HAL open science

Complex multiplication constructions of abelian extensions of quartic fields

Jared Asuncion

▶ To cite this version:

Jared Asuncion. Complex multiplication constructions of abelian extensions of quartic fields. Number Theory [math.NT]. Université de Bordeaux; Universiteit Leiden (Leyde, Pays-Bas), 2022. English. NNT : 2022BORD0169 . tel-03708516

HAL Id: tel-03708516

https://theses.hal.science/tel-03708516v1

Submitted on 29 Jun 2022

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Co-supervised thesis presented to obtain the qualification of

DOCTOR OF THE UNIVERSITY OF BORDEAUX
AND LEIDEN UNIVERSITY

Doctoral School of Mathematics and Computer Science

Specialization: Pure Mathematics

by

JARED ASUNCION

Complex multiplication constructions of abelian extensions of quartic fields

Under the supervision of Andreas Enge and Marco Streng

Defense on: 24 may 2022

Members of the examination panel:

Mr. David KOHEL	Professor, Aix-Marseille Université	President
Mr. Claus FIEKER	Professor, Technische Universität Kaiserslautern	Referee
Mr. David KOHEL	Professor, Aix-Marseille Université	Referee
Mrs. Sorina IONICA	Maître de conférences, Université de Picardie	Examiner
Mr. Ronald VAN LUIJK	Professor, Universiteit Leiden	Examiner
Mr. Andreas ENGE	Directeur de recherche, INRIA	Co-director
Mr. Marco STRENG	Associate Professor, Universiteit Leiden	Co-director

Title: Complex multiplication constructions of abelian extensions of quartic fields

Abstract: Let (K, Φ) be a primitive quartic CM pair and (K^r, Φ^r) be its reflex. In a 1962 article titled *On the class-fields obtained by complex multiplication of abelian varieties*, Shimura considered a particular family $\{F_{K^r}(m) : m \in \mathbb{Z}_{>0}\}$ of abelian extensions of K, and showed that the Hilbert class field $H_{K^r}(1)$ of K is contained in $F_{K^r}(m)$ for some positive integer m. In this thesis, we make this m explicit. We also give a way to determine, given a positive integer n, whether or not $H_{K^r}(1) \subseteq F_{K^r}(n)$. In addition, we show a way to compute defining polynomials of the extension $F_{K^r}(n)/K^r$ for any positive integer n. We also give an algorithm that computes a set of defining polynomials for the Hilbert class field $H_{K^r}(1)$ using information on $F_{K^r}(m)$. Our proof-of-concept implementation of this algorithm computes a set of defining polynomials much faster than current implementations of the generic Kummer algorithm for certain examples of quartic CM fields.

Keywords: complex multiplication, CM fields, Hilbert class fields

Title: Constructions de multiplication complexe d'extensions abéliennes de corps quartiques

Abstract: Soit (K, Φ) une paire CM quartique primitive et (K^r, Φ^r) son réflexe. Dans un article de 1962 intitulé *On the class-fields obtained by complex multiplication of abelian varieties*, Shimura considère une famille particulière $\{F_{K^r}(m) : m \in \mathbb{Z}_{>0}\}$ d'extensions abéliennes de K, et montre que le corps de classe Hilbert $H_{K^r}(1)$ de K est contenu dans $F_{K^r}(m)$ pour un certain entier positif m. Dans cette thèse, nous donnons une valeur explicite de cet entier m. Nous donnons également un moyen de déterminer, étant donné un entier positif n, si $H_{K^r}(1) \subseteq F_{K^r}(n)$ ou non. De plus, nous donnons une manière de calculer les polynômes de définition de l'extension $F_{K^r}(n)/K^r$ pour tout entier positif n. Nous donnons également un algorithme qui calcule un ensemble de polynômes de définition pour le corps de classes de Hilbert $H_{K^r}(1)$ en utilisant des informations sur $F_{K^r}(m)$. Nous avons implanté cet algorithme et nous calculons un ensemble de polynômes de définition beaucoup plus rapidement que les implantations actuelles de l'algorithme générique de Kummer pour certains exemples de corps CM quartiques.

Keywords: multiplication complexe, corps CM, corps de classes de Hilbert

Institut de Mathématiques de Bordeaux UMR 5251
Université de Bordeaux
351, cours de la Libération - F 33 405 TALENCE

Mathematisch Instituut
Universiteit Leiden
Niels Bohrweg 1 2333 CA Leiden

Complex multiplication constructions of abelian extensions of quartic fields

PROEFSCHRIFT

ter verkrijging van
de graad van doctor aan de Universiteit Leiden,
op gezag van rector magnificus prof. dr. ir. H. Bijl,
volgens besluit van het college voor promoties
te verdedigen op dinsdag 24 mei 2022
klokke 11:15 uur
door

Jared Guissmo Asuncion

geboren te Mandaluyong, de Filipijnen
in 1992

Promotores:

prof. dr. Andreas Enge (INRIA)
prof. dr. Peter Stevenhagen

Copromotor:

dr. Marco Streng

Promotiecommissie:

prof. dr. Bas Edixhoven †
prof. dr. Claus Fieker (Technische Universität Kaiserslautern)
dr. Sorina Ionica (Université de Picardie)
prof. dr. David Kohel (Aix-Marseille Université)
prof. dr. Ronald van Luijk

This work was funded by a cotutelle program between
Leiden University and University of Bordeaux.

Contents

Introduction (English) **9**

Introduction (Français) **13**

Samenvatting **17**

1 Class field theory and elliptic curves **21**

1.1 Class field theory 21

1.2 Complex multiplication theory for elliptic curves 23

1.2.1 Elliptic curves and their endomorphism rings 24

1.2.2 Fields of moduli of elliptic curves 26

1.2.3 Torsion points of elliptic curves 27

1.2.4 Elliptic curves as complex tori 28

2 CM theory on principally polarized abelian varieties **35**

2.1 CM fields 35

2.1.1 The type norm 36

2.1.2 The reflex field 37

2.1.3 The field generated by CM 38

2.2 Jacobians of hyperelliptic curves 39

2.2.1 Hyperelliptic curves and their Jacobians 39

2.2.2 Principal polarizations on complex tori 43

2.2.3 Fields of moduli of Jacobian surfaces 46

2.2.4 Primitive torsion points of Jacobian surfaces 49

2.2.5 Kummer varieties of Jacobian surfaces 50

2.2.6 The Main Theorems of Complex Multiplication 53

2.3 Theta functions 55

2.3.1 Rosenhain invariants 56

2.3.2 Mumford polynomials and theta functions 58

3 An explicit abelian extension containing the Hilbert class field **63**

3.1 Proof of the main theorem 65

3.1.1 Embedding problems 66

3.1.2 An explicit integer 70

3.2 A decision problem 75

3.2.1 The Shimura ray class group 76

3.2.2 An algorithm to answer the decision problem 79

4 Computing abelian extensions generated by CM theory **81**

4.1 Abelian extensions in terms of Kummer varieties 82

4.2 A Kummer variety over $\mathrm{CM}_{K^r,\Phi^r}(2)$ 83

4.3 An algorithm for computing $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ with $2 \mid \mathfrak{m}$ 87

4.3.1 Finding a primitive torsion point 87

4.3.2 Finding the conjugates of h_2 89

4.3.3 Computing the extension $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ 92

5 Algorithms for finitely generated abelian groups **95**

5.1 Nice groups 96

5.1.1 Definitions 96

5.1.2 Examples of nice groups 98

5.2 Subgroups and Hermite normal forms 100

5.2.1 Representing subgroups 100

5.2.2 Finding kernels 102

5.2.3 Finding images 104

5.2.4 Finding intersections 105

5.3 Building Nice Groups 106

5.3.1 Subgroups as nice groups 106

5.3.2 Finding quotients 108

5.3.3 Finding group extensions 109

5.3.4 Computing the Shimura ray class group 111

6 Examples **115**

6.1 A detailed example 116

6.1.1 Computing the cokernel of N_1 117

6.1.2 Computing the kernel of N_2 118

6.1.3 Computing the Shimura ray class group 118

6.1.4 Verifying that the Hilbert class field is in the compositum . . . 119
6.1.5 Computing the Hilbert class field of the reflex 119
6.2 An example involving torsion points 121
6.2.1 A base period matrix 122
6.2.2 The reflex field and Hilbert class field 123
6.2.3 A primitive torsion point 123
6.2.4 Approximations 125
6.3 On the division-minimality of the integer given in Corollary 3.3 126
6.4 Comparison with Kummer theory 128
6.5 An experiment 129

Bibliography **137**

Acknowledgments **141**

Curriculum Vitae **143**

Introduction

The Kronecker-Weber Theorem is a classical result in number theory. It is a statement concerning *abelian extensions*, Galois extensions of a number field with abelian Galois group.

> **Theorem 0.1** (Kronecker-Weber Theorem)**.** Every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension $\mathbb{Q}(\zeta_m)$ with $\zeta_m = \exp(2\pi i/m)$ for some $m \in \mathbb{Z}_{>0}$.
>
> The Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorphic to $(\mathbb{Z}/m\mathbb{Z})^\times$ via the map
>
> $$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &\to \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\\ a + m\mathbb{Z} &\mapsto (\zeta_m \mapsto \zeta_m^a).\end{aligned}$$

This theorem, combined with Galois theory, tells us that every abelian extension of $\mathbb{Q}$ can be expressed as $\mathbb{Q}(\boldsymbol{\alpha})$ where $\boldsymbol{\alpha}$ is a polynomial in an mth root of unity for some positive integer m. For example, the abelian extension

$$L = \mathbb{Q}[X]/(X^3 - 3X + 1)$$

is contained in the cyclotomic field $\mathbb{Q}(\zeta_9)$. Indeed, the field L is equal to

$$\mathbb{Q}(\zeta_9 + \zeta_9^8).$$

While L is also contained in other cyclotomic fields $\mathbb{Q}(\zeta_n)$ for other positive integers n, the integer 9 is the smallest integer satisfying this condition. Such an integer is called the *conductor of the extension* $L/\mathbb{Q}$.

The twelfth of Hilbert's 23 problems, also known as Kronecker's Jugendtraum[1], asks to

[1] Kronecker's dream of his youth

find an analogue of the Kronecker-Weber Theorem when the base field $\mathbb{Q}$ is replaced by another number field.

Class field theory (Section 1.1) tells us that, for every number field K and for every positive integer m there exists a bijection between the set of subgroups of a so-called ray class group $\mathrm{Cl}_K(m)$ of K and the set of abelian extensions L/K of conductor[2] dividing m. However, given a subgroup of $\mathrm{Cl}_K(m)$, the corresponding bijection does not necessarily give an explicit description of the abelian extension.

Not all hope is lost as there exists a case for which an explicit analogue of Theorem 0.1 is known. This is the case where the base field K is an imaginary quadratic number field, instead of Kronecker-Weber's $\mathbb{Q}$. Complex Multiplication (CM) theory (Section 1.2) for elliptic curves provides this analogue. Using CM theory, one may find defining polynomials of any abelian extension of any imaginary quadratic number field K.

A generalization of CM theory to higher dimensional principally polarized abelian varieties was developed by Shimura and Taniyama during the 1950s. Like its elliptic curve counterpart, the theory explicitly describes abelian extensions of so-called CM fields in terms of special values of modular functions. However, the theory does not cover *all* abelian extensions of a CM field hence it does not give an analogue of the Kronecker-Weber theorem on its own.

In this thesis, however, we show that we can use Shimura's CM theory to explicitly compute the largest unramified[3] abelian extension, called the Hilbert class field, of *any* primitive quartic CM field. With this thesis, we hope to encourage further exploration on how to utilize CM theory to advance research on abelian extensions.

This thesis is divided into the following chapters.

In Chapter 1, we review how CM theory is used to find all abelian extensions of an imaginary quadratic number field. In Chapter 2, we review the more general CM theory.

An adaptation of Shimura's [30, Theorem 2] shows that for some positive integer m, the Hilbert class field $H_{K^r}(1)$ of a primitive quartic CM field K^r with real quadratic subfield K_0^r is contained in the compositum Ξ_m of the ray class field $H_{K_0^r}(m)$ of K_0^r

[2]See the definition of conductor on page 22

[3]An abelian extension is unramified if and only if its conductor is 1.

and an abelian extension $\mathrm{CM}_{K^r,\Phi^r}(m)$ of K^r, defined in Section 2.1.3, given by CM theory.

In Chapter 3, we do several things related to this result of Shimura. First, we prove a theorem that gives us an integer m for which Shimura's result is true. Then we define, for every positive integer m, the Shimura ray class group $\mathfrak{C}_K(m)$ of a CM field K related to K^r. Using this Shimura ray class group, we give an algorithm, which takes as input a positive integer m' and outputs whether or not the Hilbert class field is contained in $\Xi_{m'}$. This algorithm enables us to find the smallest positive integer m for which Shimura's result is true.

The aforementioned result of Shimura is useful for computational purposes because both parts of the compositum can be explicitly computed. In Chapter 4, we show how to compute the abelian extension $\mathrm{CM}_{K^r,\Phi^r}(m)$. Ray class fields of real quadratic fields, such as $H_{K_0^r}(m)$, can be computed efficiently in practice and we cite the relevant articles in the introduction of the chapter.

In order to make the above theory really explicit, we have implemented most of the algorithms discussed in this thesis.

The algorithm to compute the Shimura ray class group uses algorithms to compute kernels, images, quotients and group extensions involving finitely generated abelian groups and morphisms between them. These algorithms are known and found in [6, Chapter 4]. In Chapter 5, we restate these algorithms in detail, carefully taking note of which information is needed to compute which groups.

To our knowledge, these algorithms have not been implemented as built-in functions in any computer algebra system. Hence, we have implemented these algorithms and made them available as a pair of PARI/GP [21] scripts – `fgag.gp` and `fgagshimuray.gp`. The former implements the required algorithms found in [6, Chapter 4] and the latter uses the former to implement the algorithm which computes the Shimura ray class group.

We use our code and other built-in functions from PARI/GP [21] and SAGE [27] in order to show how our method of constructing CM fields works. In Chapter 6, we give explicit examples using our CM theory algorithm, compare how our method fares against the well-known generic Kummer theory algorithms, and discuss the limitations of both approaches.

Introduction

Les polynômes sont des elements de base importants dans presque toutes les ma thé ma tiques. En théorie des nombres, un nombre qui est la racine d'un polynôme à coefficients dans $\mathbb{Q}$, comme

$$a_n x^n + \ldots + a_1 x + a_0 \qquad \text{où} \qquad a_i \in \mathbb{Q},$$

s'appelle un *nombre algébrique*. Par exemple, le nombre complexe

$$\zeta_5 := \exp(2\pi i/5)$$

qui est une racine du polynôme

$$f = x^4 + x^3 + x^2 + x + 1$$

de degré 4, dont les coefficients sont tous $1 \in \mathbb{Q}$, est un nombre algébrique.

Un corps de nombres est une extension du corps $\mathbb{Q}$ obtenue en adjoignant un ensemble fini de nombres algébriques à $\mathbb{Q}$. Par exemple, le plus petit corps contenant $\mathbb{Q}$ et toutes les racines du polynôme f est écrit $\mathbb{Q}(\zeta_5)$. Ce corps est obtenu en adjoignant l'ensemble des racines du polynôme f à $\mathbb{Q}$. Plus concrètement, ce corps de nombres $\mathbb{Q}(\zeta_5)$ est donné par

$$\left\{a + b\,\zeta_5 + c\,\zeta_5^2 + d\,\zeta_5^3 + e\,\zeta_5^4 : a, b, c, d, e \in \mathbb{Q}\right\}.$$

La théorie de Galois, developpée par le mathématicien français Évariste Galois pendant les années 1800s, décrit les symétries entre les racines des polynômes et les symétries liées dans les corps de nombres qui leur sont associés. Il a fait cette description en termes de ce qu'on appelle maintenant un *groupe de Galois*. Le groupe de Galois d'une extension de corps galoisienne $L/\mathbb{Q}$ est composé des automorphismes du corps de nombres L qui fixent $\mathbb{Q}$.

Le théorème de Kronecker-Weber est un résultat classique de la théorie des nombres. Il concerne les extensions abéliennes, extensions galoisiennes d'un corps de nombres avec un groupe de Galois abélien.

> **Théorème de Kroncker-Weber.** Toute extension abélienne finie de $\mathbb{Q}$ est contenue dans une extension cyclotomique $\mathbb{Q}(\zeta_m)$ avec $\zeta_m = \exp(2\pi i/m)$ pour un certain entier m.
>
> Le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ est isomorphe à $(\mathbb{Z}/m\mathbb{Z})^\times$ via l'application
>
> $$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\\ a + m\mathbb{Z} &\mapsto (\zeta_m \mapsto \zeta_m^a).\end{aligned}$$

Ce théorème combiné à la théorie de Galois nous dit que toute extension abélienne de $\mathbb{Q}$ peut être exprimée comme $\mathbb{Q}(\boldsymbol{\alpha})$ où $\boldsymbol{\alpha}$ est un polynôme en une racine m-ème de l'unité pour un certain entier m. Par exemple, l'extension abélienne

$$L = \mathbb{Q}[X]/(X^3 - 3X + 1)$$

est contenue dans le corps cyclotomique $\mathbb{Q}(\zeta_9)$. Effectivement, le corps L est égal à

$$\mathbb{Q}(\zeta_9 + \zeta_9^8).$$

Bien que L soit aussi contenu dans d'autres corps cyclotomiques $\mathbb{Q}(\zeta_n)$ pour d'autres entiers n, le plus petit entier vérifiant cette condition est 9. Cet entier est appelé le conducteur de l'extension $L/\mathbb{Q}$.

Le douzième problème de Hilbert, aussi connu comme le Jugendtraum de Kronecker, demande de chercher un analogue du théorème de Kronecker-Weber quand le corps de base est remplacé par un autre corps de nombres.

La théorie des corps de classes nous dit que pour tout corps de nombres K, et pour tout entier positif m, il existe une bijection entre l'ensemble des sous-groupes du groupe appelé *groupe* $Cl_K(m)$ *de classes de rayon* m de K et l'ensemble des extensions abéliennes L/K dont le conducteur divise m. Toutefois, étant donné un sous-groupe de $\mathrm{Cl}_K(m)$, la bijection correspondante ne fournit pas a priori une description explicite des extensions abéliennes.

Tout espoir n'est pas perdu parce qu'il existe un cas pour lequel un analogue explicite du théorème de Kroncker-Weber est connu. C'est le cas où le corps de base K est un corps de nombres quadratique imaginaire, au lieu du corps $\mathbb{Q}$ de Kronecker-Weber. La théorie de la multiplication complexe (CM) pour les courbes elliptiques nous fournit cet analogue. En utilisant la théorie CM, on peut trouver des polynômes de définition de n'importe quelle extension abélienne d'un corps de nombres quadratique imaginaire.

Une généralisation de la théorie CM aux variétés abéliennes principalement polarisées de dimension supérieure a éte développée par Shimura et Taniyama pendant les années 1950. Comme la théorie pour les courbes elliptiques, la généralisation de la théorie CM décrit explicitement les extensions abéliennes des corps CM en termes de valeurs spéciales de fonctions modulaires. Toutefois, la théorie ne couvre pas toutes les extensions abéliennes d'un corps CM, de sorte que ce n'est pas exactement un analogue du théorème de Kronecker-Weber.

Cette thèse est composée des chapitres suivants.

Dans le Chapitre 1, nous rappelons comment la théorie CM est utilisée pour trouver toutes les extensions d'un corps de nombres quadratique imaginaire. Dans le Chapitre 2, nous rappelons la théorie CM plus générale.

Une adaption de [30, Theorem 2] de Shimura nous montre que pour un certain entier positif m, le corps de classes de Hilbert $H_{K^r}(1)$ d'un corps CM K^r avec un sous-corps quadratique réel K_0^r est contenu dans le compositum Ξ_m du corps de classes de rayon $H_{K_0^r}(m)$ de K_0^r et d'une extension abélienne $\mathrm{CM}_{K^r,\Phi^r}(m)$ de K^r, définie dans la Section 2.1.3 et donnée par la théorie CM.

Dans le Chapitre 3, nous réalisons quelques travaux en rapport avec ce résultat de Shimura. Tout d'abord, nous donnons un théorème qui nous fournit un entier m pour lequel le résultat de Shimura est vrai. Ensuite, nous définissons, pour tout entier positif m, le groupe de classes de rayon de Shimura $\mathfrak{C}_K(m)$ d'un corps CM K lié à K^r. En utilisant ce groupe de classes de rayon de Shimura, nous donnons un algorithme qui prend en entrée un entier positif m et qui indique si le corps de classes de Hilbert est oui ou non contenu dans Ξ_m. Cet algorithme nous permet de trouver le plus petit entier positif m pour lequel le résultat de Shimura est vrai.

Le résultat sus-mentionné de Shimura est utile à des fins de calcul car les deux parties du compositum peuvent être explicitement calculées. Au Chapitre 4, nous montrons comment calculer l'extension abélienne $\mathrm{CM}_{K^r,\Phi^r}(m)$. Les corps de classes de rayon des corps reéls quadratiques, tels que $H_{K_0^r}(m)$, peuvent être calculés efficacement en pratique, et nous citons les articles pertinents dans l'introduction du chapitre.

Afin de rendre la théorie ci-dessus vraiment explicite, nous avons mis en oeuvre la plupart des algorithmes discutés dans cette thèse.

L'algorithme pour calculer le groupe de classes de rayon de Shimura utilise des algorithmes pour calculer des noyaux, des images, des quotients et des extensions de groupes abéliens finiment engendrés et les morphismes entre eux. Ces algorithmes sont connus et se trouvent dans [6, Chapter 4]. Dans le Chapitre 5, nous reformulons ces algorithmes en détail en relevant soigneusement lesquelles des informations sont nécessaires pour calculer tel ou tel groupe.

À notre connaissance, ces algorithmes n'ont éte implantés en tant que fonction intégrée dans aucun logiciel de calcul formel. Par conséquent, nous avons mis en œuvre ces algorithmes et nous les avons rendus disponibles sous la forme de deux scripts PARI/GP [21] – `fgag.gp` et `fgagshimuray.gp`. Le premier script implant les algorithmes requis trouvés dans [6] et le second utilise le premier pour implanter l'algorithme qui calcule le groupe de classes de rayon de Shimura.

Nous utilisons notre code et d'autres fonctions intégrées à PARI/GP et SAGE pour montrer comment fonctionne notre méthode de construction de corps de classes. Au Chapitre 6, nous donnons explicitement des exemples utilisant notre algorithme issu de la théorie CM, nous comparons les performances de notre méthode par rapport aux algorithmiques génériques bien connus reposant sur la théorie de Kummer, et nous discutons les limites des deux approches.

Samenvatting

Titel: Constructie van abelse uitbreidingen van kwartische lichamen door complexe vermenigvuldiging

De stelling van Kronecker-Weber is een klassiek resultaat in de getaltheorie. Het doet een uitspraak over *abelse uitbreidingen*, Galoisuitbreidingen van een getallenlichaam met een abelse Galoisgroep.

> **Stelling van Kronecker-Weber.**
> Elke eindige abelse uitbreiding van $\mathbb{Q}$ is een deeluitbreiding van een cyclotomische uitbreiding $\mathbb{Q}(\zeta_m)$ met $\zeta_m = \exp(2\pi i/m)$ voor een $m \in \mathbb{Z}_{>0}$.
>
> De Galoisgroep $\mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})$ is isomorf met $(\mathbb{Z}/m\mathbb{Z})^\times$ via de afbeelding
>
> $$\begin{aligned}(\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q})\\ a + m\mathbb{Z} &\longmapsto (\zeta_m \mapsto \zeta_m^a).\end{aligned}$$

Deze stelling, gecombineerd met de Galoistheorie, vertelt ons dat elke abelse uitbreiding van $\mathbb{Q}$ kan worden uitgedrukt als $\mathbb{Q}(\boldsymbol{\alpha})$ waarbij $\boldsymbol{\alpha}$ een polynoom is in een m-de eenheidswortel voor een positief geheel getal m. De abelse uitbreiding

$$L = \mathbb{Q}[X]/(X^3 - 3X + 1)$$

bevindt zich bijvoorbeeld in het cyclotomische lichaam $\mathbb{Q}(\zeta_9)$. Het lichaam L is namelijk gelijk aan

$$\mathbb{Q}(\zeta_9 + \zeta_9^8).$$

Hoewel L ook bevat is in andere cyclotomische lichamen $\mathbb{Q}(\zeta_n)$ voor andere positieve gehele getallen n, is het gehele getal 9 het kleinste gehele getal dat aan deze voorwaarde voldoet.

Het twaalfde van de 23 problemen van Hilbert, ook bekend als Kronecker's Jugendtraum[1], vraagt om een analogon van de stelling van Kronecker-Weber te vinden wanneer het grondlichaam $\mathbb{Q}$ wordt vervangen door een ander getallenlichaam.

De Klassenlichamentheorie vertelt ons dat er voor elk getallenlichaam K en voor elk positief geheel getal m een bijectie bestaat tussen de verzameling ondergroepen van de zogenaamde straalklassengroep $\mathrm{Cl}_K(m)$ van K en de verzameling abelse uitbreidingen L/K van conductor[2] die m deelt. Echter, gegeven een ondergroep van $\mathrm{Cl}_K(m)$, geeft de corresponderende bijectie niet noodzakelijkerwijs een expliciete beschrijving van de abelse uitbreiding.

Niet alle hoop is verloren aangezien er een geval bestaat waarvoor een expliciete analogon van de **Stelling van Kronecker-Weber** bekend is. Dit is het geval wanneer het grondlichaam K een imaginair kwadratisch getallenlichaam is, in plaats van de $\mathbb{Q}$ van Kronecker-Weber. De theorie van complexe vermenigvuldiging (CM-theorie) (Paragraaf 1.2) voor elliptische krommen levert deze analoog. Met behulp van de CM-theorie kan men definiërende polynomen vinden van elke abelse uitbreiding van elk imaginair kwadratisch lichaam K.

Shimura en Taniyama ontwikkelden in de jaren vijftig een veralgemening van de CM-theorie naar hoger dimensionale, hoofdgepolariseerde abelse variëteiten. Net als haar tegenhanger binnen de theorie van elliptische krommen, beschrijft de theorie expliciet abelse uitbreidingen van zogenaamde CM-lichamen in termen van speciale waarden van modulaire functies. De theorie dekt echter niet *alle* abelse uitbreidingen van een CM-lichaam en geeft daarom op zichzelf geen analoog van de stelling van Kronecker-Weber.

In dit proefschrift, laten we echter zien dat we Shimura's CM-theorie kunnen gebruiken om expliciet de grootste onvertakte[3] abelse uitbreiding, het Hilbert-klassenlichaam genoemd, van *elk* primitief vierdegraads CM-lichaam te vinden. Met dit proefschrift hopen we verder onderzoek te stimuleren naar het gebruik van CM-theorie om onderzoek naar abelse uitbreidingen te bevorderen.

Dit proefschrift is onderverdeeld in de volgende hoofdstukken.

[1] Kroneckers jeugddroom
[2] Zie de definitie van conductor op pagina 22
[3] Een abelse uitbreiding is onvertakt als en slechts dan als de conductor 1 is.

In Hoofdstuk 1 bekijken we hoe de CM-theorie wordt gebruikt om alle abelse uitbreidingen van een imaginair kwadratisch getallenlichaam te vinden. In Hoofdstuk 2, bespreken we de algemenere CM-theorie.

Een aanpassing van [30, Theorem 2] van Shimura laat zien dat er een positief geheel getal m bestaat waarvoor het Hilbert-klassenlichaam $H_{K^r}(1)$ van een primitief vierdegraads CM-lichaam K^r met reëel kwadratische deellichaam K_0^r zich in de compositum Ξ_m van het straalklassenlichaam $H_{K_0^r}(m)$ van K_0^r en een abelse uitbreiding

$$\mathrm{CM}_{K^r,\Phi^r}(m)$$

van K^r (gedefinieerd in Paragraaf 2.1.3, gegeven door CM-theorie) bevindt.

In Hoofdstuk 3 doen we verschillende dingen die verband houden met dit resultaat van Shimura. Om te beginnen geven we een stelling die ons een geheel getal m geeft waarvoor het resultaat van Shimura waar is. Vervolgens definiëren we, voor elk positief geheel getal m, de Shimura-straalklassengroep $\mathfrak{C}_K(m)$ van een CM-lichaam K gerelateerd aan K^r. Met behulp van deze Shimura-straalklassengroep geven we een algoritme dat een positief geheel getal m' als invoer neemt en teruggeeft of het Hilbert-klassenlichaam al dan niet is opgenomen in $\Xi_{m'}$. Dit algoritme stelt ons in staat om het kleinste positieve gehele getal m te vinden waarvoor het resultaat van Shimura waar is.

Het bovengenoemde resultaat van Shimura is nuttig voor rekenkundige doeleinden omdat beide delen van het compositum expliciet kunnen worden berekend. In Hoofdstuk 4 laten we zien hoe de abelse uitbreiding $\mathrm{CM}_{K^r,\Phi^r}(m)$ berekend kan worden. Straalklassenlichamen van reëel kwadratische lichamen, zoals $H_{K_0^r}(m)$, kunnen in de praktijk efficiënt worden berekend en we citeren de relevante artikelen in de inleiding van het hoofdstuk.

Om de bovenstaande theorie echt expliciet te maken, hebben we de meeste van de in dit proefschrift besproken algoritmen geïmplementeerd.

Het algoritme voor het berekenen van de Shimura-straalklassengroep maakt gebruik van algoritmen voor het berekenen van kernen, affbeeldingen, quotiënten en groepsuitbreidingen met eindig voortgebrachte abelse groepen en homomorfismen daartussen. Deze algoritmen zijn bekend en kunnen worden gevonden in [6, Chapter 4].

In Hoofdstuk 5 herhalen we deze algoritmen in detail, waarbij we zorgvuldig noteren welke informatie nodig is om welke groepen te berekenen.

Voor zover wij weten, zijn deze algoritmen niet geïmplementeerd in een computer-algebrasysteem op een manier die ze beschikbaar maakt voor de gebruiker. Daarom hebben we deze algoritmen geïmplementeerd en beschikbaar gemaakt als een paar PARI/GP [21] scripts – `fgag.gp` en `fgagshimuray.gp`. De eerste implementeert de vereiste algoritmen uit [6] en de laatste gebruikt de eerste om het algoritme te implementeren dat de Shimura-straalklassengroep berekent.

We gebruiken onze code en andere ingebouwde functies van PARI/GP [21] en SAGE [27] om te laten zien hoe onze methode voor het construeren van een CM-lichaam werkt. In Hoofdstuk 6 geven we expliciete voorbeelden met behulp van ons CM-theorie-algoritme, vergelijken we hoe onze methode presteert ten opzichte van de bekende generieke Kummer-theorie-algoritme en bespreken we de beperkingen van beide benaderingen.

1 Class field theory and elliptic curves

In this preliminary chapter, we review class field theory (Section 1.1). After that, we discuss the only currently known explicit analogue of the Kronecker-Weber Theorem, the Main Theorem of CM for elliptic curves (Section 1.2).

1.1 Class field theory

We begin this section with a discussion of *the Artin homomorphism*, a map which relates two a priori unrelated objects – ideals and Galois groups.

Let $\mathfrak{p}$ be an unramified prime ideal of an abelian extension L/K. There exists a unique automorphism $\mathrm{Frob}_{\mathfrak{p}}$ of L/K which induces, for each prime ideal $\mathfrak{P}$ of L above $\mathfrak{p}$, an automorphism $x \mapsto x^{N(\mathfrak{p})}$ of the residue class field $\mathcal{O}_L/\mathfrak{P}$, see [36, Chapter 1, Corollary 2 of Theorem 7] or [10, Lemma C.5.19]. The *Artin homomorphism* of L/K is a homomorphism defined on the group $I_K(\Delta_{L/K})$, the group of fractional ideals coprime to the discriminant $\Delta_{L/K}$ of L/K, defined as follows:

$$\begin{aligned} \Psi_{L/K} : I_K(\Delta_{L/K}) &\longrightarrow \mathrm{Gal}(L/K) \\ \mathfrak{p} &\longmapsto \mathrm{Frob}_{\mathfrak{p}} \end{aligned}$$

Example 1.1. Consider the cyclotomic extension $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ for some odd integer $m \in \mathbb{Z}_{>0}$. The fractional ideals of $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$ are all principal, generated by elements of $\mathbb{Q}$. When m is odd, the prime factors of $\Delta_{\mathbb{Q}(\zeta_m/\mathbb{Q})}$ are exactly the prime factors of m. And so $I_K(\Delta_{L/K})$ is the set of fractional ideals of $\mathbb{Z}$

coprime to m. A fractional ideal in $I_{\mathbb{Q}}(\Delta_{\mathbb{Q}(\zeta_m/\mathbb{Q})})$ can be expressed as $b^{-1}a\mathbb{Z}$ where $a, b \in \mathbb{Z}$ are coprime to m. We have $\Psi_{\mathbb{Q}(\zeta_m)/\mathbb{Q}}(b^{-1}a\mathbb{Z}) = (\zeta_m \mapsto \zeta_m^{ac})$ where $cb \equiv 1 \bmod m$.

