_7	β^2	26752378389772554991888148799962006835937500000000000
	β	60112011700256732672495907536744567871093750000000000
	1	21453725344632804230606597754534177246093750000000000
λ_8	β^2	17822777586497010213928636561459708213806152343750 0
	β	40047408116170507197572509922974723577499389648437 5
	1	14292753568408097213773911990250110626220703125000 0
$\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_C)$		$2^{1152} \cdot 3^{504} \cdot 5^{504} \cdot 7^{168} \cdot 71^{56} \cdot 1637^{56} \cdot 1877^{56} \cdot 5039^{21} \cdot 5039^{21} \cdot 46271^{56} \cdot 14928913^{21}$

Table E.8: $C : y^2 = f(x)$ with CM by S No. 2.4.

coef	β^2	β	1
λ_0	17945150971905905684974331024469809719	- 27493566365919293945808732824107907506	- 11712865443447096613735018567289719354
λ_1	24840293249469323791593259447993063951 2	- 38057537218403674948381648490498598688 8	- 16213349938504324319032429178550724291 2
λ_2	-65609642479133004807906938492852570245 8	10051980407232537628697615083894729498 82	42823652771372467663767226862096661358 8
λ_3	-13248146923033254730925691315293877353 36	20297338664026823963608411079998073035 04	86471137817363042440872218182603833581 6
λ_4	0	0	0
λ_5	44332882797809457077723614195387412823 84	- 67921917029413732913934085622060157294 16	- 28936234180687023469566681062216021927 04
λ_6	73469882452053623894758518998060388325 88	- 11256239037800038502377077175643345992 562	- 47954060049648240373616730601191127884 68
λ_7	-93082755104779967660705164156793121790 08	14261105459644304982919768821286922973 432	60755453512455024595136062260153774388 08
λ_8	-22502484123680276740277572463151863106 24	34475805839679635353288522486315595213 11	14687453399607794863751422556573090371 59
$\mathrm{N}_{K_0/\mathbb{Q}}(\Delta_C)$	$2^{144} \cdot 3^{24} \cdot 19^{12} \cdot 467^{21} \cdot 10083583^{21} \cdot 475392493003888418137 57^{21}$		

Table E.9: $C : y^2 = f(x)$ with CM by S No. 3.3.

λ_0	β^2	- 2425100197636199934048740878418024876804056631058792019458169962605805180704679526 4
	β	- 1345762803357391689741672576311148345357385154399521420422134334332768456883254067 2
	1	5449281410961506293400857687974442201652755756460647009285823118898454527769313280 0
λ_1	β^2	1296596662788921554673768795365295719302951226403302099555450372134608467656704000
	β	7193191314773829061628791698572572457316186298587973631189819622122988094095360 00
	1	- 2913258621190265150036490977625823022654761187686427626751553092332808161984512000
λ_2	β^2	5938491327367985451069555990581397182642319642990593711789353378242531164160000000
	β	3294520192918297367878130923180053092171269465761763664204505058106054541312000000
	1	-1334233162871257658391862634874795768251958814104638961166356351973692171878400000 0
λ_3	β^2	-3796074729264281162463210587096238056721016006523934686352278616916623360000000000
	β	- 2116007221728144732672231568495659537186730793448857071503372605183754240000000 00
	1	8541366718695542975834097374446542843697537521274978186516810392246681600000000 0
λ_4	β^2	0
	β	0
	1	0
λ_5	β^2	-29828783481828523310464590415933800313292384755816874747363637120000000000000000
	β	- 16400859733562122655932491821259486216475660730501436557063064384000000000000000
	1	66834057420867223951211588225750872498135268216825752518724399104000000000000000
λ_6	β^2	-362755101340307912229866695492316898221274018489742520033075864062500000000000000
	β	- 20102376183031995309536465009451142193244261085686641057747511468750000000000000
	1	81474154717393968191089669013566132392358359160477734256178806500000000000000000
λ_7	β^2	617919240334860393648041010069121363268125347201291627526165283203125000000000
	β	343773929640674336441817556550690425259736884185722429206562011718750000000000
	1	- 13895177191893800079181782897499380085200470558258910736205478515625000000000000
λ_8	β^2	904080509343504143002215600436221090967940581130166613641790866851806640625000
	β	501753347853497263930139502385823134087843601792255390994140625000000000000000
	1	- 203148354473696197046524364186024806189437500938930429275379818677902221679687 5
$N_{K_0/\mathbb{Q}}(\Delta_C)$		$2^{1152} \cdot 3^{504} \cdot 5^{504} \cdot 7^{201} \cdot 13^{56} \cdot 41^{56} \cdot 43^{56} \cdot 71^{56} \cdot 83^{56} \cdot 239^{112} \cdot 4088267^{21} \cdot 34990577^{56} \cdot 3646988717^{56} \cdot 3116415950405972 3^{21}$

