MASTER'S DEGREE THESIS

Master of Science in Advanced Mathematics and Mathematical Engineering

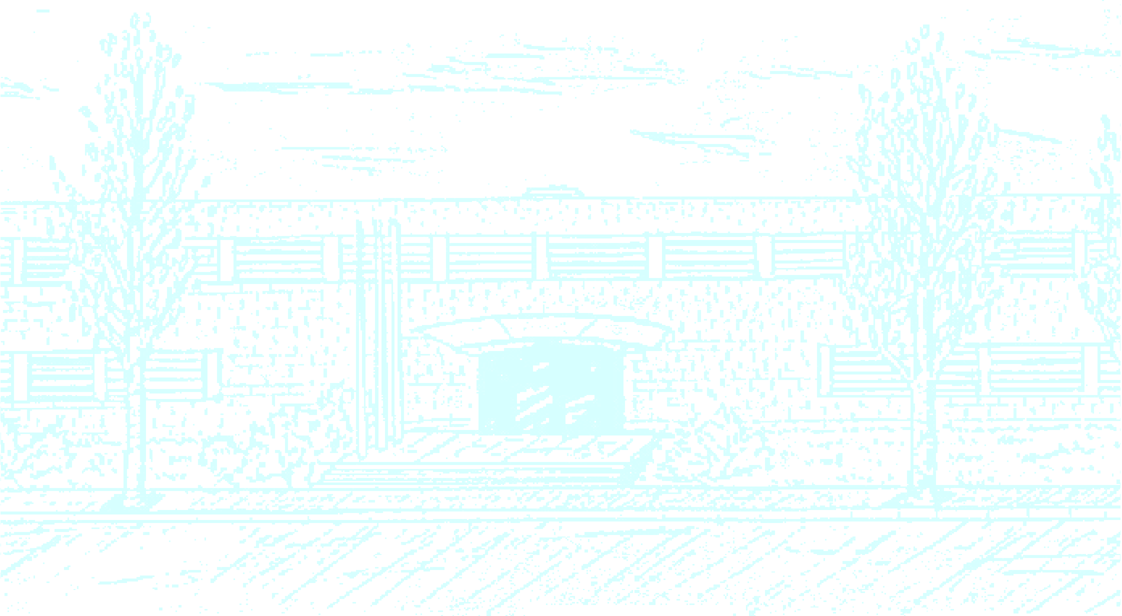
Title: Understanding the factorization mod p of polynomials via modular forms

Author: Eloi Torrents Juste

Advisor: dr. Marc Masdeu and dr. Joan C. Lario

Department: Mathematics

Academic year: 2019--2020



UNIVERSITAT POLITÈCNICA DE CATALUNYA
BARCELONATECH
Facultat de Matemàtiques i Estadística

Universitat Politècnica de Catalunya
Facultat de Matemàtiques i Estadística

Master in Advanced Mathematics and Mathematical Engineering
Master's thesis

Understanding the factorization mod p of polynomials via modular forms

Eloi Torrents Juste

Supervised by dr. Marc Masdeu and dr. Joan C. Lario

September, 2020

I would like to thank my supervisors, especially to Marc Masdeu for his valuable help during the development of this thesis.

Abstract

In this work we relate the factorization of polynomials modulo p with the splitting of primes in number fields, and we study in which cases the different possibilities of factorization or splitting can be explained by the coefficients of the q-expansion of a certain modular form.

Keywords

Class field theory, modular forms

Contents

1. Introduction

In this dissertation we explore a relation between polynomial factorization modulo a prime, ideal factorization in number fields, quadratic forms and theta series. The main goal of this work is to detail an example explained in [1, pp. 41-43], with the intention to make it accessible to a reader with basic knowledge in number theory.

In the first part of the work, we will start introducing the basic concepts of algebraic number theory following [7]. The main phenomenon that we study is the splitting of primes in number fields, which is tightly related to the factorization of polynomials modulo primes. This will allow us to understand the factorization of the polynomial $x^3 - x - 1$ modulo p through the splitting of p in $F = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - x - 1$.

To have a better understanding of the splitting of primes in F, we consider the normal closure $H = F^{\text{Gal}}$ of the extension $F/\mathbb{Q}$, which can be achieved by adjoining every root of $x^3 - x - 1$ to $\mathbb{Q}$. We have that $\sqrt{-23} \in H$ since the discriminant of $x^3 - x - 1$ is $\big((\alpha - \beta)(\alpha - \bar{\beta})(\beta - \bar{\beta})\big)^2 = -23$. Therefore the field H has the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-23})$ as a subfield. We have the following diagram of field inclusions

$$\begin{tikzcd}
 & H = F^{\text{Gal}} \arrow[dl, dash] \arrow[ddr, dash] & \\
F = \mathbb{Q}(\alpha) \arrow[ddr, dash, "3"] & & \\
 & & K = \mathbb{Q}(\sqrt{-23}) \arrow[dl, dash, "2"'] \\
 & \mathbb{Q} &
\end{tikzcd}$$

Figure 1: Field diagram of this work. α is a root of $x^3 - x - 1$.

It is well know that the splitting of a prime in a field and the splitting in its normal closure are related in the sense that if a prime splits completely in one of these fields, it splits completely in the other. On the other hand, the field extension H/K is normal, and we show that H is the Hilbert class field of K. Therefore principal primes of K split completely in H. Using these facts, we show the relation between the splitting of primes in the fields F and K.

In the second part of this work, we relate the splitting of a prime p in the imaginary quadratic field K, with the representations of p by certain quadratic forms. For each such quadratic form Q, we construct its theta series $\Theta_Q(z)$. This is the periodic function having as its n-th Fourier coefficient the number of distinct representations of n by Q. These functions satisfy a concrete transformation property described by the Hecke-Schoeneberg Theorem.

On the other hand we use a very important function in number theory, the Dedekind eta function,

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n), \quad \text{where } q = e^{2\pi i z}$$

to construct the function

$$f(z) = \eta(z)\eta(23z) = q \prod_{n=1}^{\infty} (1 - q^n)(1 - q^{23n}). \tag{1}$$

We prove that f satisfies the same transformation property as the mentioned theta series. Using the theory of modular forms, the functions f and each Θ_Q belong to a certain vector space of modular forms. In this space we find that two different forms must differ in the first four Fourier coefficients. Using this, we find that f equals a particular linear combination of theta series.

Finally, the equality of the two functions implies that for any prime p, computing the p-th coefficient of the formal product is sufficient to know the factorization of the polynomial $x^3 - x - 1$ modulo p and vice versa.

As an illustration, a few terms of (1) are

$$\begin{aligned} q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n}) =& q-q^2-q^3+q^6+q^8-q^{13}-q^{16}+q^{23}-q^{24}+q^{25}+q^{26}\\ &+q^{27}-q^{29}-q^{31}+q^{39}-q^{41}-q^{46}-q^{47}+q^{48}+q^{49}-q^{50}\\ &-q^{54}+q^{58}+2q^{59}\ldots \end{aligned}$$

The coefficients of the exponents $2, 3, 13, \ldots$ are -1, and $x^3 - x - 1$ modulo these primes is irreducible. The coefficients of the exponents $5, 7, 11, \ldots$ are 0, and $x^3 - x - 1$ has two factors modulo these primes,

$$\begin{aligned} x^3-x-1 &\equiv (x+3)(x^2+2x+3) \pmod 5\\ x^3-x-1 &\equiv (x+2)(x^2+5x+3) \pmod 7\\ x^3-x-1 &\equiv (x+5)(x^2+6x+2) \pmod{11}. \end{aligned}$$

The 23-th position is the only prime position with coefficient 1, and we have the factorization

$$x^3-x-1 \equiv (x+20)(x+13)^2 \pmod{23}.$$

Finally the coefficients of the exponents $59, \ldots$ are 2, and x^3-x-1 factors completely modulo these primes,

$$x^3-x-1 \equiv (x+17)(x+46)(x+55) \pmod{59}.$$

Part I

Algebraic number theory

2. Introduction to number fields

Every field extension of $\mathbb{Q}$ can be considered as a $\mathbb{Q}$-vector space. When this extension is of finite degree, we say that the field is a *number field*. The elements of a number field are *algebraic numbers*: if α is an element of a number field of degree n, there is some rational linear dependence between $1, \alpha, \alpha^2, \dots, \alpha^n$, and therefore α is a root of some monic polynomial with rational coefficients.

The Primitive element Theorem shows that every number field K can be constructed by adjoining only one generator α. This is usually written as $K = \mathbb{Q}(\alpha)$. If K has degree n over $\mathbb{Q}$, there are n distinct embeddings σ_i of K in $\mathbb{C}$ which are fully determined with $\sigma_i(\alpha) = \theta_i$ where $\theta_1, \dots, \theta_n$ are the complex roots of the minimal polynomial of α. Taking into account all these embeddings, we define the *norm of an element* β of a number field K to be

$$N_K(\beta) = \sigma_1(\beta) \dots \sigma_n(\beta).$$

Note that the norm is multiplicative, since the embeddings σ_i are.

The norm of a generator of K, is just the product of all their conjugates, which is the constant term of its minimal polynomial (except for the sign), so it is rational. In general, if K is a degree d extension of $\mathbb{Q}(\alpha)$, we have $N_K(\alpha) = (N_{\mathbb{Q}(\alpha)}(\alpha))^d$ since each embedding of $\mathbb{Q}(\alpha)$ in $\mathbb{C}$ extends to d embeddings of K in $\mathbb{C}$. Thus we conclude that the norm can only take rational values.

2.1 The ring of integers of a number field

The numbers whose minimal polynomial is monic and with integer coefficients are said to be *algebraic integers*. The *ring of integers* $\mathcal{O}_K$ of a number field K is the subset of algebraic integers that it contains. For example, the ring of integers of $\mathbb{Q}$ is just $\mathbb{Z}$. Therefore we can think that the ring of integers of a number field is a generalization of the regular integers.

The ring of integers of a number field is finitely generated and every basis, called integral basis, has exactly n elements (it is a free abelian group of rank n) [7, corollary of Theorem 9]. In general, it is not straightforward to explicitly find an integral basis of a number field, but for our purposes we will be able to verify that we have found one using the discriminant.

Let $\alpha_1, \dots, \alpha_n$ be elements of $\mathcal{O}_K$, and let $\sigma_1, \dots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. The *discriminant* of $\alpha_1, \dots, \alpha_n$ is defined as

$$d(\alpha_1, \dots, \alpha_n) = \begin{vmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{vmatrix}^2 .$$

Given an integral basis $\{\beta_1, \dots, \beta_n\}$, we can write any integral set $\{\alpha_1, \dots, \alpha_n\}$ as

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} = M \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_n \end{pmatrix} \tag{2}$$

for some matrix M with integer coefficients. When the determinant of M is ± 1, the matrix has an inverse with integer coefficients and in this case $\{\alpha_1, \dots, \alpha_n\}$ is also a basis.

Applying all σ_i to each row of Equation (2), we obtain

$$\begin{pmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_1(\alpha_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\alpha_1) & \cdots & \sigma_n(\alpha_n) \end{pmatrix} = M \begin{pmatrix} \sigma_1(\beta_1) & \cdots & \sigma_1(\beta_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(\beta_1) & \cdots & \sigma_n(\beta_n) \end{pmatrix},$$

and after taking determinants and squaring, we get

$$d(\alpha_1, \dots, \alpha_n) = \det(M)^2 d(\beta_1, \dots, \beta_n). \tag{3}$$

Thus $\det(\alpha_1, \dots, \alpha_n) = \det(\beta_1, \dots, \beta_n)$ if and only if the set $\{\alpha_1, \dots, \alpha_n\}$ is also an integral basis. Using this fact, the *discriminant* of the number field K is defined as $\Delta_K = d(\beta_1, \dots, \beta_n)$ for any basis $\{\beta_1, \dots, \beta_i\}$.

Let α be an algebraic number with minimal polynomial $g(x)$ of degree n. From the definition, We describe a method to compute the discriminant of $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. Let α_i be the conjugates of α. From the definition, the discriminant of $1, \alpha, \alpha^2, \dots, \alpha^n$ is the square of the determinant of a Vandermonde matrix,

$$d(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \begin{vmatrix} 1 & \alpha_1 & \dots & \alpha_1^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \dots & \alpha_n^{n-1} \end{vmatrix}^2 = \prod_{i \neq j} (\alpha_i - \alpha_j)^2 = \operatorname{disc}(g).$$

Now we observe that the minimal polynomial of α is $g(x) = \prod_{i=1}^n (x - \alpha_i)$ and its derivative is $g'(x) = \sum_{j=1}^n \prod_{i \neq j} (x - \alpha_i)$. When we evaluate it at a root α_j, almost every product becomes zero except for one: $g'(\alpha_j) = \prod_{i \neq j} (\alpha_j - \alpha_i)$. Now we consider the product $N(g'(\alpha)) = \prod_{j=i}^n g'(\alpha_j)$, which has every factor $\alpha_i - \alpha_j$ repeated twice up to the sign. If we group similar factors together we obtain $(-1)^{\binom{n}{2}} \operatorname{disc}(g)$, since we have to change one sign for each pair. We get a direct way to compute the discriminant,

$$d(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = (-1)^{\binom{n}{2}} N(g'(\alpha)). \tag{4}$$

Discriminant of a quadratic number field

We aim to understand the ring of integers of $\mathbb{Q}(\sqrt{-23})$. More generally, we will work with any quadratic field $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer. Its ring of integers consists of the algebraic numbers of the form $\theta = \alpha + \beta\sqrt{d}$ such that they are roots of some monic polynomial with integer coefficients. Since the field $\mathbb{Q}(\sqrt{d})$ is a 2 dimensional vector space over $\mathbb{Q}$, there is some linear dependence between $1, \theta$ and θ^2, for example $\theta^2 - 2\alpha\theta + \alpha^2 - d\beta^2 = 0$. This gives the minimal polynomial of θ, which has integer coefficients if both coefficients 2α and $\alpha^2 - d\beta^2$ are integers. This is the case if both α and β are integers or if α is half an integer, and $d\beta^2$ is a quarter of an integer, in which case β must be half an integer and $d \equiv 1 \pmod 4$.

Thus, we can conclude that the ring of integers is

$$\mathcal{O}_K = \begin{cases} \{\alpha + \beta\frac{1+\sqrt{d}}{2} \mid \alpha, \beta \in \mathbb{Z}\} & \text{if } d \equiv 1 \pmod 4 \\ \{\alpha + \beta\sqrt{d} \mid \alpha, \beta \in \mathbb{Z}\} & \text{otherwise} \end{cases} \tag{5}$$

Now we can compute its discriminant using the previous basis. We only need to compute the discriminant of the minimal polynomial of its generator. We obtain

$$\Delta_K = \begin{cases} \operatorname{disc}(x^2 - x + \frac{1-d}{4}) = d & \text{if } d \equiv 1 \pmod 4 \\ \operatorname{disc}(x^2 - d) = 4d & \text{otherwise} \end{cases}. \tag{6}$$

Therefore the discriminant of $K = \mathbb{Q}(\sqrt{-23})$ is $\Delta_K = -23$.

Discriminant of the cubic field F

We check that the ring of integers of the field $F = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - x - 1$, is $\mathcal{O}_F = \mathbb{Z}[\alpha]$. To do so we will see that the discriminant of $1, \alpha, \alpha^2$ is squarefree, and by Equation 3 we deduce that $1, \alpha, \alpha^2$ is a basis for the ring of integers of F.

