Class Invariants

Daniel Vallières

Master of Science

Department of Mathematics and Statistics

McGill University

Montréal,Québec

2005-19-12

A thesis submitted to McGill University in partial fulfilment of the requirements of the degree of Master of Science

Copyright ©Daniel Vallières, 2005

Library and Archives Canada

Published Heritage Branch

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque et Archives Canada

Direction du Patrimoine de l'édition

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence
ISBN: 978-0-494-24816-4
Our file Notre référence
ISBN: 978-0-494-24816-4

NOTICE:
The author has granted a non-exclusive license allowing Library and Archives Canada to reproduce, publish, archive, preserve, conserve, communicate to the public by telecommunication or on the Internet, loan, distribute and sell theses worldwide, for commercial or non-commercial purposes, in microform, paper, electronic and/or any other formats.

The author retains copyright ownership and moral rights in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

AVIS:
L'auteur a accordé une licence non exclusive permettant à la Bibliothèque et Archives Canada de reproduire, publier, archiver, sauvegarder, conserver, transmettre au public par télécommunication ou par l'Internet, prêter, distribuer et vendre des thèses partout dans le monde, à des fins commerciales ou autres, sur support microforme, papier, électronique et/ou autres formats.

L'auteur conserve la propriété du droit d'auteur et des droits moraux qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

In compliance with the Canadian Privacy Act some supporting forms may have been removed from this thesis.

While these forms may be included in the document page count, their removal does not represent any loss of content from the thesis.

Conformément à la loi canadienne sur la protection de la vie privée, quelques formulaires secondaires ont été enlevés de cette thèse.

Bien que ces formulaires aient inclus dans la pagination, il n'y aura aucun contenu manquant.

Canada

ACKNOWLEDGEMENTS

First, I would like to thank FQRNT for their financial support. Many thanks also to my parents, my brother and my sister who always listen to my mathematical stories even though I am not always able to share clearly my passion. Thanks also to my friends outside the department with whom I always have good time even though they do not like mathematics! A word of gratitude to all students and teachers of the mathematical department of the Université de Montréal and McGill, especially Danny, Olivier, Matthew, Shahab and Gabriel. Special thanks to Francisco Thaine who taught me my first class in algebraic number theory and to Abraham Broer with whom I have worked during one summer. Thanks to Farshid Hajir for the great discussions we had while he was at Montréal and his computational tricks. I am indebted also to Louis for his big gift consisting of a whole bookcase of mathematical books. It was and it will be very useful. I would like also to thank all the staff of the Department of Mathematics and Statistics.

Last but not least, I thank my supervisor Eyal Goren who gave me this marvelous project and also for his kindness and disponibility.

ABSTRACT

In this thesis, we present numerical examples of class invariants constructed by DeShalit–Goren in [14]. These class invariants are an attempt to generalize the classical theory of elliptic units. The hope is that a better understanding of these class invariants would lead to other cases of Stark's conjectures expressing the value of derivatives of Artin L-functions at $s = 0$ in term of a regulator of linear forms in logarithms of S-units.

ABRÉGÉ

Dans ce mémoire, nous présentons des exemples numériques d'invariants de classes. Ces invariants de classes, dont la construction est présentée dans [14], peuvent être vus comme une généralisation des unités elliptiques. Une meilleure compréhension de ces invariants pourrait peut-être mener à de nouveaux cas des conjectures de Stark qui expriment les valeurs des dérivés des fonctions L d'Artin en $s = 0$ en termes de régulateurs de formes linéaires en logarithmes de S-unités.

TABLE OF CONTENTS

CHAPTER 1
Introduction

In the XVIIIth century, Leonhard Euler (1707-1783) gave his marvelous proof of the infinitude of prime numbers using the infinite series

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

It was perhaps the first time that an analytical tool was used in order to prove a statement in number theory.

Later on, Gustav Lejeune Dirichlet (1805-1859) managed to prove his celebrated theorem on primes in arithmetic progressions. His idea was to adapt Euler's proof of the infinitude of prime numbers to this case. In order to do so, he introduced the concept of Dirichlet L-series. This was probably one of his greatest achievements.

Since then more and more general L-series have been introduced in number theory by Heinrich Weber (1842-1913), Erich Hecke (1887-1947), Emil Artin (1898-1962), and André Weil (1906-1998) among others. The modern notion of Artin L-function contains as particular cases all the Dedekind zeta functions and the Dirichlet L-series. These L-functions seem to encode a lot of arithmetical information. Unfortunately, it is not easy to extract their secrets. Whenever a new discovery is made about these L-functions, number theorists are well rewarded.

One of these nice discoveries is the class number formula. If $\zeta_K(s)$ is the Dedekind zeta function of a number field K, then

$$\lim_{s \to 1}(s-1)\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}\mathrm{Reg}(K)}{\omega_K\sqrt{|\Delta_K|}} \cdot h_K,$$

where h_K is the class number, r_1 the number of real embeddings, r_2 the number of pair of complex conjugate embeddings, $\mathrm{Reg}(K)$ the regulator, Δ_K the discriminant,

and ω_K the number of roots of unity in K. Using the functional equation of $\zeta_K(s)$, this statement can be translated into a simpler formula at $s = 0$:

$$\zeta_K(s) = -\frac{h_K \mathrm{Reg}(K)}{\omega_K} s^{r_1+r_2-1} + O(s^{r_1+r_2}).$$

In the 70's, Harold Stark tried to find a similar formula for a general Artin L-function. Moreover, he gave a more precise conjecture in the case of an L-function of an abelian extension with a *simple* zero at $s = 0$. If these conjectures are true, then it would give a partial solution to Hilbert's 12th problem. Hilbert's 12th problem consists in finding transcendental functions such that when evaluated at some points, they give explicit generators of abelian extensions of number field. The prototypical example is the set of cyclotomic fields which are generated by particular values of the exponential function. This is why Stark's conjectures are one of the most important open problems in number theory.

The rank one abelian conjecture predicts the existence of a unit called Stark's unit. Stark was able to prove his conjectures when the base field is either $\mathbb{Q}$ or a quadratic imaginary field. For this, he used respectively the theory of cyclotomic units and the theory of elliptic units. Indeed, in both of these cases, it is known how to explicitly construct units in abelian extensions of the base field. In the latter case, the contruction of elliptic units is possible thanks to the theory of classical modular function and the theory of complex multiplication.

It became then an outstanding problem to construct units in abelian extension of number fields. The hope is that this would lead to other cases of Stark's conjectures.

Note that the two cases which are known are exactly the fields for which explicit class field theory is known. Goro Shimura and Yukata Taniyama (1927-1958) extended the theory of complex multiplication to a wider class of number fields called CM-fields. Let K be a CM-field (i.e. a totally complex field which is a quadratic extension of a totally real field), and let K^* be a reflex field of K, which is another

CM-field associated to K. The theory of complex multiplication allows one to generate abelian extensions of the reflex field K^* using values of Siegel modular functions evaluated at CM-points associated to K.

In the paper [14], Ehud De Shalit and Eyal Goren gave an attempt to generalize the construction of elliptic units to CM-field of degree four. They constructed class invariants in the Hilbert class field of the reflex field K^*. They proved several properties of these invariants, but they ask a fundamental question: **Are these class invariants global units?** This question is the motivation of this thesis.

Our goal here is fairly modest. It consists of writing a program in order to have numerical examples of these class invariants. We remark also that the link with L-series, if any, is still unknown.

In Chapter 2, we recall Dirichlet's class number formula, and use it as a motivation for Stark's conjectures. Chapter 3 is provided to recall the main results of class field theory in classical language. The classical language is more efficient for computational purposes. We follow then with Chapter 4 that contains a brief introduction to Stark's conjectures. Chapter 5 gives an overview of the construction of elliptic units, while Chapter 6 gives the background needed for the construction of DeShalit–Goren invariants. Finally, in Chapter 7, we present the construction of the class invariants, and the algorithm used for their calculation is presented in Chapter 8. The program itself can be found in appendix A and we present some numerical results in appendix B.

1.1 Notation

We use the standard notations $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ for the set of integers, rational numbers, real numbers and complex numbers, respectively. Whenever R is a ring, $R^\times$ means the group of units of this ring. The symbol K will be used to denote a number field.

One finds below the symbols we use. For each of them, we wrote it in the chapter of its first appearance.

Chapter 2

- $\zeta(s)$: The Riemann zeta function.
- $\zeta_K(s)$: The Dedekind zeta function of the number field K.
- $\mathbb{N}(\mathfrak{a})$: The norm of the fractional ideal $\mathfrak{a}$.
- $\mathrm{Re}(s)$: The real part of s.
- $\mathrm{Cl}(K)$: The class group of K.
- h_K: The class number of K.
- κ_K: See section 2.2.3.
- $[K : \mathbb{Q}]$: The degree of the field extension $K/\mathbb{Q}$.
- ι_n: Number of integral ideals with norm n.
- $\iota(t)$: Number of integral ideals with norm $\leq t$.
- $\iota_C(t)$: Number of integral ideals in the ideal class C with norm $\leq t$.
- $\mathrm{Res}(f, s)$: Residue of f at s.
- r_1: Number of real embeddings.
- r_2: Number of pair of complex embeddings.
- Reg: Regulator of a set of units.
- ω_K: Number of roots of unity in K.
- Δ_K: Discriminant of K.
- ϕ: Euler ϕ-function.
- ζ_m: m-th root of unity.

- $\mathrm{Gal}(L/K)$: Galois group of the galois extension L/K.
- $e(\mathfrak{P}|\mathfrak{p})$: Ramification index.
- $f(\mathfrak{P}|\mathfrak{p})$: Inertia index.
- χ_1: The trivial character.

Chapter 3

- O_K: Maximal order of K.
- $I(K)$: The group of fractional ideals of K.
- $P(K)$: The group of principal ideals of K.
- $\mathrm{Cl}_+(K)$: The narrow class group of K.
- $\lambda \gg 0$: A totally positive element.
- $\mathfrak{m}$: A modulus.
- $\mathrm{Cl}_\mathfrak{m}(K)$: The ray class group modulo $\mathfrak{m}$.
- $I_\mathfrak{m}(K)$: The fractional ideals relatively prime with $\mathfrak{m}$.
- $P_\mathfrak{m}(K)$: See definition 3.2.4.
- $\varphi_{L/K}$: The Artin map of the abelian extension L/K.
- $I(\mathfrak{P}|\mathfrak{p})$: The inertia group of the prime $\mathfrak{P}$ lying above $\mathfrak{p}$.
- $D(\mathfrak{P}|\mathfrak{p})$: The decomposition group of the prime $\mathfrak{P}$ lying above $\mathfrak{p}$.
- $k_\mathfrak{p}$: The residue field $O_K/\mathfrak{p}$.
- $H_\mathfrak{m}$: An ideal subgroup modulo $\mathfrak{m}$.
- H: An ideal group (equivalence class of ideal subgroups).
- $\mathrm{Cl}_H(K)$: The ideal class group of the ideal group H.
- $\mathfrak{f}(L/K)$: The conductor of the abelian extension L/K.
- H_K: The small Hilbert class field.
- H_K^+: The big Hilbert class field.
- $\mathfrak{f}(\chi)$: The Artin conductor of the character χ.
- $G_i(\mathfrak{P}|\mathfrak{p})$: Higher ramification groups.
- $W(\chi)$: The Artin root number.

Chapter 4

- $O_{K,S}$: The S-units.
- $\mathrm{St}(L/K,S)$: Abelian rank one conjecture.

Chapter 5

- $\wp$: Weierstrass' elliptic function.
- $\mathbb{C}_{E,\Lambda}$: The field of elliptic functions with respect to Λ.
- $\mathrm{Im}(z)$: Imaginary part of the complex number z.
- $\mathbb{A}^n(k)$: The affine space of dimension n.
- g_2, g_3: Weierstrass' constants.
- $\mathrm{SL}_2(R)$: The group of matrices with coefficients in R with determinant 1.
- $\mathrm{PSL}_2(R)$: $\mathrm{SL}_2(R)/Z(\mathrm{SL}_2(R))$, where $Z(\mathrm{SL}_2(R))$ is the center of $\mathrm{SL}_2(R)$.
- $\mathrm{GL}_2(R)$: The group of matrices with coefficients in R with determinant in $R^\times$.
- $\mathrm{GL}_2^+(\mathbb{R})$: The group of matrices with determinant > 0.
- $\mathfrak{h}$: The upper-half plane.
- $\mathfrak{h}^*$: The upper-half plane with the cusps of a discrete group Γ.
- $\sigma_k(n)$: $\sum_{d|n} d^k$.
- $\Gamma(N)$: Principal congruence subgroup modulo N.
- J: The elliptic modular function.
- j: $1728 \cdot J$.
- Δ: The discriminant modular form.
- γ: The Euler constant.
- η: The Dedekind eta-function.

Chapter 6

- $M_{m\times n}(R)$: The set of $m \times n$ matrices with coefficients in R.
- $\mathbb{P}^2(\mathbb{C})$: The projective plane.
- $\mathrm{Diag}(d_1,\ldots,d_n)$: The diagonal matrix with $d_1,\ldots,d_n$ on the diagonal.
- $\mathfrak{h}_n$: The Siegel space.

- $\mathrm{Sp}_n(\mathbb{R})$: The symplectic matrices with coefficients in $\mathbb{R}$.
- ρ_a: The analytic representation.
- ρ_r: The rational representation.
- K^*: The reflex field of a CM-field K.
- Φ^*: The reflex type of a CM-type Φ.

CHAPTER 2
L-series and their value at $s = 1$

The main reference for this section is [42]. In particular, all details of the proof of Dirichlet's class number formula can be found there. Another useful reference is [13]. For some interesting historical facts, see [16].

2.1 The Pell equation

Going back to the dawn of ages, people were interested in solving the following equation

$$x^2 - dy^2 = \pm 1,$$

for $x, y \in \mathbb{Z}$ and d a positive integer. One reason why people were interested in that equation is that for x and y big enough, it gives a rational approximation of $\sqrt{d}$. Indeed, we have then $d = (\mp 1 + x^2)/y^2 \approx x^2/y^2$ when x and y are big enough. Then $\sqrt{d} \approx |x|/|y|$. Nowadays we call this equation the Pell equation following Leonhard Euler (1707-1783), even though it is often said that it has nothing to do with the english mathematician John Pell (1611-1685). Mathematicians tried to solve this equation and Joseph-Louis Lagrange (1736-1813) solved Pell equation using the theory of continued fractions.

Why is this equation so important? In modern algebraic number theory, solutions of Pell's equation correspond to units in real quadratic fields $\mathbb{Q}(\sqrt{d})$, where d is a positive square-free integer, and $d \equiv 2, 3 \pmod 4$. Moreover there exists a unit $\varepsilon = x + y\sqrt{d}$ (if we ask also that $\varepsilon > 1$ then it is unique) such that all other units are of the form $\pm \varepsilon^n = (x + y\sqrt{d})^n = x_n + y_n\sqrt{d}$, for some $n \in \mathbb{Z}$. In other words, we can find all solutions of Pell's equation if we know this fundamental unit. They are precisely the numbers $\pm(x_n, y_n)$. When n is big, it gives

a good approximation of $\sqrt{d}$. One reason why it is important to know this ε is that thanks to Gustav Lejeune Dirichlet (1805-1859), we can compute the class number of a real quadratic field if we know this fundamental unit ε. This is done through the famous Dirichlet class number formula.

2.2 The Dirichlet class number formula

2.2.1 The Riemann zeta function

Euler has been the first to introduce the zeta function of a real variable. He used it to give another proof of the infinitude of prime numbers. The proof goes like this. He defined the zeta function by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

This series converges absolutely for $s > 1$ and has an Euler product

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

for $s > 1$. Taking the logarithm, we find $\log \zeta(s) = \log \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$, for $s > 1$. A limit argument allows one to interchange the product and the logarithm to obtain $\log \zeta(s) = \sum_p \log \left(1 - \frac{1}{p^s}\right)^{-1}$, also for $s > 1$. Now using the series expansion of the logarithm function $\log \frac{1}{1-x} = \sum_{n=1}^{\infty} \frac{x^n}{n}$ which is valid for $|x| < 1$, we get $\log \zeta(s) = \sum_p \sum_{n=1}^{\infty} \frac{1}{np^{ns}} = \sum_p \frac{1}{p^s} + g(s)$, where $g(s) = \sum_p \sum_{n=2}^{\infty} \frac{1}{np^{ns}}$. Euler then showed that $g(s)$ is bounded near $s = 1$. Now let $s \to 1$ in the equation

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + g(s).$$

Suppose there exists only finitely many primes. The right-hand side would be bounded around $s = 1$. On the other hand, $\zeta(s)$ tends to the harmonic series which diverges so we have a contradiction. We conclude that

$$\sum_p \frac{1}{p} = \infty,$$

and that there are infinitely many primes.

Then, Bernhard Riemann (1826-1866) allowed complex variables and used it to study the distribution of prime numbers. He proved that it satisfies a functional equation and that it has a meromorphic continuation to the whole complex plane with only one pole at $s = 1$ which is simple and has residue 1. For the purpose of this present chapter, we just need to know that it has a meromorphic continuation on the domain $\mathrm{Re}(s) > 0$ with a pole of order 1 at $s = 1$. After Riemann, it is customary to work with zeta and L-functions of a complex variable. Euler's argument works in exactly the same way if we allow the variable s to be complex.

2.2.2 The Dedekind zeta function

Let K be any number field. Following Richard Dedekind (1831-1916), we define a generalization of the Riemann zeta function (if $K = \mathbb{Q}$, we get back the Riemann zeta function), the Dedekind zeta function:

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\iota_n}{n^s},$$

where ι_n is the number of integral ideals $\mathfrak{a}$ in K such that $\mathbb{N}(\mathfrak{a}) = n$. In order to study the convergence of that function, we recall for convenience the fundamental lemma on Dirichlet series, that is series of the form $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$, where $a_n \in \mathbb{C}$.

Lemma 2.2.1 *Let $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet's series. Suppose $\sum_{n \leq t} a_n = O(t^r)$, then the series converges for $\mathrm{Re}(s) > r$, and is a holomorphic function on this half-plane.*

Thus, we are led to study $\iota(t) = \sum_{1 \leq n \leq t} \iota_n$ which is the number of integral ideals $\mathfrak{a} \neq 0$ with $\mathbb{N}(\mathfrak{a}) \leq t$. In order to do this, we split $\iota(t)$ as a finite sum $\iota(t) = \sum_{C \in \mathrm{Cl}(K)} \iota_C(t)$, where $\iota_C(t)$ is the number of integral ideals $\mathfrak{a} \in C$ (C is an ideal class) with $\mathbb{N}(\mathfrak{a}) \leq t$. It is not easy to prove, but the following is true. If $C \in \mathrm{Cl}(K)$ then there exists a constant κ, not depending on C and made explicit below, such that

$$\iota_C(t) = \kappa \cdot t + O\left(t^{1-\frac{1}{[K:\mathbb{Q}]}}\right). \tag{2.1}$$

Summing over all ideal classes $C \in \mathrm{Cl}(K)$, we get

$$\iota(t) = h_K \cdot \kappa \cdot t + O\left(t^{1-\frac{1}{[K:\mathbb{Q}]}}\right). \tag{2.2}$$

Coming back to the Dedekind zeta function, we rewrite it as

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\iota_n - h_K \cdot \kappa}{n^s} + h_K \cdot \kappa \cdot \zeta(s), \tag{2.3}$$

where h_K is the class number of K. Using Equation (2.2) and the lemma on Dirichlet series, we see that the series on the right-hand side of this last equation represents an analytic function for $\mathrm{Re}(s) > 1 - 1/[K : \mathbb{Q}]$. Since $\zeta(s)$ represents a meromorphic function on $\mathrm{Re}(s) > 0$ with only one simple pole at $s = 1$, $\zeta_K(s)$ represents then a meromorphic function on the half-plane $\mathrm{Re}(s) > 1 - 1/[K : \mathbb{Q}]$ with only one pole of order 1 at $s = 1$ with residue $\mathrm{Res}(\zeta_K, s = 1) = \lim_{s\to 1}(s-1)\zeta_K(s) = h_K \cdot \kappa$. For $\mathrm{Re}(s) > 1$, the Equation (2.3) can be written as $\frac{\zeta_K(s)}{\zeta(s)} = \frac{1}{\zeta(s)} \sum_{n=1}^{\infty} \frac{\iota_n - h_K \cdot \kappa}{n^s} + h_K \cdot \kappa$. Letting $s \longrightarrow 1$, we get then

$$\rho := \lim_{s\to 1} \frac{\zeta_K(s)}{\zeta(s)} = h_K \cdot \kappa.$$

Therefore, if we are able to compute ρ, and if we know κ then we would be able to compute the class number. When K is abelian, using class field theory (the Kronecker-Weber theorem), L-series and Euler product, one can do this and it leads to Dirichlet's class number formula.

2.2.3 The constant κ

The constant κ which appears above is

$$\kappa = \frac{2^{r_1+r_2} \cdot \pi^{r_2} \cdot \mathrm{Reg}(K)}{\omega_K \cdot \sqrt{|\Delta_K|}},$$

where

- r_1 is the number of real embeddings.
- r_2 is the number of complex embeddings divided by 2.

- ω_K is the number of root of unity in K.
- Δ_K is the discriminant of K.
- $\mathrm{Reg}(K)$ is the regulator of K.

We recall here the definition of the regulator of any r_1+r_2-1 units in a number field. According to Dirichlet unit Theorem (see [42]), we have an isomorphism $O_K^\times \simeq W \times F$, where W is the finite group consisting of roots of unity in K and F is a free abelian group of rank $r_1 + r_2 - 1$. Let $(\mu_1, \ldots, \mu_{r_1+r_2-1})$ be any $r_1 + r_2 - 1$ units in $O_K^\times$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be the real embeddings of K and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ be a set of complex embeddings such that $\sigma_i \neq \overline{\sigma_j}$ for all $i, j = r_1 + 1, \ldots, r_1 + r_2$. Define then

$$l_i(\mu_j) = \begin{cases} \log|\sigma_i(\mu_j)|, & \text{if } \sigma_i \text{ is real;} \\ 2\log|\sigma_i(\mu_j)|, & \text{if } \sigma_i \text{ is complex,} \end{cases}$$

and consider then the $(r_1 + r_2) \times (r_1 + r_2 - 1)$ matrix

$$\begin{pmatrix} l_1(\mu_1) & \cdots & l_1(\mu_{r_1}) & l_1(\mu_{r_1+1}) & \cdots & l_1(\mu_{r_1+r_2-1}) \\ l_2(\mu_1) & \cdots & l_2(\mu_{r_1}) & l_2(\mu_{r_1+1}) & \cdots & l_2(\mu_{r_1+r_2-1}) \\ \vdots & & & & & \vdots \\ l_{r_1+r_2}(\mu_1) & \cdots & l_{r_1+r_2}(\mu_{r_1}) & l_{r_1+r_2}(\mu_{r_1+1}) & \cdots & l_{r_1+r_2}(\mu_{r_1+r_2-1}) \end{pmatrix}.$$

The regulator $\mathrm{Reg}(\mu_1, \ldots, \mu_{r_1+r_2-1})$ of this set of units is the absolute value of the determinant of any minor of rank $r_1 + r_2 - 1$ of the matrix above (they are all equal). In other words, you take the matrix above, you delete any line you want and you take the absolute value of the determinant.

Theorem 2.2.1 *The units* $\{\mu_1, \ldots, \mu_{r_1+r_2-1}\}$ *are* $\mathbb{Z}$*-linearly independant if and only if* $\mathrm{Reg}(\mu_1, \ldots, \mu_{r_1+r_2-1}) \neq 0$.

The regulator of the field K is obtained as follows. Any basis for F is called a set of fundamental units for K. Let $(\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1})$ be a set of fundamental units of K. Then the regulator of the field K is defined as

$$\mathrm{Reg}(K) = \mathrm{Reg}(\varepsilon_1, \ldots, \varepsilon_{r_1+r_2-1}).$$

2.2.4 The Euler product for the Dedekind zeta function

The absolute convergence of the Dedekind zeta function for $\mathrm{Re}(s) > 1$ allows one to write it in this half-plane in the more traditional form

$$\zeta_K(s) = \sum_{\mathfrak{a} \neq 0} \frac{1}{\mathbb{N}(\mathfrak{a})^s},$$

where the sum is taken over nonzero integral ideals of K. This function has also an Euler product for $\mathrm{Re}(s) > 1$

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathbb{N}(\mathfrak{p})^s}\right)^{-1},$$

where the product is over all nonzero prime ideals of K. Note that if $K/\mathbb{Q}$ is Galois then Hilbert's theory of Galois extensions tells us that the factorization of p in K will be of the form $p \cdot O_K = (\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdots \mathfrak{p}_{r_p})^{e_p}$, where $e_p := e(\mathfrak{p}|p)$ is the ramification index which does not depend on the prime $\mathfrak{p}$ lying above p. The same is true for the inertia index $f_p := f(\mathfrak{p}|p)$. Since $\mathbb{N}(\mathfrak{p}) = p^{f_p}$, we have in that case

$$\zeta_K(s) = \prod_{p} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}, \tag{2.4}$$

where now the product is over all positive prime numbers in $\mathbb{Z}$.

2.2.5 Dirichlet L-series

Dirichlet introduced the notion of L-series in number theory in connection with his famous Dirichlet theorem on arithmetic progression. This theorem says that in any arithmetic progression

$$a, a + m, a + 2m, \ldots, a + km, \ldots,$$

where $(a, m) = 1$, there are infinitely many primes.

His idea was to adapt Euler's proof of the infinitude of prime numbers to this case and prove that if $(a, m) = 1$, then

$$\sum_{p \equiv a \pmod{m}} \frac{1}{p} = \infty,$$

where the sum is taken over all positive prime numbers congruent to a modulo m. He introduced L-series precisely in order to gather those primes together. Let χ be a character modulo m, that is a group homomorphism $\chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times$. We extend the definition of χ to all integers by setting $\chi(n) = 0$ if $(n, m) \neq 1$, and $\chi(n) = \chi(n + m\mathbb{Z})$ otherwise. Then we define the L-series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

This is a Dirichlet series. If χ is not the trivial character, using the orthogonality relation and the lemma on Dirichlet series, we see that it represents an analytic function for $\mathrm{Re}(s) > 0$ and converges absolutely for $\mathrm{Re}(s) > 1$. We also have an Euler product

$$L(s, \chi) = \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \tag{2.5}$$

where $\mathrm{Re}(s) > 1$. For the trivial character, $L(s, \chi_1) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \cdot \prod_{p|m} \left(1 - \frac{1}{p^s}\right)$. The first product on the right-hand side is the Riemann zeta function so we get

$$L(s, \chi_1) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right). \tag{2.6}$$

Therefore, when $\chi = \chi_1$ it represents an analytic function for $\mathrm{Re}(s) > 1$. We shall now recall the proof of Dirichlet theorem. Starting from the Euler product (2.5) and taking the logarithm function define by the usual power series $-\log(1-z) = \sum_{n=1}^{\infty} \frac{z^n}{n}$ for $|z| < 1$, we get $\log L(s, \chi) = \log \prod_{p \nmid m} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \sum_{p \nmid m} \log \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$.

Again, using the series expansion of the logarithm, we get

$$\log L(s,\chi) = \sum_{p\nmid m}\sum_{n=1}^{\infty}\frac{\chi(p)^n}{np^{ns}} = \sum_{p\nmid m}\frac{\chi(p)}{p^s} + g(s),$$

where $g(s) = \sum_{p\nmid m}\sum_{n=2}^{\infty}\frac{\chi(p)^n}{np^{ns}}$ (note that this makes sense since $|\chi(p)| = 1$ and therefore $\left|\frac{\chi(p)}{p^s}\right| < 1$). Taking the inverse of $a + m\mathbb{Z}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$, say $b + m\mathbb{Z}$. Multiplying the last equation by $\chi(b)$, we get $\chi(b)\log L(s,\chi) = \chi(b)\sum_{p\nmid m}\frac{\chi(p)}{p^s} + \chi(b)g(s)$. Summing over all characters modulo m leads to $\sum_\chi \chi(b)\log L(s,\chi) = \sum_\chi\sum_p \frac{\chi(pb)}{p^s} + h(s)$, where $h(s) = \sum_\chi \chi(b)g(s)$. Changing the order of summation in the sum on the right hand side, it becomes $\sum_p \frac{1}{p^s}\sum_\chi \chi(pb)$, then using the orthogonality relations, we see that this sum is $\phi(m)\sum_{p\equiv a \pmod m}\frac{1}{p^s}$, where ϕ is the Euler ϕ-function. Finally, we are led to the equation

$$\chi(b)\log L(s,\chi_1) + \sum_{\chi\neq\chi_1}\chi(b)\log L(s,\chi) = \phi(m)\sum_{p\equiv a \pmod m}\frac{1}{p^s} + h(s).$$

One shows that $h(s)$ is bounded around $s = 1$. Moreover, we know that $L(1,\chi)$ is finite if $\chi \neq \chi_1$ and that $\log L(s,\chi_1) \to \infty$ when $s \to 1$ according to the identity (2.6). If we show that for $\chi \neq \chi_1$, $L(1,\chi) \neq 0$ then letting $s \to 1$ in the last equation, we would have

$$\infty = \phi(m)\sum_{p\equiv a \pmod m}\frac{1}{p^s},$$

since all other terms would be bounded at 1. This would prove Dirichlet theorem.

We shall indeed show that $L(1,\chi) \neq 0$ for $\chi \neq \chi_1$ and even more then that, we will relate $L(1,\chi)$ with the class number of some number fields.

2.2.6 The Dirichlet class number formula

From now on suppose that K is a finite abelian field over $\mathbb{Q}$. We shall use class field theory for $\mathbb{Q}$ encompassed by the Kronecker-Weber theorem:

Theorem 2.2.2 (Kronecker-Weber) *Let $K/\mathbb{Q}$ be a finite abelian extension. Then there exists a positive integer m such that $K \subseteq \mathbb{Q}(\zeta_m)$. That is, every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic field.*

Let χ be a character of $\mathrm{Gal}(K/\mathbb{Q})$. Using the Kronecker-Weber theorem, we can view χ as a character modulo m for some integer m. Indeed, let $\mathfrak{f}$ be the smallest positive integer m such that $K \subseteq \mathbb{Q}(\zeta_m)$ (it exists by Kronecker-Weber). It is known that p ramifies in K if and only if $p|\mathfrak{f}$. Consider χ as a character modulo $\mathfrak{f}$ through the following maps

$$(\mathbb{Z}/\mathfrak{f}\mathbb{Z})^\times \overset{\gamma}{\simeq} \mathrm{Gal}(\mathbb{Q}(\zeta_\mathfrak{f})/\mathbb{Q}) \overset{res}{\twoheadrightarrow} \mathrm{Gal}(K/\mathbb{Q}) \overset{\chi}{\to} \mathbb{C}^\times.$$

Explicitly, we have then $\chi(n) = \chi(res \circ \gamma(n+\mathfrak{f}\mathbb{Z}))$ if $(n,\mathfrak{f}) = 1$ and otherwise $\chi(n) = 0$. For brevity, let $G = \mathrm{Gal}(K/\mathbb{Q})$ and denote the group of characters of G by $\widehat{G}$. Consider then for $\mathrm{Re}(s) > 1$ the product $\prod_{\chi\in\widehat{G}} L(s,\chi) = \prod_{\chi\in\widehat{G}} \prod_{p\nmid\mathfrak{f}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$. One shows then that $\prod_{\chi\in\widehat{G}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}$, where f_p is the inertia index $f(\mathfrak{p}|p)$ of any prime $\mathfrak{p}$ of K lying above p, and r_p is the number of prime ideals of K lying above p (in proving this, we use the fact that p is ramified in K if and only if $p|\mathfrak{f}$). Changing the order of the product (which is allowed since it converges absolutely), we get $\prod_{\chi\in\widehat{G}} L(s,\chi) = \prod_{p\nmid\mathfrak{f}} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}$. Combining this with the Euler product (2.4) of ζ_K, we have $\zeta_K(s) = \prod_p \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p} = \prod_{p\nmid\mathfrak{f}} \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p} \cdot \prod_{\chi\in\widehat{G}} L(s,\chi)$ which is valid for $\mathrm{Re}(s) > 1$. Finally, using the identity (2.6) for the trivial character we get for $\mathrm{Re}(s) > 1$

$$\zeta_K(s) = \zeta(s) \prod_{\chi\neq\chi_1} L(s,\chi) \cdot \prod_{p|\mathfrak{f}} \left(1 - \frac{1}{p^s}\right) \left(1 - \frac{1}{p^{f_p s}}\right)^{-r_p}.$$

So we get another expression for $\rho = \lim_{s\to 1} \zeta_K(s)/\zeta(s)$. Indeed,

$$\rho = \prod_{\chi\neq\chi_1} L(1,\chi) \cdot \prod_{p|\mathfrak{f}} \left(1 - \frac{1}{p}\right) \left(1 - \frac{1}{p^{f_p}}\right)^{-r_p}.$$

Now, if $K = \mathbb{Q}(\zeta_\mathfrak{f})$, then since $\rho = h_K \cdot \kappa \neq 0$ we get a proof that for $\chi \neq \chi_1$

$$L(1, \chi) \neq 0,$$

for any character modulo $\mathfrak{f}$ and for any positive integer $\mathfrak{f}$. We have thus completed the proof of Dirichlet theorem on arithmetic progressions.

2.3 A particular case of Stark's conjectures

We have shown that we have $h_K = \rho/\kappa$ where

$$\rho = \prod_{\chi \neq \chi_1} L(1, \chi) \cdot \prod_{p|\mathfrak{f}} \left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{p^{f_p}}\right)^{-r_p}, \qquad \kappa = \frac{2^{r_1+r_2} \cdot \pi^{r_2} \cdot \mathrm{Reg}(K)}{\omega_K \cdot \sqrt{|\Delta_K|}}.$$

In order to compute h_K we first have to know the value of ρ, that is the value of $L(1, \chi)$ for non-trivial characters χ. We can do this directly as in [42] for example. It takes several steps, but they are not that difficult. In the case where K is a quadratic number field, it would lead to an explicit formula for the class number of quadratic number fields. Instead of doing this, we use this formula to give a motivation for Stark's conjectures.

Specializing this last formula to the case of a quadratic number field $K = \mathbb{Q}(\sqrt{d})$, we get the following. First of all, every ramified prime p, i.e. $p|\mathfrak{f}$, will have $f_p = r_p = 1$, and therefore we have

$$\rho = L(1, \chi) = \kappa \cdot h_K,$$

where χ is the unique non-trivial character of $\mathrm{Gal}(K/\mathbb{Q})$ (it is know that χ is the Kronecker symbol). The constant κ is the following:

$$\kappa = \begin{cases} \frac{2 \log \varepsilon}{\sqrt{\mathfrak{f}}}, & \text{if } d > 0; \\ \frac{2\pi}{\omega_K \sqrt{\mathfrak{f}}}, & \text{if } d < 0, \end{cases}$$

where ε is the fundamental unit in $\mathbb{Q}(\sqrt{d})$, when $d > 0$. Furthermore, it is known that in this case $\mathfrak{f} = |\Delta_K|$. Putting all this together, we get the following formula

for $L(1,\chi)$:

$$L(1,\chi) = \begin{cases} \frac{2\log\varepsilon}{\sqrt{|\Delta_K|}} \cdot h_K, & \text{if } d > 0; \\ \frac{2\pi}{\omega_K\sqrt{|\Delta_K|}} \cdot h_K, & \text{if } d < 0. \end{cases} \tag{2.7}$$

Note that this value is the quotient of a presumably transcendental value by a rational number. The general Stark's conjecture is a similar statement for a general Artin L-function.

CHAPTER 3
Class field theory

For a first reading on class field theory, we suggest the article [20]. We used mainly four references for this section, namely [9], [11], [32] and [48].

3.1 Introduction

Class field theory is the continuation of algebraic number theory "à la Dedekind". It started with Leopold Kronecker (1823-1891), Heinrich Weber (1842-1913), David Hilbert (1862-1943) and took a definitive form with Teiji Takagi (1875-1960), Emil Artin (1898-1962) and Helmut Hasse (1898-1979). Later on, Hasse discovered local class field theory and proved it with the help of global class field theory. Jacques Herbrand (1908-1931) and Claude Chevalley (1909-1984) proved local class field theory without using anything from the global theory. Then Chevalley introduced the concept of ideles in order to deduce the global theory from the local theory.

In this chapter, we shall present the classical theory of global class field theory according to Takagi, Weber and Artin.

3.2 Class field theory

We first fix our notation:

- K is a number field, that is a finite extension of $\mathbb{Q}$.
- $K^\times$ is the group of non-zero elements of K.
- O_K is the ring of integers of K.
- $O_K^\times$ is the group of units in O_K.
- $I(K)$ is the group of fractional ideals of K.
- $\iota : K^\times \to I(K)$ is the map defined by $\lambda \mapsto \iota(\lambda) = \lambda \cdot O_K$.
- $P(K)$ is the subgroup of $I(K)$ consisting of the principal ideals, i.e. $P(K) = \iota(K^\times)$.

- $\mathrm{Cl}(K) = I(K)/P(K)$ is the class group of K.

In the beginning of the XIXth century, Evariste Galois (1811-1832) stated his famous theory of the solvability of polynomials. The criterion is that for a polynomial to be solvable it is necessary and sufficient that its Galois group is solvable. In particular, every abelian group is solvable so any polynomial with abelian Galois group (which are called abelian polynomial) can be solved by extraction of roots (these abelian polynomials have been found by Niels Henrik Abel (1802-1829), hence their name). Later on in the XIXth century, Kronecker was interested in solving explicitly abelian polynomials which was possible according to Galois theory. At the same time, he was working on the theory of elliptic functions.

He started with the study of abelian polynomials with coefficients in $\mathbb{Q}$ and he formulated the following conjecture:

Conjecture 3.2.1 (Kronecker) *Every root of an abelian polynomial with rational coefficients is a rational function of roots of unity (with coefficients in $\mathbb{Q}$).*

This has been proven by Weber. Nowadays, it is called the Kronecker-Weber theorem, and we used it in the previous chapter. Then he got interested in abelian polynomials with coefficients in an imaginary quadratic number field. Here again, he formulated a conjecture (see Section 5.3 for the theory of the j-function).

Conjecture 3.2.2 (Kronecker) *Every root of an abelian polynomial with coefficients in a quadratic imaginary field K can be expressed as a rational function (with coefficients in K) of some values of the modular function $j(\tau)$.*

This conjecture became to be known as Kronecker's Jugendtraum. The conjecture is false, even though Kronecker was not far away from the truth. In order to be true, one has to add the values of some other functions like the Weber functions. The correct theorem has been proven by Takagi after he proved the main theorems of class field theory.

A little after Kronecker, Weber was interested in the distribution of prime ideals in ideal classes and wanted to prove that there are infinitely many primes in every class of $\mathrm{Cl}(K)$ for any number field K. He introduced then the concept of ray class group in connection with his work. Going back in the XVIIIth century, Carl Friedrich Gauss (1777-1855) gave the impulse to the theory of binary quadratic form and during his studies, he defined an equivalence relation between forms. Later on, Dedekind translated this language into his new discovery: The ideal theory. For an imaginary quadratic field K, both theories are equivalent, that is the study of classes of binary quadratic forms is equivalent to the study of $\mathrm{Cl}(K)$. But for real quadratic fields, it is not true anymore and one sees that the theory of binary quadratic forms is equivalent to a slightly bigger class group, namely $\mathrm{Cl}_+(K)$, the narrow class group. We defined it right now for any number field, not only for quadratic fields. Let K be a number field, then $\lambda \in K$ is said to be totally positive, and we write $\lambda \gg 0$, if $\sigma(\lambda) > 0$ for all real embedding σ of K. Let

$$P_+(K) = \{\mathfrak{a} \in I(K) | \mathfrak{a} = \lambda \cdot O_K, \text{ for some } \lambda \gg 0\},$$

and define the narrow class group as $\mathrm{Cl}_+(K) := I(K)/P_+(K)$. Weber was aware of that and he noticed then the following isomorphism (the notation will become clear after Definition 3.2.4):

Theorem 3.2.1

$$\mathrm{Cl}_{m\infty}(\mathbb{Q}) := I_m(\mathbb{Q})/P_{m\cdot\infty}(\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times,$$

where

- $I_m(\mathbb{Q})$ *is the group of fractional ideals generated by the integers relatively prime with* m. *In other words,* $I_m(\mathbb{Q})$ *is the group of fractional ideal* $\frac{a}{b} \cdot \mathbb{Z}$ *where* $(a, m) = (b, m) = 1$.

- $P_{m\cdot\infty}(\mathbb{Q})$ *is the subgroup consisting of* $\frac{a}{b}\cdot\mathbb{Z}\in I_m(\mathbb{Q})$ *such that* $\frac{a}{b}\gg 0$ *(that is for* $\mathbb{Q}$, $\frac{a}{b}>0$ *since there is only one real embedding) and* $a\equiv b \pmod m$.

Proof:

We shall use the following notation: $\overline{a} := a + m\mathbb{Z}$ for any integer a. Define the application $f : I_m(\mathbb{Q}) \to (\mathbb{Z}/m\mathbb{Z})^\times$ by the following rule. Every ideal in $I_m(\mathbb{Q})$ has two generators, one positive and one negative. Take the positive one, say $\frac{a}{b}\cdot\mathbb{Z}$ and send it to $\overline{a}\cdot(\overline{b})^{-1}$ in $(\mathbb{Z}/m\mathbb{Z})^\times$. Then $\ker(f) = P_{m\infty}(\mathbb{Q})$ and this map is clearly surjective. Therefore $\mathrm{Cl}_{m\infty}(\mathbb{Q}) \simeq (\mathbb{Z}/m\mathbb{Z})^\times$.

□

Dirichlet's theorem on arithmetic progressions can now be interpreted as follows. In every class of $\mathrm{Cl}_{m\infty}(\mathbb{Q})$, there exists infinitely many prime numbers. Note also that if $m = 1$ then it says that there are infinitely many prime numbers in $\mathbb{N}$ as was known already to Euclid. Weber proceeded then to generalized $\mathrm{Cl}_{m\infty}(\mathbb{Q})$ to other number fields. We explain this now.

Definition 3.2.1 *Let* K *be a number field and* $\mathfrak{m}_0$ *be an integral ideal of* K. *Let* $\mathfrak{m}_\infty$ *be a set of distinct real embeddings of* K. *We define a modulus* $\mathfrak{m}$ *to be a formal product* $\mathfrak{m} = \mathfrak{m}_0\cdot\mathfrak{m}_\infty$.