A *modulus of a number field* K is a pair $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ where $\mathfrak{m}_0$ is a nonzero ideal of $\mathcal{O}_K$ and $\mathfrak{m}_\infty$ is a subset of the real embeddings of K.

Let $\mathfrak{m} = (\mathfrak{m}_0, \mathfrak{m}_\infty)$ be a modulus of K. Let $x \in K^\times$. Write $x = a/b$ where $a, b \in \mathcal{O}_K$ and $b \neq 0$. We write $x \equiv 1 \bmod^* \mathfrak{m}$ to mean that $a \equiv b \bmod \mathfrak{m}_0$, and $\sigma(x) > 0$ for every $\sigma \in \mathfrak{m}_\infty$.

We define the *principal ray group of a number field K for the modulus* $\mathfrak{m}$ as follows:

$$P_K(\mathfrak{m}) = \{x\mathcal{O}_K : x \in K^\times, x \equiv 1 \bmod^* \mathfrak{m}\} \tag{1.2}$$

A modulus $\mathfrak{m}$ satisfying $P_K(\mathfrak{m}) \subseteq \ker \Psi_{L/K}$ is said to be an *admissible modulus for the abelian extension L/K*. By [18, Remark 3.8], there is a unique division-minimal admissible modulus for L/K. We call the minimal admissible modulus the *conductor* of L/K and we denote it by $\mathfrak{f}_{L/K}$.

Writing $I_K(\mathfrak{m})$ for the *group of fractional ideals of K coprime to* $\mathfrak{m}$, we find that for every admissible modulus $\mathfrak{m}$ of an abelian extension L/K, the Artin homomorphism induces the homomorphism

$$\begin{aligned} \Psi_{L/K}^{(\mathfrak{m})} : I_K(\mathfrak{m})/P_K(\mathfrak{m}) &\to \mathrm{Gal}(L/K) \\ \mathfrak{p} &\mapsto \mathrm{Frob}_{\mathfrak{p}}. \end{aligned} \tag{1.3}$$

We call the quotient $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ the *ray class group of K for the modulus* $\mathfrak{m}$ and henceforth denote it by $\mathrm{Cl}_K(\mathfrak{m})$.

Example 1.4. All ideals of $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ are principal hence all fractional ideals are, too. Hence, the class group $\mathrm{Cl}_{\mathbb{Q}}(1)$ is trivial.

Example 1.5. An ideal of $\mathbb{Z} = \mathcal{O}_{\mathbb{Q}}$ coprime to $4\mathbb{Z}$ is a principal ideal of the form $x\mathbb{Z}$ for some $x \equiv \pm 1 \bmod 4$. Since $x\mathbb{Z} = -x\mathbb{Z}$ for any integer x, we find that $\mathrm{Cl}_K(4\mathbb{Z}, \varnothing)$ is trivial. On the other hand, one can show that the group $\mathrm{Cl}_K(4\mathbb{Z}, \{\sigma\})$, where σ is the sole embedding of $\mathbb{Q}$ into $\mathbb{R}$, is a group of order 2.

The map $\Psi_{L/K}^{(\mathfrak{m})}$ is surjective ([10, Theorem C.5.23]). Moreover, for each modulus $\mathfrak{m}$ of K, the *Takagi existence theorem* [6, Theorem 3.5.1] asserts that there exists an abelian extension L of K for which $\Psi_{L/K}^{(\mathfrak{m})}$ is injective. And so, we have:

Theorem 1.6. For any modulus $\mathfrak{m}$ of a number field K, there exists an abelian extension $H_K(\mathfrak{m})$ of K such that $\Psi_{H_K(\mathfrak{m})/K}^{(\mathfrak{m})}$ is an isomorphism.

This abelian extension $H_K(\mathfrak{m})$ is called the *ray class field of K for the modulus* $\mathfrak{m}$. If L/K is an abelian extension of conductor $\mathfrak{f}_{L/K}$, then it is contained in $H_K(\mathfrak{f}_{L/K})$. Hence, we have the following result:

Theorem 1.7. Every abelian extension L of a number field K is contained in (at least) one of its ray class fields. In particular, it is contained in $H_K(\mathfrak{f}_{L/K})$.

The *Hilbert class field of K* is the ray class field of K for the modulus 1. It is the largest unramified abelian extension of K.

Example 1.8. The ideal class group $\mathrm{Cl}_{\mathbb{Q}}(1)$ of $\mathbb{Q}$ is trivial (Example 1.4). Hence, we have $H_{\mathbb{Q}}(1) = \mathbb{Q}$. Moreover, aside from itself, the number field $\mathbb{Q}$ has no other unramified abelian extensions.

1.2 Complex multiplication theory for elliptic curves

The first part of CM theory expresses the Hilbert class field of an imaginary quadratic number field K in terms of the field of moduli $\mathcal{M}(E)$ (Section 1.2.2) of an elliptic curve E whose endomorphism ring (Section 1.2.1) is isomorphic to $\mathcal{O}_K$. The second

part of CM theory asserts that appending a 'normalized' x-coordinate of a primitive m-torsion point (Section 1.2.3) to $\mathcal{M}(E)$ gives the ray class field of K for the modulus m. Associated to a complex elliptic curve E is a lattice Λ such that E is isomorphic to the complex torus $\mathbb{C}/\Lambda$ (Section 1.2.4). This isomorphism is key to computing defining polynomials of the ray class fields of K.

1.2.1 Elliptic curves and their endomorphism rings

An *elliptic curve over a field* k is a smooth projective curve of genus 1 with a distinguished k-rational point O. If $\operatorname{char} k \neq 2, 3$, then an elliptic curve over k has an affine model of the form

$$y^2 = x^3 + Ax + B \tag{1.9}$$

where $A, B \in k$ whose distinguished point O is its unique point at infinity. In this case, we denote O by ∞. Such an affine model is called *a Weierstrass form of* E. The points of an elliptic curve E form an abelian group [32, Chapter III.2] whose identity element is its distinguished point O.

Endomorphisms of an elliptic curve E are (group variety) homomorphisms of E onto itself. The endomorphisms of an elliptic curve form a ring $\operatorname{End}_{\bar{k}} E$ in which addition is point-wise and multiplication is composition.

As the points of E form an algebraic abelian group, for every integer m, the *multiplication-by-m map*

$$\begin{aligned} [\boldsymbol{m}] : E &\to E \\ P &\to mP \end{aligned}$$

is an endomorphism of E. Moreover, these endomorphisms are defined over k.

We can embed the ring $\mathbb{Z}$ of integers into the ring $\operatorname{End}_{\bar{k}} E$ of endomorphisms of E via $m \mapsto [\boldsymbol{m}]$. For example, the unit $-1 \in \mathbb{Z}$ is mapped to the endomorphism

$$\begin{aligned} [\boldsymbol{-1}] : E &\to E \\ (x, y) &\to (x, -y) \end{aligned}$$

for any elliptic curve E in Weierstrass form. Aside from endomorphisms of the form $[\boldsymbol{m}]$, an elliptic curve may have other endomorphisms. Here is one example.

Example 1.10. The elliptic curve over $k \subseteq \mathbb{C}$ with affine model $E : y^2 = x^3 + x$ has

$$\begin{aligned} [\boldsymbol{i}] : E &\to E \\ (x, y) &\to (-x, iy) \end{aligned}$$

as an element of its endomorphism ring. It satisfies $[\boldsymbol{i}]^2 = [-1]$. One can prove that the embedding $\mathrm{End}_{\bar{k}} E$ is in fact isomorphic to the ring of integers $\mathbb{Z}[i]$ of the imaginary quadratic number field $\mathbb{Q}(i)$.

More generally, the $\bar{k}$-endomorphism ring $\mathrm{End}_{\bar{k}}$ of an elliptic curve E over a field $k \subseteq \mathbb{C}$ is isomorphic to

E1 the ring of integers $\mathbb{Z}$, or

E2 an order $\mathcal{O}$ of an imaginary quadratic number field,

by [32, Corollary III.9.4].

When $\mathrm{End}_{\bar{k}} E$ satisfies **E2**, the elliptic curve E is said to have complex multiplication by $\mathcal{O}$. An elliptic curve E over $k \subseteq \mathbb{C}$ is said to have *complex multiplication by a number field* K if there exists an embedding $\iota : K \hookrightarrow \mathrm{End}_{\bar{k}} E \otimes \mathbb{Q}$ such that $\iota^{-1}(\mathrm{End}_{\bar{k}} E) = \mathcal{O}_K$, the maximal order $\mathcal{O}_K$ of K.

An *automorphism* of an elliptic curve is simply an invertible endomorphism. The automorphisms over $\bar{k}$ of an elliptic curve E over $k \subseteq \mathbb{C}$ form a group under composition and we denote it by $\mathrm{Aut}_{\bar{k}} E$. In the following example, we investigate all the possible automorphism groups $\mathrm{Aut}_{\bar{k}} E$ of an elliptic curve with complex multiplication by an imaginary quadratic number field K.

Example 1.11. We determine the automorphism group of elliptic curves over $k \subseteq \mathbb{C}$ with complex multiplication by an imaginary quadratic number field K.

1. The ring of integers of $\mathbb{Q}(i)$ is $\mathbb{Z}[i]$. Its unit group $\mathbb{Z}[i]^\times$, generated by i, is a cyclic group of order 4. Hence, the group $\mathrm{Aut}_{\bar{k}}\, E$ of E with complex multiplication by $\mathbb{Q}(i)$ is a cyclic group of order 4 generated by $[i]$ (defined in Example 1.10).

2. The ring of integers of $\mathbb{Q}(\zeta_3)$ is $\mathbb{Z}\,[\zeta_3 + 1]$. Its unit group is a cyclic group of order 6. Hence, the group $\mathrm{Aut}_{\bar{k}}\, E$ of E with complex multiplication by $\mathbb{Q}(\zeta_3)$ is a cyclic group of order 6.

3. The unit group of the ring of integers of an imaginary quadratic number field $K \neq \mathbb{Q}(i), \mathbb{Q}(\zeta_3)$ is $\langle -1 \rangle$. This means that the group $\mathrm{Aut}_{\bar{k}}\, E$ of an elliptic curve E with complex multiplication by K is generated by $[-1]$ and cyclic of order 2.

1.2.2 Fields of moduli of elliptic curves

A map $\phi : E_1 \longrightarrow E_2$ of elliptic curves E_1, E_2 defined over k is said to be an *isomorphism* if ϕ is an isomorphism of varieties such that $\phi(\infty_1) = \infty_2$ where ∞_i is the identity element of E_i for $i \in \{1, 2\}$.

For an elliptic curve E over a field $k \subseteq \mathbb{C}$ given by (1.9), we define its j-invariant as

$$j(E) = 1728\,\frac{4A^3}{4A^3 + 27B^2}. \tag{1.12}$$

Example 1.13. Using (1.12), we easily find that the j-invariant of the elliptic curve $E : y^2 = x^3 + x$, in Example 1.10 is 1728.

The j-invariant of an elliptic curve determines its isomorphism class over $\mathbb{C}$. More particularly, two elliptic curves E_1 and E_2 over $k \subseteq \mathbb{C}$ are isomorphic over $\bar{k}$ if and only if their j-invariants are equal [32, Proposition III.1.4].

The *field of moduli of an elliptic curve* E defined over a field $k \subseteq \mathbb{C}$ is a field $\mathcal{M}(E)$ which satisfies

$\sigma \in \mathrm{Aut}(\mathbb{C})$ is the identity on $\mathcal{M}(E)$ if and only if there exists an isomorphism $\phi : E \longrightarrow E^\sigma$ of elliptic curves over $\bar{k}$

where E^σ denotes the elliptic curve defined by the equation

$$E^\sigma : y^2 = x^3 + A^\sigma x + B^\sigma.$$

Example 1.14. The field of moduli $\mathcal{M}(E)$ of an elliptic curve E is unique. In particular,

$$\mathcal{M}(E) = \mathbb{Q}(j(E)).$$

Proof. Supose $\sigma \in \operatorname{Aut}\mathbb{C}$ fixes $\mathcal{M}(E)$. Then there exists an isomorphism $\phi : E \to E^\sigma$. Hence, $j(E) = j(E^\sigma)$. Moreover, $j(E^\sigma) = j(E)^\sigma$. Hence, $j(E) = j(E)^\sigma$. Thus, σ fixes $j(E)$ and $\mathbb{Q}(j(E) \subseteq \mathcal{M}(E)$.

Suppose $\sigma \in \operatorname{Aut}\mathbb{C}$ fixes $j(E)$. That is, $j(E) = j(E)^\sigma$. We know that $j(E)^\sigma = j(E^\sigma)$. We have shown that $j(E) = j(E^\sigma)$. Hence, there exists a $\bar{k}$-isomorphism $\phi : E \to E^\sigma$. Thus, σ fixes $\mathcal{M}(E)$. □

The first main theorem of complex multiplication on elliptic curves gives us the following result:

Theorem 1.15 (First Main Theorem of Complex Multiplication for Elliptic Curves)**.** The Hilbert class field $H_K(1)$ of an imaginary quadratic number field K is the field $K(j(E)) = K\mathcal{M}(E)$, where E is an elliptic curve E with complex multiplication by K.

Proof. [8, Proof of Theorem 6.9] □

1.2.3 Torsion points of elliptic curves

Suppose that E is an elliptic curve with complex multiplication by an imaginary quadratic number field K, with $\iota : \mathcal{O}_K \to \operatorname{End}_{\bar{k}} E$ as the isomorphism between $\mathcal{O}_K$ and $\operatorname{End}_{\bar{k}} E$.

Since $\mathcal{O}_K$ is a Dedekind domain, an ideal $\mathfrak{m}$ of $\mathcal{O}_K$ is generated by two elements of $\mathcal{O}_K$, say α and β. We define the $\mathfrak{m}$-*torsion subgroup* $E[\mathfrak{m}]$ *of* E to be the intersection of the kernels of $\iota(\alpha)$ and $\iota(\beta)$.

Suppose that E' is a complex elliptic curve with complex multiplication by an imaginary quadratic number field K. There exists an elliptic curve E, over the field of moduli $\mathbb{Q}(j(E'))$ of E', that is $\bar{k}$-isomorphic to E' with a short Weierstrass model. Take $n = \frac{1}{2}|\mathcal{O}_K^\times|$. The map

$$\begin{aligned} x^n : E(\mathbb{C}) &\to \mathbb{C} \\ (x, y) &\mapsto x^n \\ \infty &\mapsto 1 \end{aligned} \tag{1.16}$$

satisfies the condition:

$$\forall P, Q \in E: \quad x^n(P) = x^n(Q) \iff Q = gP \text{ for some } g \in \operatorname{Aut} E. \tag{1.17}$$

Akin to how the Kronecker-Weber Theorem describes the ray class fields of $\mathbb{Q}$ in terms of torsion points of the circle group, the second main theorem of complex multiplication describes the ray class fields of imaginary quadratic number fields in terms of torsion points of elliptic curves:

Theorem 1.18 (Second Main Theorem of Complex Multiplication for Elliptic Curves)**.** The ray class field $H_K(\mathfrak{m})$ of an imaginary quadratic number field K for the modulus $\mathfrak{m}$ of K is the field $H_K(1)(x^n(E[\mathfrak{m}]))$, where

- E is an elliptic curve over $\mathbb{Q}(j(E))$ with complex multiplication by K over $\bar{\mathbb{Q}}$,
- $n = \frac{1}{2}|\mathcal{O}_K^\times|$, and
- x^n is as given in (1.16).

Proof. [8, Proof of Theorem 6.15] □

1.2.4 Elliptic curves as complex tori

The Weierstrass $\wp$-function of a lattice Λ, defined by

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{w \in \Lambda \setminus \{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right),$$

is a meromorphic function whose poles are exactly at the lattice points of Λ [10, Theorem 10.1.i]. For any $\lambda \in \mathbb{C}^\times$, the Weierstrass $\wp$-function satisfies

$$\wp_{\lambda\Lambda}(\lambda z) = \lambda^{-2}\wp_\Lambda(z). \tag{1.19}$$

The $\wp$ function satisfies [10, Theorem 10.1.ii] the differential equation

$$(f')^2 = 4f^3 - g_2(\Lambda)f - g_3(\Lambda) \tag{1.20}$$

where

$$g_2(\Lambda) = 60 \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{w^4}$$
$$g_3(\Lambda) = 140 \sum_{w\in\Lambda\setminus\{0\}} \frac{1}{w^6}.$$

The maps g_2, g_3 satisfy the following property for $\lambda \in \mathbb{C}^\times$:

$$g_k(\lambda z) = \lambda^{-2k} g_k(z), \qquad k \in \{2, 3\}. \tag{1.21}$$

One might notice that (1.20) suspiciously resembles (1.9). In fact, the image of the map $\theta : \mathbb{C} \to \mathbb{P}^2$ given by $z \mapsto (\wp_\Lambda(z) : \wp'_\Lambda(z) : 1)$ defines an elliptic curve E_Λ over $\mathbb{C}$ with an affine equation

$$E_\Lambda : y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda) \tag{1.22}$$

and it sends elements of Λ to the point ∞ at infinity, the identity element of E_Λ. Note that

$$E'_\Lambda : y^2 = x^3 - \frac{1}{4}g_2(\Lambda)x - \frac{1}{4}g_3(\Lambda)$$

is an elliptic curve with a short Weierstrass form and is $\mathbb{C}$-isomorphic to E_Λ. The isomorphism is given by the map $(x, y) \mapsto \left(x, \frac{y}{2}\right)$ from E_Λ to E'_Λ.

We define the j-invariant of a lattice as follows:

$$j(\Lambda) := j(E_\Lambda) = j(E'_\Lambda) = 1728\frac{g_2^3(\Lambda)}{g_2^3(\Lambda) - 27\,g_3^2(\Lambda)}. \tag{1.23}$$

The map θ defines an isomorphism

$$\begin{aligned} \theta_\Lambda : \mathbb{C}/\Lambda &\to E_\Lambda \\ z &\mapsto (\wp_\Lambda(z),\ \wp'_\Lambda(z)) \end{aligned} \tag{1.24}$$

between the complex torus $\mathbb{C}/\Lambda$ and the elliptic curve E_Λ. In addition, we have the following result:

> **Theorem 1.25** ([32, Corollary VI.5.1.1])**.** For any complex elliptic curve E, there exists a lattice Λ such that $E \cong E_\Lambda$.

Hence, every complex elliptic curve is isomorphic to a complex torus.

One can show that E_Λ has complex multiplication if and only if $\Lambda = \alpha(\mathbb{Z} + \tau\mathbb{Z})$ for some $\alpha \in \mathbb{C}^\times$ where $\tau \in \mathbb{C} \setminus \mathbb{R}$ is a zero of an irreducible polynomial $ax^2 + bx + c \in \mathbb{Z}[x]$. When Λ is of such a form and $D := b^2 - 4ac$ satisfies one of the following:

1. $D = 4m$ where $m \equiv 2, 3 \bmod 4$ and m is square-free,

2. $D \equiv 1 \bmod 4$, and is square-free,

the elliptic curve E_Λ has complex multiplication by the imaginary quadratic number field $\mathbb{Q}(\sqrt{D})$.

We are now ready to prove the following result, giving a way to compute ray class fields of imaginary quadratic number fields.

> **Theorem 1.26.** The ray class field $H_K(n)$ of an imaginary quadratic number field $K \neq \mathbb{Q}(i), \mathbb{Q}(\zeta_3)$ for a positive integer n is
>
> $$H_K\left(j(\Lambda),\ (g_3(\Lambda)/g_2(\Lambda))\wp_\Lambda(z) : z \in T_n \right)$$
>
> where
>
> - $\Lambda = \tau\mathbb{Z} + \mathbb{Z}$ where τ satisfies $\mathcal{O}_K = \mathbb{Z}[\tau]$, and
> - $T_n = \{(a\tau + b)/n \ :\ a, b \in \{0, \ldots, n-1\}\}$.

Proof. Define

$$c = 27 \cdot \frac{j(\Lambda)}{j(\Lambda) - 1728} \in \mathbb{Q}(j(E)). \tag{1.27}$$

Note that c is a non-zero complex number since $j(\Lambda) \neq 0, 1728$. Moreover, this constant c satisfies

$$\lambda^{-4} g_2(\Lambda) = \lambda^{-6} g_3(\Lambda) = c \in \mathbb{Q}(j(E)) \tag{1.28}$$

where $\lambda = \sqrt{g_3(\Lambda)/g_2(\Lambda)}$. Using (1.21), we find that

$$g_2(\lambda\Lambda) = \lambda^{-4} g_2(\Lambda), \text{and} \qquad g_3(\lambda\Lambda) = \lambda^{-6} g_3(\Lambda).$$

Therefore, the elliptic curve

$$E_{\lambda\Lambda} : y^2 = 4x^3 - cx - c = 4x^3 - g_2(\lambda\Lambda)x - g_3(\lambda\Lambda)$$

is defined over $\mathbb{Q}(j(E))$. We can define an isomorphism of elliptic curves as follows:

$$\begin{aligned} \phi_{\Lambda,\lambda} : E_\Lambda &\to E_{\lambda\Lambda} \\ (x, y) &\mapsto (\lambda^2 x,\ \lambda^3 y). \end{aligned}$$

Hence, the composite map $\phi_{\Lambda,\lambda} \circ \theta_\Lambda$ given by

$$z \mapsto (\lambda^2 \wp_\Lambda(z), \lambda^4 \wp_\Lambda(z))$$

is an isomorphism between $\mathbb{C}/\Lambda$ and $E_{\lambda\Lambda}$. Hence,

$$x^1(E[n]) = \lambda^2 \wp_\Lambda(T_n)$$

for any positive integer n. Applying (1.18), we get the result. □

Let

$$\Delta(\Lambda) := g_2(\Lambda)^3 - 27 g_3(\Lambda)^2.$$

We have a better-known version of the above result. This version expresses the ray

class field in terms of the *Weber function* $h_\Lambda(z)$:

$$h_\Lambda(z) = \begin{cases} \frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z) & \text{if } j(\Lambda) \neq 0, 1728, \\ \frac{g_2(\Lambda)^2}{\Delta(\Lambda)}\wp_\Lambda(z)^2 & \text{if } j(\Lambda) = 1728, \\ \frac{g_3(\Lambda)}{\Delta(\Lambda)}\wp_\Lambda(z)^3 & \text{if } j(\Lambda) = 0. \end{cases}$$

This piecewise function satisfies the following:

Theorem 1.29. The ray class field $H_K(n)$ of an imaginary quadratic number field K for the positive integer n is

$$H_K(j(\Lambda), h_\Lambda(z) : z \in T_n)$$

where Λ and T_n are as in Theorem 1.26.

Proof. The case where $j \neq 0, 1728$ is proved by replacing λ with

$$\lambda_1 = \sqrt{\frac{g_2(\Lambda)g_3(\Lambda)}{\Delta(\Lambda)}}$$

in the proof of Theorem 1.26. This results in an elliptic curve

$$E_{\lambda_1\Lambda} : y^2 = x^3 - \frac{c}{(c-27)^2}x - \frac{c}{(c-27)^3}, \quad \text{where } c \text{ is as in (1.27)},$$

over $\mathbb{Q}(j(\Lambda))$. The rest of the proof for this case is the same as in Theorem 1.26.

Now we do the case where $j(\Lambda) = 1728$. First, notice that $g_3(\Lambda) = 0$ in this case. Indeed, using (1.23), we have

$$g_2^3(\Lambda) = g_2^3(\Lambda) - 27\, g_3^2(\Lambda)$$

which implies $g_3^2(\Lambda) = 0$. Taking

$$\lambda_2 = \sqrt[4]{\frac{g_2(\Lambda)^2}{\Delta(\Lambda)}} = g_2(\Lambda)^{-1/4},$$

we get the elliptic curve

$$E_{\lambda_2\Lambda} : y^2 = 4x^3 - g_2(\lambda_2^{-1}\,\Lambda)\,x = 4x^3 - \lambda_2^4\, g_2(\Lambda)\,x = 4x^3 - x$$

over $\mathbb{Q} = \mathbb{Q}(j)$. The squares of the x-coordinates of the n-torsion points of the elliptic curve E are given by $\wp_{\lambda_2^{-1}\Lambda}(\lambda_2^{-1}z)^2$ where $z \in T_n$, which is equal to $\lambda^4\wp_\Lambda(z)^2$ using (1.19). Using (1.18), we get the result of the theorem.

The case where $j(\Lambda) = 0$ proceeds as in the case $j(\Lambda) = 1728$ by first noticing $g_2(\Lambda) = 0$ and then replacing λ_2 by

$$\lambda_3 = \sqrt[6]{\frac{g_3(\Lambda)}{\Delta(\Lambda)}} = (-27 \cdot g_3(\Lambda))^{-1/6},$$

and using the elliptic curve

$$E_{\lambda_3\Lambda} : y^2 = 4x^3 - g_3(\lambda_3^{-1}\,\Lambda) = 4x^3 - \lambda_3^{-6}\,g_3(\Lambda) = 4x^3 - 27$$

over $\mathbb{Q} = \mathbb{Q}(j)$. □

2 CM theory on principally polarized abelian varieties

Shimura and Taniyama [31] showed that CM theory can be generalized to a certain family of fields called *CM fields*. Specializing their results to imaginary quadratic number fields lets us recover the main theorems of complex multiplication for elliptic curves, discussed in Chapter 1.

In Section 2.1, we review what CM fields are and discuss objects related to them. We also define in this section one main object of interest of this thesis – primitive quartic CM fields. Specializing Shimura-Taniyama's more general CM theory, we get that abelian extensions of primitive quartic CM fields can be obtained in terms of invariants and torsion points of Jacobians of genus 2 hyperelliptic curves. We review the theory surrounding these Jacobians in Section 2.2. In Section 2.2.6, we state the main theorems of complex multiplication for principally polarized abelian surfaces. As this thesis is not only interested in the theoretical aspects of CM theory, but also in the computational aspects, we review theta functions in Section 2.3. These functions are the building blocks that we need in order to construct the analogue of the Weber function later in Chapter 4.

2.1 CM fields

A *CM field* is a totally imaginary quadratic extension of a totally real number field K_0. That is, a CM field K is a field of the form $K = K_0(\sqrt{\delta})$ where $\sigma(\delta) < 0$ for every embedding $\sigma : K_0 \hookrightarrow \mathbb{R}$. The *degree of a CM field* is its degree as a number field.

> **Example 2.1.** The CM fields of degree 2 are exactly the imaginary quadratic number fields.

As K/K_0 is a quadratic extension, it is Galois. We denote the generator of its Galois group by ρ. For every embedding $\sigma : K \hookrightarrow \mathbb{C}$, we have $\sigma(\rho(x)) = \overline{\sigma(x)}$. It is for this reason that we will refer to the map ρ as the *complex conjugation automorphism*.

2.1.1 The type norm

Let $\boldsymbol{\sigma}$ be the set of $2g$ complex embeddings of a CM field K of degree $2g$. As K is a number field, it has a *norm map* $N_{K/\mathbb{Q}}$

$$N_{K/\mathbb{Q}}(x) = \prod_{\sigma \in \boldsymbol{\sigma}} \sigma(x), \qquad \text{for } x \in K$$

whose image is contained in $\mathbb{Q}$.

With CM fields, one can define a norm-like map called the type norm. This map is used in Section 2.1.3 to define a field which turns out to be the field of moduli of simple principally polarized abelian surfaces.

The type norm depends on the choice of a CM type. A subset Φ of $\boldsymbol{\sigma}$ containing g complex embeddings, no two of which are complex conjugates of each other, is called a *CM type of* K. Assume $K \subseteq \mathbb{C}$. Denote by $L \subseteq \mathbb{C}$ the Galois closure of K. In this case, CM types Φ of K may be viewed as a set of g embeddings of K into L, as opposed to $\mathbb{C}$.

The *type norm map* N_Φ of a CM type Φ of a CM field K is defined to be the map

$$N_\Phi(x) = \prod_{\phi \in \Phi} \phi(x), \qquad \text{for } x \in K.$$

The type norm sends an element $x \in K$ to an element in the Galois closure L. In fact, the image of this type norm is contained in a CM subfield of L called the *reflex field*, which we define in the following section, Section 2.1.2.

2.1.2 The reflex field

Suppose that K is a CM field with Galois closure L and that K' is a CM subfield[1] of K. Let Φ' be a CM type of K'. We define the *CM type induced by* Φ' *on the field* K to be

$$\Phi = \{\phi : K \hookrightarrow L \,:\, \phi|_{K'} \in \Phi'\}.$$

A CM type of K is said to be *primitive* if it is not induced by a CM type of a strict CM subfield of K.

Two CM types Φ, Φ' of the same CM field K are said to be *equivalent* if there is an automorphism σ of K such that $\Phi' = \Phi \circ \sigma$ holds.

A *CM pair* is a pair (K, Φ), where K is a CM field and Φ is a CM type of K. If the CM type Φ is primitive, we say that it is a *primitive CM pair*.

Suppose (K, Φ) is a CM pair and denote by Φ_L the CM type of the Galois closure L induced by Φ. The elements of Φ_L are automorphisms of L and so we can talk about the set

$$\Phi_L^{-1} = \{\phi^{-1} : \phi \in \Phi_L\}.$$

This set Φ_L^{-1} is a CM type of L. There exists a unique subfield K^r of L and a unique primitive CM type Φ^r that induces Φ_L^{-1} (see [16, Lemma 2.2]). This CM pair (K^r, Φ^r) is called the *reflex (pair) of* (K, Φ). We call the field K^r the *reflex field of* (K, Φ).

Let K be a quartic CM field with Galois closure L. When the Galois group $\mathrm{Gal}(L/\mathbb{Q})$ is not bicyclic, all of its CM types are primitive [31, Example 8.4(2)]. In this case, we call K a *primitive quartic CM field* and call (K, Φ) a *primitive quartic (CM) pair*.

Theorem 2.2. The reflex field K^r satisfies

$$\mathrm{Gal}(L/K^r) = \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) : \sigma\Phi = \Phi\}. \tag{2.3}$$

Proof. This is [34, Lemma 7.3]. □

From the theorem, we immediately see that the image of the type norm N_Φ of a CM type Φ is in fact contained in its reflex field K^r. Therefore, we can and we will consider the type norm N_Φ as a map from K to K^r.

[1] A CM subfield is a subfield which is also a CM field.

When Φ is a primitive CM type of K, the reflex pair (K^{rr}, Φ^{rr}) of (K^r, Φ^r) is actually equal to (K, Φ) itself [34, Lemma 7.2]. Therefore, we may define the type norm N_{Φ^r} of Φ^r as the map from K^r to K given by

$$N_{\Phi^r}(x) = \prod_{\phi^r \in \Phi^r} \phi^r(x), \qquad \text{for } x \in K^r.$$

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

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

for any positive integer m; see [34, Lemma I.8.3], which uses [16, Remark on page 63] and [28, Proposition 29] in its proof.

The notation N_{Φ^r} will be used to denote any of the above three maps and the domain will be specified whenever the context of the discussion does not make it clear.

2.1.3 The field generated by CM

Let (K, Φ) be a CM pair and let (K^r, Φ^r) be its reflex. Let $\mathfrak{m}$ be an ideal of K and let m be the smallest positive integer contained in $\mathfrak{m}$. The subgroup $I_{K^r,\Phi^r}(\mathfrak{m})$ of $I_{K^r}(m)$, defined as

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

contains the group $P_{K^r}(\mathfrak{m})$ of principal fractional ideals of K satisfying $x \equiv 1 \bmod^* \mathfrak{m}$. Hence, the congruence subgroup $I_{K^r,\Phi^r}(\mathfrak{m})$ corresponds to an abelian extension. We denote by $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ this abelian extension of conductor dividing $\mathfrak{m}$.

Similar to the case of elliptic curves, this field $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ can be expressed in terms of the field of moduli of a principally polarized abelian variety (see [31, Main Theorem 2]). We will see this result in the specific case of simple principally polarized abelian surfaces in Section 2.2.3.

2.2 Jacobians of hyperelliptic curves

CM theory uses elliptic curves and their invariants to find abelian extensions of imaginary quadratic number fields, as we have seen in Section 1.2.

In more general CM theory, abelian varieties take the role of elliptic curves. *Abelian varieties* are projective group varieties. The simplest non-trivial example of an abelian variety is an elliptic curve, which is of dimension 1.