Since the minimal polynomial of α is $g(x) = x^3 - x - 1$, using Equation (4), we need to compute the norm of $\xi = g'(\alpha) = 3\alpha^2 - 1$. This can be done by finding a linear combination of $1, \xi, \xi^2$ and ξ^3, which is $\xi^3 - 3\xi^2 - 23 = 0$. This is the minimal polynomial of ξ, and we get the norm from the constant term: $\operatorname{disc}(p) = -N(p'(\alpha)) = -23$. So we get $\operatorname{disc}(1, \alpha, \alpha^2) = -23$, which is square free. Therefore the discriminant of F is $\Delta_F = -23$.

2.2 The ideals of the ring of integers

In a number ring, the analogue of prime numbers are irreducible elements, which are those elements that cannot be obtained as the product of two noninvertible elements. It turns out that in general, the ring of integers of a number field is not a unique factorization domain. For instance in $\mathbb{Q}(\sqrt{-5})$ we have that 6 has two different factorizations: $2 \cdot 3 = 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ and every factor of this expression is irreducible. This inconvenience can be solved working with ideals instead of with elements.

We say that an additive subgroup $\mathfrak{a}$ of an arbitrary ring R, is an *ideal*, if it satisfies that whenever $a \in \mathfrak{a}$, then $ab \in \mathfrak{a}$ for any $b \in R$. In this case, the quotient group ${}^{R}\!/_{\mathfrak{a}}$ has a well-defined induced ring structure.

Since any number ring $\mathcal{O}_K$ is a free abelian group of rank n, any ideal is a subgroup of rank at most n, so it is finitely generated. Therefore, any ring of integers $\mathcal{O}_K$ is a Noetherian ring. We will prove unique factorization in any ring of integers using this together with a divisibility property.

If the generators of an ideal $\mathfrak{a}$ are the elements $\alpha_1, \dots, \alpha_k$, then one writes $\mathfrak{a} = (\alpha_1, \dots, \alpha_k)$. If a is any nonzero element of an ideal $\mathfrak{a}$, we have that $\mathfrak{a}$ contains the rank n group $a\mathcal{O}_K$ and since $\mathfrak{a}$ has rank at most n, the ideal $\mathfrak{a}$ must have rank exactly n. This means that the group ${}^{\mathcal{O}_K}\!/_{\mathfrak{a}}$ is the quotient of two free abelian groups of the same rank, so it is finite. We define the *norm* of the ideal $\mathfrak{a}$ as

$$N(\mathfrak{a}) = [\mathcal{O}_K : \mathfrak{a}] = \left|{}^{\mathcal{O}_K}\!/_{\mathfrak{a}}\right|.$$

2.3 Prime ideals and unique factorization

Let R be an arbitrary unitary commutative ring. We define the sum and the product of two ideals $\mathfrak{a}, \mathfrak{b} \subseteq R$ as

- $\mathfrak{a} + \mathfrak{b} = \{a + b \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\}$ which is the minimal ideal containing both $\mathfrak{a}$ and $\mathfrak{b}$.
- $\mathfrak{a}\mathfrak{b} = \{\sum_i a_i b_i \mid a_i \in \mathfrak{a}, b_i \in \mathfrak{b}\}$ which is the minimal ideal containing $\{ab \mid a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\}$.

An ideal $\mathfrak{a}$ is called *maximal* if there is no ideal containing it different from R. This definition is equivalent to saying that the quotient ring $R/\mathfrak{a}$ is a field. A *prime ideal* $\mathfrak{p}$ is an ideal different from R which satisfies that if $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. This definition is equivalent to $R/\mathfrak{p}$ being an integral domain. Since a field is in particular an integral domain, every maximal ideal is prime. The converse is not always true, but in a ring of integers $\mathcal{O}_K$ if $\mathfrak{p}$ is a prime ideal different from $\{0\}$ we know that the quotient $\mathcal{O}_K/\mathfrak{p}$ is a finite integral domain, so it is a field and $\mathfrak{p}$ is also maximal. This field is called the residue field of $\mathfrak{p}$, and it is often written as $\kappa(\mathfrak{p})$.

We prove that in a ring of integers $\mathcal{O}_K$, every ideal decomposes uniquely into prime ideals. Thus, they are *Dedekind domains*. To do so, we need to use the cancellation law for ideals, if $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{c}$ with $\mathfrak{c} \neq 0$, then $\mathfrak{a} = \mathfrak{b}$. This is not difficult to prove, but we will obtain a very simple proof later, while working on ideal classes.

Theorem 1. *If K is a number field, every ideal of $\mathcal{O}_K$ decomposes uniquely in prime ideal factors.*

Proof. First, we need to show that any ideal in $\mathcal{O}_K$ contains a product of prime ideals. This can be done using Noetherian induction as follows: if there were some counterexample $\mathfrak{a}_o$, there must exist an ideal $\mathfrak{a}$ containing $\mathfrak{a}_0$ such that any ideal containing it is a product of prime ideals, otherwise we could construct an infinitely increasing chain $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset ...$ of counterexamples. The ideal $\mathfrak{a}$ is not prime, so there exist some elements $r, s \in \mathcal{O}_K \setminus \mathfrak{a}$ such that $rs \in \mathfrak{a}$. Finally we have that $\mathfrak{a} \subset \mathfrak{a} + (r)$ and therefore the ideal $\mathfrak{a} + (r)$ contains some product of primes. The same is true for the ideal $\mathfrak{a} + (s)$. At the end we get to a contradiction since $(\mathfrak{a} + (r))(\mathfrak{a} + (s)) \subset \mathfrak{a}$ which means that $\mathfrak{a}$ contains some product of primes.

If some ideal does not decompose in prime factors, using the same argument as before, we know that there is some ideal maximally satisfying this property (any ideal containing it does not satisfy it). This ideal cannot be prime. We know that it must contain some product of primes but at the same time it is contained in a maximal ideal $\mathfrak{p}$. This means that $\mathfrak{p}$ contains the product of primes. Hence it contains one of them. But since a prime ideal is also a maximal ideal, they must be equal. We find that the ideal $\mathfrak{a}$ is divisible by $\mathfrak{p}$. Thus, $\mathfrak{a} = \mathfrak{a}'\mathfrak{p}$ for some ideal $\mathfrak{a}'$. Since $\mathfrak{a} \subset \mathfrak{a}'$, and we assumed that any ideal containing $\mathfrak{a}$ decomposes in prime ideal factors, so does $\mathfrak{a}$.

Now we prove uniqueness of the prime decomposition. If we have two prime decompositions of an ideal $\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_r = \mathfrak{q}_1 ... \mathfrak{q}_s$. Then $\mathfrak{p}_1$ contains a product of primes, so it contains one of them, say $\mathfrak{q}_i$. Since $\mathfrak{p}_1$ is maximal, it must be the case that $\mathfrak{p}_1 = \mathfrak{q}_i$. Cancelling $\mathfrak{p}_1$ in both sides and repeating the argument we get that $r = s$ and the primes coincide except for some permutation. □

This result can be used directly to compute the norm of an ideal $\mathfrak{a} = \mathfrak{p}_1 ... \mathfrak{p}_r$. It is only necessary to know how to compute $N(\mathfrak{a}\mathfrak{p})$ when $\mathfrak{p}$ is a prime ideal. In this case we have the equality $[\mathcal{O}_K : \mathfrak{a}\mathfrak{p}] = [\mathcal{O}_K : \mathfrak{a}][\mathfrak{a} : \mathfrak{a}\mathfrak{p}]$ which by definition is

$$N(\mathfrak{a}\mathfrak{p}) = N(\mathfrak{a})[\mathfrak{a} : \mathfrak{a}\mathfrak{p}].$$

And finally we compute the index $[\mathfrak{a} : \mathfrak{a}\mathfrak{p}]$ for any prime $\mathfrak{p}$. we know that $\mathfrak{a}\mathfrak{p} \subsetneq \mathfrak{a}$ since we have unique factorization, and if we take $\alpha \in \mathfrak{a} \setminus \mathfrak{a}\mathfrak{p}$, we have that $\mathfrak{a}\mathfrak{p} + (\alpha) = \mathfrak{a}$, by the same reason. We define the following surjective morphism

$$\begin{aligned} \varphi : \mathcal{O}_K &\to \mathfrak{a}\mathfrak{p}/\mathfrak{p} \\ x &\mapsto \alpha x + \mathfrak{p}. \end{aligned}$$

Its kernel is different than $\mathcal{O}_K$, and it contains $\mathfrak{p}$. Since $\mathfrak{p}$ is a maximal ideal, we have that $\ker \varphi = \mathfrak{p}$. Thus, $\mathcal{O}_K/\mathfrak{p} \cong \mathfrak{a}\mathfrak{p}/\mathfrak{p}$. From this we have that $[\mathfrak{a} : \mathfrak{a}\mathfrak{p}] = N(\mathfrak{p})$, and we conclude that $N(\mathfrak{a}\mathfrak{p}) = N(\mathfrak{a})N(\mathfrak{p})$. Therefore, the norm of ideals is multiplicative.

To end this section, we show some general facts about ideals that will be useful later.

A *principal ideal* is one which can be generated by a single element. A *principal ideal domain* is an integral domain for which any ideal is principal.

For any ideal $\mathfrak{a}$ in a ring of integers $\mathcal{O}_K$, there exists an ideal $\mathfrak{a}'$ such that $\mathfrak{a}\mathfrak{a}'$ is principal. This fact could be proved right now [7, Theorem 15], but later we will get this for free.

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a ring of integers $\mathcal{O}_K$. We say that $\mathfrak{a}$ divides $\mathfrak{b}$ and we write $\mathfrak{a} \mid b$ if there exist an ideal $\mathfrak{c}$ such that $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$. This directly implies that $\mathfrak{a} \supset \mathfrak{b}$. The other direction also holds, there is some ideal $\mathfrak{a}'$ such that the product $\mathfrak{a}\mathfrak{a}'$ is principal, say $\mathfrak{a}\mathfrak{a}' = (\alpha)$. We have $\mathfrak{a}\mathfrak{a}' = (\alpha) \supset \mathfrak{a}'\mathfrak{b}$, so every element of $\mathfrak{a}'\mathfrak{b}$ is a multiple of α, and $\mathfrak{c} = \frac{1}{\alpha}\mathfrak{a}'\mathfrak{b}$ is a subset of $\mathcal{O}_K$. Clearly this is an additive group, and it is an ideal; given $x \in \mathcal{O}_K$, $y \in \frac{1}{\alpha}\mathfrak{a}'\mathfrak{b}$ we have $xy \in \frac{1}{\alpha}\mathfrak{a}'\mathfrak{b}$ is equivalent to $\alpha xy \in a'\mathfrak{b}$, but αy belongs to the ideal $\mathfrak{a}'\mathfrak{b}$ and so does αxy. This proves that $xy \in \frac{1}{\alpha}\mathfrak{a}'\mathfrak{b}$, and finally $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$.

In short, $\mathfrak{a} \supset \mathfrak{b}$ and $\mathfrak{a} \mid \mathfrak{b}$ are equivalent.

Corollary 2. *A ring of integers $\mathcal{O}_K$ is a unique factorization domain if and only if it is a principal ideal domain.*

Proof. Since we have unique factorization of ideals, in a number field where every ideal is principal we have unique factorization of elements as well (take the generators of the prime ideals that appear in the factorization).

On the other hand, in a unique factorization domain any ideal $\mathfrak{a}$ can become a principal ideal when it is multiplied by some ideal. Let (α) be that principal ideal. If we have unique factorization, $\alpha = \pi_1 \dots \pi_n$. And every ideal (π_i) is actually a prime ideal, since $xy \in (\pi)$, then $\pi | xy$ and from primality of π, we have that either $\pi | x$ or $\pi | y$, which means that either x or y is in π. So we have found the unique decomposition of (α) in principal prime ideals. Since $(a) \supset \mathfrak{a}$, the ideal $\mathfrak{a}$ is a product of principal ideals, so it is principal. □

3. The splitting of primes

3.1 The splitting of primes in F

In the previous section we have seen that in a ring of integers $\mathcal{O}_K$ any ideal decomposes uniquely in prime ideals. Using the following theorem, we will find the explicit decomposition of a prime in the number field $F = \mathbb{Q}(\alpha)$, using that its ring of integers is $\mathbb{Z}[\alpha]$.

Theorem 3 (Dedekind-Kummer). *Let $g(x)$ be an irreducible polynomial with integer coefficients. We consider the factorization of $g \pmod p$*

$$\bar{g} = \bar{g}_1^{e_1} \bar{g}_2^{e_2} \cdots \bar{g}_r^{e_r} \pmod p.$$

Let α be a root of $g(x)$. Assuming that the ring of integers of the number field $K = \mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$, the prime divisors of the ideal $p\mathcal{O}_K$ are $\mathfrak{p}_i = (p, g_i(\alpha))$ and the prime factorization is given by:

$$p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Proof. We compute the set of prime ideals of $\mathcal{O}_K$ that contain the ideal $p\mathcal{O}_K$, which are in correspondence with the prime ideals of $\mathcal{O}_K/p\mathcal{O}_K$. From the assumption that $\mathcal{O}_K = \mathbb{Z}[\alpha]$, we have the isomorphism $\mathcal{O}_K \cong \mathbb{Z}[x]/(g(x))$. We deduce that

$$\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{Z}[x]/(p, g(x)) \cong \mathbb{F}_p[x]/(\bar{g}(x)).$$

The maximal ideals from the latter ring are $(\bar{g}_1), \dots, (\bar{g}_r)$, since the quotient by any of them is the finite field $\mathbb{F}_p[x]/\bar{g}_i(x)$. These ideals satisfy $(\bar{g}_1)^{e_1} \cdots (\bar{g}_r)^{e_r} = (\bar{g}(x)) = 0$, but no product of them with smaller exponents is zero.

On the one hand, the ideal $(\bar{g}_i(x))$ in $\mathbb{F}_p[x]/\bar{g}(x)$ corresponds to the ideal $(g_i(\alpha)) + p\mathcal{O}_K$ in $\mathcal{O}_K/p\mathcal{O}_K$. At the same time this corresponds to the ideal $\mathfrak{p}_\mathrm{i} = (p, g_i(\alpha))$ in $\mathcal{O}_K$. Therefore $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ are all the prime ideals that contain $p\mathcal{O}_K$.

On the other hand, the ideal $(\bar{g}_1)^{e_1} \cdots (\bar{g}_r)^{e_r} = (\bar{g}(x))$ corresponds to the ideal $(g_1(\alpha))^{e_1} \cdots (g_r(\alpha))^{e_r} = 0 + p\mathcal{O}_K$ in $\mathcal{O}_K/p\mathcal{O}_K$, which leads to $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} \subseteq (p, g_1(\alpha)^{e_1} \cdots g_r(\alpha)^{e_r}) = p\mathcal{O}_K$.