Table E.10: $C : y^2 = f(x)$ with CM by S No. 2.2.

coef	β^2	β	1
λ_0	27493566365919293945808732824107907506	- 954841539401338826083440179963809778 7	- 791645692322033026478311091298657150 96
λ_1	8232884082828735820211955930437894079955 44	- 285925063585257446362223953310171583808 6152	- 237056449236685846198590582281250200095 2720
λ_2	-4704075388825406747760682507620762737338066190	16337082377547773862524888109772851919593561 68	13544845249825081701099474654860794878066259270
λ_3	-2054816563295086119104627412485605199815772566368 8	71363030331203269005040133293235593452166905586 56	59166084864891918654524651597727127393691543362224
λ_4	0	0	0
λ_5	32178554748734778852416632304890840318985545513510093662 4	- 11175494784146684296676097937745939449250193239626992764 8	- 92654455638617622829862258259826815269478860081447118408 8
λ_6	11536158827742570070362283319737756770781569525763805970405 62	- 40064659154275374988166696442220526678263558349740939605556 8	- 33217045473030386665272341702106417917588130282274770689870 52
λ_7	-31617856996619441466406424292108423294316079600230981210549146 48	10980766498393139140197551494008998702138709098036391068047481 52	91039990806194227454348810144854134119856696412411131703989486 96
λ_8	-16535029935785828954717938076021087759783314755593682223478268768 70	57425556320346990875356119495512121275224599435106593146865973244 2	47610721166049901007618985507871030218685128171494233240569082505 03
$N_{K_0/\mathbb{Q}}(\Delta_C)$	$2^{144} \cdot 3^{24} \cdot 19^{12} \cdot 467^{21} \cdot 10083583^{21} \cdot 47539249300388841813757^{21}$		

Table E.11: $C : y^2 = f(x)$ with CM by S No. 1.4.