A modulus is just a way to pack together finitely many prime ideals and finitely many real embeddings (a real or complex embedding is also called an infinite prime). We proceed now to generalize $O_K^\times, K^\times, I(K), P(K)$, and $\mathrm{Cl}(K)$. For all these definitions, fix a modulus $\mathfrak{m} = \mathfrak{m}_0\cdot\mathfrak{m}_\infty$.

Definition 3.2.2 *We define a subgroup* $K^\times(\mathfrak{m}_0)$ *of* $K^\times$ *to be the subgroup generated by the elements* $\alpha\in O_K$ *such that* $(\alpha\cdot O_K, \mathfrak{m}_0) = 1$. *We define also* $O_K^\times(\mathfrak{m}_0) = O_K^\times\cap K^\times(\mathfrak{m}_0)$.

In other words, $\lambda\in K^\times(\mathfrak{m}_0)$ if and only if there exists $\alpha,\beta\in O_K(\neq 0)$ such that $\lambda = \alpha/\beta$ and $(\alpha\cdot O_K, \mathfrak{m}_0) = (\beta\cdot O_K, \mathfrak{m}_0) = 1$. Then we define an equivalence relation on $K^\times(\mathfrak{m}_0)$.

Definition 3.2.3 *Let* $\lambda_1, \lambda_2 \in K^\times(\mathfrak{m}_0)$. *Then, by definition* $\lambda_i = \frac{\alpha_i}{\beta_i}$ *where* α_i, β_i *are non-zero algebraic integers in* K *satisfying* $(\alpha_i \cdot O_K, \mathfrak{m}_0) = 1 = (\beta_i \cdot O_K, \mathfrak{m}_0)$ *for* $i = 1, 2$. *Define then*

$$\lambda_1 \equiv \lambda_2 \mod {}^\times\mathfrak{m} \Leftrightarrow \begin{cases} \alpha_1\beta_2 \equiv \alpha_2\beta_1 \mod \mathfrak{m}_0; \\ \textit{and} \\ \sigma\left(\frac{\alpha_1\beta_2}{\beta_1\alpha_2}\right) > 0 \textit{ for all real embeddings } \sigma \in \mathfrak{m}_\infty. \end{cases}$$

Note, that the last condition means that $\sigma(\lambda_1)$ *and* $\sigma(\lambda_2)$ *have the same sign for each* $\sigma \in \mathfrak{m}_\infty$. *Also, this equivalence relation is well-defined, that is, it does not depend on the representation of* λ_i *as a quotient* $\frac{\alpha_i}{\beta_i}$.

Next, we define a subgroup of $K^\times(\mathfrak{m}_0)$ which now depends also on the infinite part of the modulus and use it to generalize the construction of $\mathrm{Cl}(K)$ and $\mathrm{Cl}_+(K)$.

Definition 3.2.4 *Define*

$$K^\times_{\mathfrak{m}} = \{\lambda \in K^\times(\mathfrak{m}_0) | \lambda \equiv 1 \mod {}^\times\mathfrak{m}\}, \qquad O^\times_{K,\mathfrak{m}} = \{\alpha \in O^\times_K(\mathfrak{m}_0) | \alpha \equiv 1 \mod {}^\times\mathfrak{m}\}.$$

Define also $I_{\mathfrak{m}}(K)$ *to be the subgroup of* $I(K)$ *generated by all primes relatively prime with* $\mathfrak{m}_0$, *and*

$$P_{\mathfrak{m}}(K) = \iota(K^\times_{\mathfrak{m}}) = \{\mathfrak{a} \in I_{\mathfrak{m}}(K) | \mathfrak{a} = \lambda \cdot O_K \textit{ for some } \lambda \in K^\times_{\mathfrak{m}}\}.$$

Note that $P_{\mathfrak{m}}(K)$ *is a subgroup of* $I_{\mathfrak{m}}(K)$ *and that* $I_{\mathfrak{m}}(K)$ *depends only on the finite part* $\mathfrak{m}_0$ *of* $\mathfrak{m}$ *(therefore sometimes, we write* $I_{\mathfrak{m}_0}(K)$ *instead of* $I_{\mathfrak{m}}(K)$ *). Finally, we define the ray class group of modulus* $\mathfrak{m}$ *by* $\mathrm{Cl}_{\mathfrak{m}}(K) := I_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K)$.

These ray class groups are finite groups like the usual class group. Indeed, if $P(\mathfrak{m}_0, K)$ denotes the group of principal ideals $I_{\mathfrak{m}_0}(K) \bigcap P(K)$, then we have an isomorphism

$$I_{\mathfrak{m}_0}(K)/P(\mathfrak{m}_0, K) \simeq \mathrm{Cl}(K).$$

The map $I_{\mathfrak{m}}(K) \to I_{\mathfrak{m}_0}(K)/P(\mathfrak{m}_0, K)$ induces a map

$$\psi : I_{\mathfrak{m}}(K)/P_{\mathfrak{m}}(K) \to I_{\mathfrak{m}_0}(K)/P(\mathfrak{m}_0, K),$$

and $\ker \psi = P(\mathfrak{m}_0, K)/P_{\mathfrak{m}}(K)$. Therefore, we get the isomorphism $\mathrm{Cl}(K) \simeq \mathrm{Cl}_{\mathfrak{m}}(K)/J$, where $J = P(\mathfrak{m}_0, K)/P_{\mathfrak{m}}(K)$. We shall study a bit further the group J. Consider the homomorphism

$$K^{\times}(\mathfrak{m}_0) \to P(\mathfrak{m}_0, K)/P_{\mathfrak{m}}(K), \qquad \lambda \mapsto (\lambda \cdot O_K) \cdot P_{\mathfrak{m}}(K).$$

This map is surjective, and its kernel is easily seen to be $O_K^{\times} \cdot K_{\mathfrak{m}}^{\times}$. Thus

$$P(\mathfrak{m}_0, K)/P_{\mathfrak{m}}(K) \simeq K^{\times}(\mathfrak{m}_0)/(O_K^{\times} \cdot K_{\mathfrak{m}}^{\times}).$$

If we show that $K^{\times}(\mathfrak{m}_0)/(O_K^{\times} \cdot K_{\mathfrak{m}}^{\times})$ is a finite group, then $\mathrm{Cl}_{\mathfrak{m}}(K)$ would also be a finite group. Consider the map

$$K^{\times}(\mathfrak{m}_0) \to \prod_{\mathfrak{p}|\mathfrak{m}_0} \left(O_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}}^{v_{\mathfrak{p}}(\mathfrak{m}_0)}\right)^{\times} \times \prod_{\sigma \in \mathfrak{m}_{\infty}} K_{\sigma}^{\times}/K_{\sigma,+}^{\times},$$

where $O_{\mathfrak{p}}$ is the localization of O_K at $\mathfrak{p}$, $\mathfrak{m}_{\mathfrak{p}}$ is the unique maximal ideal of $O_{\mathfrak{p}}$, $K_{\sigma}^{\times}$ is the completion of K with respect to the place σ, and $K_{\sigma,+}^{\times}$ is the subgroup of $K_{\sigma}^{\times}$ consisting of positive elements. Using the approximation theorem, we see that this map is surjective. Moreover, its kernel is precisely $K_{\mathfrak{m}}^{\times}$. We see from all this that $\mathrm{Cl}_{\mathfrak{m}}(K)$ is a finite group. More precisely, we have:

Theorem 3.2.2 *The ray class groups* $\mathrm{Cl}_{\mathfrak{m}}(K)$ *are finite groups. Let* $h_{\mathfrak{m},K}$ *denotes its cardinality. Then we have*

$$h_{\mathfrak{m},K} = h_K \cdot \frac{\phi(\mathfrak{m}_0) \cdot 2^t}{[O_K^{\times} : O_{K,\mathfrak{m}}^{\times}]},$$

where ϕ *is the generalized Euler* ϕ*-function and* t *is the number of real places in* $\mathfrak{m}_{\infty}$.

If $K = \mathbb{Q}$ and $\mathfrak{m} = (m) \cdot \infty$ then $\mathrm{Cl}_{\mathfrak{m}}(\mathbb{Q}) = \mathrm{Cl}_{m\infty}(\mathbb{Q})$, the class group of the Theorem 3.2.1. Note, moreover, that when $\mathfrak{m} = O_K \cdot \infty$ where $\infty = \{\sigma_1, \ldots, \sigma_r\}$ is

the set of all real embeddings of K, then $\mathrm{Cl}_{\mathfrak{m}}(K) = \mathrm{Cl}_{+}(K)$. Also, when $\mathfrak{m} = O_K$ then, $\mathrm{Cl}_{\mathfrak{m}}(K) = \mathrm{Cl}(K)$ so ray class groups generalize both the usual class group and the narrow class group.

We make a small digression here. Remark that for the usual class group, we have the following exact sequence

$$1 \to O_K^{\times} \to K^{\times} \xrightarrow{\iota} I(K) \to \mathrm{Cl}(K) \to 1.$$

We see from this sequence that $O_K^{\times}$ is a measure of the non-injectivity of ι and $\mathrm{Cl}(K)$ is a measure of the non-surjectivity of the same map ι. We have a similar exact sequence for the ray class groups

$$1 \to O_{K,\mathfrak{m}}^{\times} \to K_{\mathfrak{m}}^{\times} \xrightarrow{\iota} I_{\mathfrak{m}}(K) \to \mathrm{Cl}_{\mathfrak{m}}(K) \to 1.$$

Recall that Weber was interested in proving that there are infinitely many prime ideals in every class of $\mathrm{Cl}(K)$, and more generally in every class of $\mathrm{Cl}_{\mathfrak{m}}(K)$, in order to generalize Dirichlet's theorem to any number field. Recall also that in proving Dirichlet's theorem, we used the fact that every abelian extension is contained in a cyclotomic field (the Kronecker-Weber theorem). In order to prove his theorem, Weber supposed the existence of some fields (the ray class fields) having similar properties as the ones cyclotomic fields have for $\mathbb{Q}$. He called them class fields. Unfortunately for him, he was not able to prove the existence of these fields even though he was convinced of this fact. Actually, he was sure of their existence for $\mathbb{Q}$ and pretty sure for a quadratic imaginary field because of the second conjecture of Kronecker. On the other hand, assuming their existence, he proved some of their properties and he was pretty sure that the class fields are finite abelian extension of K.

Hilbert, working on other problems, was led to stipulate the existence of some fields with similar properties to those of Weber. Hilbert has been the first to see

in that theory a theory of abelian extensions of number fields. Then Takagi proved all the main theorems of class field theory. Finally, Artin introduced his famous reciprocity law which nowadays is in the center of class field theory. We recall here the notion of the Artin map $\varphi_{L/K}$ (also denoted $(\_, L/K)$).

Let L/K be a finite extension of number fields. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ a prime of L lying above $\mathfrak{p}$. Let also $l_{\mathfrak{P}} = O_L/\mathfrak{P}$ and $k_{\mathfrak{p}} = O_K/\mathfrak{p}$. From algebraic number theory, we have the following exact sequence

$$1 \to I(\mathfrak{P}|\mathfrak{p}) \to D(\mathfrak{P}|\mathfrak{p}) \to \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}}) \to 1, \tag{3.1}$$

where $I(\mathfrak{P}|\mathfrak{p})$ is the inertia group and $D(\mathfrak{P}|\mathfrak{p})$ the decomposition group. Suppose now that $\mathfrak{P}$ is unramified above $\mathfrak{p}$, then $I(\mathfrak{P}|\mathfrak{p}) = 1$ and $D(\mathfrak{P}|\mathfrak{p}) \simeq \mathrm{Gal}(l_{\mathfrak{P}}/k_{\mathfrak{p}})$. By Galois theory for finite fields, the Galois group on the right is cyclic generated by the Frobenius $x \mapsto x^q$, where q is the cardinality of $k_{\mathfrak{p}}$. Under the exact sequence (3.1), the Frobenius corresponds to a unique K-automorphism of L in $D(\mathfrak{P}|\mathfrak{p})$. We call this K-automorphism by the same name, namely the Frobenius. Now, if L/K is an abelian extension, then the Frobenius does not depend on the prime $\mathfrak{P}$ lying above. Suppose from now on that L/K is abelian, and denote this Frobenius by $\sigma_{\mathfrak{p}}$. One can show that $\sigma_{\mathfrak{p}}$ is uniquely determined by the following condition. It is the unique automorphism $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(x) \equiv x^q \pmod{\mathfrak{P}}$ for all $x \in O_L$, where q is the cardinality of $O_K/\mathfrak{p}$. The Artin map is then defined as follows.

Definition 3.2.5 *Let $\mathfrak{m}_0$ be an integral ideal of K such that all ramified primes divide $\mathfrak{m}_0$. The Artin map is defined as*

$$\varphi_{\mathfrak{m}_0,L/K} : I_{\mathfrak{m}_0}(K) \to \mathrm{Gal}(L/K), \qquad \mathfrak{a} = \prod_{i=1}^{t} \mathfrak{p}_i^{\alpha_i} \mapsto \prod_{i=1}^{t} \sigma_{\mathfrak{p}_i}^{\alpha_i}.$$

Note that even though the Artin map depends only on the finite part of a modulus $\mathfrak{m}$, we shall also use the notation $\varphi_{\mathfrak{m},L/K}$ for the Artin map. We are now almost ready to state the main theorem of class field theory which classifies finite abelian extensions

of a number field, but in order to get all finite abelian extensions of K we have to consider also quotients of ray class groups.

Definition 3.2.6 *An ideal subgroup modulo* $\mathfrak{m}$ *is a group* $H_{\mathfrak{m}}$ *satisfying the two inclusions* $P_{\mathfrak{m}}(K) < H_{\mathfrak{m}} < I_{\mathfrak{m}}(K)$. *For each ideal subgroup modulo* $\mathfrak{m}$, *we define also a class group, namely*

$$\mathrm{Cl}_{\mathfrak{m},H_{\mathfrak{m}}}(K) = I_{\mathfrak{m}}(K)/H_{\mathfrak{m}} \simeq \mathrm{Cl}_{\mathfrak{m}}(K)/\left(H_{\mathfrak{m}}/P_{\mathfrak{m}}(K)\right).$$

Recall also that a real embedding σ of K is called ramified in a finite extension L/K if there exists a complex embedding τ of L such that $\tau|_K = \sigma$. We can now state the first main theorem of class field theory.

Theorem 3.2.3 *Let* L/K *be an abelian extension and let* $\mathfrak{m}$ *be a modulus divisible by all primes of* K, *finite or infinite, that ramify in* L.

- *The Artin map* $\varphi_{\mathfrak{m},L/K}$ *is surjective.*
- *If the exponents of the finite primes in* $\mathfrak{m}$ *are sufficiently large, then* $\ker(\varphi_{\mathfrak{m},L/K})$ *is a congruence subgroup modulo* $\mathfrak{m}$, *that is* $P_{\mathfrak{m}}(K) < \ker(\varphi_{\mathfrak{m},L/K}) < I_{\mathfrak{m}}(K)$, *and consequently, the Artin map gives us the isomorphism*

$$I_{\mathfrak{m}}(K)/\ker(\varphi_{\mathfrak{m},L/K}) \simeq \mathrm{Gal}(L/K).$$

Remark: The condition "for sufficiently large" seems weird at first. It should be clear after the definition of the conductor (below) what we mean: The conductor should divide $\mathfrak{m}$. See Theorem 3.2.7.

This last theorem can be satisfied by more than one modulus. In order to have a bijective correspondence between abelian extensions and some classifying objects, we shall introduce an equivalence relation between congruence subgroups. The ideal classes obtained in this way will be the classifying objects for finite abelian extensions.

Definition 3.2.7 *Let* $\mathfrak{m}_1$ *and* $\mathfrak{m}_2$ *be two moduli,* $H_{\mathfrak{m}_1}$ *an ideal subgroup modulo* $\mathfrak{m}_1$ *and* $H_{\mathfrak{m}_2}$ *an ideal subgroup modulo* $\mathfrak{m}_2$*. Then*

$$H_{\mathfrak{m}_1} \sim H_{\mathfrak{m}_2} \Leftrightarrow \text{ There exists a modulus } \mathfrak{m} \text{ s.t. } H_{\mathfrak{m}_1} \cap I_{\mathfrak{m}}(K) = H_{\mathfrak{m}_2} \cap I_{\mathfrak{m}}(K).$$

An equivalence class $[H_{\mathfrak{m}}]$ *of ideal subgroups is called an ideal group.*

Theorem 3.2.4 *Let* $\mathfrak{m}_1$ *and* $\mathfrak{m}_2$ *be two modulus,* $H_{\mathfrak{m}_1}$ *be an ideal subgroup modulo* $\mathfrak{m}_1$ *and* $H_{\mathfrak{m}_2}$ *an ideal subgroup modulo* $\mathfrak{m}_2$*. If* $H_{\mathfrak{m}_1} \sim H_{\mathfrak{m}_2}$*, then both class groups are isomorphic:* $\mathrm{Cl}_{\mathfrak{m}_1,H_{\mathfrak{m}_1}}(K) \simeq \mathrm{Cl}_{\mathfrak{m}_2,H_{\mathfrak{m}_2}}(K)$*. Thus, if* $H = [H_{\mathfrak{m}}]$ *is an ideal group, we can talk about the class group of* H*. More precisely,* $\mathrm{Cl}_H(K) = \mathrm{Cl}_{\mathfrak{m},H_{\mathfrak{m}}}(K)$.

We define next the conductor of an ideal group, but before that here are some preliminaries. The next definition extend divisibility of integral ideals to modulus.

Definition 3.2.8 *Write* $\mathfrak{m}_1 = \mathfrak{m}_{0,1} \cdot \mathfrak{m}_{\infty,1}$ *and* $\mathfrak{m}_2 = \mathfrak{m}_{0,2} \cdot \mathfrak{m}_{\infty,2}$*. We say that* $\mathfrak{m}_1 | \mathfrak{m}_2$ *if* $\mathfrak{m}_{0,1} | \mathfrak{m}_{0,2}$*, and* $\mathfrak{m}_{\infty,1} \subseteq \mathfrak{m}_{\infty,2}$*. Therefore, it makes sense to talk about the gcd of two moduli,* $gcd(\mathfrak{m}_1, \mathfrak{m}_2) = gcd(\mathfrak{m}_{0,1}, \mathfrak{m}_{0,2}) \cdot (\mathfrak{m}_{\infty,1} \cap \mathfrak{m}_{\infty,2})$.

Theorem 3.2.5 *If* H *is an ideal group (i.e. an equivalence class of ideal subgroups), and* $H_{\mathfrak{m}_1}$, $H_{\mathfrak{m}_2} \in H$*, where* $H_{\mathfrak{m}_i}$ *is an ideal subgroup modulo* $\mathfrak{m}_i$*. Let* $\mathfrak{m} = gcd(\mathfrak{m}_1, \mathfrak{m}_2)$*. Then there exists an ideal subgroup* $H_{\mathfrak{m}}$ *modulo* $\mathfrak{m}$ *such that* $H_{\mathfrak{m}} \in H$.

Definition 3.2.9 *Let* H *be an ideal group. The gcd of all* $\mathfrak{m}$ *for which there exists an ideal subgroup* $H_{\mathfrak{m}} \in H$ *is called the conductor of* H *and is denoted by* $\mathfrak{f} = \mathfrak{f}(H)$*.* $\mathfrak{f}$ *is thus characterized by the two conditions:*

- $H_{\mathfrak{f}} \in H$.
- $H_{\mathfrak{m}} \in H \Rightarrow \mathfrak{f} | \mathfrak{m}$.

Note also that if H is an ideal group and $\mathfrak{m}$ is a modulus, then there is at most one ideal subgroup modulo $\mathfrak{m}$ in H. We denote it by $H_{\mathfrak{m}}$.

We can now precise Theorem 3.2.3.

Theorem 3.2.6 *To any finite abelian extension L/K, there exists a unique ideal group H such that $\mathrm{Cl}_H(K) \simeq \mathrm{Gal}(L/K)$, and the isomorphism is given by the Artin map for any modulus $\mathfrak{m}$ such that there exists a $H_\mathfrak{m}$ in H.*

Definition 3.2.10 *Let L be a finite abelian extension of K. Then the conductor of L/K is the conductor of the ideal group corresponding to it under the last theorem. It is denoted by $\mathfrak{f}(L/K)$.*

Theorem 3.2.7 *Let L/K be a finite abelian extension of K.*

- *A prime $\mathfrak{p}$ of K (finite or infinite) is ramified in L if and only if $\mathfrak{p}|\mathfrak{f}(L/K)$.*
- *Let $\mathfrak{m}$ be a modulus divisible by all primes (finite or infinite) which are ramified in L. Then $\ker(\varphi_{\mathfrak{m},L/K})$ is a congruence subgroup modulo $\mathfrak{m}$ that is $P_\mathfrak{m}(K) < \ker(\varphi_{\mathfrak{m},L/K}) < I_\mathfrak{m}(K)$ if and only if $\mathfrak{f}(L/K)|\mathfrak{m}$.*

We also have the converse of Theorem 3.2.3, namely

Theorem 3.2.8 *Let $\mathfrak{m}$ be a modulus of K and let $H_\mathfrak{m}$ be a congruence subgroup modulo $\mathfrak{m}$, that is $P_\mathfrak{m}(K) < H_\mathfrak{m} < I_\mathfrak{m}(K)$. There exists then a unique abelian extension L/K such that its ramified primes (finite or infinite) divide $\mathfrak{m}$ and such that the Artin map $\varphi_{\mathfrak{m},L/K} : I_\mathfrak{m}(K) \to \mathrm{Gal}(L/K)$ gives us the isomorphism*

$$\mathrm{Cl}_{\mathfrak{m},H_\mathfrak{m}}(K) = I_\mathfrak{m}(K)/H_\mathfrak{m} \simeq \mathrm{Gal}(L/K),$$

i.e. $H_\mathfrak{m} = \ker(\varphi_{\mathfrak{m},L/K})$.

We thus have a one-to-one and onto correspondence between the ideal groups and the finite abelian extension of K. This correspondence is actually order reversing. To understand this last fact, we have to explain the order relation on the set of ideal groups.

Definition 3.2.11 *Let H_1 and H_2 be two ideal groups for K. We say that $H_1 \subseteq H_2$ if there exists a modulus $\mathfrak{m}$, an $H_{1,\mathfrak{m}} \in H_1$ and an $H_{2,\mathfrak{m}} \in H_2$ such that $H_{1,\mathfrak{m}} \subseteq H_{2,\mathfrak{m}}$.*

After this definition, we can state:

Theorem 3.2.9 *Let L and M be two finite abelian extensions of K. Let H_L and H_M be their corresponding ideal group. Then $L \subseteq M$ if and only if $H_L \supseteq H_M$.*

3.2.1 Ray class fields and the Hilbert class field

Definition 3.2.12 *Let K be a number field and $\mathfrak{m}$ any modulus. The finite abelian extension of K corresponding to the ideal subgroup $P_{\mathfrak{m}}(K)$ is called the ray class field of modulus $\mathfrak{m}$ and is denoted $K_{\mathfrak{m}}$.*

By the theorems above, we have $\mathrm{Gal}(K_{\mathfrak{m}}/K) \simeq \mathrm{Cl}_{\mathfrak{m}}(K)$ and every abelian extension is contained in a ray class field for some modulus $\mathfrak{m}$. We have another characterization of the conductor, namely:

Theorem 3.2.10 *Let L/K be an abelian extension. The conductor $\mathfrak{f}(L/K)$ is the g.c.d. of all modulus $\mathfrak{m}$ such that $L \subseteq K_{\mathfrak{m}}$.*

It is thus the smallest $K_{\mathfrak{m}}$ such that $K \subseteq K_{\mathfrak{m}}$. The ray class fields are the generalization of the cyclotomic fields for the base field $\mathbb{Q}$. Indeed:

Theorem 3.2.11 *Let $K = \mathbb{Q}$ and let $m \in \mathbb{Z}$. The ray class fields corresponding to the modulus $\mathfrak{m} = m\mathbb{Z} \cdot \infty$ is $\mathbb{Q}(\zeta_m)$ and the ones corresponding to the modulus $\mathfrak{m} = m\mathbb{Z}$ is $\mathbb{Q}(\zeta_m + \zeta_m^{-1})$, that is, the maximal real subfield of $\mathbb{Q}(\zeta_m)$.*

On the other hand, for a general base field K, we do not know explicit generators for the ray class fields $K_{\mathfrak{m}}$ (as the roots of unity for $\mathbb{Q}$). When K is quadratic imaginary, such generators can be given by the main theorems of complex multiplication.

Among the ray class fields, two are particularly important: The Hilbert class fields. There are two notions of a Hilbert class field of a number field K. One is the small Hilbert class field, denoted by H_K, and the other is the big Hilbert class field, denoted by H_K^+. They are defined as follows:

- The small Hilbert class field (or Hilbert class field) is the ray class field associated to the modulus $\mathfrak{m} = O_K$.

- The big Hilbert class field (or the narrow Hilbert class field) is the ray class field associated to the modulus $\mathfrak{m} = O_K \cdot \infty$ where $\infty = \{\sigma_1, \ldots, \sigma_r\}$ is the set of all real embeddings of K.

A direct consequence of the theorems above is that $\mathrm{Gal}(H_K/K) \simeq \mathrm{Cl}(K)$ and also that $\mathrm{Gal}(H_K^+/K) \simeq \mathrm{Cl}_+(K)$. We also have $H_K \subseteq H_K^+$ by Theorem 3.2.9. The Hilbert class fields have the following property

Theorem 3.2.12 *The small Hilbert class field is the maximal finite everywhere unramified abelian extension of K. In other words, if L/K is a finite abelian extension such that all finite and infinite primes are unramified then $L \subseteq H_K$.*

Proof:

Let L be a finite unramified abelian extension of K at every prime (including the infinite ones) and $\mathfrak{f} = \mathfrak{f}(L/K)$ its conductor. By Theorem 3.2.7, $\mathfrak{f} = O_K$ since all primes are unramified. By the second part of the same theorem, $\ker(\varphi_{O_K,L/K})$ is a congruence subgroup that is $P_{O_K}(K) \subseteq \ker(\varphi_{O_K,L/K})$. Then by Theorem 3.2.9, we necessarily have $L \subseteq H_K$.

□

Theorem 3.2.13 *The big Hilbert class field is the maximal finite unramified abelian extension of K (excluding the infinite primes). In other words, if L/K is a finite abelian extension such that all finite primes are unramified then $L \subseteq H_K^+$.*

Proof:

Let L be a finite unramified abelian extension of K at the finite primes and $\mathfrak{f}$ its conductor. Set also $\mathfrak{m} = O_K \cdot \infty$. Since all finite primes are unramified in L, $\mathfrak{m}$ is divisible by all ramified primes and $\mathfrak{f}|\mathfrak{m}$. By the second part of the Theorem 3.2.7, the group $\ker(\varphi_{\mathfrak{m},L/K})$ is a congruence subgroup modulo $\mathfrak{m}$, that is $P_{\mathfrak{m}}(K) \subseteq \ker(\varphi_{\mathfrak{m},L/K})$. Then by Theorem 3.2.9, we necessarily have $L \subseteq H_K^+$.

□

Remark: When K is totally complex, then $H_K = H_K^+$.

3.3 Generalized L-series

In order to prove his theorem on the infinitude of primes in any ideal class, Weber generalized the notion of Dirichlet series to any number field.

Definition 3.3.1 *Let $\mathfrak{m}$ be a modulus and $\mathrm{Cl}_{\mathfrak{m}}(K)$ the ray class group modulo $\mathfrak{m}$. Let $\chi : \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathbb{C}^{\times}$ be a character. We extend the definition of χ to any integral ideal of K by setting $\chi(\mathfrak{a}) = \chi([\mathfrak{a}])$ if $(\mathfrak{a}, \mathfrak{m}_0) = 1$, and $\chi(\mathfrak{a}) = 0$ if $(\mathfrak{a}, \mathfrak{m}_0) \neq 1$. The generalized Dirichlet L-series modulo $\mathfrak{m}$ is defined to be*

$$L(s, \chi) = \sum_{\mathfrak{a} \neq 0} \frac{\chi(\mathfrak{a})}{\mathbb{N}(\mathfrak{a})^s},$$

where the sum is taken over all non-zero integral ideal of K.

If $\chi \neq \chi_1$, then $L(s, \chi)$ represents an analytic function for $\mathrm{Re}(s) > 1 - \frac{1}{[K:\mathbb{Q}]}$. For χ_1, it represents an analytic function for $\mathrm{Re}(s) > 1$. They also have an Euler product

$$L(s, \chi) = \prod_{\mathfrak{p}} \left(1 - \frac{\chi(\mathfrak{p})}{\mathbb{N}(\mathfrak{p})^s}\right)^{-1},$$

valid for $\mathrm{Re}(s) > 1$.

3.4 Artin L-functions

First of all, the main reference for this section is [48]. The class of Artin L-functions contains all L-series we have seen so far. Moreover, they are defined for any finite galois extension of number fields not necessarily abelian. When the extension is abelian, they reduced to the ones above. We introduce Artin L-functions here in order to explain Stark's conjectures in Chapter 4.

Let K/k be a finite galois extension of number fields. Let $\rho : \mathrm{Gal}(K/k) \to \mathrm{GL(V)}$ be a finite dimensional complex representation of $G = \mathrm{Gal}(K/k)$ with character χ. Let $\mathfrak{p}$ be a prime ideal of k and $\mathfrak{P}$ be any prime ideal of K above $\mathfrak{p}$. Recall from Equation (3.1) that we have the isomorphism

$$D(\mathfrak{P}|\mathfrak{p})/I(\mathfrak{P}|\mathfrak{p}) \simeq \mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}}).$$

We will denote the coset corresponding to the Frobenius element of $\mathrm{Gal}(K_{\mathfrak{P}}/K_{\mathfrak{p}})$ by $\sigma_{\mathfrak{P}}$. This coset induces a well-defined automorphism on

$$V^{I(\mathfrak{P}|\mathfrak{p})} = \{v \in V | \sigma \cdot v = v, \text{ for all } \sigma \in I(\mathfrak{P}|\mathfrak{p})\}.$$

We can now define the Artin L-function:

$$L(s, \rho, K/k) := \prod_{\mathfrak{p}} \frac{1}{\det(1 - \sigma_{\mathfrak{P}}\mathbb{N}(\mathfrak{p})^{-s}|V^{I(\mathfrak{P}|\mathfrak{p})})}.$$

Remark: The notation $\det(1 - \sigma_{\mathfrak{P}}\mathbb{N}(\mathfrak{p})^{-s}|V^{I(\mathfrak{P}|\mathfrak{p})})$ means the determinant of the operator $1 - \sigma_{\mathfrak{P}}\mathbb{N}(\mathfrak{p})^{-s}$ acting on $V^{I(\mathfrak{P}|\mathfrak{p})}$.

Using a standard argument on infinite product, one can show that the Artin L-function represents an analytic function for $\mathrm{Re}(s) > 1$. The argument goes as follows. It suffices to prove that the product is absolutely and uniformly convergent on any half-plane $\mathrm{Re}(s) \geq 1 + \delta$ for any $\delta > 0$. This is equivalent to the convergence (absolutely and uniformly) of the following series:

$$\sum_{\mathfrak{p}} \log\left(\frac{1}{\det(1 - \sigma_{\mathfrak{P}}\mathbb{N}(\mathfrak{p})^{-s}|V^{I(\mathfrak{P}|\mathfrak{p})})}\right),$$

where the log is given by the principal branch. Note that we can decompose the determinant as follows:

$$\det(1 - \sigma_{\mathfrak{P}}\mathbb{N}(\mathfrak{p})^{-s}|V^{I(\mathfrak{P}|\mathfrak{p})}) = \prod_{i=1}^{d_{\mathfrak{P}}}(1 - \varepsilon_i\mathbb{N}(\mathfrak{p})^{-s}),$$

where the ε_i are roots of unity, and $d_{\mathfrak{P}} = \dim(V^{I(\mathfrak{P}|\mathfrak{p})})$. This is true because the operator $1 - \sigma_{\mathfrak{P}}\mathbb{N}(\mathfrak{p})^{-s}$ preserves the hermitian pairing $H(x, y) := \sum_{\sigma \in G} < \sigma x, \sigma y >$, where $< , >$ is the usual hermitian product on V (after having chosen a basis). Therefore, this operator is diagonalizable and moreover the eigenvalues are roots of unity since $\mathrm{Gal}(K/k)$ is a finite group. Thus we are led to consider the series

$$\sum_{\mathfrak{p}} \sum_{i=1}^{d_{\mathfrak{P}}} \log(1 - \varepsilon_i\mathbb{N}(\mathfrak{p})^{-s})^{-1}.$$

Using the usual series for the logarithm, this last series is equal to

$$\sum_{\mathfrak{p}} \sum_{i=1}^{d_{\mathfrak{p}}} \sum_{n=1}^{\infty} \frac{\varepsilon_i^n}{n\mathbb{N}(\mathfrak{p})^{ns}}.$$

But, we have the following chain of inequalities:

$$\begin{aligned}
\sum_{\mathfrak{p}} \sum_{i=1}^{d_{\mathfrak{p}}} \sum_{n=1}^{\infty} \left| \frac{\varepsilon_i^n}{n\mathbb{N}(\mathfrak{p})^{ns}} \right| &\leq \dim(V) \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{n\mathbb{N}(\mathfrak{p})^{n\mathrm{Re}(s)}} \\
&\leq \dim(V) \cdot [K:k] \cdot \sum_{p} \sum_{n=1}^{\infty} \frac{1}{np^{n(1+\delta)}} \\
&\leq \dim(V) \cdot [K:k] \cdot \log \zeta(1+\delta).
\end{aligned}$$

We can conclude with this last inequality.

It is also known (using Brauer's theorem on induced representations) that the Artin L-functions can be extended to a meromorphic function on the complex plane.

If ρ' is an equivalent representation, it is known that the corresponding Artin L-functions agree. Therefore, we can write $L(s, \chi, K/k)$ instead of $L(s, \rho, K/k)$ since two representations are equivalent if and only if they have the same character.

The Artin L-functions have three fundamental properties that we record in the next theorem.

Theorem 3.4.1 *The Artin L-functions behave as follows under direct sum, induction and inflation:*

- $L(s, \chi + \chi', K/k) = L(s, \chi, K/k) \cdot L(s, \chi', K/k)$.
- *Suppose we have* $k \subseteq L \subseteq K$ *and that* χ *is a character of* $H = \mathrm{Gal}(K/L)$, *then* $L(s, \mathrm{Ind}_H^G(\chi), K/k) = L(s, \chi, K/L)$.
- *Suppose we have* $k \subseteq L \subseteq K$, $H = \mathrm{Gal}(K/L)$ *is a normal subgroup of* G, *and* χ *is a character of* $G/H \simeq \mathrm{Gal}(L/k)$, *then* $L(s, \mathrm{Infl}(\chi), K/k) = L(s, \chi, L/k)$.

How do we get back the Dedekind zeta functions from these new ones? Taking the trivial representation $\rho = 1$, we get

$$L(s, 1, K/k) = \zeta_k(s).$$

When K/k is an abelian extension, then we get back the generalized Dirichlet L-series up to a finite Euler product. This is the content of the next theorem.

Theorem 3.4.2 *Let K/k be an abelian extension, let $\mathfrak{f}$ be the conductor of K/k and let $\chi \neq \chi_1$ be an irreducible character of $\mathrm{Gal}(K/k)$. Consider the sequence of maps:*

$$\mathrm{Cl}_{\mathfrak{f}}(K) \to \mathrm{Cl}_{\mathfrak{f}}(K)/H_{\mathfrak{f}} \simeq \mathrm{Gal}(K/k) \xrightarrow{\chi} \mathbb{C}^{\times}.$$

Through this last sequence of maps, we can consider χ as a character on $\mathrm{Cl}_{\mathfrak{f}}(K)$. We shall denote it by χ' and we consider the generalized Dirichlet L-series $L(s, \chi')$.

We then have the following equality:

$$L(s, \chi, K/k) = \prod_{\mathfrak{p} \in S} \left(1 - \frac{\chi(\sigma_{\mathfrak{P}})}{\mathbb{N}(\mathfrak{p})^s}\right)^{-1} \cdot L(s, \chi'),$$

where $S = \{$primes $\mathfrak{p} \mid \chi(I(\mathfrak{P}|\mathfrak{p})) = 1,$ and $\mathfrak{p}|\mathfrak{f}\}$.

3.4.1 Functional equation

While studying the distribution of prime numbers, Riemann was led to prove a functional equation for the Riemann zeta function. This allowed him to extend the definition of this function to the whole complex plane and along the way he stated his famous Riemann hypothesis, which is still unproved. Here, we state the functional equation for Artin L-functions. We give first the definition of the relevant mathematical objects.

Let V be a finite complex representation of $\mathrm{Gal}(K/k)$ with character χ. The Artin conductor of χ is defined as follows. Let $\mathfrak{p}$ be a prime ideal of k and let $\mathfrak{P}$ be a prime ideal of K lying above $\mathfrak{p}$. Let $G_i(\mathfrak{P}|\mathfrak{p})$ be the higher ramification groups. Note

that $G_0(\mathfrak{P}|\mathfrak{p}) = I(\mathfrak{P}|\mathfrak{p})$. Define

$$f(\chi, \mathfrak{p}) = \sum_{i=1}^{\infty} \frac{|G_i(\mathfrak{P}|\mathfrak{p})|}{|I(\mathfrak{P}|\mathfrak{p})|} \cdot \mathrm{codim}(V^{G_i(\mathfrak{P}|\mathfrak{p})}).$$

Note first that this sum is a finite sum, and that this number does not depend on the prime $\mathfrak{P}$ lying above $\mathfrak{p}$. It is also known that this number is actually an integer though it is not clear from the definition. Define then the Artin conductor of χ to be the integral ideal of k:

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\chi,\mathfrak{p})}.$$

Next, for any infinite real place v of k, let w be a place of K lying above v, and let

$$n_+ = \dim(V^{D(w|v)}), \qquad n_- = \mathrm{codim}(V^{D(w|v)}).$$

These numbers depend only on v. Define then

$$L_v(s, \chi, K/k) = \begin{cases} \Gamma_{\mathbb{R}}(s)^{n_+} \cdot \Gamma_{\mathbb{R}}(s+1)^{n_-}, & \text{for } v \text{ real;} \\ (\Gamma_{\mathbb{R}}(s) \cdot \Gamma_{\mathbb{R}}(s+1))^{\chi(1)}, & \text{for } v \text{ complex,} \end{cases}$$

where $\Gamma_{\mathbb{R}}(s) = \pi^{-s/2}\Gamma(s/2)$. Let also ∞ denote the set of all infinite primes of k.

We can now define the completed Artin L-function Λ:

$$\Lambda(s, \chi, K/k) = \left(|\Delta_K|^{\chi(1)} \cdot \mathbb{N}(\mathfrak{f}(\chi))\right)^{s/2} \cdot \left(\prod_{v|\infty} L_v(s, \chi, K/k)\right) \cdot L(s, \chi, K/k).$$

Theorem 3.4.3 *The completed Artin L-function satisfies the following functional equation:*

$$\Lambda(1-s, \chi, K/k) = W(\chi) \cdot \Lambda(s, \overline{\chi}, K/k),$$

where $\overline{\chi}$ is the character of the dual representation and $W(\chi)$ is a complex number of norm one such that $W(1) = 1$ ($W(\chi)$ is called the Artin root number).

CHAPTER 4
Stark's conjectures

The main reference for this chapter is [73]. For another nicely written reference in english, see [12]. Moreover, the papers by Stark are still interesting, see [68], [69], [70], and [71].

For the abelian rank one conjecture, see in particular Chapter 4 of [68].

Recall Formula 2.7 of Chapter 2 for a quadratic field $K = \mathbb{Q}(\sqrt{d})$:

$$L(1,\chi) = \begin{cases} \frac{2\log\varepsilon}{\sqrt{|\Delta_K|}} \cdot h_K, & \text{if } d > 0; \\ \frac{2\pi}{\omega_K\sqrt{|\Delta_K|}} \cdot h_K, & \text{if } d < 0, \end{cases}$$

where again χ is the non-trivial character of $\mathrm{Gal}(K/\mathbb{Q})$, h_K is the class number, Δ_K is the discriminant, ε is the fundamental unit in the case where $d > 0$, and ω_K is the number of roots of unity in K.

Stark's conjecture is an attempt to generalize this last formula to any general Artin L-function. As Stark noticed, it seems to be more natural to look at $s = 0$ instead of $s = 1$. Indeed, for instance, we have

$$\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}\mathrm{Reg}(K)}{\omega_K\sqrt{|\Delta_K|}} \cdot h_K \cdot \frac{1}{s-1} + O(s-1),$$

but using the functional equation for the Dedekind zeta function (which is a particular case of the general functional equation of an Artin L-function with $\chi = \chi_1$, see Theorem 3.4.3), we get the following formula for the Taylor series at $s = 0$:

$$\zeta_K(s) = -\frac{h_K\mathrm{Reg}(K)}{\omega_K}s^{r_1+r_2-1} + O(s^{r_1+r_2}).$$

This last formula is much simpler.

Let K/k be any finite galois extension of number fields. Let $G = \mathrm{Gal}(K/k)$, and V be a finite dimensional complex representation of G with character χ. Following Tate, we shall work with any finite set of primes S containing the set of infinite ones S_∞. In that case, we define

$$L_S(s,\chi,K/k) = \prod_{\mathfrak{p}\notin S} \frac{1}{\det(1-\sigma_{\mathfrak{P}}\mathbb{N}(\mathfrak{p})^{-s}|V^{I(\mathfrak{P}|\mathfrak{p})})}.$$

This function also represents an analytic function on $\mathrm{Re}(s) > 1$, and can be extended to a meromorphic function on the complex plane. Write the Taylor expansion of $L_S(s,\chi,K/k)$ at $s=0$:

$$L_S(s,\chi,K/k) = c_S(\chi)s^{r_S(\chi)} + O(s^{r_S(\chi)+1}).$$

The order $r_S(\chi)$ is known explicitly:

Theorem 4.0.4 *For any $v \in S$, let w be any place of K lying above v. The order $r_S(\chi)$ is given by the formula*

$$r_S(\chi) = \sum_{v\in S} \dim(V^{D(w|v)}) - \dim(V^G).$$

We get as an immediate consequence the following corollary:

Corollary 4.0.1 *If χ is the character of a one-dimensional representation, then*

$$r_S(\chi) = \begin{cases} |S|-1, & \text{if } \chi = \chi_1; \\ |\{v\in S \,|\, \chi(D(w|v)) = 1\}|, & \text{if } \chi \neq \chi_1. \end{cases}$$

Stark's conjecture is an attempt to describe $c_S(\chi)$. We will not state the general non-abelian Stark conjecture, see [73]. Instead, we shall present the abelian rank one conjecture that Stark gave. In that case, it is more precise and predicts the existence of a unit which is called a Stark unit. First, we recall here the definition of S-units

in a number field K, where S is a finite set of primes of K containing S_∞:

$$O_{K,S}^{\times} := \{\lambda \in K \big| \, |\lambda|_w = 1, \text{ for all } w \notin S\}.$$

Note, that when $S = S_\infty$, one gets back the usual units of O_K.