Finally, any ideal obtained from some product $\prod(\bar{g}_i(x))^{e_i'}$ with some $e_i' < e_i$, is different from zero, so it does not correspond to $p\mathcal{O}_K$ in $\mathcal{O}_K/p\mathcal{O}_K$. From this, we have $\mathfrak{p}_1^{e_1'} \cdots \mathfrak{p}_r^{e_r'} \subseteq (p, g_1(\alpha)^{e_1'} \cdots g_r(\alpha)^{e_r'}) \not\subset p\mathcal{O}_K$. □

Let α be a root of the polynomial $x^3 - x - 1$. The ring of integers of the cubic number field $F = \mathbb{Q}(\alpha)$ is $\mathcal{O}_F = \mathbb{Z}[\alpha]$, as we saw at the end of Section 2.1. Therefore for the number field F, Theorem 3 can be applied and we obtain a direct relation between the factorization of $x^3 - x - 1 \pmod p$ and the splitting of p in the number field F. As an illustration, in Table 1 we show an example of each possible kind of decomposition. Note that the prime 23 has one factor with multiplicity 2. In section 3.2 we will show that this is the only prime with some multiplicity. Note also that the number ring $\mathcal{O}_F$ is a principal ideal domain. Thus, every ideal on the right column is in fact a principal ideal.

p	factorization of $x^3-x-1 \pmod p$	prime decomposition of $p\mathcal{O}_F$
2	x^3+x+1	$(2,\alpha^3+\alpha+1)=(2)$
5	$(x+3)(x^2+2x+3)$	$(5,\alpha+3)(5,\alpha^2+2\alpha+3)$ $(-\alpha^2+\alpha+2)(2\alpha^2+2\alpha+3)$
23	$(x+20)(x+13)^2$	$(23,\alpha+20)(23,\alpha+13)^2$ $(-3\alpha^2+\alpha+1)(\alpha^2-3\alpha-1)^2$
59	$(x+17)(x+46)(x+55)$	$(59,\alpha+17)(59,\alpha+46)(59,\alpha+55)$ $(-\alpha^2-3\alpha+2)(-2\alpha^2+3\alpha+4)(\alpha^2-4\alpha)$

Table 1: Applying Theorem 3 we have a correspondence between the factorization of x^3-x-1 modulo p and the splitting of p in $F=\mathbb{Q}[x]/(x^3-x-1)$. Every ideal is also written in its principal form.

3.2 Splitting in the extension H/K

Following the main setting of this thesis, we consider the normal closure $H=F^{\text{Gal}}$ of the field extension $F/\mathbb{Q}$. As we explained in the introduction, H contains the field $K=\mathbb{Q}(\sqrt{-23})$. Before dealing with the splitting of primes in the extension H/K, we study its behaviour in general extensions.

Let L/K be a degree n extension of number fields. For every prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ we consider the factorization of the ideal $\mathfrak{p}\mathcal{O}_L$ in prime ideals of $\mathcal{O}_L$,

$$\mathfrak{p}\mathcal{O}_L=\mathfrak{P}_1^{e_1}\dots\mathfrak{P}_r^{e_r}. \tag{7}$$

This product is called the *splitting* of $\mathfrak{p}$ in L. We say that the primes $\mathfrak{P}_i$ of $\mathcal{O}_L$ *lie over the prime* $\mathfrak{p}$ of $\mathcal{O}_K$ and that $\mathfrak{p}$ *lies under* each $\mathfrak{P}_i$. Every prime of $\mathcal{O}_K$ lies under at least one prime of $\mathcal{O}_L$, given by the factorization above, and every prime $\mathfrak{P}$ of $\mathcal{O}_L$ lies over a unique prime of $\mathcal{O}_K$ namely $\mathfrak{P}\cap\mathcal{O}_K$. For each prime $\mathfrak{P}_i$ over $\mathfrak{p}$, we define two important numbers. The *ramification indices* e_i are the exponents that appear in Equation 7, and the *inertial degrees* f_i are defined as the degrees of the extension of finite fields $[{}^{\mathcal{O}_L}/_{\mathfrak{P}_i}:{}^{\mathcal{O}_K}/_{\mathfrak{p}}]$. This is a field extension because we have a ring homomorphism $\mathcal{O}_K\to{}^{\mathcal{O}_L}/_{\mathfrak{P}_i}$ induced from the inclusion $\mathcal{O}_K$ in $\mathcal{O}_L$, and whose kernel is $\mathcal{O}_K\cap\mathfrak{P}_i=\mathfrak{p}$ [7, Theorem 19]. Therefore, we have an embedding ${}^{\mathcal{O}_K}/_{\mathfrak{p}}\hookrightarrow{}^{\mathcal{O}_L}/_{\mathfrak{P}_i}$.

The ramification indexes and the inertial degrees will be written as $e(\mathfrak{P}_i|\mathfrak{p})$ and $f(\mathfrak{P}_i|\mathfrak{p})$ if the extension is not clear from the context.

We say that a prime $\mathfrak{p}$ *ramifies* in L/K if some e_i is greater than 1. Otherwise we say that $\mathfrak{p}$ is *unramified*. We say that an unramified prime is *inert* if $r=1$, and we say that it *splits completely* if its inertial degrees are all 1.

We have a precise control in how much a prime can split in a extension of finite degree.

Proposition 4. *Let L/K be a field extension of degree n. If the splitting of a prime $\mathfrak{p}\subset\mathcal{O}_K$ is $\mathfrak{p}\mathcal{O}_L=\mathfrak{P}_1^{e_1}\dots\mathfrak{P}_r^{e_r}$, then the ramification indexes and the inertial degrees satisfy $\sum_{i=1}^r e_if_i=n$.*

Proof. We compute the norm $N_L(\mathfrak{p}\mathcal{O}_L)$ in two different ways. On the one hand this is $N_K(\mathfrak{p})^n$ since every embedding of K extends to n embeddings of H. On the other, using that the norm is multiplicative, we have $N_L(\mathfrak{p}\mathcal{O}_L)=N_L(\mathfrak{P}_1)^{e_1}\cdots N_L(\mathfrak{P}_r)^{e_r}$. Since the quotient ${}^{\mathcal{O}_L}/_{\mathfrak{P}_i}$ is a finite field of degree f_i over ${}^{\mathcal{O}_K}/_{\mathfrak{p}}$, by definition we have $N_L(\mathfrak{P}_i)=N_K(\mathfrak{p})^{f_i}$. Combining this, we get

$$N_K(\mathfrak{p})^n=N_K(\mathfrak{p})^{f_1e_1}\cdots N_K(\mathfrak{p})^{f_re_r}.$$

The equality is obtained directly from the exponents. □

Proposition 5. *The ramification indexes and the inertial degrees are multiplicative in towers. This means that if we have a tower extension $H/L/K$ and a prime $\mathfrak{P} \subset \mathcal{O}_H$ with the primes $\mathfrak{p} = L \cap \mathfrak{P}$, $p = K \cap \mathfrak{P}$ under it, then the ramification indices satisfy $e(\mathfrak{P}|p) = e(\mathfrak{P}|\mathfrak{p})e(\mathfrak{p}|p)$ and the inertial degrees satisfy $f(\mathfrak{P}|p) = f(\mathfrak{P}|\mathfrak{p})f(\mathfrak{p}|p)$.*

Proof. The multiplicativity of the ramification indexes follows directly from unique factorization. For the inertial degrees it follows from multiplicativity of the indexes of field extensions. □

Splitting in normal extensions

Now we will prove that when the extension H/K is Galois, the splitting of a prime $\mathfrak{p} \subset \mathcal{O}_K$ is of the form

$$\mathfrak{p}\mathcal{O}_H = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e.$$

First, we prove that the Galois group acts transitively over the primes over $\mathfrak{p}$.

Lemma 6. *Given a normal extension H/K, the primes lying over a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ are transitively permuted by* $\mathrm{Gal}(H/K)$ *i.e. for any two primes $\mathfrak{P}, \mathfrak{P}'$ over $\mathfrak{p}$ there exist some $\sigma \in \mathrm{Gal}(H/K)$ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$.*

Proof. Since H/K is normal, H is invariant under any automorphism $\sigma \in \mathrm{Gal}(H/K)$. The ideal $\sigma(\mathfrak{P})$ is a prime in $\sigma(\mathcal{O}_H) = \mathcal{O}_H$ over $\sigma(\mathfrak{p}) = \mathfrak{p}$.

For the sake of contradiction, let's assume that there is some pair of primes $\mathfrak{P}, \mathfrak{P}'$ over $\mathfrak{p}$ which do not satisfy this property. Using the Chinese Remainder Theorem for ideals, we have that the following system of equations has a solution $\alpha \in \mathcal{O}_H$

$$\begin{cases} x \equiv 0 & (\mathrm{mod}\ \mathfrak{P}) \\ x \equiv 1 & (\mathrm{mod}\ \sigma(\mathfrak{P}') \quad \text{for all } \sigma \in \mathrm{Gal}(H/K) \end{cases}.$$

One of the factors of the relative norm $N_K^H(\alpha)$ is α, which belongs to $\mathfrak{P}$ (by the first equation). Therefore we have $N_K^H(\alpha) \in \mathcal{O}_K \cap \mathfrak{P}' = \mathfrak{p}$ [7, Theorem 19]. On the other hand we know that $\alpha \notin \sigma(\mathfrak{P})$ for all $\sigma \in \mathrm{Gal}(H/K)$, therefore we have $\sigma^{-1}(\alpha) \notin \mathfrak{P}$, and

$$N_K^H(\alpha) = \prod_{\sigma \in \mathrm{Gal}(H/K)} \sigma^{-1}(\alpha) \notin \mathfrak{P}.$$

But we have already seen that $N_K^H(\alpha) \in \mathfrak{p} \subset \mathfrak{P}$. This is a contradiction from the assumption that $\sigma(\mathfrak{P}) \neq \mathfrak{P}'$ for all $\sigma \in \mathrm{Gal}(H/K)$. Therefore there is some σ such that $\sigma(\mathfrak{P}) = \mathfrak{P}'$. □

Proposition 7. *Given a normal extension of number fields H/K, the factorization of a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ in $\mathcal{O}_H$ is*

$$\mathfrak{p}\mathcal{O}_H = (\mathfrak{P}_1 \dots \mathfrak{P}_r)^e,$$

where the primes $\mathfrak{P}_1, \dots, \mathfrak{P}_r$ are all distinct and they have the same inertial degree f. Moreover, we have that

$$efr = n.$$

Proof. For any pair of primes $\mathfrak{P}_i, \mathfrak{P}_j \subset \mathcal{O}_H$ over $\mathfrak{p}$, there is an automorphism such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Since $\sigma(\mathfrak{p}) = \mathfrak{p}$ and we have unique factorization of ideals in $\mathcal{O}_H$, it follows that the ramification indexes e_i are all equal.

For the inertial degrees, we have the following isomorphism between the fields $\mathcal{O}_H/\mathfrak{P}$ and $\mathcal{O}_H/\mathfrak{P}'$,

$$\mathcal{O}_H/\mathfrak{P} \to \mathcal{O}_H/\mathfrak{P}'$$
$$x + \mathfrak{P} \mapsto \sigma(x) + \mathfrak{P}'.$$

□

Using the normal closure of a number field K, we can find a condition that we can use to find the ramified primes of K.

Proposition 8. *Any prime that is ramified in K divides the discriminant Δ_K.*

Proof. Let $\{\beta_1, \dots, \beta_n\}$ be a basis of $\mathcal{O}_K$. If the prime p ramifies in K there is a prime $\mathfrak{p}_i$ over p such that $\mathfrak{p}_i^2 | p$. Then we can write $p\mathcal{O}_K = \mathfrak{p}\mathfrak{a}$ with $\mathfrak{a}$ divisible by all primes of $\mathcal{O}_K$ lying over p. We consider an element $\alpha \in \mathfrak{a} \setminus p\mathcal{O}_K$. When we write it as $\alpha = \alpha_1\beta_1 + \cdots + \alpha_n\beta_n$ one of the α_i is not multiple of p (since $\alpha \notin p\mathcal{O}_K$). Without loss of generality we can assume it is α_1 after a suitable rearrangement of the basis of $\mathcal{O}_K$. We have

$$d(\alpha, \beta_2, \dots, \beta_n) = \alpha_1^2 d(\beta_1, \dots, \beta_n) = \alpha_1^2 \Delta_K.$$

By assumption, we have that α is contained in every prime $\mathfrak{p}$ over p. Now we consider the normal closure H of K. Every prime ideal $\mathfrak{P} \subset \mathcal{O}_H$ over p also contains α. Therefore the prime $\sigma^{-1}(\mathfrak{P}) \subset \sigma(\mathcal{O}_H) = \mathcal{O}_H$ contains α. Applying σ we have $\sigma(\alpha) \in \mathfrak{P}$.

This means that the prime $\mathfrak{p}$ contains $d(\alpha, \beta_2, \dots, \beta_n)$. Since the discriminant is integer, it is in the ideal $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$. Therefore, $p \mid \alpha_1^2\Delta_K$ and $p \mid \Delta_K$. □

In the fields $F = \mathbb{Q}(\alpha)$ and $\mathbb{Q}(\sqrt{-23})$, the prime 23 is ramified since it splits as $(-3\alpha^2 + \alpha + 1)(\alpha^2 - 3\alpha - 1)^2$ and $(\sqrt{-23})^2$ respectively. Using the previous theorem, we know that there is no other ramified prime in these fields, since both have discriminant -23.

Proposition 9. *The field extension H/K defined above is normal, abelian and unramified.*

Proof. Since $H/\mathbb{Q}$ is a normal extension, the extension H/K is also normal. Since the extension has degree 3, it's Galois group is the cyclic group of order 3, thus abelian.

Finally, assuming for the sake of contradiction that a prime $\mathfrak{p} \subset \mathcal{O}_K$ ramifies in $\mathcal{O}_H$, we must have that the factorization of $\mathfrak{p}\mathcal{O}_H$ is $\mathfrak{P}^3$ for some prime in $\mathfrak{P} \subset \mathcal{O}_H$, since the extension H/K is normal. By multiplicativity on towers, we have the ramification index in H of the prime under $\mathfrak{p}$ must be either 3 or 6, since $K/\mathbb{Q}$ is a degree 2 extension.

On the other hand the only prime which ramifies in F is 23, and its ramification indexes are 1 and 2. Since H/F is a degree 2 extension, any ramification index is at most 2. We get a contradiction, since it is impossible to get 3 or 6 form the product of two numbers that are at most 2. □

4. Relating the splitting in K and F

Using the results of the previous section, we classify the different ways in which a prime p distinct from 23 can split in F. There are three categories, it can be inert, split completely or split as the product of two primes. These are related with the factorization of the polynomial $x^3 - x - 1$ modulo p, which may be irreducible, factor in three linear factors or factor as the product of two polynomials. Now we will describe a classification of the different ways a prime different from 23 can split in K in terms of the ideal class group, and later we will find that they are closely related to the splitting in F.

4.1 The ideal class group of $K = \mathbb{Q}(\sqrt{-23})$

For any number field K we define an important equivalence relation for the ideals of its number ring $\mathcal{O}_K$. We say that two ideals $\mathfrak{a}, \mathfrak{b} \subset \mathcal{O}_K$ belong to the same class if there exist some element $\alpha \in K$ such that $\mathfrak{a} = \alpha\mathfrak{b}$. This is easily seen to be an equivalence relation, and we write it as $\mathfrak{a} \sim \mathfrak{b}$. The following result implies that in a number ring $\mathcal{O}_K$, there are a finite number of ideal classes.