λ_0	β^2	-18449163088294655929006831779916558051275376642942630842412793132755931507364419568368969725130559277460056683632939079261183816632231953210976705038409765897690572187773256096701027715692174688389677092238327618433112356072847738233340140657784693459267608824613547782656308876702072724103437949539217605184861434054484951040
	β	-607880038430429831323673185868547138380568661574700951404385723189544792775189291225221411200964293491711221206290289246886705628565752223678363031709473329607570243115069626962936715990680429288491412737303780573099841601690340928093541921187103634377725077846662365840283600755622467220576185947475890250169419260560429547 52
	1	13724910615142047015362043777042089947039800887371008043024279482402876112735753111926276352914110141243887821380104528788274515602210769031654542423436138430296498366424394565451191397596176026013419646465249323214081008745678867006497775038812286947963929871361721496810859501632499380968902247544404200704266361291403165696
λ_1	β^2	3339933579800229775567524683257694219007274970464860171618387339896651722821101828718043771025707961426839952676973996822202907070013196468234515271622747060059685030017961510062969327439641319285453760965294439279645191937313097644126823578411497439381503622872978267240060490944580553797662405052745463992997727971573760000
	β	1096196473173124134711982907947392917313100328814227109909412741227889491488000398520840143170676481799783871826699827196005040329892750305901015665366414316725259328626221864764981283406591460852323684025721429068544756786743029395762363441336209647680498551165629462263458444129999687714636990348877813399386103277735116800 0
	1	-2634628827804093757826397294923765118555630605731405171120368728405590341850381721064092328667365740510433175570785490533067606390780935474275571489304673839828880983169321540146819664441256076745339737048728569430271409587131303904619720581175728598440310917783646043558913400330266722394405476298518142514249287656800256000
λ_2	β^2	291077705757089874659491462601467979233490853274888531331113488776251447472804995217897432869896678539895122881958304388176481890209563624254438950353585940154629576049672106240316085654248254895224654008723478435921643274448108420587313714111111420658139483634943241436041631199233307478350740254597404867704195335061504000000
	β	956863168780246580094872532953439872079743563811145214064762621150354915785339030221227734019414803963147696583604370950414810918300115886447997130830842455196292608798612459919433513115625950561055298890304983365692204341095134145810518060765716617879530753300815314602310409145717714156180811333166126431542155631656960000 0
	1	-224280057391984143072941272760398063868865582529804521133604414728935173740051533224487149359160796550663485660545812862594751906377466003357394820574376407078368882175641989021576017730219377704559082923767110309980434366231337151299377031361177801759496702826200610196159525284181658952212398242069416770500610605711360000 0
λ_3	β^2	-91719179809949237928235407223137587428755401914956081966096432650808795393708398657688581146803731008814449166059744247615005759085485639037943877598623742514098384582309306898126178548884864983876184292894969953205656770551545068614678201072855416209811251696307200828577170248089251589755336156350466275901660200960000000000
	β	-301321648242004787235311718047433470259955171469939135557309086904704941349401894369395969914087515573336719620972363979953946145782191644857313486172923239050431712892865145402906256386668719970469413374174316133429176383668228887946806413111289012593332438596760881023644037997099665187842800533155951731123054182400000000000
	1	71330042587427200463638139355593436395718503539561844574026646814082775268013260374654683557134346984426274937393473053810880333309912441384303743002754459993964083789080101366828130387281918213540492753559229355181529959051793125872090152843700664728611587645135203881254775891246792160987342588434374242842265518080000000000
λ_4	β^2	0
	β	0
	1	0
λ_5	β^2	-442000699199282216205659552114304266859687201486396369143325081444941131260604026667010002197471471820161569786043187822254885151279187404250137923978146236046738373756668057150426611905407096857623816199861343683423650973466579724766982250605980676631071071532081420702858912510869869841550282167251912029356800000000000000