Suppose now that K/k is an abelian extension of number fields. Let S be a set of primes of k satisfying:

S1. $|S| \geq 2$;

S2. S contains S_∞ and all primes which ramify in K;

S3. S contains at least one place which splits completely in K.

Note that v splits completely if and only if $D(w|v) = 1$. Therefore, the conditions that we impose on S are precisely the ones that we should ask in order to have $r_S(\chi) \geq 1$ by Corollary 4.0.1.

Let now S_K denotes the set of primes of K lying above those in S. Fix a place v of S which splits completely in K, and fix a w in S_K above v. If $|S| \geq 3$, define

$$U^v = \{u \in O_{K,S_K}^{\times} \big| \, |u|_{w'} = 1, \text{ for all } w' \nmid v\}.$$

If $S = \{v_1, v_2\}$, and w_2 is above v_2, then define

$$U^v = \{u \in O_{K,S_K}^{\times} \big| \, |u|_{\sigma w_2} = |u|_{w_2}, \text{ for all } \sigma \in G\}.$$

Finally, define

$$U_{K/k}^{ab} = \{u \in O_{K,S_K}^{\times} | K(u^{\frac{1}{\omega_K}})/k \text{ is an abelian extension}\}.$$

Conjecture 4.0.1 (Stark) *There exists a S-unit $\varepsilon \in U_{K/k}^{ab} \bigcap U^v$ such that*

$$L_S'(0, \chi, K/k) = -\frac{1}{\omega_K} \sum_{\sigma \in G} \chi(\sigma) \log |\varepsilon^\sigma|_w,$$

for all $\chi \in \widehat{G}$.

The ε in the conjecture is called a Stark unit, and we shall denote this conjecture by $\mathrm{St}(K/k, S, v)$.

Theorem 4.0.5 *The conjecture* $\mathrm{St}(K/k, S, v)$ *is true if* S *contains another totally split place* v'.

Note that this last theorem is trivial if either $|S| = 2$ and $\chi \neq \chi_1$, or $|S| \geq 3$. Indeed, it suffices to take $\epsilon = 1$. The interesting case is thus when we have simultaneously $|S| = 2$ and $\chi = \chi_1$.

Therefore, the conjecture is independent of the choice of v in S, so from now on, we shall denote $\mathrm{St}(K/k, S, v)$ by $\mathrm{St}(K/k, S)$. Some consequences follow from this last theorem.

Corollary 4.0.2 *The conjecture* $\mathrm{St}(k/k, S)$ *is true.*

Corollary 4.0.3 *If* S *contains two complex places, then* $\mathrm{St}(K/k, S)$ *is true.*

Corollary 4.0.4 *If* S *contains a finite place* v *which splits completely and* k *is not totally real then* $\mathrm{St}(K/k, S)$ *is true.*

What happens if we change the set S? It is clear that if $S \subseteq S'$, then S' satisfies also properties **S1**, **S2**, and **S3**.

Theorem 4.0.6 *If the conjecture* $\mathrm{St}(K/k, S)$ *is true, then* $\mathrm{St}(K/k, S')$ *is true for any* $S' \supseteq S$.

It is also clear that if S satisfies the condition **S1**, **S2**, and **S3** for K/k then S satisfies them also for any intermediate field $k \subseteq L \subseteq K$.

Theorem 4.0.7 *If* $k \subseteq L \subseteq K$, *then* $\mathrm{St}(K/k, S)$ *implies* $\mathrm{St}(L/k, S)$.

This conjecture is also known to be true for the base fields $\mathbb{Q}$ and $k = \mathbb{Q}(\sqrt{d})$, with $d < 0$. In the latter case, Stark used the theory of elliptic units that has been introduced by Siegel. We will give an introduction to these units in Chapter 5.

CHAPTER 5
Classical theory of elliptic units

We used several books for this section. For the theory of elliptic functions, we used [35] amongs other. See also [36], [41] and [81]. For a historical survey of these functions which were so important for the development of mathematics in the XIXth century, see the article of Houzel in either [29] or [16].

The theory of elliptic curves can be found in [35] or in [66].

The theory of classical modular function is often presented only for some particular groups and this presentation is often *ad hoc*. For a more general perspective, we found really useful the following two references: [64] and [61].

For the theory of complex multiplication of elliptic curves, the book [5] is good for a first reading. Then, we used also [11], the article of Jean-Pierre Serre in [8] and [15].

5.1 Introduction

Let K be an imaginary quadratic number field and let $K_{\mathfrak{m}}$ be any ray class field modulo $\mathfrak{m}$, for some modulus $\mathfrak{m}$. In [65], Siegel gave a class number formula relating both class numbers $h_{K_{\mathfrak{m}}}$ and h_K. First he computed the values of L-series at $s = 1$ using Kronecker's limit formula, and by the way he constructed some units in $K_{\mathfrak{m}}$. These units are now called elliptic units and they have been studied by Ramachandra in [51] and Robert in [55].

Stark used this construction in order to prove his rank one abelian conjecture when the base field is a quadratic imaginary field.

In this chapter, we present the background in order to understand Siegel's construction and then we give a sketch of the proof of Stark's conjecture when the base field is quadratic imaginary.

5.2 Elliptic functions and elliptic curves

The theory of elliptic functions is a vast subject and it is difficult to get acquainted with it. One can view the birth of several mathematical disciplines in the development of this theory (such as Riemann surfaces and some topics in algebraic topology). We shall first explain how people got interested in these and then state the main results.

In the XVIth and XVIIth centuries, calculus has been mostly invented by Gottfried Leibniz (1646-1716) and Issac Newton (1643-1727). It was then natural to try to compute the arc length of an ellipse. Let

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

where $a > b > 0$, be the equation of an ellipse. Given any curve $y = f(x)$ of class C^1, the arc length between two points is given by the formula

$$L(\lambda_1, \lambda_2) = \int_{x=\lambda_1}^{\lambda_2} \sqrt{1 + f'(x)}\, dx.$$

If we compute the arc lentgh of the ellipse above with $\lambda_1 = 0$ we get

$$L(\lambda) = \int_{x=0}^{\lambda} \sqrt{\frac{a^2 - ex^2}{a^2 - x^2}}\, dx = \int_{x=0}^{\lambda} \frac{a^2 - ex^2}{\sqrt{(a^2 - x^2)(a^2 - ex^2)}}\, dx, \tag{5.1}$$

where $e = 1 - \frac{b^2}{a^2}$. Other integrals coming from physical problems lead to similar integrals. An integral of the type

$$\int R(x, y)\, dx,$$

where R is a rational function in x and y, and $y = \sqrt{P(x)}$ for some cubic or quartic polynomial $P(x)$, is called an elliptic integral (because of the particular case of the ellipse). Mathematicians suspected that these are not integrable by elementary functions (rational functions, trigonometric function, exp, log, etc). Adrien-Marie

Legendre (1752-1833) wrote a treatise on elliptic integrals and reduced them to three types:

- $F(k,x) = \int_{t=0}^{x} \frac{1}{\sqrt{(1-t^2)(1-k^2t^2)}}\,dt$,
- $E(k,x) = \int_{t=0}^{x} \frac{1-k^2t^2}{\sqrt{(1-t^2)(1-k^2t^2)}}\,dt$,
- $\Pi(k,n,x) = \int_{t=0}^{x} \frac{1}{(1+nt^2)\sqrt{(1-t^2)(1-k^2t^2)}}\,dt$,

which are called elliptic integrals of the first, second and third type, respectively. Note that if in Equation (5.1) we set $e = k^2$ and make the change of variable $x = au$ then we get an elliptic integral of the second kind.

In order to study these integrals, Abel and Carl Jacobi (1804-1851) had the idea of inverting these integrals and study instead their inverses. Consider the arcsin function

$$u = \arcsin(x) = \int_{t=0}^{x} \frac{1}{\sqrt{1-t^2}}\,dt,$$

where $-1 \leq x \leq 1$. It is easier to work with the inverse $\sin(u) = x$. In particular, we have the addition formula

$$\sin(u+v) = \sin(u)\sqrt{1-\sin^2(v)} + \sqrt{1-\sin^2(u)}\sin(v).$$

Recall that an addition formula for a function f is an algebraic relation of the form $F(f(u+v), f(u), f(v))$, where F is a polynomial. Here is an example leading to the concept of elliptic function. Set $u(x) = F(k,x)$, the elliptic integral of the first kind. Set also $K = \int_{t=0}^{1} \frac{1}{\sqrt{(1-t^2)(1-k^2t^2)}}\,dt$. Define for $-K \leq u \leq K$, the inverse $x = \mathrm{sn}(u)$ which is called a Jacobian elliptic function because he used it extensively during his research on elliptic functions. This function also has an addition theorem:

$$\mathrm{sn}(u+v) = \frac{\mathrm{sn}(u)\sqrt{1-\mathrm{sn}^2(v)}\sqrt{1-k^2\mathrm{sn}^2(v)} + \mathrm{sn}(v)\sqrt{1-\mathrm{sn}^2(u)}\sqrt{1-k^2\mathrm{sn}^2(u)}}{1-k^2\mathrm{sn}^2(u)\mathrm{sn}^2(v)}.$$

Using this addition theorem, we can extend $\mathrm{sn}(u)$ to all real values of u. Moreover this function is periodic of period $4K$, that is $\mathrm{sn}(u+4K) = \mathrm{sn}(u)$. While Augustin

Louis Cauchy (1789-1857) was developping his theory of complex integration, it was natural to try to extend the definition of an elliptic function to complex variables as mathematicians did for the trigonometric functions. There is one big problem now. Consider the complex integral

$$L(a,b) = \int_\gamma R(z, \sqrt{P(z)})\, dz,$$

where γ is a C^1 path going from a to b, R is a rational function, and $P(z)$ is a polynomial of degree 3 or 4. When the variable is real, we are able to chose a canonical root using the order relation on $\mathbb{R}$. We do not have such an order relation on $\mathbb{C}$ so this expression is ambigous. Riemann discovered the theory of Riemann surfaces (or created depending on the point of view!) precisely because he was trying to explain the meaning of such integrals. One can fully understand this expression only within this theory. Before Riemann, mathematicians tried to study these integrals in many ways. One soon noticed that the inverse of such integrals are doubly periodic functions on the complex plane and that they still satisfy an addition theorem. As we will see, the addition theorem of elliptic functions is an important property of these functions. Joseph Liouville (1809-1882) and Gotthold Eisenstein (1823-1852) have been the first ones to study doubly periodic functions without any references to elliptic integrals. Liouville's approach was more function theoretical and Eisenstein's approach more constructive.

5.2.1 Liouville's approach

Starting, as Liouville did, with an arbitrary meromorphic function $f : \mathbb{C} \to \mathbb{C}$, we call such a function doubly periodic if there exist two numbers ω_1 and ω_2 such that $f(z+\omega_1) = f(z+\omega_2) = f(z)$ for all $z \in \mathbb{C}$. If ω_1/ω_2 is rational, then one can show that f reduces to a function with only one period (singly periodic function) and if ω_1/ω_2 is irrational ($\in \mathbb{R} - \mathbb{Q}$) then Jacobi showed that the function reduces to a constant. So we are led to the following definition:

Definition 5.2.1 *Let ω_1 and ω_2 be two $\mathbb{R}$-linearly independent periods in $\mathbb{C}$ (so the quotient ω_1/ω_2 is not real). An elliptic function is a complex-valued meromorphic function f such that $f(z+\omega_1) = f(z+\omega_2) = f(z)$, for all $z \in \mathbb{C}$.*

It is then clear from the definition that if $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, then $f(z+\omega) = f(z)$ for all $\omega \in \Lambda$. A discrete free $\mathbb{Z}$-module of rank 2 contained in $\mathbb{C}$ is called a lattice. The $\mathbb{Z}$-module Λ above is such a lattice and every lattice in $\mathbb{C}$ is of this form for some $\mathbb{R}$-linearly independent numbers (ω_1, ω_2). Given a lattice $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, the set $P = \{z = t_1\omega_1 + t_2\omega_2 \in \Lambda | 0 \leq t_1, t_2 < 1\}$ is called a fundamental parallelogram for Λ. $\mathbb{C}$ is then the disjoint union $\mathbb{C} = \coprod_{\omega\in\Lambda}(\omega + P)$. The set of all elliptic functions for a fixed lattice Λ is clearly a field and we denote this field by $\mathbb{C}_{E,\Lambda}$. We state here Liouville's theorems. For these theorems, fix a lattice Λ and an elliptic function f for this lattice.

Theorem 5.2.1 (Liouville) *If f is entire (holomorphic on all $\mathbb{C}$) then f is constant.*

Theorem 5.2.2 (Liouville) *The sum of the residues of f in a fundamental parallelogram P is equal to zero (counting multiplicities).*

Theorem 5.2.3 (Liouville) *The number of zeros of f in a fundamental parallelogram P is equal to the number of its poles (counting multiplicities).*

5.2.2 Eisenstein's approach

Eisenstein's approach was to construct directly doubly periodic functions. He defined for $n \geq 1$ the following function. Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$, then define

$$E_n(z) = \sum_{\omega\in\Lambda} \frac{1}{(z+\omega)^n} = \sum_{m_1,m_2\in\mathbb{Z}} \frac{1}{(z+m_1\omega_1+m_2\omega_2)^n}.$$

For $n \geq 3$ there is no problem and these series are absolutely convergent. For $n = 1, 2$ we have to define a summation process, namely Eisenstein summation given by

$$\sum_e = \lim_{N\to\infty} \sum_{-N}^{N} \left(\lim_{M\to\infty} \sum_{-M}^{M} \right).$$

These functions $E_n(z)$ are elliptic functions with respect to the lattice Λ.

For more details, and to see how Kronecker improved Eisenstein's work, see the marvelous little book [79] by Weil. We just introduced Eisenstein's work because now it is more natural to introduce the Weierstrass $\wp$-function.

5.2.3 Weierstrass' theory

Weierstrass' theory provides the link between elliptic functions and algebraic geometry, namely the concept of elliptic curves which is more suitable for arithmetical purpose than the analytic theory of elliptic functions.

Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. Weierstrass defined the so-called $\wp$-function (actually, he found it by taking the second derivative of the logarithm of the σ-function which he introduced before in relation with his theory on the development of entire functions as infinite convergent products)

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

When there is no danger of confusion, we simply write $\wp(z)$ instead of $\wp(z,\Lambda)$. In contrast to $E_2(z)$, this series converges absolutely and uniformly, so it represents a meromorphic function on $\mathbb{C}$. The periodicity is, on the other hand, less obvious than for $E_2(z)$. Anyway, one can prove that $\wp(z)$ is an elliptic function for Λ. The derivative is

$$\wp'(z) = -2\sum_{\omega\in\Lambda} \frac{1}{(z-\omega)^3},$$

and note that the derivative of an elliptic function is still an elliptic function for the same lattice.

Theorem 5.2.4 *We have* $\mathbb{C}_{E,\Lambda} = \mathbb{C}(\wp(z,\Lambda), \wp'(z,\Lambda))$ *or in words: The field of elliptic functions for the fixed lattice* Λ *is generated by* $\wp(z)$ *and* $\wp'(z)$.

The Weierstrass $\wp$-function satisfies also an addition theorem:

Theorem 5.2.5 (Addition theorem) *The Weierstrass function satisfies the following addition formula*

$$\wp(z_1+z_2) = -\wp(z_1) - \wp(z_2) + \frac{1}{4}\left(\frac{\wp'(z_1)-\wp'(z_2)}{\wp(z_1)-\wp(z_2)}\right)^2,$$

for all $z_1, z_2 \in \mathbb{C}$.

It is also known that the only functions defined over $\mathbb{C}$ with an addition theorem are the elliptic functions, the trigonometric functions and the rational functions. Moreover, $\wp$ satisfies a differential equation. Define first

$$G_k = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^k}.$$

This series converges absolutely for $k \geq 3$. Note also that for odd k, $G_k = 0$.

Theorem 5.2.6 *As is traditional, set* $g_2 = g_2(\Lambda) = 60G_4$ *and* $g_3 = g_3(\Lambda) = 140G_6$. *Then we have the following differential equation*

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) + g_3$$

and $g_2^3 - 27g_3^2 \neq 0$.

This differential equation provides the link between elliptic functions and algebraic geometry. Indeed, the equation $y^2 = 4x^3 - g_2x - g_3$ defines a curve and Theorem 5.2.6 means that the point $(\wp(z), \wp'(z))$ lies on this curve (the fact that $g_2^3 - 27g_3^2 \neq 0$ means that the curve is non-singular). The converse is also true, namely:

Theorem 5.2.7 *Suppose that* c_2 *and* c_3 *are two complex numbers satisfying the condition* $c_2^3 - 27c_3^2 \neq 0$. *Then the equation* $y^2 = 4x^3 - c_2x - c_3$ *defines a non-singular algebraic curve and there exists two* $\mathbb{R}$*-linearly independent periods* ω_1 *and* ω_2 *such that* $g_2(\omega_1, \omega_2) = c_2$ *and* $g_3(\omega_1, \omega_2) = c_3$.

5.2.4 Elliptic curves

As explained above, the curve with equation $y^2 = 4x^3 - g_2x - g_3$ is parametrized by elliptic functions. Complex algebraic curves which can be parametrized by elliptic functions are called elliptic curves. Alfred Clebsch (1833-1872) discovered other curves that can be parametrized by these, for example the intersection of two quadrics in the affine space $\mathbb{A}^3(\mathbb{C})$ admits such a parametrization.

Next, if we introduce some topological notions, we can characterize elliptic curves through their genus. It is true that every non-singular projective algebraic curve gives via the implicit function theorem a compact Riemann surface. It is also true that a Riemann surface is a non-singular projective algebraic curve if and only if it is compact. The Riemann surface associated with the projectivization of the curve of equation $y^2 = 4x^3 - g_2x - g_3$ is a torus, namely $\mathbb{C}/\Lambda$. The field of elliptic functions for the lattice Λ is isomorphic to the field of meromorphic functions on $\mathbb{C}/\Lambda$. One can show that every non-singular algebraic curve of genus 1 defined over $\mathbb{C}$ is isomorphic to the projectivization of a non-singular plane cubic with equation $y^2 = 4x^3 - g_2x - g_3$, where $g_2^3 - 27g_3^2 \neq 0$. We can reinterpret Theorem 5.2.6 and 5.2.7 as follows:

Theorem 5.2.8 *Given any elliptic curve E defined over $\mathbb{C}$ in the projective form*

$$y^2z = 4x^3 - c_2xz^2 - c_3z^3,$$

there exists a lattice $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ such that $g_2(\Lambda) = c_2$, $g_3(\Lambda) = c_3$ and such that the map $\mathbb{C}/\Lambda \to E(\mathbb{C})$ defined by

$$z + \Lambda \mapsto \begin{cases} [\wp(z) : \wp'(z) : 1] \text{ if } z \notin \Lambda; \\ [0 : 1 : 0] \text{ if } z \in \Lambda, \end{cases}$$

is a biholomorphic map.

Therefore, over $\mathbb{C}$, we can view an elliptic curve as a torus $\mathbb{C}/\Lambda$ for some lattice Λ. We can then tranport the structure of the abelian group $\mathbb{C}/\Lambda$ on the curve E. We

get this really nice geometric interpretation called secant-tangent process. Using the addition theorem for the Weierstrass function, we can describe explicitly this group law on the coordinates of the points of E and thus define this group law algebraically. Kronecker already used this in his research on elliptic functions. This allows one to extend the definition of the group law to elliptic curves defined over any field. The modern notion of an elliptic curve is the following:

Definition 5.2.2 *Let k be an algebraic closed field. An elliptic curve over k is a non-singular (irreducible) projective curve E, which is also a group, and such that the group law*

$$+ : E \times E \to E$$

and the inverse map

$$- : E \to E$$

are morphisms of algebraic varieties.

Remark: One can prove that the group law is necessarily commutative. This is why we use the additive symbol $+$. Moreover, one can show that a non-singular projective curve which has a group law given by an algebraic map is necessarily of genus one. An alternative definition for an elliptic curve is thus a non-singular curve of genus one with a distinguished point (the zero element).

We shall now explain the link between the analytic structure of $\mathbb{C}/\Lambda$ and the algebraic structure of the associated elliptic curve.

Definition 5.2.3 *Let E_1 and E_2 be elliptic curves. A morphism of elliptic curves is an algebraic morphism $\phi : E_1 \to E_2$ such that ϕ is also a group homomorphism. The set of all morphisms of elliptic curves between E_1 and E_2 is denoted by* $\mathrm{Hom}(E_1, E_2)$. *A morphism $\phi : E_1 \to E_2$ is called an isomorphism if there exists another morphism $\psi : E_2 \to E_1$ such that $\phi \circ \psi = id_{E_2}$ and $\psi \circ \phi = id_{E_1}$. If $E_1 = E_2$, then a morphism is called an endomorphism and we denote the ring of endomorphisms of an elliptic curve E by* $\mathrm{End}(E)$.

Let $E_i \simeq \mathbb{C}/\Lambda_i$ be elliptic curves defined over $\mathbb{C}$, $(i = 1, 2)$. If $\phi \in \mathrm{Hom}(E_1, E_2)$, then it is given by rational functions and therefore it induces a holomorphic map

$$\bar{\phi} : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2,$$

such that $\bar{\phi}(0) = 0$. Actually, this correspondence is a bijection (in fancy language, we have an equivalence of categories).

Theorem 5.2.9 *Let $E_i \simeq \mathbb{C}/\Lambda_i$ be elliptic curves defined over $\mathbb{C}$ $(i = 1, 2)$ and let $\phi \in \mathrm{Hom}(E_1, E_2)$. Then the correspondence $\phi \mapsto \bar{\phi}$ makes the following diagram commutative*

$$\begin{array}{ccc} E_1 & \xrightarrow{\simeq} & \mathbb{C}/\Lambda_1 \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\bar{\phi}} \\ E_2 & \xrightarrow{\simeq} & \mathbb{C}/\Lambda_2 \end{array},$$

and this correspondence is a bijection between $\mathrm{Hom}(E_1, E_2)$ and the set of holomorphic maps $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ such that $\phi(0) = 0$.

Theorem 5.2.10 *Let $E_i \simeq \mathbb{C}/\Lambda_i$ be elliptic curves $(i = 1, 2)$. Let $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ be a holomorphic map such that $\phi(0) = 0$. There exists a linear map $L_\phi : \mathbb{C} \to \mathbb{C}$ such that $L_\phi(\Lambda_1) \subseteq \Lambda_2$ and such that the following diagram is commutative*

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{L_\phi} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}/\Lambda_2 \end{array}.$$

This gives a bijection between

$$\{\mathbb{C}\text{-linear map } L : \mathbb{C} \to \mathbb{C} \text{ such that } L(\Lambda_1) \subseteq \Lambda_2\},$$

and

$$\{\text{holomorphic maps } \phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2 \text{ s.t. } \phi(0) = 0\}.$$

According to these theorems, we identify $\mathrm{Hom}(E_1, E_2)$ with the set $\{\alpha \in \mathbb{C} | \alpha\Lambda_1 \subseteq \Lambda_2\}$ since every $\mathbb{C}$-linear map $L : \mathbb{C} \to \mathbb{C}$ is of the form $L(z) = \alpha \cdot z$ for some $\alpha \in \mathbb{C}$. In

particular, if $E_1 = E_2 = E \simeq \mathbb{C}/\Lambda$, then we identify $\mathrm{End}(E)$ with the set

$$\{\alpha \in \mathbb{C} | \alpha\Lambda \subseteq \Lambda\}.$$

In Section 5.4 of this chapter, we will explain the link between elliptic curves and number theory.

5.3 Modular functions

The first appearance of modular (or automorphic) functions came through the theories of binary quadratic forms and elliptic functions. Indeed, let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$ and suppose $\mathrm{Im}(\omega_1/\omega_2) > 0$ (this amounts to choosing an orientation). The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper-half plane by

$$z \mapsto \alpha \cdot z = \frac{az+b}{cz+d}, \qquad \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).$$

To verify that, one uses the formula $\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \frac{(ad-bc)\mathrm{Im}(z)}{|cz+d|^2}$, which is valid for any matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in M_2(\mathbb{R})$.

Set $\tau = \omega_1/\omega_2$. If Λ' is another lattice, we have $\lambda \cdot \Lambda = \Lambda'$ for some $\lambda \in \mathbb{C}$ if and only if there exists an $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ such that $\alpha \cdot \tau = \tau'$. We can view the Weierstrass' constants g_2 and g_3 as functions on the upper-half plane $\mathfrak{h}$ by setting

$$g_i(\tau) := g_i(\tau, 1),$$

where $\tau \in \mathfrak{h}$ and $i = 1, 2$. Then a simple calculation shows that g_i satisfies the following transformation formula

$$g_i(\gamma \cdot \tau) = (c\tau + d)^{2i} g_i(\tau), \qquad \text{for all } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z}).$$

Furthermore, the discriminant function $\Delta = g_2^3 - 27g_3^2$ (actually it is only the discriminant of the following polynomial up to a constant) of $4x^3 - g_2 x - g_3$ considered as a function on $\mathfrak{h}$ satisfies

$$\Delta(\gamma \cdot \tau) = (cz + d)^{12} \Delta(\tau).$$

We thus get a $SL_2(\mathbb{Z})$-invariant function by considering the modular function

$$J = \frac{g_2^3}{\Delta}.$$

This is the classical elliptic modular function ($SL_2(\mathbb{Z})$-automorphic function) and we shall explain it in more details in this section. The theory of automorphic functions has been developed initially by two mathematicians at the end of the XIXth century: Henri Poincaré (1854-1912) in France and Felix Klein (1849-1925) in Germany.

Through the work of Poincaré, automorphic functions can be viewed as an analogue of elliptic functions. This is actually the first application of non-euclidean geometry to other parts of mathematics. A lattice Λ gives a group of transformations of the Euclidean plane by setting $z \mapsto z + \omega$ for all $\omega \in \Lambda$. It is a discrete subgroup of the isometries of the Euclidean plane (isometries corresponding to the euclidean metric) and an elliptic function is a meromorphic function invariant under the action of this group. An automorphic function is the analogue, but in the hyperbolic plane.

Recall that the plane hyperbolic geometry is the geometry where the famous parallel axiom of Euclid in plane Euclidean geometry is replaced by the following one: "Through a given point not on a given line there passes more than one line that does not meet the given line". There exist several models for this geometry like the unit disk, the right half-plane (used by Gauss) or the more traditional upper half-plane. Poincaré noted that the modular transformations of the upper half-plane coming from the theory of elliptic functions are precisely hyperbolic isometries in this model. More precisely, this model consists of the upper half-plane

$$\mathfrak{h} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\},$$

where "lines" are taken to be half circles with center on the real line and lines perpendicular to the real axis. Figure 5–1 shows that the hyperbolic axiom above is

satisfied and one can verify that all other axioms are also satisfied. Thus this is a

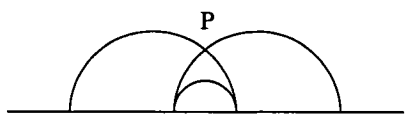

Figure 5–1: Plane hyperbolic geometry

model of plane hyperbolic geometry. Given two points $z, w \in \mathbb{C}$ and a curve γ joining z and w, we define

$$||\gamma|| = \int_\gamma \frac{|dz|}{\mathrm{Im}(z)},$$

and the hyperbolic metric d is given by $d(z,w) = \inf\ ||\gamma||$, where the infimum is taken over all curves between z and w. It is true then that the isometries of the hyperbolic plane are given in this model by the transformations

$$z \mapsto \frac{az+b}{cz+d}, \qquad \text{where } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R}).$$

If we denote the set of scalar matrices by $\mathbb{R}^\times \cdot I_2$, then $\mathrm{GL}_2^+(\mathbb{R})/(\mathbb{R}^\times \cdot I_2)$ is isomorphic to the group of biholomorphic automorphisms of the upper-half plane. We also have the isomorphism

$$\mathrm{PSL}_2(\mathbb{R}) := \mathrm{SL}_2(\mathbb{R})/\{\pm I_2\} \simeq \mathrm{GL}_2^+(\mathbb{R})/(\mathbb{R}^\times \cdot I_2).$$

Therefore, depending on personal taste, one can work either with $\mathrm{GL}_2^+(\mathbb{R})$ or $\mathrm{SL}_2(\mathbb{R})$. Next, Poincaré asked himself for which subgroups of $\mathrm{PSL}_2(\mathbb{R})$ are there non-constant meromorphic functions invariant under the action of the subgroup. He saw that necessarily, such subgroups must be discrete, and then started the theory of discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$ or, equivalently $\mathrm{SL}_2(\mathbb{R})$.

Given a discrete subgroup Γ of $\mathrm{PSL}_2(\mathbb{R})$, he defined the concept of automorphic function with respect to Γ by declaring a meromorphic function on $\mathfrak{h}$ to be Γ-automorphic if it is invariant under Γ.

Let Γ be a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. The space of orbits $\mathfrak{h}/\Gamma$ is not necessarily compact. In order to compactify it, we have to add points called cusps. We explain this here. First, we need to classify the fractional transformation of the Riemann sphere $\mathbb{C} \cup \{\infty\}$:

$$z \mapsto \frac{az+b}{cz+d}, \qquad \text{where } \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C}).$$

Suppose now that α is not a scalar matrix. There are two possibilities for the Jordan normal form of α:

$$\left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right) \text{ or } \left(\begin{smallmatrix} \lambda & 0 \\ 0 & \mu \end{smallmatrix}\right),$$

where $\lambda, \mu \in \mathbb{C}$, $\lambda \neq \mu$. In the first case, α is called parabolic. In the second case, the transformation is of the form $z \mapsto cz$, where $c = \lambda/\mu$. If $|c| = 1$ then α is called elliptic, if c is real and positive then α is called hyperbolic, and otherwise α is called loxodromic. If we restrict ourselves to $\mathrm{SL}_2(\mathbb{C})$ then we have the following theorem:

Theorem 5.3.1 *Let $\alpha \in \mathrm{SL}_2(\mathbb{C})$ and suppose that $\alpha \neq \pm I_2$. Then*

- *α parabolic $\Leftrightarrow \mathrm{Tr}(\alpha) = \pm 2$;*
- *α elliptic $\Leftrightarrow \mathrm{Tr}(\alpha)$ is real and $|\mathrm{Tr}(\alpha)| < 2$;*
- *α hyperbolic $\Leftrightarrow \mathrm{Tr}(\alpha)$ is real and $|\mathrm{Tr}(\alpha)| > 2$;*
- *α loxodromic $\Leftrightarrow \mathrm{Tr}(\alpha)$ is not real.*

If we specialize further to $\mathrm{SL}_2(\mathbb{R})$, the group we are interested in, then we first see from the last theorem that it does not have any loxodromic element. Further:

Theorem 5.3.2 *Let $\alpha \in \mathrm{SL}_2(\mathbb{R})$ and suppose that $\alpha \neq \pm I_2$. Then*

- *α parabolic $\Leftrightarrow$ α has only one fixed point on $\mathbb{R} \cup \{\infty\}$;*
- *α elliptic $\Leftrightarrow$ α has one fixed point $z \in \mathfrak{h}$ and the other fixed point is $\overline{z}$;*
- *α hyperbolic $\Leftrightarrow$ α has two fixed points on $\mathbb{R} \cup \{\infty\}$.*

We can now define the notion of cusp. First note that if $\alpha \in \mathrm{PSL}_2(\mathbb{R})$, it makes sense to talk about the type of α (parabolic, elliptic or hyperbolic).

Definition 5.3.1 *Let Γ be any discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. Then*

- $z \in \mathfrak{h}$ *is called elliptic if there exists an elliptic element* $\alpha \in \Gamma$ *such that* $\alpha \cdot z = z$.
- $s \in \mathbb{R} \cup \{\infty\}$ *is called a cusp if there exists a parabolic element* $\alpha \in \Gamma$ *such that* $\alpha \cdot s = s$.

Definition 5.3.2 *Let* Γ *be any discrete subgroup of* $\mathrm{PSL}_2(\mathbb{R})$. *The completed upper-half plane* $\mathfrak{h}^*$ *consists of the union of the upper-half plane with all the cusps of* Γ.

Note that $\mathfrak{h}^*$ depends on Γ. The group Γ acts on $\mathfrak{h}^*$ so we can talk about the space of orbits $\mathfrak{h}^*/\Gamma$. The analogue of a fundamental parallelogram for an elliptic function is the concept of a fundamental region.

Definition 5.3.3 *Let* Γ *be a discrete subgroup of* $\mathrm{PSL}_2(\mathbb{Z})$. *Then a fundamental region for* Γ *is a subset* F *of* $\mathfrak{h}^*$ *such that*

- F *is a connected open subset of* $\mathfrak{h}$;
- *No two distinct points of* F *are* Γ*-equivalent;*
- *Every* $z \in \mathfrak{h}$ *is* Γ*-equivalent to a point of* $\overline{F}$.

Now, we define a topology on $\mathfrak{h}^*$ as follows (see Figure 5–2). If $s \neq \infty$ is a cusp then take as a basis of open neighborhoods the sets of the form $\{s\}$ union with the interior of a circle in $\mathfrak{h}$ tangent to the real axis at s. For ∞ take the sets $\{\infty\} \cup \{z \in \mathfrak{h} | \mathrm{Im}(z) > c\}$ for some positive number c and, finally, if $z \in \mathfrak{h}$, take as a basis of open neighborhoods those in $\mathfrak{h}$. This defines a Hausdorff topology on $\mathfrak{h}^*$.

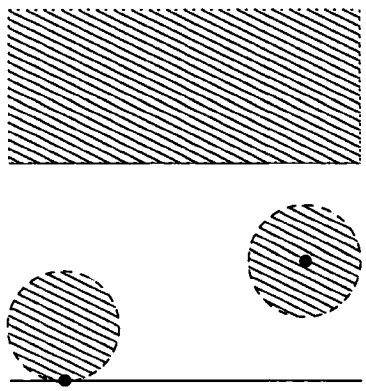

Figure 5–2: Topology on $\mathfrak{h}^*$

Theorem 5.3.3 *The space of orbits $\mathfrak{h}^*/\Gamma$ with the quotient topology is a locally compact Hausdorff space.*

Definition 5.3.4 *A discrete subgroup Γ of $\mathrm{PSL}_2(\mathbb{R})$ is called a Fuchsian group of the first kind if $\mathfrak{h}^*/\Gamma$ is compact.*

Next, we shall add a structure of Riemann surface on the space $\mathfrak{h}^*/\Gamma$. For this, we need a lemma.

Lemma 5.3.1 *Let Γ be a Fuchsian group of the first kind. Let $z \in \mathfrak{h}^*$ and look at its stabilizer $\mathrm{Stab}_\Gamma(z) = \{\gamma \in \Gamma | \gamma \cdot z = z\}$. Then there exists an open neighborhood U of z in $\mathfrak{h}^*$ such that*

$$\mathrm{Stab}_\Gamma(z) = \{\gamma \in \Gamma | \gamma(U) \cap U \neq \varnothing\}.$$

According to this last lemma, we can identify the set

$$U/\mathrm{Stab}_\Gamma(z) = \{\mathrm{Stab}_\Gamma(z) \cdot x | x \in U\},$$

with the image of U in $\mathfrak{h}^*/\Gamma$, which is open by definition of the quotient topology.

Lemma 5.3.2 *The group $\mathrm{Stab}_\Gamma(z)$ is a cyclic group, finite if z is not a cusp.*

We can now construct the atlas on $\mathfrak{h}^*/\Gamma$. There are three different kind of points to consider. For each point $z \in \mathfrak{h}^*$, we take an open neighborhood U of z such that

$$\mathrm{Stab}_\Gamma(z) = \{\gamma \in \Gamma | \gamma(U) \cap U \neq \varnothing\},$$

and we identify it with $\pi(U)$ by the previous discussion, where $\pi : \mathfrak{h}^* \to \mathfrak{h}^*/\Gamma$ is the natural projection.

- If $z \in \mathfrak{h}^*$ is neither a cusp nor an elliptic element, then $\mathrm{Stab}_\Gamma(z) = \{id\}$, therefore $U \simeq \pi(U)$ and we can take the chart $\pi^{-1} : U/\mathrm{Stab}_\Gamma(z) \to U \subseteq \mathbb{C}$.
- If $z \in \mathfrak{h}^*$ is an elliptic element. Let $n = \#\mathrm{Stab}_\Gamma(z)$. Take an isomorphism $\lambda : \mathfrak{h} \to D$, where D is the unit disc, such that $\lambda(z) = 0$. Take then the chart $\varphi : U/\mathrm{Stab}_\Gamma(z) \to \mathbb{C}$ defined by $\varphi(\pi(z)) = \lambda(z)^n$.

- If $s \in \mathbb{R} \cup \{\infty\}$ is a cusp then take a $\rho \in \mathrm{PSL}_2(\mathbb{R})$ such that $\rho(s) = \infty$. Then one can show that $\rho \cdot \mathrm{Stab}_\Gamma(z) \cdot \rho^{-1}$ is generated by a transformation of the form $z \mapsto z+h$ for some real number $h > 0$. Take then the chart $\varphi : U/\mathrm{Stab}_\Gamma(z) \to \mathbb{C}$ defined by $\varphi(\pi(z)) = e^{\frac{2\pi i \rho z}{h}}$.

This defines for a Fuchsian group of the first type a structure of compact Riemann surface on $\mathfrak{h}^*/\Gamma$. We are thus led to the generalization of elliptic functions.

Definition 5.3.5 *Let Γ be a Fuchsian group of the first kind. A Γ-automorphic function is a meromorphic function on the Riemann surface $\mathfrak{h}^*/\Gamma$.*

The analogue of the Eisenstein series are contained in the next definition.

Definition 5.3.6 *Let k be an integer and let Γ be a Fuchsian group of the first kind. A function $f : \mathfrak{h} \to \mathbb{C}$ is called a Γ-automorphic form of weight k if*

- *f is meromorphic on $\mathfrak{h}$.*
- *$f(\alpha \cdot z) = (cz + d)^k f(z)$ for all $z \mapsto \alpha \cdot z = \frac{az+b}{cz+d} \in \Gamma$.*
- *f is meromorphic at each cusp of Γ.*

5.3.1 The case of $\mathrm{SL}_2(\mathbb{Z})$

There is a family of discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$ which are particularly important for arithmetic purposes. Consider the subgroup $\mathrm{SL}_2(\mathbb{Z})$ with the reduction map modulo an integer N, $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ defined by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \left(\begin{smallmatrix} a+N\mathbb{Z} & b+N\mathbb{Z} \\ c+N\mathbb{Z} & d+N\mathbb{Z} \end{smallmatrix}\right)$. The kernel of this map is called the principal congruence subgroup of level N, and is denoted by $\Gamma(N)$. A $\Gamma(N)$-modular form of weight k is called a modular form of level N and weight k.

If we specialize the theory of the last section to the group $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$ we get the following. A fundamental region (see Figure 5–3) for this group consist of the set of $z \in \mathfrak{h}$ such that

- $-1/2 < \mathrm{Re}(z) < 1/2$;
- $|z| > 1$.

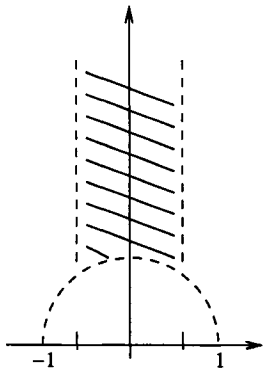

Figure 5–3: Fundamental domain for $\mathrm{SL}_2(\mathbb{Z})$

The elliptic points of $\Gamma(1)$ are those equivalent to i and ζ_3. The point ∞ is a cusp. Indeed, the transformation $z \mapsto z+1 \in \Gamma(1)$ is a parabolic element and fixes ∞. One can show that the cusps of $\Gamma(1)$ are $\mathbb{Q} \cup \{\infty\}$ and that each cusp is equivalent to ∞.

A $\Gamma(1)$-modular function (or automorphic) is thus a function $f : \mathfrak{h} \to \mathbb{C}$ such that:

- $f(\gamma \cdot z) = f(z)$ for all $\gamma \in \Gamma(1)$;
- $f(e^{2\pi i z}) = \sum_{n \geq -m} a_n e^{2\pi i n z}$, for $\mathrm{Im}(z) > a$ for some $a > 0$.

A $\Gamma(1)$-modular form of weight k is a function $f : \mathfrak{h} \to \mathbb{C}$ such that:

- $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ for all transformation $z \mapsto \frac{az+b}{cz+d} \in \Gamma(1)$;
- $f(e^{2\pi i z}) = \sum_{n \geq -m} a_n e^{2\pi i n z}$, for $\mathrm{Im}(z) > a$ for some $a > 0$.

From now on, we will use the usual notation $q = e^{2\pi i z}$. For example, the function

$$G_{2k}(\tau) = \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \frac{1}{\omega^{2k}},$$

defined by Eisenstein, is a $\Gamma(1)$-modular form of weight $2k$ and its Fourier expansion is

$$G_{2k}(\tau) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n \geq 1} \sigma_{2k-1}(n) q^n, \qquad \sigma_k(n) = \sum_{d|n} d^k.$$

The discriminant function

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

is a $\Gamma(1)$-modular form of weight 12 and its Fourier expansion is

$$\Delta(\tau) = (2\pi)^{12} \sum_{n \geq 1} \tau(n) q^n,$$

where $\tau(n) \in \mathbb{Z}$ is the Ramanujan function. Finally the function

$$J(\tau) = \frac{g_2(\tau)^3}{\Delta(\tau)}$$

is a $\Gamma(1)$-modular function and its Fourier expansion at infinity is

$$J(\tau) = \frac{1}{1728} \left(\frac{1}{q} + \sum_{n \geq 0} c(n) q^n \right),$$

where $c(n) \in \mathbb{Z}$.