Theorem 10 (Minkowski bound). *Every ideal class of a number ring $\mathcal{O}_K$ contains an ideal $\mathfrak{a}$ with norm*

$$N(\mathfrak{a}) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s \sqrt{|\Delta_K|}.$$

Where s is the number of pairs of complex embeddings of K to $\mathbb{C}$.

The proof of Minkowski's Theorem [7, Corollary 2 of Theorem 37] requires an accurate use of geometry of numbers. Here we will give a proof of a slightly better bound that only works for quadratic fields.

After realizing that there is a finite number of ideal classes, we can see that the product of equivalence classes is well-defined, and it actually forms a group. We can also see that the set of principal ideals $\mathcal{P}$ forms a class, and that $[\mathfrak{a}]\mathcal{P} = \mathcal{P}[\mathfrak{a}] = [\mathfrak{a}]$. So it behaves as the neutral element. For any ideal $\mathfrak{a}$, the sequence $[\mathfrak{a}], [\mathfrak{a}]^2, [\mathfrak{a}]^3, \ldots$ eventually repeats, therefore $[\mathfrak{a}]^n = [\mathfrak{a}]^m$ for some integers n and m. The inverse of $[\mathfrak{a}]$ is $[\mathfrak{a}]^{m-n-1}$.

Remark 11. When $\mathcal{O}_K$ is a principal ideal domain, all the ideals belong to the same class, thus the class group $\mathrm{Cl}(K)$ is trivial. In some sense, the class group is a measure on how far from a principal ideal domain the ring $\mathcal{O}_K$ is.

Now we can prove the cancellation law that we used to prove unique factorization. If we have $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$, then we can multiply both sides of the equality by some ideal $\mathfrak{a}'$ belonging to the class $[\mathfrak{a}]^{-1}$ to make the product $\mathfrak{a}'\mathfrak{a}$ principal. Let α be its generator, we have $\alpha\mathfrak{b} = \alpha\mathfrak{c}$ and it follows that $\mathfrak{b} = \mathfrak{c}$.

Proposition 12. *Every ideal class of a quadratic number ring $\mathcal{O}_K$ contains an ideal $\mathfrak{a}$ with norm*

$$N(\mathfrak{a}) \leq \sqrt{|\Delta_K|/3}.$$

In particular, the class group of a quadratic field is finite.

Proof. We start with any ideal $\mathfrak{a}$, of norm $N(\mathfrak{a}) = a$, and we will reduce its norm as much as we can while staying on the same ideal class. First, if $\mathfrak{a}$ is divisible by a principal ideal (k) with $k \in \mathbb{Z}$, dividing $\mathfrak{a}$ by k doesn't change its ideal class. Therefore we may assume that $\mathfrak{a}$ is not divisible by any integer different from ± 1.

Each class of $\mathcal{O}_K/\mathfrak{a}$ has an integer representative: Let m be an integer. Since $\mathfrak{a}|a$, we have that $a|m$ implies $\mathfrak{a}|m$. On the other hand, if $\mathfrak{a}|m$, then $a|m$: Let $\mathfrak{a} = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_n}$ be the prime factorization of $\mathfrak{a}$, and let $p_i = N(\mathfrak{p}_\mathrm{i})$, so $a = p_1^{e_1} \dots p_n^{e_n}$. We check that $\mathfrak{p}_i^{e_i}|m$ implies that $p_i^{e_i}|m$ for every i.

- The prime p_i can't be inert, since then $\mathfrak{a}$ would be divisible by an integer.
- If p_i ramifies, the exponent e_i must be 1 (otherwise $p_1|\mathfrak{a}$). We have $\mathfrak{p}_\mathrm{i}|m$. After taking the norm, we obtain $p_i|m^2$ and therefore $p_i|m$.
- If p_i splits, then $\mathfrak{p}_i^{e_i}|m$ and this is also true for the conjugate: $\bar{\mathfrak{p}}_i^{e_i}|m$. Therefore, since $p = \mathfrak{p}_i\bar{\mathfrak{p}}_i$, we conclude that $p_i^{e_i}|m$.

Since $a|m$ is equivalent to $\mathfrak{a}|m$, the characteristic of $\mathcal{O}/\mathfrak{a}$ is a, and therefore $\mathbb{Z}/aZ \subseteq \mathcal{O}_K/\mathfrak{a}$. But this is in fact an equality, since $N(\mathfrak{a}) = |\mathcal{O}/\mathfrak{a}| = a$.

Using this, we can find an integer s such that $\alpha \equiv s \pmod{\mathfrak{a}}$, where α is the following generator of $\mathcal{O}_K$:

$$\alpha = \begin{cases} \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \pmod 4 \\ \sqrt{d} & \text{otherwise .} \end{cases}$$

Let

$$r = \begin{cases} \frac{2s-1}{2} & \text{if } d \equiv 1 \pmod 4 \\ s & \text{otherwise .} \end{cases}$$

In both cases we have that $r - \frac{\sqrt{\Delta}}{2}$ belongs to the ideal $\mathfrak{a}$. This remains true even if we add a multiple of a to r. Therefore we can add the restriction $|r| \leq a/2$.

We have that $\mathfrak{a}|r - \frac{\sqrt{\Delta}}{2}$, so there exist an ideal $\mathfrak{b}$ such that $\mathfrak{a}\mathfrak{b} = \left(r - \sqrt{\Delta}/2\right)$. Its norm is $N(\mathfrak{a}\mathfrak{b}) = \left|r^2 - \frac{\Delta}{4}\right|$, which is bounded by $r^2 + \frac{|\Delta|}{4} \leq \frac{1}{4}a^2 + \frac{|\Delta|}{4}$.

Since $N(\mathfrak{b}) = \mathfrak{b}\bar{\mathfrak{b}}$, and both $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{b}\bar{\mathfrak{b}}$ are principal, we have $\mathfrak{a} \sim \bar{\mathfrak{b}}$. Now if $N(\mathfrak{a}) \leq N(\mathfrak{b})$, then $N(\mathfrak{a})^2 \leq N(\mathfrak{a}\mathfrak{b}) \leq \frac{N(\mathfrak{a})^2}{4} + \frac{|\Delta|}{4}$, and we deduce that $N(\mathfrak{a}) \leq \sqrt{|\Delta|/3}$.

Otherwise, $N(\bar{\mathfrak{b}}) = N(\mathfrak{b}) < N(\mathfrak{a})$. We repeat this process again with the ideal $\bar{\mathfrak{b}}$, until we obtain an ideal with norm bounded by $\sqrt{|\Delta|/3}$. □

Using the previous result, we show that the class number of $\mathbb{Q}(\sqrt{-23})$ is 3. Every ideal class contains an ideal with norm bounded by $\sqrt{\frac{23}{3}} \approx 2.77 < 3$. Therefore we only need to consider all ideals with norm at most two to determine the class number. Those are the principal ideal (1) and the factors of (2).

Using Theorem 3, we can compute the factorization of the ideal (2) by factoring the polynomial $x^2 - x + 6 \pmod 2$

$$x^2 - x + 6 \equiv x(x+1) \pmod 2 \implies (2) = \mathfrak{p}_2\mathfrak{p}_2' = (2, \frac{1+\sqrt{-23}}{2})(2, \frac{1+\sqrt{-23}}{2} + 1).$$

Finally, the ideals $(2, \frac{1+\sqrt{-23}}{2})$, $(2, \frac{1+\sqrt{-23}}{2} + 1)$ are not principal, since its generator would be an element of norm 2, which do not exist. They belong to different ideal classes since the ideal $(2, \frac{1+\sqrt{-23}}{2})^2 = (4, 1+\sqrt{-23}, \frac{1+\sqrt{-23}}{2}^2)$ is not principal (it has norm 4, but it is not generated by any elemeny of norm 4, which are ± 2), but $(2, \frac{1+\sqrt{-23}}{2})(2, \frac{1+\sqrt{-23}}{2} + 1)$ is. Therefore, there are exactly 3 ideal classes in $\mathcal{O}_K$.

4.2 The Frobenius automorphism

Before relating the splitting in F and K, we will relate the splitting of primes in F and $H = F^{\mathrm{Gal}}$. In particular, we will prove that if a prime splits completely in F, it also splits completely in H.

Let's consider an arbitrary normal extension L/K. For each prime $\mathfrak{P}$ of $\mathcal{O}_L$, we define the *decomposition group*

$$D_{\mathfrak{P}} = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\},$$

which is a subgroup of $\mathrm{Gal}(L/K)$. The prime $\mathfrak{P}$ lies over some prime $\mathfrak{p} \subset \mathcal{O}_K$, hence we can define the group homomorphism

$$\begin{aligned} \varphi_{\mathfrak{P}} : D_{\mathfrak{P}} &\to \mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}}) \\ \sigma &\mapsto \sigma|_{\mathcal{O}_L} \pmod{\mathfrak{P}} \end{aligned}$$

which is well defined since for any element $x \in \mathcal{O}_L$ we can write its the class $\bar{x}$ as $x + \mathfrak{P}$. We have

$$\bar{\sigma}(\bar{x}) = \bar{\sigma}(x + \mathfrak{P}) \equiv \sigma(x + \mathfrak{P}) \equiv \sigma(x) \pmod{\mathfrak{P}}$$

since for any $\sigma \in D_{\mathfrak{P}}$ we have $\sigma(\mathfrak{P}) = \mathfrak{P}$. The kernel of $\varphi_{\mathfrak{P}}$ is

$$\ker \varphi_{\mathfrak{P}} = \{\sigma \in D_{\mathfrak{P}} \text{ such that } \varphi_{\mathfrak{P}}(\sigma) = \mathrm{id}\}.$$

Using the chain of equivalences

$$\bar{\sigma}(\bar{x}) = \bar{x} \iff \sigma(x + \mathfrak{P}) = x + \mathfrak{P} \iff \sigma(x) \equiv x \pmod{\mathfrak{P}},$$

the *inertia group* is defined as

$$I_{\mathfrak{P}} := \ker \varphi = \{\sigma \in D_{\mathfrak{P}} : \sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}} \quad \forall \alpha \in \mathcal{O}_L\}.$$

Proposition 13. *When the prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is not ramified in $\mathcal{O}_L$, then the homomorphism $\varphi_{\mathfrak{P}}$ is an isomorphism.*

Proof. Let $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1 \cdots \mathfrak{P}_r$ be the prime factorization of $\mathfrak{p}$ in $\mathcal{O}_L$ into distinct primes (p is unramified). Let f be the intertial degrees, which are all equal since the extension is normal. Let $\mathfrak{P}$ be one of the primes over p.

Since the decomposition group $D_{\mathfrak{P}}$ is a subgroup of the Galois group, we can partition the latter into cosets of the form $\sigma_i D_{\mathfrak{P}}$. Any member of such coset sends $\mathfrak{P}$ to $\sigma_i(\mathfrak{P})$. It is clear that $\sigma D_{\mathfrak{P}} = \tau D_{\mathfrak{P}}$ is equivalent to $\sigma(\mathfrak{P}) = \tau(\mathfrak{P})$. So there is a one to one correspondence between the right cosets $D_{\mathfrak{P}}\sigma$ and the primes $\sigma(\mathfrak{P})$. Since the Galois group acts transitively over the primes over $\mathfrak{p}$, these primes include all primes of $\mathcal{O}_L$ lying over $\mathfrak{p}$. Hence $[\mathrm{Gal}(L/K) : D_{\mathfrak{P}}] = |\{\text{primes over } \mathfrak{p}\}| = r$. Since $|\mathrm{Gal}(L/K)| = n = ref$, this implies that $|D_{\mathfrak{P}}| = f$. By the first isomorphism Theorem, we have $D_{\mathfrak{P}}/I_{\mathfrak{P}} \cong \mathrm{Im}(\varphi)$.

If we prove that $|D/I| \geq |\mathrm{Gal}(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})| = f$, we are done. We will write L^D, L^I for the subfields of L fixed by the decomposiotion and inertia groups respectively.

We have $[L^I : L^D] = |D/I|$. By multiplicativity on towers, we have $f = f(\mathfrak{P}|\mathfrak{P}^I)f(\mathfrak{P}^I|\mathfrak{P}^D)f(\mathfrak{P}^D|\mathfrak{p})$. We prove that the first and the last factor are 1, therefore $[L^I : L^D] \geq f(\mathfrak{P}^I|\mathfrak{P}^D) = f$ and we will be done.

- $f(\mathfrak{P}^D|\mathfrak{p}) = 1$: $\mathfrak{P}$ is the only prime lying over $\mathfrak{P}^D$, since H/H^D is a normal extension with Galois group D, which fixes $\mathfrak{P}$. Therefore, since $e = 1$ and $[L^D : K] = r$, $f = [L : L^D] = f(\mathfrak{P}|\mathfrak{P}^D)$.

- $f(\mathfrak{P}|\mathfrak{P}^I) = 1$: By definition, we have to prove that $\kappa(\mathfrak{P}) \cong \kappa(\mathfrak{P}^I)$. We will show that the Galois group $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}^I)$ is trivial. For each element $\theta \in \kappa(\mathfrak{P})$, the polynomial $(x-\theta)^m$ has coefficients in $\kappa(\mathfrak{P}^I)$ for some $m \geq 1$: Picking any element $\alpha \in \mathcal{O}_L$ of the class θ, the following polynomial has coeficients in $\mathcal{O}_L^I$,
$$g(x) = \prod_{\sigma \in I_{\mathfrak{P}}} (x - \sigma(\alpha)).$$
Since $\sigma(\alpha) \equiv \alpha \pmod{\mathfrak{P}}$ for any element σ of the inertia group, we have that the reduced polynomial $\bar{g}(x) = (x-\theta)^{|I_{\mathfrak{P}}|}$ has coefficients in $\kappa(\mathfrak{P}_I)$. Thus, any element of the Galois group $\mathrm{Gal}(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}^I))$ maps θ to the only root of $\bar{g}$, which is θ itself. We conclude that this Galois group is trivial.

□

The Galois group of a extension of finite fields is cyclic, generated by the Frobenius endomorphism $\bar{x} \mapsto x^{N(\mathfrak{p})}$. When $\mathfrak{p}$ is unramified in H, since φ is onto, some element $\sigma \in D_{\mathfrak{P}}$ has the Frobenius as image, and $\sigma(\bar{x}) = \bar{x}^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$ for all $x \in \mathcal{O}_H$. This element is called the *Frobenius automorphism* $F_{\mathfrak{P}} \in D_{\mathfrak{P}}$.

Now, if H/K is an abelian extension and $\mathfrak{p} \subset \mathcal{O}_K$ is an unramified prime, we can talk about the Frobenius $F_{\mathfrak{p}}$ as an element of $\mathrm{Gal}(H/K)$. We can extend it for any ideal of $\mathcal{O}_K$ which is not contained in a ramified prime, mapping $\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_n^{e_r}$ to $F_{\mathfrak{p}_1}^{e_1} \dots F_{\mathfrak{p}_r}^{e_r}$.

When the extension H/K is unramified, then this map is defined for any ideal of $\mathcal{O}_K$ and induces a surjective map $\mathrm{Cl}(K) \to \mathrm{Gal}(L/K)$.

4.3 Relating the splitting in K and F using the Artin symbol

We finish the first part of this dissertation with a correspondence between the splitting of primes in the fields F and K. We assume H/K to be an Abelian extension.