	β	-14520447451466099779543533587027350866700189257952463683187854747212829339986071794198223879748028938510226048727504916802091106345913941629562377252657045074695727253372969873571144420072608334937003456149050095095026738404166533518597665296864358263161195793167812568450091255301569879864280951392638887170944000000000000000
	1	343898064638227770183791211118813865452963852187013857022573957048299540463781571953200320684318438495519778546122577893686187073782369760647397990218132335351876035966381124343997405438285114751753746144894437860625325430480286937887858327768951004971784603476448552341061211200802723699026637831523903689305600000000000000
λ_6	β^2	-677190257764955735947021091159962390737748712884661897762652883712379754077318175245434183636103335584557779912321615148293363264678649138967332349223907021176023714480222082675916376741170413532024509177670761039841189023125191184733180993236984469641844886259154363433297667614788052586531873537471951768500000000000000000
	β	-22247126699020266720159979186054033526363968175978877287275476618128214217580422392353779966728207364612940514796368323795555164937018706334475623832317019404440632572559875071852765321307968010484259455074290802809657021311223130530787709772621689455359118049862992621375099639687026466895554501075969907565031250000000000000
	1	526775907658215855079372634822575264483672080224482676952899578872695482377369299411164217162651833788124073998213953827555021129878083468463356748189637951125074071476064549695288481626324086695317450148185188562463775427191737444873461319477436442762204951316377309727534297416138881322338929176221417445903125000000000000 0
λ_7	β^2	372617448822071472315741674236638417214366753082734516032748605829743936858457212306040769869557985576622234132203814868418890107291044573671777137153803751732236694531459039673686789782482415154900638151066922836138522106942058923983229065667813650166249699919732625259437325342381874861110983543445415969482421875000000000
	β	12240950342267755083532485428721611318108642797246427134299859102418595237442859337803122127579095685749746521640661202901127573244865622691985436703657096189612198665554546183099247195420356702148730494293978072630780708437754696531828055479611116994138286312811382050734127189124291636311804758465630361914306640625000000000
	1	-289964881332364363655164803285369475618486982543834304196867699478562901321758655426648271567900140346489879548254251007417148742316280797744524332939106642335125684584760997339913603726586681220099485041215019947677221100505704453744286649594375933434271389346055881113855520223822733794509381317814426712158203125000000000
λ_8	β^2	1003750660833953338381506614734579940123454316476980684028841550932570714630296364571687555222977958399842944080625119555723152025561445187954585862035729918275077830334690991015759885268774797514604724649324542154128785612667852595623638608120479301935628380518564180064012519962104031752685945626748585042774677276611328125
	β	329747356058633921481805931689392374962727408195208674233836561420365766239341571504550994298308290121154815366876643190791788167962325355817294113852528882614592374792212345928808941563491965014408935864688379319555694016140605559158778712833820779071723228481738894047379605552845772824933259990022030154418945312500000000 0
	1	-781008566488945133347701926966946840536433918759041430856515779655230391770930801983314361393306909069601758976718701437122497161474778014705101593889013554862122383242964268123487020701017141456123461157257032437056269999281585641619952670719529356249087633394591233815934087297374261616656697904148852662384510040283203125
$N_{K_0/\mathbb{Q}}(\Delta_C)$		$2^{1152} \cdot 3^{504} \cdot 5^{504} \cdot 7^{1166} \cdot 11^{640} \cdot 19^{12} \cdot 31^{12} \cdot 83^{12} \cdot 103^{56} \cdot 107^{77} \cdot 179^{56} \cdot 227^{56} \cdot 419^{56} \cdot 487^{56} \cdot 571^{56} \cdot 1481^{21} \cdot 3079^{56} \cdot 4751^{56} \cdot 5807^{56} \cdot 22003^{56} \cdot 56897^{56} \cdot 4224357323^{112} \cdot 85732107883^{112} \cdot 278290597943^{56} \cdot 669214525779853^{21} \cdot 110055216388228199611^{56} \cdot 12767681249414430824137629180954067009^{56} \cdot 91946198033397389412215801409731835233807599^{21} \cdot 16243651702850066219924469727508061844538381491^{21}$