5.4 Application to number theory and complex multiplication

There are several applications arising from the theory of elliptic functions to number theory. We will focus here on complex multiplication. Recall, that for an elliptic curve $E \simeq \mathbb{C}/\Lambda$, we identified $\mathrm{End}(E)$ with the set $\{\alpha \in \mathbb{C} | \alpha\Lambda \subseteq \Lambda\}$. The link with number theory is provided by the following theorem:

Theorem 5.4.1 *Let $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ be a lattice and $f : \mathbb{C} \to \mathbb{C}$ an elliptic function for Λ. For $\alpha \in \mathbb{C}$ the following are equivalent:*

1. *$f(\alpha z)$ is a rational function in $f(z)$;*
2. *$\alpha\Lambda \subseteq \Lambda$.*

We see from this last theorem that the elliptic function is not really relevant apart the fact that it is an elliptic function for the lattice Λ. The core is really the lattice or what amounts to the same, the elliptic curve $\mathbb{C}/\Lambda$. From now on, we shall work with elliptic curves instead of elliptic functions. Note that we always have $\mathrm{End}(E) \supseteq \mathbb{Z}$. In general, $\mathrm{End}(E) = \mathbb{Z}$, but note that if $\alpha\Lambda \subseteq \Lambda$ and $\alpha \notin \mathbb{Z}$ then, necessarily $\alpha \in \mathbb{C} - \mathbb{R}$. Indeed, suppose that $\alpha \in \mathbb{R} - \mathbb{Z}$, then $\alpha\omega_1 = a\omega_1 + b\omega_2$ for some $a, b \in \mathbb{Z}$. Since, ω_1 and ω_2 are $\mathbb{R}$-linearly independent, we have $b = \alpha - a = 0$ and hence $\alpha = a \in \mathbb{Z}$,

contradicting the hypothesis $\alpha \in \mathbb{R} - \mathbb{Z}$. This is why we are led to the following definition:

Definition 5.4.1 *An elliptic curve E such that* $\mathrm{End}(E) \supsetneq \mathbb{Z}$ *is called an elliptic curve with complex multiplication.*

The family $\mathrm{End}(E)$ is not just a set of complex numbers, but more precisely:

Theorem 5.4.2 *Let E be an elliptic curve with complex multiplication. Then the ring* $\mathrm{End}(E)$ *is an order in an imaginary quadratic field.*

We shall prove this theorem, but before that we recall the notion of orders in a number field.

5.4.1 Orders in number field

Definition 5.4.2 *Let K be a number field. An order in K is a subset $O \subseteq O_K$ such that*

- *O is a subring of O_K;*
- *O contains a $\mathbb{Q}$-basis of K.*

Theorem 5.4.3 *A subset $O \subseteq O_K$ is an order if and only if O is a subring of O_K and is a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.*

Note that if $O \neq O_K$ is a non-maximal order, then O is not integrally closed and therefore is not a Dedekind domain. In order to define a class group for an order, we have to introduce the concept of proper ideals. Remark that if $\mathfrak{a}$ is a fractional ideal of O (non-zero finitely generated O-module) then

$$O \subseteq \{\alpha \in K | \alpha \cdot \mathfrak{a} \subseteq \mathfrak{a}\},$$

but that the equality does not always happen.

Definition 5.4.3 *Let $\mathfrak{a}$ be a fractional ideal. The ideal $\mathfrak{a}$ is called a proper fractional ideal for the order O if we have the equality $O = \{\alpha \in K | \alpha \cdot \mathfrak{a} \subseteq \mathfrak{a}\}$.*

Is a fractional proper ideal invertible? The following theorem answer this question when K is a quadratic number field:

Theorem 5.4.4 *Let O be an order in a quadratic field K and let $\mathfrak{a}$ be any proper fractional ideal for O. Then $\mathfrak{a}$ is proper if and only if $\mathfrak{a}$ is invertible.*

Note also that given a lattice of rank 2 in K, say Λ, then Λ is a fractional ideal for some order. Indeed, define the order associated with Λ by

$$O_\Lambda = \{\alpha \in K | \alpha\Lambda \subseteq \Lambda\}.$$

Then O_Λ is an order in K and Λ is a proper fractional ideal for O_Λ.

We can now define the class group of an order in a quadratic number field.

Definition 5.4.4 *Let K be a quadratic field and O be an order in K. Let $I(O)$ be the group of fractional proper ideals of O (which is the set of invertible fractional ideal by the last theorem) and let*

$$P(O) = \{\mathfrak{a} \in I(O) | \mathfrak{a} = \lambda \cdot O \text{ for some } \lambda \in K\}.$$

Define then the class group of the order O by $\mathrm{Cl}(O) := I(O)/P(O)$.

Note that if $O = O_K$, then $\mathrm{Cl}(O)$ is the usual class group of K. We shall now define the ring class field associated to an order. For this, we have to relate $\mathrm{Cl}(O)$ with some $\mathrm{Cl}_{\mathfrak{m},H_\mathfrak{m}}(K)$. Note first that since O and O_K are both free $\mathbb{Z}$-module of the same rank, the quotient O_K/O is finite.

Definition 5.4.5 *Let O be an order in a quadratic field K. The conductor f of O is define by $f = [O_K : O]$.*

See [11] to see why one calls f the conductor.

Theorem 5.4.5 *Let K be a quadratic number field and O an order in K of conductor f. Set $\mathfrak{m}_0 = f \cdot O_K$ and*

$$H_{\mathfrak{m}_0} = \{\alpha \cdot O_K | \alpha \in K^\times_{\mathfrak{m}_0},\ \alpha \equiv a \mod {}^\times\mathfrak{m}_0 \text{ for some } a \in \mathbb{Z} \text{ s.t. } (a \cdot O_K, \mathfrak{m}_0) = 1\}.$$

The group $H_{\mathfrak{m}_0}$ is a congruence subgroup modulo $\mathfrak{m}_0$ and then

$$\mathrm{Cl}(O) \simeq I_{\mathfrak{m}_0}(K)/H_{\mathfrak{m}_0} = \mathrm{Cl}_{\mathfrak{m}_0,H_{\mathfrak{m}_0}}(K).$$

We can now define the ring class field of a quadratic number field:

Definition 5.4.6 *The ring class field of O is the abelian extension L corresponding to the congruence subgroup $H_{\mathfrak{m}_0}$ by class field theory. The Artin map gives us the isomorphism* $\mathrm{Gal}(L/K) \simeq I_{\mathfrak{m}_0}(K)/H_{\mathfrak{m}_0} \simeq \mathrm{Cl}(O)$.

Note that if $O = O_K$, then $\mathfrak{m}_0 = O_K$, $I_{\mathfrak{m}_0}(K) = I(K)$ and $H_{\mathfrak{m}_0} = P(K)$ so we get the usual class group and the ring class field is the Hilbert class field of K. We can now come back to the proof of Theorem 5.4.2.

Proof [Theorem 5.4.2]:

Let $E \simeq \mathbb{C}/\Lambda$ be an elliptic curve with complex multiplication and let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Let $\Omega = \{\alpha \in \mathbb{C} | \alpha \cdot \Lambda \subseteq \Lambda\}$. We show first that $\Omega \subset O_K$ for some quadratic imaginary field K. Let $\alpha \in \Omega$ and since E has complex multiplication, we can suppose that $\alpha \notin \mathbb{Z}$. We claim that α is quadratic imaginary. We have $\alpha\omega_1 = a\omega_1 + b\omega_2$, and $\alpha\omega_2 = c\omega_1 + d\omega_2$ for some $a, b, c, d \in \mathbb{Z}$. This means that $\det \left(\begin{smallmatrix} \alpha - a & -b \\ -c & \alpha - d \end{smallmatrix} \right) = 0$. Therefore, α is a root of a monic quadratic polynomial with coefficients in $\mathbb{Z}$ that is an integral number. Let $\tau = \omega_1/\omega_2 \in \mathfrak{h}$, then from the equation $\alpha\omega_2 = c\omega_1 + d\omega_2$, we see that $K = \mathbb{Q}(\tau) = \mathbb{Q}(\alpha)$ is a quadratic imaginary field. Doing this last argument for all multipliers $\alpha \in \Omega$ shows that $\Omega \subseteq O_K$. Moreover, Ω is clearly a ring. Let α be any complex multiplier in Ω. Then $\mathbb{Z} \oplus \mathbb{Z}\alpha$ is a free abelian group of rank 2 and the inclusions $\mathbb{Z} \oplus \mathbb{Z}\alpha \subseteq \Omega \subseteq O_K$ shows that Ω is a free $\mathbb{Z}$-module of rank 2. We conclude using Theorem 5.4.3.

□

In order to emphasize the ring of multipliers of an elliptic curve, an elliptic curve such that $\mathrm{End}(E)$ is an order O in some imaginary quadratic field will be called an elliptic curve with CM by O (CM stands for complex multiplication).

Theorem 5.4.6 *Let $K \subset \mathbb{C}$ be a quadratic imaginary field and let O be an order in K. There is a bijection between* $\mathrm{Cl}(O)$ *and the set of isomorphism classes of elliptic curves with CM by O.*

Proof:

Let $\mathrm{Isom}(O)$ denotes the set of all isomorphism classes of elliptic curves with complex multiplication by O. If E is such an elliptic curve, we shall denote its class by $[E]$. Define then the map

$$\mathrm{Cl}(O) \to \mathrm{Isom}(O)$$

by $[\mathfrak{a}] \to [\mathbb{C}/\mathfrak{a}]$. It is well-defined since the fact that $\mathfrak{a}$ is an O-ideal implies that $\mathbb{C}/\mathfrak{a}$ has complex multiplication by O and also for all $\lambda \in K$, $\mathbb{C}/\mathfrak{a} \simeq \mathbb{C}/(\lambda \cdot \mathfrak{a})$. Since there is an isomorphism $\mathbb{C}/\Lambda_1 \simeq \mathbb{C}/\Lambda_2$ if and only if $\lambda \cdot \Lambda_1 = \Lambda_2$ for some $\lambda \in \mathbb{C}$, this map is injective. It is also surjective since if $\mathbb{C}/\mathfrak{a}$ is an elliptic curve with CM by O then $\mathfrak{a}$ is a proper fractional ideal in O.

□

5.4.2 Main theorems of complex multiplication

First of all, note that if $\mathfrak{a}$ is a fractional ideal in an imaginary quadratic number field K, then $\mathfrak{a} = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ for some $\mathbb{R}$-linearly independent complex numbers ω_1, ω_2. Suppose moreover that $\tau = \omega_1/\omega_2 \in \mathfrak{h}$ (if it is not the case, just interchange ω_1 and ω_2). For any modular form h of weight k, we define $h(\mathfrak{a})$ by

$$h(\mathfrak{a}) := \omega_2^{-2k} h(\tau).$$

In particular, if h is an automorphic function (thus of weight 0), we have $h(\lambda \cdot \mathfrak{a}) = h(\mathfrak{a})$ for all $\lambda \in K$ so we can speak about $h(C)$ where C is any ideal class in K.

Theorem 5.4.7 (First Main Theorem) *Let K be an imaginary quadratic field, and O an order in K. Let $\mathrm{Cl}(O) = \{C_1, \ldots, C_t\}$ be its class group.*

- *The numbers $J(C_i)$ form a full set of distinct conjugate algebraic numbers.*
- *The ring class field of O is precisely $K(J(C_i))$ for any $i = 1, \ldots, t$.*

In particular, for the maximal order O_K, we get:

Theorem 5.4.8 *$K(J(C_i))$ is the Hilbert class field of K.*

Theorem 5.4.9 (Explicit reciprocity law) *Let K be an imaginary quadratic field and O_K its maximal order. Let $[\mathfrak{a}]$ be any ideal class in $\mathrm{Cl}(K)$. Then by the last theorem, we have that $K(J(\mathfrak{a}))$ is the Hilbert class field of K. We now describe explicitly the action of the Artin symbol on $J(\mathfrak{a})$; if $\mathfrak{p}$ is a prime of K, then we have*

$$J(\mathfrak{a})^{(\mathfrak{p},H_K/K)} = J(\mathfrak{p}^{-1}\mathfrak{a}).$$

Therefore, for any ideal $\mathfrak{b}$ of K, we have

$$J(\mathfrak{a})^{(\mathfrak{b},H_K/K)} = J(\mathfrak{b}^{-1}\mathfrak{a}).$$

Remark: In some books, one find instead the following reciprocity law

$$J(\mathfrak{a})^{(\mathfrak{b},H_K/K)} = J(\overline{\mathfrak{b}}\mathfrak{a}).$$

It is exactly the same thing since $\overline{\mathfrak{b}} \in [\mathfrak{b}^{-1}]$ and $J(\mathfrak{a})$ depends only on the ideal class $[\mathfrak{a}]$ of $\mathfrak{a}$. Indeed, in an imaginary quadratic field, the complex conjugation is a well-defined automorphism, and therefore it makes sense to talk about the ideal $\overline{\mathfrak{b}}$. In order to verify our claim, it suffices to verify that for every prime ideal $\mathfrak{p}$ of K, we have that $\mathfrak{p} \cdot \overline{\mathfrak{p}}$ is principal. So let $\mathfrak{p}$ be a prime ideal and let p be a prime below. There are three possibilities for the ramification, namely:

- $p \cdot O_K = \mathfrak{p}^2$ (ramified);
- $p \cdot O_K = \mathfrak{p}$ (inert);
- $p \cdot O_K = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ (split totally).

Then, since in a Galois extension the Galois group acts transitively on the primes lying above a fixed one, in the first case we necessarily have $\mathfrak{p} = \overline{\mathfrak{p}}$ and therefore $\mathfrak{p} \cdot \overline{\mathfrak{p}} = p \cdot O_K$. In the second case, we have then $\mathfrak{p} \cdot \overline{\mathfrak{p}} = p^2 \cdot O_K$ and in the last case, we have $\mathfrak{p} \cdot \overline{\mathfrak{p}} = p \cdot O_K$. Thus in each case, $\overline{\mathfrak{p}} \in [\mathfrak{p}^{-1}]$ and our claim is proved.

In the case of the rational field $\mathbb{Q}$, we have an explicit description of the ray class fields, see Theorem 3.2.11. Do we have such a description for a quadratic imaginary

field? This is the content of the second main theorem of complex multiplication. See for instance [5].

5.5 Integrality question

We shall now deal with integrality questions. In the classical theory this can be achieved through the modular equation.

When dealing with integrality questions, we work with

$$j = 1728 \cdot J = 2^6 3^3 \cdot J,$$

instead of J alone. Indeed, while $J(\tau)$ is an algebraic number for an imaginary quadratic number τ, it is not an algebraic integer. On the other side, $j(\tau)$ is integral for an imaginary quadratic number τ. The classical proof of this uses the modular equation.

Theorem 5.5.1 *If $\tau \in \mathfrak{h}$ is an imaginary quadratic number then $j(\tau)$ is an algebraic integer.*

Proof:

See [5] for the classical proof.

□

5.6 Elliptic units and a special case of Stark's conjecture

In this section, we will sketch a proof of the abelian rank one Stark conjecture when the base field is quadratic imaginary following [73].

First of all, we explain the utility of limit formulas such as the Kronecker limit formulas. This is useful when one wants to compute the value of a L-series at $s = 1$ (or at $s = 0$ by the functional equation). Let K be a number field and let $K_{\mathfrak{m}}$ be the ray class field modulo $\mathfrak{m}$. By class field theory, we then have an isomorphism $\mathrm{Cl}_{\mathfrak{m}}(K) \simeq \mathrm{Gal}(K_{\mathfrak{m}}/K)$. Let χ be a character of $\mathrm{Cl}_{\mathfrak{m}}(K)$ and consider the L-series

$$L(s, \chi) = \sum_{\mathfrak{a} \neq 0} \frac{\chi(\mathfrak{a})}{\mathbb{N}(\mathfrak{a})^s}.$$

We can rewrite this last series as follows:

$$L(s,\chi) = \sum_{C \in \mathrm{Cl}_{\mathfrak{m}}(K)} \chi(C)\zeta_K(s,C),$$

where $\zeta_K(s,C)$ is the partial zeta function:

$$\zeta_K(s,C) = \sum_{\mathfrak{a} \in C} \frac{1}{\mathbb{N}(\mathfrak{a})^s}.$$

Suppose then that we know the Laurent expansion of $\zeta_K(s,C)$ around $s=1$:

$$\zeta_K(s,C) = \frac{a_{-1}}{s-1} + a_0(C) + a_1(C)(s-1) + \ldots.$$

Note that a_{-1} does not depend on C. This is precisely Dedekind's discovery. On the other hand, the other coefficients could depend on C. Plugging this last equation into the L-series, we get

$$L(s,\chi) = \sum_C \chi(C) \left(\frac{a_{-1}}{s-1} + a_0(C) + a_1(C)(s-1) + \ldots \right).$$

Suppose $\chi \neq \chi_1$. Letting $s \to 1$ and using the orthogonality relation, we get

$$L(1,\chi) = \sum_C \chi(C) a_0(C),$$

thus we can compute the value of the L-series at $s=1$. In the literature, limit formulas are usually given around $s=1$, but then using the functional equation they can be translated into a formula for $L(0,\chi)$.

When the base field K is quadratic imaginary, such a formula is known since a long time and it is called Kronecker's limit formula. Before stating it, we define first the Siegel-Ramachandra invariant.

Let K be a quadratic imaginary number field and let $\mathfrak{m}_0 \neq O_K$ be an integral ideal of K. We shall denote the only infinite place of K by v_∞ (thus $S_\infty = \{v_\infty\}$).

Let $\zeta(z,\Lambda)$ and $\sigma(z,\Lambda)$ be the classical Weierstrass functions with respect to a lattice Λ. That is, ζ is defined by the equations

$$\frac{d\zeta(z)}{dz} = -\wp(z), \qquad \lim_{z\to 0}\left(\zeta(z) - \frac{1}{z}\right) = 0,$$

and σ by

$$\frac{d\log\sigma(z)}{dz} = \zeta(z), \qquad \lim_{z\to 0}\frac{\sigma(z)}{z} = 1.$$

The function $\zeta(z)$ is not doubly periodic, but it satisfies the following transformation rule $\zeta(z_1+z_2,\Lambda) = \zeta(z_1,\Lambda) + \eta(z_2,\Lambda)$, where η is some $\mathbb{R}$-linear function, see [81]. Define the function

$$G(z,\Lambda) = e^{-6z\eta(z,\Lambda)}\cdot\sigma^{12}(z,\Lambda)\cdot\Delta(\Lambda).$$

Note that this function is the same as the function given in [54] up to the constant i. Then, let f be the smallest positive integer in $\mathfrak{m}_0\bigcap\mathbb{Z}$. Consider the ray class group $\mathrm{Cl}_{\mathfrak{m}_0}(K)$ and for each ideal class $C\in\mathrm{Cl}_{\mathfrak{m}_0}(K)$, define the Siegel-Ramachandra invariant

$$g_{\mathfrak{m}_0}(C) = G(1,\mathfrak{m}_0\mathfrak{a}^{-1})^f,$$

where $\mathfrak{a}$ is an integral ideal in the ideal class C.

Theorem 5.6.1 *The Siegel–Ramachandra invariants have the following properties:*

1. $g_{\mathfrak{m}_0}(C)$ *is independent of the choice of* $\mathfrak{a}\in C$.
2. $g_{\mathfrak{m}_0}(C)\in K_{\mathfrak{m}_0}$.
3. *The explicit action of the Galois group* $\mathrm{Gal}(K_{\mathfrak{m}_0}/K)$ *is given by*

$$g_{\mathfrak{m}_0}(C) = g_{\mathfrak{m}_0}(1)^{(C,K_{\mathfrak{m}_0}/K)}.$$

4. *If* $\mathfrak{m}_0$ *has at least 2 different prime divisors, then* $g_{\mathfrak{m}_0}(C)$ *is a unit. Otherwise, if* $\mathfrak{m}_0$ *is the power of a unique prime ideal* $\mathfrak{p}$, *then* $g_{\mathfrak{m}_0}(C)$ *is a* $\{v_\infty,\mathfrak{p}\}$*-unit. Moreover,* $g_{\mathfrak{m}_0}(C)^{1-\sigma}$ *is a unit for all* $\sigma\in\mathrm{Gal}(K_{\mathfrak{m}_0}/K)$.
5. *The extension* $K(g_{\mathfrak{m}_0}(C)^{\frac{1}{12f}})$ *of* K *is abelian.*

Proof:

These facts are consequences of the theory of complex multiplication. See [15].

□

Now, we can state Kronecker's limit formula at $s = 0$.

Theorem 5.6.2 *Let K be a quadratic imaginary number field and let $\mathfrak{m}_0$ be an integral ideal of K. Consider the ray class group $\mathrm{Cl}_{\mathfrak{m}_0}(K)$ and let $C \in \mathrm{Cl}_{\mathfrak{m}_0}(K)$ be any ideal class. The derivative of $\zeta_K(s, C)$ at $s = 0$ is given by*

$$\zeta_K'(0, C) = -\frac{1}{12f\omega(\mathfrak{m}_0)} \log \left| g_{\mathfrak{m}_0}(1)^{(C, K_{\mathfrak{m}_0}/K)} \right|,$$

where $\omega(\mathfrak{m}_0)$ is the number of roots of unity λ in K satisfying $\lambda \equiv 1 \mod \mathfrak{m}_0$, and $|z| = z \cdot \overline{z}$ is the normalized valuation.

We are now in position to sketch the proof of Stark's conjectures. Let K be a quadratic imaginary field and let L/K be a finite abelian extension. Moreover, let S be a set of primes of K satisfying **S1**, **S2** and **S3** of Chapter 4. Note that v_∞ is a totally split place, thus we shall prove $\mathrm{St}(L/K, S, v_\infty)$. We can choose an integral ideal $\mathfrak{m}_0$ of K such that

- $\mathfrak{p} \mid \mathfrak{m}_0$ if and only if $\mathfrak{p} \in S \setminus \{v_\infty\}$;
- $\omega(\mathfrak{m}_0) = 1$;
- $L \subseteq K_{\mathfrak{m}_0}$.

Indeed, it suffices to take $\mathfrak{m}_0 = \left(\prod_{\mathfrak{p} \in S \setminus \{v_\infty\}} \mathfrak{p}\right)^n$ for n big enough. The set S still satisfies conditions **S1**, **S2**, and **S3** for $K_{\mathfrak{m}_0}$. By Theorem 4.0.7, it suffices to prove $\mathrm{St}(K_{\mathfrak{m}_0}/K, S, v_\infty)$ in order to prove $\mathrm{St}(L/K, S, v_\infty)$. First, we need a lemma which can be found in [73].

Lemma 5.6.1 *With the notation above, there exists a unit $\varepsilon \in U^{ab}_{K_{\mathfrak{m}_0}/K}$ such that*

$$\varepsilon^{12f} = g_{\mathfrak{m}_0}(1)^{\omega_{K_{\mathfrak{m}_0}}} \cdot \zeta,$$

with $\zeta^{\omega_{K_{\mathfrak{m}_0}}} = 1$.

Fix a place w of $K_{\mathfrak{m}_0}$ lying above v_∞. From Kronecker's limit formula, we see that

$$\zeta'_K(0,C) = -\frac{1}{\omega_{K_{\mathfrak{m}_0}}} \log \left|\varepsilon^{(C,K_{\mathfrak{m}_0}/K)}\right|_w .$$

Moreover, from Property (4) of Theorem 5.6.1, we see that if $|S| \geq 3$, then $|\varepsilon|_{w'} = 1$ for all $w' \nmid v_\infty$, and if $S = \{v_\infty, v_\mathfrak{p}\}$, then $|\varepsilon|_{\sigma w'} = |\varepsilon|_{w'}$ for all $\sigma \in \mathrm{Gal}(K_{\mathfrak{m}_0}/K)$ and some w' lying above $v_\mathfrak{p}$.

We conclude that there exists $\varepsilon \in U^{ab}_{K_{\mathfrak{m}_0}/K} \bigcap U^{v_\infty}$ such that

$$\begin{aligned} L'_S(0,\chi,K_{\mathfrak{m}_0}/K) &= \sum_{C\in \mathrm{Cl}_{\mathfrak{m}_0}(K)} \chi(C)\zeta'_K(0,C) \\ &= -\frac{1}{\omega_{K_{\mathfrak{m}0}}} \sum_{C\in \mathrm{Cl}_{\mathfrak{m}_0}(K)} \chi(C) \log \left|\varepsilon^{(C,K_{\mathfrak{m}_0}/K)}\right|_w \\ &= -\frac{1}{\omega_{K_{\mathfrak{m}_0}}} \sum_{\sigma\in G} \chi(\sigma) \log |\varepsilon^\sigma|_w, \end{aligned}$$

and $\mathrm{St}(K_{\mathfrak{m}_0}/K, S, v_\infty)$ is true. Thus $\mathrm{St}(L/K, S, v_\infty)$ is true when K is an imaginary quadratic number field.

Siegel also constructed elliptic units in unramified abelian extensions of K in order to give a class number formula relating the class number of K and the one of its Hilbert class field. He constructed them using quotients of the Δ function, see [41]. This is the construction that DeShalit–Goren attempt to generalize in [14].

CHAPTER 6
Higher dimensional theory

For the theory of abelian varieties, we used [72], [28] and [4], and for the theory of complex multiplication of abelian varieties, we used [40] and [62].

6.1 Introduction

We shall explain now the background materials that one needs to construct class invariants. If we look at the construction of elliptic units, we notice that there are three main ingredients:

- Elliptic curves over $\mathbb{C}$;
- Modular forms;
- Complex multiplication of elliptic curves.

In order to construct a generalization of elliptic units, we have to explain one possible generalization of these three concepts, namely:

- Abelian varieties over $\mathbb{C}$;
- Siegel modular forms;
- Complex multiplication of abelian varieties.

We shall first explain these concepts and then explain the construction of DeShalit–Goren.

6.2 Abelian functions and abelian varieties

Once again, we have three different perspectives on the subject:

- Abelian functions (analysis);
- Function fields (algebra);
- Abelian varieties (algebraic geometry).

The analogues in the one dimensional case were the elliptic functions, the function field $\mathbb{C}(\wp(z), \wp'(z))$ and the elliptic curve. The concept tying up all these different

points of view was the topological surface $\mathbb{C}/\Lambda$. It will be the same in the higher dimensional case, but here there will be one fundamental difference: $\mathbb{C}^n/\Lambda$ is not always an algebraic variety. We explain this now.

As in the case of elliptic curves, the concept of abelian functions arose in connection with the computation of some particular integrals. An integral of the type

$$\int R(x,y)\,dx,$$

where R is a rational function in x and y, $y = \sqrt{P(x)}$, and $P(x)$ is a polynomial of degree > 4, is called an abelian integral (because Abel studied them extensively). When one allows complex variables, then the same problem as with an elliptic integral happens, namely one cannot give a precise definition of the square root of a complex function. Mathematicians tried to invert these integrals, but then they got complex-valued functions with more than two periods. It was known at the time that a complex-valued function of one variable cannot have more than two $\mathbb{R}$-linearly independent periods. It became clear that one should work with functions of several complex variables.

Let $f : \mathbb{C}^n \to \mathbb{C}$ be a meromorphic function of several complex variables. A n-tuple $\omega = (p_1, p_2, \ldots, p_n) \in \mathbb{C}^n$ is a period for f if $f(z+\omega) = f(z)$, for all $z \in \mathbb{C}^n$. The set of periods of a meromorphic function forms an additive abelian group in $\mathbb{C}^n$. Recall that a lattice (sometimes called a full lattice) in $\mathbb{C}^n$ is a discrete free $\mathbb{Z}$-module of rank $2n$. We shall restrict ourselves to meromorphic functions such that their group of periods, say Λ, is a lattice. In that case, there exist $2n$ $\mathbb{R}$-linearly independent periods $\omega_1, \ldots, \omega_{2n} \in \mathbb{C}^n$ such that $\Lambda = \oplus_{i=1}^{2n} \mathbb{Z}\omega_i$.

Definition 6.2.1 *Let $f : \mathbb{C}^n \to \mathbb{C}$ be a meromorphic function. Let Λ be its set of periods. We call f an abelian function for Λ if Λ is a lattice in $\mathbb{C}^n$. If $\Lambda = \oplus_{i=1}^{2n} \mathbb{Z}\omega_i$, the matrix*

$$P = (\omega_1^t, \ldots, \omega_{2n}^t) \in M_{n\times 2n}(\mathbb{C})$$

is called a period matrix for f (or for Λ).

One can consider the complex manifold $\mathbb{C}^n/\Lambda$ and then, as in the one dimensional case, the field of meromorphic functions on $\mathbb{C}^n/\Lambda$ is identified with the set of abelian functions for the lattice Λ.

Here is an example of an abelian function. Let (ω_1, ω_2) be two $\mathbb{R}$-linearly independent complex numbers and set $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$. Recall that the Weierstrass' function for Λ is $\wp(z, \Lambda) = \frac{1}{z^2} + \sum_{\substack{\omega \in \Lambda \\ \omega \neq 0}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$. Let us define the $2n$ vectors $p_1 = (\omega_1, 0, \ldots, 0)$, $p_2 = (\omega_2, 0, \ldots, 0), \ldots, p_{2n-1} = (0, \ldots, 0, \omega_1)$, $p_{2n} = (0, \ldots, 0, \omega_2)$, and let $f(z) = \wp(z_1) \cdot \wp(z_2) \cdot \ldots \wp(z_{n-1}) \cdot \wp(z_n)$. Then f is an abelian function for the period-matrix

$$P = \begin{pmatrix} \omega_1 & \omega_2 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & \omega_1 & \omega_2 \end{pmatrix} \in M_{n \times 2n}(\mathbb{C}).$$

6.2.1 Abelian varieties

The analogue of elliptic curves in higher dimensional algebraic geometry are the abelian varieties.

Definition 6.2.2 *Let k be an algebraic closed field. An abelian variety over k is a non-singular projective (connected) variety A, which is also a group and such that the group law*

$$+ : A \times A \to A,$$

and the inverse map

$$- : A \to A,$$

are morphisms of algebraic varieties.

Remark: It is known that the group law is necessarily commutative and this is why we use the additive symbol $+$ for the group law. If A is defined over the complex

numbers $\mathbb{C}$, then it becomes a complex Lie group and it is also known that in this case $A \simeq \mathbb{C}^n/\Lambda$ is a complex torus for some lattice Λ.

We are led to the following question. Given a lattice $\Lambda = \oplus_{i=1}^{2n} \mathbb{Z}\omega_i$, we can ask whether or not $\mathbb{C}^n/\Lambda$ is an algebraic variety. The answer is contained in the next theorem.

Theorem 6.2.1 *Let Λ be a lattice in $\mathbb{C}^n$, then the following are equivalent:*

1. *$\mathbb{C}^n/\Lambda$ is an algebraic variety.*
2. *$\mathbb{C}^n$ admits a positive definite Hermitian form $H = S+iE$ such that $E = \mathrm{Im}(H)$ is integer-valued on Λ (such an H is called a Riemann form).*

Remarks: Point (1) means that there exists a projective embbeding. For the point (2), we recall here the definition of a Hermitian form.

Definition 6.2.3 *A Hermitian form on $\mathbb{C}^n$ is a map $H : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{C}$ such that*

- *The map $z \mapsto H(z,w)$ is $\mathbb{C}$-linear in z for all $w \in \mathbb{C}^n$;*
- *The map $w \mapsto H(z,w)$ is anti-linear in w for all $z \in \mathbb{C}^n$ (i.e. additive and $H(z,\lambda w) = \bar{\lambda} \cdot H(z,w)$);*
- *$H(z,w) = \overline{H(w,z)}$.*

Moreover, H is said to be positive if $H(z,z) \geq 0$ and positive definite if H is positive and satisfies also $H(z,z) = 0$ if and only if $z = 0$.

Sometimes, it is preferable to work only with the imaginary part of a Hermitian form.

Theorem 6.2.2 *A Hermitian form H can be written $H(z,w) = S(z,w) + iE(z,w)$. We have the following properties:*

- *$S, E : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{R}$ are $\mathbb{R}$-bilinear, where $\mathbb{C}^n$ is considered as a $\mathbb{R}$-vector space;*
- *S is symmetric;*
- *E is alternating ($E(z,w) = -E(w,z)$);*
- *$S(z,w) = E(iz,w)$;*
- *$E(iz,iw) = E(z,w)$;*
- *If H is positive, then $H(z,z) = S(z,z) = E(iz,z) \geq 0$ for all $z \in \mathbb{C}^n$;*

- *If H is positive definite, the last condition is satisfied and moreover $E(iz, z) = 0 \Leftrightarrow z = 0$;*
- *If H is a Riemann form for some lattice Λ, then $E(z, w) \in \mathbb{Z}$ for all $z, w \in \Lambda$.*

We have a converse of this theorem, namely:

Theorem 6.2.3 *Consider $\mathbb{C}^n$ as a $\mathbb{R}$-vector space. Suppose we are given a lattice Λ of $\mathbb{C}^n$ and an $\mathbb{R}$-alternating form $E : \mathbb{C}^n \times \mathbb{C}^n \to \mathbb{R}$ satisfying:*

- *$E(iz, iw) = E(z, w)$ for all $z, w \in \mathbb{C}^n$;*
- *$E(iz, z) \geq 0$ for all $z \in \mathbb{C}^n$;*
- *$E(iz, z) = 0 \Leftrightarrow z = 0$ for all $z \in \mathbb{C}^n$;*
- *$E(z, w) \in \mathbb{Z}$ for all $z, w \in \Lambda$.*

Then $H(z, w) = E(iz, w) + iE(z, w)$ is a Riemann form for $\mathbb{C}^n/\Lambda$.

In the sequel, we shall work mainly with the imaginary part of a Riemann form and we also call such an E a Riemann form.

Definition 6.2.4 *An abelian manifold is a complex torus with a Riemann form.*

Thus, according to Theorem 6.2.1, every abelian manifold is an abelian variety and vice-versa.

Scholie: When $n = 1$, we get back the theory of elliptic functions and elliptic curves. Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. The Weierstrass' function gives us an explicit projective embedding of $\mathbb{C}/\Lambda$ into $\mathbb{P}^2(\mathbb{C})$ by Theorem 5.2.8. Therefore, according to Theorem 6.2.1, there should be a hidden Riemann form somewhere. It is actually true for every lattice and this is why we did not meet it previously.

Theorem 6.2.4 *Let $\Lambda = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ be a lattice in $\mathbb{C}$. Then $\mathbb{C} = \mathbb{R}\omega_1 \oplus \mathbb{R}\omega_2$. If the numbers z, $w \in \mathbb{C}$, then $\binom{z}{w} = \left(\begin{smallmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{smallmatrix}\right)\binom{\omega_1}{\omega_2}$ for some $\alpha_i, \beta_i \in \mathbb{R}$. Define the pairing $E(z, w) = \det \left(\begin{smallmatrix} \alpha_1 & \alpha_2 \\ \beta_1 & \beta_2 \end{smallmatrix}\right) = \alpha_1 \cdot \beta_2 - \beta_1 \cdot \alpha_2$. Then E is a Riemann form on $\mathbb{C}/\Lambda$.*

Weil introduced the concept of polarization in analogy with the concept of orientability in differential geometry. Over $\mathbb{C}$, it can be defined as follows:

Definition 6.2.5 *Let $\mathbb{C}^n/\Lambda$ be an abelian manifold and let E, E' be two Riemann forms on $\mathbb{C}^n/\Lambda$. We define an equivalence relation $\sim$ by*

$$E \sim E' \Leftrightarrow \text{ there exists } \lambda \in \mathbb{C} \text{ such that } E = \lambda \cdot E'.$$

Note that λ is necessarily a positive rational number since E, E' are integer valued on Λ and $E(iz, z) \geq 0$.

Definition 6.2.6 *Let $\mathbb{C}^n/\Lambda$ be an abelian manifold. A polarization on $\mathbb{C}^n/\Lambda$ is an equivalence class of Riemann forms.*

A class of polarizations which is particularly important is the class of principal ones. Here is the explication of this concept.

Definition 6.2.7 *Let $\mathbb{C}^n/\Lambda$ be an abelian manifold, and E an associated Riemann form. According to the elementary divisor theorem, there exists a basis of the lattice Λ, say $(\varepsilon_1, \ldots, \varepsilon_n, \zeta_1, \ldots, \zeta_n)$, such that the matrix of E is given by*

$$(E(\varepsilon_i, \zeta_j)) = \begin{pmatrix} 0 & -D \\ D & 0 \end{pmatrix},$$

where $D = \mathrm{Diag}(d_1, \ldots, d_n)$ is a diagonal matrix with integers $d_i > 0$, $(i = 1, \ldots, n)$ satisfying $d_i | d_{i+1}$, $(i = 1, \ldots, n-1)$. Moreover, the numbers $d_1, \ldots, d_n$ are uniquely determined by E and Λ. The vector $(d_1, \ldots, d_n)$ is called the type of E and the basis $(\varepsilon_1, \ldots, \varepsilon_n, \zeta_1, \ldots, \zeta_n)$ is called a symplectic basis for Λ.

Definition 6.2.8 *Let $\mathbb{C}^n/\Lambda$ be an abelian manifold with a polarization P. The polarization is said to be principal if there exists an $E \in P$ such that E is of type $(1, \ldots, 1)$.*

Let us come back to an abelian variety A.

Definition 6.2.9 *Let A_1 and A_2 be two abelian varieties. A homomorphism of abelian varieties is an algebraic morphism*

$$\phi : A_1 \to A_2$$

which is also a group homomorphism. The set of homomorphisms between two abelian varieties is denoted by $\mathrm{Hom}(A_1, A_2)$. *An homomorphism* $\phi : A_1 \to A_2$ *is called an isomorphism if there exists a homomorphism of abelian varieties* $\psi : A_2 \to A_1$ *such that* $\phi \circ \psi = id_{A_2}$ *and* $\psi \circ \phi = id_{A_1}$. *When* $A_1 = A_2$, *we call such a homomorphism (resp. isomorphism) an endomorphism (resp. automorphism) and denote the ring of endomorphisms of an abelian variety* A *by* $\mathrm{End}(A)$ *(resp.* $\mathrm{Aut}(A)$*).*

If A_i are abelian varieties over $\mathbb{C}$, then there exist lattices Λ_i such that $A_i \simeq \mathbb{C}^{n_i}/\Lambda_i$, for $i = 1, 2$. Let $\phi \in \mathrm{Hom}(A_1, A_2)$, then ϕ is given by rational functions and thus induces a holomorphic map

$$\bar{\phi} : \mathbb{C}^{n_1}/\Lambda_1 \to \mathbb{C}^{n_2}/\Lambda_2,$$

such that $\bar{\phi}(0) = 0$. As in the case of elliptic curves, this correspondence is actually a bijection.

Theorem 6.2.5 *Let* $A_i \simeq \mathbb{C}^{n_i}/\Lambda_i$ *be abelian varieties defined over* $\mathbb{C}$, *(*$i = 1, 2$*). Then the correspondence* $\phi \mapsto \bar{\phi}$ *makes the following diagram commutative*

$$\begin{array}{ccc} A_1 & \xrightarrow{\simeq} & \mathbb{C}^{n_1}/\Lambda_1 \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\bar{\phi}} \\ A_2 & \xrightarrow{\simeq} & \mathbb{C}^{n_2}/\Lambda_2 \end{array},$$

and this correspondence is a bijection between $\mathrm{Hom}(A_1, A_2)$ *and the set of holomorphic maps* $\phi : \mathbb{C}^{n_1}/\Lambda_1 \to \mathbb{C}^{n_2}/\Lambda_2$ *such that* $\phi(0) = 0$.

Theorem 6.2.6 *Let* $A_i \simeq \mathbb{C}^{n_i}/\Lambda_i$ *be abelian varieties defined over* $\mathbb{C}$, *for* $i = 1, 2$. *Let* $\phi : \mathbb{C}^{n_1}/\Lambda_1 \to \mathbb{C}^{n_2}/\Lambda_2$ *be a holomorphic map such that* $\phi(0) = 0$, *then there exists a* $\mathbb{C}$*-linear map* $L_\phi : \mathbb{C}^{n_1} \to \mathbb{C}^{n_2}$ *such that* $L_\phi(\Lambda_1) \subseteq \Lambda_2$ *and such that the following diagram is commutative*

$$\begin{array}{ccc} \mathbb{C}^{n_1} & \xrightarrow{L_\phi} & \mathbb{C}^{n_2} \\ \downarrow & & \downarrow \\ \mathbb{C}^{n_1}/\Lambda_1 & \xrightarrow{\phi} & \mathbb{C}^{n_2}/\Lambda_2 \end{array}.$$

This correspondence sets a bijection between

$$\{\mathbb{C}\text{-}\textit{linear maps } L : \mathbb{C}^{n_1} \to \mathbb{C}^{n_2} \textit{ such that } L(\Lambda_1) \subseteq \Lambda_2\},$$

and

$$\{\textit{holomorphic maps } \phi : \mathbb{C}^{n_1}/\Lambda_1 \to \mathbb{C}^{n_2}/\Lambda_2 \textit{ such that } \phi(0) = 0\}.$$

Moreover, $\mathrm{End}(A)$ depends only on the isomorphism class of A.

If E is an elliptic curve, note that the extension of scalars $\mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbb{Q}$ is a $\mathbb{Q}$-algebra and that we have $\mathrm{End}(E) \otimes_{\mathbf{Z}} \mathbb{Q} \simeq \mathbb{Q}$ or K, where K is a quadratic imaginary field (the latter case being the CM-case). This provided the link with number theory. Similarly, we shall study the structure of $\mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbb{Q}$ for an arbitrary abelian manifold A in the section on complex multiplication of abelian varieties.

6.3 Siegel modular functions

In this section, we proceed to generalize the theory of classical modular forms. We mainly use the reference [18] (german). The new mathematical object is called a Siegel modular form. Siegel discovered these functions while he was working on the theory of quadratic forms. For a general overview, recall that a domain of $\mathbb{C}^n$ is called homogeneous if the group of biholomorphic automorphisms acts transitively on it. Moreover, it is called symmetric if for each point of the domain there exists an involution in the group having only this point as a fixed point. Élie Cartan (1869-1951) proved that every bounded symmetric domain is automatically homogeneous, and he classified them. He found four main types plus two exceptional ones which appear only for dimension 16 and 27. We shall not explain his results, see [63] for instance. One is relevant for us, namely the generalization of the unit circle. First, we introduce the Siegel space that generalizes the Poincaré upper half-plane.