Lemma 14. *For any $\sigma \in \mathrm{Gal}(H/K)$, we have $F_{\sigma(\mathfrak{P})} = \sigma F_{\mathfrak{P}} \sigma^{-1}$.*

Proof. By definition we have $F_{\sigma(\mathfrak{P})}\sigma^{-1}(x) \equiv (\sigma^{-1}(x))^{N(\mathfrak{p})} \pmod{\mathfrak{P}}$. After applying σ, we obtain
$$\sigma F_{\sigma(\mathfrak{P})}\sigma^{-1}(x) \equiv \sigma\left(\sigma^{-1}(x)^{N(\mathfrak{p})}\right) \equiv x^{N(\mathfrak{p})} \pmod{\sigma(\mathfrak{P})}.$$

□

In particular, when $\mathrm{Gal}(H/K)$ is an abelian group, we have $F_{\sigma(\mathfrak{P})} = F_{\mathfrak{P}}$, so if $\mathfrak{p} \subset \mathcal{O}_K$ is unramified, we can define the *Artin symbol* $\left(\frac{H/K}{\mathfrak{p}}\right) \in$ *Gal*$(H/K) = F_{\mathfrak{P}}$ for any prime $\mathfrak{P}$ over $\mathfrak{p}$. This definition of the Artin symbol can be extended for any ideal $\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ where $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ are unramified primes, as $\left(\frac{H/K}{\mathfrak{a}}\right) = \prod \left(\frac{H/K}{\mathfrak{p}_i}\right)^{e_i}$.

Definition 15 (Hilbert class field)**.** The Hilbert Class Field of a field K is the maximally unramified abelian extension of K.

Theorem 16 (Class Field Theory)**.** *If H is the Hilbert class field of K, then the Artin map is an isomorphism between the ideal class group of K and the Galois group* $\mathrm{Gal}(H/K)$. *[3, Theorem 5.23]*

Using Theorem 16, we know that the degree of the extension H/K is finite and equals the class number of K. Since in Theorem 9 we have found a unramified abelian extension of K of degree 3, and we have also proved that the class group of K has tree elements, we can conclude that H is the Hilbert class field of K.

Theorem 17. *A prime ideal of K is a principal ideal if and only if it splits completely in H.*

Proof. Using class field theory, we know that $\mathrm{Cl}(K) \cong \mathrm{Gal}(H/K)$ via the Artin map and therefore their neutral elements correspond to each other. In other words, a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ is principal if and only if $(H/K, \mathfrak{p})$ is trivial. This is equivalent to the congruence $x^{N(\mathfrak{p})} \equiv x \pmod{\mathfrak{P}}$ holding for all $x \in \mathcal{O}_H/\mathfrak{P} \cong \mathbb{F}_{q^f}$, which means that $f = 1$ and $r = efr = [H : K]$. This is, the prime splits in r primes in a r degree extension. □

Continuing with the main setting, let $F = \mathbb{Q}(\alpha)$ where α is a root of $x^3 - x - 1$ and let $K = \mathbb{Q}(\sqrt{-23})$.

Corollary 18. *A prime ideal of $K = \mathbb{Q}(\sqrt{-23})$ is non-principal if and only if it is inert in $H = F^{\mathrm{Gal}}$.*

Proof. Since H/K is a normal extension of degree three, a prime either splits completely or it is inert, by Theorem 7. Using the contrapositive of Theorem 17 we get the result. □

Corollary 19. *There are no inert primes in the extension $H/\mathbb{Q}$.*

Proof. If a prime were inert in $H/\mathbb{Q}$, it would be inert in $K/\mathbb{Q}$. Hence it would be principal. But since principal ideals split completely we get a contradiction. □

Since F/K is a degree 3 extension, a prime p can split in three different ways in $\mathcal{O}_F$: either it is inert, it splits completely or it is the product of two prime ideals with inertias 1 and 2. At the same time, it can also split in three different ways in $\mathcal{O}_K$, either it is inert, it splits in principal ideals or it splits in non principal ideals. The following result shows that there is a one to one correspondence between them.

Proposition 20. *Given a prime $p \neq 23$, we have the following equivalences between the splitting of p in K and F.*

$$\begin{aligned} p \text{ splits in two non-principal primes in } K &\iff p \text{ is inert in } F. \\ p \text{ splits in two principal primes in } K &\iff p \text{ splits completely in } F. \\ p \text{ is prime in } K &\iff p \text{ splits in two primes in} F. \end{aligned}$$

Lemma 21. *If a prime p splits completely in the fields F and K, then it splits completely in the composite field KF [7, Theorem 31].*

Lemma 22. *If a prime p splits completely in F, then it also splits completely in its normal closure $H = F^{Gal}$.*

Proof. If a prime p splits completely in F, it also splits completely in $\sigma(F)$ for any $\sigma \in \mathrm{Gal}(H/F)$. Since H is the composite field of $\sigma(F)$ for every embedding σ in $\mathbb{C}$, by the previous lemma p must split completely in H as well. □

Proof. Since there are three different possibilities for the splitting of p in $\mathcal{O}_F$ and in $\mathcal{O}_K$, we only need to prove that two of them are in correspondence and the third equivalence will automatically follow.

1. If p splits into two non-principal primes in $\mathcal{O}_K$, then by Corollary 18 they cannot split further in H. Therefore $p\mathcal{O}_H = \mathfrak{P}_1\mathfrak{P}_2$ with $f(\mathfrak{P}_\mathrm{i}|p) = 3$. Let $\mathfrak{p}$ be the prime under $\mathfrak{P}_1$ in $\mathcal{O}_F$. Since the extension H/F is of degree 2, the only possibility is that $f(\mathfrak{p}|p) = 3$, therefore p is inert in $\mathcal{O}_F$. On the other hand, if p is inert in $\mathcal{O}_F$, it must split in $\mathcal{O}_H$. If it remained inert in H, it would be also inert in $\mathcal{O}_K$, and it would be principal, but this would mean that it would split in $\mathcal{O}_H$. Therefore $p\mathcal{O}_H = \mathfrak{P}_1\mathfrak{P}_2$. If p splits into a principal prime in $\mathcal{O}_K$, it would split in at least 3 primes in $\mathcal{O}_H$. Therefore it splits into non principal primes.

2. If p splits into two principal ideals (π) and (π'), they split completely in H. Therefore $p\mathcal{O}_H = \mathfrak{P}_1 \dots \mathfrak{P}_6$. The only compatible possibility for $p\mathcal{O}_F$ is that it splits completely. Conversely, if p splits completely in F, then it also splits completely in H by lemma 22. all the primes in H over p must have inertial degree 1 over K. Therefore p splits completely in K and the primes over it must be principal, since they also split completely in H.

□

This ends the part on algebraic number theory. Now we will explore quadratic forms and theta series, and we will get another interpretation of each of the possible cases.

Part II

Quadratic forms and modular forms

5. Quadratic forms

A *binary quadratic form* is a homogeneous quadratic polynomial on two variables, $ax^2 + bxy + c^2$ where a, b, c are integers.

If a prime p splits into principal ideals in the field $K = \mathbb{Q}(\sqrt{-23})$, then $p\mathcal{O}_K = (\pi)(\bar{\pi})$ for some element π in the ring of integers of K. We know that $\pi = x + y\frac{1+\sqrt{-23}}{2}$ for some integers x, y, and its norm is given by the following quadratic form:

$$p = N(\pi) = \left(x + y\frac{1+\sqrt{-23}}{2}\right)\left(x + y\frac{1-\sqrt{-23}}{2}\right) = x^2 + xy + 6y^2.$$

On the other hand, if a prime p can be represented as $x^2 + xy + 6y^2$ for some integers x, y, then there exists an element in $\mathcal{O}_K$ of norm p, given by $\pi = x + y\frac{1+\sqrt{-23}}{2}$. Since the norm of a principal ideal is the norm of its generator, the ideal (π) has norm p, and p splits as $p\mathcal{O}_K = (\pi)(\bar{\pi})$.

In this section we generalize this fact. We associate a quadratic form to any ideal class of an imaginary quadratic field in such a way that a prime over p belongs to a certain ideal class if and only if p can be represented by its associated quadratic form.

In a quadratic field $K = \mathbb{Q}(D)$ with $D < 0$ and squarefree, any ideal of $\mathcal{O}_K$ is a rank 2 $\mathbb{Z}$-module. We associate the following quadratic form to any ideal $\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z}$,

$$q_{\mathfrak{a},\alpha,\beta}(x, y) = \frac{N(x\alpha + y\beta)}{N(\mathfrak{a})} = \frac{N(\alpha)}{N(\mathfrak{a})}x^2 + \frac{Tr(\bar{\alpha}\beta)}{N(\mathfrak{a})}xy + \frac{N(\beta)}{N(\mathfrak{a})}y^2,$$

and its discriminant is

$$\frac{Tr(\alpha\bar{\beta})^2 - 4N(\alpha\beta)}{N(\mathfrak{a})^2} = \frac{(\alpha\bar{\beta} + \bar{\alpha}\beta)^2 - 4\alpha\beta\overline{\alpha\beta}}{N(\mathfrak{a})^2} = \frac{(\alpha\bar{\beta} - \bar{\alpha}\beta)^2}{N(\mathfrak{a})^2} = \Delta_K.$$

There is a slight inconvenience that we face. This quadratic form depends on whichever basis of $\mathfrak{a}$ we pick.

Definition 23. We say that the basis (α, β) is *ordered* if the signed area of the parallelogram spanned by α and β is positive, which is $\text{Im}(\bar{\alpha}\beta) = (\alpha\bar{\beta} - \bar{\alpha}\beta)/2i > 0$.

We observe that for any pair of ordered bases (α, β), (α', β'), the matrix σ which transforms one into the other $(\alpha', \beta') = (\alpha, \beta)\sigma$, satisfies $\alpha\bar{\beta} - \bar{\alpha}\beta = (\alpha'\bar{\beta}' - \bar{\alpha}'\beta')\det\sigma$, and therefore $\det\sigma = 1$. Conversely, applying any change of basis σ with $\det\sigma = 1$ to an ordered basis, we obtain another ordered basis.

Given two ordered bases of an ideal $\mathfrak{a}$, they are related by a change of variables $\sigma \in \text{SL}_2(\mathbb{Z})$, for instance $(\alpha', \beta') = (\alpha, \beta)\sigma$. We have

$$x\alpha + y\beta = (x, y)(\alpha, \beta)^T = (x, y)\sigma^T(\alpha', \beta')^T = (X, Y)(\alpha', \beta')^T,$$

Where $(x, y) = (X, Y)\sigma^T$. Therefore $q_{\mathfrak{a},\alpha,\beta}(x, y) = q_{\mathfrak{a},\alpha',\beta'}(X, Y)$. The forms associated to an ideal and a pair of ordered basis differ only by a change of variables in $\text{SL}_2(\mathbb{Z})$.

This motivates the following equivalence relation among quadratic forms. We say that to quadratic forms $Q(x, y)$, $\tilde{Q}(x, y)$ are equivalent if there exists a change of variables $(X, Y) = (x, y)\sigma$ with $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, such that $\tilde{Q}(X, Y) = Q(x, y)$. This change of variables is called a unimodular transformation of Q.

The discriminant of a quadratic form Q is defined as $\Delta_Q = b^2 - 4ac$, and it is an invariant under any unimodular transformation. To show this it is more convenient to express quadratic forms in matrix form, $A_Q = \frac{1}{2}\left(\begin{smallmatrix} 2a & b \\ b & 2c \end{smallmatrix}\right)$. With this notation $Q(x, y) = (x, y)A_Q\left(\begin{smallmatrix} x \\ y \end{smallmatrix}\right)$, and the discriminant of a quadratic form equals the determinant of its associated matrix with opposite sign. If two quadratic forms $Q, \tilde{Q}$ are equivalent, there exists a matrix σ with determinant 1, such that $\sigma^T A_Q \sigma = A_{\tilde{Q}}$, and then $\Delta_Q = \Delta_{\tilde{Q}}$.

We have proved that unimodular transformations define an equivalence relation of quadratic forms of a given discriminant. Now we show that there is a finite number of equivalence classes of quadratic forms of negative discriminant. We define reduced forms in such a way that each equivalence class has exactly one reduced form.

Definition 24. A positive definite quadratic form is *reduced* if it satisfies

$$|b| \leq a \leq c, \quad \text{with } b \geq 0 \text{ if } a = |b| \text{ or } a = c.$$

Any form can be transformed into a reduced one of the same equivalence class, using the pair of unimodular substitutions S and T_k defined as follows,

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} : (a, b, c) \mapsto (c, -b, a)$$

$$T_k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} : (a, b, c) \mapsto (a, b + 2ka, k^2a + kb + c).$$

If $a > c$, we can apply S to decrease a without changing $|b|$. On the other hand, if $a \leq c$ and $|b| > a$, using T_k with $k = \lfloor \frac{a-b}{2a} \rfloor$ reduces $|b|$ while keeping a unchanged. It is clear that after repeating this process a finite number of times, we obtain a reduced quadratic form.

Moreover, each equivalence class contains only one reduced form [3, Theorem 2.8]. Indeed, for quadratic forms with $|b| < a < c$, Legendre observed that the smallest value represented by the reduced quadratic form $ax^2 + bxy + cy^2$ is a, and the second smallest with $\gcd(x, y) = 1$ is c. These values are obtained only by the values $(x, y) = (\pm 1, 0)$ and $(0, \pm 1)$ respectively. Once a and c are fixed, b is determined up to sign. Since two equivalent forms represent the same integers, two reduced forms with different a or c are not equivalent. It only remains to see that the reduced quadratic forms $ax^2 \pm bxy + cy^2$ are not equivalent.

Let Q and $\tilde{Q}$ be equivalent reduced quadratic forms. We show that in fact they are equal. There is some change of variables $(X, Y) = (x, y)\sigma$ with $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\tilde{Q}(X, Y) = Q(x, y)$. On the one hand, using Legendre's observation, we have that the smallest value represented by Q and $\tilde{Q}$, is $Q(1, 0) = \tilde{Q}((1, 0)\sigma)$, and by Legendre's observation on $\tilde{Q}$, we have that $(0, 1)\sigma = (\pm 1, 0)$. Using the same argument with the second smallest value properly represented by Q and $\tilde{Q}$, we have that $Q(0, 1) = \tilde{Q}((0, 1)\sigma))$, which implies $(0, 1)\sigma = (0, \pm 1)$. Since $\det \sigma = 1$, we have $\sigma = \pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. This proves that $Q(x, y) = \tilde{Q}(x, y)$ as we wanted. For quadratic forms with $a = |b|$ or $a = c$, the only representations of a are $\pm(1, 0)$, and the ones for c with $\gcd(x, y) = 1$ are $\pm(0, 1)$ and $\pm(1, -1)$. This determines the coefficients a and c of a reduced quadratic form, and b is also determined since in this case $b > 0$.