Table E.12: $C \,:\, y^2 = f(x)$ with CM by S No. 1.2.

λ_0	β^2	-3024292084953929636911564644268442945408051017059497508351204254167579208137486179640595926825314404332229436218673576595998321982845400412265556899092011130042053287069085090962764268680395964963488290233037805880580901106241189355532791476022771680159024180690954166992896
	β	-63408347873406245180641469859611877280433671375653170154737435624938351452405077853638475007436486010241195640713373165111853665125737556688923527279443246646419687578999625576728417805018113620432378378058699143987951599824411485404417110815924905502106185858803514212352
	1	131437703449920717233919237953509514897021966148059181025143482232996532530121185678142185964864446890397728678818391759959823349289737298267098843660310195767647101390497833369033818938423594977638115267502165972335659691636731568489279682938560355124313272790880299778048
λ_1	β^2	477359638791256164130676200146190116790051464569706872066143250482458028625679401250798593704578881672344756614040484765461633635179530147807053373735296270384089167213064091658928867332854094168492213010980092936105202137064244181573857013920241035413246320119415570432000
	β	1042255972467454576369788498515802035273342563595361698142220086175861413306929038109436510900917592249913033302198427984271936327065768748119663053372835130010599418240962076466691001730451622721907406730782429699209469794769124901126268797013081799751708587952808394752000
	1	-2127850405154982981232288752494321699777635332221381370683749722327169798364521316022901895928614611109191666198260797361969507272890440203560520568238607965653027808805989507401062155959215255259158511637023875236459619493724171965705499886079525314904069759612884090880000
λ_2	β^2	-2376077740093004728161681296181494459971306889136907047374141933646053177762867885880924513940835920200122353071648759239755074754970332179217495512221339450625879144438143160229993932736828811442394305299165306451480502525066115142273216074740309116584634676288684032000000
	β	-5245780886506091332243856545453690462173611803208115585719505395508187052968778568189835958120450700715763455455767710660401881666583217898398049499012012078530471300030893058791791498066121182489886929048081805226706254222517886301071816486028583632551867723240439808000000
	1	10665884950355276684885534418701752813066960538492240925800818695214012295519574155500417544086953697129224342398395780522572209245338000128742593730998845363324545660067996025809307634128752332169239690601728379273429473229665855490804071904246371872196101401284182016000000
λ_3	β^2	4292212887104218959523695383834267653183558687521153825273471220180891198132247635788409586724230937958068313935741404012312248614979963740952290901236377957379402451740929578155055299771868978318022494841850809306426400836537523998342552229100834939075503304212480000000000
	β	9511440827255764453062359269281958477977686250904392429309850977218581423023883333683139280571602679740888320586407486413392478083959785310910609299181616962446056756402996308552727945672226469952653407487161728984019323825793588523557604901469636810894732173508608000000000
	1	-193125376973909821106028136306175665014891611431590191404220720215701485266951845984771019228200549577440586831886590852794994784487177842139284645148927898655338594284453423618963446726559786070002966704183217447512233069892573503305141300611037184924488719086387200000000000
λ_4	β^2	0
	β	0
	1	0
λ_5	β^2	-105910288083895402742479421356670686776380864573639028556870863449159675316751204693741936969480358943024158016195573724364641419273728354435681423801096197961366349199881483112873234560312452477980909508056505550400012169414308004864924766250681160380871695232000000000000000000
	β	-235189153492653827567868439195940912097624599990414753769106312748558640909577731066346382419185618739543744049411401394073434210048546575423390280794658622359437026837301293408512789556909877793000056013357522125118342652781397347961002858214192441335488337920000000000000000
	1	477172072059930995244788812440137110478812900381748371714212208578635508593719865894842080559839188340960978087682626769411920086679485386752440859537806132558633601275122728738060173201117813193316017225975152430734681038421711089112514308170736542716441156480000000000000000
λ_6	β^2	144506101771703605182933773520725034226100248007158032946774772039564127814695148016083651888994667884356270157754226227083366519056511388386246326527933695983957715618599464011263145762939240702700685653996018178784352335131759838372479565018404135665567610312500000000000000
	β	320985670318001553172306541989450794263890308610992103225434339857032483130882134725083834208677774948228394494235364403258878602771119145549929993840301927298001137389240157539383988407850038588733359919327302411859403982758620289957871910073512410724990341593750000000000000
	1	-651177326814938469045149932865784086502327751744730239273373662310127621609281867509315744401072128504111030494947263717700766232786588555806685047622183821438737410364429873585017020030267114742126873002934200617884699132594847812258845694358613922772760381875000000000000000
λ_7	β^2	-7124970714969915281219408126780318615068822400332331970969982019923232272251503418659812124241221420978913972655410783406895816308314902630240352496971321908944085280987241515397436472373349836744707167991941827693240978998376153270738991014252437044577797607421875000000000
	β	15828294113219196614047798792064827859050499845423267938657311095118015929548435301741066799553810337986750690783815779841147229218846975705679732234156988691027741126134197657253019508808351874829372143679967056579514223483510846847384266403637518995511267333984375000000000
	1	32109152102947155232144760288966448736866627464412769346756646642689011628104856807735132276694194170319221060561753762760691569876700599362186369579965523908002692789038675160031361062034034917291671200473430382039055722241894722190608804315336805818374675048828125000000000
λ_8	β^2	1088979856736857036023973529175013539361224331095272487673089303774046573571087119000834053521853589712141223405155528744090984187479310815816272097776043021603463799386907270441572749962693334691219207275796243558127566759541715415560695155309580705935134589672088623046875
	β	2419312197513245775497875151674929266071450208643952916744199397604364260908276226542025217878598876704608609613220975088040273775643821135719490731419041509364163842603745201748478360960787977882595021084189456753804260012626819539360705644481309068005020380020141601562500
	1	-4907710428676468887449723566273582672563688648289418252951441469533359434851947818078743837105375057866099694602283513053140918869788931201940437592244412112038494169253367071479086678122087456326418674634571588264130971966695420754974803680779486134731250643730163574218750
$N_{K_0/\mathbb{Q}}(\Delta_C)$		$2^{1152} \cdot 3^{504} \cdot 5^{504} \cdot 7^{865} \cdot 11^{584} \cdot 19^{168} \cdot 31^{56} \cdot 83^{56} \cdot 103^{12} \cdot 151^{56} \cdot 179^{56} \cdot 229^{56} \cdot 353^{112} \cdot 467^{56} \cdot 1151^{56} \cdot 1787^{56} \cdot 2957^{21} \cdot 6619^{112} \cdot 19867^{56} \cdot 22751^{56} \cdot 2452585523^{21} \cdot 159305741669^{112} \cdot 1171785483040540391^{21} \cdot 122187983271679542336351 97^{56} \cdot 1367226421107681665842903727145 7^{56} \cdot 224890685367496037899257973054950403913219194996721735 9^{21}$