Definition 6.3.1 *The Siegel space $\mathfrak{h}_n$ is the set of all complex symmetric matrices (n-rowed) such that the imaginary part is positive definite:*

$$\mathfrak{h}_n = \{Z = X + iY \in M_n(\mathbb{C}) | Z^t = Z \ , \ Y > 0\}.$$

Note that $\mathfrak{h}_1$ is merely the upper half-plane. In the classical case, the group of biholomorphic automorphisms acts on $\mathfrak{h}_1$, but also on the Riemann sphere, and we have the inclusions $\mathfrak{h}_1 \subseteq \mathbb{C} \subseteq \overline{\mathbb{C}}$, where the Riemann sphere is a compact Riemann surface. We have a similar thing for $\mathfrak{h}_n$. Define first

$$P_n = \{Z \in M_n(\mathbb{C}) | Z^t = Z\}.$$

Clearly, $\mathfrak{h}_n$ embeds in P_n. Next, define C_n to be the set of $W = \binom{W_1}{W_2} \in M_{2n \times n}(\mathbb{C})$, where $W_i \in M_n(\mathbb{C})$ satisfy both $\text{rank}(W) = n$, and $W_1^t \cdot W_2 = W_2^t \cdot W_1$. Note that when $\det(W_2) \neq 0$, the last condition is equivalent to $W_1 W_2^{-1}$ being symmetric. The group $\text{GL}_n(\mathbb{C})$ acts on C_n by right multiplication, namely $W \cdot U = \binom{W_1 U}{W_2 U}$, whenever $U \in \text{GL}_n(\mathbb{C})$. The analogue of the Riemann sphere is $S_n := C_n / \text{GL}_n(\mathbb{C})$, the space of orbits of this action. We also have an embedding of P_n into S_n defined by $Z \mapsto \binom{Z}{I_n} \cdot \text{GL}_n(\mathbb{C})$. This map is clearly injective, and after having identified P_n with its image, we have the inclusions $\mathfrak{h}_n \subseteq P_n \subseteq S_n$. When $n = 1$, then $P_1 \simeq \mathbb{C}$ and $S_1 \simeq \mathbb{P}^1(\mathbb{C}) \simeq \overline{\mathbb{C}}$. One can show that S_n is a compact complex manifold.

We shall see next that we also have an action of a group of biholomorphic automorphisms of $\mathfrak{h}_n$. First, we identify $\mathfrak{h}_n$ with a domain of $\mathbb{C}^{\frac{n(n+1)}{2}}$. This identification is made through the map

$$Z = (z_{ij}) \in P_n \mapsto (z_{11}, z_{12}, \ldots, z_{1n}, z_{21}, \ldots, z_{2n}, \ldots, z_{nn}) \in \mathbb{C}^{\frac{n(n+1)}{2}}.$$

The group we are interested in is $\text{Sp}_n(\mathbb{R})$ which is defined as follows. From now on, J stands for the matrix $J = \left(\begin{smallmatrix} 0 & I_n \\ -I_n & 0 \end{smallmatrix}\right)$. We can now define $\text{Sp}_n(\mathbb{R})$.

Definition 6.3.2 *The symplectic group is defined as follows*

$$\mathrm{Sp}_n(\mathbb{R}) := \{M \in \mathrm{GL}_{2n}(\mathbb{C}) | M^t J M = J\}.$$

Note that $M^t J M = J$ if and only if $M^t J^t M = J^t$. This latter group acts on C_n by multiplication on the left. Indeed, if $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, where $A, B, C, D \in M_n(\mathbb{R})$ then the action is defined by $M \cdot \left(\begin{smallmatrix} W_1 \\ W_2 \end{smallmatrix}\right) := \left(\begin{smallmatrix} AW_1+BW_2 \\ CW_1+DW_2 \end{smallmatrix}\right)$. This action induces an action on each of the three spaces $\mathfrak{h}_n$, P_n and S_n. Using the fact that if $Z \in \mathfrak{h}_n$, then $\det(CZ+D) \neq 0$ we see that the action on $\mathfrak{h}_n$ is given by

$$Z \in \mathfrak{h}_n \mapsto M \cdot Z := (AZ+B)(CZ+D)^{-1}.$$

In summary, we have

Theorem 6.3.1 *The group* $\mathrm{Sp}_n(\mathbb{R})$ *acts on* $\mathfrak{h}_n$ *by* $M \cdot Z := (AZ+B)(CZ+D)^{-1}$, *whenever* $Z \in \mathfrak{h}_n$, *and* $M \in \mathrm{Sp}_n(\mathbb{R})$.

The action of $\mathrm{Sp}_n(\mathbb{Z})$ is discontinuous and we can talk about its fundamental region. The closure of it is contained in the next theorem.

Theorem 6.3.2 *Let* n *be any positive integer. The Siegel's fundamental domain is the subset* F_n *of* $\mathfrak{h}_n$ *of* $Z = X + iY$ *such that*

1. $|\det(CZ+D)| \geq 1$, *for all* $M \in \mathrm{Sp}_n(\mathbb{Z})$;
2. $Y \in R_n$, *where* R_n *is the Minkowski's reduced domain (see below);*
3. $|x_{ij}| \leq 1/2$, *for* $i \leq j$, *where* $X = (x_{ij})$.

The Minkowski's reduced domain in the theorem is the set of $Y = (y_{ij}) \in M_n(\mathbb{R})$ satisfying

1. $g^t Y g \geq y_{ii}$, for all g integral with $(g_i, \ldots, g_n) = 1$, $(1 \leq i \leq n)$;
2. $y_{i,i+1} \geq 0$, $(1 \leq i \leq n-1)$.

Note that when $n = 1$ we get the closure of the fundamental region of $\mathrm{SL}_2(\mathbb{Z})$ acting on the Poincaré upper half-plane, see Section 5.3.1.

The domain $\mathfrak{h}_n$ is biholomorphically equivalent to the generalized unit circle which is one the four main bounded symmetric domain of Cartan.

Definition 6.3.3 *The unit circle of degree n is defined as*

$$D_n := \{Z \in M_n(\mathbb{C}) | Z^t = Z \ , \ I_n - Z\overline{Z} > 0\}.$$

Theorem 6.3.3 *The generalized Cayley transformation* $\mathfrak{h}_n \to D_n$ *defined by*

$$Z \mapsto (Z - iI_n)(Z + iI_n)^{-1}$$

is a biholomorphic map.

Using this fact, it is often more expedient to prove some facts about the action of $\mathrm{Sp}_n(\mathbb{R})$ on $\mathfrak{h}_n$. See [26]. Let us come back to the action of $\mathrm{Sp}_n(\mathbb{R})$ on $\mathfrak{h}_n$.

Theorem 6.3.4 *We have an isomorphism* $\mathrm{Bihol}(\mathfrak{h}_n) \simeq \mathrm{Sp}_n(\mathbb{R})/\{\pm I_{2n}\}$.

Next, as in the classical case, we are interested in discrete subgroups of $\mathrm{Sp}_n(\mathbb{R})$. In particular, $\mathrm{Sp}_n(\mathbb{Z})$ is such a discrete subgroup and it acts discontinuously on $\mathfrak{h}_n$.

Theorem 6.3.5 *The matrix* $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, *where* $A, B, C, D \in \mathrm{M}_n(\mathbb{Z})$, *is in* $\mathrm{Sp}_n(\mathbb{Z})$ *if and only if we have we have the following equalities:* $A^tD - C^tB = I_n$, $A^tC = C^tA$ *and* $B^tD = D^tB$.

From this last theorem we see that when $n = 1$, $\mathrm{Sp}_1(\mathbb{Z}) = \mathrm{SL}_2(\mathbb{Z})$. In general, we have the inclusion $\mathrm{Sp}_n(\mathbb{Z}) \subseteq \mathrm{SL}_{2n}(\mathbb{Z})$, but for $n \geq 2$, this is not an equality. This inclusion is a consequence of the next theorem.

Theorem 6.3.6 *The group* $\mathrm{Sp}_n(\mathbb{Z})$ *is generated by the element* J *and the matrices* $\left(\begin{smallmatrix} I_n & S \\ 0 & I_n \end{smallmatrix}\right)$, *where* $S = S^t$.

We see that the analogy with the classical case is really strong. We can now define what a Siegel modular form is.

Definition 6.3.4 *A function* $f : \mathfrak{h}_n \to \mathbb{C}$ *is called a Siegel modular form of weight k and level* 1 *if the following conditions are satisfied:*

- f *is holomorphic,*

- $f(M \cdot Z) = \det(CZ + D)^k f(Z)$ *for all* $Z \in \mathrm{Sp}_n(\mathbb{Z})$,
- *In every region* $Y \geq Y_0$, $(Y_0 > 0)$, f *is bounded.*

Note that for $n > 1$, it is known that the last condition is not necessary. This is the Koecher principle.

It is also true that every Siegel modular form has a Fourier expansion of the form

$$f(Z) = \sum_{T \geq 0} a(T) e^{2\pi i \mathrm{Tr}(TZ)},$$

where T runs over all half-integral positive symmetric matrices of degree n. Recall that half-integral means that t_{ii} and $2t_{ij}$, $(i \neq j)$, are integers.

6.4 Complex multiplication of abelian varieties

6.4.1 Structure of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$

We study here the structure of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and see how number theory comes into the picture. We follow mainly [4]. Some information can also be found in [40],[60] and [62]. For the general theory of associative algebras, see [50].

Start with an abelian variety $A \simeq \mathbb{C}^n/\Lambda$ defined over $\mathbb{C}$. According to Theorems 6.2.5 and 6.2.6, we have a faithful (that is, injective) complex representation

$$\rho_a : \mathrm{End}(A) \hookrightarrow \mathrm{End}_{\mathbb{C}}(\mathbb{C}^n),$$

defined by $\phi \mapsto L_{\bar{\phi}}$ (with the notation of Theorems 6.2.5 and 6.2.6), which is called the analytic representation (hence the subscript a). It can be viewed as the induced action on the tangent space. Now, if we restrict $L_{\bar{\phi}}$ to Λ we get a faithful rational representation

$$\rho_r : \mathrm{End}(A) \hookrightarrow \mathrm{End}_{\mathbb{Z}}(\Lambda),$$

which is called the rational representation. Since the representation is faithful, we can identify $\mathrm{End}(A)$ with a subring of $\mathrm{End}_{\mathbb{Z}}(\Lambda) \simeq M_{2n}(\mathbb{Z}) \simeq \mathbb{Z}^{4n^2}$, and we get:

Theorem 6.4.1 *Let A be an abelian variety. Then* $\mathrm{End}(A)$ *is a free* $\mathbb{Z}$*-module of finite rank. Therefore,* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a finite dimensional* $\mathbb{Q}$*-algebra.*

We conclude that there are embeddings

$$\rho_a : \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \hookrightarrow M_n(\mathbb{C}), \qquad \rho_r : \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \hookrightarrow M_{2n}(\mathbb{Q}).$$

We shall now see that the $\mathbb{Q}$-algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ has an anti-involution. Recall first the definition of an involution and an anti-involution of an algebra:

Definition 6.4.1 *Let A be a R-algebra (here R stands for a commutative ring with unity).*

- *An involution on A is an automorphism of R-algebras $\rho : A \to A$, such that $\rho(\rho(a)) = a$ for all $a \in A$.*
- *An anti-involution on A is a automorphism of R-module $\rho : A \to A$, such that*
  - *$\rho(a_1 \cdot a_2) = \rho(a_2) \cdot \rho(a_1)$ for all $a_1, a_2 \in A$;*
  - *$\rho(\rho(a)) = a$, for all $a \in A$.*

Note that since we extended the representation ρ_a to a representation of $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, it makes sense to talk about $\phi \cdot z$, where $\phi \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and $z \in \mathbb{C}^n$. Explicitly, we have $\phi \cdot z := \rho_a(\phi)(z)$.

Theorem 6.4.2 (Rosati involution) *Let $A \simeq \mathbb{C}^n/\Lambda$ be an abelian variety and let E be an associated Riemann form. The adjoint of E defines an anti-involution R on* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$*, called the Rosati involution. That is, for every $\phi \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, there exists a unique $R(\phi) \in \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that*

$$E(\phi \cdot z, w) = E(z, R(\phi) \cdot w),$$

for all $z, w \in \mathbb{C}^n$ and the association $\phi \mapsto R(\phi)$ defines an anti-involution on the $\mathbb{Q}$-algebra $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

It is clear that the Rosati involution does not depend on the representative of a polarization.

The rational representation gives us a trace function $T_r := \mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbb{Q} \to \mathbb{Q}$ defined by $T_r(\phi) = \mathrm{Tr}(\rho_r(\phi))$, where Tr is the usual trace of a linear transformation. We can define a bilinear symmetric form, which we call also T_r, on $\mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbb{Q}$ by setting $T_r(\phi_1, \phi_2) := \mathrm{Tr}_r(\phi_1 \cdot R(\phi_2))$.

Definition 6.4.2 *Let A be a $\mathbb{Q}$-algebra with a linear form $T : A \to \mathbb{Q}$. Suppose also that A has an anti-involution ρ. Then ρ is said to be positive (respectively positive definite) if the associated bilinear form $T(a_1 \cdot \rho(a_2))$ is positive (respectively positive definite).*

Theorem 6.4.3 *The Rosati involution is positive definite with respect to the rational trace.*

Up to now, we know that $\mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbb{Q}$ is a finite dimensional $\mathbb{Q}$-algebra with a positive definite involution with respect to the rational trace.

In order to go further in the description of the structure of $\mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbb{Q}$, we have to introduce a subclass of endomorphisms: The isogenies.

Definition 6.4.3 *Let A_1 and A_2 be two abelian varieties defined over $\mathbb{C}$. A homomorphism $\phi : A_1 \to A_2$ of abelian varieties is called an isogeny if ϕ is surjective and has a finite kernel.*

Here is an example of an isogeny. For any abelian variety A and non-zero integer $n \in \mathbb{Z}$, let $n_A : A \to A$ be defined by $a \mapsto n \cdot a$, then n_A is an isogeny. Isogenies are "almost isomorphisms". Indeed, if $f : A_1 \to A_2$ is an isogeny, let $e = e(f)$ be the exponent of the group $\ker(f)$, then we have:

Theorem 6.4.4 *Let A_1 and A_2 be abelian varieties over $\mathbb{C}$ and let $\phi \in \mathrm{Hom}(A_1, A_2)$ be an isogeny. There exists a unique isogeny $\psi : A_2 \to A_1$ such that*

- $\phi \circ \psi = e(\phi)_{A_2}$;
- $\psi \circ \phi = e(\psi)_{A_1}$,

and $e(\phi) = e(\psi)$.

Therefore, it makes sense to talk about isogenous abelian varieties.

Definition 6.4.4 *Two abelian varieties A_1 and A_2 are called isogenous if there exists an isogeny $\phi : A_1 \to A_2$. This defines an equivalence relation on the set of abelian varieties.*

Note also that because of Theorem 6.4.4, the isogenies of A into itself are precisely the invertible elements in $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$.

Definition 6.4.5 *An abelian variety A is simple if the only sub-abelian varieties of A are $\{0\}$ and A itself.*

Theorem 6.4.5 *If A is a simple abelian variety, then $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division $\mathbb{Q}$-algebra.*

If A is not simple, then it can be decomposed up to isogeny as a product of simple ones.

Theorem 6.4.6 (Poincaré complete reducibility theorem) *Suppose that A is an abelian variety, then there exists an isogeny*

$$A \to A_1^{n_1} \times \ldots A_t^{n_t},$$

such that all A_i are simple abelian varieties. Moreover, the pairs (A_i, n_i) are uniquely determined up to isogeny $(i = 1, \ldots, t)$.

Corollary 6.4.1 *With the same notation as in the last theorem, we have*

$$\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q} \simeq M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t),$$

where $D_i = \mathrm{End}(A_i) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a division $\mathbb{Q}$-algebra $(i = 1, \ldots, t)$.

This last theorem together with Wedderburn's theorem tells us that $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ is a semisimple algebra with a positive involution. Because of Corollary 6.4.1 we can restrict our study to $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$, where A is simple. In this particular case we have established:

Theorem 6.4.7 *Let A be a simple abelian variety. Then* $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ *is a simple finite dimensional division $\mathbb{Q}$-algebra with a positive definite involution (Rosati involution) with respect to the rational trace.*

Abraham Adrian Albert (1905-1972) classified the structure of such algebras, see [1], [2] and [3]. His results are clearly explained in [4]. So let $(D, ')$ be a finite dimensional division $\mathbb{Q}$-algebra with a positive anti-involution $x \mapsto x'$. We shall denote the center of D by K. The anti-involution induces an involution on K (since K is commutative). Let K_0 be its fixed field.

Theorem 6.4.8 *With the notation above, K_0 is a totally real number field.*

Definition 6.4.6 *The pair $(D, ')$ is called of the first type if $K = K_0$ and of the second type otherwise.*

Theorem 6.4.9 *Let $(D, ')$ be of the second type. Then its center K is totally imaginary, the restriction of the anti-involution to K is the non-trivial automorphism of K over K_0, and $[K : K_0] = 2$.*

We give a special name to the kind of fields which appear in the last theorem.

Definition 6.4.7 *A CM-field is a number field which is a totally imaginary quadratic extension of a totally real field.*

Note that quadratic imaginary fields are CM-fields and cyclotomic fields provide another example of such fields. Here is a characterization of CM-field.

Theorem 6.4.10 *Let K be a number field, and fix an embedding of K in $\mathbb{C}$. Then K is a CM-field if and only if the following two conditions are satisfied:*

- *Complex conjugation τ induces a non-trivial automorphism of K.*
- *Complex conjugation commutes with all other embeddings, that is $\tau \circ \sigma = \sigma \circ \tau$ for all $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(K, \mathbb{C})$.*

It therefore follows that complex conjugation does not depend on the chosen embedding.

We shall not pursue the general study of such $\mathbb{Q}$-algebra $(D, ')$. See again [4] for this theory and to see which ones can be realized as $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ for some simple abelian variety A. We just state the final result.

Theorem 6.4.11 *Let $(D, ')$ be as above. Then we have the following possibilities for D:*

Type	Structure
First type	D = totally real number field
	D = totally indefinite quaternion algebra
	D = totally definite quaternion algebra
Second type	D = division algebra and $Z(D)$ is a CM-field

Table 6–1: The center of a finite dimensional division $\mathbb{Q}$-algebra with a positive anti-involution

We are now ready to define the generalization of an elliptic curve with complex multiplication by a quadratic imaginary field.

Definition 6.4.8 *Let $A \simeq \mathbb{C}^n/\Lambda$ be a polarized abelian variety of dimension n defined over $\mathbb{C}$. Let K be a CM-field and suppose that $[K : \mathbb{Q}] = 2n$. We say that A has complex multiplication by K if there exists an embedding*

$$\iota : K \hookrightarrow \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q},$$

such that the Rosati involution induces complex conjugation on K.

When $n = 1$, we get back the old notion of complex multiplication of elliptic curves.

6.4.2 Construction of abelian varieties with CM

Now that we have defined the right generalization of complex multiplication to abelian varieties, we should explain how we can construct such abelian varieties. Instead of stating directly one big theorem, we shall state several small results that we collect in one big theorem at the end, see Theorem 6.4.12.

Definition 6.4.9 *Let K be a CM-field and suppose moreover that $[K : K_0] = 2n$. Let $\Phi = \{\varphi_1, \ldots, \varphi_n\}$ be a set of embeddings $\varphi_i : K \to \mathbb{C}$ such that none of them is the complex conjugate of another one, that is*

$$\varphi_i \neq \bar{\varphi}_j,$$

for all $i, j = 1, \ldots, n$. Then we call (K, Φ) a CM-type.

Lemma 6.4.1 *Let K be a CM-field and let K_0 be its associated totally real subfield. Then, there exists $\xi \in K$ such that*

- *$K = K_0(\xi)$, $(\xi \neq 0)$;*
- *$-\xi^2$ is totally positive.*

Proof:

By the primitive element theorem, there exists $\xi' \in K$ such that $K = K_0(\xi')$ and since the extension is quadratic, ξ' satifies a quadratic polynomial with coefficients in K_0:

$$a_2\xi'^2 + a_1\xi' + a_0 = 0,$$

for some $a_i \in K_0$, $(i = 0, 1, 2)$. Then

$$\xi' = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2a_0}}{2a_2}.$$

Set $\xi = \sqrt{a_1^2 - 4a_2a_0}$, we have $K = K_0(\xi)$, and $\xi^2 = a_1^2 - 4a_2a_0 \in K_0$. Since $[K : K_0] = 2$, $\xi \neq 0$. This proves the first part.

Now, we want to show that $-\xi^2$ is totally positive. Suppose that it is not. Then there exists a real embedding $\sigma : K_0 \to \mathbb{R}$ such that $\sigma(-\xi^2) < 0$. Let $\tilde{\sigma}$ be any extension of σ to K. Then we have

$$0 > \sigma(-\xi^2) = \tilde{\sigma}(-\xi^2) = -\tilde{\sigma}(\xi)\tilde{\sigma}(\xi),$$

and therefore $\tilde{\sigma}(\xi)\tilde{\sigma}(\xi) > 0$. Write $\tilde{\sigma}(\xi) = a + ib$ for some $a, b \in \mathbb{R}$. The product becomes then $(a+ib)(a+ib) = (a^2 - b^2) + 2abi > 0$ implies that a or $b = 0$. If $a = 0$

then $a^2 > b^2 > 0$ implies that $b = 0$ but since $\xi \neq 0$, $\tilde{\sigma}(\xi) \neq 0$. Thus $b = 0$, but then $\tilde{\sigma}(\xi) \in \mathbb{R}$ which is a contradiction since K is totally imaginary.

□

Lemma 6.4.2 *Let (K, Φ) be a CM-type and let K_0 be its associated totally real subfield. Then by the last lemma, we can choose $\xi \in K$ such that $K = K_0(\xi)$, the element $-\xi^2$ is in K_0 and $-\xi^2$ totally positive. We claim that we can choose ξ such that in addition $\mathrm{Im}(\varphi(\xi)) > 0$ for all $\varphi \in \Phi$.*

Proof:

Suppose that ξ' satisfies the hypothesis of Lemma 6.4.1. We can choose an $\alpha \in K_0$ with any sign distribution, so choose $\alpha \in K_0$ such that $\varphi(\alpha) \cdot \mathrm{Im}(\varphi(\xi')) > 0$, for all $\varphi \in \Phi$, and set $\xi = \alpha \cdot \xi'$.

□

Lemma 6.4.3 *Let $(K, \Phi = \{\varphi_1, \ldots, \varphi_n\})$ be a CM-type and suppose $[K : \mathbb{Q}] = 2n$. Consider then the map*

$$\Phi : K \to \mathbb{C}^n, \qquad \lambda \mapsto \Phi(\lambda) = (\varphi_1(\lambda), \ldots, \varphi_n(\lambda)).$$

For any free $\mathbb{Z}$-module $\mathfrak{a} \subseteq K$ of rank $2n$, the image $\Phi(\mathfrak{a})$ is a lattice in $\mathbb{C}^n$. Therefore, $\mathbb{C}^n/\Phi(\mathfrak{a})$ is a complex torus.

We can now construct some abelian varieties from a CM-type. According to Theorem 6.2.1, it suffices to find a Riemann form on $\mathbb{C}^n/\Phi(\mathfrak{a})$.

Lemma 6.4.4 *Let $(K, \Phi = \{\varphi_1, \ldots, \varphi_n\})$ be a CM-type and let K_0 be its associated totally real subfield. Let ξ be as in Lemma 6.4.2. Define for any $z = (z_1, \ldots, z_n)$, and $w = (w_1, \ldots, w_n) \in \mathbb{C}^n$:*

$$E(z, w) := \sum_{i=1}^{n} \varphi_i(\xi)(\overline{z_i} w_i - z_i \overline{w_i}).$$

Let $\mathfrak{a} \subseteq K$ be a free $\mathbb{Z}$-module of rank $2n$. For $\alpha, \beta \in K$ we have

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

and for a suitable integer m, $m \cdot E$ is a Riemann form on the torus $\mathbb{C}^n/\Phi(\mathfrak{a})$, which is thus an abelian variety.

Proof:

We have to check the conditions on Theorem 6.2.3. The facts that E is $\mathbb{R}$-alternating and that $E(iz, iw) = E(z, w)$ $(\forall z, w \in \mathbb{C}^n)$ are straightforward computations.

Next we check that $E(iz, z) \geq 0$. Note first that for any $i = 1, \ldots, n$, $\varphi_i(\xi)$ is a pure imaginary number (a complex number z is pure imaginary if $\overline{z} = -z$ or, in other words, has no real part). Indeed, the quadratic extension K/K_0 is Galois and the non-trivial Galois automorphism is defined by $\xi \mapsto -\xi$ and this is equal to the complex conjugation. Thus we have

$$\overline{\varphi_i(\xi)} = \varphi_i(\overline{\xi}) = \varphi_i(-\xi) = -\varphi_i(\xi),$$

and it is pure imaginary (note that we used the fact that complex conjugation commute with any embedding, see Theorem 6.4.10). So we have

$$E(iz, z) = \sum_{k=1}^{n} \varphi_k(\xi)(-i\overline{z_k}z_k - iz_k\overline{z_k}),$$

and $\varphi_k(\xi)$ pure imaginary implies that $-i\varphi_k(\xi) = \operatorname{Im}\varphi_k(\xi)$, and therefore

$$E(iz, z) = 2\sum_{k=1}^{n}(\operatorname{Im}\varphi_k(\xi))|z_k|^2 \geq 0,$$

since $\operatorname{Im}\varphi_k(\xi) > 0$ for all $k = 1, \ldots, n$.

From this last equation, it is also clear that $E(iz, z) = 0 \Leftrightarrow z = 0$.

The only thing we still have to check in order to have a Riemann form is that E is integer-valued on $\Phi(\mathfrak{a})$. But this is not always the case and this is why we have to multiply by a suitable integer. First let $\alpha, \beta \in K$ then

$$\begin{aligned}\operatorname{Tr}_{K/\mathbb{Q}}(\xi \cdot \overline{\alpha} \cdot \beta) &= \sum_{\varphi \in \operatorname{Hom}_{\mathbb{Q}}(K, \mathbb{C})} \varphi(\xi \cdot \overline{\alpha} \cdot \beta) \\ &= \sum_{\varphi \in \Phi} \varphi(\xi \cdot \overline{\alpha} \cdot \beta) + \sum_{\varphi \in \Phi} \varphi \circ \tau(\xi \cdot \overline{\alpha} \cdot \beta),\end{aligned}$$

where τ is the complex conjugation. Further

$$\mathrm{Tr}_{K/\mathbb{Q}}(\xi \cdot \overline{\alpha} \cdot \beta) = \sum_{\varphi \in \Phi} \left(\varphi(\xi)\varphi(\overline{\alpha})\varphi(\beta) + \varphi(\overline{\xi})\varphi(\alpha)\varphi(\overline{\beta})\right),$$

and since $\overline{\xi} = -\xi$, we get

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(\xi \cdot \overline{\alpha} \cdot \beta) &= \sum_{\varphi \in \Phi} \left(\varphi(\xi)\varphi(\overline{\alpha})\varphi(\beta) + \varphi(-\xi)\varphi(\alpha)\varphi(\overline{\beta})\right) \\ &= \sum_{\varphi \in \Phi} \varphi(\xi)\Big(\varphi(\overline{\alpha})\varphi(\beta) - \varphi(\alpha)\varphi(\overline{\beta})\Big).\end{aligned}$$

This last sum is exactly $E(\Phi(\alpha), \Phi(\beta))$. According to this equality, $E(\Phi(\alpha), \Phi(\beta)) \in \mathbb{Q}$ for all $\alpha, \beta \in K$. Finally, since $\mathfrak{a}$ is in particular a finitely generated $\mathbb{Z}$-module the denominators of the reduced fractions that E takes on $\Phi(\mathfrak{a})$ are bounded. Therefore, we can find m in $\mathbb{Z}$ such that $m \cdot E$ is integer-valued on $\Phi(\mathfrak{a})$ and this conclude the proof.

□

Next, we want to see if this abelian variety has complex multiplication by K.

Lemma 6.4.5 *Let (K, Φ) be a CM-type and let the notation be as in Lemma 6.4.4. Then for any free $\mathbb{Z}$-module $\mathfrak{a} \subseteq K$ of rank $2n$, $A \simeq \mathbb{C}^n/\Phi(\mathfrak{a})$ is an abelian variety. Moreover, this abelian variety has complex multiplication by K.*

Proof:

So we have to check two things: Firstly that K can be embedded in $\mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ and then that the Rosati involution induces the complex conjugation on K.

Let O be the order associated to $\mathfrak{a}$, that is

$$O = \{\lambda \in K | \lambda \cdot \mathfrak{a} = \mathfrak{a}\}.$$

For any $\lambda \in O$ define $S_\lambda \in \mathrm{Hom}_{\mathbb{C}}(\mathbb{C}^n, \mathbb{C}^n)$ by

$$S_\lambda(z) = (\varphi_1(\lambda)z_1, \ldots, \varphi_n(\lambda)z_n),$$

for any $z \in \mathbb{C}^n$. We claim, that S_λ induces an endomorphism on $\mathbb{C}^n/\Phi(\mathfrak{a})$. We thus have to check that $S_\lambda(\Phi(\mathfrak{a})) \subseteq \Phi(\mathfrak{a})$. Let $\alpha \in \mathfrak{a}$, then

$$S_\lambda(\Phi(\alpha)) = (\varphi_1(\lambda \cdot \alpha), \ldots, \varphi_n(\lambda \cdot \alpha)).$$

By definition of O, $\lambda \cdot \mathfrak{a} = \mathfrak{a}$ thus

$$S_\lambda(\Phi(\alpha)) = \Phi(\lambda \cdot \alpha) \in \Phi(\mathfrak{a}).$$

We thus have an induced map $\phi_\lambda : \mathbb{C}^n/\Phi(\mathfrak{a}) \to \mathbb{C}^n/\Phi(\mathfrak{a})$, defined by $z + \Phi(\mathfrak{a}) \mapsto S_\lambda(z) + \Phi(\mathfrak{a})$. This gives us an embedding

$$O \hookrightarrow \mathrm{End}(A)$$

Next, since O is an order, $\mathrm{Frac}(O) = K$. Using the universal property of the fraction field, we get an embedding

$$K \hookrightarrow \mathrm{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

The fact that the Rosati involution induces complex conjugation on K is clear.

□

We summarise our results as follows:

Theorem 6.4.12 *Let $(K, \Phi = \{\varphi_1, \ldots, \varphi_n\})$ be a CM-type and K_0 its totally real subfield. Suppose moreover that $[K : \mathbb{Q}] = 2n$. Then*

1. *There exists $\xi \in K$ such that*
   (a) $K = K_0(\xi)$;
   (b) $-\xi^2 \gg 0$;
   (c) $\mathrm{Im}\,\varphi(\xi) > 0$ *for all* $\varphi \in \Phi$.
2. *For any free $\mathbb{Z}$-module $\mathfrak{a} \subseteq K$ of rank $2n$, $\mathbb{C}^n/\Phi(\mathfrak{a})$ is a complex torus, where $\Phi : K \to \mathbb{C}^n$ is defined by $\lambda \mapsto (\varphi_1(\lambda), \ldots, \varphi_n(\lambda))$.*

3. *A suitable integer multiple of the $\mathbb{R}$-bilinear form*

$$E(z,w) = \sum_{i=1}^{n} \varphi(\xi)(\overline{z_i}w_i - z_i\overline{w_i})$$

is a Riemann form on $\mathbb{C}^n/\Phi(\mathfrak{a})$ and in this way $\mathbb{C}^n/\Phi(\mathfrak{a})$ becomes an abelian variety with complex multiplication by K.

We have also the converse, namely:

Theorem 6.4.13 *Every abelian variety defined over $\mathbb{C}$ with complex multiplication by a CM-field K can be constructed as in the previous theorem.*

Definition 6.4.10 *A CM-type (K,Φ) is called primitive if every abelian variety with complex multiplication by K is simple.*

6.4.3 The reflex field

Definition 6.4.11 *Let (K,Φ) be a CM-type. We define the type norm (or half-norm) and the type trace (or half-trace) as follows:*

- $N_\Phi(\lambda) = \prod_{\varphi\in\Phi} \varphi(\lambda)$;
- $T_\Phi(\lambda) = \sum_{\varphi\in\Phi} \varphi(\lambda)$,

for all $\lambda \in K$.

Definition 6.4.12 *Let (K,Φ) be a CM-type, we define the reflex field to be*

$$K^* := \mathbb{Q}(\{T_\Phi(\lambda) | \lambda \in K\}).$$

Theorem 6.4.14 *Let (K,Φ) be a CM-type, then the reflex field K^* is also a CM-field.*

Associated to the reflex field, there is also a reflex type. This notion is contained in the next theorem.

Theorem 6.4.15 *Let (K,Φ) be a CM-type, and $L/\mathbb{Q}$ a finite Galois extension containing K. Let $G = \mathrm{Gal}(L/\mathbb{Q})$ and define*

- $S = \{\sigma \in G | \sigma$ *induces a* $\varphi \in \Phi$ *on* $K\}$;
- $S^* = \{\sigma^{-1} | \sigma \in S\}$;

- $H^* = \{\gamma \in G | S^*\gamma = S^*\}$.

Then $K^* = L^{H^*}$, *the fixed field of* L *by* H^*. *Moreover, if*

$$\Phi^* = \{\psi : K^* \to \mathbb{C} | \psi \text{ is induced by } \sigma \in S^*\},$$

then (K^*, Φ^*) *is a primitive* CM*-type. Finally, all this does not depend on the Galois extension* L *containing* K.

There is a link between ideals in K and ideals in K^*:

Theorem 6.4.16 *Let* (K, Φ) *be a* CM*-type and* (K^*, Φ^*) *its reflex field. Let also* $L/\mathbb{Q}$ *be a Galois extension containing* K. *If* $\mathfrak{a}$ *is an ideal in* K^*, *then there exists an ideal* $\mathfrak{b}$ *in* K *such that*

$$\mathfrak{b} \cdot O_L = \prod_{\varphi \in \Phi^*} \varphi(\mathfrak{a}) \cdot O_L, \qquad \mathfrak{b} \cdot \overline{\mathfrak{b}} = \mathbb{N}(\mathfrak{a}) \cdot O_K.$$

To conclude this chapter, we say a word on explicit class field theory. Using this theory, Taniyama and Shimura were able to generate abelian extensions of the reflex field of a CM-field using values of Siegel modular functions evaluated at CM-points. Yet, it is also known that we do not get $(K^*)^{ab}$ in this case. Note that if K is a quadratic imaginary field, then $K^* = K$, and this is why the reflex field did not appear in the theory of complex multiplication of elliptic curves.

CHAPTER 7
DeShalit–Goren invariants

7.1 Stark's conjectures again

The construction of elliptic units in abelian extensions of a quadratic imaginary number field used explicit class field theory provided by the theory of complex multiplication. It is thus natural to try to construct units in abelian extensions of the reflex field of a CM-field. The hope is that it would lead to other cases of Stark's conjectures. Let (K, Φ) be a CM-type of degree four, then there are three possibilities:

1. K is Galois, $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In that case Φ is non-primitive, and K^* is quadratic imaginary;
2. K is Galois, $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$. In that case $K = K^*$, and Φ is primitive;
3. K is non-Galois. In that case K^* is another CM-field of degree 4 over $\mathbb{Q}$.

We shall not deal with the case (1). In that case, one can use the theory of elliptic units in order to construct units in abelian extensions of K^*. Case (2) will be called the cyclic case and case (3) will be referred to as the non-Galois case.

Let thus K be any CM-field of degree 4 falling in either the cyclic case or the non-Galois case. Then K^* is a CM-field of degree 4 over $\mathbb{Q}$. Let L/K^* be any abelian extensions and let S be any set of primes of K^* containing S_∞. Moreover, let χ be any character of $\mathrm{Gal}(L/K^*)$. Here S satisfies automatically conditions **S1** and **S3** of Chapter 4. Suppose that S satisfies also **S2**, then from Theorem 4.0.3, we see that $\mathrm{St}(L/K^*, S)$ is true in that case. Actually, from Corollary 4.0.1, we see that if $\chi \neq \chi_1$, then $r_S(\chi) \geq 2$ and thus we can take $\varepsilon = 1$ as a Stark unit. If $\chi = \chi_1$, then the only way to get a rank one L-function is to take an unramified abelian extension

L/K^* and $S = S_\infty$. The rank one abelian conjecture is also known to be true in that case.

Anyway, except this last case, the L-functions will have a zero of order at least 2 at $s = 0$. Karl Rubin stated a generalization of Stark's conjectures for zeros of higher orders at $s = 0$, see [56]. This is the case of interest for us and this can be viewed as a motivation of constructing S-units in abelian extension of CM-fields of degree greater than two.

7.2 Class invariants

In this section, we explain the construction of DeShalit–Goren. First of all, we let K be a CM-field of degree four and we fix a CM-type (K, Φ). Moreover, let (K^*, Φ^*) be its reflex field. The construction of DeShalit–Goren concerns the cyclic and non-Galois cases, but in this thesis, we deal only with the cyclic case. Therefore, we suppose K to be Galois with Galois group isomorphic to the cyclic group of order four.

Let $\mathfrak{h}_2$ be the Siegel space. For $\tau \in \mathfrak{h}_2$ and $u \in M_{2\times 1}(\mathbb{C})$, we define the theta function with characteristics $r, s \in M_{2\times 1}(\mathbb{Q})$ by

$$\theta\begin{bmatrix} r \\ s \end{bmatrix}(u, \tau) = \sum_{n\in\mathbb{Z}^2} \exp\left(2\pi i \left(\frac{1}{2}(n+r)^t\tau(n+r) + (n+r)^t(u+s)\right)\right).$$

Definition 7.2.1 *The characteristics are called integral if $r, s \in \frac{1}{2}\mathbb{Z}^2$ and are called even if they are integral and $r^t \cdot s \in \frac{1}{2}\mathbb{Z}$.*

Theta functions with integral characteristics depend only on $r, s \mod \mathbb{Z}^2$, up to ± 1. We shall work with the square of this function so this sign ambiguity does not matter. In our case, ten out of the sixteen integral characteristics are even:

$$\begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1/2 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1/2 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 0 \\ 1/2 \\ 1/2 \end{bmatrix}, \begin{bmatrix} 0 \\ 1/2 \\ 0 \\ 0 \end{bmatrix},$$
$$\begin{bmatrix} 0 \\ 1/2 \\ 1/2 \\ 0 \end{bmatrix}, \begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1/2 \\ 0 \\ 0 \\ 1/2 \end{bmatrix}, \begin{bmatrix} 1/2 \\ 1/2 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} 1/2 \\ 1/2 \\ 1/2 \\ 1/2 \end{bmatrix}.$$

Consider then

$$\theta_{ev}(u,\tau) = \prod_{even} \theta \begin{bmatrix} r \\ s \end{bmatrix} (u,\tau),$$

where the product is over all the even characteristics (this is defined up to a sign) and set

$$\theta_{ev}(\tau) = \theta_{ev}(0,\tau).$$

Igusa proved in [30] that $\theta_{ev}^2(\tau)$ is a Siegel modular form of level 1 and weight 10.

Let Λ be a lattice in $\mathbb{C}^2$ and let $\mathbb{C}^2/\Lambda$ be an abelian surface with a principal polarization given by a Riemann form E. Let $\Omega = (\omega_1, \omega_2)$ be a symplectic basis of Λ. The function

$$\Delta(\Lambda, E) = \det(\omega_2)^{-10} \theta_{ev}^2(\omega_2^{-1}\omega_1),$$

depends only on Λ and E. Next, we shall evaluate this function at some CM-points. We have seen in the last chapter how to construct abelian surfaces with complex multiplication by a CM-field. We explain now a condition for that surface to admit a principal polarization.

Let $\mathfrak{a}$ be a fractional ideal of K. We have seen in the last chapter that $\mathbb{C}^2/\Phi(\mathfrak{a})$ is an abelian manifold. We have seen also that there exists a $\delta \in K$ (in Theorem 6.4.12, take $\delta = \xi^{-1}$) satisfying $\overline{\delta} = -\delta$ and $\mathrm{Im}(\varphi(\delta)) > 0$ for $\varphi \in \Phi$, such that for $u, v \in \mathfrak{a}$

$$E_\delta(\Phi(u), \Phi(v)) = \mathrm{Tr}_{K/\mathbb{Q}}(\delta^{-1}\overline{u}v),$$

is a Riemann form for this abelian manifold. The following lemma is immediate.

Lemma 7.2.1 *The polarization induced by the Riemann form E_δ on $\mathbb{C}^2/\Phi(\mathfrak{a})$ is principal if and only if*

$$\mathcal{D}_{K/\mathbb{Q}}\overline{\mathfrak{a}}\mathfrak{a} = \delta \cdot O_K$$

where $\mathcal{D}_{K/\mathbb{Q}}$ is the different of the field K.

We can now define the class invariants in the cyclic case. Let K be a cyclic quartic CM-field and F its associated totally real subfield. We suppose moreover that $h_F = 1$,

the fundamental unit of F has norm -1 (these last two conditions imply $h_F^+ = 1$), and that the different $\mathcal{D}_{K/\mathbb{Q}}$ is generated by a pure imaginary number δ. Since the norm of the fundamental unit is -1, we can choose δ such that

$$\operatorname{Im} \varphi(\delta) > 0,$$

for all $\varphi \in \Phi$. For any ideal $\mathfrak{a}$ of O_K, choose a such that

$$\mathfrak{a} \cdot \overline{\mathfrak{a}} = a \cdot O_K, \qquad 0 \ll a \in F.$$

Then using the fact that the fundamental unit of F has norm -1, we can find a generator in F which is totally positive.