In this chapter, we discuss Jacobians of hyperelliptic curves of genus 2 (Section 2.2.1) with complex multiplication by a primitive quartic CM field K. These Jacobians are abelian surfaces and we use them to describe abelian extensions of the reflex field K^r. Jacobians have a canonical principal polarization. Polarizations are induced by a Riemann form of a complex torus that they are isomorphic to (see Section 2.2.2).

Given the reflex (K^r, Φ^r) of a primitive quartic CM pair (K, Φ), one can express the field $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ in terms of the field of moduli (Section 2.2.3), primitive torsion points (Section 2.2.4), and a normalized Kummer variety (Section 2.2.5) of a Jacobian surface with complex multiplication. These are the Main Theorems of Complex Multiplication of Shimura-Taniyama for Simple Principally Polarized Abelian Surfaces (Section 2.2.6).

2.2.1 Hyperelliptic curves and their Jacobians

An *(odd) hyperelliptic curve C over a field $k \subseteq \mathbb{C}$* is a smooth projective curve of genus $g \geq 2$ with an affine model of the form

$$C : y^2 = f(x) = (x - a_1) \cdots (x - a_{2g-1}) \tag{2.4}$$

where $f \in k[X]$ and $a_i \in \bar{k}$ for $i \in \{1, \ldots, 2g-1\}$. With this model, there is a single point at infinity, which we denote by ∞. Since a hyperelliptic curve is symmetric with respect to the x-axis, it has an automorphism called the hyperelliptic involution. The hyperelliptic involution is a map which sends (x, y) to $(x, -y)$, similar to the $[-1]$ map of an elliptic curve. For this reason, we denote the hyperelliptic involution map by $[-1]$. However, we clarify that despite having a point ∞ and an automorphism which resembles the $[-1]$ map of an elliptic curve, the points of a hyperelliptic curve do not form a group structure useful for our purposes.

We do, however, have a group involving the divisors of a hyperelliptic curve C. A *divisor* D on C is a formal sum

$$D = \sum_{P \in C(\bar{k})} n_P \cdot P, \quad n_P \in \mathbb{Z}$$

with $n_P \neq 0$ for all but finitely many $P \in C$. The set of divisors on C forms a free abelian group, which we denote by $\operatorname{Div} C$. The integer n_P is said to be the *order of D at the point P*.

The *degree* of a divisor D is simply the sum

$$\deg D = \sum_{P \in C} n_P$$

of its n_P's. We write $D \geq 0$ if $n_P \geq 0$ holds for each $P \in C$. The degree 0 divisors form a subgroup $\operatorname{Div}^0 C$ of $\operatorname{Div} C$.

A *principal divisor* on C is a divisor of the form

$$\operatorname{div} r = \sum_{P \in C} \operatorname{ord}_P(r) \cdot P$$

for some rational function r on C, where $\operatorname{ord}_P(C)$ is

$$\operatorname{ord}_P(r) = \begin{cases} m, & \text{if } r \text{ has a zero of multiplicity } m \text{ at } P, \\ -m, & \text{if } r \text{ has a pole of multiplicity } m \text{ at } P, \text{ and} \\ 0, & \text{otherwise.} \end{cases}$$

The multiplicities of zeros and poles of a rational function add up to 0, hence $\operatorname{div} r$ is a degree 0 divisor for any rational function r on C. Moreover, the group of principal divisors of C is a subgroup $\operatorname{PDiv} C$ of $\operatorname{Div}^0 C$.

Example 2.5. Take $i \in \{1, \ldots, 5\}$ and consider the function $x - a_i$. This function has a zero at $(a_i, 0)$ of multiplicity 2 and a pole at ∞ of multiplicity 2. It has no other zeros nor poles. Hence,

$$\operatorname{div}(x - a_i) = 2 \cdot (a_i, 0) - 2 \cdot \infty$$

Example 2.6. Consider a point $P = (x_0, y_0) \in C$ with $y_0 \neq 0$. Then

$$P' = [-1](P) = (x_0, -y_0)$$

is also a point in C. Consider the function $x - x_0$. This function has zeroes of multiplicity 1 at both P and P' and a pole at ∞ of multiplicity 2. It has no other zeros nor poles. Hence,

$$\operatorname{div}(x - x_0) = (x_0, y_0) + (x_0, -y_0) - 2 \cdot \infty$$

Example 2.7. The zeros of the function y on a hyperelliptic curve C are exactly at the points $(a_i, 0)$ for $i \in \{1, \ldots, 5\}$. As C is a smooth curve, these five roots are all distinct. The only pole of y is at ∞ and it is a pole of multiplicity 5. Hence

$$\operatorname{div} y = \sum_{i=1}^{5} (a_i, 0) - 5 \cdot \infty.$$

As $\operatorname{PDiv} C$ is a (normal) subgroup of the abelian group $\operatorname{Div}^0 C$, the quotient

$$\operatorname{Pic}^0 C := \operatorname{Div}^0 C / \operatorname{PDiv} C$$

is a group, which we call the *divisor class group of* C.

There is a variety $J(C)$ over k', called the *Jacobian variety of* C, which is an algebraic group satisfying the condition that for any field extension k'/k, there is a bijective map between $\operatorname{Pic}^0(C(k'))$ and $J(C)(k')$ that is a group homomorphism.

As with the case of an elliptic curve, the Jacobian of a hyperelliptic curve C has a multiplication-by-m endomorphism for each integer m.

Each divisor class $[D'] \in \operatorname{Pic}^0 C$ contains a unique divisor of the form

$$D = P_1 + \ldots + P_r - r \cdot \infty \tag{2.8}$$

such that

- $P_j \neq [-1](P_i)$ for $i \neq j$, and

- $r \leq g$.

Such a divisor is called a *reduced divisor of* C. For each $r \leq g$, we denote by $\mathrm{RDiv}_r(C)$ the set of equivalence classes in $\mathrm{Pic}^0 C$ whose unique reduced divisors are of the form (2.8). The set $\mathrm{Pic}^0 C$ is then bijective with the disjoint union given by

$$\mathrm{RDiv}_0(C) \cup \ldots \cup \mathrm{RDiv}_g(C).$$

We now introduce Mumford polynomials and loosely follow [19, Chapter 3]. Let

$$D = (x_1, y_1) + \ldots + (x_r, y_r) - r\infty \in \mathrm{RDiv}_r(C)$$

for some non-negative integer $r \leq g$ and suppose that D is defined over a field extension k'/k. There exists a unique pair $(U_D(x), V_D(x))$ of polynomials defined over k, called the *Mumford polynomials of the divisor* D, such that

M1 $U_D(x) = (x - x_1) \cdots (x - x_r)$,

M2 $V_D(x) - y$ has a zero of multiplicity of at least $n_{(x_i, y_i)}$ at $P = (x_i, y_i)$, for all $i \in \{1, \ldots, r\}$, and

M3 $V_D(x)$ has degree strictly less than r.

From Examples 2.5 and 2.6, we have

$$\mathrm{div}\, U_D = D + [-1]D$$

and by Item **M2**, we have

$$\mathrm{div}(V_D^2 - f) = \mathrm{div}(V_D - y) + \mathrm{div}(V_D + y) \geq D + [-1]D.$$

Hence, $U_D \mid V_D^2 - f$.

We may compute the coefficients of the polynomial $V_D(x)$ using Lagrange interpolation if all the x_i are distinct.

In fact, when

$$D = (x_1, y_1) + (x_2, y_2) \in \mathrm{RDiv}_2\, C$$

and $x_1 \neq x_2$, we find that

$$\begin{aligned} U_D(x) &= (x - x_1)(x - x_2) \\ V_D(x) &= \frac{x - x_2}{x_1 - x_2} y_1 + \frac{x - x_1}{x_2 - x_1} y_2. \end{aligned}$$

When $x_1 = x_2$, we must have $y_1 = y_2$ (lest $[-1](x_1, y_1) = (x_1, y_2)$). In this case, we have

$$\begin{aligned} U_D(x) &= (x - x_1)^2 \\ V_D(x) &= ax + b, \end{aligned}$$

where a, b is the (unique) solution to the system of equations:

$$\begin{aligned} ax_1 + b - y_1 &= 0 \\ a - \frac{1}{2y_1} f'(x_1) &= 0. \end{aligned}$$

There exists a bijection between RDiv_r and the set

$$\mathrm{MumPol}_r(C) := \left\{ (U, V) \in \bar{k}[X]^2 : \begin{array}{rcl} U & & \text{monic} \\ \deg U & = & r \\ \deg V & < & r \\ U & \mid & V^2 - f \end{array} \right\}. \tag{2.9}$$

In later sections, we will be dealing with the Jacobians $J(C)$ of genus 2 hyperelliptic curves C over a field $k \subseteq \mathbb{C}$. In this case, we denote by Θ the union

$$\mathrm{RDiv}_0(C) \cup \mathrm{RDiv}_1(C).$$

2.2.2 Principal polarizations on complex tori

The set $J(C)(\mathbb{C})$ of complex points of the Jacobian variety $J(C)$ of a hyperelliptic curve C over $k \subseteq \mathbb{C}$ is known to be complex analytically isomorphic to a polarizable complex torus. In this section, we discuss this statement in more detail for the case of the Jacobians of hyperelliptic curves of genus 2. A more general treatment of this topic is in [2, Chapter 11].

Treated as a Riemann surface, a complex hyperelliptic curve C of genus 2 with an affine model as in (2.4) has 6 branch points:

$$a_1, a_2, a_3, a_4, a_5, \infty.$$

We will sometimes denote the sixth branch point, ∞, as a_6.

Consider the 'map'

$$\begin{aligned} \mathrm{Int} : C(\mathbb{C}) &\dashrightarrow \mathbb{C}^2 \\ P &\mapsto \left(\int_\infty^P \varphi_1, \int_\infty^P \varphi_2 \right) \end{aligned}$$

from the complex points $C(\mathbb{C})$ of C where

$$\boldsymbol{\varphi} = (\varphi_1, \varphi_2)$$

is a basis of the space of holomorphic differentials of C, such as $\left\{ \frac{dx}{y}, \frac{x\,dx}{y} \right\}$.

The 'map' Int is not well-defined. Its output may vary depending on the path taken from ∞ to P. To remove this dependency, define Λ to be the image of the map

$$\begin{aligned} H_1(C, \mathbb{Z}) &\to \mathbb{C}^2 \\ \gamma &\mapsto \left(\int_\gamma \varphi_1, \int_\gamma \varphi_2 \right). \end{aligned}$$

It turns out that the set Λ is a lattice.

The resulting well-defined map

$$\begin{aligned} \mathrm{Int} : C(\mathbb{C}) &\to \mathbb{C}^2/\Lambda \\ P &\mapsto \left(\int_\infty^P \varphi_1, \int_\infty^P \varphi_2 \right) \end{aligned}$$

can be extended additively to become a group homomorphism on divisors of C.

The Abel part of the Abel-Jacobi Theorem [2, Abel-Jacobi Theorem 11.1.3] asserts that two divisors map to the same point in the complex torus $\mathbb{C}^2/\Lambda$ if and only if they are linearly equivalent divisors. Hence, Int can be treated as a map on $\mathrm{Pic}^0(C)$, the Jacobian of C. This map on the Jacobian of C is shown to be surjective by the Jacobi

part of the Abel-Jacobi theorem. Hence, the map

$$\begin{aligned} \mathrm{Int} : \mathrm{Pic}^0(C(\mathbb{C})) &\to \mathbb{C}^2/\Lambda \\ D = \sum_{i=1}^{r} n_i P_i &\mapsto \sum_{i=1}^{r} n_i \left(\int_{\infty}^{P_i} \varphi_1, \int_{\infty}^{P_i} \varphi_2) \right) \end{aligned} \tag{2.10}$$

is an isomorphism between $\mathrm{Pic}^0(C(\mathbb{C}))$ and the complex torus $\mathbb{C}^2/\Lambda$.

Not all complex tori are complex analytically isomorphic to an abelian variety. To determine whether or not there exists an abelian variety that is complex analytically isomorphic to a complex torus, we look at the existence of a Riemann form.

A *Riemann form* on a complex torus $\mathbb{C}^2/\Lambda$ is an antisymmetric bilinear map

$$E : \Lambda \times \Lambda \to \mathbb{Z}$$

such that

1. the $\mathbb{R}$-linear extension $E_{\mathbb{R}} : \mathbb{C}^2 \times \mathbb{C}^2 \to \mathbb{R}$ satisfies $E(\vec{v}, \vec{w}) = E(i\vec{v}, i\vec{w})$ for every $v, w \in \mathbb{C}^2$, and

2. the associated Hermite form

$$H(\vec{v}, \vec{w}) := E_{\mathbb{R}}(i\vec{v}, \vec{w}) + iE_{\mathbb{R}}(\vec{v}, \vec{w})$$

   is positive definite.

If a complex torus $\mathbb{C}^2/\Lambda$ admits a Riemann form, then it is complex analytically isomorphic to an abelian surface A_Λ [2, Theorem 4.2.1].

A Riemann form on a complex torus $\mathbb{C}^2/\Lambda$ induces a so-called *polarization* C_E, defined in [2, Section 4.1], on the corresponding abelian surface A_Λ. This polarization is said to be *principal* if the matrix defining the Riemann form E, with respect to a basis of Λ, has determinant 1. An abelian surface together with a (principal) polarization is called a *(principally) polarized abelian surface*. We denote such a pair by (A, C_E).

An isomorphism $\alpha : (A, C_E) \to (A', C_{E'})$ of complex principally polarized abelian surfaces, with $A(\mathbb{C}) \cong \mathbb{C}^2/\Lambda$ and $A'(\mathbb{C}) \cong \mathbb{C}^2/\Lambda'$, is a $\mathbb{C}$-linear isomorphism $\alpha : \mathbb{C}^2 \to \mathbb{C}^2$ satisfying

1. $\alpha(\Lambda) = \Lambda'$, and

2. $E(\vec{v}, \vec{w}) = E'(\alpha(\vec{v}), \alpha(\vec{w}))$ for all $\vec{v}, \vec{w} \in \mathbb{C}^2$.

The Jacobian $J(C)$ of a hyperelliptic curve C has a canonical principal polarization [2, Proposition 11.1.2], which we denote by $\mathcal{C}$. Hence $(J(C), \mathcal{C})$ is a principally polarized abelian variety. Observe that, despite the fact that this polarization is canonical, we still write $(J(C), \mathcal{C})$ to insist that we are treating the Jacobian as a principally polarized abelian variety, as opposed to just an abelian variety. When the curve C has genus 2, the Jacobian has dimension 2 and is therefore a principally polarized abelian surface.

2.2.3 Fields of moduli of Jacobian surfaces

A principally polarized abelian surface $(A, \mathcal{C}_E)$ over $k \subseteq \mathbb{C}$ is, over $\bar{k}$, either one of the following objects:

1. the Jacobian of a hyperelliptic curve C of genus 2, or
2. the product of two elliptic curves equipped with the product polarization.

This result is shown in [37, Satz 2].

Let C be a hyperelliptic curve over k with a unique point ∞ at infinity. We can embed C into $J(C)$ as follows

$$\begin{aligned} j : C &\hookrightarrow J(C) \\ P &\mapsto [P - \infty]. \end{aligned}$$

Consider a $\bar{k}$-isomorphism

$$\begin{aligned} f : C &\to C' \\ P &\mapsto P' \end{aligned}$$

of hyperelliptic curves over k of genus 2. Using the embedding j, the isomorphism f induces a $\bar{k}$-isomorphism $f_J : (J(C), \mathcal{C}) \to (J(C'), \mathcal{C}')$ where

$$\phi_J([P - \infty]) = [P' - \infty].$$

Torelli's theorem gives us the converse.

Theorem 2.11 (Torelli's theorem, specialized to genus 2 hyperelliptic curves)**.** Let C and C' be hyperelliptic curves of genus 2 over $k \subseteq \mathbb{C}$. For any $\bar{k}$-isomorphism

$$\phi : (J(C), C) \to (J(C'), C')$$

between the Jacobians of C and C', there exists a unique $\bar{k}$-isomorphism

$$\tilde{\phi} : C \to C'$$

such that $\phi = \tilde{\phi}_J$.

Proof. This is [17, Appendix, Théorème 1]. □

Given an automorphism $\sigma \in \operatorname{Aut} \mathbb{C}$, and a Jacobian (J, C) of a hyperelliptic curve C over a field $k \subseteq \mathbb{C}$, denote by C_σ the polarization induced by taking the Jacobian of C^σ. In addition, we denote by $(J, C)^\sigma$ the principally polarized abelian surface $(J(C^\sigma), C_\sigma)$.

The *field of moduli of the Jacobian* (J, C) *of a hyperelliptic curve* C *of genus* 2 defined over a field $k \subseteq \mathbb{C}$ is the field $\mathcal{M}(J(C), C) \subseteq \mathbb{C}$ which satisfies

$\sigma \in \operatorname{Aut}(\mathbb{C})$ is the identity on $\mathcal{M}(J(C), C)$ if and only if the following equivalent conditions hold:

F1. there exists a $\mathbb{C}$-isomorphism $\phi : C \to C^\sigma$ of genus 2 hyperelliptic curves

F2. there exists a $\mathbb{C}$-isomorphism $\phi : (J, C) \to (J, C)^\sigma$ of principally polarized abelian surfaces,

An *automorphism of* (J, C) *over* k is a k-isomorphism of (J, C) to itself. The automorphisms of (J, C) over k form a group which we denote by $\operatorname{Aut}_k(J, C)$.

As in the case of elliptic curves, we also have a notion of principally polarized abelian surfaces with complex multiplication.

A principally polarized abelian surface (A, C_E) over a field $k \subseteq \mathbb{C}$ is said to have *complex multiplication by a quartic CM field* K if there exists an embedding

$$\iota : K \hookrightarrow \operatorname{End}_{\bar{k}}(A) \otimes \mathbb{Q}$$

such that

$$\iota^{-1}(\mathrm{End}(A)) \;=\; \mathcal{O}_K.$$

We denote such an abelian surface by a triple (A, ι, C_E).

Moreover, if (A, ι, C_E) has complex multiplication by a *primitive* quartic CM field K then it is simple over $\mathbb{C}$. Hence, $(A, \iota, C_E) \;=\; (J(C), \iota, C)$ for some hyperelliptic curve C of genus 2.

There is also a concept of a field of moduli for other objects such as (J, ι, C).

Let (J, ι, C) and (J', ι', C') be Jacobian surfaces over a field $k \;\subseteq\; \mathbb{C}$, with complex multiplication by K. An *isomorphism* $\phi : (J, \iota, C) \to (J', \iota', C')$ *over* $k \;\subseteq\; \mathbb{C}$ is an isomorphism of principally polarized abelian surfaces satisfying $\phi \circ \iota(a) = \iota'(a) \circ \phi$ for all $a \in \mathcal{O}_K$.

Suppose $\iota(a) \in \mathrm{End}\, J(C)$ with $a \in K$ and $\sigma \in \mathrm{Aut}\, \mathbb{C}$. The endomorphism

$$\iota^{\sigma}(\alpha) \;:=\; \iota(a)^{\sigma}$$

is obtained by letting σ act on the coefficients of $\iota(a)$. We denote by $(J, \iota, C)^{\sigma}$ the triple $(J(C), \iota^{\sigma}, C_{\sigma})$

An automorphism of (J, ι, C) over a field $k \;\subseteq\; \mathbb{C}$ is a k-isomorphism of (J, ι, C) to itself. Like the k-automorphisms of (J, C), the automorphisms of (J, ι, C) form a group which we denote by $\mathrm{Aut}_k(J, \iota, C)$.

> **Example 2.12.** The automorphism group $\mathrm{Aut}_k(J, \iota, C)$ of the Jacobian of a hyperelliptic curve of genus 2, over k, with complex multiplication by a primitive quartic CM field $K \not\cong \mathbb{Q}(\zeta_5)$ is $\langle [-1] \rangle$.

Let T be a finite set of points of a Jacobian $(J(C), \iota, C)$, with complex multiplication by K, of a genus 2 hyperelliptic curve. The *field of moduli of* $(J(C), \iota, C; T)$ is defined as the field $\mathcal{M}(J(C), \iota, C; T)$ satisfying

$\sigma \in \mathrm{Aut}(\mathbb{C})$ is the identity on $\mathcal{M}(J(C), \iota, C; T)$ if and only if there exists a $\mathbb{C}$-isomorphism $\phi : (J(C), \iota, C) \to (J(C), \iota, C)^{\sigma}$ such that $\phi(t) = t^{\sigma}$ for all $t \in T$.

The field of moduli exists if $(J, \iota, \mathcal{C})$ and all points in T are defined over a number field [16, page 135]. When T is the empty set, we drop the T in the notation. In other words, we denote the field of moduli of $\mathcal{M}(J(\mathcal{C}), \iota, \mathcal{C}; T)$ by $\mathcal{M}(J(\mathcal{C}), \iota, \mathcal{C})$.

We define the field of moduli $\mathcal{M}(J(\mathcal{C}), \mathcal{C}; T)$ of $(J(\mathcal{C}), \mathcal{C}; T)$ by dropping all instances of ι in the above definition. That is, the *field of moduli of* $(J(\mathcal{C}), \mathcal{C}; T)$ where T is a finite set of points of a Jacobian $(J(\mathcal{C}), \mathcal{C})$, is defined as the field $\mathcal{M}(J(\mathcal{C}), \mathcal{C}; T)$ satisfying

$\sigma \in \mathrm{Aut}(\mathbb{C})$ is the identity on $\mathcal{M}(J(\mathcal{C}), \mathcal{C}; T)$ if and only if there exists a $\mathbb{C}$-isomorphism $\phi : (J(\mathcal{C}), \mathcal{C}) \to (J(\mathcal{C}), \mathcal{C})^{\sigma}$ such that $\phi(t) = t^{\sigma}$ for all $t \in T$.

2.2.4 Primitive torsion points of Jacobian surfaces

Let $(J, \iota, \mathcal{C})$ be a principally polarized abelian surface over k with complex multiplication by K. Let $\mathfrak{m} = m_1 O_K + m_2 O_K$ be an ideal of O_K. We define $J[\mathfrak{m}]$ to be the set of points P of J such that $\iota(m_1)(P) = \iota(m_2)(P) = 0$. The set $J[\mathfrak{m}]$ is a subgroup of J and we call it its $\mathfrak{m}$-*torsion subgroup*.

The map ι allows us to view $J[\mathfrak{m}]$ as an $O_K/\mathfrak{m}$-module. The $O_K/\mathfrak{m}$-module $J[\mathfrak{m}]$ is free of rank 1 [16, Chapter 4 Proposition 5.3]; see also [16, page 138].

A basis element of $A[\mathfrak{m}]$ as an $O_K/\mathfrak{m}$-module is called a *primitive* $\mathfrak{m}$-*torsion point*. In [31], a primitive $\mathfrak{m}$-torsion point is called a proper $\mathfrak{m}$-section point. Clearly, a primitive $\mathfrak{m}$-torsion point is an element of the $\mathfrak{m}$-torsion subgroup $J[\mathfrak{m}]$.

The following theorem shows that to find the field of moduli of $(J, \iota, \mathcal{C}; J[\mathfrak{m}])$ with $T = J[\mathfrak{m}]$, it suffices to just find the field of moduli of $(J, \iota, \mathcal{C}; t)$ where t is a primitive $\mathfrak{m}$-torsion point.

Theorem 2.13. Let (K, Φ) be a primitive quartic CM pair. Let $(J, \iota, \mathcal{C})$ be a principally polarized abelian surface over $k \subseteq \mathbb{C}$ with complex multiplication by K. If t is a primitive $\mathfrak{m}$-torsion point, then

$$\mathcal{M}(J, \iota, \mathcal{C}; t) = \mathcal{M}(J, \iota, \mathcal{C}; J[\mathfrak{m}]).$$

Proof. We first show $\mathcal{M}(J, \iota, C; t) \subseteq \mathcal{M}(J, \iota, C; J[\mathfrak{m}])$. Suppose $\sigma \in \mathrm{Aut}(\mathbb{C})$ fixes $\mathcal{M}(J, \iota, C; J[\mathfrak{m}])$. Then there exists a $\mathbb{C}$-isomorphism

$$\phi : (J, \iota, C) \to (J, \iota, C)^{\sigma}$$

satisfying $\phi(s) = s^{\sigma}$ for each $s \in J[\mathfrak{m}]$. Note that since $t \in J[\mathfrak{m}]$, we have

$$\phi(t) = t^{\sigma}$$

and hence σ fixes $\mathcal{M}(J, \iota, C; t)$.

Now, we show $\mathcal{M}(J, \iota, C; t) \supseteq \mathcal{M}(J, \iota, C; J[\mathfrak{m}])$. Suppose $\sigma \in \mathrm{Aut}(\mathbb{C})$ fixes the field $\mathcal{M}(J, \iota, C; t)$. Then there exists a $\mathbb{C}$-isomorphism

$$\phi : (J, \iota, C) \to (J, \iota, C)^{\sigma}$$

satisfying $\phi(t) = t^{\sigma}$. Take $t' \in J[\mathfrak{m}]$. Since t is a primitive $\mathfrak{m}$-torsion point, the point t' is equal to $\iota(a)t$ for some $a \in \mathcal{O}_K$. Then

$$\phi(t') = \phi(\iota(a)t) = \iota^{\sigma}(a)\phi(t) = \iota(a)^{\sigma} t^{\sigma} = t'^{\sigma}.$$

Hence, for every $s \in J[\mathfrak{m}]$, the isomorphism ϕ satisfies $\phi(s) = s^{\sigma}$. Hence, the automorphism σ fixes $\mathcal{M}(J, \iota, C; J[\mathfrak{m}])$. □

2.2.5 Kummer varieties of Jacobian surfaces

Let A be a variety over k and let $G \subseteq \mathrm{Aut}_k A$ be a subgroup of the k-automorphism group of A. A pair (W, h), consisting of a variety W over k and a surjective morphism $h : A \to W$ over k, is called a *quotient variety of the abelian variety A by G* if

Q1 for every $a \in A$, we have $h^{-1}(h(a)) = Ga := \{a^g : g \in G\}$, and

Q2 for any G-invariant morphism $f : A \to V$ over $k' \supseteq k$ of varieties, there is a

morphism $f_W : W \to V$ over k' which makes the following diagram

$$\begin{tikzcd} A \arrow[r, "h"] \arrow[dr, "f"'] & W \arrow[d, dashed, "f_W"] \\ & V \end{tikzcd}$$

commute.

The morphism f_W is unique by the surjectivity of h. Moreover, when the group G is finite, the quotient of a variety A by G exists [15, Theorem A.8.3.1]. When quotient varieties exist, we have the following lemma concerning their uniqueness.

Lemma 2.14. Quotient varieties of a variety A over $k \subseteq \mathbb{C}$ by a group $G \subseteq \mathrm{Aut}_k A$ are unique up to unique k-isomorphism. More precisely, if (W_1, h_1) and (W_2, h_2) are quotient varieties of a variety A by a subgroup $G \subseteq \mathrm{Aut}_k A$ of the automorphism group of A then there exists a unique k-isomorphism ϕ which makes the diagram

$$\begin{tikzcd} A \arrow[r, "h_1"] \arrow[dr, "h_2"'] & W_1 \arrow[d, dashed, "\phi"] \\ & W_2 \end{tikzcd} \tag{2.15}$$

commute.

Proof. Let (W_1, h_1) and (W_2, h_2) be quotient varieties of the same variety A. As h_2 is a G-invariant morphism, by property (**Q2**) of (W_1, h_1), there exists a unique mor-

phism f_1 such that

$$\begin{tikzcd} A \arrow[r, "h_1"] \arrow[dr, "h_2"'] & W_1 \arrow[d, dashed, "f_1"] \\ & W_2 \end{tikzcd}$$

commutes. Morever, h_1 is a G-invariant morphism as well, and by property (**Q2**) of (W_2, h_2), there exists a unique morphism such that

$$\begin{tikzcd} A \arrow[r, "h_1"] \arrow[dr, "h_2"'] & W_1 \\ & W_2 \arrow[u, dashed, "f_2"] \end{tikzcd}$$

commutes. Let $i \in \{1, 2\}$. Using property (**Q2**) of (W_i, h_i) on the G-invariant morphism h_i, we find that there exists a unique morphism g_i such that $g_i \circ h_i = h_i$. Therefore, $g_i = \mathrm{id}_{W_i}$.

Observing that $(f_2 \circ f_1) \circ h_1 = h_1$, then $f_2 \circ f_1$ must be g_1, by the uniqueness of g_1. Using a similar argument, $f_1 \circ f_2 = g_2$ by the uniqueness of g_2.

Having shown that $f_2 \circ f_1 = \mathrm{id}_{W_1}$ and $f_1 \circ f_2 = \mathrm{id}_{W_2}$, we conclude that both f_1 and f_2 are unique isomorphisms. □

The automorphism group $\mathrm{Aut}_k(A, C_E)$ of a *polarized* abelian variety (A, C_E) over k is finite [16, Chapter 3, Theorem 4.2]. A quotient variety of A by $\mathrm{Aut}_{\bar{k}}(A, C_E)$, the group of automorphisms of $\mathrm{Aut}_{\bar{k}}(A, C_E)$ over $\bar{k}$, is called a *Kummer variety of* (A, C_E).

Theorem 2.16. Let (J, C) be a simple principally polarized abelian surface over $k \subseteq \mathbb{C}$ such that $\mathrm{Aut}_{\bar{k}}(J, C) = \mathrm{Aut}_k(J, C)$. There exists a Kummer variety (W, h), defined over k, of (J, C) which satisfies the following:

K1. There exists a variety W_0 defined over the field of moduli $k_0 := \mathcal{M}(J, C)$ such that W is the base change of W_0 to k.

K2. For every $\sigma \in \mathrm{Aut}(\bar{k}/k_0)$ and for every $\bar{k}$-isomorphism

$$f_\sigma : (J, C) \to (J, C)^\sigma,$$

the diagram

(2.17)
$$\begin{tikzcd} (J,C) \arrow[r, "h"] \arrow[d, "f_\sigma"] & W \\ (J,C)^\sigma \arrow[ur, "h^\sigma"] & \end{tikzcd}$$

commutes.

Proof. The proof of the above theorem is the same as in the proof of [16, Chapter 5, Theorem 3.2] (see also [31, Section 4.4, Theorem 3]), applied to simple prinicpally polarized abelian surfaces. □

Later on, in Section 4.2, we discuss how to find an explicit formula for the map h for the case we are interested in.

We call a variety (W, h), whose existence is guaranteed by Theorem 2.16, a *normalized Kummer variety of* (J, C) *over* k. Note that such varieties are referred to in [16] as *Kummer varieties over a field of moduli*.

2.2.6 The Main Theorems of Complex Multiplication

We are now ready to state the main theorems of complex multiplication for simple principally polarized abelian surfaces. As one can observe from the works cited in the proofs, there are versions of these statements applicable to higher dimensional principally polarized abelian varieties. We specialize these theorems to the case of simple principally polarized abelian surfaces as this is the only case we will be using.

Theorem 2.18 (The First Main Theorem of Complex Multiplication for Simple Principally Polarized Abelian Surfaces)**.** Let (K^r, Φ^r) be the reflex pair of a primitive quartic CM pair (K, Φ). Let (J, ι, C) be a principally polarized abelian surface

with complex multiplication by K. We have

$$\mathrm{CM}_{K^r,\Phi^r}(1) = K^r\mathcal{M}(J,C) = \mathcal{M}(J,\iota,C)$$

where $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ is as defined in Section 2.1.3.

It is not a coincidence that Theorem 2.18 and its elliptic curve counterpart Theorem 1.15 share some similarities, as they are both specializations of a theorem applicable for principally polarized abelian varieties.

Proof. The first equality,

$$\mathrm{CM}_{K^r,\Phi^r}(1) = K^r\mathcal{M}(J,C),$$

is given in Shimura-Taniyama [31, Main Theorem 1, p128]. The second equality,

$$K^r\mathcal{M}(J,C) = \mathcal{M}(J,\iota,C),$$

is true by taking $F = \mathbb{Q}$ in [29, Proposition 5.17(i)]. □

We can express $\mathrm{CM}_{K^r,\Phi^r}(1)$ in terms of Cardona-Quer invariants as follows:

Example 2.19. For a hyperelliptic curve C of genus 2 defined over $k \subseteq \mathbb{C}$, one can define what is called its piecewise Cardona-Quer invariants

$$(j_1(C), j_2(C), j_3(C)),$$

defined in [4]. This set of invariants determines the $\mathbb{C}$-isomorphism class of C. In other words, two hyperelliptic curves C and C' are isomorphic over $\mathbb{C}$ if and only if

$$(j_1(C), j_2(C), j_3(C)) = (j_1(C'), j_2(C'), j_3(C')).$$

Let (A, ι, C_E) be the Jacobian $(J(C), \iota, C)$ of a hyperelliptic curve C of genus 2 with complex multiplication by a primitive quartic CM field K. The field of moduli of (A, C_E) is then $\mathbb{Q}(j_1(C), j_2(C), j_3(C))$. Therefore,

$$\mathrm{CM}_{K^r,\Phi^r}(1) = K^r(j_1(C), j_2(C), j_3(C)).$$

As in the case of the Kronecker-Weber Theorem and the Second Main Theorem of Complex Mutiplication for Elliptic Curves ((1.18)), the Second Main Theorem of Complex Multiplication for Simple Principally Polarized Abelian Surfaces concerns a map evaluated at the torsion points of some variety.