References

[AK13] Allen Altman and Steven Kleiman. *A Term of Commutative Algebra*. Worldwide Center of Mathematics, 2013.

[AM93] A Oliver L Atkin and François Morain. "Elliptic curves and primality proving". In: *Mathematics of computation* 61.203 (1993), pp. 29–68.

[Bak68] Alan Baker. "Linear Forms in the Logarithms of Algebraic Numbers (IV)". In: *Mathematika* 15.2 (1968), pp. 204–216.

[Bal+16] Jennifer S Balakrishnan et al. "Constructing Genus-3 Hyperelliptic Jacobians with CM". In: *LMS Journal of Computation and Mathematics* 19.A (2016), pp. 283–300.

[BGL11] Reinier Bröker, David Gruenewald, and Kristin Lauter. "Explicit CM Theory for Level 2-Structures on Abelian Surfaces". In: *Algebra & Number Theory* 5.4 (2011), pp. 495–528.

[Bis11] Gaetan Bisson. "Endomorphism Rings in Cryptography". PhD thesis. Technische Universiteit Eindhoven, 2011.

[BL04] Christina Birkenhake and Herbert Lange. *Complex Abelian Varieties*. Springer, 2004.

[Bos+22] W. Bosma et al. *Magma*. 2022. URL: `http://magma.maths.usyd.edu.au/magma/`.

[BS15] Florian Bouyer and Marco Streng. "Examples of CM Curves of Genus Two Defined over the Reflex Field". In: *LMS Journal of Computation and Mathematics* 18.1 (2015), pp. 507–538.

[BS17] Gaetan Bisson and Marco Streng. "On Polarised Class Groups of Orders in Quartic CM-Fields". In: *Mathematical Research Letters* 24.2 (2017), pp. 247–270.

[BS22] Florian Bouyer and Marco Streng. *Reduction of binary forms and hyperelliptic curve equations*. 2022. URL: `https://bitbucket.org/mstreng/reduce/src/master`.

[Coh+05] Henri Cohen et al. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC press, 2005.

[Coh12] Henri Cohen. *Advanced Topics in Computational Number Theory*. Springer Science & Business Media, 2012.

[Cox13] David A. Cox. *Primes of the Form x^2+ny^2; Fermat, Class Field Theory and Complex Multiplication*. Wiley, 2013.

[DCD00] Ilaria Del Corso and Roberto Dvornicich. "Relations among Discriminant, Different and Conductor of an Order". In: *Journal of Algebra* 224.1 (2000), pp. 77–90.

[DH76] Whitfield Diffie and Martin Hellman. "New directions in cryptography". In: *IEEE Transactions on information theory* 22.6 (1976), pp. 644–654.

[DTZ61] EC Dade, O Taussky, and H Zassenhaus. "On the semigroup of ideal classes in an order of an algebraic number field". In: (1961).

[Fue14] Rudolf Fueter. "Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern". In: *Mathematische Annalen* 75.2 (1914), pp. 177–255.

[Has27] Helmut Hasse. "Neue Begründung der komplexen Multiplikation. Erster Teil: Einordnung in die allgemeine Klassenkörpertheorie." In: 1927.157 (1927), pp. 115–140.