Consider the lattice $\Phi(\mathfrak{a})$ with the Riemann form

$$E_{a\delta}(\Phi(u), \Phi(v)) = \operatorname{Tr}_{K/\mathbb{Q}}(a^{-1}\delta^{-1}\overline{u}v).$$

The complex torus $\mathbb{C}^2/\Phi(\mathfrak{a})$ becomes a principally polarized abelian manifold. Define

$$\Delta(\Phi(\mathfrak{a})) = \Delta(\Phi(\mathfrak{a}), E_{a\delta}),$$

and set

$$u(\Phi; \mathfrak{a}) = \frac{\Delta(\Phi(\mathfrak{a}^{-1}))}{\Delta(\Phi(O_K))}.$$

Theorem 7.2.1 *The invariants $u(\Phi; \mathfrak{a})$ have the following properties:*

1. *$u(\Phi; \mathfrak{a})$ is well-defined and $u(\Phi; \mathfrak{a}) \neq 0, \infty$.*
2. *$u(\Phi; \mathfrak{a}) \in H_K$, and $\sqrt{u(\Phi; \mathfrak{a})} \in K^{ab}$.*
3. *The explicit reciprocity law is given by the following rule: If C is any ideal of K and $\mathfrak{c} = N_{\Phi^*}(C)$, then*

$$u(\Phi; \mathfrak{a})^{(C, H_K/K)} = \frac{u(\Phi; \mathfrak{ac})}{u(\Phi; \mathfrak{c})}.$$

4. *If $\lambda \in K^\times$, then $u(\Phi; \lambda \cdot \mathfrak{a}) = N_\Phi(\lambda)^{10} \cdot u(\Phi, \mathfrak{a})$.*

5. *The invariant* $u(\Phi;\mathfrak{a},\mathfrak{b}) = u(\Phi;\mathfrak{ab})/u(\Phi;\mathfrak{a})u(\Phi;\mathfrak{b})$ *depends only on the classes of* $\mathfrak{a}$ *and* $\mathfrak{b}$. *Its norm from* H_K *to* K *is 1.*

6. *The invariants behave as follows under a change of CM-type:* $u(\Phi\sigma,\sigma^{-1}\mathfrak{a}) = u(\Phi,\mathfrak{a})$ *for any* $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$. *The Galois group acts transitively on the four CM-types of* K.

7. *Assume* $(h_K, 10) = 1$. *Then the* $u(\Phi;\mathfrak{a})$ *generate* H_K. *In particular, if* $h_K > 1$ *they are non-trivial.*

8. *Assume* h_K *is prime and different from 5 and 2. Then the group generated by the* $u(\Phi;\mathfrak{a},\mathfrak{b})$ *in* $H_K^\times$ *has rank* $h_K - 1$.

The invariants we are interested in are the $u(\Phi;\mathfrak{a},\mathfrak{b})$.

Theorem 7.2.2 *The following properties are equivalent:*

1. *The* $u(\Phi;\mathfrak{a},\mathfrak{b})$ *are units, for all* $\mathfrak{a}$, $\mathfrak{b}$.

2. *For every* $\mathfrak{a}$, $(u(\Phi;\mathfrak{a}))$ *is* $\mathrm{Gal}(H_K/K)$*-invariant.*

3. *For every* $\mathfrak{a}$, $(u(\Phi;\mathfrak{a})) = N_\Phi(\mathfrak{a})^{10}$.

4. *If* $\mathfrak{a}$ *is integral,* $u(\Phi;\mathfrak{a},\mathfrak{b})$ *is integral.*

7.3 Some further results

Since the publication of [14], others properties of these invariants have been discovered. We list them here.

1. A prime $\mathfrak{p}$ of H_K over p appears in the denominator of a class invariant if and only if there is a smooth genus 2 curve C, defined over an extension H of H_K, such that $Jac(C)$ has CM by O_K and there is a prime $\mathfrak{P}$ of H over $\mathfrak{p}$ such that C is isomorphic modulo $\mathfrak{P}$ to two supersingular elliptic curves E, E' intersecting transversely at their origins. See [14] and [23].

   Note that in [76], the author gives examples of such curves having CM by O_K.

2. A prime $\mathfrak{p}$ as above has the property that p is either ramified or decomposes as $\mathfrak{p}_1\mathfrak{p}_2$ in K, see [14].

In all examples of class number two and four we have studied, we verified this last fact and it was always true. For example, take the field $\mathbb{Q}(\sqrt{-41+4\sqrt{41}})$ (**B.2.X.**). Using MAGMA, we computed, for each invariant $u(\Phi;\mathfrak{a},\mathfrak{b})$, the number field $L = \mathbb{Q}(u(\Phi;\mathfrak{a},\mathfrak{b}))$. If x is a root of the minimal polynomial of $u(\Phi;\mathfrak{a},\mathfrak{b})$, then we computed the factorization of the ideal $x \cdot O_L$. We saw that the primes appearing below were 2, 5, 23, 31, 59 and 359. They all factorize into $\mathfrak{p}_1 \cdot \mathfrak{p}_2$ in K except 2 which factorizes as $\mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$.

3. Let us write $K = \mathbb{Q}(\sqrt{d})(\sqrt{r})$, where r is a totally negative algebraic integer of $\mathbb{Q}(\sqrt{d})$, d a square-free integer. A prime $\mathfrak{p}$ as above has the property that $p < 16 \cdot d^2 \cdot \mathrm{Tr}(r)^2$. This is the main result of [23].

   Here again, in all examples of class number two or four we have studied, we computed also this bound. All primes which appear are smaller than this bound. In the example above, the bound is 180848704.

4. In fact, if p is unramified in K and $\mathfrak{p}$ is as above, then if the denominator of $u(\Phi;\mathfrak{a},\mathfrak{b})$ has valuation n at $\mathfrak{p}$ then $n \leq \frac{1}{2} + 6 \cdot \frac{\log(d \cdot \mathrm{Tr}(-r)/2)}{\log(p)}$. The proof of this fact is not yet written in detail and so some caution has to be exercised. For instance, the exact constants may change, though qualitatively this is the result one gets. The reference for this is [21].

5. Let K be a quartic primitive CM-field. We say that a rational prime is "evil" (for K) if for some prime P of $\overline{\mathbb{Q}}$, there is a principally polarized abelian variety with complex multiplication by O_K whose reduction modulo P is the product of two supersingular elliptic curves with the product polarization. The result is: Let p be a rational prime and let L be a real quadratic field of strict class number one. There is a constant $N = N(L,p)$ such that p is evil for every primitive CM-field K such that $F = L$, $p = \mathfrak{p}_1 \cdot \mathfrak{p}_2$ in K and $\mathbb{N}(\Delta_{K/L}) > N$. See [24].

7.4 Analysis of the numerical results

We list here some observations we made concerning our numerical results.

- First of all, we find only two global units among all the examples we computed, namely **B.1.II.** and the last one in **B.2.I.**. This shows that in general one should not expect the DeShalit-Goren invariants to be units and so the focus should be on studying their factorization, going further than the results of Goren and Lauter.
- We never reach the theoretical bound for the size of the primes appearing in the ideal generated by an invariant $u(\mathfrak{a}, \mathfrak{b})$. Recall from Section 7.3, point 3, that if K is written as $\mathbb{Q}(\sqrt{d})(\sqrt{r})$, where r is a totally negative algebraic integer of $\mathbb{Q}(\sqrt{d})$, d a square-free integer, then the primes appearing in the decomposition of $u(\mathfrak{a}, \mathfrak{b})$ are above rational primes p bounded by $16 \cdot d^2 \cdot \mathrm{Tr}(r)^2$. However, in general, the size of the primes seems to be much smaller. For example, in **B.2.II.**, the largest prime decomposing in K as $\mathfrak{p}_1 \cdot \mathfrak{p}_2$ is 5345323 while the largest prime appearing in the decomposition of the elements $u(\mathfrak{a}, \mathfrak{b})$ is 47.
- Moreover, it seems that only few primes appear. For example, in **B.2.IV.** the bound is 50176. There are exactly 5152 primes below this bound and two of them are ramified, namely 2 and 7. Among the 5150 unramified primes, 2597 decompose as $\mathfrak{p}$, 1252 as $\mathfrak{p}_1 \cdot \mathfrak{p}_2$ and 1301 as $\mathfrak{p}_1 \cdot \mathfrak{p}_2 \cdot \mathfrak{p}_3 \cdot \mathfrak{p}_4$ in the CM-field K. Thus there are 1301 primes that could appear, but only three of them actually occur, namely 17, 31, and 47.
- Among the class number two examples, only unramified primes appear.
- On the other hand, among the class number four examples, there are six of them where a ramified prime appear.
    1. **B.2.II.** There are two ramified primes: $2 \cdot O_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ and $17 \cdot O_K = \mathfrak{p}^4$. Only 2 appears.

2. **B.2.IV.** There are two ramified primes: $2 \cdot O_K = \mathfrak{p}^4$ and $7 \cdot O_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$. Only 7 appears.
3. **B.2.VI.** There are two ramified primes: $2 \cdot O_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ and $17 \cdot O_K = \mathfrak{p}^4$. Only 2 appears.
4. **B.2.IX.** There are two ramified primes: $5 \cdot O_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ and $29 \cdot O_K = \mathfrak{p}^4$. Only 5 appears.
5. **B.2.X.** There are two ramified primes: $2 \cdot O_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ and $41 \cdot O_K = \mathfrak{p}^4$. Only 2 appears.
6. **B.2.XI.** There are two ramified primes: $3 \cdot O_K = \mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ and $73 \cdot O_K = \mathfrak{p}^4$. Only 3 appears.

Hence, we notice that every ramified prime that appear is of the form $\mathfrak{p}_1^2 \cdot \mathfrak{p}_2^2$ in K.

- Recall that Theorem 7.2.1 guarantees that the span of the class invariants is "big" provided the class number is prime to 10. From example **B.2.V.**, we see that the condition of the class number is necessary. Indeed, the field spanned by the invariants is $\mathbb{Q}(\sqrt{5})$, while the Hilbert class field has degree 4 over K.
- We note also that for all class number four examples, all prime ideals appearing in their factorization are raised at a power either two or four.

CHAPTER 8
Computation

8.1 Algorithm

All computations have been done with the software MAGMA V2.11-13. The computer on which we ran the computations was a Intel(R) Pentium(R) 4 CPU 2.53GHz with 512MB of RAM. The approximate running time varies from one example to another. For instance, example **B.1.I.** takes about 41 seconds for a precision of about 300 digits. On the other hand, example **B.2.XIII.** takes about 10515 seconds for a precision of about 1800 digits.

We present here the algorithm that we haved used for computing the class invariants.

1. Take a CM-field K Galois over $\mathbb{Q}$ with Galois group $\mathbb{Z}/4\mathbb{Z}$.

   In the article [49], the authors determine all non-quadratic imaginary cyclic number fields of 2-power degree with relative class number smaller or equal to 20. Thus it gives us all the cyclic quartic CM-fields with small class number (smaller or equal to 20). For instance, there are exactly eight of them with class number two. They are listed in the following table:

$\mathbb{Q}(\sqrt{-5+\sqrt{5}})$	$\mathbb{Q}(\sqrt{-6+3\sqrt{2}})$
$\mathbb{Q}(\sqrt{-65+26\sqrt{5}})$	$\mathbb{Q}(\sqrt{-65+10\sqrt{13}})$
$\mathbb{Q}(\sqrt{-10+5\sqrt{2}})$	$\mathbb{Q}(\sqrt{-85+34\sqrt{5}})$
$\mathbb{Q}(\sqrt{-13+3\sqrt{13}})$	$\mathbb{Q}(\sqrt{-119+28\sqrt{17}})$

Table 8–1: Cyclic quartic CM-fields with class number 2

2. Among the cyclic quartic CM-fields provided by [49], we choose the ones such that $h_F = 1$ (F is the totally real subfield associated to K) and also such that the fundamental unit of F has norm -1.

   It follows that $h_F^+ = 1$. Indeed, let $\mathfrak{a}$ be any fractional ideal of F. Since $h_F = 1$, the ideal $\mathfrak{a} = \alpha \cdot O_K$ for some $\alpha \in K^\times$. Then, multiplying α by -1 or $\pm\eta$, we can get a positive generator, and therefore $h_F^+ = 1$. Here are some examples of some real quadratic number fields with class number one and with a fundamental unit of norm -1: $K = \mathbb{Q}(\sqrt{d})$, where $d = 2, 5, 13, 17, 29, 41, 73$ (we will use these ones).

3. Fix a CM-type of K.

   In our case, suppose $G = \mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma, \tau, \sigma\tau\}$, where σ is a generator of G, and τ is the complex conjugation. There are four CM-types which are given abstractly by

$$\Phi_1 = \{1, \sigma\}, \qquad \Phi_2 = \{1, \sigma\tau\}, \qquad \Phi_3 = \{\sigma, \tau\}, \qquad \Phi_4 = \{\sigma\tau, \tau\}.$$

   Note also that by property 6 of Theorem 7.2.1, it suffices to compute all the invariants $u(\Phi; \mathfrak{a}, \mathfrak{b})$ (by all, we mean $u(\Phi; \mathfrak{a}, \mathfrak{b})$, where $[\mathfrak{a}]$ and $[\mathfrak{b}]$ run over all ideal classes of $\mathrm{Cl}(K)$) for only one CM-type.

4. Find a good generator δ for the different $\mathcal{D}_{K/\mathbb{Q}}$.

   First, we find a generator of $\mathcal{D}_{K/\mathbb{Q}}$ and we check whether or not it is pure imaginary. In all examples we have studied, it is always the case. Then, we multiply it by $\pm\eta$, where η is the fundamental unit of F, in order to have $\mathrm{Im}\,\varphi(\delta) > 0$ for all $\varphi \in \Phi$.

5. Find a representative for each ideal class in K.

6. For each such representative $\mathfrak{a}$, we find a generator $a \in F$ of $\mathfrak{a} \cdot \bar{\mathfrak{a}}$ such that $a \gg 0$. We multiply a generator by ± 1, $\pm\eta$, where η is the fundamental unit of F, in order to get a totally positive generator.

7. We compute the Riemann form which gives a principal polarization on $\mathbb{C}^2/\Phi(\mathfrak{a})$. It is given by $E_{a\delta}(\Phi(u),\Phi(v)) = \mathrm{Tr}_{K/\mathbb{Q}}(a^{-1}\delta^{-1}\overline{u}v)$.
8. For each $\mathfrak{a}$, we find a symplectic basis $(e_1, e_2, \epsilon_1, \epsilon_2)$ for $\mathfrak{a}$ with respect to the alternating form $E_{a\delta}$.

   Here, we proceeded as follows. We find a $\mathbb{Z}$-basis $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ of $\mathfrak{a}$. Let $A = (E_{a\delta}(\alpha_i, \alpha_j))$ and let $[n_1\ n_2\ n_3\ n_4]^t$ denotes the coordinate of any vector $x = n_1\alpha_1 + n_2\alpha_2 + n_3\alpha_3 + n_4\alpha_4 \in \mathfrak{a}$. First, we take $\lambda_1 = [1\,0\,0\,0]^t$ and we find $\lambda_2 = [0\ x\ y\ z]^t$ such that $\lambda_2^t A\lambda_1 = -1$. For this, we used the command `Solution` provided by MAGMA. Then, we set $M = [A\cdot\lambda_1^t\ A\cdot\lambda_2^t] \in M_{4\times 2}(\mathbb{Z})$. Then the command `Solution` gives a basis of the nullspace of M. We denote this basis by λ_3 and λ_4. We necessarily have $E_{a\delta}(\lambda_3, \lambda_4) = \pm 1$. Thus, if $E_{a\delta}(\lambda_3, \lambda_4) = 1$, then we take $e_1 = \lambda_2$, $e_2 = \lambda_4$, $\varepsilon_1 = \lambda_1$, and $\varepsilon_2 = \lambda_3$. If $E_{a\delta}(\lambda_3, \lambda_4) = -1$, we take instead $e_1 = \lambda_2$, $e_2 = \lambda_3$, $\varepsilon_1 = \lambda_1$, and $\varepsilon_2 = \lambda_4$. We get in that way a symplectic basis.
9. Find the period matrix (ω_1, ω_2).

   Recall from Chapter 6, that $\omega_1 = \begin{pmatrix} \varphi_1(e_1) & \varphi_1(e_2) \\ \varphi_2(e_1) & \varphi_2(e_2) \end{pmatrix}$ and that $\omega_2 = \begin{pmatrix} \varphi_1(\varepsilon_1) & \varphi_1(\varepsilon_2) \\ \varphi_2(\varepsilon_1) & \varphi_2(\varepsilon_2) \end{pmatrix}$.
10. Find the corresponding point $\tau = \omega_2^{-1}\cdot\omega_1 \in \mathfrak{h}_2$.
11. For the ten even characteristics, compute $\theta\begin{bmatrix} r \\ s \end{bmatrix}(0,\tau)$ to a high precision.

    Say we would like to compute this theta series up to the precision 10^{-m} for some integer m. Note that we have

$$\left|\exp\left(\pi i(n+r)^t\tau(n+r) + 2\pi i(n+r)^t s\right)\right| = \exp\left(-\pi(n+r)^t\mathrm{Im}(\tau)(n+r)\right),$$

    and thus, we want to find a constant C such that

$$\left|\sum_{\substack{n\in\mathbb{Z}^2 \\ (n+r)^t\mathrm{Im}(\tau)(n+r)>C}} \exp\left(\pi i(n+r)^t\tau(n+r) + 2\pi i(n+r)^t s\right)\right| \leq 10^{-m}.$$

This is done in [80]. We just state the result here. We should take C such that

$$C > m + 0.35 - 2\log_{10}(\min \tau),$$

where $\min \tau = \min_{n \in \mathbb{Z}^2} n^t \cdot \mathrm{Im}(\tau) \cdot n$. Moreover, if $C \geq 75$, then we can take

$$C > \frac{1}{2}(m + 0.35 - 2\log_{10}(\min \tau)).$$

Next, we have to compute all $n \in \mathbb{Z}^2$ such that

$$(n+r)^t \mathrm{Im}(\tau)(n+r) \leq C.$$

Here again, we used an algorithm presented in [80].

12. Compute $\Delta(\Phi(\mathfrak{a}), E_{a\delta})$ for each representative $\mathfrak{a}$.

    We see that the bigger is the imaginary part the faster will be the convergence of the theta series. We used here a trick suggested by Van Wamelen in [76]. In order to increase the imaginary part, we apply a generator of $\mathrm{Sp}_2(\mathbb{Z})$ to $\tau = \omega_2^{-1}\omega_1$ in order to bring it back in the fundamental domain. Thus, if we have $\tau' = M \cdot \tau$ for some $M \in \mathrm{SL}_2(\mathbb{Z})$ then

    $$\theta_{ev}^2(\tau) = \det(CZ + D)^{-10} \cdot \theta_{ev}^2(\tau'),$$

    where $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{Sp}_2(\mathbb{Z})$, since θ_{ev}^2 is a Siegel modular form of weight 10. Van Wamelen implemented a function in MAGMA in order to do this. The name of this function is `To2DUpperHalfSpaceFundamentalDomian`.

13. Compute $u(\Phi; \mathfrak{a})$ for all representatives $\mathfrak{a}$.
14. Compute $u(\Phi; \mathfrak{a}, \mathfrak{b})$, where $\mathfrak{a}$ and $\mathfrak{b}$ run over all representatives of $\mathrm{Cl}(K)$.
15. Choose any one of the class invariants, say $u(\Phi; \mathfrak{a}, \mathfrak{b})$.
16. Compute the reflex type.

    With the same notation as in step 3, we have then:

    $$\Phi_1^* = \{1, \sigma\tau\}, \qquad \Phi_2^* = \{1, \sigma\}, \qquad \Phi_3^* = \{\sigma\tau, \tau\}, \qquad \Phi_4^* = \{\sigma, \tau\}.$$

17. Compute the action of the Galois group $\mathrm{Gal}(H_K/K)$ on $u(\Phi;\mathfrak{a},\mathfrak{b})$.

    By Property 3 of Theorem 7.2.1, we know the action of $\mathrm{Gal}(H_K/K)$ on $u(\Phi;\mathfrak{a})$. Let $\mathcal{C}$ be an ideal of $\mathrm{Cl}(K)$, and let $\mathfrak{c} = N_{\Phi^*}(\mathcal{C})$. The action of $(\mathcal{C}, H_K/K)$ on $u(\Phi;\mathfrak{a},\mathfrak{b})$ is thus given by

$$\begin{aligned} u(\mathfrak{a},\mathfrak{b})^{(\mathcal{C},H_K/K)} &= \left(\frac{u(\mathfrak{ab})}{u(\mathfrak{a})u(\mathfrak{b})}\right)^{(\mathcal{C},H_K/K)} \\ &= \frac{u(\mathfrak{ab})^{(\mathcal{C},H_K/K)}}{u(\mathfrak{a})^{(\mathcal{C},H_K/K)}u(\mathfrak{b})^{(\mathcal{C},H_K/K)}} \\ &= \frac{u(\mathfrak{abc})u(\mathfrak{c})}{u(\mathfrak{ac})u(\mathfrak{bc})}. \end{aligned}$$

18. Compute its minimal polynomial over K. Call this minimal polynomial $f(X)$.

    It is given by

$$f(X) = \prod_{\mathcal{C}} \left(X - u(\Phi;\mathfrak{a},\mathfrak{b})^{(\mathcal{C},H_K/K)}\right),$$

    where $\mathcal{C}$ runs through a complete set of representatives of $\mathrm{Cl}(K)$.

19. Find $g = f(X)\cdot\overline{f(X)}$.

    The coefficients of $g(X)$ are now in $K\bigcap\mathbb{R} = F$.

20. Try to recognize the coefficients of $g(X)$ as algebraic numbers in F.

    Here, we used the command `PowerRelation` provided by MAGMA. We increased the precision until the polynomial obtained by `PowerRelation` for a coefficient of $g(X)$ has roots in F.

21. Once this is done, let σ be the non-trivial automorphism of F. Compute $h(X) = g(X)\cdot g^{\sigma}(X)$.

    The polynomial $h(X)$ has coefficients in $\mathbb{Q}$ and $h(u(\Phi;\mathfrak{a},\mathfrak{b})) = 0$.

22. Factorize $h(X)$ and find the minimal polynomial of $u(\Phi;\mathfrak{a},\mathfrak{b})$ over $\mathbb{Q}$.

    The minimal polynomial of $u(\Phi;\mathfrak{a},\mathfrak{b})$ is a factor of $h(X)$.

23. Repeat steps 15 to 22 for all class invariants $u(\Phi;\mathfrak{c},\mathfrak{d})$.

See figure 8–1 to see the programming tree.

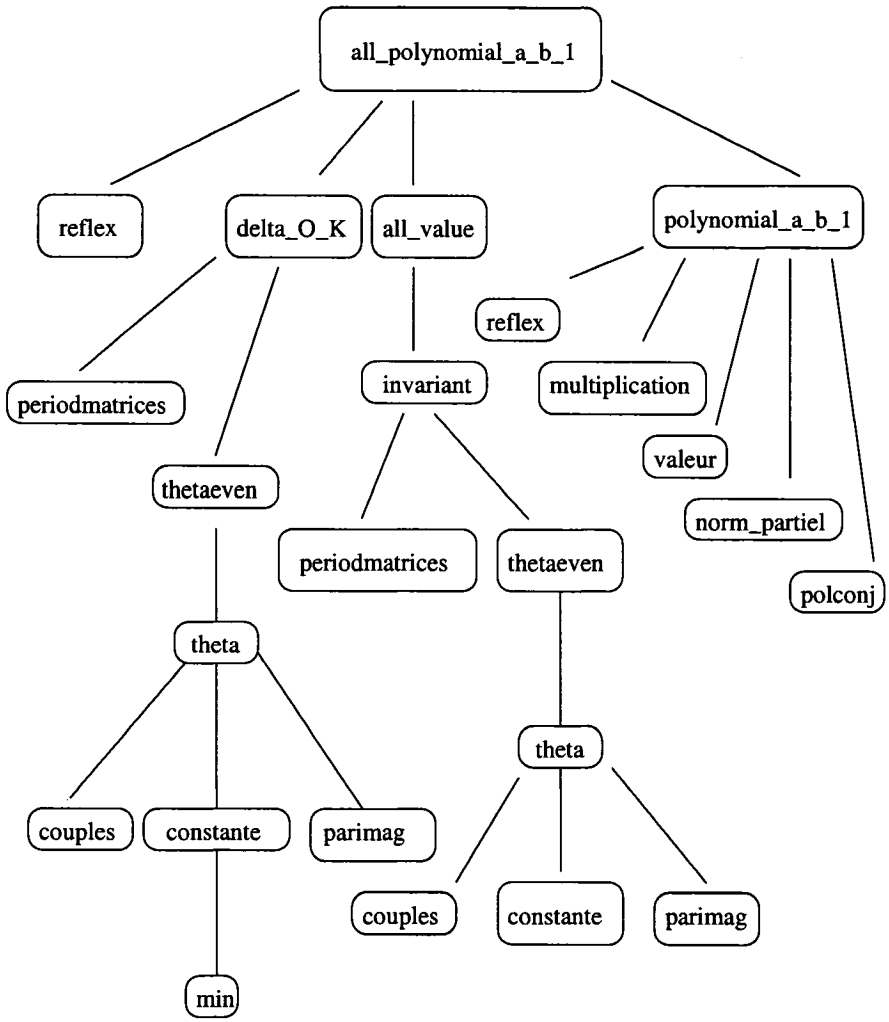

Figure 8–1: Programming tree

8.2 Description of the program

We give here a description of the functions in the program.

- `precision(precision)`
  - Input: Precision.
  - Output: No output.
  - Effect: Change the precision of the default real field. This will have an effect on the precision of the period matrices.
- `multiplication(field,ideal1,ideal2)`

- Input: Number field, ideal, ideal.
- Output: The multiplication of these two ideals.

- `cm_type(field)`
  - Input: Number field.
  - Output: A list of four elements. The first one is the list of the four embeddings. The second one is the list of the four CM-types. The third one is the list of the four embeddings, but abstractly. The last one is the list of the 4 CM-types, but abstractly.
- `reflex(field,automorphismsabstractly,cmtypeabstractly)`
  - Input: Field, set of automorphisms, CM-type (the abstract one here).
  - Output: The reflex type of `cmtypeabstractly` abstractly.
- `idealrep(field)`
  - Input: Number field.
  - Output: A list of representatives for the ideal class group.
- `parimag(matrix)`
  - Input: A two by two complex matrix.
  - Output: The imaginary part of that matrix.
- `nouvellematrice(A)`
  - Input: A two by two real matrix.
  - Output: New matrix as in [80].
- `couples(RealSymmetricMatrix,epsilon,constant)`
  - Input: A real symmetric matrix, a vector in $\mathbb{Z}^2$, a constant.
  - Output: The list of couple $n = (n1, n2) \in \mathbb{Z}^2$ such that $(n + \texttt{epsilon})^t \cdot \texttt{RealSymmetricMatrix} \cdot (n + \texttt{epsilon}) \leq \texttt{constant}$.
- `periodmatrices(CM-field,Real subfield,cmtype,ideal)`
  - Input: A CM-field, its real subfield, a CM-type, an ideal.
  - Output: A list of 3 matrices. In order: $\omega_1, \omega_2, \omega_2^{-1}\omega_1$.

- `min(realsymmetricmatrix)`
  - Input: A real symmetric matrix.
  - Output: The first successive minima of $\omega_2^{-1}\omega_1$.
- `constante(prec,Realsymmetricmatrix)`
  - Input: An integer, a real symmetric matrix.
  - Output: The constant we need in the function couples in order to have precision `prec` for the theta series.
- `theta(delta,epsilon,omega,precision)`
  - Input: The two characteristics delta and epsilon, the period matrix, precision.
  - Output: The value of $\theta\left[\begin{smallmatrix}\delta\\ \epsilon\end{smallmatrix}\right](0,\mathtt{omega})$.
- `thetaeven(omega,precision)`
  - Input: Period matrix, precision.
  - Output: The value of $\theta_{ev}(0,\mathtt{omega})$.
- `delta_0_K(cmfield,real subfield,cmtype,0_K,precision)`
  - Input: CM-field, real subfield, CM-types, the representative 1 of O_K, precision.
  - Output: The value of $\Delta(\mathtt{cmtype}(O_K))$, i.e. the denominator of the invariants $u(\Phi;\mathfrak{a})$.
- `invariant(K,F,cmtype,ideal,denominator,precision)`
  - Input: Clear (denominator is the value given by `delta_0_K`).
  - Output: The value of $u(\mathtt{cmtype};\mathtt{ideal})$.
- `all_value(K,F,cmtype,rep,denom,precision)`
  - Input: CM-field, real subfield, CM-type, representatives of the ideal class group, $\Delta(\mathtt{cmtype}(O_K))$, precision.
  - Output: A list containing the set of values $u(\mathtt{cmtype};\mathfrak{a})$ where $\mathfrak{a}$ runs through the representatives of the class group.

- `u_phi(K,F,cmtype,ideal1,ideal2,denom,precision)`
  - Input: Clear.
  - Output: The value of $u(\texttt{cmtype};\texttt{ideal1},\texttt{ideal2})$.
- `pol_conj(f)`
  - Input: A polynomial with complex coefficients $a_0 + a_1x + ...a_nx^n$.
  - Output: The polynomial with complex conjugates coefficients $\overline{a_0} + \overline{a_1}x + ... + \overline{a_n}x^n$.
- `valeur(K,rep,ideal)`
  - Input: CM-field, representatives, ideal.
  - Output: Find the ideal `rep[1]` for which `ideal` is equivalent to `rep[1]`. If $\texttt{ideal}(\texttt{rep[1]}^{-1}) = \alpha \cdot O_K$ then it returns two values, namely α and `1`.
- `norm_partiel(alpha,cmtype)`
  - Input: Number alpha, CM-type.
  - Output: The partial norm of alpha.
- `polynomial_a_b_1(K,F,cmtype,ideal1,ideal2,denom,precision,...`
  `automorphisme,cmtypeaut,rep,toutevaleur)`
  - Input: CM-field, real quadratic field, ideal1, ideal2, $\Delta(O_K)$, precision, abstract automorphisms, abstractcmtype, representatives, values of $u(\texttt{cmtype};\mathfrak{a})$ given by the function `all_value`.
  - Output: That function computes $f(x) = \prod_{\mathcal{C}}(x - u(a,b)^{(\mathcal{C},H_K/K)})$, where $\mathcal{C}$ runs over a complete set of representatives of $\mathrm{Cl}(K)$. Then $f(x)$ has coefficients in K. It computes then $f \cdot \overline{f} = g$ which has now coefficients in F. Then I use `PowerRelation` provide by MAGMA to recognize each coefficient as the root of a polynomial of degree 2 with coefficients in $\mathbb{C}$. There are three outputs: Coefficients of $f \cdot \overline{f} \in \mathbb{R}$, a list where each component is a list of three integers defining a polynomial of degree 2 for the corresponding coefficient of $f \cdot \overline{f}$, value of $u(\texttt{ideal1},\texttt{ideal2})$ in $\mathbb{C}$.

- `all_polynomial_a_b_1(K,F,cmtype,precision,automorphisme,...`
  `cmtypeaut,rep)`
  - Input: Clear.
  - Output: 5 things: List of the values of the $u(\mathfrak{a},\mathfrak{b})$, $\Delta(O_K)$, a list where each component is the first output of the function `polynomial_a_b_1`, a list where each component is the second output of the function `polynomial_a_b_1`, a list where each component is the third output of the function `polynomial_a_b_1`.
- `pol_over_Q(F,coef,pol,quad)`
  - Input: Real quadratic field, output (2) of `polynomial_a_b_1`, output (3) of `polynomial_a_b_1`, d, where $F = \mathbb{Q}(\sqrt{d})$.
  - Output: 3 things: If f is the polynomial given by `polynomial_a_b_1` with coefficients if F, then it ouputs the polynomial with coefficients in $\mathbb{Q}$: $f \cdot f^\sigma$, where σ is the quadratic conjugation in F, the coefficients of f in F, the coefficients of f^σ in F.

8.3 How to run the program

Put the program in a text file under a name (for example `invariant`). In the same folder, run magma, and type `load "invariant"`. Then you can use every function. Here is an example of a computation for the field $\mathbb{Q}(\sqrt{-5+\sqrt{5}})$.

```
[vallieres@scribe computation]$ magma
Magma V2.11-13     Wed Oct  5 2005 19:55:03     [Seed = 2492706851]
Type ? for help.  Type <Ctrl>-D to quit.
> load "invariant";
Loading "invariant"
> F := QuadraticField(5);
> G<y> := PolynomialRing(F);
> L<l> := ext<F|y^2 - (-5 + F.1)>;
```

```
> K<k> := AbsoluteField(L);
> precision_def(500);
> a1,a2,a3,a4 := cm_type(K);
> b := idealrep(K);
> u,delta,coef,coefseq,valeur := ...
           all_polynomial_a_b_1(K,F,a2[1],300,a3,a4[1],b);
1
0
> polQ := pol_over_Q(F,coef[1],coefseq[1],5);
> Factorization(polQ);
[
    <x - 1/14641, 8>
]
```

CHAPTER 9
Conclusion

The motivation of this thesis was **to see whether or not the DeShalit-Goren class invariants are global units**. Thanks to the numerical results presented in this thesis, we know now that they are not. On the other hand, we have today much information on the primes appearing in these class invariants. For example, a bound is known for these primes even though our numerical results suggest that it might be a little big. Another observation that is worth to point out is that apparently only few primes are an obstruction for these class invariants to be global units. At this point, we do not really understand this phenomena.

While working on this thesis, we asked ourselves several questions related with these class invariants.

First of all, it would be great to implement a program computing these invariants also in the non-Galois case.

Then it would be nice to find a link with Stark's conjectures. For this, a good understanding of Rubin's paper [56] is probably indispensable. It seems also that for a complete solution of these conjectures in the case where the base field is a CM-field of degre four, one would have to construct units in arbitrary ray class fields of the reflex field, not only in the Hilbert class field. In the proof of Stark's conjectures for the case where the base field is quadratic imaginary, the Kronecker's limit formulas were important. Konno found a limit formula for CM-fields in the paper [38]. The next step would be to connect this limit formula to the class invariants of this thesis.

Another possibility would be to try to generalize this construction to CM-fields of degree six and compare with the case treated in this master thesis.

Finally, the Shimura reciprocity law gives us the explicit action of the Galois group $\mathrm{Gal}(\overline{K}/K)$ on these invariants. It would be nice to generalize the Shimura reciprocity law to the group $\mathrm{Gal}(\overline{K}/\mathbb{Q})$. If this action were known, then it would have been possible to compute directly the minimal polynomial of the invariants $u(\Phi; \mathfrak{a}, \mathfrak{b})$ over $\mathbb{Q}$ instead of the minimal polynomial over K.