Theorem 2.20 (The Second Main Theorem of Complex Multiplication for Simple Principally Polarized Abelian Surfaces)**.** Let (K^r, Φ^r) be the reflex pair of a primitive quartic CM pair (K, Φ). Let (J, ι, C) be a principally polarized abelian surface over k with complex multiplication by K. Let (W, h) be a normalized Kummer variety of (J, C). Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ and let t be a primitive $\mathfrak{m}$-torsion point. We have

$$\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) = \mathrm{CM}_{K^r,\Phi^r}(1)(h(t)) = \mathcal{M}(J, \iota, C; J[\mathfrak{m}]).$$

where $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ is as defined in Section 2.1.3.

Proof. The first equality is given in Shimura-Taniyama [31, Main Theorem 2, page 135]. To prove the second equality, note that by Theorem 2.18,

$$\mathrm{CM}_{K^r,\Phi^r}(1)(h(t)) = \mathcal{M}(J, \iota, C)(h(t)).$$

Using [16, Chapter 5, Theorem 3.3], we find that $\mathcal{M}(J, \iota, C)(h(t))$ is equal to the field of moduli $\mathcal{M}(J, \iota, C; t)$. With this obervation in mind, a direct application of Theorem 2.13 proves the second equality. □

2.3 Theta functions

Let $g \in \mathbb{Z}_{>0}$. Let $\mathbb{H}_g$ denote the set of $g \times g$ symmetric matrices over $\mathbb{C}$ with positive definite imaginary part. For any $\vec{\mathbf{a}}, \vec{\mathbf{b}} \in \mathbb{Q}^g$, the *theta function with characteristic* $\begin{bmatrix}\vec{\mathbf{a}}\\ \vec{\mathbf{b}}\end{bmatrix}$ is the function

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

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

Let $a_1, a_2, b_1, b_2 \in \{0, 1/2\}$. We use the following short-hand notation, used in [12, 34, 9], for the sixteen theta functions with half-integer characteristics as follows:

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

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

Note that different articles use different indexings for their theta functions.

2.3.1 Rosenhain invariants

Let $\boldsymbol{\tau} \in \mathbb{H}_2$. The set of *Rosenhain invariants of* $\boldsymbol{\tau}$ is the triple $(\lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau}))$

$$\lambda_1(\boldsymbol{\tau}) := \frac{\vartheta_0(\boldsymbol{\tau})^2\vartheta_8(\boldsymbol{\tau})^2}{\vartheta_4(\boldsymbol{\tau})^2\vartheta_{12}(\boldsymbol{\tau})^2}, \quad \lambda_2(\boldsymbol{\tau}) := \frac{\vartheta_2(\boldsymbol{\tau})^2\vartheta_8(\boldsymbol{\tau})^2}{\vartheta_6(\boldsymbol{\tau})^2\vartheta_{12}(\boldsymbol{\tau})^2}, \quad \lambda_3(\boldsymbol{\tau}) := \frac{\vartheta_0(\boldsymbol{\tau})^2\vartheta_2(\boldsymbol{\tau})^2}{\vartheta_4(\boldsymbol{\tau})^2\vartheta_6(\boldsymbol{\tau})^2}.$$

Following the discussion in [35], we find that the Jacobian $J_{\boldsymbol{\tau}} := J(C_{\boldsymbol{\tau}})$ of the hyperelliptic curve $C_{\boldsymbol{\tau}}$ given by:

$$C_{\boldsymbol{\tau}} : \ y^2 = f(x) = x(x-1)(x-\lambda_1(\boldsymbol{\tau}))(x-\lambda_2(\boldsymbol{\tau}))(x-\lambda_3(\boldsymbol{\tau})) \tag{2.21}$$

defined over $\mathbb{Q}(\lambda_i(\boldsymbol{\tau}) : \ i \in \{1, \ldots, 3\})$ is isomorphic to the polarizable complex torus $(\mathbb{C}^2/\Lambda_{\boldsymbol{\tau}}, E)$.

The 2-torsion subgroup $J_{\boldsymbol{\tau}}[2] \cong \mathrm{Pic}^0(C)[2]$ contains the divisor classes which have a representative of the form

$$W + W' - 2\infty$$

where

$$W, W' \in \mathcal{W} = \{(a_i, 0) \in C\} \cup \{\infty\}.$$

Theorem 2.22. The field of moduli $\mathcal{M}(J_{\boldsymbol{\tau}}, C, J_{\boldsymbol{\tau}}[2])$ is $\mathbb{Q}(\lambda_i(\boldsymbol{\tau}) : \ i \in \{1, \ldots, 3\})$.

Proof. We first show that $\mathbb{Q}(\lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau})) \subseteq \mathcal{M}(J_{\boldsymbol{\tau}}, C, J_{\boldsymbol{\tau}}[2])$.

Let $\sigma \in \mathrm{Aut}\ \mathbb{C}$ be an automorphism which fixes $\mathcal{M}(J_{\boldsymbol{\tau}}, C, J_{\boldsymbol{\tau}}[2])$. Then, there exists an isomorphism $\phi : (J_{\boldsymbol{\tau}}, C) \to (J_{\boldsymbol{\tau}}, C)^{\sigma}$ such that $\phi(t) = t^{\sigma}$ for each

point $t \in J_{\boldsymbol{\tau}}[2]$. By Theorem 2.11, there exists an isomorphism $\tilde{\phi} : C_{\boldsymbol{\tau}} \to C_{\boldsymbol{\tau}}^{\sigma}$ where

$$C_{\boldsymbol{\tau}} : y^2 = (x - a_1) \cdots (x - a_5)$$

and

$$(a_1, a_2, a_3, a_4, a_5) := (0, 1, \lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau}))$$

such that $\phi([\sum_{P \in C_{\boldsymbol{\tau}}} n_P P]) = [\sum_{P \in C_{\boldsymbol{\tau}}} n_P \tilde{\phi}(P)]$.

For each $P, P' \in \{\infty, (0,0), (1,0)\}$, we have

$$\phi([P - P']) = [P - P']^{\sigma} = [P - P']$$

where the first equality is due to the fact that $\phi(t) = t^{\sigma}$ and the second equality is due to the fact that the coordinates of P, P' are fixed by σ. In particular, we have

$$\begin{aligned} \phi([(0,0) - \infty]) &= [(0,0) - \infty], \\ \phi([(1,0) - \infty]) &= [(1,0) - \infty], \\ \phi([(0,0) + (1,0) - 2\infty]) &= [(0,0) + (1,0) - 2\infty]. \end{aligned}$$

Note that the right hand side of each of the three equations above is given by a reduced representative of its divisor class.

On the other hand, we have

$$\phi([(0,0) - \infty]) = [\tilde{\phi}((0,0)) - \tilde{\phi}(\infty)].$$

Since $\tilde{\phi}$ sends Weierstrass points to Weierstrass points, we know that

$$[2\tilde{\phi}(\infty) - 2\infty]$$

is trivial in $\mathrm{Pic}^0(C^{\sigma})$. Hence

$$\phi([(0,0) - \infty]) = [\tilde{\phi}((0,0)) + \tilde{\phi}(\infty) - 2\infty].$$

Since reduced representatives are unique, we have

$$\tilde{\phi}((0,0)) + \tilde{\phi}(\infty) - 2\infty = (0,0) - \infty.$$

So,

$$\tilde{\phi}((0,0)) + \tilde{\phi}(\infty) = (0,0) + \infty. \tag{2.23}$$

Repeating the argument for $[(1,0) - \infty]$, we find that

$$\tilde{\phi}((1,0)) + \tilde{\phi}(\infty) = (1,0) + \infty, \tag{2.24}$$

From (2.23) and (2.24), we conclude that

$$\tilde{\phi}(P) = P$$

for each $P \in \{\infty, (0,0), (1,0)\}$.

Now, for any hyperelliptic curve C of genus 2 over $\mathbb{C}$, let $x_C : C \to \mathbb{P}^1(\mathbb{C})$ be the projection $P \mapsto x(P)$. Since $\tilde{\phi}$ is a $\mathbb{C}$-isomorphism of hyperelliptic curves, there exists an automorphism $f : \mathbb{P}^1(\mathbb{C}) \to \mathbb{P}^1(\mathbb{C})$ such that $f \circ x_{C_\tau} = x_{C_\tau^\sigma} \circ \tilde{\phi}$. Since f is an automorphism of $\mathbb{P}^1(\mathbb{C})$, it is a Mobius transformation. That is, it is of the form $(x : z) \mapsto (ax + bz : cx + dz)$ for some $a, b, c, d \in \mathbb{C}$ such that $ad - bc \neq 1$. This transformation fixes the three points $(0:1), (0:1), (1:1)$. Solving for a, b, c, d, we find that f is the identity map. This means that

$$(\lambda_i(\boldsymbol{\tau}) : 1) = f(\lambda_i(\boldsymbol{\tau})) = (\lambda_i(\boldsymbol{\tau}) : 1)^\sigma = (\lambda_i(\boldsymbol{\tau})^\sigma : 1)$$

for $i \in \{1, \ldots, 3\}$. Hence, σ fixes $\mathbb{Q}(\lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau}))$.

We now show $\mathbb{Q}(\lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau})) \supseteq \mathcal{M}(J_\tau, C, J_\tau[2])$. Let $\sigma \in \operatorname{Aut}\mathbb{C}$ be an automorphism that fixes $\mathbb{Q}(\lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau}))$. Since σ fixes the field extension $\mathbb{Q}(\lambda_1(\boldsymbol{\tau}), \lambda_2(\boldsymbol{\tau}), \lambda_3(\boldsymbol{\tau}))$, we have $C_\tau = C_\tau^\sigma$ and $(J_\tau, C) = (J_\tau, C)^\sigma$. Then there exists an isomorphism $\phi : (J_\tau, C) \to (J_\tau, C)^\sigma$. Therefore, σ fixes the field of moduli $\mathcal{M}(J_\tau, C, J_\tau[2])$. □

2.3.2 Mumford polynomials and theta functions

Let $\boldsymbol{\tau} \in \mathbb{H}_2$, where $\mathbb{H}_2$ is defined in the beginning of Section 2.3. Let $D \in J(C_\tau) \setminus \Theta$, where $\vec{\mathbf{z}} = \operatorname{Int}([D])$, the symbol $\Theta = \operatorname{RDiv}_0 C \cup \operatorname{RDiv}_1 C$ (as defined towards the end of Section 2.2.1), and Int as in (2.10). We would like to find the pair of Mumford polynomials $(U_{\vec{\mathbf{z}},\tau}, V_{\vec{\mathbf{z}},\tau}) := (U_D, V_D)$ in terms of theta functions.

Conveniently, van Wamelen gives a formula for computing (U_D, V_D) in terms of his modified set of theta functions. In his paper [35], this set of modified theta functions are indexed by subsets of $\{1, \ldots, 5\}$ but we denote them as follows:

$$
\begin{aligned}
t_0(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_4^2\,\vartheta_6^2\,\vartheta_{12}^2}{\vartheta_1\,\vartheta_2\,\vartheta_3\,\vartheta_8\,\vartheta_9\,\vartheta_{15}} \cdot \theta_{14}(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_1(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_{15}} \cdot \theta_{15}(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_2(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_{12}} \cdot \theta_{12}(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_3(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0\,\vartheta_{12}}{\vartheta_8\,\vartheta_9} \cdot \theta_{13}(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_4(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0\,\vartheta_4\,\vartheta_6\,\vartheta_{12}}{\vartheta_1\,\vartheta_3\,\vartheta_9\,\vartheta_{15}} \cdot \theta_{10}(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_5(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_4\,\vartheta_6\,\vartheta_{12}}{\vartheta_2\,\vartheta_8\,\vartheta_{15}} \cdot \theta_{11}(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_6(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_8} \cdot \theta_8(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_7(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_9} \cdot \theta_9(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_8(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_6} \cdot \theta_6(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_9(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0\,\vartheta_6}{\vartheta_2\,\vartheta_3} \cdot \theta_7(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_{10}(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_4} \cdot \theta_4(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_{11}(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_4}{\vartheta_1} \cdot \theta_5(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_{12}(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_2} \cdot \theta_2(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_{13}(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_3} \cdot \theta_3(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_{14}(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \theta_0(\vec{\mathbf{z}}, \boldsymbol{\tau}) \\
t_{15}(\vec{\mathbf{z}}, \boldsymbol{\tau}) &= \frac{\vartheta_0}{\vartheta_1} \cdot \theta_1(\vec{\mathbf{z}}, \boldsymbol{\tau})
\end{aligned}
$$

where we write ϑ_i for the theta constant $\vartheta_i(\boldsymbol{\tau})$.

Applying van Wamelen's theorem [35, Theorem 5][2], we find that

$$U_0 := U_{\vec{\mathbf{z}},\boldsymbol{\tau}}(0) = \frac{t_4(\vec{\mathbf{z}},\boldsymbol{\tau})}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})} = \frac{\vartheta_0^2\vartheta_2^2\vartheta_8^2}{\vartheta_4^2\vartheta_6^2\vartheta_{12}^2}\frac{\theta_{10}(\vec{\mathbf{z}},\boldsymbol{\tau})^2}{\theta_{14}(\vec{\mathbf{z}},\boldsymbol{\tau})^2},$$

and

$$U_1 := U_{\vec{\mathbf{z}},\boldsymbol{\tau}}(1) = \frac{t_5(\vec{\mathbf{z}},\boldsymbol{\tau})}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})} = \frac{\vartheta_1^2\vartheta_3^2\vartheta_9^2}{\vartheta_4^2\vartheta_6^2\vartheta_{12}^2}\frac{\theta_{11}(\vec{\mathbf{z}},\boldsymbol{\tau})^2}{\theta_{14}(\vec{\mathbf{z}},\boldsymbol{\tau})^2}.$$

By Lagrange Interpolation, we find that

$$U_{\vec{\mathbf{z}},\boldsymbol{\tau}}(x) = x^2 + u_1 x + u_0,$$

where $u_0 := U_0$ and $u_1 := U_1 - U_0 - 1$, is the unique monic quadratic polynomial that satisfies $U_{\vec{\mathbf{z}},\boldsymbol{\tau}}(i) = U_i$ for $i \in \{0, 1\}$. Following Cosset [9, Exemple 5.2.2], we may express $V^2_{\vec{\mathbf{z}},\boldsymbol{\tau}}(x)$ in terms of theta functions as follows:

$$V^2_{\vec{\mathbf{z}},\boldsymbol{\tau}}(x) = (x-1)^2 v_0^2 + x^2 v_1^2 - x(x-1)v_0 v_1$$

where

$$\begin{aligned}
v_0^2 &= V^2_{\vec{\mathbf{z}},\boldsymbol{\tau}}(0) = (\lambda_1(\boldsymbol{\tau}) - 1)^2 \left(Y_{1,2}^2 + Y_{1,3}^2 - 2Y_{1,2}Y_{1,3}\right)\\
v_1^2 &= V^2_{\vec{\mathbf{z}},\boldsymbol{\tau}}(1) = \lambda_1(\boldsymbol{\tau})^2 \left(Y_{1,2}^2 + Y_{2,3}^2 - 2Y_{1,2}Y_{2,3}\right)\\
v_0 v_1 &= V_{\vec{\mathbf{z}},\boldsymbol{\tau}}(0)V_{\vec{\mathbf{z}},\boldsymbol{\tau}}(1) = \lambda_1(\boldsymbol{\tau})(\lambda_1(\boldsymbol{\tau}) - 1)\left(Y_{1,2}^2 - Y_{1,2}Y_{1,3} - Y_{1,2}Y_{2,3} + Y_{1,3}Y_{2,3}\right)
\end{aligned}$$

and

$$\begin{aligned}
Y_{1,2}^2 &= \frac{t_1(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_4(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_5(\vec{\mathbf{z}},\boldsymbol{\tau})^2}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})^6},\\
Y_{1,3}^2 &= \frac{t_4(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_9(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_{13}(\vec{\mathbf{z}},\boldsymbol{\tau})^2}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})^6},\\
Y_{2,3}^2 &= \frac{t_5(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_9(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_{12}(\vec{\mathbf{z}},\boldsymbol{\tau})^2}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})^6},\\
Y_{1,2}Y_{1,3} &= \frac{t_1(\vec{\mathbf{z}},\boldsymbol{\tau}) t_4(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_5(\vec{\mathbf{z}},\boldsymbol{\tau}) t_9(\vec{\mathbf{z}},\boldsymbol{\tau}) t_{13}(\vec{\mathbf{z}},\boldsymbol{\tau})}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})^6},\\
Y_{1,2}Y_{2,3} &= \frac{t_1(\vec{\mathbf{z}},\boldsymbol{\tau}) t_4(\vec{\mathbf{z}},\boldsymbol{\tau}) t_5(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_9(\vec{\mathbf{z}},\boldsymbol{\tau}) t_{12}(\vec{\mathbf{z}},\boldsymbol{\tau})}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})^6},
\end{aligned}$$

[2] Alternatively, see example [9, Exemple 5.2.2] from Cosset's PhD thesis.

$$Y_{1,3}Y_{2,3} = \frac{t_4(\vec{\mathbf{z}},\boldsymbol{\tau})t_5(\vec{\mathbf{z}},\boldsymbol{\tau})t_9(\vec{\mathbf{z}},\boldsymbol{\tau})^2 t_{12}(\vec{\mathbf{z}},\boldsymbol{\tau})t_{13}(\vec{\mathbf{z}},\boldsymbol{\tau})}{t_0(\vec{\mathbf{z}},\boldsymbol{\tau})^6}.$$

Notice that the expressions for the $Y_{i,j}^2$ are in terms of squares of theta functions. By [9, Exemple 5.2.2], the products of the form $Y_{i,j}Y_{i,k}$ can be expressed in terms of theta constants and squares of theta functions as follows:

$$\begin{aligned}
Y_{1,2}Y_{1,3} &= \frac{\vartheta_0^4\vartheta_1^4\vartheta_2^4\vartheta_3^2\vartheta_8^4\vartheta_9^4\vartheta_{15}^2}{\vartheta_4^{10}\vartheta_6^8\vartheta_{12}^{10}} \cdot \vartheta_0\vartheta_4\vartheta_8\vartheta_{12} \cdot \frac{\theta_{10}^2}{\theta_{14}^6} \cdot \theta_3\theta_7\theta_{11}\theta_{15} \\
Y_{1,2}Y_{2,3} &= \frac{\vartheta_0^4\vartheta_1^4\vartheta_2^4\vartheta_3^2\vartheta_8^4\vartheta_9^4\vartheta_{15}^2}{\vartheta_4^{10}\vartheta_6^8\vartheta_{12}^{10}} \cdot \vartheta_1\vartheta_4\vartheta_9\vartheta_{12} \cdot \frac{\theta_{11}^2}{\theta_{14}^6} \cdot \theta_2\theta_7\theta_{10}\theta_{15} \\
Y_{1,3}Y_{2,3} &= \frac{\vartheta_0^4\vartheta_1^4\vartheta_2^2\vartheta_3^2\vartheta_8^4\vartheta_9^4\vartheta_{15}^4}{\vartheta_4^{10}\vartheta_6^8\vartheta_{12}^{10}} \cdot \vartheta_0\vartheta_1\vartheta_8\vartheta_9 \cdot \frac{\theta_7^2}{\theta_{14}^6} \cdot \theta_2\theta_3\theta_{10}\theta_{11}
\end{aligned}$$

We have now seen that $u_0, u_1, v_0^2, v_0v_1, v_1^2$ can be expressed in terms of sums of quotients of the form

$$\prod_{(\vec{\mathbf{i_1}},\vec{\mathbf{i_2}})\in\mathcal{I}} \frac{\vartheta\left[\vec{\mathbf{i_1}}\right](\boldsymbol{\tau})}{\vartheta\left[\vec{\mathbf{i_2}}\right](\boldsymbol{\tau})} \prod_{(\vec{\mathbf{j_1}},\vec{\mathbf{j_2}})\in\mathcal{J}} \frac{\theta\left[\vec{\mathbf{j_1}}\right](\vec{\mathbf{z}},\boldsymbol{\tau})}{\theta\left[\vec{\mathbf{j_2}}\right](\vec{\mathbf{z}},\boldsymbol{\tau})}$$

where

$$\mathcal{I},\mathcal{J} \subseteq \frac{1}{2}\mathbb{Z}^4 \times \frac{1}{2}\mathbb{Z}^4.$$

3 An explicit abelian extension containing the Hilbert class field

For any number field K and any positive integer m, let $E_K(m)$ be the smallest subfield of the ray class field $H_K(m)$ such that $E_K(m) \supseteq K$ and $\mathrm{Gal}(H_K(m)/E_K(m))$ is of exponent at most 2. The main result of this chapter is as follows.

Theorem 3.1. Let K be a number field without real embeddings. Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that

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

Let

$$P_S = \{p : p \text{ is a rational prime below } \mathfrak{p} \text{ for some } \mathfrak{p} \in S\}$$

and

$$m_S = 4 \cdot \prod_{p \in P_S} p.$$

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

This result is generalized later as Theorem 3.21.

The existence of a positive integer m such that $H_K(1) \subseteq E_K(m)$ was already known by Shimura, via the proof of [30, Theorem 2]. Theorem 3.1 gives a formula for such an m thereby making Shimura's result effective.

We state a result of Shimura [30] which was later refined by Streng [34].

Theorem 3.2 ([34, Theorem I.10.3]). Let (K^r, Φ^r) be the reflex of a primitive quartic CM pair (K, Φ) and let m be a positive integer. Then the Galois group

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

is abelian of exponent at most 2. Equivalently, we have

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

There is also an analogous result [34, Theorem I.10.5] when K is not primitive.

When $m = 1$, Theorem 3.2 gives us a field that is 'close' but not necessarily equal to the Hilbert class field $H_{K^r}(1)$. In particular, the theorem tells us that the field $H_{K^r}(1)$ is obtained by adjoining to $H_{K_0^r}(1)\,\mathrm{CM}_{K^r,\Phi^r}(1)$ square roots of elements from this field.

One can determine which square roots must be added using a generic algorithm given by Kummer theory. However, the Kummer theory algorithm requires the computation of ray class groups of the compositum $H_{K_0^r}(1)\,\mathrm{CM}_{K^r,\Phi^r}(1)$. Algorithms to compute class groups are known to not perform very well [1, page 3] for large-degree number fields.

Using Theorems 3.1 and 3.2, we find that the Hilbert class field is contained in $H_{K_0^r}(m)\,\mathrm{CM}_{K^r,\Phi^r}(m)$ for some explicit positive integer m.

Before we formally state this result, we first fix the following notation. Suppose that m is an integer and that (K, Φ) and (K^r, Φ^r) are as in the assumptions of Theorem 3.2. We denote by $(\star_m)$ the expression

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

Corollary 3.3. Let (K^r, Φ^r) be the reflex of a primitive quartic CM pair (K, Φ) and m_S be as in Theorem 3.1. Then $(\star_{m_S})$ holds.

Proof. Theorem 3.2 gives

$$H_{K^r}(1) \;\subseteq\; E_{K^r}(m_S)$$

and Theorem 3.1 gives

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

□

Using this corollary, one can compute

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

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

Later on in the introduction of the next chapter, Chapter 4, we explain how to compute $H_{K_0^r}(m_S)\,\mathrm{CM}_{K^r,\Phi^r}(m_S)$ using CM theory and Stark's conjectures. Our method only requires that we compute ray class groups of number fields with degree at most 4. Therefore, we avoid the aforementioned problem of computing class groups of large degree fields. Of course, if the integer m_S is too large, we might end up working with large ray class fields. In Section 3.2, we discuss an algorithm to possibly find a smaller integer m for which $(\star_m)$ holds.

Finally, note that one may use any other field containing $H_{K^r}(1)$ to compute $H_{K^r}(1)$, so long as we can determine how the Galois automorphisms act.

We prove Theorem 3.1 in Section 3.1. In applications, we find that m_S might be too large. In Section 3.2, we address this issue by showing how to determine whether or not $(\star_m)$ holds given a positive integer m.

3.1 Proof of the main theorem

The aim of this section is to prove Theorem 3.1, which gives a formula to find an integer m such that $(\star_m)$ holds. In Section 3.1.1, we find out why the set P_S is chosen as such. In Section 3.1.2, we see how to use the primes in the set P_S to 'construct' an integer satisfying the properties promised in Theorem 3.1.

3.1.1 Embedding problems

We state a result of Richter used in Shimura's original proof [30, Proof of Theorem 2].

> **Lemma 3.4.** Let a be a non-negative integer. Let K be a totally imaginary number field. Let L/K be an unramified cyclic Galois extension of degree 2^a. Then there exists a cyclic Galois extension M/K of degree 2^{a+1} which contains L.

Even though Lemma 3.4 is a special case of [23, Satz 1b], we prove it here to keep thing self-contained. The proof concerns *embedding problems*, which we define in this section.

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

$$1 \to A \xrightarrow{\iota} E \xrightarrow{\pi} G \to 1 \tag{3.5}$$

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

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

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

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

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(M/L) \arrow[r] \arrow[d] & \mathrm{Gal}(M/K) \arrow[r] \arrow[d, "\phi"'] & G \arrow[r] \arrow[d, "\mathrm{id}_G"'] & 1 \\
1 \arrow[r] & A \arrow[r, "\iota"] & E \arrow[r, "\pi"] & G \arrow[r] & 1.
\end{tikzcd}$$

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

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

$$(\varepsilon_{2,a}) \qquad 1 \to C_2 \to C_{2^{a+1}} \to G \to 1.$$

by $(\varepsilon_{2,a})$. This central group extension is unique up to non-unique isomorphism.

Example 3.6. Take L/K to be $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ and denote its Galois group by G.

1. The embedding problem $(L/K, \varepsilon_{2,1})$ has $\mathbb{Q}(\zeta_5)$ as a solution.
2. The embedding problem $(L/K, \varepsilon)$ in which ε is of the form

$$1 \to C_2 \to C_2 \times C_2 \to G \to 1$$

has $\mathbb{Q}(\sqrt{5}, i)$ as a solution.

A global embedding problem $(L/K, \varepsilon)$ has one or more associated local embedding problems for each place of L as we will see in the next few paragraphs.

Let $(L/K, \varepsilon)$ be a global embedding problem where ε is an exact sequence

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

Let w be a place of L over a place v of K and denote by $\widetilde{G}$ the decomposition group $D(w/v)$, which is the Galois group of L_w/K_v. Let $\widetilde{E}$ be a subgroup of E such that

$$\pi(\widetilde{E}) = \widetilde{G}. \tag{3.7}$$

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

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

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

We now go through an example concerning two local embedding problems induced by the same global embedding problem with respect to the same (archimedean) place but for different subgroups $\tilde{E}$ of E.

Example 3.8. Let L/K be $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ with Galois group $\mathrm{Gal}(L/K)$. Consider the embedding problem $(L/K, \varepsilon_{2,1})$. Recall that $(\varepsilon_{2,1})$ is the exact sequence

$$1 \to C_2 \to C_4 \to C_2 \to 1.$$

Let w be a real place of $\mathbb{Q}(\sqrt{5})$ over the unique (real) archimedean place v of $\mathbb{Q}$. Note that $L_w = \mathbb{R}$ and $K_v = \mathbb{R}$ and the decomposition group $D(w/v) = \widetilde{G}$ is trivial. The subgroups of C_4 which satisfy (3.7) are exactly the trivial group and the unique subgroup of order 2.

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

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

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

Lemma 3.9 (Richter, [22, Satz 5])**.** If a global embedding problem $(L/K, \varepsilon)$ is solvable, then for each place w of L there exists a subgroup $\widetilde{E}$ of E such that the local embedding problem with respect to w and $\widetilde{E}$ is solvable.

The following example applies Lemma 3.9 to show that $\mathbb{Q}$ has no cyclic field extension of degree 4 containing $\mathbb{Q}(\sqrt{-5})$.

Example 3.10. Let L/K be $\mathbb{Q}(\sqrt{-5})/\mathbb{Q}$. Let w be the complex place of L, which is above the unique (real) archimedean place v of $\mathbb{Q}$.

The decomposition group $D(w/v)$ in this case is of order 2. Consider the embedding problem $(L/K, \varepsilon_{2,1})$ where ε_2 is the exact sequence

$$1 \to C_2 \to C_4 \to C_2 \to 1.$$

Take $\widetilde{E} = E = C_4$, and note that this is the only subgroup of E which satisfies

(3.7). There does not exist a number field M' such that $\mathrm{Gal}(M'/\mathbb{R}) \cong \widetilde{E} = C_4$. So, this induced local embedding problem is not solvable. Moreover, since C_4 is the only subgroup of E satisfying (3.7), this is the only induced local embedding problem and hence all induced local problems are not solvable. As all valid candidates of $\widetilde{E}$ result in a local problem which is not solvable, there does not exist a cyclic field extension of $\mathbb{Q}$ of degree 4 which contains $\mathbb{Q}(\sqrt{-5})$.

The following shows that if a number field K has no real embeddings, then for each archimedean place w of K there exists an induced local embedding problem with respect to w which is solvable.

Example 3.11. If K has no real embeddings, then all its archimedean places are complex and hence $\widetilde{G}$ is always trivial. In this case, taking the trivial group is the only valid choice for $\widetilde{E}$. Hence, for each *archimedean* place w of L, the global embedding problem $(L/K, \varepsilon)$ induces a local embedding problem with respect to w which is solvable.

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

Lemma 3.12 ([22, Satz 6])**.** Let ℓ be a prime and let m, n, u be positive integers. Let K be a nonarchimedean local field of characteristic 0 with unique prime ideal $\mathfrak{p}$. Suppose that K contains the ℓ^u-th roots of unity, but not all ℓ^{u+1}-th roots of unity. Let L be a cyclic extension of K of degree ℓ^n. Then, there exists a Galois extension M of K containing L such that $\mathrm{Gal}(M/K) = C_{\ell^{m+n}}$ if and only if at least one of the following is true:

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

- $u \geq n + m$
- $0 < u < n + m$ and $\zeta_{\ell^{\min(u,m)}} \in N_{L/K}(L)$.

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

Lemma 3.13. For any non-negative integer a and any cyclic field extension L/K of degree 2^a, the global embedding problem $(L/K, \varepsilon)$ is solvable if and only if for every place w of L, the unique induced local embedding problem is solvable.

Proof. This is a special case of [22, Satz 9] obtained by substituting ℓ, m, and n with 2, 1, and a, respectively, and noticing that the condition $B(2)$, defined in [22, Definition 3], is trivially satisfied. □

Finally, we end this subsection with a proof of Lemma 3.4.

Proof of Lemma 3.4. When $a = 0$, the field $K = L$. Let ε be any generator of the unit group O_K. The field $K(\sqrt{\varepsilon})$ is a cyclic Galois extension of degree 2^1 which contains $L = K$.

Let a be a positive integer. We are interested in the solvability of the embedding problem $(L/K, \varepsilon)$ where ε is of the form $1 \to C_2 \to C_{2^{a+1}} \to G \to 1$, where the group G is equal to $\mathrm{Gal}(L/K) = C_{2^a}$. If we show that the global embedding problem is solvable, then we will have proven the lemma. Since K has no real embeddings, each archimedean place has a local embedding problem which is solvable thanks to Example 3.11. Now, since L/K is unramified, we may use Lemma 3.12 to show that each nonarchimedean place has a local embedding problem which is solvable. Finally, using Lemma 3.13, we find that since each place of K has an induced local embedding problem which is solvable, then the global embedding problem is solvable. □

3.1.2 An explicit integer

The following result of Crespo is one of the key ingredients in the proof of our main result.

Theorem 3.14 ([11, Theorem 6])**.** Let n be a positive integer, and let A be an abelian group of exponent n. Let S be a finite set of prime ideals of $\mathcal{O}_K$ which contains the prime ideals dividing n.

Let K be a number field and let L/K be a Galois extension of K, with Galois group $G = \mathrm{Gal}(L/K)$, unramified outside S.

For each prime number p dividing n, we denote by a_p the p-rank of A, by r_p the p-rank of $\mathrm{Hom}(G, A)$. Moreover, let $\delta_p = 0$ if K contains a primitive $p^{\mathrm{ord}_p(n)}$ - th root of unity and $\delta_p = 1$ if it does not.

Suppose that

1. the order h_S of the group $\mathrm{Cl}_{K^r}(1)/\langle S\rangle$ is coprime to n, and
2. for every prime number $p \mid n$, we have $r_p + a_p + \delta_p < \#S$.