[Hee52] Kurt Heegner. "Diophantische Analysis und Modulfunktionen". In: *Mathematische Zeitschrift* 56.3 (1952), pp. 227–253.

[Hil96] David Hilbert. "Ein neuer Beweis des Kronecker'schen Fundamentalsatzes über Abel'sche Zahlkörper". In: *Nachr. Ges. Wiss. Göttingen* (1896), pp. 29–39.

[IS23] Federal Office for Information Security. *BSI- Technical Guideline*. 2023. URL: `https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TG02102/BSI-TR-02102-1.pdf?__blob=publicationFile`.

[Jan96] Gerald J Janusz. *Algebraic Number Fields*. American Mathematical Society, 1996.

[JT15] Christian U Jensen and Anders Thorup. "Gorenstein Orders". In: *Journal of Pure and Applied Algebra* 219.3 (2015), pp. 551–562.

[JW19] Dimitar Jetchev and Benjamin Wesolowski. "Horizontal Isogeny Graphs of Ordinary Abelian Varieties and the Discrete Logarithm Problem". In: *Acta Arithmetica* 187 (2019), pp. 381–404.

[Kıl16] Pınar Kılıçer. "The CM class number one problem for curves". PhD thesis. Universiteit Leiden and l'Université de Bordeaux, 2016.

[Kro53] Leopold Kronecker. "Über die algebraisch auflösbaren Gleichungen (I), Monatsbericht". In: *Kgl. Preuss. Akad. Wiss. Berlin* (1853), pp. 365–374.

[KW05] Kenji Koike and Annegret Weng. "Construction of CM Picard Curves". In: *Mathematics of computation* 74.249 (2005), pp. 499–518.

[Lan12] Serge Lang. *Algebra*. Springer Science & Business Media, 2012.

[Lan19] Serge Lang. *Abelian Varieties*. Dover Publications, 2019.

[Lan83] Serge Lang. *Complex Multiplication*. Springer, 1983.

[Lan87] Serge Lang. *Elliptic Functions*. Springer, 1987.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press on Demand, 2002.

[LR12] Reynald Lercier and Christophe Ritzenthaler. "Hyperelliptic Curves and their Invariants: Geometric, Arithmetic and Algorithmic Aspects". In: *Journal of algebra* 372 (2012), pp. 595–636.

[LT16] Hugo Labrande and Emmanuel Thomé. "Computing Theta Functions in Quasi-Linear Time in Genus Two and Above". In: *LMS Journal of Computation and Mathematics* 19.A (2016), pp. 163–177.

[Mar20] Stefano Marseglia. "Computing the Ideal Class Monoid of an Order". In: *Journal of the London Mathematical Society* 101.3 (2020), pp. 984–1007.

[Mar21] Stefano Marseglia. *Isomorphism Classes of Abelian Varieties and Polarizations over Finite Fields*. 2021. URL: `https://github.com/stmar89/AbVarFq`.

[Mat58] Teruhisa Matsusaka. "Polarized varieties, fields of moduli and generalized Kummer varieties of polarized abelian varieties". In: *American Journal of Mathematics* 80.1 (1958), pp. 45–82.

[McD74] Bernard R McDonald. *Finite Rings with Identity*. Marcel Dekker Incorporated, 1974.

[MU01] Naoki Murabayashi and Atsuki Umegaki. "Determination of all Q-Rational CM-Points in the Moduli Space of Principally Polarized Abelian Surfaces". In: *Journal of Algebra* 235.1 (2001), pp. 267–274.

[Mum07] David Mumford. *Tata Lectures on Theta II*. Springer, 2007.

[Mum99] David Mumford. *The Red Book of Varieties and Schemes*. Springer Science & Business Media, 1999.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Spinger, 1999.

[San91] Jonathan W Sands. "Generalization of a Theorem of Siegel". In: *Acta Arithmetica* 58.1 (1991), pp. 47–57.

[SC03] Michael Stoll and John E. Cremona. "On the reduction theory of binary forms". In: *Journal für die reine und angewandte Mathematik* 565 (2003), pp. 79–99.