APPENDIX A
Program

```
precision_def := procedure(P)
    AssertAttribute(FldPr,"Precision",P);
end procedure;

corps1 := function(d,a,b)
    F<f> := QuadraticField(d);
    G<y> := PolynomialRing(F);
    L<l> := ext<F|y^2 - (a + b*f)>;
    K<k> := AbsoluteField(L);
return K,F;
end function;

multiplication := function(K,ideal1,ideal2)
    return ideal1*ideal2;
end function;

cm_type := function(K)
    C<i> := ComplexField();
    coef := Coefficients(DefiningPolynomial(K));
    rac := [Sqrt((-coef[3]+Sqrt(coef[3]^2 - 4 * coef[1]))/2),-Sqrt((-coef[3]+  ...
             ... Sqrt(coef[3]^2 - 4 * coef[1]))/2),Sqrt((-coef[3]-Sqrt(coef[3]^2 - 4 * ...
                 ...coef[1]))/2),-Sqrt((-coef[3]-Sqrt(coef[3]^2 - 4 * coef[1]))/2)];
    phi_1 := hom<K -> C | rac[1]>;
    phi_2 := hom<K -> C | rac[2]>;
    phi_3 := hom<K -> C | rac[3]>;
    phi_4 := hom<K -> C | rac[4]>;

    f := Automorphisms(K);
    for l := 1 to 4 do
            if f[l](K.1) eq -K.1 then
                    indiceconj := l;
            end if;
    end for;
    for l := 1 to 4 do
            if f[l](K.1) eq K.1 then
                    indiceid := l;
            end if;
    end for;
    aut_1 := f[indiceid];
    aut_2 := f[indiceconj];
    indicerestant := [];
    j := 1;
    for l := 1 to 4 do
            if l ne indiceconj and l ne indiceid then
                    indicerestant[j] := l;
                    j := j + 1;
            end if;
    end for;
    Cpre<i> := ComplexField(10);
    phi3_k := Cpre!phi_3(K.1);
    phi4_k := Cpre!phi_4(K.1);
    if  Imaginary(Cpre!phi_1(f[indicerestant[1]](K.1)))*i eq phi3_k then
            aut_3 := f[indicerestant[1]];
            aut_4 := f[indicerestant[2]];
    end if;
    if Imaginary(Cpre!phi_1(f[indicerestant[1]](K.1)))*i eq phi4_k then
            aut_4 := f[indicerestant[1]];
```

```
            aut_3 := f[indicerestant[2]];
    end if;

return [phi_1,phi_2,phi_3,phi_4],[[phi_1,phi_3],[phi_1,phi_4],[phi_2,phi_3],[phi_2,phi_4]],...
              ...[aut_1,aut_2,aut_3,aut_4],[[aut_1,aut_3],[aut_1,aut_4],[aut_2,aut_3],[aut_2,aut_4]];
end function;

reflex := function(K,automorphismes,cmtype)
    bidon := [];
    for l:= 1 to 4 do
        if (cmtype[1]^(-1))(K.1) eq automorphismes[l](K.1) then
            bidon[1] := automorphismes[l];
        end if;
    end for;
    for l:=1 to 4 do
        if (cmtype[2]^(-1))(K.1) eq automorphismes[l](K.1) then
            bidon[2] := automorphismes[l];
        end if;
    end for;
return bidon;
end function;

idealrep := function(K)
    Cl, homo := ClassGroup(K);
    representative := [];
    l := 1;
    for x in Cl do
        representative[l] := homo(x);
        l := l + 1;
    end for;
return representative;
end function;

parimag := function(A)
    return Matrix(RealField(),2,2,[Imaginary(A[i,j]):i,j in [1..2]]);
end function;

nouvellematrice := function(A)
    R := RealField();
    Q := Matrix(R,2,2,[A[1,1],A[1,2]/A[1,1],0,A[2,2] - ((A[1,2]^2)/A[1,1])]);
    return Q;
end function;

couples := function(B,epsilon,constante)
    A := nouvellematrice(B);
    R := RealField();
    liste := [];
    T := [];
    U := [];
    x := [];
    OS := [];
    l := 1;
    i := 2;
    T[2] := R!constante;
    U[2] := R!0;
    while i le 2 do
        bool_value := 1;
        Z := Sqrt(T[i]/A[i,i]);
        OS[i] := Floor(Z - U[i] - epsilon[i]);
        x[i] := Ceiling(-Z - U[i] - epsilon[i]) - 1;
        while bool_value eq 1 and i le 2 do
            x[i] := x[i] + 1;
            if x[i] le OS[i] then
                if i eq 1 then
                    liste[l] := x;
                    l := l + 1;
                else
                    i := i - 1;
```

```
                U[i] := A[1,2]*(x[2] + epsilon[2]);
                T[i] := constante - A[i+1,i+1]*(x[i+1] + epsilon[i+1] + U[i+1]);
                bool_value := 0;
            end if;
        else
            i := i + 1;
        end if;
    end while;
end while;

return liste;
end function;

periodmatrices := function(K,F,cmtype,ideal)
    C<i> := ComplexField();
    n := FundamentalUnit(F);

    /* Now I choose a good generator for the different */

    O := MaximalOrder(K);
    D := Different(O);
    bool,deltaprime := IsPrincipal(D);
    n1 := elt<K|n>;
    if Imaginary(cmtype[1](deltaprime))*Imaginary(cmtype[2](deltaprime)) gt 0 then
        if Imaginary(cmtype[1](deltaprime)) gt 0 then
            delta := deltaprime;
        else
            delta := -deltaprime;
        end if;
    else
        if Imaginary(cmtype[1](deltaprime)) gt 0 then
            if Real(cmtype[1](n1)) gt 0 then
                delta := n1*deltaprime;
            else
                delta := -n1*deltaprime;
            end if;
        else
            if Real(cmtype[1](n1)) gt 0 then
                delta := -n1*deltaprime;
            else
                delta := n1*deltaprime;
            end if;
        end if;
    end if;

    /* Find the complex conjugation.  It's the one such that f(k) = -k */

    G := Automorphisms(K);
    for l := 1 to 4 do              /* Since [K:Q] = 4 */
        if G[l](K.1) eq -K.1 then
            conj := G[l];
        end if;
    end for;

    /* Find representatives of A * conj(A) */

    bool, aprime := IsPrincipal(ideal*conj(ideal));

    if bool eq false then
        return "a*conj(a) is not principal.  Check if the class number of the real field is 1";
    end if;

    /* Now we want to find a representative which is totally positive */

    if Real(cmtype[1](aprime))*Real(cmtype[2](aprime)) gt 0 then
        if Real(cmtype[1](aprime)) gt 0 then
            a := aprime;
        else
```

```
        a := -aprime;
    end if;
else
    if Real(cmtype[1](aprime)) gt 0 then
        if Real(cmtype[1](n1)) gt 0 then
            a := n1*aprime;
        else
            a := -n1*aprime;
        end if;
    else
        if Real(cmtype[1](n1)) gt 0 then
            a := -n1*aprime;
        else
            a := n1*aprime;
        end if;
    end if;
end if;

/* Now, we want to define the Riemann form */

K2 := CartesianProduct(K,K);
riemannform := map<K2 -> C | x :->  Trace((a*delta)^(-1)*conj(x[1])*x[2])>;

/* Now I want to find the symplectic basis */

baseprime := BasisMatrix(ideal);
alpha := [];
alpha[1] := RowSequence(baseprime)[1];
alpha[2] := RowSequence(baseprime)[2];
alpha[3] := RowSequence(baseprime)[3];
alpha[4] := RowSequence(baseprime)[4];
E := Matrix(IntegerRing(),4,4,[riemannform(O!alpha[i],O!alpha[j]):i,j in [1..4]]);

eta1 := Matrix(IntegerRing(),1,4,[1,0,0,0]);

V := Vector(1,[-1]);
tampon := Matrix(IntegerRing(),1,3,[(E*Transpose(eta1))[j,1]:j in [2..4]]);
e1prime := Solution(Transpose(tampon),V);

e1 := Matrix(IntegerRing(),1,4,[0,e1prime[1],e1prime[2],e1prime[3]]);

A := HorizontalJoin(E*Transpose(eta1),E*Transpose(e1));
B := Vector(2,[0,0]);
_,noyau := Solution(A,B);
e2prime := Matrix(IntegerRing(),1,4,[Basis(noyau)[1][j]:j in [1..4]]);
eta2prime := Matrix(IntegerRing(),1,4,[Basis(noyau)[2][j]:j in [1..4]]);
passage := Transpose(Matrix(IntegerRing(),4,4,alpha));
coeff_max_order_e2 := passage * Transpose(e2prime);
coeff_max_order_eta2 := passage * Transpose(eta2prime);
e2primesuite := [coeff_max_order_e2[j,1]:j in [1..4]];
eta2primesuite := [coeff_max_order_eta2[j,1]:j in [1..4]];

if riemannform(O!e2primesuite,O!eta2primesuite) eq -1 then
    e2 := e2prime;
    eta2 := eta2prime;
else
    e2 := eta2prime;
    eta2 := e2prime;
end if;

nouvellebase := [passage*Transpose(e1),passage*Transpose(e2),passage*Transpose(eta1),...
        ...passage*Transpose(eta2)];
symplecticbasis := [[nouvellebase[l][m,1]:m in [1..4]]:l in [1..4]];

/* Find the period matrix */

omega1 := Matrix(C,2,2,[cmtype[i](O!symplecticbasis[j]):i,j in [1..2]]);
omega2 := Matrix(C,2,2,[cmtype[i](O!symplecticbasis[j+2]):i,j in [1..2]]);
```

```
    bigomega := HorizontalJoin(omega1,omega2);
    omega2_inv_omega1 := omega2^(-1) * omega1;

return [omega1,omega2,omega2_inv_omega1],symplecticbasis;
end function;

min := function(A)
    R := RealField();
    a := [1,0];
    b := [0,1];
    aval := Matrix(R,2,1,a);
    bval := Matrix(R,2,1,b);
    e1 := Transpose(aval)*A*aval;
    e2 := Transpose(bval)*A*bval;
    liste := [e1[1,1],e2[1,1]];
    bon, mauvais := Maximum(liste);
    bidon := bon;
    l := 1;
    liste1 := couples(A,[0,0],bon);
    while l le #liste1 do
        changetype := Matrix(R,2,1,liste1[l]);
        formematricielle := Transpose(changetype)*A*changetype;
        if formematricielle[1,1] le bidon and liste1[l] ne [0,0] then
            bidon := formematricielle[1,1];
        end if;
            l := l + 1;
    end while;
return bidon;
end function;

constante := function(s,A)
    C := s + 0.35 - 2 * Log(10,min(A));
    if C ge 75 then
        C := 1/2*( s + 0.35 - 2 * Log(10,min(A)));
    end if;
return C;
end function;

theta := function(del,ep,Omega,precision)
    C<i> := ComplexField();

    sommation := couples(parimag(Omega),del,constante(precision,parimag(Omega)));
    del1 := Matrix(C,2,1,del);
    ep1 := Matrix(C,2,1,ep);

    bidon := 0;
    l := 1;
    while l le #sommation do
        mat := Matrix(C,2,1,sommation[l]);
        partiel := Transpose(mat + del1)*Omega*(mat + del1);
        partiel2 := Transpose(mat + del1)*ep1;
        bidon1 := Exp(Pi(C)*i*(partiel[1,1] + 2*partiel2[1,1]));
        bidon := bidon + bidon1;
        l := l + 1;
    end while;

return bidon;
end function;

thetaeven := function(Omega,precision)
    duo1 := [0,0];
    duo2 := [0,1/2];
    duo3 := [1/2,0];
    duo4 := [1/2,1/2];
    thetabidon := [[duo1,duo1],[duo1,duo3],[duo1,duo2],[duo1,duo4],[duo3,duo1],[duo3,duo2],...
              ...[duo2,duo1],[duo2,duo3],[duo4,duo1],[duo4,duo4]];

    l := 1;
```

```
    bidon := 1;
    while l le 10 do
        bidon1 := theta(thetabidon[l][1],thetabidon[l][2],Omega,precision);
        bidon := bidon * bidon1;
        l := l + 1;
    end while;
return bidon;
end function;

/* To be faster we first compute Delta(O_K) and we give it to the function when we call it */

delta_O_K := function(K,F,cmtype,prin,precision)
    B := periodmatrices(K,F,cmtype,prin);
    l,m := HasAttribute(FldPr,"Precision");
    heu := ChangeRing(B[3],ComplexField(m));
    heu,heu1 := To2DUpperHalfSpaceFundamentalDomian(heu);
    C := Matrix(ComplexField(),2,2,[heu1[3,1],heu1[3,2],heu1[4,1],heu1[4,2]]);
    D := Matrix(ComplexField(),2,2,[heu1[3,3],heu1[3,4],heu1[4,3],heu1[4,4]]);
    heu := ChangeRing(heu,ComplexField());
    facteur := Determinant(C*B[3] + D)^(-10);
return facteur*Determinant(B[2])^(-10)*(thetaeven(heu,precision)^2);
end function;

invariant := function(K,F,cmtype,ideal,denom,precision)
    A := periodmatrices(K,F,cmtype,ideal);
    l,m := HasAttribute(FldPr,"Precision");
    hip := ChangeRing(A[3],ComplexField(m));
    hip,hip1:= To2DUpperHalfSpaceFundamentalDomian(hip);
    C := Matrix(ComplexField(),2,2,[hip1[3,1],hip1[3,2],hip1[4,1],hip1[4,2]]);
    D := Matrix(ComplexField(),2,2,[hip1[3,3],hip1[3,4],hip1[4,3],hip1[4,4]]);
    hip := ChangeRing(hip,ComplexField());
    facteur := Determinant(C*A[3] + D)^(-10);
    numer := facteur*Determinant(A[2])^(-10)*(thetaeven(hip,precision)^2);
return numer/denom;
end function;

all_value := function(K,F,cmtype,rep,denom,precision)
    C<i> := ComplexField();
    h := ClassNumber(K);
    liste := [];

    for l:= 1 to h do
        print h-l;
            liste[l] := invariant(K,F,cmtype,rep[l],denom,precision);
    end for;
    return liste;
end function;

u_phi := function(K,F,cmtype,ideal1,ideal2,denom,precision)
    if ideal1 ne ideal2 then
        produit := multiplication(K,ideal1,ideal2);
        bidon := (invariant(K,F,cmtype,produit,denom,precision)/...
        ... (invariant(K,F,cmtype,ideal1,denom, precision)*...
   ...invariant(K,F,cmtype,ideal2,denom,precision)));
    else
        produit := multiplication(K,ideal1,ideal2);
        bidon := (invariant(K,F,cmtype,produit,denom,precision)/...
        ... (invariant(K,F,cmtype,ideal1,denom,precision))^2);
    end if;
return bidon;
end function;

/*  Here is a procedure to compute the polynomial over the real field */

pol_conj := function(f)
    C<i> := ComplexField();
    Q<x> := PolynomialRing(C);
    deg := Degree(f);
```

```
    coef := Coefficients(f);
    g := 0;
    for l:= 1 to deg + 1 do
        g := g + ComplexConjugate(coef[l])*x^(l-1);
    end for;
return g;
end function;

valeur := function(K,rep,ideal)
    h := ClassNumber(K);
    bool := false;
    l := 1;
    while bool eq false do
        bool,a  := IsPrincipal(ideal*(rep[l]^(-1)));
        l := l+1;
    end while;
return K!a,l-1;
end function;

norm_partiel := function(alpha,cmtype)
    return (cmtype[1](alpha) * cmtype[2](alpha));
end function;

polynomial_a_b_1 := function(K,F,cmtype,ideal1,ideal2,denom,precision,automorphisme,...
            ...cmtypeaut,rep,toutevaleur)
    bool,prec := HasAttribute(FldPr,"Precision");
    C<i> := ComplexField();
    Q<x> := PolynomialRing(C);
    ref := reflex(K,automorphisme,cmtypeaut);
    h := ClassNumber(K);
    hip := [];
    for l := 1 to h do
        c := multiplication(K,ref[1](rep[l]),ref[2](rep[l]));
        ab := multiplication(K,ideal1,ideal2);
        abc := multiplication(K,ab,c);
        ac := multiplication(K,ideal1,c);
        bc := multiplication(K,ideal2,c);

        val_c,num_c := valeur(K,rep,c);
        val_abc,num_abc := valeur(K,rep,abc);
        val_ac,num_ac := valeur(K,rep,ac);
        val_bc,num_bc := valeur(K,rep,bc);
        hip[l] := ((norm_partiel(val_abc^(-1),cmtype)^10)*toutevaleur[num_abc] *...
 ...(norm_partiel(val_c^(-1),cmtype)^10)*toutevaleur[num_c])/...
   ...((norm_partiel(val_ac^(-1),cmtype)^10)*...
     ...toutevaleur[num_ac](norm_partiel(val_bc^(-1),cmtype)^10)*toutevaleur[num_bc]);
    end for;
    g := 1;
    for l:=1 to h do
        g := g*(x-hip[l]);
    end for;
    f := pol_conj(g);

    liste := Coefficients(f*g);
    bidonpol := [];
    precision_def(precision);
        for l:=1 to 2*h do
            bidonpol[l] := Q!PowerRelation(liste[l],2);
        end for;
    bidonpolcoef := [];
        for l:=1 to 2*h do
            bidonpolcoef[l] := Coefficients(bidonpol[l]);
        end for;
    precision_def(prec);
    nombre := hip[1];

return Coefficients(f*g),bidonpolcoef,nombre;
end function;
```

```
all_polynomial_a_b_1 := function(K,F,cmtype,precision,automorphisme,cmtypeaut,rep)
    bool,prec := HasAttribute(FldPr,"Precision");
    C<i> := ComplexField();
    Q<x> := PolynomialRing(C);
    ref := reflex(K,automorphisme,cmtypeaut);
    h := ClassNumber(K);
    denom := delta_0_K(K,F,cmtype,rep[1],precision);
    liste := all_value(K,F,cmtype,rep,denom,precision);

    h := ClassNumber(K);
    liste1 := [];
    liste2 := [];
    liste3 := [];
    y := 1;
    for l:=2 to h do
        z := l;
        while z le h do
            liste1[y],liste2[y],liste3[y] := polynomial_a_b_1(K,F,cmtype,rep[l],rep[z],denom,...
                      ...precision,automorphisme,cmtypeaut,rep,liste);
            y := y + 1;
            z := z + 1;
        end while;
    end for;
return liste,denom,liste1,liste2,liste3;
end function;

signe := function(F,ele,nombre,quad)
    d := Sqrt(quad);
    elesuite := ElementToSequence(ele);
    hip := elesuite[1] + d*elesuite[2];
    hip1 := elesuite[1] - d*elesuite[2];
    P := 50;
    R := RealField(P);
    nombreprime := R!Real(nombre);
    hipprime := R!hip;
    hip1prime := R!hip1;
    if hipprime eq nombreprime then
        return ele;
    else
        if hip1prime eq nombreprime then
            return (elesuite[1] - elesuite[2]*F.1);
        else
            return "achtung,achtung!!";
        end if;
    end if;
end function;

pol_over_Q := function(F,coef,pol,quad)
    G<y> := PolynomialRing(F);
    longueur := #pol;
    Q<x> := PolynomialRing(RationalField());
    for l := 1 to longueur do
        if IsIrreducible(Q!pol[l]) ne true then
            return "achtung pol_over_Q_1!  Some polynomial are not irreducible!!",_,_;
        end if;
    end for;
    alpha := [];
    for l := 1 to longueur do
        field := NumberField(Q!pol[l]);
        if #pol[l] ne 2 then
        bool,appli := IsIsomorphic(field,F);
            if bool eq true then
                alpha[l] := signe(F,appli(field.1),coef[l],quad);
            else
                return "Achtung in function pol_over_Q_2.  Increase the precision!",_,_;
            end if;
        else
```

```
            alpha[l] := F![-pol[l][1]/pol[l][2],0];
        end if;
    end for;
    alpha[longueur + 1] := 1;
    beta := [];

    for l:=1 to longueur do
        if #pol[l] ne 2 then
            beta[l] := F![ElementToSequence(alpha[l])[1],-ElementToSequence(alpha[l])[2]];
        else
            beta[l] := alpha[l];
        end if;
    end for;
    beta[longueur+1] := 1;
    reponse := Q!(G!alpha * G!beta);
return reponse,alpha,beta;
end function;
```

APPENDIX B
Results

B.1 Quartic cyclic CM-fields with class number 2

There are exactly eight quartic cyclic CM-fields with class number two. We computed the class invariants for all of them.

★

I.	Field :	$K = \mathbb{Q}(\sqrt{-5+\sqrt{5}})$
	Defining polynomial:	$x^4 + 10x^2 + 20$
	Bound:	40000
	Integral basis:	$[1, x, \frac{1}{2}x^2, \frac{1}{2}x^3]$
	Rep. for Cl(K):	• O_K
		• $\mathfrak{a} = ([[2,0,0,0],[0,1,0,0]])$
	$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$:	0.000068301345536...
	Minimal pol. over $\mathbb{Q}$:	$t - \frac{1}{14641}$
	Factorization:	$14641^{-1} = 11^{-4}$

II.	Field:	$K = \mathbb{Q}(\sqrt{-6+3\sqrt{2}})$
	Defining polynomial:	$x^4 + 12x^2 + 18$
	Bound:	9216
	Integral basis:	$[1, x, \frac{1}{3}x^2, \frac{1}{3}x^3]$
	Rep. for Cl(K):	• O_K
		• $([2,0,0,0],[0,1,0,0])$
	$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$:	0.000866551777220...
	Minimal pol. over $\mathbb{Q}$:	$t^2 - 1154 \cdot t + 1$
	Factorization in $\mathbb{Q}(\sqrt{2})$:	unit

III.	Field:	$K = \mathbb{Q}(\sqrt{-65+26\sqrt{5}})$
	Defining polynomial:	$x^4 + 130x^2 + 845$
	Bound:	6760000
	Integral basis:	$[1, \frac{1}{2}(x+1), \frac{1}{52}(x^2+39), \frac{1}{104}(x^3+x^2+39x+39)]$
	Rep. for Cl(K):	• O_K
		• $([5,0,0,0],[-1,2,0,0])$
	$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$:	0.000000005610331...
	Minimal pol. over $\mathbb{Q}$:	$t - \frac{14641}{2609649624481}$
	Factorization:	$14641 \cdot (2609649624481)^{-1} = 11^4 \cdot 31^{-4} \cdot 41^{-4}$

IV. Field: $K = \mathbb{Q}(\sqrt{-65 + 10\sqrt{13}})$
Defining polynomial: $x^4 + 130x^2 + 2925$
Bound: 45697600
Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{20}(x^2+15), \frac{1}{120}(x^3+3x^2+55x+45)]$
Rep. for $\mathrm{Cl}(K)$:
- O_K
- $([5,0,0,0],[1,3,0,0])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.000000126734986...
Minimal pol. over $\mathbb{Q}$: $t - \frac{1}{7890481}$
Factorization: $7890481^{-1} = 53^{-4}$

V. Field: $K = \mathbb{Q}(\sqrt{-10 + 5\sqrt{2}})$
Defining polynomial: $x^4 + 20x^2 + 50$
Bound: 25600
Integral basis: $[1, x, \frac{1}{5}x^2, \frac{1}{5}x^3]$
Rep. for $\mathrm{Cl}(K)$:
- O_K
- $([2,0,0,0],[0,1,0,0])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.000011973036721...
Minimal pol. over $\mathbb{Q}$: $t - \frac{1}{83521}$
Factorization: $83521^{-1} = 17^{-4}$

VI. Field: $K = \mathbb{Q}(\sqrt{-85 + 34\sqrt{5}})$
Defining polynomial: $x^4 + 170x^2 + 1445$
Bound: 11560000
Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{68}(x^2+51), \frac{1}{136}(x^3+x^2+51x+51)]$
Rep. for $\mathrm{Cl}(K)$:
- O_K
- $([5,0,0,0],[-1,2,0,0])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 4.436167004826079...
Minimal pol. over $\mathbb{Q}$: $t - \frac{25411681}{572829674183924641}$
Factorization: $25411681 \cdot 572829674183924641^{-1} = 71^4 \cdot 11^{-4} \cdot 41^{-4} \cdot 61^{-4}$

VII. Field: $K = \mathbb{Q}(\sqrt{-13 + 3\sqrt{13}})$
Defining polynomial: $x^4 + 26x^2 + 52$
Bound: 1827904
Integral basis: $[1, x, \frac{1}{6}(x^2+4), \frac{1}{6}(x^3+4x)]$
Rep. for $\mathrm{Cl}(K)$:
- O_K
- $([2,0,0,0],[0,1,0,0])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.000000003395586...
Minimal pol. over $\mathbb{Q}$: $t - \frac{1}{294499921}$
Factorization: $294499921^{-1} = 131^{-4}$

VIII. Field: $K = \mathbb{Q}(\sqrt{-119 + 28\sqrt{17}})$
Defining polynomial: $x^4 + 238x^2 + 833$
Bound: 261921856
Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{56}(x^2+35), \frac{1}{112}(x^3+x^2+35x+35)]$
Rep. for $\mathrm{Cl}(K)$:
- O_K
- $([7,0,0,0],[1,5,0,0])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 1.215349828304578...
Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{73930664135570539887406840 97}{8985161996360911 36} \cdot t + 1$
Factorization in $\mathbb{Q}(\sqrt{17})$: $P_{2,1}^8 \cdot P_{2,2}^{-8} \cdot P_{43,1}^4 \cdot P_{43,2}^{-4} \cdot P_{179,1}^4 \cdot P_{179,2}^{-4}$

B.2 Quartic cyclic CM-fields with class number 4

There are exactly 13 quartic cyclic CM-fields with the properties we want. We computed the class invariants for all of them. For each of these class invariants u, we computed the factorization of $u \cdot O_L$ where $L = \mathbb{Q}(u)$. The symbol $P_{p,n}$ denotes a prime of L lying above the rational prime p.

★

I.

Field:	$K = \mathbb{Q}(\sqrt{-15+6\sqrt{5}})$
Defining polynomial:	$x^4 + 30x^2 + 45$
Bound:	360000
Integral basis:	$[1, x, \frac{1}{12}(x^2+9), \frac{1}{12}(x^3+9x)]$
Rep. for Cl(K):	• O_K • $\mathfrak{a} = ([3,0,0,0],[0,1,0,0])$ • $\mathfrak{b} = ([2,0,0,0],[1,1,0,0])$ • $\mathfrak{c} = ([6,0,0,0],[30,34,33,1])$
$u(\Phi;\mathfrak{a}^{-1},\mathfrak{a}^{-1})$:	0.000000098473203...
Minimal pol. over $\mathbb{Q}$:	$t^2 - \frac{10155047}{923521} \cdot t + \frac{1}{923521}$
Factorization:	$P_{31,1}^{-4}$
$u(\Phi;\mathfrak{a}^{-1},\mathfrak{b}^{-1})$:	0.001040582726326...
Minimal pol. over $\mathbb{Q}$:	$t - \frac{1}{961}$
Factorization:	$P_{31,1}^{-4} \cdot P_{31,2}^{-4}$
$u(\Phi;\mathfrak{a}^{-1},\mathfrak{c}^{-1})$:	0.000094632748485...
Minimal pol. over $\mathbb{Q}$:	$t^2 - \frac{10155047}{961} \cdot t + 1$
Factorization:	$P_{31,1}^{-2} \cdot P_{31,2}^{2}$
$u(\Phi;\mathfrak{b}^{-1},\mathfrak{b}^{-1})$:	0.000000048054000...
Minimal pol. over $\mathbb{Q}$:	$t^2 - \frac{20809922}{923521} \cdot t + \frac{1}{923521}$
Factorization:	$P_{31,2}^{-4}$
$u(\Phi;\mathfrak{b}^{-1},\mathfrak{c}^{-1})$:	0.000046179894477...
Minimal pol. over $\mathbb{Q}$:	$t^2 - \frac{20809922}{961} \cdot t + 1$
Factorization:	$P_{31,1}^{2} \cdot P_{31,2}^{-2}$
$u(\Phi;\mathfrak{c}^{-1},\mathfrak{c}^{-1})$:	0.000000004370130...
Minimal pol. over $\mathbb{Q}$:	$t^2 - 228826127 \cdot t + 1$
Factorization:	unit

II. Field: $K = \mathbb{Q}(\sqrt{-17+4\sqrt{17}})$

Defining polynomial: $x^4 + 34x^2 + 17$

Bound: 5345344

Integral basis: $[1, x, \frac{1}{8}(x^2-3), \frac{1}{8}(x^3+x^2-3x-3)]$

Rep. for $\mathrm{Cl}(K)$:
- O_K
- $\mathfrak{a} = ([2,0,0,0],[1,1,1,0])$
- $\mathfrak{b} = ([2,0,0,0],[0,1,1,0])$
- $\mathfrak{c} = ([2,0,0,0],[3,3,2,2])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.000066349314922...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{18023839694417}{9759362}t^3 + \frac{205985001591681}{78074896}x^2 - \frac{148798913105}{9759362}x + 1$

Factorization: $P_{2,1}^2 \cdot P_{2,2}^{-2} \cdot P_{47,1}^{-4} \cdot P_{47,2}^4$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 11.069576293863622...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{98609}{8836}t + 1$

Factorization: $P_{2,1}^{-2} \cdot P_{2,2}^2 \cdot P_{47,1}^{-2} \cdot P_{47,2}^2$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.000005993844132...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{368579716}{2209}t^3 + \frac{12873474384774}{4879681}t^2 - \frac{368579716}{2209}t + 1$

Factorization: $P_{47,1}^{-2} \cdot P_{47,2}^2 \cdot P_{47,3}^2 \cdot P_{47,4}^{-2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 0.702860141688946...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{148798913105}{9759362}t^3 + \frac{205985001591681}{78074896}t^2 - \frac{18023839694417}{9759362}t + 1$

Factorization: $P_{2,1}^2 \cdot P_{2,2}^{-2} \cdot P_{47,1}^4 \cdot P_{47,2}^{-4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.063494764662182...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{368579716}{2209}t^3 + \frac{12873474384774}{4879681}t^2 - \frac{368579716}{2209}t + 1$

Factorization: $P_{47,1}^2 \cdot P_{47,2}^{-2} \cdot P_{47,3}^2 \cdot P_{47,4}^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 0.000000380577722...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{12873464625412}{4879681}t^3 + \frac{135825260107630470}{4879681}t^2 - \frac{12873464625412}{4879681}t + 1$

Factorization: $P_{47,1}^4 \cdot P_{47,2}^{-4}$

III. Field: $K = \mathbb{Q}(\sqrt{-105 + 42\sqrt{5}})$

Defining polynomial: $x^4 + 210x^2 + 2205$

Bound: 17640000

Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{84}(x^2+63), \frac{1}{168}(x^3+x^2+63x+63)]$

Rep. for Cl(K):
- O_K
- $\mathfrak{a} = ([3,0,0,0],[1,1,0,0])$
- $\mathfrak{b} = ([5,0,0,0],[-1,2,0,0])$
- $\mathfrak{c} = ([15,0,0,0],[220,1,224,224])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 1.857285586735647...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{53842015850642}{5498121804761041}t + \frac{1}{5498121804761041}$

Factorization: $P_{79}^{-4} \cdot P_{109}^{-4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 0.000001377164651...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{53842015850642}{74149321}t + 1$

Factorization: $P_{79,1}^{-2} \cdot P_{79,2}^{2} \cdot P_{109,1}^{-2} \cdot P_{109,2}^{2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.000000013486300...

Minimal pol. over $\mathbb{Q}$: $t - \frac{1}{74149321}$

Factorization: $74149321^{-1} = 79^{-2} \cdot 109^{-2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 5.954938537669610...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{24586315891229282}{14641}t + 1$

Factorization: $P_{11,1}^{4} \cdot P_{11,2}^{-4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.000000432405706...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{25106519019566095 22}{1085620208761}t + 1$

Factorization: $P_{11,1}^{-4} \cdot P_{11,2}^{4} \cdot P_{79,1}^{2} \cdot P_{79,2}^{-2} \cdot P_{109,1}^{-2} \cdot P_{109,2}^{2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 5.831553147050240...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{2510651901956609522}{804980013435064012 81}t + \frac{1}{5498121804761041}$

Factorization: $P_{11,1}^{-4} \cdot P_{11,4}^{2} \cdot P_{79}^{-4} \cdot P_{109}^{-4}$

IV. Field: $K = \mathbb{Q}(\sqrt{-14+7\sqrt{2}})$

Defining polynomial: $x^4 + 28x^2 + 98$

Bound: 50176

Integral basis: $[1, x, \frac{1}{7}x^2, \frac{1}{7}x^3]$

Rep. for Cl(K):

- O_K
- $\mathfrak{a} = ([7,0,0,0],[2,1,6,0])$
- $\mathfrak{b} = ([2,0,0,0],[0,1,0,0])$
- $\mathfrak{c} = ([14,0,0,0],[24,1,2,194])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.000000000927464...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{1092526569053864921738377 1716}{18442932323956519729}t^3 + \frac{1028404704063672221077851309923450541173479878}{4072529695597996115767741417439521}t^2 - \frac{19885336741405849536945104452}{18442932323956519729}t + 1$

Factorization: $P_{7,1}^2 \cdot P_{7,2}^{-2} \cdot P_{17,3}^{-4} \cdot P_{17,4}^4 \cdot P_{31,1}^{-4} \cdot P_{31,2}^{-4} \cdot P_{31,3}^4 \cdot P_{31,4}^4 \cdot P_{47,1}^{-4} \cdot P_{47,2}^4 \cdot P_{47,3}^{-4} \cdot P_{47,4}^4$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 0.000466063228750...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{56516}{17}t^3 + \frac{211254318726}{83521}t^2 - \frac{56516}{17}t + 1$

Factorization: $P_{17,1}^{-2} \cdot P_{17,2}^2 \cdot P_{17,3}^{-2} \cdot P_{17,4}^2$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.000001989996339...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{320685890429201712313 94}{63816374823378961}t + 1$

Factorization: $P_{7,1}^{-2} \cdot P_{7,2}^2 \cdot P_{17,1}^2 \cdot P_{17,2}^{-2} \cdot P_{31,1}^{-4} \cdot P_{31,2}^4 \cdot P_{47,1}^{-4} \cdot P_{47,2}^4$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 0.000000395358280...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{211254151684}{83521}t^3 + \frac{500574365574}{83521}t^2 - \frac{211254151684}{83521}t + 1$

Factorization: $P_{17,2}^4 \cdot P_{17,3}^{-4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.000848293228291...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{56516}{17}t^3 + \frac{211254318726}{83521}t^2 - \frac{56516}{17}t + 1$

Factorization: $P_{17,1}^{-2} \cdot P_{17,2}^2 \cdot P_{17,3}^2 \cdot P_{17,4}^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 0.000000001688100...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{19885336741405849536945104452}{18442932323956519729}t^3 + \frac{1028404704063672221077851309923450541173479878}{4072529695597996115767741417439521}t^2 - \frac{1092526569053864921738377 1716}{18442932323956519729}t + 1$

Factorization: $P_{7,1}^2 \cdot P_{7,2}^{-2} \cdot P_{17,1}^4 \cdot P_{17,2}^{-4} \cdot P_{31,1}^4 \cdot P_{31,2}^4 \cdot P_{31,3}^{-4} \cdot P_{31,4}^{-4} \cdot P_{47,1}^4 \cdot P_{47,2}^4 \cdot P_{47,3}^{-4} \cdot P_{47,4}^{-4}$

V. Field: $K = \mathbb{Q}(\sqrt{-15+3\sqrt{5}})$

Defining polynomial: $x^4 + 30x^2 + 180$

Bound: 360000

Integral basis: $[1, x, \frac{1}{6}x^2, \frac{1}{6}x^3]$

Rep. for $\mathrm{Cl}(K)$:

- O_K
- $\mathfrak{a} = ([3,0,0,0],[0,1,0,0])$
- $\mathfrak{b} = ([2,0,0,0],[0,1,0,0])$
- $\mathfrak{c} = ([6,0,0,0],[12,1,24,35])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 2.448552006301927...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{377170261290387352127}{44928340772666930881}t + \frac{1}{48648964964161}$

Factorization: $P_{19,1}^{-4} \cdot P_{31,1}^{4} \cdot P_{31,2}^{-4} \cdot P_{139,1}^{-4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 0.000000143371621...

Minimal pol. over $\mathbb{Q}$: $t - \frac{1}{6974881}$

Factorization: $P_{19,1}^{-2} \cdot P_{19,2}^{-2} \cdot P_{139,1}^{-2} \cdot P_{139,2}^{-2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.000000017078358...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{377170261290387352127}{6441449076001}t + 1$

Factorization: $P_{19,1}^{-2} \cdot P_{19,2}^{2} \cdot P_{31,1}^{4} \cdot P_{31,2}^{-4} \cdot P_{139,1}^{-2} \cdot P_{139,2}^{2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 5.741619808076916...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{25499772694177442}{712269496040281201}t + \frac{1}{48648964964161}$

Factorization: $P_{11,1}^{4} \cdot P_{11,2}^{-4} \cdot P_{19,2}^{-4} \cdot P_{139,2}^{-4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.000004004711490...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{25499772694177442}{102119232721}t + 1$

Factorization: $P_{11,1}^{4} \cdot P_{11,2}^{-4} \cdot P_{19,1}^{2} \cdot P_{19,2}^{-2} \cdot P_{139,1}^{2} \cdot P_{139,2}^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 6.839389999673570...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{197697030899617385838047}{13521270961}t + 1$

Factorization: $P_{11,1}^{4} \cdot P_{11,2}^{-4} \cdot P_{31,1}^{4} \cdot P_{31,2}^{-4}$

VI. Field: $K = \mathbb{Q}(\sqrt{-17+\sqrt{17}})$

Defining polynomial: $x^4 + 34x^2 + 272$

Bound: 5345344

Integral basis: $[1, x, \frac{1}{2}x^2, \frac{1}{4}(x^3 - 2x)]$

Rep. for Cl(K):
- O_K
- $\mathfrak{a} = ([2,0,0,0],[1,1,1,0])$
- $\mathfrak{b} = ([2,0,0,0],[0,0,1,1])$
- $\mathfrak{c} = ([2,0,0,0],[0,2,0,1])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.000000069824614...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{25849829027231000608283770279331 3}{3583949899882919778744002}t^3 + \frac{2179218404558007970750473479066739 3}{28671599199063358229952016}t^2 - \frac{5132807666206000234489830435952 1}{3583949899882919778744002}t + 1$

Factorization: $P_{2,1}^{-2} \cdot P_{2,2}^{2} \cdot P_{47,1}^{4} \cdot P_{47,2}^{-4} \cdot P_{103,1}^{-4} \cdot P_{103,2}^{4} \cdot P_{239,1}^{4} \cdot P_{239,2}^{-4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 2.244151203918937...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{14402520990641}{5354586744004}t + 1$

Factorization: $P_{2,1}^{2} \cdot P_{2,2}^{-2} \cdot P_{47,1}^{2} \cdot P_{47,2}^{-2} \cdot P_{103,1}^{-2} \cdot P_{103,2}^{2} \cdot P_{239,1}^{-2} \cdot P_{239,2}^{2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.000000031114041...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{43023907708338058948}{1338646686001}t^3 + \frac{13620114970521166011189722313052 86}{17919749499414598893720001}t^2 - \frac{43023907708338058948}{1338646686001}t + 1$

Factorization: $P_{47,1}^{-2} \cdot P_{47,2}^{2} \cdot P_{47,3}^{-2} \cdot P_{47,4}^{2} \cdot P_{103,1}^{-2} \cdot P_{103,2}^{2} \cdot P_{103,3}^{-2} \cdot P_{103,4}^{2} \cdot P_{239,1}^{-2} \cdot P_{239,2}^{2} \cdot P_{239,3}^{-2} \cdot P_{239,4}^{2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 0.095066059419262...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{5132807666206000234489830435952 1}{3583949899882919778744002}t^3 + \frac{2179218404558007970750473479066739 3}{28671599199063358229952016}t^2 - \frac{2584982902723100060828377027933 13}{3583949899882919778744002}t + 1$

Factorization: $P_{2,1}^{-2} \cdot P_{2,2}^{2} \cdot P_{47,1}^{-4} \cdot P_{47,2}^{4} \cdot P_{103,1}^{4} \cdot P_{103,2}^{-4} \cdot P_{239,1}^{-4} \cdot P_{239,2}^{4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.042361699716690...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{43023907708338058948}{1338646686001}t^3 + \frac{13620114970521166011189722313052 86}{17919749499414598893720001}t^2 - \frac{43023907708338058948}{1338646686001}t + 1$

Factorization: $P_{47,1}^{-2} \cdot P_{47,2}^{-2} \cdot P_{47,3}^{2} \cdot P_{47,4}^{2} \cdot P_{103,1}^{2} \cdot P_{103,2}^{2} \cdot P_{103,3}^{-2} \cdot P_{103,4}^{-2} \cdot P_{239,1}^{-2} \cdot P_{239,2}^{2} \cdot P_{239,3}^{-2} \cdot P_{239,4}^{2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 0.000000001318043...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{13620114934681667012360524525612 84}{17919749499414598893720001}t^3 + \frac{18510539104726005269380430711956390001 34}{17919749499414598893720001}t^2 - \frac{13620114934681667012360524525612 84}{17919749499414598893720001}t + 1$

Factorization: $P_{47,1}^{4} \cdot P_{47,2}^{-4} \cdot P_{103,1}^{4} \cdot P_{103,2}^{-4} \cdot P_{239,1}^{-4} \cdot P_{239,2}^{4}$

VII. Field: $K = \mathbb{Q}(\sqrt{-35+14\sqrt{5}})$

Defining polynomial: $x^4 + 70x^2 + 245$

Bound: 1960000

Integral basis: $[1, x, \frac{1}{28}(x^2+21), \frac{1}{28}(x^3+21x)]$

Rep. for $\mathrm{Cl}(K)$:

- O_K
- $\mathfrak{a} = ([5,0,0,0],[0,1,0,0])$
- $\mathfrak{b} = ([2,0,0,0],[1,1,0,0])$
- $\mathfrak{c} = ([10,0,0,0],[29,99,3,1])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 1.492212566211723...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{1763459273190826016180816348092 07}{71647986553395726551744212 81}t + \frac{25411681}{691896698282364961}$

Factorization: $P_{11,1}^4 \cdot P_{11,2}^{-4} \cdot P_{29,1}^4 \cdot P_{29,2}^{-4} \cdot P_{71,1}^4 \cdot P_{151,2}^{-4} \cdot P_{191,1}^{-4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 0.000006060327141...

Minimal pol. over $\mathbb{Q}$: $t - \frac{5041}{831803281}$

Factorization: $P_{71,1}^2 \cdot P_{71,2}^2 \cdot P_{151,1}^{-2} \cdot P_{151,2}^{-2} \cdot P_{191,1}^{-2} \cdot P_{191,2}^{-2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.000000000246226...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{1763459273190826016180816348092 07}{4342102375232971190304 1}t + 1$

Factorization: $P_{11,1}^4 \cdot P_{11,2}^{-4} \cdot P_{29,1}^4 \cdot P_{29,2}^{-4} \cdot P_{71,1}^2 \cdot P_{71,2}^{-2} \cdot P_{151,1}^2 \cdot P_{151,2}^{-2} \cdot P_{191,1}^{-2} \cdot P_{191,2}^2$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 1.061841908253816...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{2393169906223529711042}{691896698282364961}t + \frac{25411681}{691896698282364961}$

Factorization: $P_{71,1}^4 \cdot P_{151,1}^{-4} \cdot P_{191,2}^{-4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.000000001752119...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{2393169906223529711042}{4193120339521}t + 1$

Factorization: $P_{71,1}^2 \cdot P_{71,2}^{-2} \cdot P_{151,1}^{-2} \cdot P_{151,2}^2 \cdot P_{191,1}^2 \cdot P_{191,2}^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 4.314181558995886...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{6099548782250156210092 3394697057892 7}{263145608745794401}t + 1$

Factorization: $P_{11,1}^4 \cdot P_{11,2}^{-4} \cdot P_{29,1}^4 \cdot P_{29,2}^{-4} \cdot P_{71,1}^4 \cdot P_{71,2}^{-4}$

VIII. Field: $K = \mathbb{Q}(\sqrt{-145+58\sqrt{5}})$

Defining polynomial: $x^4 + 290x^2 + 4205$

Bound: 33640000

Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{116}(x^2+87), \frac{1}{232}(x^3+x^2+87x+87)]$

Rep. for Cl(K):
- O_K
- $\mathfrak{a} = ([5,0,0,0],[-1,2,0,0])$
- $\mathfrak{b} = ([19,0,0,0],[14,2,0,0])$
- $\mathfrak{c} = ([95,0,0,0],[116,2,9023,2])$

$u(\Phi;\mathfrak{a}^{-1},\mathfrak{a}^{-1})$: 3.114124375091707...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{6102171347060903514912067469712 2}{19002920532868561}t + 1$

Factorization: $P_{59,1}^4 \cdot P_{59,2}^{-4} \cdot P_{199,1}^{-4} \cdot P_{199,2}^4$

$u(\Phi;\mathfrak{a}^{-1},\mathfrak{b}^{-1})$: 1.640090008311705...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{710414144063248075137753592800 4}{1165042506264695562001}t^3 + \frac{435860575211754582244509007440243602624521025031083810400 6}{135732404140352319783151056955502523512400 1}t^2 - \frac{710414144063248075137753592800 4}{1165042506264695562001}t + 1$

Factorization: $P_{109,1}^2 \cdot P_{109,2}^{-2} \cdot P_{149,1}^2 \cdot P_{149,2}^{-2} \cdot P_{149,3}^{-2} \cdot P_{149,4}^2 \cdot P_{179,1}^2 \cdot P_{179,2}^{-2} \cdot P_{179,3}^{-2} \cdot P_{179,4}^2 \cdot P_{199,1}^2 \cdot P_{199,2}^{-2} \cdot P_{199,3}^{-2} \cdot P_{199,4}^{-2}$

$u(\Phi;\mathfrak{a}^{-1},\mathfrak{c}^{-1})$: 0.000001898752116...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{710414144063248075137753592800 4}{1165042506264695562001}t^3 + \frac{435860575211754582244509007440243602624521025031083810400 6}{135732404140352319783151056955502523512400 1}t^2 - \frac{710414144063248075137753592800 4}{1165042506264695562001}t + 1$

Factorization: $P_{109,1}^2 \cdot P_{109,2}^{-2} \cdot P_{149,1}^2 \cdot P_{149,2}^{-2} \cdot P_{149,3}^{-2} \cdot P_{149,4}^2 \cdot P_{179,1}^2 \cdot P_{179,2}^{-2} \cdot P_{179,3}^{-2} \cdot P_{179,4}^2 \cdot P_{199,1}^2 \cdot P_{199,2}^{-2} \cdot P_{199,3}^{-2} \cdot P_{199,4}^{-2}$

$u(\Phi;\mathfrak{b}^{-1},\mathfrak{b}^{-1})$: 1.827155559290797...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{710414144063248075137753592800 4}{1045764584228840304367208753281}t^3 + \frac{435860575211754582244509007440243602624521025031083810400 6}{109362356562731922745038277513500394180741234333418632826496 1}t^2 - \frac{134999435250597407730264152883732109361291082244}{160117426243495808091010542107515927120023241187558220321272940 01}t + \frac{361110988778517554345143302210721}{234427923763102212626048534699614068896426027422703990372375711468641}$

Factorization: $P_{11,1}^{-4} \cdot P_{11,2}^{-4} \cdot P_{59,1}^4 \cdot P_{59,2}^4 \cdot P_{109,1}^{-4} \cdot P_{109,2}^{-4} \cdot P_{149,1}^{-4} \cdot P_{149,2}^{-4} \cdot P_{179,1}^{-4} \cdot P_{179,2}^{-4} \cdot P_{199,1}^4 \cdot P_{199,2}^4$

$u(\Phi;\mathfrak{b}^{-1},\mathfrak{c}^{-1})$: 0.000000001114058...

Minimal pol. over $\mathbb{Q}$: $t - \frac{137851081}{123737784357464761}$

Factorization: $137851081 \cdot 123737784357464761^{-1} = 59^2 \cdot 199^2 \cdot 11^{-4} \cdot 109^{-2} \cdot 149^{-2} \cdot 179^{-2}$

$u(\Phi;\mathfrak{c}^{-1},\mathfrak{c}^{-1})$: 2.115320176587490...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{710414144063248075137753592800 4}{1045764584228840304367208753281}t^3 + \frac{435860575211754582244509007440243602624521025031083810400 6}{109362356562731922745038277513500394180741234333418632826496 1}t^2 - \frac{134999435250597407730264152883732109361291082244}{160117426243495808091010542107515927120023241187558220321272940 01}t + \frac{361110988778517554345143302210721}{234427923763102212626048534699614068896426027422703990372375711468641}$

Factorization: $P_{11,1}^{-4} \cdot P_{11,2}^{-4} \cdot P_{59,1}^4 \cdot P_{59,2}^4 \cdot P_{109,1}^{-4} \cdot P_{109,2}^{-4} \cdot P_{149,1}^{-4} \cdot P_{149,2}^{-4} \cdot P_{179,1}^{-4} \cdot P_{179,2}^{-4} \cdot P_{199,1}^4 \cdot P_{199,2}^4$

IX. Field: $K = \mathbb{Q}(\sqrt{-145 + 10\sqrt{29}})$

Def. pol.: $x^4 + 290x^2 + 18125$

Bound: 1131649600

Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{20}(x^2+15), \frac{1}{200}(x^3+5x^2+15x+75)]$

Rep. for $\mathrm{Cl}(K)$:
- O_K
- $\mathfrak{a} = ([5,0,0,0],[1,3,3,0])$
- $\mathfrak{b} = ([5,0,0,0],[1,0,3,3])$
- $\mathfrak{c} = ([5,0,0,0],[0,0,8,24])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 1.465872679682312...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{1896310733933419540080 4}{3448231591506025}t^3 + \frac{3822353294706004747840865962333160447526}{11890301108660174062927611300625}t^2 - \frac{3687754433165779326154031617350119102 44}{8318484381371429424859314184945501562 5}t + \frac{3781855934127419349692710188403 21}{5819632469418405454205138352073335256878906 25}$

Factorization: $P_{5,1}^{-4} \cdot P_{5,2}^{-4} \cdot P_{7,1}^{4} \cdot P_{7,2}^{4} \cdot P_{23,1}^{-4} \cdot P_{23,2}^{-4} \cdot P_{149,1}^{-4} \cdot P_{149,2}^{-4} \cdot P_{241,1}^{4} \cdot P_{241,2}^{4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 0.000897847040873...