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

Given a finite abelian extension L/K, we denote its conductor, as defined in [6, Chapter 2], by $\mathfrak{f}_{L/K}$. One key property of the conductor that we use is that it is the minimal modulus $\mathfrak{m}$ such that $H_K(\mathfrak{m}) \supseteq L$.

Lemma 3.15. Let a be a non-negative integer. Let K be a number field with no real embeddings. Let L/K be an unramified cyclic Galois extension of degree 2^a. Let S be a finite set of prime ideals of K such that

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

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

Proof. Lemma 3.4 shows that the embedding problem $(L/K, \varepsilon_{2,a})$ is solvable. Keeping the notation of Theorem 3.14, the 2-rank a_2 of $A = C_2$ for this embedding problem is 1. Moreover, $\mathrm{Hom}(\mathrm{Gal}(L/K), C_2) \cong C_2$ and hence $r_2 = 1$. Finally $\delta_2 = 0$

since K contains the second roots of unity. Using Theorem 3.14, we prove the lemma.

□

Denote by $\mathfrak{d}_{L/K}$ the relative discriminant ideal of a field extension L/K, as defined in [6, Chapter 2, Section 2.4] and in [20, Section III.2.8].

We now state the following lemma.

Lemma 3.16 (Cohen, [6, Proposition 3.3.21])**.** Let L/K be an abelian extension of degree n Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ such that $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_{L/K}) \neq 0$. Finally, let ℓ be the prime number below $\mathfrak{p}$.

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

From Lemma 3.16, we conclude that since 2 is the only prime divisor of $[M : L]$, with M, L as in Lemma 3.15, then for a prime ideal $\mathfrak{P}$ of L not above 2, we have

$$\mathrm{ord}_{\mathfrak{P}}(\mathfrak{f}_{M/L}) \leq 1.$$

Using [6, Corollary 10.1.24] gives us the bound $\mathrm{ord}_{\mathfrak{P}_2}(\mathfrak{f}_{M/L}) \leq 2e(\mathfrak{P}_2/2) + 1$ for any $\mathfrak{P}_2$ above 2, where $e(\mathfrak{P}_2/2)$ is the ramification index of $\mathfrak{P}_2$ over 2. To summarize, for any prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$, we have:

$$\mathrm{ord}_{\mathfrak{P}}(\mathfrak{f}_{M/L}) \leq \begin{cases} 2e(\mathfrak{P}/2) + 1 & \text{if } \mathfrak{P} \mid 2 \\ 1 & \text{if } \mathfrak{P} \nmid 2. \end{cases} \tag{3.17}$$

Proposition 3.18, below, enables us to bound the valuation of $\mathfrak{f}_{M/K}$ at the primes $\mathfrak{p}$ of $\mathcal{O}_K$ using the bounds on the valuations of $\mathfrak{f}_{M/L}$ at the primes $\mathfrak{P}$ of $\mathcal{O}_L$.

Proposition 3.18. Let K be a number field and let L be an unramified extension of K of degree 2^a. Let M be a cyclic extension of K of degree 2^{a+1} which contains L. Let $\mathfrak{p}$ be an ideal of $\mathcal{O}_K$.

Let c be an integer and suppose $\mathrm{ord}_{\mathfrak{P}}(\mathfrak{f}_{M/L}) \leq c$ for every prime ideal $\mathfrak{P}$ of $\mathcal{O}_L$

above $\mathfrak{p}$. Then

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

Proof. Note that

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

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

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

Let g be the number of prime ideals $\mathfrak{P}$ of $\mathcal{O}_L$ above $\mathfrak{p}$. For each of these g prime ideals, the norm $N_{L/K}(\mathfrak{P})$ is given by the residue class degree $f = [\mathcal{O}_L/\mathfrak{P} : \mathcal{O}_K/\mathfrak{p}]$. Hence, we have $\sum_{\mathfrak{P}|\mathfrak{p}} \mathrm{ord}_{\mathfrak{p}}(N_{L/K}(\mathfrak{P})) = fg$. Now, since L/K is unramified, we have $2^a = [L : K] = fg$. Corollary III.2.10 of [20] states that for a tower of fields $K \subseteq L \subseteq M$ one has

$$\mathfrak{d}_{M/K} = \mathfrak{d}_{L/K}^{[M:L]} N_{L/K}(\mathfrak{d}_{M/L}). \tag{3.19}$$

The conductor-discriminant formula [20, Section VII.11.9] gives us

$$\mathfrak{d}_{M/L} = \mathfrak{f}_{M/L}, \qquad \mathfrak{d}_{M/K} = \mathfrak{f}_{M/K}^{2^a} \tag{3.20}$$

Combining (3.19), (3.20) and the fact that $\mathfrak{d}_{L/K} = 1$ since L/K is unramified, we obtain

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

And thus

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

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

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

Theorem 3.21. Let K be a number field without real embeddings. Let S be a finite set of prime ideals of $\mathcal{O}_K$ such that

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

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

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

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

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

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

by Galois theory. Fix an $i \in \{1, \ldots, t\}$. Since L_i/K is an unramified cyclic number field extension of degree 2^{a_i}, Lemma 3.15 gives us the existence of a field extension M_i of K containing L_i which is cyclic of degree 2^{a_i+1} and is unramified outside S. Let $\mathfrak{P}_i$ be a prime ideal of $\mathcal{O}_{L_i}$ above a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, and a rational prime ℓ. Since L_i/K is unramified, we find that

$$e(\mathfrak{P}/\ell) = e(\mathfrak{P}/\mathfrak{p})e(\mathfrak{p}/\ell) = e(\mathfrak{p}/\ell).$$

Proposition 3.18 and (3.17) then tell us that

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

Since the conductor of a compositum of fields divides the least common multiple of the conductors of the fields being composed, the field $L_0 M_1 \cdots M_t$ has a conductor which divides

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

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

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

Let $\sigma \in \boldsymbol{G}_{E_K}(\mathfrak{m})$ and note that $\sigma^2 = \mathrm{id}$. Note that $[\boldsymbol{G}_K : \boldsymbol{G}_{L_0}]$ is an odd integer and hence $\sigma \in \boldsymbol{G}_{L_0}$. On the other hand, for each $i \in \{1, \ldots, t\}$, since $\sigma^2 = \mathrm{id} \in \boldsymbol{G}_{M_i}$ then by definition of M_i, $\sigma \in \boldsymbol{G}_{L_i}$. Hence σ fixes $L_0 L_1 \cdots L_t = H_K(1)$. And therefore $\sigma \in \boldsymbol{G}_{H_K(1)}$. □

The smallest positive integer m contained in $\mathfrak{m}$ is given by $m = 4P$ where P is the product of all primes p such that p is below some $\mathfrak{p} \in S$. With this observation and the fact that $E_K(\mathfrak{m}) \subseteq E_K(\mathfrak{n})$ when $\mathfrak{m} \mid \mathfrak{n}$, Theorem 3.1 becomes a direct consequence of Theorem 3.21.

3.2 A decision problem

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

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

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

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

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

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

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

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

$$\pi_m : \mathrm{Cl}_{K^r}(m) \longrightarrow \mathrm{Cl}_{K^r}(1). \tag{3.22}$$

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

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

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

$$\eta = N_{K/K_0} : \mathrm{Cl}_{K^r}(m) \longrightarrow \mathrm{Cl}_{K_0^r}(m). \tag{3.23}$$

We can also compute the Galois group $\boldsymbol{G}(\, \mathrm{CM}_{K^r,\Phi^r}(m)\,)$ as a kernel of a map r which we define in Section 3.2.1. The codomain of r is the Shimura class group studied in [3, Section 3.1]. We generalize this Shimura class group by defining, in the same section, the Shimura *ray* class group of K for a modulus m, which we denote by $\mathfrak{C}_K(m)$.

Section 3.2.2 details how we can extract and use information about the group $\mathfrak{C}_K(m)$ to determine whether or not $(\star\star_m)$ holds for the given integer m.

3.2.1 The Shimura ray class group

Let (K, Φ) be a CM pair and (K^r, Φ^r) its reflex pair. The Shimura class group of K, in conjunction with a group morphism involving the type norm map, was used in [13, Section 2.2] to compute the Galois group $\mathrm{Gal}(H_{K^r}(1)/\mathrm{CM}_{K^r,\Phi^r}(1))$. This section generalizes the Shimura class group and introduces the concept of a *Shimura ray class group* for each modulus $\mathfrak{m}$ of K. We define it as follows.

Definition 3.24 (Shimura ray class group for the modulus $\mathfrak{m}$)**.** Let $\mathfrak{m}$ be a modulus of a CM field K. The Shimura ray class group $\mathfrak{C}_K(\mathfrak{m})$ is the group given by

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

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

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

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

$$\begin{aligned} r : \mathrm{Cl}_{K^r}(m) &\to \mathfrak{C}_K(m) \\ [\mathfrak{b}] &\mapsto [\big(N_{\Phi^r}(\mathfrak{b}), N_{K^r/\mathbb{Q}}(\mathfrak{b})\big)]. \end{aligned} \tag{3.25}$$

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

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

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

Example 3.26. Let K be a primitive quartic CM field different from $\mathbb{Q}(\zeta_5)$. Dirichlet's unit theorem gives us

$$\mathcal{O}_{K_0}^\times = \langle -1 \rangle \times \langle \varepsilon_0 \rangle$$

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

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

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

$$s : \mathcal{O}_K^\times \to (\mathcal{O}_K/\mathfrak{m})^\times . \tag{3.27}$$

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

element. Thus, the norm $N_{K/K_0} : K \to K_0$ induces maps

$$N_1 := N_{K/K_0} : \mathcal{O}_{K,\mathfrak{m},1}^{\times} \to \mathcal{O}_{K_0}^{\times\,+} \quad : \quad x \mapsto x\bar{x}. \tag{3.28}$$

and

$$N_2 := N_{K/K_0} : \mathrm{Cl}_K(\mathfrak{m}) \to \mathrm{Cl}_{K_0}^{+}(1) \quad : \quad [\mathfrak{a}] \mapsto [\mathfrak{a}\bar{\mathfrak{a}}]. \tag{3.29}$$

We define the maps f and g as follows

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

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

Lemma 3.30. The sequence

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

is exact. Consequently, the sequence

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

is exact.

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

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

hence $u \in \mathcal{O}_{K_0}^{\times\,+}$. Since

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

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

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

3.2.2 An algorithm to answer the decision problem

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

We have established in Section 3.2.1 that $\ker r$ is exactly $I_{K^r,\Phi^r}(m)/P_{K^r}(m)$, which is isomorphic to $\mathrm{Gal}(H_{K^r}(m)/\mathrm{CM}_{K^r,\Phi^r}(m))$ via the Artin map. Recall the functions π_m and η defined in (3.22) and (3.23), respectively. We have the following isomorphisms via the Artin map:

$$\begin{aligned}
\mathrm{Gal}(H_{K^r}(m)/H_{K^r}(1)) &\cong \ker \pi_m = \ker(\mathrm{Cl}_{K^r}(m) \xrightarrow{\pi_m} \mathrm{Cl}_{K^r}(1)),\\
\mathrm{Gal}(H_{K^r}(m)/H_{K_0^r}(m)) &\cong \ker \eta = \ker(\mathrm{Cl}_{K^r}(m) \xrightarrow{\eta} \mathrm{Cl}_{K_0^r}(m)),\\
\mathrm{Gal}(H_{K^r}(m)/\mathrm{CM}_{K^r,\Phi^r}(m)) &\cong \ker r = \ker(\mathrm{Cl}_{K^r}(m) \xrightarrow{r} \mathfrak{C}_K(m)).
\end{aligned} \tag{3.31}$$

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

$$\ker \pi_m \supseteq \ker \eta \cap \ker r. \tag{3.32}$$

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

> **Algorithm 3.33.** INPUT. A primitive quartic CM pair (K, Φ) with reflex (K^r, Φ^r) and a positive integer m.

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

We remark that we have not yet covered how to compute the above groups, much less their kernels and intersections. This discussion is postponed to Chapter 5, where we have collected these algorithms.

4 Computing abelian extensions generated by CM theory

Let (K, Φ) be a primitive quartic CM pair with $K \not\cong \mathbb{Q}(\zeta_5)$ and let (K^r, Φ^r) be its reflex.

In Chapter 3, we made Shimura's theorems explicit and found an integer m for which

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

consistently referred to in this thesis as $(\star_m)$, holds.

The compositum on the right hand side consists of two parts, a ray class field for the modulus m of the real quadratic subfield K_0^r of K^r, and $\mathrm{CM}_{K^r,\Phi^r}(m)$. In this chapter, we compute $\mathrm{CM}_{K^r,\Phi^r}(m)$. Algorithms to compute the ray class field $H_{K_0^r}(m)$ can be found in a series of articles by Roblot [26, 24, 25], see also [7]. These algorithms are implemented in PARI/GP [21] as `bnrstark`.

Note that one may use the Cardona-Quer invariants (see Example 2.19) in order to compute $\mathrm{CM}_{K^r,\Phi^r}(1)$. When $m = 2$, we have seen in Theorem 2.22 that $\mathrm{CM}_{K^r,\Phi^r}(2)$ can be computed in terms of Rosenhain invariants.

Beyond $m = 2$, however, we only know from Theorem 2.20 that there exists a map h that gives $\mathrm{CM}_{K^r,\Phi^r}(m)$, but at this point, this map h has not been made explicit. We sidestep this problem in Section 4.1 by proving the following result:

$$\mathrm{CM}_{K^r,\Phi^r}(m) = \mathrm{CM}_{K^r,\Phi^r}(2)(h_2(t))$$

when $2 \mid m$ for some map h_2 we define in the same section. We compute this map h_2 explicitly in Section 4.2. Finally, in Section 4.3, we find an appropriate torsion point t, and a way to find the conjugates of $h_2(t)$, and conclude by giving an algorithm to

compute $\mathrm{CM}_{K^r,\Phi^r}(m)$ when $2 \mid m$. For the cases where $2 \nmid m$, we compute the Galois extension $\mathrm{CM}_{K^r,\Phi^r}(2m)/K^r$ and then use the action of the Galois group to find its subfield $\mathrm{CM}_{K^r,\Phi^r}(m)$.

4.1 Abelian extensions in terms of Kummer varieties

In this section, we express $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$, for some reflex pair (K^r, Φ^r) of a primitive quartic CM pair (K, Φ) and an ideal $\mathfrak{m}$ of K, in terms of a map h_2 involving a Kummer variety, evaluated at a primitive $\mathfrak{m}$-torsion point.

Theorem 2.20 tells us that computing $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ is equivalent to computing the field $\mathrm{CM}_{K^r,\Phi^r}(1)$ and a *normalized* Kummer variety (W, h). However, a map $h_2(t)$, satisfying weaker conditions compared to $h(t)$, can be used to compute $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ when $2 \mid \mathfrak{m}$.

Theorem 4.1. Let (K^r, Φ^r) be the reflex pair of a primitive quartic CM pair (K, Φ), as in Theorem 2.20. Let (J, ι, C) be a principally polarized abelian surface over $\mathrm{CM}_{K^r,\Phi^r}(2)$ with complex multiplication by K. Let (W_2, h_2) be a (not necessarily normalized) Kummer variety[a] of (J, C). Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ such that $2 \mid \mathfrak{m}$. Let t be a primitive $\mathfrak{m}$-torsion point of J.

Then

$$\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) = \mathrm{CM}_{K^r,\Phi^r}(2)(h_2(t)).$$

[a] By definition of a Kummer variety, both W_2 and h_2 are defined over $\mathrm{CM}_{K^r,\Phi^r}(2)$.

Proof. Let (W, h) be a normalized Kummer variety of (J, C).

First, we show that

$$\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) = \mathrm{CM}_{K^r,\Phi^r}(2)(h(t)).$$

Since $\mathrm{CM}_{K^r,\Phi^r}(1) \subseteq \mathrm{CM}_{K^r,\Phi^r}(2)$, we have $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) \subseteq \mathrm{CM}_{K^r,\Phi^r}(2)(h(t))$. Indeed, by Theorem 2.20, the field $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ is equal to $\mathrm{CM}_{K^r,\Phi^r}(1)(h(t))$ and

$$\mathrm{CM}_{K^r,\Phi^r}(1)(h(t)) \subseteq \mathrm{CM}_{K^r,\Phi^r}(2)(h(t)).$$

On the other hand,

$$\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) \supseteq \mathrm{CM}_{K^r,\Phi^r}(2)(h(t))$$

because $h(t) \in \mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ and $2 \mid \mathfrak{m}$ implies $\mathrm{CM}_{K^r,\Phi^r}(2) \subseteq \mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$. Hence

$$\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) = \mathrm{CM}_{K^r,\Phi^r}(2)(h(t)).$$

Now, we want to show that

$$\mathrm{CM}_{K^r,\Phi^r}(2)(h(t)) = \mathrm{CM}_{K^r,\Phi^r}(2)(h_2(t)). \tag{4.2}$$

Since (W, h) and (W_2, h_2) are both Kummer varieties of (J, C), there is a unique isomorphism $\varphi : W \to W_2$ over $\mathrm{CM}_{K^r,\Phi^r}(2)$ such that $h_2 = \varphi \circ h$. Hence, the element $h(t)$ can be expressed in terms of rational functions in $h_2(t)$ with coefficients in $\mathrm{CM}_{K^r,\Phi^r}(2)$ and vice-versa. This proves (4.2) and finishes the proof of this theorem. □

Despite the fact that this theorem assumes $2 \mid \mathfrak{m}$, we can still use this result to compute $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{n})$ when $2 \nmid \mathfrak{n}$. We do this by first computing $\mathrm{CM}_{K^r,\Phi^r}(2\mathfrak{n})$ and then using Galois theory to compute its subfield $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{n})$.

4.2 A Kummer variety over $\mathrm{CM}_{K^r,\Phi^r}(2)$

Let (J, ι, C) be the Jacobian, with complex multiplication by a primitive quartic CM field $K \not\cong \mathbb{Q}(\zeta_5)$, of a hyperelliptic curve C over a field $k \subseteq \mathbb{C}$ with an affine model as in (2.4). We again denote its unique point at infinity by ∞.

The quotient variety of (J, C) by the (finite) automorphism group

$$G = \mathrm{Aut}_{\bar{k}}(J, C) = \langle [-1] \rangle$$

exists by [15, Theorem A.8.3.2], and the proof shows us that it is obtained by gluing together quotient varieties of an open affine cover of J as follows.

Let $\mathcal{J} = \{J_i : i \in \mathcal{I}\}$ be an open affine cover of J where the J_i are G-invariant and where $\mathcal{I}$ is an index set. Denote by $A_i := k[J_i]$ the ring of regular functions of the subvariety J_i. Let $A_i^G = \{a \in A : [-1]^*(a) = a\}$ be the k-subalgebra of A_i fixed

by G. Because the category of affine varieties is equivalent to the category of finitely generated k-algebras, we denote by W_i an affine variety such that $k[W_i] = A_i^G$ and denote by $h_i : J_i \longrightarrow W_i$ the morphism corresponding to the natural inclusion $A_i^G \hookrightarrow A_i$. The pair (W_i, h_i) is the quotient variety of the affine variety J_i by $\mathrm{Aut}_{\bar{k}}(J, C)$. The Kummer variety (W, h) of J is obtained by gluing the h_is, as shown in [15, Theorem A.8.3.1].

Recall $\Theta = \mathrm{RDiv}_0\, C \cup \mathrm{RDiv}_1\, C$, as we defined towards the end of Section 2.2.1). Without loss of generality, we may assume that one of the J_i is $J \setminus \Theta$. Indeed, if it is not part of the original open cover, we can replace the open cover $\mathcal{J}$ by $\mathcal{J} \cup \{J \setminus \Theta\}$.

The points of the affine variety $J \setminus \Theta$ are represented by divisors of C of the form

$$D = P_1 + P_2 - 2\infty,$$

where $P_1 \neq [-1]P_2$. Denote by (x_i, y_i) the coordinates of P_i. Such divisors can be represented by polynomials $(U_D, V_D) \in \mathrm{MumPol}_2(C)$. In other words, U_D is monic, $\deg U_D = 2$, $\deg V_D \leq 1$ and $U_D \mid V_D^2 - f$, as was defined in Section 2.2.1. Using the coefficients of the two polynomials, we may view (U_D, V_D) as an ordered 4-tuple $(u_0, u_1, v_0, v_1) \in \mathbb{A}^4(\bar{k})$.

The condition $U_D \mid V_D^2 - f$ is equivalent to having a remainder of 0 when $V_D^2 - f$ is divided by U_D. More explicitly, since

$$V_D^2 - f = U_D \cdot Q_D + R_D$$

with

$$\begin{aligned} Q_D(x) &= x^3 + (-u_1 + f_4)x^2 + (-u_0 + u_1^2 - u_1 f_4 + f_3)x \\ &\quad + 2u_0u_1 - u_0 f_4 - u_1^3 + u_1^2 f_4 - u_1 f_3 - v_1^2 + f_2 \\ R_D(x) &= r_1 x + r_0, \end{aligned}$$

where C is given by $y^2 = x^5 + f_4x^4 + f_3x^3 + f_2x^2 + f_1x + f_0$, and

$$\begin{aligned} r_1 &= u_0^2 - 3u_0u_1^2 + 2u_0u_1f_4 - u_0f_3 + u_1^4 - u_1^3f_4 + u_1^2f_3 + u_1v_1^2 - u_1f_2 - 2v_0v_1 + f_1 \\ r_0 &= -2u_0^2u_1 + u_0^2f_4 + u_0u_1^3 - u_0u_1^2f_4 + u_0u_1f_3 + u_0v_1^2 - u_0f_2 - v_0^2 + f_0. \end{aligned}$$

We find that $U_D \mid V_D^2 - f$ is equivalent to having the polynomials r_0, r_1 to be equal to 0.

Mumford [19, Chapter IIIa, Proposition 1.3], together with van Wamelen [35, page 3087], shows that r_0, r_1 generate a prime ideal I of $k[u_0, u_1, v_0, v_1]$ and we find that the ring $A := k[J \setminus \Theta]$ is given by

$$A := k[J \setminus \Theta] = \frac{k[u_0, u_1, v_0, v_1]}{I}. \tag{4.3}$$

Lemma 4.4. Let A be as in (4.3) and $G = \mathrm{Aut}_{\bar{k}}(J, C) = \langle [-1] \rangle$. We have

$$A^G = \frac{k[u_0, u_1, v_0^2, v_1^2, v_0 v_1]}{(r_0, r_1)}.$$

The natural inclusion $A^G \hookrightarrow A$ corresponds to the projection

$$\begin{aligned} h_{J\setminus\Theta} : J \setminus \Theta &\to \frac{J \setminus \Theta}{\langle [-1] \rangle} \\ (u_0, u_1, v_0, v_1) &\mapsto (u_0, u_1, v_0^2, v_1^2, v_0 v_1). \end{aligned}$$

Proof. Denote by R the polynomial ring $k[u_0, u_1, v_0, v_1]$ and denote by $R^{\pm}$ the set

$$R^{\pm} = \{r \in R : r^{\sigma} = \pm r\},$$

where $\sigma : (u_0, u_1, v_0, v_1) \mapsto (u_0, u_1, -v_0, -v_1)$ is the automorphism on $\mathbb{A}^4$ corresponding to applying $[-1]$ on (U_D, V_D). In other words,

$$r^{\sigma} = [-1] r = (u_0, u_1, -v_0, -v_1).$$

Consider the homomorphism $\varphi_1 : R \to R^+ \oplus R^-$ defined by

$$r \mapsto \left(\frac{r + r^{\sigma}}{2}, \frac{r - r^{\sigma}}{2} \right).$$

The homomorphism $\Sigma : R^+ \oplus R^- \to R$ of k-vector spaces, defined by

$$(r^+, r^-) \mapsto r^+ + r^-$$

satisfies $\Sigma \circ \varphi_1 = \mathrm{id}_R$ and $\varphi_1 \circ \Sigma = \mathrm{id}_{R^+ \oplus R^-}$. Hence, φ_1 is in fact an isomorphism of k-vector spaces.

Define $I^{\pm} := I \cap R^{\pm}$. The map φ_1 on R induces a map on $I \to I^+ \oplus I^-$ and using

the same argument for φ_1, we find that this induced map on I gives an isomorphism between the k-vector spaces I and $I^+ \oplus I^-$. There exist natural projections $\pi^\pm$ from $R^\pm$ to the quotient $R^\pm/I^\pm$. The map $(\pi^+ \oplus \pi^-) \circ \varphi_1$ is clearly surjective, and its kernel consists of the elements $r \in R$ such that $\frac{r \pm \sigma(r)}{2} \in I^\pm$. Hence,

$$\ker(\pi^+ \oplus \pi^-) \circ \varphi_1 = I$$

and the map $(\pi^+ \oplus \pi^-) \circ \varphi_1$ defines a k-vector space isomorphism between R/I and $R^+/I^+ \oplus R^-/I^-$.

In other words,

$$A = k[J \setminus \Theta] = R/I \cong R^+/I^+ \oplus R^-/I^-$$

and

$$A^G = k[J \setminus \Theta]^G = R^+/I^+.$$

Recall that $r \in R^+$ if and only if $r = r^\sigma$. Applying σ to a basis element

$$r = u_0^a u_1^b v_1^c v_2^d$$

of R (as a vector space), we find that $r = r^\sigma$ if and only if $c + d$ is even. Hence, as a ring, A^G is generated by u_0, u_1, v_0^2, v_1^2, and $v_0 v_1$. □

As the map h in the Kummer variety (W, h) of J is obtained by gluing the h_i-maps of the open affine varieties which cover J, we find that $h|_{J\setminus\Theta} = h_{J\setminus\Theta}$.

Now, let (K, Φ) and (K^r, Φ^r) be as in Theorem 4.1, with the additional condition that $K \not\cong \mathbb{Q}(\zeta_5)$. Let $\boldsymbol{\tau} \in \mathbb{H}_2$ and let (W_2, h_2) be a Kummer variety of the Jacobian (J, C), with complex multiplication by K, of the hyperelliptic curve $C_{\boldsymbol{\tau}}$ over

$$\mathbb{Q}(\lambda_i(\boldsymbol{\tau}) : i \in \{1, \ldots, 3\}),$$

where $C_{\boldsymbol{\tau}}$ is as in (2.21). Using Theorems 2.20 and 2.22 we find that

$$\mathbb{Q}(\lambda_i(\boldsymbol{\tau}) : i \in \{1, \ldots, 3\}) = \mathcal{M}(J_{\boldsymbol{\tau}}, C, J_{\boldsymbol{\tau}}[2]) = \mathrm{CM}_{K^r,\Phi^r}(2),$$

and so $C_{\boldsymbol{\tau}}$ is defined over $\mathrm{CM}_{K^r,\Phi^r}(2)$. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ such that $2 \mid \mathfrak{m}$ and let t be a primitive $\mathfrak{m}$-torsion point of J such that $t \in J \setminus \Theta$. Writing U_t

as $x^2 + u_{1,t}x + u_{0,t}$ and V_t as $v_{1,t}x + v_{0,t}$, from the above discussion, we have

$$\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) = \mathrm{CM}_{K^r,\Phi^r}(2)(u_{0,t},\ u_{1,t},\ v_{0,t}^2,\ v_{0,t}v_{1,t},\ v_{1,t}^2).$$

4.3 An algorithm for computing $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ with $2 \mid \mathfrak{m}$

In this section, we give an algorithm that computes $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ given the reflex pair (K^r, Φ^r) of a primitive quartic CM pair (K, Φ), with $K \not\cong \mathbb{Q}(\zeta_5)$, and an ideal $\mathfrak{m}$ of $\mathcal{O}_K$ such that $2 \mid \mathfrak{m}$.

We saw in Theorem 4.1 that it suffices to first compute $\mathrm{CM}_{K^r,\Phi^r}(2)$, which is expressible in terms of Rosenhain invariants, and then compute the map h_2 of a Kummer variety (W_2, h_2) of a simple principally polarized abelian surface (J, C) with complex multiplication by K.

The discussion in Section 4.2 shows that appending $h_2(t)$, where t is a primitive $\mathfrak{m}$-torsion point, is equivalent to adding the coefficients of the polynomials U_t and V_t^2 corresponding to the primitive $\mathfrak{m}$-torsion point t.

To find these polynomials, we first need to find a primitive $\mathfrak{m}$-torsion point t (Section 4.3.1). We then find conjugates of t (Section 4.3.2). Finally, we compute the polynomial whose roots are exactly these conjugates Section 4.3.3 in order to find a defining polynomial for the extension $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})/\mathrm{CM}_{K^r,\Phi^r}(2)$.

4.3.1 Finding a primitive torsion point

Given a torsion point $T \in J[\mathfrak{m}]$, we may define a morphism of $\mathcal{O}_K/\mathfrak{m}$-modules as follows:

$$\begin{aligned} \varphi_T : \mathcal{O}_K/\mathfrak{m} &\to J[\mathfrak{m}] \\ \alpha &\mapsto \iota(\alpha)T. \end{aligned}$$

The subgroups of the domain $\mathcal{O}_K/\mathfrak{m}$ of φ_T are exactly the groups $\mathfrak{n}/\mathfrak{m}$ where $\mathfrak{n}$ is an ideal of $\mathcal{O}_K$ containing $\mathfrak{m}$.

Lemma 4.5. Let (J, ι, C) be a principally polarized abelian surface with complex multiplication by a CM field K. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$. If $T \in J[\mathfrak{m}]$ and $T \notin J[\mathfrak{n}]$ for every ideal $\mathfrak{n} \supsetneq \mathfrak{m}$ of $\mathcal{O}_K$, then T is a primitive $\mathfrak{m}$-torsion point.

Proof. Suppose that $\mathfrak{n} \supsetneq \mathfrak{m}$ is an ideal of $\mathcal{O}_K$. If $T \notin J[\mathfrak{n}]$ for any such ideal $\mathfrak{n}$, then under the hypotheses of the lemma, the kernel of φ_T is trivial. Since $J[\mathfrak{m}]$ is a rank 1 module over $\mathcal{O}_K/\mathfrak{m}$ and both are finite groups, we can conclude that φ_T is an isomorphism. Then for every $T' \in J[\mathfrak{m}]$, there exists a unique $\alpha \in \mathcal{O}_K/\mathfrak{m}$ such that $\varphi(\alpha)T = T'$. This shows that T is actually a primitive $\mathfrak{m}$-torsion point. □

If we wanted to find a primitive $\mathfrak{m}$-torsion point of (J, ι, C) algebraically, we would need to write down the addition formulas and find division polynomials. Analytically, however, finding an $\mathfrak{m}$-torsion point is much simpler.

Suppose that the set of complex points of (J, ι, C) is complex analytically isomorphic to $\mathbb{C}^2/\Lambda$ and let $\vec{\mathbf{b}} := (b_1, b_2, b_3, b_4)$ be a basis of Λ. Let m be the smallest positive integer in $\mathfrak{m}$. We can express a point $T \in J[\mathfrak{m}]$ as a vector

$$\vec{\mathbf{a}} := (a_1/m,\ a_2/m,\ a_3/m,\ a_4/m) \in \frac{1}{m}\mathbb{Z}^4 \tag{4.6}$$

with respect to the chosen basis $\vec{\mathbf{b}}$ of Λ. Given an element $\alpha \in K$, the element $\iota(\alpha)T$ can then be expressed as the vector $M_\alpha\vec{\mathbf{a}}$, where M_α is the 4×4 matrix of the endomorphism $\iota(\alpha)$ with respect to $\vec{\mathbf{b}}$.

We first find an $\mathfrak{m}$-torsion point $T \in J[\mathfrak{m}]$, not necessarily primitive. We do this by first finding a random vector $\vec{\mathbf{a}} \in \frac{1}{m}\mathbb{Z}^4$ as in (4.6). This is clearly an m-torsion point. We may check if $\vec{\mathbf{a}}$ is in $J[\mathfrak{m}]$ by checking if the generators of $\mathfrak{m} = m_1\mathcal{O}_K + m_2\mathcal{O}_K$ send $\vec{\mathbf{a}}$ to an integer vector. In other words, if $M_{m_1}\vec{\mathbf{a}}$ and $M_{m_2}\vec{\mathbf{a}}$ are both integer vectors. If at least one of these vectors is not an integer vector, then $P \notin J[\mathfrak{m}]$ and we simply choose a different vector until we do find an $\mathfrak{m}$-torsion point.

Let $\mathfrak{n} \supsetneq \mathfrak{m}$ be an ideal of $\mathcal{O}_K$. Suppose that $\mathfrak{n} = n_1\mathcal{O}_K + n_2\mathcal{O}_K$. If either $M_{n_1}\vec{\mathbf{a}}$ or $M_{n_2}\vec{\mathbf{a}}$ has a non-integer entry, this means that $T \notin J[\mathfrak{n}]$. If for every $\mathfrak{n}$, at least one of the two ideal generators of $\mathfrak{n}$ sends $\vec{\mathbf{a}}$ to an vector with a non-integer entry, then by Lemma 4.5, we find that T is a primitive $\mathfrak{m}$-torsion point.