[SCV21] Jeroen Sijsling, Edgar Costa, and John Voight. *Rigorous Computation of the Endomorphism Ring of a Jacobian*. 2021. URL: `https://github.com/edgarcosta/endomorphism`.

[Shi16] Goro Shimura. *Abelian Varieties with Complex Multiplication and Modular Functions*. Princeton University Press, 2016.

[Shi55] Goro Shimura. "On Complex Multiplication". In: *Proceedings of the International Symposium on Algebraic Number Theory, Tokyo & Nikko*. 1955, pp. 23–30.

[Shi67] Tetsuji Shioda. "On the Graded Ring of Invariants of Binary Octavics". In: *American Journal of Mathematics* 89.4 (1967), pp. 1022–1046.

[Shi71] Goro Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions*. Princeton University Press, 1971.

[Sij21] Jeroen Sijsling. *A Magma package for Calculating with CM Curves*. 2021. URL: `https://github.com/JRSijsling/cm-calculations`.

[Sij22] Jeroen Sijsling. *Geometric and Arithmetic Reconstruction of Curves from their Period Matrices*. 2022. URL: `https://github.com/JRSijsling/curve_reconstruction`.

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

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

[ST61] Goro Shimura and Yutaka Taniyama. *Complex Multiplication of Abelian Varieties and its Applications to Number Theory*. Mathematical Society of Japan, 1961.

[Sta+67] Harold M Stark et al. "A Complete Determination of the Complex Quadratic Fields of Class-Number One." In: *Michigan Mathematical Journal* 14.1 (1967), pp. 1–27.

[Ste08] Peter Stevenhagen. "The Arithmetic of Number Rings". In: *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography* 44 (2008), pp. 209–266.

[Ste12] Peter Stevenhagen. “Number rings”. In: *Lecture notes* (2012).

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

[Str21] Marco Streng. *Recip*. 2021. URL: `https://bitbucket.org/mstreng/recip/src/master/`.

[Sut19] Andrew Sutherland. “Number Theory I”. In: *Lecture notes* (2019).

[Tak20] Teiji Takagi. *Über eine Theorie des relativ Abel'schen Zahlkörpers*. Vol. 41. 9. 1920.

[Tan55] Yutaka Taniyama. “Jacobian Varieties and Number Fields”. In: *Proceedings of the International Symposium on Algebraic Number Theory, Tokyo & Nikko*. 1955, pp. 31–45.

[The21] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 8.7.)* `https://www.sagemath.org`. 2021.

[VW99] Paul Van Wamelen. “Examples of Genus Two CM Curves Defined over the Rationals”. In: *Mathematics of Computation* 68.225 (1999), pp. 307–320.

[Web86] Heinrich Weber. “Theorie der Abel'schen Zahlkörper”. In: *Acta Mathematica* 8.1 (1886), pp. 193–263.

[Web97] Hermann-Josef Weber. “Hyperelliptic Simple Factors of $J_0(N)$ with Dimension at least 3”. In: *Experimental Mathematics* 6.4 (1997), pp. 273–287.

[Wei55] Andrew Weil. “On the Theory of Complex Multiplication”. In: *Proceedings of the International Symposium on Algebraic Number Theory, Tokyo & Nikko*. 1955, pp. 149–156.

[Wen01a] Annegret Weng. “A Class of Hyperelliptic CM-Curves of Genus Three”. In: *Journal-Ramanujan Mathematical Society* 16.4 (2001), pp. 339–372.

[Wen01b] Annegret Weng. “Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation”. PhD thesis. Universität GH Essen, 2001.

Selbstständigkeitserklärung

Hiermit versichere ich, dass ich diese Dissertation selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Sie wurde weder in ihrer Gesamtheit noch in Teilen einer anderen wissenschaftlichen Hochschule zur Begutachtung in einem Promotionsverfahren vorgelegt.

Außerdem erkläre ich, dass ich die allgemeinen Prinzipien wissenschaftlicher Arbeit und Veröffentlichung, wie sie in den Leitlinien guter wissenschaftlicher Praxis der Carl von Ossietzky Universität Oldenburg festgelegt sind, befolgt habe.

Oldenburg, den 31.01.2024

Marco Melles