Min. pol. /$\mathbb{Q}$: $t - \frac{139452481}{155318751025}$

Factorization: $139452481 \cdot 155318751025^{-1} = 7^4 \cdot 241^2 \cdot 5^{-2} \cdot 23^{-4} \cdot 149^{-2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 1.632653016549247...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{7898003889768511204}{1289456281}t^3 + \frac{6630503454856472492009465656027 26}{1662697500610350961}t^2 - \frac{7898003889768511204}{1289456281}t + 1$

Factorization: $P_{149,1}^{2} \cdot P_{149,2}^{2} \cdot P_{149,3}^{-2} \cdot P_{149,4}^{-2} \cdot P_{241,1}^{2} \cdot P_{241,2}^{-2} \cdot P_{241,3}^{-2} \cdot P_{241,4}^{2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 0.000000013790347...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{1896310733933419540080 4}{3448231591506025}t^3 + \frac{3822353294706004747840865962333160447526}{11890301108660174062927611300625}t^2 - \frac{3687754433165779326154031617350119102 44}{8318484381371429424859314184945501562 5}t + \frac{3781855934127419349692710188403 21}{5819632469418405454205138352073335256878906 25}$

Factorization: $P_{5,1}^{-4} \cdot P_{5,2}^{-4} \cdot P_{7,1}^{4} \cdot P_{7,2}^{4} \cdot P_{23,1}^{-4} \cdot P_{23,2}^{-4} \cdot P_{149,1}^{-4} \cdot P_{149,2}^{-4} \cdot P_{241,1}^{4} \cdot P_{241,2}^{4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.000015359350223...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{7898003889768511204}{1289456281}t^3 + \frac{6630503454856472492009465656027 26}{1662697500610350961}t^2 - \frac{7898003889768511204}{1289456281}t + 1$

Factorization: $P_{149,1}^{2} \cdot P_{149,2}^{2} \cdot P_{149,3}^{-2} \cdot P_{149,4}^{-2} \cdot P_{241,1}^{2} \cdot P_{241,2}^{-2} \cdot P_{241,3}^{-2} \cdot P_{241,4}^{2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 2.507648947509065...

Min. pol. /$\mathbb{Q}$: $t^2 - \frac{1345245140613050068886402}{3373402561}t + 1$

Factorization: $P_{241,1}^{-4} \cdot P_{241,2}^{4}$

X. Field: $K = \mathbb{Q}(\sqrt{-41 + 4\sqrt{41}})$

Defining polynomial: $x^4 + 82x^2 + 1025$

Bound: 180848704

Integral basis: $[1, x, \frac{1}{8}(x^2+5), \frac{1}{40}(x^3+37x)]$

Rep. for Cl(K):
- O_K
- $\mathfrak{a} = ([2,0,0,0],[1,1,1,0])$
- $\mathfrak{b} = ([2,0,0,0],[0,1,1,0])$
- $\mathfrak{c} = ([2,0,0,0],[3,3,2,2])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.006234747377822...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{1401569345332154922525692072115111845598178771 53}{650210492253078245979821331012 50}t^3 + \frac{5404569038315670866205769667935559403576129081323065761}{393941763030912623389214689168947900625000 0}t^2 - \frac{1134365141201159654040160485010985429315 3}{650210492253078245979821331012 50}t + 1$

Factorization: $P_{2,1}^{-2} \cdot P_{2,2}^{2} \cdot P_{5,1}^{4} \cdot P_{5,2}^{-4} \cdot P_{23,1}^{-4} \cdot P_{23,2}^{4} \cdot P_{31,1}^{4} \cdot P_{31,2}^{-4} \cdot P_{59,1}^{-4} \cdot P_{59,2}^{4} \cdot P_{59,3}^{4} \cdot P_{59,4}^{-4} \cdot P_{359,1}^{4} \cdot P_{359,2}^{-4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 1159283.725388456395615...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{2300942421977382355150271681}{19847966219008753225 00}t + 1$

Factorization: $P_{2,1}^{-2} \cdot P_{2,2}^{2} \cdot P_{5,1}^{-4} \cdot P_{5,2}^{4} \cdot P_{23,1}^{-2} \cdot P_{23,2}^{2} \cdot P_{31,1}^{2} \cdot P_{31,2}^{-2} \cdot P_{59,1}^{-4} \cdot P_{59,2}^{4} \cdot P_{359,1}^{-2} \cdot P_{359,2}^{2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.000000005378103...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{121825775935133172 52}{655191050 89}t^3 + \frac{1201200632510187463303030055603718}{4292753131663425697921}t^2 - \frac{121825775935133172 52}{655191050 89}t + 1$

Factorization: $P_{23,1}^{-2} \cdot P_{23,2}^{-2} \cdot P_{23,3}^{2} \cdot P_{23,4}^{2} \cdot P_{31,1}^{-2} \cdot P_{31,2}^{2} \cdot P_{31,3}^{2} \cdot P_{31,4}^{-2} \cdot P_{359,1}^{-2} \cdot P_{359,2}^{2} \cdot P_{359,3}^{-2} \cdot P_{359,4}^{2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 174453353.410440115446805...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{1134365141201159654040160485010985429315 3}{650210492253078245979821331012 50}t^3 + \frac{5404569038315670866205769667935559403576129081323065761}{393941763030912623389214689168947900625000 0}t^2 - \frac{1401569345332154922525692072115111845598178771 53}{650210492253078245979821331012 50}t + 1$

Factorization: $P_{2,1}^{-2} \cdot P_{2,2}^{2} \cdot P_{5,1}^{4} \cdot P_{5,2}^{-4} \cdot P_{23,1}^{4} \cdot P_{23,2}^{-4} \cdot P_{31,1}^{-4} \cdot P_{31,2}^{4} \cdot P_{59,1}^{-4} \cdot P_{59,2}^{4} \cdot P_{59,3}^{-4} \cdot P_{59,4}^{4} \cdot P_{359,1}^{-4} \cdot P_{359,2}^{4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 150.483742322858662...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{121825775935133172 52}{655191050 89}t^3 + \frac{1201200632510187463303030055603718}{4292753131663425697921}t^2 - \frac{121825775935133172 52}{655191050 89}t + 1$

Factorization: $P_{23,1}^{2} \cdot P_{23,2}^{-2} \cdot P_{23,3}^{-2} \cdot P_{23,4}^{2} \cdot P_{31,1}^{2} \cdot P_{31,2}^{-2} \cdot P_{31,3}^{-2} \cdot P_{31,4}^{2} \cdot P_{359,1}^{-2} \cdot P_{359,2}^{2} \cdot P_{359,3}^{2} \cdot P_{359,4}^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 0.000000809317078...

Minimal pol. over $\mathbb{Q}$: $t^4 - \frac{1201200632424332400669762042078 76}{4292753131663425697921}t^3 + \frac{1484149565818462347019081661939410199 10}{4292753131663425697921}t^2 - \frac{1201200632424332400669762042078 76}{4292753131663425697921}t + 1$

Factorization: $P_{23,1}^{4} \cdot P_{23,2}^{-4} \cdot P_{31,1}^{4} \cdot P_{31,2}^{-4} \cdot P_{359,1}^{4} \cdot P_{359,2}^{-4}$

XI. Field: $K = \mathbb{Q}(\sqrt{-219 + 24\sqrt{73}})$

Def. pol.: $x^4 + 438x^2 + 5913$

Bound: 4089346704

Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{48}(x^2+3), \frac{1}{288}(x^3+3x^2+51x+153)]$

Rep. for $\mathrm{Cl}(K)$:
- O_K
- $\mathfrak{a} = ([3,0,0,0],[0,0,2,1])$
- $\mathfrak{b} = ([3,0,0,0],[0,0,0,1])$
- $\mathfrak{c} = ([3,0,0,0],[8,0,8,2])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 0.002061212756340...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{33065828654499982143470409393285456638172 17}{476808207021896824663430414 4}t^3 + \frac{257085696176799108972543462392789519802432664601}{279621550562852772391333117657600 8}t^2 - \frac{88954665824053310156629306087099283478 5}{476808207021896824663430414 4}t + 1$

Factorization: $P_{2,1}^4 \cdot P_{2,2}^{-4} \cdot P_{3,1}^{-2} \cdot P_{3,2}^2 \cdot P_{19,1}^{-4} \cdot P_{19,2}^4 \cdot P_{251,1}^{-4} \cdot P_{251,2}^4 \cdot P_{503,1}^4 \cdot P_{503,2}^{-4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 0.016401918901501...

Min. pol. /$\mathbb{Q}$: $t^2 - \frac{4560605187435538321}{74782558202144004}t + 1$

Factorization: $P_{2,1}^{-2} \cdot P_{2,2}^2 \cdot P_{3,1}^{-2} \cdot P_{3,2}^2 \cdot P_{19,1}^4 \cdot P_{19,2}^{-4} \cdot P_{251,1}^2 \cdot P_{251,2}^{-2} \cdot P_{503,1}^2 \cdot P_{503,2}^{-2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 0.125669000604070...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{3626133239093268994820 81}{31879640018}t^3 + \frac{3737610860422907400228138111912962 25}{4065245790709068161296}t^2 - \frac{3626133239093268994820 81}{31879640018}t + 1$

Factorization: $P_{2,1}^2 \cdot P_{2,2}^{-2} \cdot P_{2,3}^{-2} \cdot P_{2,4}^2 \cdot P_{251,1}^{-2} \cdot P_{251,2}^2 \cdot P_{251,3}^2 \cdot P_{251,4}^{-2} \cdot P_{503,1}^{-2} \cdot P_{503,2}^2 \cdot P_{503,3}^2 \cdot P_{503,4}^{-2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 1.441996848178209...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{88954665824053310156629306087099283478 5}{476808207021896824663430414 4}t^3 + \frac{257085696176799108972543462392789519802432664601}{279621550562852772391333117657600 8}t^2 - \frac{33065828654499982143470409393285456638172 17}{476808207021896824663430414 4}t + 1$

Factorization: $P_{2,1}^4 \cdot P_{2,2}^{-4} \cdot P_{3,1}^{-2} \cdot P_{3,2}^2 \cdot P_{19,1}^{-4} \cdot P_{19,2}^4 \cdot P_{251,1}^{-4} \cdot P_{251,2}^4 \cdot P_{503,1}^4 \cdot P_{503,2}^{-4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 8.791635032692373...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{3626133239093268994820 81}{31879640018}t^3 + \frac{3737610860422907400228138111912962 25}{4065245790709068161296}t^2 - \frac{3626133239093268994820 81}{31879640018}t + 1$

Factorization: $P_{2,1}^2 \cdot P_{2,2}^{-2} \cdot P_{2,3}^{-2} \cdot P_{2,4}^2 \cdot P_{251,1}^{-2} \cdot P_{251,2}^2 \cdot P_{251,3}^2 \cdot P_{251,4}^{-2} \cdot P_{503,1}^{-2} \cdot P_{503,2}^2 \cdot P_{503,3}^2 \cdot P_{503,4}^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 1.104835988234184...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{3737610860422826095312323930549736 33}{4065245790709068161296}t^3 + \frac{2629768453527670934256460150292642625499570461 93}{203262289535453408064 8}t^2 - \frac{3737610860422826095312323930549736 33}{4065245790709068161296}t + 1$

Factorization: $P_{2,1}^{-4} \cdot P_{2,2}^4 \cdot P_{251,2}^4 \cdot P_{251,2}^{-4} \cdot P_{503,1}^4 \cdot P_{503,2}^{-4}$

XII. Field: $K = \mathbb{Q}(\sqrt{-221 + 34\sqrt{13}})$

Def. pol.: $x^4 + 442x^2 + 33813$

Bound: 132066064

Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{68}(x^2+51), \frac{1}{408}(x^3+3x^2+187x+153)]$

Rep. for Cl(K):
- O_K
- $\mathfrak{a} = ([13,0,0,0],[-1,2,0,0])$
- $\mathfrak{b} = ([17,0,0,0],[5,15,15,0])$
- $\mathfrak{c} = ([221,0,0,0],[692,0,2,1])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 7.901417107596603...

Min. pol. /$\mathbb{Q}$: $t^2 - \frac{2307797132797468266337874614980162444962}{18234867745948307281}t + 1$

Factorization: $P_{101,1}^4 \cdot P_{101,2}^{-4} \cdot P_{647,1}^{-4} \cdot P_{647,2}^4$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 1.005700406975535...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{92282790993104040533022608678880416093 2}{4070445870193174182722857 4569}t^3 + \frac{20969060810931373448100763983085603900121453177096772796329645719087693021347 8}{1656852958217266700854707724494525992640103841459593535761}t^2 - \frac{92282790993104040533022608678880416093 2}{4070445870193174182722857 4569}t + 1$

Factorization: $P_{43,1}^{-2} \cdot P_{43,2}^2 \cdot P_{43,3}^{-2} \cdot P_{43,4}^2 \cdot P_{101,1}^{-2} \cdot P_{101,2}^2 \cdot P_{101,3}^{-2} \cdot P_{101,4}^{-2} \cdot P_{257,1}^{-2} \cdot P_{257,2}^2 \cdot P_{257,3}^{-2} \cdot P_{257,4}^2 \cdot P_{491,1}^2 \cdot P_{491,2}^{-2} \cdot P_{491,3}^2 \cdot P_{491,4}^{-2} \cdot P_{569,1}^{-2} \cdot P_{569,2}^2 \cdot P_{569,3}^{-2} \cdot P_{569,4}^2 \cdot P_{647,1}^2 \cdot P_{647,2}^{-2} \cdot P_{647,3}^{-2} \cdot P_{647,4}^{-2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 7.856631112797008...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{92282790993104040533022608678880416093 2}{4070445870193174182722857 4569}t^3 + \frac{20969060810931373448100763983085603900121453177096772796329645719087693021347 8}{1656852958217266700854707724494525992640103841459593535761}t^2 - \frac{92282790993104040533022608678880416093 2}{4070445870193174182722857 4569}t + 1$

Factorization: $P_{43,1}^{-2} \cdot P_{43,2}^2 \cdot P_{43,3}^{-2} \cdot P_{43,4}^2 \cdot P_{101,1}^{-2} \cdot P_{101,2}^2 \cdot P_{101,3}^{-2} \cdot P_{101,4}^{-2} \cdot P_{257,1}^{-2} \cdot P_{257,2}^2 \cdot P_{257,3}^{-2} \cdot P_{257,4}^2 \cdot P_{491,1}^2 \cdot P_{491,2}^{-2} \cdot P_{491,3}^2 \cdot P_{491,4}^{-2} \cdot P_{569,1}^{-2} \cdot P_{569,2}^2 \cdot P_{569,3}^{-2} \cdot P_{569,4}^2 \cdot P_{647,1}^2 \cdot P_{647,2}^{-2} \cdot P_{647,3}^{-2} \cdot P_{647,4}^{-2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 4.505357520544783...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{92282790993104040533022608678880416093 2}{9086180285488556975780978729941216608 1}t^3 + \frac{20969060810931373448100763983085603900121453177096772796329645719087693021347 8}{8255867218040091474811939074657669894415435582136678873750114691316326898561}t^2 - \frac{16827644889862418287545483567822580228778676833434911345892}{8255867218040091474811939074657669894415435582136678873750114691316326898561}t + \frac{33251040171222590072721038938919761296 1}{8255867218040091474811939074657669894415435582136678873750114691316326898561}$

Factorization: $P_{43,1}^{-4} \cdot P_{43,2}^{-4} \cdot P_{101,1}^4 \cdot P_{101,2}^{-4} \cdot P_{257,1}^{-4} \cdot P_{257,2}^{-4} \cdot P_{491,1}^{-4} \cdot P_{491,2}^{-4} \cdot P_{569,1}^{-4} \cdot P_{569,2}^{-4} \cdot P_{647,1}^4 \cdot P_{647,2}^4$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 0.000000000447982...

Min. pol. /$\mathbb{Q}$: $t - \frac{4270230409}{9532145763409494241}$

Factorization: $4270230409 \cdot 9532145763409494241^{-1} = (101 \cdot 647)^2 \cdot (43 \cdot 257 \cdot 491 \cdot 569)^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 3.519629884274990...

Min. pol. /$\mathbb{Q}$: $t^4 - \frac{92282790993104040533022608678880416093 2}{9086180285488556975780978729941216608 1}t^3 + \frac{20969060810931373448100763983085603900121453177096772796329645719087693021347 8}{8255867218040091474811939074657669894415435582136678873750114691316326898561}t^2 - \frac{16827644889862418287545483567822580228778676833434911345892}{8255867218040091474811939074657669894415435582136678873750114691316326898561}t + \frac{33251040171222590072721038938919761296 1}{8255867218040091474811939074657669894415435582136678873750114691316326898561}$

Factorization: $P_{43,1}^{-4} \cdot P_{43,2}^{-4} \cdot P_{101,1}^4 \cdot P_{101,2}^{-4} \cdot P_{257,1}^{-4} \cdot P_{257,2}^{-4} \cdot P_{491,1}^{-4} \cdot P_{491,2}^{-4} \cdot P_{569,1}^{-4} \cdot P_{569,2}^{-4} \cdot P_{647,1}^4 \cdot P_{647,2}^4$

XIII. Field: $K = \mathbb{Q}(\sqrt{-255 + 60\sqrt{17}})$

Defining polynomial: $x^4 + 510x^2 + 3825$

Bound: 300675600

Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{120}(x^2+75), \frac{1}{240}(x^3+x^2+75x+75)]$

Rep. for Cl(K):
- O_K
- $\mathfrak{a} = ([3,0,0,0],[1,1,0,0])$
- $\mathfrak{b} = ([5,0,0,0],[1,3,0,0])$
- $\mathfrak{c} = ([15,0,0,0],[217,1,16,223])$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{a}^{-1})$: 4.107898863385631...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{19285791861760407530460433819948245 14}{79224082468417441}t + 1$

Factorization: $P_{19,1}^{-4} \cdot P_{19,2}^{4} \cdot P_{883,1}^{-4} \cdot P_{883,2}^{4}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{b}^{-1})$: 1.890754071253506...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{771120018670072703988078 74}{14579983147255201}t + 1$

Factorization: $P_{13,1}^{-2} \cdot P_{13,2}^{2} \cdot P_{67,1}^{-2} \cdot P_{67,2}^{2} \cdot P_{157,1}^{2} \cdot P_{157,2}^{-2} \cdot P_{883,1}^{2} \cdot P_{883,2}^{-2}$

$u(\Phi; \mathfrak{a}^{-1}, \mathfrak{c}^{-1})$: 2.172624629422181...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{87455419495947554273648370302 42}{1900077983733445049521}t + 1$

Factorization: $P_{13,1}^{-2} \cdot P_{13,2}^{2} \cdot P_{19,1}^{-4} \cdot P_{19,2}^{4} \cdot P_{67,1}^{2} \cdot P_{67,2}^{-2} \cdot P_{157,1}^{-2} \cdot P_{157,2}^{2} \cdot P_{883,1}^{-2} \cdot P_{883,2}^{2}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: 2.657837652996455...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{12337920298721163263809259 84}{16595242354792272935045400001}t + \frac{155626223800576}{787582338746527577270996742820858321}$

Factorization: $P_{2,1}^{4} \cdot P_{2,2}^{4} \cdot P_{13}^{-4} \cdot P_{67}^{-4} \cdot P_{83,1}^{-4} \cdot P_{83,2}^{-4} \cdot P_{157}^{-4} \cdot P_{883}^{4}$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: 1.405702461999406...

Minimal pol. over $\mathbb{Q}$: $t - \frac{12475024}{887458358880306889}$

Factorization: $12475024 \cdot 887458358880306889^{-1} = 2^4 \cdot 883^2 \cdot 13^{-2} \cdot 67^{-2} \cdot 83^{-4} \cdot 157^{-2}$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: 3.054063790579308...

Minimal pol. over $\mathbb{Q}$: $t^2 - \frac{13992867119351608683783739248 3872}{21627085789188838011680515735303 21}t + \frac{155626223800576}{787582338746527577270996742820858321}$

Factorization: $P_{2,1}^{4} \cdot P_{2,2}^{4} \cdot P_{13}^{-4} \cdot P_{19,1}^{-4} \cdot P_{19,2}^{4} \cdot P_{67}^{-4} \cdot P_{83,1}^{-4} \cdot P_{83,2}^{-4} \cdot P_{157}^{-4} \cdot P_{883}^{4}$

B.3 One example of quartic cyclic CM-field with class number 5

Field: $K = \mathbb{Q}(\sqrt{-101 + 10\sqrt{101}})$

Def. pol.: $x^4 + 202x^2 + 101$

Bound: 6659865664

Integral basis: $[1, \frac{1}{2}(x+1), \frac{1}{20}(x^2+11), \frac{1}{40}(x^3+x^2+11x+11)]$

Rep. for $\mathrm{Cl}(K)$:

- O_K
- $\mathfrak{a} = ([5,0,0,0],[2,2,4,3])$
- $\mathfrak{b} = ([25,0,0,0],[12,2,4,18])$
- $\mathfrak{c} = ([125,0,0,0],[32,72,119,63])$
- $\mathfrak{d} = ([625,0,0,0],[77,467,384,33])$

$u(\Phi;\mathfrak{a}^{-1},\mathfrak{a}^{-1})$: $36032.758844207454189... + i \cdot 22689.622629195781996...$

Min. pol. :

$$t^{10} - \frac{1090106108033096004700909106668157 8}{92085105098381079407240401}t^9 + \frac{476373325814753057254417073284530421842493833321415075943293235 97}{84796665809798890641369769579879512913901022066640801}t^8 - \frac{854395755212922630502570219282222630488571510182806910437289003964833 84}{14330636521856012518391491058999637682449272729222955369}t^7 - \frac{321183826179643974073375250236499778495172232859489994426366646001648350681550}{2421877572193666115608161988970938768333927091238679173 61}t^6 - \frac{141586057247533852699047880088840128651601432668048970184573757895736583988285670 0}{1424633865996274185651859993512316922549368877199223043 3}t^5 + \frac{363714415566453341541448654443831416309054656163877735173331822891308192397112 02}{14330636521856012518391491058999637682449272729222955369}t^4 + \frac{34776461324616144272257869320290221502305384308776463537790938 4}{14933815680222712402436381144940028819968 1}t^3 + \frac{853295190713305364811321959242970511902785221}{155623827616264024198236277 69}t^2 + \frac{69930434159639391094818 2}{1621740634847281}t + 1$$

$u(\Phi;\mathfrak{a}^{-1},\mathfrak{b}^{-1})$: $-1.821825785942248... - i \cdot 0.771604398148303...$

Min. pol. :

$$t^{10} - \frac{7512276365122982176497 70}{1621740634847281}t^9 + \frac{1326804402363435371736156482529052950140 85}{155623827616264024198236277 69}t^8 - \frac{817974420722977008166208068153562227991693505053667258328 8}{14933815680222712402436381144940028819968 1}t^7 - \frac{212555350715706243046391508810248303289547661906372674442790334107953 4}{84796665809798890641369769579879512913901022066640801}t^6 - \frac{207920014678264769069768529342673188180356937604309613518799031150 36}{501755418992892844031773784496328478780479420511 29}t^5 - \frac{212555350715706243046391508810248303289547661906372674442790334107953 4}{84796665809798890641369769579879512913901022066640801}t^4 - \frac{817974420722977008166208068153562227991693505053667258328 8}{14933815680222712402436381144940028819968 1}t^3 + \frac{132680440236343537173615648252905295014085}{155623827616264024198236277 69}t^2 - \frac{7512276365122982176497 70}{1621740634847281}t + 1$$

$u(\Phi;\mathfrak{a}^{-1},\mathfrak{c}^{-1})$: $0.000077790150867... + i \cdot 0.000048984014104...$

Min. pol. :

$$t^{10} - \frac{7512276365122982176497 70}{1621740634847281}t^9 + \frac{1326804402363435371736156482529052950140 85}{155623827616264024198236277 69}t^8 - \frac{817974420722977008166208068153562227991693505053667258328 8}{14933815680222712402436381144940028819968 1}t^7 - \frac{212555350715706243046391508810248303289547661906372674442790334107953 4}{84796665809798890641369769579879512913901022066640801}t^6 - \frac{207920014678264769069768529342673188180356937604309613518799031150 36}{501755418992892844031773784496328478780479420511 29}t^5 - \frac{212555350715706243046391508810248303289547661906372674442790334107953 4}{84796665809798890641369769579879512913901022066640801}t^4 - \frac{817974420722977008166208068153562227991693505053667258328 8}{14933815680222712402436381144940028819968 1}t^3 + \frac{132680440236343537173615648252905295014085}{155623827616264024198236277 69}t^2 - \frac{7512276365122982176497 70}{1621740634847281}t + 1$$

$u(\Phi;\mathfrak{a}^{-1},\mathfrak{d}^{-1})$: $3.914422541565896...$

Min. pol. :

$$t^{10} + \frac{6993043415963939109481 82}{1621740634847281}t^9 + \frac{853295190713305364811321959242970511902785221}{155623827616264024198236277 69}t^8 + \frac{347764613246161442722578693202902215023053843087764635377909384 1}{14933815680222712402436381144940028819968 1}t^7 + \frac{363714415566453341541448654443831416309054656163877735173331822891308192397112 02}{14330636521856012518391491058999637682449272729222955369}t^6 - \frac{141586057247533852699047880088840128651601432668048970184573757895736583988285670 0}{1424633865996274185651859993512316922549368877199223043 3}t^5 - \frac{321183826179643974073375250236499778495172232859489994426366646001648350681550}{2421877572193666115608161988970938768333927091238679173 61}t^4 - \frac{854395755212922630502570219282222630488571510182806910437289003964833 84}{14330636521856012518391491058999637682449272729222955369}t^3 + \frac{476373325814753057254417073284530421842493833321415075943293235 97}{84796665809798890641369769579879512913901022066640801}t^2 - \frac{109010610803309600470090910666815 78}{92085105098381079407240401}t + 1$$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{b}^{-1})$: $-0.000000003933090... - i \cdot 0.000000001665795...$

Min. pol. : $t^{10} - \frac{109010610803309600470090910666815 78}{92085105098381079407240401} t^9 + \frac{4763733258147530572544170732845304218424938333214150759432932 3597}{847966658097988906413697695798795129139010220664080 1} t^8 - \frac{8543957552129226305025702192822226304885715101828069104372890039648338 4}{143306365218560125183914910589996376824492727292229536 9} t^7 - \frac{3211838261796439740733752502364997784951722328594899944263666460016483506815 50}{24218775721936661156081619889709387683339270912386791736 1} t^6 - \frac{1415860572475338526990478800888401286516014326680489701845737578957365839882856700}{1424633865996274185651859993512316922549368877199223043 3} t^5 + \frac{3637144155664533415414486544438314163090546561638777351733318228913081923971120 2}{143306365218560125183914910589996376824492727292229536 9} t^4 + \frac{3477646132461614427225786932029022150230538430877646353779093 84}{14933815680222712402436381144940028819968 1} t^3 + \frac{8532951907133053648113219592429705119027852 21}{15562382761626402419823627769} t^2 + \frac{699304341596393910948182}{1621740634847281} t + 1$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{c}^{-1})$: $0.000000008450741...$

Min. pol. : $t^{10} + \frac{699304341596393910948182}{1621740634847281} t^9 + \frac{8532951907133053648113219592429705119027852 21}{15562382761626402419823627769} t^8 + \frac{3477646132461614427225786932029022150230538430877646353779093 84}{14933815680222712402436381144940028819968 1} t^7 + \frac{3637144155664533415414486544438314163090546561638777351733318228913081923971120 2}{143306365218560125183914910589996376824492727292229536 9} t^6 - \frac{1415860572475338526990478800888401286516014326680489701845737578957365839882856700}{1424633865996274185651859993512316922549368877199223043 3} t^5 - \frac{3211838261796439740733752502364997784951722328594899944263666460016483506815 50}{24218775721936661156081619889709387683339270912386791736 1} t^4 - \frac{8543957552129226305025702192822226304885715101828069104372890039648338 4}{143306365218560125183914910589996376824492727292229536 9} t^3 + \frac{4763733258147530572544170732845304218424938333214150759432932 3597}{847966658097988906413697695798795129139010220664080 1} t^2 - \frac{1090106108033096004700909 1066681578}{92085105098381079407240401} t + 1$

$u(\Phi; \mathfrak{b}^{-1}, \mathfrak{d}^{-1})$: $0.000077790150867... - i \cdot 0.000048984014104...$

Min. pol. : $t^{10} - \frac{7512276365122982176497 70}{1621740634847281} t^9 + \frac{1326804402363435371736156482529052950140 85}{15562382761626402419823627769} t^8 - \frac{8179744207229770081662080681535622279916935050536672583288}{14933815680222712402436381144940028819968 1} t^7 - \frac{2125553507157062430463915088102483032895476619063726744427903341079534}{847966658097988906413697695798795129139010220664080 1} t^6 - \frac{2079200146782647690697685293426731881803569376043096135187990311503 6}{501755418992892844031773784496328478780479420511 29} t^5 - \frac{2125553507157062430463915088102483032895476619063726744427903341079534}{847966658097988906413697695798795129139010220664080 1} t^4 - \frac{8179744207229770081662080681535622279916935050536672583288}{14933815680222712402436381144940028819968 1} t^3 + \frac{1326804402363435371736156482529052950140 85}{15562382761626402419823627769} t^2 - \frac{7512276365122982176497 70}{1621740634847281} t + 1$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{c}^{-1})$: $-0.000000003933090... + i \cdot 0.000000001665795...$

Min. pol. : $t^{10} - \frac{109010610803309600470090910666815 78}{92085105098381079407240401} t^9 + \frac{4763733258147530572544170732845304218424938333214150759432932 3597}{847966658097988906413697695798795129139010220664080 1} t^8 - \frac{8543957552129226305025702192822226304885715101828069104372890039648338 4}{143306365218560125183914910589996376824492727292229536 9} t^7 - \frac{3211838261796439740733752502364997784951722328594899944263666460016483506815 50}{24218775721936661156081619889709387683339270912386791736 1} t^6 - \frac{1415860572475338526990478800888401286516014326680489701845737578957365839882856700}{1424633865996274185651859993512316922549368877199223043 3} t^5 + \frac{3637144155664533415414486544438314163090546561638777351733318228913081923971120 2}{143306365218560125183914910589996376824492727292229536 9} t^4 + \frac{3477646132461614427225786932029022150230538430877646353779093 84}{14933815680222712402436381144940028819968 1} t^3 + \frac{8532951907133053648113219592429705119027852 21}{15562382761626402419823627769} t^2 + \frac{699304341596393910948182}{1621740634847281} t + 1$

$u(\Phi; \mathfrak{c}^{-1}, \mathfrak{d}^{-1})$: $-1.821825785942248... + i \cdot 0.771604398148303...$

Min. pol. : $t^{10} - \frac{7512276365122982176497 70}{1621740634847281} t^9 + \frac{1326804402363435371736156482529052950140 85}{15562382761626402419823627769} t^8 - \frac{8179744207229770081662080681535622279916935050536672583288}{14933815680222712402436381144940028819968 1} t^7 - \frac{2125553507157062430463915088102483032895476619063726744427903341079534}{847966658097988906413697695798795129139010220664080 1} t^6 - \frac{2079200146782647690697685293426731881803569376043096135187990311503 6}{501755418992892844031773784496328478780479420511 29} t^5 - \frac{2125553507157062430463915088102483032895476619063726744427903341079534}{847966658097988906413697695798795129139010220664080 1} t^4 + \frac{8179744207229770081662080681535622279916935050536672583288}{14933815680222712402436381144940028819968 1} t^3 + \frac{1326804402363435371736156482529052950140 85}{15562382761626402419823627769} t^2 - \frac{7512276365122982176497 70}{1621740634847281} t + 1$

$u(\Phi;\mathfrak{d}^{-1},\mathfrak{d}^{-1})$: 36032.758844207454189... $- i \cdot$ 22689.622629195781996...

Min. pol. : $t^{10} - \frac{109010610803309600470090910666815 78}{92085105098381079407240401} t^9 +$

$\frac{476373325814753057254417073284530421842493833321415075943293235 97}{847966658097988906413697695798795129139010220664080 1} t^8 -$

$\frac{854395755212922630502570219282222630488571510182806910437289003964833 84}{143306365218560125183914910589963768244927272922295369} t^7 -$

$\frac{321183826179643974073375250236499778495172232859489994426366646001648350681550}{24218775721936661156081619889709387683339270912386791736 1} t^6 -$

$\frac{141586057247533852699047880088840128651601432668048970184573757895736583988285670 0}{142463386599627418565185999351231692254936887719922304 33} t^5 +$

$\frac{363714415566453341541448654443831416309054656163877735173331822891308192397112 02}{143306365218560125183914910589996376824492727292229536 9} t^4 +$

$\frac{347764613246161442722578693202902215023053843087764635377909384}{14933815680222712402436381144940028819968 1} t^3 +$

$\frac{853295190713305364811321959242970511902785221}{15562382761626402419823627769} t^2 + \frac{69930434159639391094818 2}{1621740634847281} t + 1$

References

[1] A.A. Albert. On the construction of riemann matrices I. *Ann. of Math.*, 35:1–28, 1934.

[2] A.A. Albert. A solution of the principal problem in the theory of riemann matrices. *Ann. of Math.*, 35:500–515, 1934.

[3] A.A. Albert. On the construction of riemann matrices II. *Ann. of Math.*, 36:376–394, 1935.

[4] Ch. Birkenhake and H. Lange. *Complex Abelian Varieties.* Springer-Verlag, 1992.

[5] A. Borel, S. Chowla, C.S. Herz, K. Iwasawa, and J.-P. Serre. *Seminar on Complex Multiplication.* Lecture Notes in Mathematics 21, Springer-Verlag, 1966.

[6] A.I. Borevich and I.R. Shafarevich. *Number Theory.* Academic Press, 1966.

[7] M.J. Borwein and P.B. Borwein. *Pi and the AGM.* John Wiley and Sons, 1987.

[8] J.W.S. Cassels and A. Frolich. *Algebraic Number Theory.* Academic Press, 1967.

[9] H. Cohn. *Introduction to the Construction of Class Fields.* Cambridge University Press, 1985.

[10] D. Cox. The arithmetic-geometric mean of gauss. *L'ens. Math.*, 30:275–330, 1984.

[11] D.A. Cox. *Primes of the Form x^2+ny^2, Fermat Class Field Theory and Complex Multiplication.* John Wiley & Sons, 1989.

[12] S. Dasgupta. Stark's conjectures. Honors thesis, Harvard.

[13] H. Davenport. *Multiplicative Number Theory.* Springer-Verlag, 2000.

[14] E. DeShalit and E.Z. Goren. On special values of theta functions of genus two. *Extrait des Annales de l'Institut Fourier*, 47(3):775–799, 1997.

[15] M. Deuring. *Die klassenkorper der Komplexen Multiplication, Enzyklopedie der Mathematischen Wissenschaften.* Teubner, 1958.

[16] J. Dieudonné. *Abrégé d'Histoire des Mathématiques, 1700-1900, I, II.* Hermann, 1978.

[17] D.S. Dummit and R.M. Foote. *Abstract Algebra.* John Wiley & Sons, 2004.

[18] E. Freitag. *Siegelsche Modulfunktionen.* Springer-Verlag, 1983.

[19] W. Fulton. *Algebraic Curves, An Introduction to Algebraic Geometry.* Addison-Wesley Publishing, 1989.

[20] D. Garbanati. Class field theory summarized. *Rocky Mountain Journal of Mathematics*, 11(2):195–225, 1981.

[21] E. Goren. Private communication. October 5, 2005.

[22] E. Goren. On certain reduction problems concerning abelian surfaces. *Manuscripta Math.*, 94:33–43, 1997.

[23] E. Goren and K. Lauter. Class invariants for quartic CM-fields. Preprint.

[24] E. Goren and K. Lauter. Evil primes and superspecial moduli. In preparation.

[25] P.A. Griffiths. *Introduction to Algebraic Curves.* American Mathematical Society, 1989.

[26] Klingen. H. *Introductory Lectures on Siegel Modular Forms.* Cambrigde studies in advanced mathematics, 1990.

[27] H. Hasse. *Bericht uber neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkorper, Teil I,Ia,II.* Physica-Verlag, 1965.

[28] M. Hindry and J.H. Silverman. *Diophantine Geometry, An Introduction.* Springer-Verlag, 2000.

[29] C. Houzel. *La Géométrie Algébrique, Recherches Historiques.* Édition Albert Blanchard, 2002.

[30] J.I. Igusa. On siegel modular forms of genus two II. *Am. J. Math.*, 86:392–412, 1964.

[31] S. Iyanaga. *The Theory of Numbers.* North. Holland Publishing Company, 1975.

[32] G. J. Janusz. *Algebraic Number Fields.* American Mathematical Society, 1996.

[33] F. Kirwan. *Complex Algebraic Curves*, volume 23. London Mathematical Society, 1992.

[34] F. Klein. *Lectures on the Icosahedron and the Solution of Equations of the Fifth Degree.* Kegan Paul, 1913.

[35] W. Knapp. *Elliptic Curves.* Princeton University Press, 1992.

[36] K. Knopp. *Theory of Functions I,II,III,IV and V.* Dover Publications, 1945.

[37] H. Koch. *Number Theory, Algebraic Numbers and Functions.* American Mathematical Society, 2000.

[38] S. Konno. On Kronecker's limit formula in a totally imaginary quadratic field over a totally real algebraic number field. *J. Math. Soc. Japan*, 17(4):411–424, 1965.

[39] S.-H. Kwon. The non-normal quartic cm-fields and the octic dihedral cm-fields with relative class number two. *Journal of Number Theory*, 79:175–193, 1999.

[40] S. Lang. *Complex Multiplication.* Springer-Verlag, 1983.

[41] S. Lang. *Elliptic Functions.* Springer-Verlag, 1987.

[42] D. A. Marcus. *Number Fields.* Springer-Verlag, 1977.

[43] H. McKean and V. Moll. *Elliptic Curves.* Cambridge University Press, 1997.

[44] K. Miyake. *Class Field Theory-Its Centenary and Prospect.* Mathematical Society of Japan, 2000.

[45] D. Mumford. *Tata Lectures on Theta I, II.* Birkhauser, 1983.

[46] D. Mumford. *The Red Book of Varieties, Second Expanded Edition.* Springer-Verlag, 1999.

[47] W. Narkiewicz. *Elementary and Analytic Theory of Algebraic Numbers.* Springer-Verlag, 2004.

[48] J. Neukirch. *Algebraic Number Theory.* Springer-Verlag, 1999.

[49] Y.-H. Park and S.-H. Kwon. Determination of all non-quadratic imaginary cyclic number fields of 2-power degree with relative class number ≤ 20. *Acta Mathematica*, LXXXIII(3):211–221, 1998.

[50] R.S. Pierce. *Associative Algebras.* Springer-Verlag, 1982.

[51] K. Ramachandra. Some applications of Kronecker's limit formulas. *Ann. Math.*, 80:104–148, 1964.

[52] R. Remmert. *Theory of Complex Functions.* Springer-Verlag, 1989.

[53] P. Ribenboim. *Classical Theory of Algebraic Numbers.* Springer-Verlag, 2001.

[54] A. Robert. Introduction aux variétés abéliennes complexes. *Enseign. Math.*, 28:91–137, 1982.

[55] G. Robert. Unités elliptiques. *Bull. Soc. Math. France, Mémoire*, 36, 1973.

[56] K. Rubin. A Stark conjecture over $\mathbb{Z}$ for abelian L-functions with multiple zeros. *Annales de l'Institut Fourier*, 46(1):33–62, 1996.

[57] C. Sasaki, M. Sugiura, and J.W. Dauben. *The Intersection of History and Mathematics.* Birkhauser, 1994.

[58] J.-P. Serre. *Cours d'Arithmétique.* Presses Universitaires de France, 1970.

[59] I.R. Shafarevich. *Basic Algebraic Geometry I and II.* Springer-Verlag, 1994.

[60] G. Shimura. *Automorphic Functions and Number Theory.* Lectures Notes in Mathematics,Springer-Verlag, 1968.

[61] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton university press, 1971.

[62] G. Shimura and Y. Taniyama. *Complex Multiplication of Abelian Varieties and its Applications to Number Theory.* The Mathematical Society of Japan, 1961.

[63] C.L. Siegel. *Analytic Functions of Several Complex Variables.* Institute for Advanced Study, 1954.

[64] C.L. Siegel. *Topics in Complex Function Theory I,II,III.* Wiley-Interscience, 1969.

[65] C.L. Siegel. *Advanced Analytic Number Theory.* Tata Institute of Fundamental Research, 1980.

[66] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[67] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves.* Springer-Verlag, 1994.

[68] H.M. Stark. Values of L-functions at $s = 1$ I. L-functions for quadratic forms. *Advances in Math.*, 7:301–343, 1971.

[69] H.M. Stark. L-functions at $s = 1$ II. Artin L-functions with rational characters. *Advances in Math.*, 17:60–92, 1975.

[70] H.M. Stark. L-functions at $s = 1$ III. Totally real fields and hilbert's twelfth problem. *Advances in Math.*, 22:64–84, 1976.

[71] H.M. Stark. L-functions at $s = 1$ IV. First derivatives at s=0. *Advances in Math.*, 35:197–235, 1980.

[72] H.P.F. Swinnerton-Dyer. *Analytic Theory of Abelian Varieties.* Cambridge University Press, 1974.

[73] J. Tate. *Les Conjectures de Stark sur les Fonctions L d'Artin en s=0.* Birkhauser, 1984.

[74] B.L. van der Waerden. *Algebra.* Springer-Verlag, 1991.

[75] S.G. Vladut. *Kronecker's Jugentraum and Modular Functions.* Gordon and breach science publishers, 1991.

[76] P.V. Wamelen. Examples of genus two CM-curves defined over the rationals. *Math. Comp.*, 68(225):307–320, 1999.

[77] L.C. Washington. *Introduction to Cyclotomic Field.* Springer-Verlag, 1982.

[78] A. Weil. *Basic Number Theory*, volume 144. Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen, Springer-Verlag, 1967.

[79] A. Weil. *Elliptic Functions According to Eisenstein and Kronecker*, volume 88. Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag, 1976.

[80] A. Weng. Constructing hyperelliptic curves of genus 2 suitable for cryptography. *Math. Comp.*, 72(241):435–458, 2003.

[81] G. Whittaker E., Watson. *A Course of Modern Analysis.* Cambridge university press, 1927.