See Section 6.2.3 for an example.

4.3.2 Finding the conjugates of h_2

Let $\boldsymbol{\tau} \in \mathbb{H}_2$. Suppose $(J_{\boldsymbol{\tau}}, \iota, \mathcal{C})$ is the Jacobian, with complex multiplication by K, of the hyperelliptic curve $\mathcal{C}_{\boldsymbol{\tau}}$ (as defined in Section 2.3.1). Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ and let m be the smallest integer in $\mathfrak{m}$.

Let $T \in J(\mathcal{C}_{\boldsymbol{\tau}}) \setminus \Theta$ be a primitive $\mathfrak{m}$-torsion point of $(J, \iota, \mathcal{C})$. Suppose that the corresponding point of T in $\mathbb{C}^2/\Lambda_{\boldsymbol{\tau}}$ is $\vec{\mathbf{z}}$. In Section 2.3.2, we found formulas for the pair of Mumford polynomials $(U_{\vec{\mathbf{z}},\boldsymbol{\tau}}, V_{\vec{\mathbf{z}},\boldsymbol{\tau}}) := (U_P, V_P)$ in terms of van Wamelen's theta functions.

At the end of Section 4.2, we found that

$$\mathsf{CM}_{K^r,\Phi^r}(\mathfrak{m}) = \mathsf{CM}_{K^r,\Phi^r}(2)(\mathcal{H}_{\vec{\mathbf{z}},\boldsymbol{\tau}})$$

where

$$\mathcal{H}_{\vec{\mathbf{z}},\boldsymbol{\tau}} = \{u_0(\vec{\mathbf{z}},\boldsymbol{\tau}), u_1(\vec{\mathbf{z}},\boldsymbol{\tau}), v_0^2(\vec{\mathbf{z}},\boldsymbol{\tau}), (v_0v_1)(\vec{\mathbf{z}},\boldsymbol{\tau}), v_1^2(\vec{\mathbf{z}},\boldsymbol{\tau})\}.$$

Let $\alpha \in \mathcal{H}_{\vec{\mathbf{z}},\boldsymbol{\tau}}$. From Section 2.3.2, we know that α can be expressed as sum of quotients of the form

$$\prod_{(\vec{\mathbf{i}_1},\vec{\mathbf{i}_2})\in\mathcal{I}} \frac{\vartheta\left[\vec{\mathbf{i}_1}\right](\boldsymbol{\tau})}{\vartheta\left[\vec{\mathbf{i}_2}\right](\boldsymbol{\tau})} \prod_{(\vec{\mathbf{j}_1},\vec{\mathbf{j}_2})\in\mathcal{J}} \frac{\theta\left[\vec{\mathbf{j}_1}\right](\vec{\mathbf{z}},\boldsymbol{\tau})}{\theta\left[\vec{\mathbf{j}_2}\right](\vec{\mathbf{z}},\boldsymbol{\tau})}$$

where

$$\mathcal{I}, \mathcal{J} \subseteq \frac{1}{2}\mathbb{Z}^4 \times \frac{1}{2}\mathbb{Z}^4.$$

Writing the $\mathfrak{m}$-torsion point $\vec{\mathbf{z}}$ as $\boldsymbol{\tau}\vec{\mathbf{c}} + \vec{\mathbf{d}}$ with $\vec{\mathbf{c}}, \vec{\mathbf{d}} \in \frac{1}{m}\mathbb{Z}^2$, we may write α in terms of theta constants with characteristics in $\frac{1}{2m}\mathbb{Z}^4$ using the following formula

$$\theta\begin{bmatrix}\vec{\mathbf{a}}\\ \vec{\mathbf{b}}\end{bmatrix}(\boldsymbol{\tau}\vec{\mathbf{c}} + \vec{\mathbf{d}}, \boldsymbol{\tau}) = v \cdot \vartheta\begin{bmatrix}\vec{\mathbf{a}}+\vec{\mathbf{c}}\\ \vec{\mathbf{b}}+\vec{\mathbf{d}}\end{bmatrix}(\boldsymbol{\tau}) \tag{4.7}$$

derived from [9, Propriété 3.1.2, equation (3.2)], where v is an explicit $(2m)$th root of unity. Therefore α can be expressed as a sum of quotients of the form

$$v_Q \cdot \prod_{(\vec{\mathbf{q}_1},\vec{\mathbf{q}_2})\in Q} \frac{\vartheta\left[\vec{\mathbf{q}_1}\right](\boldsymbol{\tau})}{\vartheta\left[\vec{\mathbf{q}_2}\right](\boldsymbol{\tau})}$$

where

$$Q \subseteq \frac{1}{2m}\mathbb{Z}^4 \times \frac{1}{2m}\mathbb{Z}^4.$$

and v_Q is a $(2m)$th root of unity.

To find the Galois conjugates of α, we use explicit Shimura reciprocity. In order to state the relevant theorem, we first recall the following result.

Theorem 4.8. Let (J, ι, C) be a complex principally polarized abelian surface with complex multiplication by a primitive quartic CM field K. Then there exists a triple $(\Phi, \mathfrak{b}, \xi)$ consisting of

1. a CM type $\Phi = \{\phi_1, \phi_2\}$ of K,
2. a fractional ideal $\mathfrak{b}$ of $\mathcal{O}_K$, and
3. an element $\xi \in K$ such that
   a) $\xi\mathcal{O}_K = (\mathfrak{b}\bar{\mathfrak{b}}\mathcal{D})^{-1}$ where $\mathcal{D}$ is the different ideal of K,
   b) $\phi(\xi)$ lies on the positive imaginary axis for each $\phi \in \Phi$

such that (J, C) is isomorphic to $(\mathbb{C}^2/\Phi(\mathfrak{b}), E_{\Phi,\mathfrak{b},\xi})$ where

$$\Phi(\mathfrak{b}) = \{(\phi_1(\beta), \phi_2(\beta)) \in \mathbb{C}^2 : \beta \in \mathfrak{b}\},$$

and $E_{\Phi,\mathfrak{b},\xi}$ is the Riemann form on $\Phi(\mathfrak{b}) \times \Phi(\mathfrak{b})$ given by

$$\begin{aligned} E_{\Phi,\mathfrak{b},\xi} : \Phi(\mathfrak{b}) \times \Phi(\mathfrak{b}) &\longrightarrow \mathbb{Z} \\ (\Phi(\beta_1), \Phi(\beta_2)) &\longmapsto \mathrm{Tr}(\xi\bar{\beta}_1\beta_2). \end{aligned}$$

Proof. This is a well-known result found in [29, Section 5.5B]. See also [34, Lemma I.4.1] and [34, Theorem I.5.2]. □

Let K and $(\Phi, \mathfrak{b}, \xi)$ be as in Theorem 4.8. A basis $B = (b_1, \ldots, b_4)$ of $\mathfrak{b}$ is said to be *symplectic* if the matrix E whose coordinates are given by

$$E_{i,j} = (E_{\Phi,\mathfrak{b},\xi}(b_i, b_j)),$$

is equal to

$$\Omega := \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{bmatrix}.$$

If $B = \{b_1, b_2, b_3, b_4\}$ is a symplectic basis of $\mathfrak{b}$, we can define $\boldsymbol{\tau}(\Phi, \mathfrak{b}, \xi, B) \in \mathcal{H}_2$ as follows:

$$\boldsymbol{\tau}(\Phi, \mathfrak{b}, \xi, B) = (\Phi(b_3) \mid \Phi(b_4))^{-1}(\Phi(b_1) \mid \Phi(b_2)).$$

The following theorem, an application of explicit Shimura reciprocity, enables us to find the Galois conjugates of such numbers.

Theorem 4.9. Let (J, ι, C) be a complex principally polarized abelian surface isomorphic to $(\mathbb{C}^2/\Phi(\mathfrak{b}), E_{\Phi,\mathfrak{b},\xi})$. Let $B = \{b_1, b_2, b_3, b_4\}$ be a symplectic basis for $\Phi(\mathfrak{b})$ and let $\boldsymbol{\tau}(\Phi, \mathfrak{b}, \xi, B) \in \mathbb{H}_2$. Let $2m \in 2\mathbb{Z}_{>0}$ and $\vec{\mathbf{c}}_1, \vec{\mathbf{c}}_2, \vec{\mathbf{c}}_3, \vec{\mathbf{c}}_4 \in \frac{1}{2m}\mathbb{Z}^2$. Let $\sigma \in \mathrm{Gal}(H_{K^r}(8m^2)/\mathrm{CM}_{K^r,\Phi^r}(2))$. Let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ such that $[\mathfrak{a}] = \Psi_{L/K}^{(8m^2)}(\sigma)$, where $\Psi_{L/K}^{(8m^2)}$ is as in (1.3). Then

$$\left(\frac{\vartheta\begin{bmatrix}\vec{\mathbf{c}}_1\\ \vec{\mathbf{c}}_2\end{bmatrix}(\boldsymbol{\tau})}{\vartheta\begin{bmatrix}\vec{\mathbf{c}}_3\\ \vec{\mathbf{c}}_4\end{bmatrix}(\boldsymbol{\tau})}\right)^{\sigma} = u \cdot \frac{\vartheta\begin{bmatrix}\vec{\mathbf{d}}_1\\ \vec{\mathbf{d}}_2\end{bmatrix}(\boldsymbol{\tau}')}{\vartheta\begin{bmatrix}\vec{\mathbf{d}}_3\\ \vec{\mathbf{d}}_4\end{bmatrix}(\boldsymbol{\tau}')}$$

for some $(2m)$th root of unity $u \in \mathbb{C}$, some $\vec{\mathbf{d}}_1, \vec{\mathbf{d}}_2, \vec{\mathbf{d}}_3, \vec{\mathbf{d}}_4 \in \frac{1}{2m}\mathbb{Z}^2$ and $\boldsymbol{\tau}' \in \mathbb{H}_2$.

Proof sketch. We may apply [33, Theorem 2.4] with

$$f = \frac{\vartheta\begin{bmatrix}\vec{\mathbf{c}}_1\\ \vec{\mathbf{c}}_2\end{bmatrix}(\boldsymbol{\tau})}{\vartheta\begin{bmatrix}\vec{\mathbf{c}}_3\\ \vec{\mathbf{c}}_4\end{bmatrix}(\boldsymbol{\tau})}$$

(due to the first part of [34, Proposition 6.1]) and $N = 8m^2$ and find that

$$f(\boldsymbol{\tau})^{\sigma} = f(\boldsymbol{\tau})^{[\mathfrak{a}]} = f^{U}(\boldsymbol{\tau}')$$

for some explicit matrix U with entries in $\mathbb{Z}/8m^2\mathbb{Z}$. Using [33, Proposition 6.1], we find explicit formulas for $u, \vec{\mathbf{d}}_1, \vec{\mathbf{d}}_2, \vec{\mathbf{d}}_3, \vec{\mathbf{d}}_4, \boldsymbol{\tau}'$, and see that they can be computed

using $\mathfrak{a}, \vec{\mathbf{c}}_1, \vec{\mathbf{c}}_2, \vec{\mathbf{c}}_3, \vec{\mathbf{c}}_4$, and the quadruple $(\Phi, \mathfrak{b}, \xi, B)$. □

As mentioned in the proof of Theorem 4.9, one can compute $u, \vec{\mathbf{d}}_1, \vec{\mathbf{d}}_2, \vec{\mathbf{d}}_3, \vec{\mathbf{d}}_4$ and $\boldsymbol{\tau}'$ explicitly when one follows the formulas given in [33, Proposition 6.1]. In fact, these computations are already implemented in Streng's SAGE [27] RECIP[1] package as

```
tau.Shimura_reciprocity(a, N, period_matrix=True).
```

See the complete article [33] for more details.

4.3.3 Computing the extension $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$

At the end of Section 4.2, we have seen that

$$\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) = \mathrm{CM}_{K^r,\Phi^r}(2)(u_0, u_1, v_0^2, v_0 v_1, v_1^2).$$

where u_0, u_1, v_0, v_1 are the coefficients of the Mumford polynomials of some primitive $\mathfrak{m}$-torsion point. We have also seen in Section 4.3.2 that the conjugates of these coefficients can be expressed in terms of theta constants.

The polynomial whose set of roots consists of x and its Galois conjugates is a polynomial p_x defining the extension $\mathrm{CM}_{K^r,\Phi^r}(2)(x)/\mathrm{CM}_{K^r,\Phi^r}(2)$.

We have expressed x and its Galois conjugates in terms of theta constants. However, we remind ourselves of the unfortunate truth that theta constants are defined by infinite series. One thing we can do in the real world is to approximate theta constants up to a certain precision. In doing so, we then obtain an approximation $\tilde{p}_x$ of p_x.

We may then use a shortest vector algorithm such as LLL in order to recover the polynomial p_x from this approximation. We now end up with the following algorithm:

Algorithm 4.10.
INPUT. A primitive quartic CM pair (K, Φ) and its reflex (K^r, Φ^r), a matrix $\boldsymbol{\tau} \in \mathbb{H}_2$ such that the Jacobian $(J, \iota, \mathcal{C}) := J(\mathcal{C}_{\boldsymbol{\tau}})$ has complex multiplication by K, and an ideal $\mathfrak{m}$ of $\mathcal{O}_K$ such that $2 \mid \mathfrak{m}$.

[1] https://pub.math.leidenuniv.nl/ strengtc/code.html

OUTPUT. A set of polynomials that define the extension $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$.

1. Find a primitive $\mathfrak{m}$-torsion point P of $(J, \iota, \mathcal{C})$, where

$$\mathfrak{m} = m_1 \mathcal{O}_K + m_2 \mathcal{O}_K.$$

   To do this, we do the following:

   a) Choose a random vector in $\vec{\mathbf{z}} = \frac{1}{m}\mathbb{Z}^4$, where m is the smallest positive integer in $\mathfrak{m}$.

   b) Check if $M_{m_1}\vec{\mathbf{z}}$ and $M_{m_2}\vec{\mathbf{z}}$ are integer vectors. If it is, go back to step 1a. Otherwise, proceed to the next step.

   c) Check if every $\mathfrak{n} = n_1 \mathcal{O}_K + n_2 \mathcal{O}_K \supsetneq \mathfrak{m}$, either $M_{n_1}\vec{\mathbf{z}}$ or $M_{n_2}\vec{\mathbf{z}}$ is an integer vector. If it is, go back to step 1a. Otherwise, proceed to the next step.

2. For each $x \in \{u_0, u_1, v_0^2, v_0 v_1, v_1^2\}$ and for each automorphism

$$\sigma \in \mathrm{Gal}(\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})/\mathrm{CM}_{K^r,\Phi^r}(2)),$$

   do the following:

   a) Use Shimura reciprocity to find the appropriate u, $\vec{\mathbf{d}}_i$'s, and $\boldsymbol{\tau}'$ to compute x^σ (see Theorem 4.9).

   b) Compute an approximation for the theta constants needed to compute x^σ.

   c) Compute approximations $\tilde{x^\sigma}$ using the approximated theta constants.

3. For each $x \in \{u_0, u_1, v_0^2, v_0 v_1, v_1^2\}$, do the following:

   a) Construct the polynomial $\tilde{p}_x(X)$, by taking the product $(X - x^\sigma)$ over each $\sigma \in \mathrm{Gal}(\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})/\mathrm{CM}_{K^r,\Phi^r}(2))$.

   b) Use $\tilde{p}_x(X)$ to recover the polynomial $p_x(X)$ over $\mathrm{CM}_{K^r,\Phi^r}(2)$ using LLL as in the command `recognize_polynomial` found in the SAGE RECIP package.

4. Output the polynomials $p_x(X)$.

Note that we do not need to verify that $M_{n_1}\vec{\mathbf{z}}$ and $M_{n_2}\vec{\mathbf{z}}$ is not an integer vector for literally every $\mathfrak{n} \supsetneq \mathfrak{m}$. We only need to verify that this is the case for every $\mathfrak{n}$ of the form $\mathfrak{m}/\mathfrak{p}$ where $\mathfrak{p} \mid \mathfrak{m}$ is a prime ideal. This is because every other $\mathfrak{n}' \supsetneq \mathfrak{m}$ divides $\mathfrak{m}/\mathfrak{p}$ for some prime ideal $\mathfrak{p} \mid \mathfrak{m}$.

To approximate theta constants and theta functions whose characteristics are in $\frac{1}{2}\mathbb{Z}^4$, we refer to [13, Section 5]. The Galois conjugate x^σ is expressed in terms of theta constants whose characteristics are in $\frac{1}{2n}\mathbb{Z}^4$ for some integer n. We may use (4.7) to convert these theta constants into theta functions whose characteristics are in $\frac{1}{2}\mathbb{Z}^4$, thus enabling us to use the known approximation algorithms.

In practice, one might only need to compute one of $u_0, u_1, v_0^2, v_0v_1, v_1^2$ in order to compute $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$. That is, the field extension $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ is likely to be equal to say, the field $\mathrm{CM}_{K^r,\Phi^r}(2)(u_0)$.

If for all $x \in \{u_0, u_1, v_0^2, v_0v_1, v_1^2\}$, we have $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m}) \neq \mathrm{CM}_{K^r,\Phi^r}(2)(x)$, we can construct the tower of fields

$$\mathrm{CM}_{K^r,\Phi^r}(2)(u_0) \subseteq \mathrm{CM}_{K^r,\Phi^r}(2)(u_0, u_1) \subseteq \ldots \subseteq \mathrm{CM}_{K^r,\Phi^r}(2)(u_0, u_1, v_0^2, v_0v_1, v_1^2)$$

to compute $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})$ and determine a primitive element to find a single polynomial defining the extension $\mathrm{CM}_{K^r,\Phi^r}(\mathfrak{m})/\mathrm{CM}_{K^r,\Phi^r}(2)$.

5 Algorithms for finitely generated abelian groups

In this chapter, we review algorithms to compute kernels, images, quotients, and group extensions involving finitely generated abelian groups. These algorithms are found in [6, Chapter 4] and implemented internally in PARI/GP to compute ray class groups. To access and adapt them to compute similar groups, such as the Shimura ray class group, one must normally dive into the source code.

To write an implementation of an algorithm which computes the Shimura ray class group, we found ourselves with two choices: optimize for speed by hard-coding the needed matrices for the linear algebra computations or implement these linear algebra algorithms generically, sacrificing speed for readability and reusability. We chose the second option. In this way scientists who would like to use PARI/GP to use these algorithms (kernels, images, ...) on their favorite finitely generated abelian groups can avoid recoding the non-complicated, but tedious, linear algebra parts of the computation.

In the context of this chapter, we say that an algorithm is *nice* if it is efficient and practical in the sense that fast implementations are available[1] in PARI/GP [21]. We note that this 'definition' of a nice algorithm is admittedly vague.

In the algorithms found in this chapter, nice algorithms are used, but sparingly. They are used at most $O(n)$ times where n is the number of generators of the finitely generated abelian group G involved. Notice that $n \sim O(\log |G|)$ where $|G|$ is the order of the group.

While the algorithms found in this chapter are a careful rewriting of the algorithms of [6], they are currently not natively available in PARI/GP. We have implemented

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

these algorithms in a file `fgag.gp`[2], which includes algorithms involving finitely generated abelian groups and morphisms between them. We have also implemented code to compute the Shimura ray class group. This implementation is available in a file `fgagshimuray.gp`[3] and heavily depends on the machinery in `fgag.gp`.

In this chapter, all groups are assumed to be **finitely generated and abelian**. Moreover, we write our groups multiplicatively.

5.1 Nice groups

In this section, we define and give examples of *nice groups*. These are groups that for our purposes are 'ready for linear algebra computations'. We will see what exactly this means in the following.

5.1.1 Definitions

For any (finitely generated abelian) group G, the fundamental theorem of finitely generated abelian groups tells us that there exists a unique integer vector

$$\vec{\mathbf{d}} = (d_1, \ldots, d_n)$$

where $d_i \in \mathbb{Z}_{\geq 0} \setminus \{1\}$ for each $i \in \{1, \ldots, n\}$ and such that for some integer r satisfying $1 \leq r \leq n$ we have

- $d_{i+1} \mid d_i$ for each $i < r$,
- $d_i \neq 0$ for each $i \leq r$, and
- $d_i = 0$ for each $i > r$.

We say that a presentation for a group G is *nice* if it consists of the following data:

G1 the unique integer vector $\vec{\mathbf{d}}$ guaranteed by the fundamental theorem of finitely generated abelian groups

[2] https://math.guissmo.com/code.php
[3] https://math.guissmo.com/code.php

G2 a (finite) set of n generators $\vec{\mathbf{g}}_G = (g_1, \ldots, g_n) \in G^n$ of G such that $g_i \in G$ is an element of infinite order if $d_i = 0$ and an element of order d_i otherwise.

G3 the following nice algorithms

G3.a Given as input two elements $a, b \in G$, output their product ab.

G3.b Given as input an element $a \in G$ and an integer $x \in \{0, -1\}$, output a^x.

G3.c Given as input an element $a \in G$, output the unique vector

$$\vec{\mathbf{x}} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$$

such that $a = g_1^{x_1} \cdots g_n^{x_n}$ where

- $x_i \in \mathbb{Z}$ for each $i \in \{1, \ldots, n\}$, and
- $0 \leq x_i < d_i$ holds when $d_i \neq 0$.

We refer to such a presentation as *nice group data* for (the group) G. In what follows, when we say that a group G is (a) *nice* (group), we mean that nice group data for G is known.

We make a few remarks.

First, we can use **G3.a**, **G3.b**, and a square-and-multiply[4] algorithm to compute a^x for any $x \in \mathbb{Z}$.

In addition, we call the nice algorithm given in **G3.c** a *discrete logarithm algorithm with respect to the generators* $\vec{\mathbf{g}}_G$ *of* G. It is particular in the sense that it outputs an integer vector $\vec{\mathbf{x}}$, as opposed to the nice algorithms given in **G3.a** and **G3.b** which output elements of the group G.

Let r and s be positive integers and consider a vector $\vec{\mathbf{a}} = (a_1, \ldots, a_r) \in G^r$ and an $r \times s$ integer matrix $M = (m_{ij})$. We denote by $\vec{\mathbf{a}}M$ the row vector of length s whose jth entry is:

$$a_1^{m_{1,j}} \ldots a_r^{m_{r,j}}.$$

One can think of this notation as matrix multiplication but since our groups are multiplicative, we exponentiate instead.

[4] In additive groups, this is called double-and-add.

Let G be a nice group. In particular, we have a vector $\vec{\mathbf{g}}_G = (g_1, \ldots, g_n)$ giving a set of generators of G and a vector $\vec{\mathbf{d}} = (d_1, \ldots, d_n)$ giving the order of each element.

It is convenient to write the orders $d_1, \ldots, d_n$ of the generators $\vec{\mathbf{g}}_G$ of G given by **G1** as a diagonal matrix

$$D_G = \begin{bmatrix} d_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & d_n \end{bmatrix}.$$

In this way, we have the equality

$$\vec{\mathbf{g}}_G D_G = \mathbf{1} \tag{5.1}$$

where $\mathbf{1}$ is the length n column vector all entries of which are the identity element of G. Written out, equation (5.1) simply means $g_i^{d_i} = 1_G$ for each i, which we already know by definition anyway.

We sometimes write A or B for nice groups later in this section. In these cases, we of course denote the generators by $\vec{\mathbf{g}}_A$ and $\vec{\mathbf{g}}_B$ and the diagonal matrix whose entries are the orders as D_A and D_B.

An $n \times n$ matrix $D = (d_{i,j})$ is said to be in *Smith normal form* if it is a diagonal matrix with nonnegative integer coefficients such that $d_{i+1,i+1} \mid d_{i,i}$ for all $i < n$. The condition on the divisibility of the d_i shows that the matrix D_G is in Smith normal form, for a finite abelian group G.

If M is an invertible square integer matrix, then there exists a unique matrix D in Smith normal form such that $D = UMV$, where U and V are invertible square integer matrices [5, Theorem 2.4.12]. In our context, a *Smith normal form algorithm* is an algorithm which takes an integer matrix M, and outputs the matrices U, V, D. A Smith normal form algorithm is found in [5, Algorithm 2.4.14] and it is available as `matsnf` with `flag` set to 1.

5.1.2 Examples of nice groups

Example 5.2. Let K be a number field and let $\mathfrak{m}$ be a modulus of K. We would like to show that $\mathrm{Cl}_K(\mathfrak{m})$ is nice.

Generators and their respective orders (**G2** and **G1**) can be computed using [5, Algorithm 6.5.9], available as `bnrinit`. Taking products (**G3.a**) in $\mathrm{Cl}_K(\mathfrak{m})$ means multiplying ideals representing the classes, see [5, Section 4.6] for more details. This ideal multiplication is available as `idealmul`. Taking powers (**G3.b**) of elements in $\mathrm{Cl}_K(\mathfrak{m})$ is available as `idealpow`.

Finally, the discrete logarithm algorithm (**G3.c**) algorithm is given as an auxiliary result to [5, Algorithm 6.5.10], available as `bnrisprincipal`.

Therefore, ray class groups are nice.

Using `idealpow` may result in choosing ideal class representatives whose norms are prohibitively large. While not required by the constraints we gave to qualify as a nice group, it is a good idea to use representatives with low enough norm. To find such representatives for an ideal class $[\mathfrak{a}] \in \mathrm{Cl}_K(\mathfrak{m})$, one can find $\alpha \in P_K(\mathfrak{m})$ such that $\alpha\mathfrak{a}$ is a fractional ideal with small norm. When $\mathfrak{m} = 1$, one can use `idealred`, available in PARI/GP [21]. The PARI C Library has indirect solutions for reducing when $\mathfrak{m} \neq 1$, but we have not used this in the implementation we have at the time of writing this thesis.

Recalling Lemma 3.30, we see that the above example will be useful in our ultimate goal of computing the Shimura ray class group because the exact sequence involves groups related to class groups. We discuss another family of groups that appear in the lemma.

Example 5.3. Let K be a number field. We would like to show that $\mathcal{O}_K^\times$ is nice.

Generators and their respective orders (**G2** and **G1**) are computed alongside other information in [5, Chapter 6.5.4, Number fields], available as `bnfinit`. In particular, if `K` is the output of `bnfinit`, one may access the finite-order generators by `K.tu` (torsion units) and the infinite-order generators by `K.fu` (fundamental units).

Multiplying and exponentiating (**G3.a** and **G3.b**) are done by using data output by `nfinit`. These operations are available as `nfeltmul` and `nfeltpow`, respectively.

A discrete logarithm algorithm with respect to the above generators is given

in [6, Chapter 5, Algorithm 5.3.10], available as `bnfisunit`.

Therefore, the unit groups of number fields are nice.

One group that we need that does not explicitly appear in Lemma 3.30 is $(\mathcal{O}_K/\mathfrak{m})^\times$. We see later that this group helps us compute the group $\mathcal{O}_{K,\mathfrak{m},1}^\times$.

Example 5.4. Let K be a number field and let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$. We would like to show that $(\mathcal{O}_K/\mathfrak{m})^\times$ is nice.

Generators and their respective orders (**G2** and **G1**) are computed in [6, Algorithm 4.2.21], available as `idealstar`.

Multiplying and exponentiating (**G3.a** and **G3.b**) are again done by using data output by [5, Chapter 4.1.2, Number fields], available as the functions `nfeltmul` and `nfeltpow`.

A discrete logarithm algorithm with respect to the above generators is given in [6, Algorithm 4.2.24], available as `ideallog`.

Therefore, groups of the form $(\mathcal{O}_K/\mathfrak{m})^\times$ are nice.

5.2 Subgroups and Hermite normal forms

In Section 5.2.1, we see that subgroups can be represented using a so-called HNF matrix. In the rest of the sections, we present algorithms involving subgroups, such as kernels (Section 5.2.2), images (Section 5.2.3, and intersections of subgroups (Section 5.2.4).

5.2.1 Representing subgroups

We represent subgroups using matrices in Hermite normal form. We use the definition found in [5, Definition 2.4.2].

A rectangular $m \times n$ integer matrix $H = (h_{i,j})$ is said to be in *Hermite normal form* if

1. the first $r \leq n$ columns of H are 0 for some nonnegative integer r,

2. for each $i \in \{1, \ldots, m\}$, there exists $l_i \in \{1, \ldots, m\}$ such that

   a) $h_{i,k} = 0$ if $k < l_i$,

   b) $h_{i,l_i} \geq 1$, and

   c) $0 \leq h_{i,k} < h_{i,l_i}$ if $k \geq l_i$,

3. if $i < i'$ then $l_i < l_{i'}$.

Let M, N be two matrices with the same number of rows. We denote their (horizontal) concatenation by $(M \mid N)$. In our context, a *Hermite normal form algorithm* is an algorithm which takes a rectangular integer matrix M, and outputs a matrix H in Hermite normal form and an invertible integer square matrix U such that $MU = (0 \mid H)$. Such an algorithm can be found in [5, Algorithm 2.4.4] and it is available as `mathnf` with `flag` set to `1`.

In [6, Proposition 4.1.6], we find that there is a natural one-to-one correspondence between the subgroups of a finite group G and invertible integer square matrices H in Hermite normal form such that $H^{-1}D_G$ is an integer matrix. The same proposition tells us that given such a matrix H in Hermite normal form, the subgroup it corresponds to is generated by $\vec{\mathbf{g}}H$ with relations between these generators given by $H^{-1}D_G$.

While the result stated in [6, Proposition 4.1.6] deals with *finite* groups, the given correspondence (and the proof) still works between *finite-index* subgroups of a finitely generated abelian group G and invertible integer square matrices H in Hermite normal form such that $H^{-1}D_G$ is an integer matrix.

We make the following remarks:

1. The trivial subgroup of a group G is represented by the matrix D_G. Indeed, the generators of the subgroup D_G correspond to $\vec{\mathbf{g}}_G D_G$, which is column vector whose entries are all 1.

2. The matrix representing G as a subgroup of itself is represented by the identity $n \times n$ matrix. Indeed, the generators of G are simply $\vec{\mathbf{g}}_G$.

3. The index of the subgroup of G corresponding to the matrix H is equal to the determinant $\det H$.

As an example, we continue from Example 3.26.

Example 3.26 (continuing from p. 77)**.** The unit group $\mathcal{O}_{K_0}^{\times}$ is generated by $\vec{\mathbf{g}} = (-1, \varepsilon_0)$ and the vector $\vec{\mathbf{d}}$ is $(2, 0)$. We would like to find the Hermite normal form matrix representing the subgroup ${\mathcal{O}_{K_0}^{\times}}^{+}$ of $\mathcal{O}_{K_0}^{\times}$.

In the case where $\varepsilon_0^+ = \varepsilon_0^2$, the corresponding matrix H is

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}.$$

That is, the generators of ${\mathcal{O}_{K_0}^{\times}}^{+}$ are $(-1)^2\varepsilon_0^0 = 1$ and $(-1)^0\varepsilon_0^2 = \varepsilon_0^2$.

In the case where $\varepsilon_0^+ = \varepsilon_0$, the corresponding matrix H is

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix}.$$

That is, the generators of ${\mathcal{O}_{K_0}^{\times}}^{+}$ are $(-1)^2\varepsilon_0^0 = 1$ and $(-1)^0\varepsilon_0 = \varepsilon_0$.

Finally, in the case where $\varepsilon_0^+ = -\varepsilon_0$, the corresponding matrix H is

$$\begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}.$$

That is, the generators of ε_0^+ are $(-1)^2\varepsilon_0^0$ and $(-1)^1\varepsilon_0^1 = -\varepsilon_0$.

5.2.2 Finding kernels

The kernel of $N_2 : \mathrm{Cl}_K(\mathfrak{m}) \longrightarrow \mathrm{Cl}_{K_0}^{+}(1)$, defined in (3.29), is one part of the exact sequence in Lemma 3.30. In this section, we represent the subgroup $\ker N_2$ of $\mathrm{Cl}_K(\mathfrak{m})$ as a Hermite normal form matrix.

Algorithm 5.5. Suppose A and B are nice groups where $\vec{\mathbf{g}}_A$ and $\vec{\mathbf{g}}_B$ have lengths n_A

and n_B, respectively. Let $\phi : A \to B$ be a group homomorphism. Assume that we have a nice algorithm to compute $\phi(a) \in B$ for any $a \in A$. The following algorithm gives the kernel of ϕ as a Hermite normal form matrix H with respect to the generators of A.