Now we find all reduced quadratic forms of discriminant -23. Since a reduced quadratic form has $|b| \leq a \leq c$, we have $b^2 = 4ac - 23 \geq 4b^2 - 23$, which leads to $|b| \leq \sqrt{23/3} \approx 2.77$. Moreover, since $-23 = b^2 - 4ac$, we only need to check the odd possibilities for b, which are $b = \pm 1$ so $ac = 6$. Doing case analysis, we obtain the three reduced forms of discriminant -23:

$$\begin{cases} b=1, a=1, c=6 & Q_0(x,y)=x^2+xy+6y^2 \\ b=1, a=2, c=3 & Q_1(x,y)=2x^2+xy+3y^2 \\ b=-1, a=2, c=3 & Q_2(x,y)=2x^2-xy+3y^2 \end{cases}$$

5.1 The class group

The quadratic form associated to an ideal remains unchanged after scaling $\mathfrak{a}, \alpha, \beta$ by some nonzero $\gamma \in \mathcal{O}_K$,

$$q_{\gamma\mathfrak{a},\gamma\alpha,\gamma\beta}(x,y) = \frac{N(x\gamma\alpha + y\gamma\beta)}{N(\gamma\mathfrak{a})} = q_{\mathfrak{a},\alpha,\beta}(x,y). \tag{8}$$

This is true since in an imaginary quadratic field $K = Q(\sqrt{D})$, every nonzero element γ has positive norm. Equation (8) implies that this is a well defined application between ideal classes and reduced quadratic forms. This application is in fact an isomorphism [10, Theorem 2.28], whose inverse is

$$Q(x,y) = ax^2 + bxy + cy^2 \mapsto \mathfrak{a}_Q = \left[a, \frac{b+\sqrt{\Delta_K}}{2}\right]. \tag{9}$$

In Section 4.1 we defined a group structure for ideal classes in a number field. We can transport the group structure of the ideals in $K = \mathbb{Q}(\sqrt{D})$ with $D < 0$ and squarefree, to the set of equivalence classes of quadratic forms of discriminant Δ_K.

5.2 Representability of a number by quadratic forms

Let w be the number of units of the field $\mathbb{Q}(\sqrt{D})$, $D < 0$. The total number of ways of representing a prime by some reduced quadratic form of discriminant D is

$$\sum_{[Q]} R(p,Q) = w\left(1 + \left(\frac{D}{p}\right)\right). \tag{10}$$

We prove this following the approach from [5, Section 4.4]. We show that there is a correspondence between the ways of representing n by a quadratic form Q and factorizations of the ideal (n) of the form $(n) = \mathfrak{a}\bar{\mathfrak{a}}$ with $\mathfrak{a}$ belonging to the ideal class $\mathfrak{a}_Q$.

First, for any factorization $(n) = \mathfrak{a}\bar{\mathfrak{a}}$ with $\mathfrak{a} \sim \mathfrak{a}_Q$, we have $N(\mathfrak{a}) = n$. After fixing some oriented basis (α, β) of $\mathfrak{a}$, we have that $n = N(\mathfrak{a}) = \alpha x + \beta y$ for some integers x, y, since $N(\mathfrak{a}) \in \mathfrak{a}$. Therefore the quadratic form $q_{\mathfrak{a},\alpha,\beta}(x,y) = \frac{N(\alpha x+\beta y)}{N(\mathfrak{a})}$ represents n. Moreover, for each unit $\gamma \in K$ we have $\gamma n \in \mathfrak{a}$, and setting $\gamma n = \alpha x + \beta y$ we get distinct representations of n.

Now suppose that n is representable by a quadratic form Q, we want to find a factorization $(n) = \mathfrak{a}\bar{\mathfrak{a}}$ with $\mathfrak{a} \in [\mathfrak{a}_Q]$.

Lemma 25. *If an integer n is representable by a quadratic form $Q(x,y) = ax^2 + bxy + cy^2$, then Q is uniquely equivalent to a form*

$$\tilde{Q}(x,y) = nx^2 + b'xy + c'y^2 \quad \textit{with } 0 \le b' \le 2n, c' \in \mathbb{Z}.$$

Proof. Let $Q(p,q)=n$, for some coprime p,q. There exist integers r,s such that $ps-qr=1$, and all solutions are given by $r=r_0+kp$, $s=s_0+kq$ with $k\in\mathbb{Z}$. Then

$$\begin{aligned}
Q(px+ry,qx+sy) &= Q(p,q)x^2+(2apr+bps+brq+2cqs)xy+Q(r,s)y^2\\
&= nx^2+\left(b_0'+2k(ap^2+bpq+cq^2)\right)xy+Q(r,s)y^2\\
&= nx^2+(b_0'+2kn)xy+Q(r,s)y^2.
\end{aligned}$$

Where $b_0=2apr_0+bps_0+br_0q+2cqs_0$. For a unique k the last quadratic form is of the desired form. □

Finally the ideal corresponding to $\tilde{Q}$ given by (9), has norm n, and therefore $(n)=\mathfrak{a}_{\tilde{Q}}\overline{\mathfrak{a}_{\tilde{Q}}}$.

Using Theorem 3, we can compute the splitting of a prime p in $K=\mathbb{Q}(\sqrt{D})$, D squarefree. Using the structure of the ring of integers of a quadratic field, computed at (5), we know that the index $[\mathcal{O}_K:Z[\sqrt{D}]]$ is less than two. We have that the decomposition of any odd prime is given by the factorization of the minimal polynomial of $\sqrt{D}$ modulo p, which is $x^2-D \pmod p$. If $D\equiv 1 \pmod 4$, then 2 divides the index $[\mathcal{O}_K:Z[\sqrt{D}]]$, and we have to work with $\frac{1+\sqrt{D}}{2}$, whose minimal polynomial is $x^2-x+\frac{1-D}{4}$. This polynomial has no roots modulo 2 when $\frac{1-D}{4}$ is odd, and have different roots if $\frac{1-D}{4}$ is even. This coincide with $\left(\frac{D}{2}\right)=1$ and $\left(\frac{D}{2}\right)=-1$ respectively. Taking everything into account, we have

$$p\mathcal{O}_K=\begin{cases}\text{prime} & \mathit{if}\ \left(\frac{D}{p}\right)=-1\\ \mathfrak{p}\overline{\mathfrak{p}} & \mathit{if}\ \left(\frac{D}{p}\right)=1\\ \mathfrak{p}^2 & \text{if}\ \left(\frac{D}{p}\right)=0.\end{cases}$$

Note that $\left(\frac{D}{p}\right)+1$ gives the number of ordered decompositions of p as the product of two primes, and Equation (10) follows.

5.3 Theta series

Given a positive definite binary quadratic form Q, we define its *theta series* as

$$\Theta_Q(z)=\sum_{x,y\in\mathbb{Z}}q^{Q(x,y)}\ \text{where}\ q=e^{2\pi iz},$$

which is absolutely convergent in the complex plane. When we collect the terms with the same exponent, we get the q-expansion of Θ, which is $\Theta_Q(z)=\sum_{n\geq 0}r_Q(n)q^n$ where $r_Q(n)$ is the number of representations of n as values of $Q(x,y)$ with integers x,y.

Note that the prime coefficients of the theta series of quadratic forms of discriminant 23 satisfy the following relation

$$\frac{r_{Q_0}(p)+2r_{Q_1}(p)}{2}=1+\left(\frac{-23}{p}\right). \tag{11}$$

It is clear that every theta series satisfies the functional equation $\Theta(z+1)=\Theta(z)$, but they satisfy additional functional equations. One of those is given by the Hecke-Schoeneberg Theorem [1, p.32],[9, Theorem 19].

6. Modular forms and bounds on dimensions

In this section, we will introduce modular forms, which will have a connection with the number of representations of quadratic forms.

Definition 26. A holomorphic function f is said to be *weakly modular of weight k* (usually an integer) if it satisfies the pair of functional equations

$$f(z+1) = f(z), \quad f\left(-\frac{1}{z}\right) = z^k f(z). \tag{12}$$

We can define the following action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathbb{H}$,

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} &\to \mathbb{H} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} z &\mapsto \frac{az+b}{cz+d}. \end{aligned}$$

This is a group action since a direct computation shows that the imaginary part of γz is $\frac{1}{|cz+d|^2}\,\mathrm{Im}(z)$, which means that $\mathbb{H}$ is invariant under it. Additionally, it satisfies that $(\gamma_1\gamma_2)z = \gamma_1(\gamma_2 z)$ for any pair $\gamma_1, \gamma_2 \in \mathrm{SL}_2(\mathbb{Z})$ and any $z \in \mathbb{H}$.

Observing that $z+1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \cdot z$ and $-\frac{1}{z} = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot z$ and the fact that this two matrices together generate the hole special linear group $\mathrm{SL}_2(\mathbb{Z})$, we can express the equations in 12 as

$$f(\gamma \cdot z) = f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z) \quad \text{for any } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

If we define the weight k slash operator to be $f|_{\gamma,k}(z) = (cz+d)^{-k} f(\gamma \cdot z)$, the last condition simply becomes $f|_{\gamma,k}(z) = f(z)$ for any matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

We generalize the definition of weakly modularity for some subgroups of $\mathrm{SL}_2(\mathbb{Z})$.

We define the *principal congruence subgroup* of level N,

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

A congruence subgroup is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ which contains a principal congruence subgroup of some level. For this work, the congruence subgroup $\Gamma_0(N)$ will be specially important:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

Definition 27. Let Γ be a congruence subgroup. A meromorphic function $f : \mathbb{H} \to \mathbb{C}$ is said to be *weakly modular of weight k with respect to* Γ if

$$f(\gamma \cdot z) = (cz+d)^k f(z), \text{ for any } \gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$$

The valence formula

Recall that a meromorphic function on $\mathbb{H}$ is holomorphic on $\mathbb{H}$ except on some isolated points, called poles. The *valuation* $v_p(f)$ of a meromorphic function f at a point $p \in \mathbb{H} \cup \{\infty\}$ is defined as the integer n which satisfies that the function $(z-p)^{-n}f(z)$ is holomorphic and non-vanishing at p. We say that a function f is *meromorphic at infinity* if it is of the form $f(z) = \sum_{n \geq n_0} a_n q^n$ for some integer n_0. If a_{n_0} is the first nonzero coefficient, we define $v_\infty(f) = n_0$.

Definition 28. For a congruence subgroup Γ, we say that its set of cusps is $\text{Cusps}(\Gamma) = \Gamma \backslash P^1(\mathbb{Q})$. In other words: Γ acts on $\mathbb{Q} \cup \{\infty\}$, and the cusps of Γ are the orbits of this action.

Let P be a cusp of a congruence subgroup Γ. Let γ_P be any element of Γ such that $\gamma_P(\infty) = P$. Let H_P be group $\gamma_P^{-1}\Gamma\gamma_P \cap \text{SL}_2(\mathbb{Z})_\infty \subseteq \text{SL}_2(\mathbb{Z})_\infty$, which does not depend on the choice of representative for P [8, Lemma 2.2.4].

Definition 29. We define the *width of a cusp* P for Γ as the minimum nonnegative integer h such that H_P contains either $\left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} -1 & h \\ 0 & -1 \end{smallmatrix}\right)$, and we write it as $h_P(\Gamma)$.

Definition 30. Let f be a weakly modular form of weight k for Γ, and let P be a cusp of Γ of width $h_\Gamma(P)$. Since $f(z+N) = f(z)$, we can write f as a Laurent series in $q_N = e^{2\pi i z/N}$, say

$$f(q_N) = \sum_{n \geq n_0} a_n q_N^n, \quad a_{n_0} \neq 0.$$

We define the *order of vanishing* of a weakly modular form f at P as $v_P(f) = h_\Gamma(P)n_0/N$.

Theorem 31 (Valence formula for congruence subgroups)**.** *Let $\Gamma \subset \text{SL}_2(\mathbb{Z})$ be a congruence subgroup. Let $f \neq 0$ be a weakly modular form for Γ of weight k. Then*

$$\sum_{z \in \Gamma \backslash \mathbb{H}} \frac{v_z(f)}{\#\bar{\Gamma}_z} + \sum_{P \in \text{Cusps}(\Gamma)} v_P(f) = \frac{k}{12}\left[\text{PSL}_2(\mathbb{Z}) : \bar{\Gamma}\right],$$

Where $\bar{\Gamma}$ is the image of Γ into $\text{PSL}_2(\mathbb{Z}) = {}^{\text{SL}_2(\mathbb{Z})}/_{\{\pm 1\}}$.

The proof of this theorem uses the Valence formula, which can be proved using complex analysis by computing a contour integral using the Residue Theorem [8, Theorem 2.6.1].

Using the Valence formula, we can bound the dimensions of modular spaces.

Theorem 32. *Let f be a modular form of weight k for the congruence subgroup Γ. If the terms of the q expansion of f are zero up to the term $\frac{k}{12}[\text{PSL}_2(\mathbb{Z}) : \bar{\Gamma}]$, then it is identically zero.*

Proof. Every term in the Valence formula is nonnegative. This means that $v_\infty(f) \leq \frac{k}{12}[\text{PSL}_2(\mathbb{Z}) : \bar{\Gamma}]$. If $f \neq 0$, the hypothesis is that $v_\infty(f) \geq \frac{k}{12}[\text{PSL}_2(\mathbb{Z}) : \bar{\Gamma}]$. Therefore it must be $f = 0$. □

7. Hecke-Schoenberg Theorem

Now we will follow [6, Chapter 10] to prove the Hecke-Schoeneberg Theorem. Given a quadratic form $Q(v) = \frac{1}{2}A[v]$, it describes the transformation property of its theta series with respect to the congruence subgroup $\Gamma_0(N)$, where N is the least integer such that NA^{-1} is integral.

Theorem 33. *(Hecke, Schoeneberg). Let $Q : \mathbb{Z}^{2k} \to \mathbb{Z}$ be a positive definite integer-valued form in $2k$ variables of level N and discriminant Δ. Then Θ_Q is a modular form on $\Gamma_0(N)$ of weight k and character χ_Δ, i.e., we have*

$$\Theta_Q\left(\frac{az+b}{cz+d}\right) = \chi_\Delta(a)(cz+d)^k\Theta_Q(z) \text{ for all } z \in \mathfrak{H} \text{ and } \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$$

We will prove this statement for binary quadratic forms, which means that we set $k = 1$. And for all $z \in \mathfrak{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$,

$$\Theta_Q\left(\frac{az+b}{cz+d}\right) = \left(\frac{\Delta}{a}\right)(cz+d)\Theta_Q(z). \tag{13}$$

This section is devoted to prove it using Poisson summation formula.

Poisson summation formula

Recall that the *d-dimensional Fourier transform* of a Lebesgue integrable periodic function f is

$$\hat{f}(\xi) = \int_{\mathbb{R}^d} f(x)e^{-2\pi i\langle \xi, x\rangle}\, dx \quad \forall \xi \in \mathbb{R}^d.$$

Lemma 34 (Poisson summation formula)**.** *Let $f : \mathbb{R} \to \mathbb{C}$ be a Schwarz function. Then*

$$\sum_{n=-\infty}^{\infty} f(x+n) = \sum_{n=-\infty}^{\infty} \hat{f}(n)e^{2\pi i n x} \quad \text{for all } x \in \mathbb{R}.$$

Proof. We write $F(x)$ for the left hand side and $G(x)$ for the right hand side. Since both functions are periodic with period 1, to prove the equality we only need to see that all of their Fourier coefficients coincide, namely,

$$\int_0^1 F(x)e^{-2\pi i\ell x}\, dx = \int_0^1 G(x)e^{-2\pi i\ell x}\, dx \quad \text{for all } \ell \in \mathbb{Z}.$$

We start with $F(x)$. Using absolute convergence, we have

$$\int_0^1 F(x)e^{-2\pi i\ell x}\, dx = \sum_{n=-\infty}^{\infty}\int_0^1 f(x+n)e^{-2\pi i\ell x}\, dx = \int_{-\infty}^{\infty} f(x)e^{-2\pi i\ell x} dx,$$

which is $\hat{f}(\ell)$. On the other hand, a direct computation shows that the ℓ-th Fourier coefficient of $G(x)$ is $\hat{f}(\ell)$:

$$\int_0^1 \left(\sum_{n=-\infty}^{\infty} \hat{f}(n)e^{2\pi i n x}\right) e^{-2\pi i\ell x}\, dx = \sum_{n=-\infty}^{\infty} \hat{f}(n)\int_0^1 e^{2\pi i n x}e^{-2\pi i\ell x}\, dx = \hat{f}(\ell),$$

since the integral $\int_0^1 e^{2\pi i n x}e^{-2\pi i\ell x}\, dx$ is nonzero only when $n = \ell$. □

Remark 35. Poisson summation formula for $x = 0$, is just $\sum f(n) = \sum \hat{f}(n)$, with both sums running trough $\mathbb{Z}$. For higher dimensions, Poisson summation formula remains true, and the idea of the proof is similar.