1. For each component a_i of $\vec{\mathbf{g}}_A$, compute $p_i := \phi(a_i) \in B$.
2. Use the discrete logarithm algorithm of B (which exists by **G3.c** of B) to construct an $n_B \times n_A$ matrix P whose ith column is the discrete logarithm of p_i with respect to $\vec{\mathbf{g}}_B$.
3. Use a Hermite normal form algorithm to find matrices H' and U' such that $(P \mid D_B)U' = (0 \mid H')$.
4. Use a Hermite normal form algorithm to find matrices H and U such that $(U_1 \mid D_A)U = (0 \mid H)$, where U_1 is the upper-left $n_A \times n_A$ submatrix of U'.
5. Output the matrix H.

This algorithm is implemented in `fgag.gp` as `fgagmorker` (which uses the more general function `fgagmorsubgpinvimg`).

Proof. See the proof of the more general [6, Algorithm 4.1.11]. □

One application of Algorithm 5.5 in our context is to find ker N_2 where N_2 is as in (3.29).

Example 5.6. Let K be a CM field and K_0 its totally real subfield. We are interested in the kernel of the relative norm $N_2 := N_{K/K_0} : \mathrm{Cl}_K(\mathfrak{m}) \to \mathrm{Cl}^+_{K_0}(1)$. Both domain and codomain are nice groups and a nice algorithm for computing N_2 is given by [6, Algorithm 2.5.2]. This algorithm is available as `rnfidealnormrel`, where the first argument is the output of the appropriate `rnfinit` command to compute the extension K/K_0.

The subgroup $\mathcal{O}^\times_{K,\mathfrak{m},1}$ of $\mathcal{O}^\times_K$ is also a kernel by definition. It is the kernel of the natural map $s : \mathcal{O}^\times_K \to (\mathcal{O}_{K_0}/\mathfrak{m})^\times$, as seen in (3.27).

Example 5.7. Let K be a CM field. We are interested in the kernel of the map $s : \mathcal{O}_K^\times \to (\mathcal{O}_{K_0}/\mathfrak{m})^\times$. The domain and codomain are nice groups by Example 5.3 and Example 5.4, respectively. A nice algorithm for computing s is given by [6, Algorithm 2.5.2]. This algorithm is available as `rnfeltnorm`, where the first argument is the output of the appropriate `rnfinit` command to compute the extension K/K_0. We use Algorithm 5.5 to compute a Hermite normal form matrix representing the subgroup $\mathcal{O}_{K,\mathfrak{m},1}^\times = \ker s$ of $\mathcal{O}_K^\times$.

5.2.3 Finding images

The cokernel of N_1, defined in (3.28), is

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

We would like to find the image of the subgroup $\mathcal{O}_{K,\mathfrak{m},1}^\times$ under the morphism

$$N_{K/K_0} : \mathcal{O}_K^\times \to \mathcal{O}_{K_0}^\times.$$

We have the following algorithm.

Algorithm 5.8. Suppose A and B are nice groups, where the vectors $\vec{\mathbf{g}}_A$ and $\vec{\mathbf{g}}_B$ have lengths n_A and n_B, respectively. Let $\phi : A \to B$ be a group homomorphism. Assume that we have a nice algorithm to compute $\phi(a) \in B$ for any $a \in A$. Let H' be a matrix in Hermite normal form representing a subgroup A' of A. The following algorithm gives the image $\phi(A')$ as a Hermite normal form matrix H with respect to the generators of B.

1. For each component a'_i of $\vec{\mathbf{g}}_{A'} := \vec{\mathbf{g}}_A H'$, compute $p_i := \phi(a'_i) \in B$.
2. Use the discrete logarithm algorithm of B (which exists by **G3.c** of B) to construct an $n_B \times n_A$ matrix P whose ith column is the discrete logarithm of p_i with respect to $\vec{\mathbf{g}}_B$.
3. Use a Hermite normal form algorithm to find matrices H and U such that $(PH' \mid D_B)U = (0 \mid H)$.

4. Output the matrix H.

Proof. See [6, Proof of Algorithm 4.1.10]. □

This algorithm is implemented in `fgag.gp` as `fgagmorsubgpimg`.

We apply Algorithm 5.8 to find the image of the subgroup $\mathcal{O}_{K,\mathfrak{m},1}^{\times}$ under N_{K/K_0}.

Example 5.9. Denote by H' the Hermite normal form of the subgroup $\mathcal{O}_{K,\mathfrak{m},1}^{\times}$ of $\mathcal{O}_K^{\times}$. We showed how to compute this in Example 5.7. Both the domain $\mathcal{O}_K^{\times}$ and codomain $\mathcal{O}_{K_0}^{\times}$ are nice groups by Example 5.3. A nice algorithm to compute N_{K/K_0} is available as `rnfeltnorm`. Applying Algorithm 5.8, we find a Hermite normal form matrix for the subgroup $N_{K/K_0}(\mathcal{O}_{K,\mathfrak{m},1}^{\times})$ of $\mathcal{O}_{K_0}^{\times}$.

In Section 5.3, we talk about taking quotients, enabling us to finally compute nice group data for coker N_1. For now, we look at one more algorithm involving subgroups.

5.2.4 Finding intersections

The following algorithm computes intersections of subgroups of a group G. This algorithm is important as it is used in Algorithm 3.33.

Algorithm 5.10. Suppose that G is a nice group, that n is the length of $\vec{\mathbf{g}}_G$, that A and B are subgroups of G, and with H_A and H_B as their corresponding Hermite normal form matrices. This algorithm computes the Hermite normal form matrix of the intersection $A \cap B$.

1. Use a Hermite normal form algorithm to find matrices H' and U' such that
$$(H_A \mid H_B)U' = (0 \mid H').$$

2. Use a Hermite normal form algorithm to find matrices H and U such that $(H_A U_1 \mid D_G)U = H$, where U_1 is the $n \times n$ matrix consisting of the first n rows and first n columns of U'.

3. Output the matrix H.

Proof. See [6, Proof of Algorithm 4.1.14]. □

This algorithm is implemented in `fgag.gp` as `fgagsubgpint`.

5.3 Building Nice Groups

In the previous section, we dealt with *subgroups* of nice groups. In this section, we will construct *new* nice groups from known nice groups. In particular, we discuss how to compute quotients and group extensions.

5.3.1 Subgroups as nice groups

The attentive reader might have noticed that we have so far represented subgroups as matrices, always with respect to a larger group. However, we can use these matrices to get nice group data for subgroups. In this way, we can treat a subgroup as a bona fide nice group – complete with generators and a discrete logarithm algorithm.

Algorithm 5.11. Let G be a nice group, and let G' be a subgroup of G. Let H be the HNF matrix of G' with respect to the generators $\vec{\mathbf{g}}_G$ of G. Take $M := H^{-1}D_G$ to be a matrix of relations defining the subgroup G'. This algorithm outputs nice group data of G'. In particular, it outputs a vector $\vec{\mathbf{g}}_{G'}$ of generators of G' and their respective orders.

1. Use a Smith normal form algorithm to compute invertible square integer matrices U, V and a Smith normal form matrix D' such that $UMV = D'$.
2. Let m be the largest integer such that the (m, m)-th entry of D' is not equal to 1. If such an integer does not exist, G' is the trivial group. Otherwise, proceed to the next step.
3. Output the following:

a) the vector $\vec{\mathbf{g}}_{G'}$ of length m, the row vector obtained by taking the first m entries of the $\vec{\mathbf{g}}U^{-1}$, and

b) the (first m) diagonal entries $d_1, \ldots, d_m$ of D'.

Proof. See [6, Algorithm 4.1.3] □

The above algorithm gives **G2** and **G1** for G'. The multiplication and exponentiation maps are obviously the same, which covers **G3.a** and **G3.b**. The only thing left to make sure that G' is a nice group is to find a discrete logarithm algorithm on the generators $\vec{\mathbf{g}}_{G'}$.

Algorithm 5.12. Take as input $a' \in G' \leq G$. This algorithm returns the discrete logarithm of a' with respect to the generators $\vec{\mathbf{g}}_{G'}$ given in Algorithm 5.11. Let U and m be as in Algorithm 5.11. Let U' be the not necessarily square matrix consisting only of the first m rows of U.

1. Compute the discrete logarithm $\operatorname{dlog}(a') \in \mathbb{Z}^n$ of a' with respect to the generators $\vec{\mathbf{g}}_G$ of G.
2. Output the length m column vector $U' \operatorname{dlog}(a')$.

Proof. See [6, discussion below Algorithm 4.1.14]. □

When implementing these algorithms, one can simply choose to output U' as part of Algorithm 5.11. In this way, the matrix U' can be baked into the discrete logarithm algorithm of G'.

At this point, we have shown that any Hermite normal form corresponding to a subgroup of a finite group G can be viewed as a nice group. In other words, we can find the nice group data for the subgroup.

Example 5.13. In Example 3.26, we solved for the Hermite normal form matrix H of ${\mathcal{O}_{K_0}^{\times}}^{+}$. Running Algorithm 5.11 with input $\vec{\mathbf{g}} = \vec{\mathbf{g}}_G$ and H, we can find the nice group data for ${\mathcal{O}_{K_0}^{\times}}^{+}$.

5.3.2 Finding quotients

Notice that

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

is a quotient of a subgroup $B := {\mathcal{O}_{K_0}^{\times}}^{+}$ of the finitely generated (but not finite) abelian group $G := \mathcal{O}_{K_0}^{\times}$ by another subgroup $A := N_{K/K_0}(\mathcal{O}_{K,\mathfrak{m},1}^{\times}) \leq B$ of the same group G.

Both subgroups A and B have finite index from the overgroup G. Therefore, B/A is a finite abelian group. A simple generalization of Algorithm 5.11 and Example 5.13 gives us the following algorithm to compute the nice group data **G2**, **G1** and **G3.c** of B/A.

> **Algorithm 5.14.** Let H_A and H_B be the Hermite normal forms of the subgroups A and B with respect to the generators $\vec{\mathbf{g}}_G$ of G. Assume $A \leq B$. This algorithm outputs the quotient B/A, including all the data needed to show that it is a nice group.
>
> 1. Compute the vector $\vec{\mathbf{g}}' = \vec{\mathbf{g}}_G H_B$ and the matrix $H := H_B^{-1} H_A$.
> 2. Use (the aforementioned generalization of) Algorithm 5.11 on $\vec{\mathbf{g}}'$ and H, compute the corresponding discrete logarithm algorithm and output the result.

As the above algorithm is a modified version of [6, Algorithm 4.1.7], we provide a proof sketch here.

Proof sketch. A (not necessarily minimal) set of generators of B is given by $\vec{\mathbf{g}}_G H_B$.

The discrete logarithms of a set of generators of A with respect to $\vec{\mathbf{g}}_G$ is given by the columns of H_A. With respect to $\vec{\mathbf{g}}_G H_B$, the discrete logarithms for the same set of generators are then $H_B^{-1} H_A$ since

$$\vec{\mathbf{g}}_G \, H_A = \vec{\mathbf{g}}_G \, H_B \; H_B^{-1} \, H_A.$$

Because $A \leq B$, the discrete logarithms of A in terms of these generators of B must consist of integer coefficients.

The quotient B/A has $\vec{\mathbf{g}}_G H_B$ as representatives for the generators (which are cosets of A) and the relations are given by the integer matrix $H_B^{-1} H_A$. We then use the Smith normal form algorithm to find the nice group data. □

Example 5.15. We compute the nice group data for

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

Recall that $\mathcal{O}_{K_0}^{\times}$ is nice by Example 5.3 and let us fix the set of generators for the purposes of this example. We compute a Hermite normal form matrix H_B for the subgroup ${\mathcal{O}_{K_0}^{\times}}^{+}$ of $\mathcal{O}_{K_0}^{\times}$ as in Example 3.26 and a Hermite normal form matrix H_A for the subgroup $N_{K/K_0}(\mathcal{O}_{K,\mathfrak{m},1}^{\times})$ as in Example 5.9. Note that both matrices are computed with respect to the same set of generators of $\mathcal{O}_{K_0}^{\times}$. We may apply Algorithm 5.14 to obtain the nice group data for coker N_1.

5.3.3 Finding group extensions

Let A and C be nice groups and let B be a group which fits as the middle term of the exact sequence

$$1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1.$$

Assume that we can represent elements of B. These representatives need not be unique. Assume we know how to represent the identity element, how to find the inverse of an element, and how to multiply two elements of B given in the representation we chose.

We would like to find a set of generators for B and their corresponding orders and a discrete logarithm algorithm with respect to this set of generators. This can be done provided more information on the maps f and g.

Algorithm 5.16. Let A and C be nice groups, let n_A and n_C be the lengths of $\vec{\mathbf{g}}_A$ and $\vec{\mathbf{g}}_C$ respectively, and let B be a group which fits as the middle term of the exact sequence

$$1 \to A \xrightarrow{f} B \xrightarrow{g} C \to 1$$

where $f : A \to B$ and $g : B \to C$ are group homomorphisms. Suppose further that B satisfies **G3.a** and **G3.b**.

Fix two arbitrary lifts $f' : \operatorname{im} f \to A$ and $g' : C \to B$ such that $f'(f(a)) = a$ for all $a \in A$ and $g'(g(b)) = b$ for all $b \in B$.

Suppose that there exist nice algorithms to do the following:

GX1 Given an element $a \in A$, output $f(A) \in B$.

GX2 Given an element $b \in B$, output $g(B) \in C$.

GX3 Given an element $b \in \operatorname{im} f$, output $f'(b) \in A$.

GX4 Given an element $c \in C = \operatorname{im} g$, output $g'(c) \in B$.

The following algorithm gives a set of generators for B and their corresponding orders.

1. Compute the length n_C vector $\vec{\mathbf{g}}_{B_2} := g'(\vec{\mathbf{g}}_C)$.
2. Compute the length n_C vector $\vec{\mathbf{g}}_{B_1} := \vec{\mathbf{g}}_{B_2} D_C$.
3. Compute the length n_C vector $\vec{\mathbf{g}}_{A_1} := f'(\vec{\mathbf{g}}_{B_1})$.
4. Compute the $n_A \times n_C$ matrix P, whose columns are the discrete logarithms of the components of $\vec{\mathbf{g}}_{A_1}$ with respect to the given generators $\vec{\mathbf{g}}_A$ of A.
5. Let $\vec{\mathbf{b}}'$ be the concatenation of the vectors $f(\vec{\mathbf{g}}_A)$ and $\vec{\mathbf{g}}_{B_2}$ and let

$$M = \left[\begin{array}{c|c} D_A & -P \\ \hline 0 & D_C \end{array}\right]$$

   Apply Algorithm 5.11 with $\vec{\mathbf{b}}'$ and M as input and output the result.

Proof. See [6, Algorithm 4.1.8]. □

We remark that the nice algorithm given by **GX2** is not used in the above algorithm. However, we included it anyway because we need it for the discrete logarithm algorithm.

Algorithm 5.17. Suppose $b \in B$. And suppose we know nice algorithms to compute **GX2** and **GX3**. This algorithm outputs the discrete logarithm of b with respect to the generators returned by Algorithm 5.16. It uses several intermediate results of Algorithm 5.16.

1. Compute $L_2 := \operatorname{dlog}(g(b))$ by using **GX2** and the (known) discrete logarithm algorithm on C.
2. Compute $\beta := \vec{\mathbf{g}}_{B_2} L_2 \in B$.
3. Compute $\alpha := f'(b/\beta)$. Note that $b/\beta \in \ker g = \operatorname{im} f$.
4. Compute $L_1 := \operatorname{dlog}(\alpha)$.
5. Output $U_a(L_1 \mid L_2)^{\mathsf{T}}$.

Proof. See discussion below [6, Algorithm 4.1.8]. □

5.3.4 Computing the Shimura ray class group

The preceding sections have equipped us with the tools we need to finally compute the Shimura ray class group, a group extension (see Lemma 3.30). The algorithm to compute this is implemented in our PARI/GP script `fgagshimuray.gp` [5].

Example 5.18. Take A to be the nice group coker N_1, whose data we have computed in Example 5.15.

We compute the nice group data of ker N_2 by applying Algorithm 5.11 with input: the generators of the group $\mathrm{Cl}_K(\mathfrak{m})$ and the matrix $H^{-1}D$, where H is the Hermite normal form obtained in Example 5.6 and $D = D_{\mathrm{Cl}_K(\mathfrak{m})}$ is the diagonal matrix giving the orders of each generator. At this point, we can view ker N_2 as a nice group.

The morphisms f and g in Lemma 3.30 are given as follows:

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

[5] https://math.guissmo.com/code.php

$$\begin{aligned} u &\mapsto [(\mathcal{O}_K, u)] \\ g : \mathfrak{C}_K(m) &\to \ker N_2 \leq \mathrm{Cl}_K(\mathfrak{m}) \\ [(\mathfrak{a}, a)] &\mapsto [\mathfrak{a}]. \end{aligned}$$

The morphisms f and g are not complicated. A nice algorithm we can use to satisfy **GX1** is one which outputs $(\mathcal{O}_K, u)$ given an input u. Similarly, for **GX2** we can use the algorithm in which one 'forgets' the second component of the input $(\mathfrak{a}, a)$. These algorithms are trivial to implement.

The exciting part is finding the maps f' and g'.

GX3 basically asks: given an element $\beta = [(\mathfrak{b}, b)] \in \operatorname{im} f \leq B$, find $\alpha \in A$ such that $f(\alpha) = [(\mathfrak{b}, \beta)]$. If we are able to find a representative of β of the form $[(\mathcal{O}_K, a)]$, then a is the α that we are looking for.

Since $\beta \in \operatorname{im} f = \ker g$, there exists x such that

$$\mathfrak{b} = x\mathcal{O}_K$$

where $x \in K^\times$ satisfies $x \equiv 1 \bmod^* \mathfrak{m}$. We may find this using [6, Algorithm 4.3.2], available as `bnrisprincipal`.

By definition of the Shimura ray class group, we have

$$[(\mathfrak{b}, b)] = [(\mathfrak{b}/(x\mathcal{O}_K), b/(x\bar{x}))].$$

The components $\mathfrak{b}/(x\mathcal{O}_K)$ and $b/(x\bar{x})$ are elements of nice groups and can therefore be computed using the relevant nice algorithms.

We take $f'(\beta) = f'([(\mathfrak{b}, b)]) := b/x\bar{x}$.

On to Item **GX4**! Given an element $\mathfrak{c} \in C = \operatorname{im} g$, we would like to find β such that $g(\beta) = [\mathfrak{c}]$. One representative for β would be $[\mathfrak{c}, c]$ where $c = N_{K/K_0}(\mathfrak{c}) \in K_0$.

Computing relative norms of ideals is done in [6, Algorithm 2.5.2] and finding the generating element c can be done by [6, Algorithm 4.3.2], available as `bnrisprincipal`.

> Using Algorithms 5.16 and 5.17, we finally find the missing nice group data for the Shimura ray class group.

As remarked in Example 5.2, computing the ray class groups in PARI/GP is done using the command `bnrinit`. The ideal class group can be computed using `bnfinit`. Because the ray class group fits in an exact sequence involving $(\mathcal{O}_K/\mathfrak{m})^\times$, the unit group $\mathcal{O}_K^\times$, and the ideal class group $\mathrm{Cl}_K(1)$, one may reinvent the wheel for the purposes of learning by following the above group extension algorithm to compute the ray class group $\mathrm{Cl}_K(\mathfrak{m})$.

6 Examples

This chapter gives concrete examples to make the discussion in the previous chapters more explicit. The examples are coded by the author in PARI/GP [21] and SAGE [27], depending on where the necessary functions are.

In Section 6.1, we go through a small example in detail. This covers the steps in computing a Hilbert class field of a primitive quartic CM field using CM theory. It includes explicit examples of objects obtained from implementing the algorithms in Chapter 5.

In Section 6.2, we give an example which uses information from a primitive 6-torsion point in order to find $\mathrm{CM}_{K^r,\Phi^r}(3)$ for some reflex pair (K^r, Φ^r) of a primitive quartic pair (K, Φ).

In Section 6.3, we give an example for which the bound given in Theorem 3.1 is a division-minimal m.

In Section 6.4, we discuss when our algorithm fares better against Kummer theory algorithms and when it does not. We give an example of a CM field for which our CM theory algorithm returns a conjectural defining polynomial for the Hilbert class field, but an implementation of the Kummer theory algorithm does not finish within 24 hours.

Finally, in Section 6.5, we report observations involving an experiment motivated by getting an idea on how

$$\min\{m : (\star_m) \text{ holds for } K^r\}$$

is distributed as K^r varies.

In what follows, we denote by

$$\langle \alpha \rangle_n$$

the cyclic group generated by α of order $n \in \mathbb{Z}_{>0}$. In addition, we denote by

$$\langle \alpha \rangle_\infty$$

the cyclic group generated by α of infinite order.

6.1 A detailed example

In this section, we consider a specific primitive quartic CM pair (K, Φ) and its reflex (K^r, Φ^r). The purpose of this section is to give a simple example that applies the theory and algorithms we encountered in the previous chapters.

Let K_0 be the real quadratic field

$$K_0 = \mathbb{Q}(\alpha_0) = \mathbb{Q}[X] \,/\, (X^2 + 53\,X + 500).$$

Consider the quartic CM field $K = K_0(\alpha)$ where α is a root of $X^2 - \alpha_0$.

The CM field

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

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

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

The reflex of the quartic CM pair (K^r, Φ^r) of (K, Φ) is

$$K^r = \mathbb{Q}(\alpha_r) = \mathbb{Q}[X] \,/\, (X^4 + 106\,X^2 + 809).$$

The ray class field $H_{K_0^r}(2)$ of its totally real subfield $K_0^r = \mathbb{Q}(\sqrt{5})$ is K_0^r itself. In other words, $\mathrm{Cl}_{K_0^r}(2)$ is trivial.

$$\begin{tikzcd}
H_{K^r}(2) \arrow[d, dash, "4"] \\
H_{K^r}(1) \arrow[d, dash, "8"] \\
K^r \arrow[d, dash, "2"] \\
K_0^r \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}$$

The ideal class group $\mathrm{Cl}_{K^r}(1)$ is cyclic of order 8. Therefore, the Hilbert class field is a cyclic extension of K^r of degree 8.

In the next few subsections, we verify that $(\star_2)$ holds. After that, we compute the Hilbert class field of K^r.

6.1.1 Computing the cokernel of N_1

As explained in Example 5.3, we can find the generators of the nice groups $\mathcal{O}_K^\times$ and $\mathcal{O}_{K_0}^\times$. In particular, their fundamental units are

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

and

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

respectively. Having $\varepsilon = \varepsilon_0$ corresponds to one of the three possible cases as discussed in Example 3.26. The complete sets of generators of the nice groups $\mathcal{O}_K^\times$ and $\mathcal{O}_{K_0}^\times$ are then as follows:

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

Meanwhile, doing the same for $(\mathcal{O}_K/2\mathcal{O}_K)^\times$ (see Example 5.4), we get

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

Notice that

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

Hence, we find that the map $s : \mathcal{O}_K^\times \to (\mathcal{O}_K/2\mathcal{O}_K)^\times$ sends all elements of its domain to 1. The kernel $\ker s = \mathcal{O}_{K,\mathfrak{m},1}^\times$ is then equal to $\mathcal{O}_K^\times$. We managed to compute this kernel by inspection, but if we are faced with an example with a less obvious kernel, we may refer to Algorithm 5.5 to do the job.

The image of the group $\mathcal{O}_{K,\mathfrak{m},1}^\times$ under the relative norm map N_{K/K_0}, which we compute by Algorithm 5.8, is the index 4 subgroup

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

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

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

Recalling that

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

we have shown that coker N_1 is the trivial group.

6.1.2 Computing the kernel of N_2

We now compute $\ker\left(N_2 = N_{K/K_0} : \mathrm{Cl}_K(\mathfrak{m}) \longrightarrow \mathrm{Cl}_{K_0}^{+}(1)\right)$, as in (3.29). The ray class groups $\mathrm{Cl}_K(2)$ and $\mathrm{Cl}_{K_0}^{+}(1)$, nice groups according to Example 5.2, have the following generators:

$$\mathrm{Cl}_K(2) = \langle [\mathfrak{a}_1] \rangle_8 \times \langle [\mathfrak{a}_2] \rangle_4 \tag{6.1}$$

where

$$\begin{aligned} \mathfrak{a}_1 &= \left(1313, -\frac{1}{5}\alpha^3 - \alpha^2 - \frac{2653}{5}\alpha + 175\right) \\ \mathfrak{a}_2 &= (167, \alpha - 62). \end{aligned}$$

and

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

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

6.1.3 Computing the Shimura ray class group

Having explicitly computed the groups coker N_1 and ker N_2, we use Algorithms 5.16 and 5.17 and the discussion in Section 5.3.4 to find

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

where

$$\begin{aligned}
\mathfrak{a}_1' &= (219271, \frac{1487}{10}\alpha^3 + \alpha^2 + \frac{433471}{10}\alpha + 96582) \\
a_1' &= 35786618930050222\alpha^2 + 1457283466248917073 \\
\mathfrak{a}_2' &= \mathfrak{a}_2 \text{ (as in (6.1))} \\
a_2' &= -29828194489091522 * \alpha^2 - 366246600018109417.
\end{aligned}$$

6.1.4 Verifying that the Hilbert class field is in the compositum

We do the first step of Algorithm 3.33. We get

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

where $\mathfrak{b}_1 = (11, \frac{1}{40}\alpha_r^3 + \frac{73}{40}\alpha_r + 1)$ and $\mathfrak{b}_2 = (\frac{1}{40}\alpha_r^3 + \frac{73}{40}\alpha_r + 1)$. Continuing with the rest of the steps of Algorithm 3.33, we find that $(\star_2)$ holds. In particular, since $H_{K_0^r}(2) = K_0^r \subseteq K^r$, we find that $H_{K^r}(1) = \mathrm{CM}_{K^r,\Phi^r}(2)$. In the next section, we compute $\mathrm{CM}_{K^r,\Phi^r}(2)$.

6.1.5 Computing the Hilbert class field of the reflex

We choose a complex principally polarized abelian surface J with complex multiplication by $\mathcal{O}_K$. One such principally polarized abelian surface is isomorphic to the torus $\mathbb{C}^2/(\Phi(\mathfrak{o}))$ where $\mathfrak{o}$ is the ideal $(7, \alpha - 2)$ of $\mathcal{O}_K$, and this is what we will use moving forward. Note that this choice is arbitrary and replacing it with another choice would result in similar computations and ultimately lead to a correct result. Let

$$\xi = \frac{214997029}{566300}\alpha^3 + \frac{8754993487}{566300}\alpha.$$

A symplectic basis for $\mathbb{C}^2/(\Phi(\mathfrak{o}))$ with respect to $E_{\Phi,\mathfrak{o},\xi}$ is given by $B = \{b_1, b_2, b_3, b_4\}$ where

$$\begin{aligned} b_1 &= -298\alpha^2 - 3659, \\ b_2 &= \frac{219}{2}\alpha^3 + 1314\alpha^2 + \frac{2689}{2}\alpha + 16134, \\ b_3 &= \frac{298}{5}\alpha^3 + \frac{3659}{5}\alpha, \\ b_4 &= -\frac{219}{2}\alpha^3 + 219\alpha^2 - \frac{2689}{2}\alpha + 2689. \end{aligned}$$

Our chosen principally polarized abelian surface J is isomorphic to $J_{\boldsymbol{\tau}}$ where

$$\boldsymbol{\tau} \approx \begin{bmatrix} 0.0128\ldots + 1.3610\ldots\, i & 0.0960\ldots + 0.2842\ldots\, i \\ 0.0960\ldots + 0.2842\ldots\, i & -0.2821\ldots + 2.1236\ldots\, i \end{bmatrix}.$$

Take

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

and

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

By applying explicit Shimura reciprocity, we find, for each $[\mathfrak{g}] \in G$, a set of integers i_0, i_1, i_2, i_3, an 8th root of unity μ, and a period matrix $\boldsymbol{\tau}'$ such that

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

For each period matrix encountered in the previous step, we may then compute approximations $\tilde{\lambda}_1(\boldsymbol{\tau})$ from the squares of the relevant theta constants.

Consider the polynomial

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

where for each $[\mathfrak{g}] \in G$, the value $\widetilde{\lambda}_1(\boldsymbol{\tau})^{[\mathfrak{g}]}$ is a floating point approximation of the algebraic number $\lambda_1(\boldsymbol{\tau})^{[\mathfrak{g}]}$ with sufficiently high precision for the next steps. Using the approximating polynomial $\widetilde{p}_1(X)$ and the methods in [34, Section II.10] to recover a polynomial with coefficients in K^r from this approximation, we find a defining polynomial $p_1(X)$ of the extension $K^r(\lambda_1(\boldsymbol{\tau}))/K^r$ as follows:

$$
\begin{aligned}
d \cdot p_1(X) = dX^8 + \\
&(817037187007755454694649278206581222362877912\alpha_r^2 + \\
&652012490382096238416341412917986624598565557 6)X^7 + \\
&(-198696405384279373116960972638731931838423166 07\alpha_r^2 - \\
&849248853329871492953496544174130102365723253791)X^6 + \\
&(107334236165900575521782279233121270701940120896\alpha_r^2 + \\
&674224780191057841814522004399716222937776804332 8)X^5 + \\
&(-120818129772268450199947445206960131597987213020\alpha_r^2 - \\
&217123203014158226975333387348618526684104918728 60)X^4 + \\
&(-126436531077699593944245450915895440185655197440\alpha_r^2 + \\
&366220511676338176530393597479584117589785394700 80)X^3 + \\
&(-608686781238528841454687097765319948216262843824\alpha_r^2 - \\
&413378082854386368383560259428727748338775086935 52)X^2 + \\
&(155522952239486078905905399773792126905932430131 2\alpha_r^2 + \\
&300706491129631067213438699156981195126572280258 56)X - \\
&792805013447238765068184304616726331641601736704\alpha_r^2 - \\
&969027523371122090369919789032935113957118646067 2
\end{aligned}
$$

where $d = 2 \cdot 5 \cdot 11^8 \cdot 59^4 \cdot 61^4 \cdot 271^2 \cdot 479^2 \cdot 631^2 \cdot 911^2$. Observe that this polynomial satisfies

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

and is irreducible. Finally, one may verify that the extension of K^r defined by this polynomial is unramified and cyclic of degree 8. Since the ideal class group $\mathrm{Cl}_{K^r}(1)$ is also cyclic of degree 8, this means that

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

6.2 An example involving torsion points

In this example we compute the field $\mathrm{CM}_{K^r,\Phi^r}(6)$ for the reflex pair (K^r, Φ^r) of some primitive quartic CM field (K, Φ).

Let K_0 be the real quadratic field $\mathbb{Q}(\alpha_0) = \mathbb{Q}[X] \,/\, (X^2 + 5X + 2)$. Consider the

quartic CM field $K = K_0(\alpha)$ where α is a root of $X^2 - \alpha_0$. The CM field

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}[X] \,/\, (X^4 + 5\,X^2 + 2)$$

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

$$\Phi = \{\, \alpha \mapsto 2.1357792\ldots i \;,\; \alpha \mapsto 0.6621534\ldots i \,\}$$
$$\Phi' = \{\, \alpha \mapsto 2.7979326\ldots i \;,\; \alpha \mapsto 1.4736257\ldots i \,\}$$

6.2.1 A base period matrix

We denote by Φ the map

$$\begin{aligned} \Phi : K/O_K &\to \mathbb{C}^2/\Phi(O_K) \\ x &\mapsto (\phi_1(x), \phi_2(x)). \end{aligned}$$

The principally polarized abelian surface $(\mathbb{C}^2/\Phi(O_K), E_{\Phi,O_K,\xi})$ where

$$\xi = \frac{1}{68}\alpha^3 + \frac{11}{68}\alpha$$

has complex multiplication by K. A symplectic basis for O_K with respect to $E_{\Phi,O_K,\xi}$ is given by

$$B = (b_1, b_2, b_3, b_4) := \left(-\frac{1}{2}\alpha^3 - \frac{1}{2}\alpha^2 - 2\alpha - 2,\ \alpha,\ \frac{1}{2}\alpha^3 - \frac{1}{2}\alpha^2 + 2\alpha - 2,\ 1\right).$$

We will be using the corresponding period matrix

$$\boldsymbol{\tau} := \boldsymbol{\tau}(\Phi, O_K, \xi, B) \approx \begin{bmatrix} 0.1464\ldots + 0.9892\ldots i & -0.3535\ldots + 0.4097\ldots i \\ -0.3535\ldots + 0.4097\ldots i & -0.1464\ldots + 1.8087\ldots i \end{bmatrix}$$

for our computations. Consider

$$\Phi(O_K) = \begin{bmatrix} \phi_1(b_1) & \phi_1(b_2) \\ \phi_2(b_1) & \phi_2(b_2) \end{bmatrix} \mathbb{Z}^2 + \begin{bmatrix} \phi_1(b_3) & \phi_1(b_4) \\ \phi_2(b_3) & \phi_2(b_4) \end{bmatrix} \mathbb{Z}^2.$$

We have

$$\Lambda_{\boldsymbol{\tau}} = \boldsymbol{\tau}\mathbb{Z}^2 + \mathbb{Z}^2$$

equal to

$$\begin{bmatrix} \phi_1(b_3) & \phi_1(b_4) \\ \phi_2(b_3) & \phi_2(b_4) \end{bmatrix}^{-1} \Phi(\mathcal{O}_K)$$

Moreover, we have an isomorphism

$$\begin{aligned} \rho : \mathbb{C}^2/\Phi(\mathcal{O}_K) &\to \mathbb{C}^2/\Lambda_{\boldsymbol{\tau}} \\ \vec{\mathbf{z}} &\mapsto \begin{bmatrix} \phi_1(b_3) & \phi_1(b_4) \\ \phi_2(b_3) & \phi_2(b_4) \end{bmatrix}^{-1} \vec{\mathbf{z}}. \end{aligned}$$

6.2.2 The reflex field and Hilbert class field

The reflex of the quartic CM pair (K^r, Φ^r) of (K, Φ) is

$$K^r = \mathbb{Q}(\alpha_r) = \mathbb{Q}[X] \,/\, (X^4 + 10\,X^2 + 17).$$

The class number of K^r is 1. Therefore, we have $K^r = H_{K^r}(1)$. Moreover, by Theorem 3.2, we have $\mathrm{CM}_{K^r,\Phi^r}(1) = H_{K^r}(1)$.