To prove Hecke-Shoenberg Theoren we will also need the Fourier transform of a linear transformation.

Lemma 36. *Given a function f in $\mathcal{L}^1(\mathbb{R})^2$, and let $\varphi(x) = f(\gamma x)$ where γ is an invetible linear transformation, then its Fourier transform is*

$$\hat{\varphi}(\xi) = \int\limits_{\mathbb{R}^2} f(Mx)e^{-2\pi i \langle x,\xi\rangle}\,dx = \frac{1}{\det M}\int\limits_{\mathbb{R}^2} f(x)e^{-2\pi i \langle M^{-1}x,\xi\rangle}\,dx$$
$$= \frac{1}{\det M}\int\limits_{\mathbb{R}^2} f(x)e^{-2\pi i \langle x,M^{-t}\xi\rangle}\,dx = \frac{1}{\det M}\hat{f}(M^{-t}\xi),$$

where $M^{-t} = \left(M^t\right)^{-1}$.

Proof of the Hecke-Schoeneberg Theorem

We start with a proposition that will turn out to be quite useful.

Proposition 37. *Let A be the matrix associated to a positive definite quadratic form Q, so that $Q(v) = \frac{1}{2}A[v] = \frac{1}{2}v^tAv$. Then for any $z \in \mathbb{H}$ we have*

$$\sum_{v\in\mathbb{Z}^2} q^{\frac{1}{2}A[v+x]} = \frac{i}{\sqrt{|A|z}}\sum_{v\in\mathbb{Z}^2} e^{2\pi i\left(\frac{-A^{-1}[v]}{2z}+v^tx\right)} \tag{14}$$

Proof. Let M be such that $M^TM = A$. We can prove the equality using Poisson summation formula applied to $\varphi(v) = q^{\frac{1}{2}A[v]}$.

$$\sum_{v\in\mathbb{Z}^2} q^{\frac{1}{2}A[v+x]} = \sum_{v\in\mathbb{Z}^2}\varphi(v+x) = \sum_{v\in\mathbb{Z}^2}\hat{\varphi}(v)e^{-2\pi i\langle v,x\rangle}.$$

We have $\varphi(v) = f(\sqrt{-iz}Mv)$ where $f(v) = e^{-\pi|v|^2}$ is the 2-dimensional Gaussian. Combining Lemma 36 with the well known fact that the Fourier transform of the Gaussian is its own Fourier transform, we have

$$\hat{\varphi}(v) = \frac{1}{-iz\det M}\hat{f}\left(\frac{1}{\sqrt{-iz}}M^{-t}v\right) = \frac{1}{-iz\det M}f\left(\frac{1}{\sqrt{-iz}}M^{-t}v\right) = \frac{i}{z\sqrt{A}}e^{-\pi|M^{-t}v/\sqrt{-iz}|^2}.$$

Now since $|M^{-t}v/\sqrt{-iz}|^2 = A^{-1}[v](-iz)^{-1}$, we arrive to the desired result. □

Congruent theta series

Definition 38. Given $h \in \mathbb{Z}^2$, we define the congruent theta series of A as:

$$\Theta_{A,h}(z) = \sum_{m\equiv h} q^{\frac{A[v]}{2N^2}},$$

where the sum runs for all $v \in \mathbb{Z}^2$ with $v \equiv h \pmod{N}$. Note that for $h = 0$ we have the original theta series.

Lemma 39. *If h is such that $Ah \equiv 0 \pmod{N}$, then*

$$\Theta_{A,h}(z+1) = e^{\pi i \frac{A[h]}{N^2}} \Theta_{A,h}(z).$$

Proof. For any v equivalent to h, we have $v = h + wN$ for some $w \in \mathbb{Z}^2$. Since A is symmetric, $A[w]$ is even, so we have

$$A[v] \equiv A[h] + 2Nw^T Ah + N^2 A[w] \equiv A[h] \pmod{2N^2}.$$

Therefore

$$\Theta_{A,h}(z+1) = \sum_{v \equiv h} e^{2\pi i \frac{A[v]}{2N^2}(z+1)} = \sum_{v \equiv h} e^{2\pi i \left(\frac{A[v]}{2N^2} z + \frac{A[h]}{2N^2}\right)} = e^{2\pi i \frac{A[h]}{2N^2}} \Theta_{A,h}(z),$$

where the sums run over $v \in \mathbb{Z}^2$ such that $v \equiv h \pmod{N}$. □

Now we establish the transformation property for $\Theta_{A,h}(z)$ with respect to the involution $z \mapsto -\frac{1}{z}$. Let $\mathcal{H} = \{h \pmod{N} : Ah \equiv 0 \pmod{N}\}$.

Proposition 40. *For any $h \in \mathbb{Z}^2$ with $Ah \equiv 0 \pmod{N}$ we have*

$$\Theta_A\left(-\frac{1}{z}; h\right) = |A|^{-1/2}(-iz) \sum_{\ell \in \mathcal{H}} e^{2\pi i \frac{h^t A \ell}{N^2}} \Theta_{A,\ell}(z).$$

Proof. We use Equation (14) with $x = hN^{-1}$,

$$\sum_v q^{\frac{1}{2}A[v+hN^{-1}]} = \frac{i}{\sqrt{|A|z}} \sum_v e^{2\pi i \left(\frac{-A^{-1}[v]}{2z} + v^t hN^{-1}\right)}$$

$$\Theta_{A,h}(z) = \frac{i}{\sqrt{|A|z}} \sum_{Aw \equiv 0} e^{2\pi i \left(\frac{-N^{-2}A[w]}{2z} + N^{-2} w^t Ah\right)},$$

where we have changed v to $w = NA^{-1}v$, and the condition $v \in \mathbb{Z}^2$ is equivalent to $w \in \mathbb{Z}^2$ and $Aw \equiv 0 \pmod{N}$. Changing z to $-\frac{1}{z}$ we have

$$\Theta_A\left(-\frac{1}{z}; h\right) = \frac{-iz}{\sqrt{|A|}} \sum_{Aw \equiv 0} e^{2\pi i \left(\frac{A[w]}{2N^2} z + \frac{w^t Ah}{N^2}\right)} = \frac{-iz}{\sqrt{|A|}} \sum_{Aw \equiv 0} e^{2\pi i \frac{w^t Ah}{N^2}} q^{\frac{A[w]}{2N^2}}.$$

Finally, splitting the summation into classes modulo N, we get the result. □

Now we will find the transformation properties for the group $\Gamma_0(D)$.

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, The case $d = 0$ is already covered, since $\gamma = \pm\left(\begin{smallmatrix} T & -1 \\ 1 & 0 \end{smallmatrix}\right) = \pm\left(\begin{smallmatrix} 1 & T \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. And we are done since we know how Θ transforms under $\tau \mapsto \tau + T$ and $\tau \mapsto -\frac{1}{z}$.

We can assume $d > 0$, since the transformation for $-\gamma$ is the same that the one for γ. We compute first the transformation for

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}.$$

Since $d\gamma z = b - (dz-c)^{-1}$, we have

$$\Theta(d\gamma z; h) = \sum_{v\equiv h} e^{2\pi i \frac{A[v]}{2N^2}\left(b - \frac{1}{dz-c}\right)}$$

Changing $d\gamma z$ to γz and splitting the sum into classes modulo dN,

$$\Theta(\gamma z; h) = \sum_{v\equiv h \pmod N} e^{2\pi i \frac{A[v]}{2N^2}\left(\frac{b}{d} - \frac{1}{d(dz-c)}\right)} = \sum_{\substack{g \pmod{dN} \\ g\equiv h \pmod N}} e^{2\pi i \frac{A[g]}{2N^2}\frac{b}{d}} \sum_{v\equiv g \pmod{dN}} e^{2\pi i \frac{dA[v]}{2(dN)^2}\frac{-1}{(dz-c)}}.$$

Here the innermost sum is the theta function associated with the matrix dA and the residue class g modulo dN, evaluated at the point $-(dz-c)^{-1}$. Since $dAg \equiv 0 \pmod{dN}$, We can apply Proposition 40 to this sum, giving

$$\sum_{v\equiv g \pmod{dN}} e^{-2\pi i \frac{dA[v]}{2(dN)^2}\frac{1}{(dz-c)}} = \frac{i(c-dz)}{\sqrt{|dA|}} \sum_{\substack{\ell \pmod{dN} \\ A\ell\equiv 0 \pmod N}} e^{2\pi i \frac{\ell^t Ag}{dN^2}} \sum_{v\equiv \ell \pmod{dN}} e^{2\pi i \frac{A[v]}{2dN^2}(dz-c)}.$$

Hence we deduce that

$$\Theta(\gamma z; h) = \frac{i(c-dz)}{d\sqrt{|A|}} \sum_{\substack{\ell \pmod{dN} \\ A\ell\equiv 0 \pmod N}} \varphi(h,\ell) \sum_{v\equiv \ell \pmod{dN}} e^{2\pi i \frac{A[v]}{2N^2}},$$

where

$$\varphi(h,\ell) = \sum_{\substack{g \pmod{dN} \\ g\equiv h \pmod N}} e^{2\pi i \frac{bA[g]+2\ell^t Ag - cA[\ell]}{2dN^2}}.$$

We shift g to $g + c\ell$ so the new variable ranges over classes modulo dN which are congruent to $h - c\ell$ modulo N, and since $ad - bc = 1$, the fraction in the exponential becomes

$$\frac{bA[g] + 2ad\ell^t Ag + acdA[\ell]}{2dN^2}.$$

In the middle term, we can replace g by its class $h - c\ell \pmod N$, and using that $c \equiv 0 \pmod N$ and that $A[\ell] \equiv 0 \pmod{2N}$ for any ℓ with $A\ell \equiv 0 \pmod N$, we get

$$\varphi(h,\ell) = \sum_{\substack{g \pmod{dN} \\ g\equiv h-c\ell \pmod N}} e^{2\pi i\left(\frac{2a\ell^t Ah - acA[\ell]}{2N^2} + \frac{bA[g]}{2dN^2}\right)} = e^{2\pi i \frac{a\ell^t Ah}{N^2}} \varphi(h-c\ell, 0) \tag{15}$$

Therefore $\varphi(h,\ell)$ only depends on $\ell \pmod N$, and we get

$$\Theta(\gamma z, h) = \frac{i(c-dz)}{d\sqrt{|A|}} \sum_{h'\in\mathcal{H}} \varphi(h,h')\Theta(z,h').$$

Now we obtain the transformation for $\tau = \gamma S^{-1}$, so $\gamma(-\frac{1}{z}) = \tau z$. We set $h = 0$ and we change in the previous equation $z \mapsto -\frac{1}{z}$, and we apply Proposition 40 to each $\Theta(-\frac{1}{z}, h')$ inside the sum. We obtain

$$\begin{aligned}\Theta(\tau z) &= \frac{(cz+d)}{d|A|} \sum_{h' \in \mathcal{H}} \varphi(0, h') \sum_{\ell \in \mathcal{H}} e^{2\pi i \frac{h'^t A \ell}{N^2}} \Theta(z, \ell) \\ &= \frac{(cz+d)}{d|A|} \sum_{h' \in \mathcal{H}} \Theta(z, h') \sum_{\ell \in \mathcal{H}} \varphi(0, h') e^{2\pi i \frac{h'^t A \ell}{N^2}}.\end{aligned}$$

Using Equation (15),

$$\Theta(\tau z) = \frac{(cz+d)}{d|A|} \sum_{h' \in \mathcal{H}} \Theta(z, h') \sum_{\ell \in \mathcal{H}} \varphi(-ch', 0) e^{2\pi i \frac{h'^t A \ell}{N^2}}.$$

Since $c \equiv 0 \pmod{N}$,

$$\Theta(\tau z) = \frac{(cz+d)}{d|A|} \varphi(0,0) \sum_{h' \in \mathcal{H}} \Theta(z, h') \sum_{\ell \in \mathcal{H}} e^{2\pi i \frac{\ell^t A h'}{N^2}}.$$

And by the orthogonality of the characters,

$$\begin{aligned}\Theta(\tau z) &= \frac{(cz+d)}{d|A|} \varphi(0,0) \sum_{h' \in \mathcal{H}} \Theta(z, h') \begin{cases} |A| & \text{if } l \equiv 0 \pmod{N} \\ 0 & \text{otherwise} \end{cases} \\ &= \frac{(cz+d)}{d} \varphi(0,0) \Theta(z, 0) = \frac{(cz+d)}{d} \varphi(0,0) \Theta(z).\end{aligned}$$

It remains to compute the Gaussian sum associated with the quadratic form $\frac{1}{2}A[x]$

$$\varphi(0,0) = \sum_{x \pmod{d}} e^{2\pi i \frac{bA[x]}{2d}}.$$

Assuming that $d \equiv 1 \pmod{2}$. Then $(d, 2c|A|) = 1$ and changing x to $2cx$ modulo d we get

$$G = \sum_{x \pmod{d}} e^{-2\pi i \frac{2cA[x]}{d}}.$$

This is a generalized Gaussian sum, which is evaluated in [6, Lemma 10.5] as

$$\left(\frac{|A|}{d}\right)\left(\frac{-1}{d}\right) d = d \left(\frac{-|A|}{d}\right).$$

Since $\Delta = -|A|$, we get

$$\Theta(\tau z) = \left(\frac{\Delta}{d}\right)(cz+d)\Theta(z).$$

Now we return to the original setting of quadratic forms of discriminant -23. The Jacobi symbol satisfies $\left(\frac{-23}{d}\right) = \left(\frac{d}{23}\right)$, and if $\gamma \in \Gamma_0(23)$, we have that $ad \equiv 1 \pmod{23}$. We have that the theta series of a quadratic form of discriminant -23 satisfies

$$\Theta(\tau z) = \left(\frac{a}{23}\right)(cz+d)\Theta(z) \quad \text{for any } \gamma \in \Gamma_0(23)$$

8. A special eta product

In this section we set ourselves the goal of constructing a function which satisfies the functional equation

$$f(\gamma z) = \left(\frac{a}{23}\right)(cz+d)f(z), \quad \text{for any } \gamma \in \Gamma_0(23).$$

Observe that this is the same functional equation that the theta series of quadratic forms of discriminant -23 satisfy. This function will be constructed by taking an appropriate product of the *Dedekind eta function*, which is defined as

$$\eta(z) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1-q^n) \quad z \in \mathbb{C}, \quad \text{where } q = e^{2\pi i z}. \tag{16}$$

We can check that it is holomorphic and non-vanishing on the upper half plane by taking the logarithm and differentiating. The Dedekind eta function in addition to the functional equation $\eta(z+1) = e^{\frac{\pi i}{12}}\eta(z)$, it also satisfies $\eta\left(-\frac{1}{z}\right) = \sqrt{-iz}\eta(z)$. This makes the function $\Delta(z) = \eta(z)^{24}$ a modular form of weight 12, and we say that $\eta(z)$ is a modular form of weight 1/2. Using this functional equations, we show that the eta product $f(z) = \eta(z)\eta(23z)$ satisfies Equation (16).