Using the algorithms in Chapter 5 we find that:

- the field $\mathrm{CM}_{K^r,\Phi^r}(2)$ is a quadratic extension of $H_{K^r}(1)$, and
- $\mathrm{CM}_{K^r,\Phi^r}(3) = \mathrm{CM}_{K^r,\Phi^r}(6)$.

Moreover, the extension $\mathrm{CM}_{K^r,\Phi^r}(6)/\mathrm{CM}_{K^r,\Phi^r}(2)$ is cyclic of degree 10. We would like to find a polynomial defining this extension.

$$\begin{tikzcd}[column sep=small] \mathrm{CM}_{K^r,\Phi^r}(6) \arrow[d, dash, "10"] \\ \mathrm{CM}_{K^r,\Phi^r}(2) \arrow[d, dash, "2"] \\ K^r \arrow[d, dash, "2"] \\ K_0^r \arrow[d, dash, "2"] \\ \mathbb{Q} \end{tikzcd}$$

6.2.3 A primitive torsion point

For this example, we intend to compute $\mathrm{CM}_{K^r,\Phi^r}(6)$.

We claim that the class mod $\Lambda_{\boldsymbol{\tau}}$ of the element

$$\vec{\mathbf{p}} = \rho\left(\Phi\left(\frac{1}{6}b_3\right)\right) = \boldsymbol{\tau}\begin{bmatrix} 0 \\ 0 \end{bmatrix} + \begin{bmatrix} \frac{1}{6} \\ 0 \end{bmatrix} = \begin{bmatrix} \frac{1}{6} \\ 0 \end{bmatrix} \in \mathbb{C}^2$$

is a primitive 6-torsion point.

The ideal $6\mathcal{O}_K$ can be factored into a product of prime ideals as follows:

$$6\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

where

$$\begin{aligned}
\mathfrak{p}_1 &= (\alpha) \\
\mathfrak{p}_2 &= \left(\frac{1}{2}\alpha^3 + \frac{1}{2}\alpha^2 + 2\alpha + 2\right) \\
\mathfrak{p}_3 &= \left(\frac{1}{2}\alpha^3 - \frac{1}{2}\alpha^2 + 2\alpha - 2\right) \\
\mathfrak{p}_4 &= (3).
\end{aligned}$$

By Lemma 4.5, if we check that the point corresponding to $\vec{\mathbf{p}}$ is not in $J[\mathfrak{n}]$ for each ideal in the set $\mathfrak{n} \supsetneq \mathfrak{m}$, then $\vec{\mathbf{p}}$ is a primitive torsion point. It suffices to show that $\vec{\mathbf{p}} \notin J[\mathfrak{n}]$ for each $\{\mathfrak{n}_1, \mathfrak{n}_2, \mathfrak{n}_3, \mathfrak{n}_4\}$ where

$$\begin{aligned}
\mathfrak{n}_1 &= \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4 = (9\alpha^3 + 27\alpha) \\
\mathfrak{n}_2 &= \mathfrak{p}_1^2\mathfrak{p}_3\mathfrak{p}_4 = \left(-\frac{3}{2}\alpha^3 - \frac{3}{2}\alpha^2 - 6\alpha - 3\right) \\
\mathfrak{n}_3 &= \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_4 = \left(\frac{3}{2}\alpha^3 - \frac{3}{2}\alpha^2 + 6\alpha - 3\right) \\
\mathfrak{n}_4 &= \mathfrak{p}_1^2\mathfrak{p}_2\mathfrak{p}_3 = (-\alpha^3 - 5\alpha)
\end{aligned}$$

The generator $9\alpha^3 + 27\alpha$ of $\mathfrak{n}_1$ has the multiplication matrix

$$\begin{bmatrix} 9 & 18 & 9 & -9 \\ -9 & 0 & -9 & -9 \\ -9 & 18 & -9 & 9 \\ 18 & 54 & -18 & 0 \end{bmatrix}$$

with respect to the symplectic basis B. Right-multiplying the column vector

$$\begin{pmatrix} 0 & 0 & \frac{1}{6} & 0 \end{pmatrix}^{\mathsf{T}}$$

corresponding to $\vec{\mathbf{p}}$, we obtain the vector

$$\begin{pmatrix} \frac{3}{2} & -\frac{3}{2} & -\frac{3}{2} & -3 \end{pmatrix}^{\mathsf{T}}.$$

This is not an integer vector. We can do the same computation for the generators of $\mathfrak{n}_2, \mathfrak{n}_3, \mathfrak{n}_4$ and find that none of the computations result in an integer vector. By our discussion towards the end of Section 4.3.1, we have shown that $\vec{\mathbf{p}}$ is a primitive torsion point.

6.2.4 Approximations

By approximating the theta constants and theta functions in the formula for u_0 in Section 2.3.2, we find that

$$u_0 \approx \tilde{u_0} := 0.2476\ldots + 0.1055\ldots i,$$

where $\tilde{u_0}$ has 20000 digits of precision.

As $\mathrm{CM}_{K^r,\Phi^r}(6)$ is a degree 80 number field, we use `algdep` in PARI/GP [21] to find a degree 80 polynomial with integer coefficients whose root is $\tilde{u_0}$. In doing so, we find the polynomial

$$\begin{aligned} q(x) = {} & 1099511627776x^{80} - 211106232532992x^{79} + \ldots \\ & + 3831440292x^2 + 5563728x + 6561 \end{aligned}$$

which has a real number close to $\tilde{u_0}$ as one of its roots.

Computing $\mathrm{CM}_{K^r,\Phi^r}(2)$ by Rosenhain invariants as in Section 6.1.5, we find that

$$\mathrm{CM}_{K^r,\Phi^r}(2) = \mathbb{Q}(\beta) = \frac{\mathbb{Q}[X]}{(r(X))}$$

where

$$r(X) = X^8 - 4X^7 + 14X^6 - 28X^5 + 43X^4 - 44X^3 + 30X^2 - 12X + 2.$$

Factoring the polynomial q over $\mathrm{CM}_{K^r,\Phi^r}(2)$, we find one of its factors $p(x)$

$$\begin{aligned}1024p(x) = 1024x^{10} + (&-101376\beta^7 + 353280\beta^6 - \\ &1222656\beta^5 + 2156544\beta^4 - 3081216\beta^3 + 2601984\beta^2 - \\ &1363968\beta + 282624)x^9 + \ldots + (49846272\beta^7 - 175232514\beta^6 + \\ &612393360\beta^5 - 1087129533\beta^4 + 1587598824\beta^3 - \\ &1368002514\beta^2 + 777057984\beta - 187050261)\end{aligned}$$

This polynomial defines the extension $\mathrm{CM}_{K^r,\Phi^r}(6)/\mathrm{CM}_{K^r,\Phi^r}(2)$. We may use `rnfconductor` to verify the conductor of the extension defined by $p(x)$. The output says it has conductor 3.

6.3 On the division-minimality of the integer given in Corollary 3.3

Let (K, Φ) be a primitive quartic CM pair and let (K^r, Φ^r) be its reflex. Choosing a set S satisfying the assumption in Corollary 3.3, we find a positive integer m_S for which $(\star_{m_S})$ holds. We give an example for which the given m_S is division-minimal. That is, the condition $(\star_{m_S})$ holds, but for any proper divisor $n \mid m_S$, the condition $(\star_n)$ does not hold.

We take

$$K = \mathbb{Q}(\alpha) = \mathbb{Q}[X] \,/\, (X^4 + 65\,X^2 + 425)$$

and let L be its Galois closure. Fix an embedding $\iota_{\mathbb{C}} : L \to \mathbb{C}$. Choose the CM type Φ of K such that both embeddings send α to the positive imaginary axis. The reflex field is

$$K^r = \mathbb{Q}(\alpha_r) = \mathbb{Q}[X] \,/\, (X^4 + 130\,X^2 + 2525).$$

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

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

The ideal class group $\mathrm{Cl}_{K^r}(1)$ of K^r is cyclic of order 8 and is generated by the class $[\mathfrak{p}_1]$. We may take $S = \{\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3\}$. After verifying that this set S satisfies the hypotheses of Corollary 3.3, we find that $m_S = 8$ and conclude that

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

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

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

where

$$\begin{aligned}
\mathfrak{a}_1 &:= \left(443, \frac{1}{2}\alpha_r - \frac{263}{2}\right),\\
\mathfrak{a}_2 &:= \left(170999, \frac{1}{2}\alpha_r + \frac{120011}{2}\right),\\
\mathfrak{a}_3 &:= \left(41051, \frac{1}{2}\alpha_r - \frac{37351}{2}\right),\\
\mathfrak{a}_4 &:= \left(292141, \frac{1}{2}\alpha_r + \frac{198863}{2}\right),\\
\mathfrak{a}_5 &:= \left(172229, \frac{1}{2}\alpha_r + \frac{51253}{2}\right).
\end{aligned}$$

We compute the kernels of π_m, η, r, as defined in (3.22), (3.23), (3.25), respectively. We find that

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

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

Moreover one can check using Algorithm 3.33 that, in this example, the statement $(\star_n)$ does not hold for any proper divisor n of $m_S = 8$. In addition, computing the kernels

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

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

Finally, we remark that 8 is not the minimum integer m for which $(\star_m)$ holds. One can verify that the smallest integer for which $(\star_m)$ holds is $m = 5$. This is done by recalling that $(\star_m)$ does not hold for $m = 1, 2, 4$ as they are proper divisors of 8 and then applying Algorithm 3.33 to $m = 3$ and then $m = 5$.

6.4 Comparison with Kummer theory

Other methods for computing abelian extensions, and in particular Hilbert class fields, are known.

One approach is an algorithm based on Kummer theory [14]. This algorithm can find abelian extensions L/K, say of degree d, of a general number field K. The algorithm requires that the base field K contains the dth roots of unity or that we consider the larger field $K' = K(\zeta_d)$ to find abelian extensions of the original base field K. If the field K' is small enough so that computing its class group is still practical, we expect that using the Kummer theory algorithm is generally faster than the methods we outlined in this thesis.

Let (K, Φ) be a primitive quartic CM field and (K^r, Φ^r) its reflex. We can decompose

the Galois group $\mathrm{Gal}(H_{K^r}(1)/K^r)$ as follows:

$$G_0 \times G_1 \times \cdots \times G_r$$

where G_0 is a group of odd order and $G_1, \ldots, G_r$ are cyclic groups whose order is a power of 2. Using Galois correspondence, we find that

$$H_{K^r}(1) = L_0 L_1 \cdots L_r.$$

By Theorem 3.2, we know that $L_0 \in H_{K_0^r}(1)\,\mathrm{CM}_{K^r,\Phi^r}(1)$. It remains to compute the cyclic extensions L_i for each $i \in \{1, \ldots, r\}$, whose degrees are powers of 2.

Kummer theory is typically faster in finding defining polynomials for these cyclic extensions when the degree is small, like $1, 2, 4$ or 8. However, for primitive quartic CM fields whose class groups are cyclic of order 32, there are examples for which our implementation of the CM theory algorithm outperforms current implementations of the Kummer theory algorithm. For example, computing a very likely defining polynomial of the cyclic degree 32 extension H_{K^r} of

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

which satisfies $(\star_2)$, takes less than 10 minutes using our implementation while the `bnrclassfield` function of PARI and the `HilbertClassField` function of Magma do not finish within twenty-four hours [1].

6.5 An experiment

In this section, we give results of an experiment that we ran using CM fields from the Echidna database[2]. We highlight some interesting observations.

The purpose of this experiment is to get an idea on how

$$\min\{m : (\star_m) \text{ holds for } K^r\}$$

is distributed as K^r varies.

We ran Algorithm 3.33 on the set $\mathcal{E}$ of primitive quartic CM fields K^r satisfying

[1] The machine used is a laptop with 16 GB of RAM with an *AMD Ryzen 7 2700U* processor.
[2] https://www.i2m.univ-amu.fr/perso/david.kohel/dbs/complex_multiplication2.html

1. the field K^r appears in the Echidna database,
2. the extension $K^r/\mathbb{Q}$ is not Galois, and
3. the ideal class group $\mathrm{Cl}_{K^r}(1)$ of K^r is cyclic of even order $2 \leq h \leq 64$.

This set has more than 10^6 elements.

As hinted by the notation, these K^r are reflex fields of some CM pair (K, Φ). The choice of CM type does not affect the structure of the class group as the reflexes of two non-equivalent CM pairs are conjugate to each other [34, Example 7.7].

Motivated by Section 6.4, where we have shown that we can reduce to the case of solving unramified extensions corresponding to cyclic subgroups $\mathrm{Cl}_{K^r}(1)$, we focus on examples involving cyclic ideal class groups.

If the ideal class group of K^r has odd order, the field K^r is contained in the compositum $H_{K_0^r}(1)\,\mathrm{CM}_{K^r,\Phi^r}(1)$ by Theorem 3.2. The minimal m for these CM fields is guaranteed to be $m = 1$. In light of this observation, we only treat ideal class groups of even order.

We denote by $\mathcal{E}_h$ the subset of $\mathcal{E}$ such that the class group is cyclic of order h for the positive even integer $h \leq 64$.

Unfortunately, some elements of $\mathcal{E}$ did not finish within three minutes since our implementation gets stuck when the size of the ideals involved explode. This problem could be avoided by finding a smaller representative after each multiplication. Therefore, we only ran our experiment on a subset $\mathcal{E}'$ of $\mathcal{E}$.

Nevertheless, the examples for which our implementation does not finish make up a small percentage of $\mathcal{E}$. For each even integer $h \leq 64$, we have noted in the $(*)$ column of Table 6.1 how many examples had this problem.

For an even integer $h \leq 64$ and a positive integer m, let $\mathcal{M}'_{h,m}$ be the subset of $\mathcal{E}'_h$ such that m is the smallest positive integer for which $(\star_m)$ holds. The columns of Table 6.1 labelled by a positive integer $m \leq 2$ give the cardinality of $\mathcal{M}'_{h,m}$. The column labelled % to their right shows $|\mathcal{M}'_{h,m}|/|\mathcal{E}'_h|$.

Notice that for each $h \leq 64$, a large majority (at least 70%) of the elements of $\mathcal{E}'_h$ are also in $\mathcal{M}'_{h,1}$. Moreover, at least a third of $\mathcal{E}'_h \setminus \mathcal{M}'_{h,1}$ are in $\mathcal{M}'_{h,2}$.

The column labelled $\sum$ % of Table 6.1 adds the two % columns. Equivalently, this is the percentage of the CM fields in $\mathcal{E}_h$ wherein it suffices to compute $H_{K_0^r}(1)\,\mathrm{CM}_{K^r,\Phi^r}(1)$ or $H_{K_0^r}(2)\,\mathrm{CM}_{K^r,\Phi^r}(2)$ in order to compute $H_{K^r}(1)$. We make this distinction as we do not need to find primitive torsion points, nor find the Mumford polynomials of such torsion points.

In Table 6.2, we rewrite the data in Table 6.1 but this time, we sort the first percentage columns. We also add stars next to the h values. The number of stars represent the exponent of 2 in the prime factorization of h. Observe that when $h = 4d$ for some odd integer d, the chance that $(\star_1)$ holds tends to be less compared to the integers $h' = 2d'$ for some odd integer d'.

We now turn our attention to Table 6.3, an extension of Table 6.1 which includes larger values of m. The 0 entries of the table are marked – to be more prominent.

We make the following observation. The set $\mathcal{M}'_{h,6}$ is empty for all $h \leq 64$. This trend applies for integers m which are twice an odd prime such as $10, 14, 22, 26$, etc, looking at Table 6.4. In the interest of space, in Table 6.4, we do not include the columns for which all entries are 0.

h	$\lvert\mathcal{E}_h\rvert$	$*$	1	1 (%)	2	2 (%)	$\sum$ %
2	205	–	183	89%	14	7%	96%
4	477	–	398	83%	39	8%	92%
6	883	–	790	89%	46	5%	95%
8	979	2	838	86%	77	8%	93%
10	1562	–	1435	92%	61	4%	96%
12	1963	23	1620	83%	164	8%	91%
14	2208	2	2011	91%	101	5%	96%
16	2024	7	1763	87%	133	7%	94%
18	3019	9	2756	91%	123	4%	95%
20	3060	70	2480	81%	228	7%	88%
22	3204	16	2910	91%	131	4%	95%
24	3589	33	3073	86%	245	7%	92%
26	3514	28	3201	91%	146	4%	95%
28	3809	176	2931	77%	328	9%	86%
30	5372	70	4899	91%	227	4%	95%
32	3569	47	3041	85%	248	7%	92%
34	4092	59	3653	89%	196	5%	94%
36	4972	231	3843	77%	464	9%	87%
38	4352	94	3892	89%	190	4%	94%
40	4649	151	3787	81%	385	8%	90%
42	6181	168	5409	88%	304	5%	92%
44	4797	305	3574	75%	469	10%	84%
46	4453	130	3949	89%	213	5%	93%
48	5387	143	4395	82%	485	9%	91%
50	5365	160	4666	87%	312	6%	93%
52	5086	378	3650	72%	564	11%	83%
54	5694	216	4887	86%	300	5%	91%
56	5157	227	4067	79%	469	9%	88%
58	4590	185	3925	86%	258	6%	91%
60	7772	651	5623	72%	872	11%	84%
62	4720	223	4016	85%	277	6%	91%
64	4411	220	3453	78%	442	10%	88%

Table 6.1: Cardinalities of the $\mathcal{E}_h$, number of failed cases (i.e. $\lvert\mathcal{E}_h \setminus \mathcal{E}'_h\rvert$), cardinalities of the $\mathcal{M}'_{h,m}$ for $m \in \{1, 2\}$.

	h	1 (%)	2 (%)
★	10	92%	4%
★	18	91%	4%
★	30	91%	4%
★	26	91%	4%
★	14	91%	5%
★	22	91%	4%
★	6	89%	5%
★	38	89%	4%
★	34	89%	5%
★	2	89%	7%
★	46	89%	5%
★	42	88%	5%
★★★★	16	87%	7%
★	50	87%	6%
★	54	86%	5%
★★★	24	86%	7%
★★★	8	86%	8%
★	58	86%	6%
★★★★★	32	85%	7%
★	62	85%	6%
★★	4	83%	8%
★★	12	83%	8%
★★★★	48	82%	9%
★★★	40	81%	8%
★★	20	81%	7%
★★★	56	79%	9%
★★★★★★	64	78%	10%
★★	36	77%	9%
★★	28	77%	9%
★★	44	75%	10%
★★	60	72%	11%
★★	52	72%	11%

Table 6.2: Sorted % columns.

h	1	2	3	4	5	6	7	8
2	183	14	6	–	2	–	–	–
4	398	39	11	1	24	–	–	3
6	790	46	25	8	12	–	–	–
8	838	77	14	2	31	–	2	6
10	1435	61	30	8	23	–	3	2
12	1620	164	58	6	85	–	2	2
14	2011	101	43	10	29	–	4	8
16	1763	133	29	8	57	–	2	11
18	2756	123	77	8	31	–	5	6
20	2480	228	117	8	138	–	5	9
22	2910	131	68	32	38	–	4	5
24	3073	245	64	5	106	–	3	24
26	3201	146	71	22	36	–	6	2
28	2931	328	154	17	184	–	5	9
30	4899	227	87	25	52	–	2	9
32	3041	248	42	19	110	–	1	26
34	3653	196	94	30	33	–	10	15
36	3843	464	194	17	192	–	7	16
38	3892	190	96	20	44	–	2	11
40	3787	385	83	16	142	–	3	43
42	5409	304	156	39	72	–	10	10
44	3574	469	210	15	200	–	11	5
46	3949	213	78	11	52	–	11	5
48	4395	485	89	21	149	–	5	42
50	4666	312	130	27	44	–	12	10
52	3650	564	225	29	209	–	11	14
54	4887	300	151	60	65	–	6	7
56	4067	469	101	30	150	–	3	53
58	3925	258	120	28	55	–	6	10
60	5623	872	273	40	284	–	12	12
62	4016	277	110	42	39	–	4	5
64	3453	442	64	29	141	–	2	31

Table 6.3: Cardinality of $\mathcal{M}'_{h,m}$ for $1 \leq m \leq 8$.

h	11	12	13	17	19	21	24	28
2	–	–	–	–	–	–	–	–
4	1	–	–	–	–	–	–	–
6	2	–	–	–	–	–	–	–
8	–	3	2	1	–	–	1	–
10	–	–	–	–	–	–	–	–
12	1	1	1	–	–	–	–	–
14	–	–	–	–	–	–	–	–
16	1	6	4	2	–	1	–	–
18	2	1	1	–	–	–	–	–
20	3	1	–	1	–	–	–	–
22	–	–	–	–	–	–	–	–
24	–	13	15	7	–	–	–	1
26	2	–	–	–	–	–	–	–
28	2	1	–	2	–	–	–	–
30	1	–	–	–	–	–	–	–
32	4	17	5	5	1	2	1	–
34	2	–	–	–	–	–	–	–
36	4	2	–	2	–	–	–	–
38	1	2	–	–	–	–	–	–
40	2	20	6	10	1	–	–	–
42	4	3	6	–	–	–	–	–
44	2	1	3	2	–	–	–	–
46	3	–	1	–	–	–	–	–
48	1	32	11	10	–	4	–	–
50	1	3	–	–	–	–	–	–
52	4	2	–	–	–	–	–	–
54	1	1	–	–	–	–	–	–
56	3	25	19	10	–	–	–	–
58	2	1	–	–	–	–	–	–
60	4	–	–	1	–	–	–	–
62	3	1	–	–	–	–	–	–
64	1	13	8	6	–	1	–	–

Table 6.4: Cardinality of $\mathcal{M}'_{h,m}$ for $11 \leq m \leq 28$, with empty columns skipped.

Bibliography

[1] Karim Belabas. "Topics in computational algebraic number theory". In: *J. Théor. Nombres Bordeaux* 16.1 (2004), pp. 19–63. DOI: 10.5802/jtnb.433. URL: http://jtnb.cedram.org/item?id=JTNB_2004__16_1_19_0.

[2] Christina Birkenhake and Herbert Lange. *Complex abelian varieties*. Second. Vol. 302. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, 2004, pp. xii+635. ISBN: 3-540-20488-1. DOI: 10.1007/978-3-662-06307-1.

[3] 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. ISSN: 1937-0652. DOI: 10.2140/ant.2011.5.495.

[4] Gabriel Cardona and Jordi Quer. "Field of moduli and field of definition for curves of genus 2". In: *Computational aspects of algebraic curves*. Vol. 13. Lecture Notes Ser. Comput. World Sci. Publ., Hackensack, NJ, 2005, pp. 71–83. DOI: 10.1142/9789812701640_0006.

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

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

[7] Henri Cohen and Xavier-François Roblot. "Computing the Hilbert class field of real quadratic fields". In: *Math. Comp.* 69.231 (2000), pp. 1229–1244. ISSN: 0025-5718. DOI: 10.1090/S0025-5718-99-01111-4. URL: https://doi.org/10.1090/S0025-5718-99-01111-4.

[8] Henri Cohen and Peter Stevenhagen. "Computational class field theory". In: *Algorithmic number theory: lattices, number fields, curves and cryptography*. Vol. 44. Math. Sci. Res. Inst. Publ. Cambridge Univ. Press, Cambridge, 2008, pp. 497–534.

[9] Romain Cosset. "Applications des fonctions thêta à la cryptographie sur courbes hyperelliptiques." Theses. Université Henri Poincaré - Nancy I, Nov. 2011. URL: https://tel.archives-ouvertes.fr/tel-00642951.

[10] David A. Cox. *Primes of the form $x^2 + ny^2$*. Second. Pure and Applied Mathematics (Hoboken). Fermat, class field theory, and complex multiplication. John Wiley & Sons, Inc., Hoboken, NJ, 2013, pp. xviii+356. ISBN: 978-1-118-39018-4. DOI: 10.1002/9781118400722. URL: https://doi.org/10.1002/9781118400722.

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

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

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

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

[15] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*. Vol. 201. Graduate Texts in Mathematics. An introduction. Springer-Verlag, New York, 2000, pp. xiv+558. ISBN: 0-387-98975-7; 0-387-98981-1. DOI: 10.1007/978-1-4612-1210-2. URL: https://doi.org/10.1007/978-1-4612-1210-2.

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

[17] Kristin Lauter. "Geometric methods for improving the upper bounds on the number of rational points on algebraic curves over finite fields". In: *J. Algebraic Geom.* 10.1 (2001). With an appendix in French by J.-P. Serre, pp. 19–36. ISSN: 1056-3911.

[18] J.S. Milne. *Class Field Theory (v4.03)*. Available at www.jmilne.org/math/. 2020.

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

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

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

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

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

[24] Xavier-François Roblot. "Algorithmes de Factorisation dans les Extensions Relatives et Applications de la Conjecture de Stark à la Construction des Corps de Classes de Rayon". PhD thesis. Université Bordeaux I, 1997.

[25] Xavier-François Roblot. "Stark's conjectures and Hilbert's twelfth problem". In: *Experiment. Math.* 9.2 (2000), pp. 251–260. ISSN: 1058-6458. URL: http://projecteuclid.org/euclid.em/1045952349.

[26] Xavier-François Roblot. "Unités de Stark et corps de classes de Hilbert". In: *C. R. Acad. Sci. Paris Sér. I Math.* 323.11 (1996), pp. 1165–1168. ISSN: 0764-4442.

[27] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.4)*. https://www.sagemath.org. 2021.

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

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

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

[31] Goro Shimura and Yutaka Taniyama. *Complex multiplication of abelian varieties and its applications to number theory*. Vol. 6. Publications of the Mathematical Society of Japan. The Mathematical Society of Japan, Tokyo, 1961, pp. xi+159.

[32] Joseph H. Silverman. *The arithmetic of elliptic curves*. Second. Vol. 106. Graduate Texts in Mathematics. Springer, Dordrecht, 2009, pp. xx+513. ISBN: 978-0-387-09493-9. DOI: 10.1007/978-0-387-09494-6. URL: https://doi.org/10.1007/978-0-387-09494-6.

[33] Marco Streng. "An explicit version of Shimura's reciprocity law for Siegel modular functions". In: (2021). arXiv: 1201.0020 [math.NT].

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

[35] Paul van Wamelen. "Equations for the Jacobian of a hyperelliptic curve". In: *Trans. Amer. Math. Soc.* 350.8 (1998), pp. 3083–3106. ISSN: 0002-9947. DOI: 10.1090/S0002-9947-98-02056-X.

[36] André Weil. *Basic number theory*. Third. Die Grundlehren der mathematischen Wissenschaften, Band 144. Springer-Verlag, New York-Berlin, 1974, pp. xviii+325.

[37] André Weil. "Zum Beweis des Torellischen Satzes". In: *Nachr. Akad. Wiss. Göttingen. Math.-Phys. Kl. IIa.* 1957 (1957), pp. 33–53. ISSN: 0065-5295.

Acknowledgments

I would like to thank my PhD supervisors – Andreas Enge and Marco Streng – who have both always made sure that my work is the best as it can be given the time constraints. Both of you have been supportive and patient with me through the many questions, requests for comments, and administrative procedures that a cotutelle PhD entails. I would also like to thank my jury for agreeing to read my manuscript and be involved in my defense.

Je voudrais remercier Paul Geniet, et Aurel Page pour corriger les épreuves dans l'introduction français. Graag wil ik Bas Jacobs en Peter Koymans bedanken voor hun hulp bij de Nederlandse samenvatting.

I am happy to be part of the friendly number theory teams of both universities whose members have always answered questions kindly, notably Bill Allombert, Karim Belebas, and Peter Bruin who I'm sure to have asked more than several times!

At the beginning of the PhD, language was a bigger barrier than it is now. Thankfully, I had several good friends who always helped me with bureaucracy, such as Christopher Niesen and Krisztian Benyo.

For all the interesting conversations throughout my PhD, I would like to thank my Leiden officemates Rosa, Ruihua, and Stefan, my Bordeaux lunchmates Abhi, Edo, Emmanuele, and Quentin. For agreeing to be my officemate and for all the chats in and out of the office, I would like to thank Fredrik Johansson.

When I came to visit Leiden at the start of my PhD, I didn't expect I would make friends within that one short week. But I did. Thank you Francesco, for all the crazy adventures all over Europe – mathematical or otherwise, Sebastiano, for geeking out with me when it comes to Linux and open-source, Sergej, for always offering to host whenever I go to The Netherlands, and Matteo for all the board games we've played. I can't wait for the day where we can all hang-out together again!

I would like to thank several people for the online conversations about anything and everything. Without my calls with Giovanni, Goma, Guido, Martina, Miggy, Roberto, and Stevan, I would have probably gone insane from isolating during the lockdowns. I look forward to our future conversations, hopefully some of them in-person.

I would like to thank Corentin Prigent, who has been an all-around good friend and one of the few ones who is consistently within walking distance. I would also like to thank my former-acquaintance now-friend Marco Bravin for helping me find an apartment in Bordeaux, for all the delicious weekend pasta dishes, and for being the best quasi-coloc. See you both in Bordeaux, or anywhere else in the world!

I would have never had considered going to Europe much less enter a PhD programme here if it weren't for the encouragement of Fidel Nemenzo and Peter Stevenhagen during the CIMPA-ICTP Manila Summer School. Thank you for believing in my mathematics and programming skills from the very start.

While my scientific eureka moments came with colleagues, most of my recent life realizations came while I started to be with Pierre Brun. Your patience and support enabled me to be better.

Maraming sa mga kaibigan na game pa ring makipagkita at nagpaparamdam pa rin after all these years kahit wala na ako sa Pilipinas, pati na rin sa yaya, sa kapatid, at sa mga pinsan kong forever supportive.

Kay mom and dad na hindi pa rin tumigil ang suporta kahit umabot na sa point na hindi niyo na naiintindihan o nakikita kung ano'ng ginagawa ko, salamat!

Curriculum Vitae

Jared Asuncion was born in the Philippines in 1992. As a grade school student in Pasig Catholic College, he competed in various spelling bees, writing contests and mathematics competitions. After graduating as valedictorian, he started his high school studies in Ateneo de Manila High School where he joined a student organization which teaches English and Mathematics to Filipino grade school students.

During his undergraduate studies which started in 2008, he joined several ACM-ICPC team programming competitions. He would later help found the Philippines' National Olympiad in Informatics with the friends he met in these competitions.

He wrote his bachelor thesis on ranks of elliptic curves of the form $y^2 = x^3 + px$ for primes $p < 1000$ under the supervision of Fidel Nemenzo and graduated cum laude in 2012 from the University of the Philippines, Diliman.

A year after, he attended the *CIMPA-ICTP school on Algebraic Curves over Finite Fields* held in Quezon City, Philippines. In this school, he met Peter Stevenhagen who encouraged him to apply to the ALGANT Masters Programme.

In 2014, he moved to Leiden for his first year of the ALGANT programme and he wrote his Master thesis *Tower decomposition of Hilbert class fields* in Bordeaux under the supervision of Andreas Enge. He obtained Masters diplomas from both Leiden University and University of Bordeaux in 2016.

After finishing his Masters, he was hired as an engineer in INRIA and implemented the Elliptic Curve Primality Proving (ECPP) algorithm in the open-source computer algebra system PARI/GP.

He started his PhD in 2017 under a cotutelle between Leiden University and University of Bordeaux under the supervision of Andreas Enge and Marco Streng.

After the PhD, he intends to stay in Europe to find a job but also intends to continue helping advance math and programming education in whatever way he can.