8.1 Transformation property of the eta function

As we mentioned, the Dedekind eta function satisfies $\eta(z+1) = e^{\frac{\pi i}{12}}\eta(z)$. In this section we prove the following transformation property

$$\eta\left(-\frac{1}{z}\right) = \sqrt{-iz}\eta(z).$$

Lemma 41. *For any $z \neq 0$ we have*

$$\sum_{n\in\mathbb{Z}} \frac{1}{(z+n)^2} = -4\pi^2 \sum_{n=1}^{\infty} nq^n. \tag{17}$$

Proof. On the one hand, we compute the second derivative of the logarithm of Euler's product formula $\sin(\pi z) = \pi z \prod_{i=1}^{\infty}\left(1 - \frac{z^2}{n^2}\right)$,

$$-\pi^2 \csc^2(\pi z) = -\frac{1}{z^2} - \sum_{n=1}^{\infty}\left(\frac{1}{(z-n)^2} + \frac{1}{(z+n)^2}\right).$$

This sum can be reordered to match the left hand side of Equation 17. On the other hand, the first derivative of $\sin(\pi z)$ is $\pi\cot(\pi z) = \pi\cos(\pi z)/\sin(\pi z)$. Using the exponential form of the trigonometric functions, we have

$$\pi\cot(\pi z) = \pi i \frac{(e^{i\pi z} + e^{-i\pi z})}{(e^{i\pi z} - e^{-i\pi z})} = \pi i \left(1 - \frac{2}{1-e^{2\pi i z}}\right) = \pi i \left(1 - 2\sum_{n=1}^{\infty} e^{2\pi i n z}\right). \tag{18}$$

Finally differentiating this again we obtain $-(2\pi i)^2 \sum ne^{\pi i n z}$ as we wanted. □

Remark 42. Replacing z with mz in Equation (17), and adding over m we have

$$\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}} \frac{1}{(mz+n)^2} = -4\pi^2 \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} nq^{nm}.$$

Theorem 43. *The Dedekind eta function satisfies the functional equation*

$$\eta\left(-\frac{1}{z}\right) = \sqrt{-iz}\,\eta(z).$$

Proof. To prove the equality, we compute the logarithmic derivative of the eta function evaluated at $-1/z$, and we obtain the equality except for a multiplicative constant, which turns out to be 1.

The logarithmic derivative of the eta function is

$$\begin{aligned}\frac{d}{dz}\log\eta(z) = \frac{d}{dz}\left(\frac{2\pi iz}{24} + \sum_{n=1}^{\infty}\log(1-q^n)\right) &= \frac{\pi i}{12} + \sum_{n=1}^{\infty}\frac{-2\pi i n q^n}{1-q^n}\\ &= \frac{\pi i}{12} - 2\pi i\sum_{n=1}^{\infty} n\sum_{m=1}^{\infty} q^{nm}.\end{aligned}$$

Using Remark 42, this sum can be rewritten as

$$\frac{d}{dz}\log\eta(z) = \frac{\pi i}{12} - \frac{1}{2\pi i}\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2}. \tag{19}$$

Evaluating this expression at $-1/z$, we have

$$\frac{d}{dz}\log\eta\left(-\frac{1}{z}\right) = \frac{\pi i}{12} - \frac{1}{2\pi i}\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{z^2}{(m-nz)^2} = \frac{\pi i}{12} - \frac{z^2}{2\pi i}\left(\sum_{m=1}^{\infty}\sum_{n\neq 0}\frac{1}{(m+nz)^2} + \zeta(2)\right).$$

We can include $\frac{\pi i}{12}$ inside the sum as twice the 0-th term, since for $m=0$ we have

$$-\frac{z^2}{2\pi i}\sum_{n\neq 0}\frac{1}{(m+nz)^2} = -\frac{z^2}{2\pi i}\frac{2\pi^2}{6z^2} = \frac{\pi i}{6}.$$

Writing $\sum_{m\in\mathbb{Z}}$ with the meaning of $\sum_{m=0}^{\infty} + \sum_{m=-1}^{-\infty}$,

$$\begin{aligned}\frac{d}{dz}\log\eta\left(-\frac{1}{z}\right) &= -\frac{z^2}{4\pi i}\left(\sum_{m\in\mathbb{Z}}\sum_{n\neq 0}\frac{1}{(m+nz)^2} + 2\zeta(2)\right)\\ &= z^2\left(-\frac{1}{4\pi i}\sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\frac{1}{(mz+n)^2} + \frac{\pi i}{12}\right).\end{aligned} \tag{20}$$

On the other hand, from Equation 19, and using that $\frac{d}{dz}\log\left(\sqrt{-iz}\right) = -\frac{1}{2z}$,

$$\frac{d}{dz}\log\left(\sqrt{-iz}\,\eta(z)\right) = -\frac{1}{2z} + \frac{\pi i}{12} - \frac{1}{4\pi i}\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2}.$$

We subtract $\sum_{n\in Z}\frac{1}{(mz+n)(mz+n+1)} = \sum_{n\in Z}\frac{1}{mz+n} - \frac{1}{mz+n+1} = 0$ term by term to the previous sum,

$$\begin{aligned}\frac{d}{dz}\log\left(\sqrt{-iz}\,\eta(z)\right) &= -\frac{1}{2z} + \frac{\pi i}{12} - \frac{1}{4\pi i}\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2} - \frac{1}{(mz+n)(mz+n+1)}\\ &= -\frac{1}{2z} + \frac{\pi i}{12} - \frac{1}{4\pi i}\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2(mz+n+1)}.\end{aligned} \tag{21}$$

Now subtracting Equations 20 and 21,

$$\begin{aligned} z^{-2}\frac{d}{dz}\left(\log\eta\big(-\frac{1}{z}\big)-\sqrt{-iz}\eta(z)\right) &= \frac{1}{2z}+\frac{1}{4\pi i}\left(\sum_{m\neq 0}\sum_{n\in\mathbb{Z}}\frac{1}{(mz+n)^2(mz+n+1)}-\sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\frac{1}{(mz+n)^2}\right)\\ &= \frac{1}{2z}-\frac{1}{4\pi i}\sum_{n\in\mathbb{Z}}\sum_{m\neq 0}\frac{1}{(mz+n)(mz+n+1)}. \end{aligned}$$

This sum is absolutely convergent, so we can change the order of summation.

$$\begin{aligned} \lim_{N\to\infty}\sum_{n=-N}^{N-1}\sum_{m\neq 0}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right) &= \lim_{N\to\infty}\sum_{m\neq 0}\sum_{n=-N}^{N-1}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right)\\ &= \lim_{N\to\infty}-\frac{1}{z}\sum_{m\neq 0}\left(\frac{1}{N/z+m}+\frac{1}{N/z-m}\right)\\ &= \lim_{N\to\infty}\frac{-2\pi}{z}\cot(\pi N/z) \end{aligned}$$

Finally using Equation (18),

$$\lim_{N\to\infty}\sum_{n=-N}^{N-1}\sum_{m\neq 0}\left(\frac{1}{mz+n}-\frac{1}{mz+n+1}\right)=\lim_{N\to\infty}-\frac{2\pi i}{z}+\frac{4\pi i}{z}\sum e^{2\pi i m N/z}=-\frac{2\pi i}{z}.$$

In conclusion, $\frac{d}{dz}\left(\log\eta\big(-\frac{1}{z}\big)-\sqrt{-iz}\eta(z)\right)=0$. Which means that $\log\eta(-\frac{1}{z})=C\log\left(\sqrt{-iz\eta(z)}\right)$. Evaluating this equality at $z=i$, we find that $C=1$. □

8.2 Transformation property of the eta product

Now we will proof the transformation property of f for $\Gamma_0(23)$ described in Equation 16. We will write $f(\gamma z)=\eta(\gamma z)\eta(23\gamma z)$ in terms of $f(z)=\eta(z)\eta(23z)$ for any $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma_0(23)$. First, we can write 23 as an action on γz, and it satisfies

$$\begin{pmatrix}23&0\\0&1\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}a&23b\\c/23&d\end{pmatrix}\begin{pmatrix}23&0\\0&1\end{pmatrix}.$$

Let $\tilde\gamma$ denote $\left(\begin{smallmatrix}a&23b\\c/23&d\end{smallmatrix}\right)$. With this notation we have

$$\eta(\gamma z)\eta(23\gamma z)=\eta(\gamma z)\eta(\tilde\gamma 23z).$$

To compute the transformation property of η for γ and $\tilde\gamma$, we write both matrices as a product of S and T, and then we can successively apply the transformation properties for S and T.

If two matrices $\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$, $\gamma'=\left(\begin{smallmatrix}a'&b'\\c'&d'\end{smallmatrix}\right)$ of $\Gamma_0(23)$ satisfy

$$f(\gamma z)=\left(\frac{a}{23}\right)(cz+d)f(z),$$

then its product also satisfies it.

$$f(\gamma\gamma' z) = \left(\frac{a}{23}\right)(c(\gamma' z) + d)f(\gamma' z) = \left(\frac{a}{23}\right)(c\frac{a'z + b'}{c'z + d'} + d)\left(\frac{a'}{23}\right)(c'z + d')f(z)$$
$$= \left(\frac{aa'}{23}\right)((ca' + c'd)z + (cb' + dd'))f(z).$$

Note that the fist entry of $\gamma\gamma'$ is congruent to aa' modulo 23. Therefore it is only necessary to check that this trasnformation property holds for any set of generators of $\Gamma_0(23)$. Using the computer algebra system SageMath, we have checked that for each element of a set of generators of $\Gamma_0(23)$, the following identity holds

$$\left(\frac{f(\gamma z)}{f(z)(cz + d)}\right)^2 = 1.$$

Since $\frac{f(\gamma z)}{f(z)(cz+d)}$ is continuous and takes the values ±1, it must be constant. Evaluating it at some point will be enough to know how it behaves for any $z \in \mathbb{H}$. We choose to evaluate it at i, and we find that the following transformation property holds for all the generators of $\Gamma_0(N)$,

$$f(\gamma z) = \left(\frac{a}{23}\right)(cz + d)f(z).$$

Since the Legendre symbol $\left(\frac{a}{23}\right)$ is multiplicative, we deduce that this property holds for any matrix $\gamma \in \Gamma_0(N)$. These computations are detailed at the appendix, with the required code included.

8.3 The Sturm bound

The q-expansions of the Theta series of the quadratic forms of discriminant -23 are

$$\begin{aligned} \Theta_{Q_0}(z) &= 1 + 2q \qquad\qquad +2q^4 + 4q^6 + \ldots \\ \Theta_{Q_1}(z) &= 1 \qquad +2q^2 + 2q^3 + 2q^4 + 2q^6 + \ldots \end{aligned}$$

Now we use Theorem 32 to deduce that $f(z) = \frac{\Theta_{Q_0}(z) - \Theta_{Q_1}(z)}{2} = q - q^2 - q^3 + q^6 + \ldots$.

Both functions are weakly-modular for $\Gamma_0(23)$ with character $\chi(\gamma) = \left(\frac{a}{23}\right)$.

The value of the index $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)]$ is well known [8, Lemma 2.1.2],

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right).$$

For $N = 23$ we have $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(23)] = 24$. We use this to compute a bound on the number of Fourier coefficients that we have to check in order to decide that two functions of the modular space $M_1(23, \chi)$ coincide. This bound is the Sturm bound.

For any modular form $f \in \mathcal{M}_1(\Gamma_0(23), \chi)$, we construct a modular function in $M_2(23)$ in the following way

$$\begin{aligned} M_1(23, \chi) &\hookrightarrow M_2(23) \\ f &\to f\bar{f}. \end{aligned}$$

If the first four Fourier coefficients of f are zero, then the first four Fourier coefficients of $f\bar{f}$ are also zero as well. Using Theorem 32, we deduce that all of them are zero.

Since first four coefficients of $f(z)$ and $\frac{\Theta_{Q_0}(z) - \Theta_{Q_1}(z)}{2}$ coincide, we deduce that this is true for all of them.

9. Consequences of the equality and conclusions

The equality obtained in the previous section gives a complete description of the prime coefficients of the Fourier expansion of the modular form f. We have,

$$a_p(f) = \frac{r_{Q_0}(p) - r_{Q_1}(p)}{2}.$$

Recalling the relation

$$\frac{r_{Q_0}(p) + 2r_{Q_1}(p)}{2} = 1 + \left(\frac{-23}{p}\right),$$

we can deduce that if $\left(\frac{-23}{p}\right) = -1$, then p is not representable by a quadratic form of discriminant -23, and we have $r_{Q_0}(p) = r_{Q_1}(p) = 0$, so $a_p(f) = 0$. Otherwise, p is representable either by Q_0 or Q_1. in the first case, $r_{Q_1}(p) = 0$, which implies $r_{Q_0}(p) = 4$ and $a_p(f) = 2$, and in the second case, $r_{Q_0}(p) = 0$ and $a_p(f) = -1$. Finally, since $r_{Q_0}(23) = 2$, we have that $a_p(f) = 1$.

We have the following relations,

$$a_p(f) = \begin{cases} 1 & \text{if } p = 23 \\ 0 & \text{if } (p/23) = -1 \\ 2 & \text{if } p \text{ is representable as } x^2 + xy + 6y^2 \\ -1 & \text{if } p \text{ is representable as } 2x^2 + xy + 3y^2 \end{cases}$$

In Section 5.2, we have related the representations of primes by quadratic forms of negative discriminant and the splitting of primes in imaginary quadratic fields.

The representations of primes by quadratic forms of discriminant -23 is related to the splitting of primes in $\mathbb{Q}(\sqrt{-23})$ in the following way

$$\begin{aligned} \left(\frac{p}{23}\right) = -1 &\iff p \text{ is inert} \\ p \text{ splits in principal primes} &\iff p \text{ is represented by } x^2 + xy + 6y^2 \\ p \text{ splits in nonprincipal primes} &\iff p \text{ is represented by } 2x^2 + xy + 3y^2 \end{aligned}$$

Morover, using class field Theory we proved that the splitting in $K = \mathbb{Q}(\sqrt{-23})$ and the splitting in $F = \mathbb{Q}(\alpha)$, where α is a root of $x^3 - x - 1$ are related in the following way,

$$\begin{aligned} p \text{ splits in non-principal primes in } K &\iff p \text{ is inert in } F. \\ p \text{ splits in principal primes in } K &\iff p \text{ splits completely in } F. \\ p \text{ is inert in } K &\iff p \text{ splits in two primes in } F. \end{aligned}$$

Finally, the splitting of a prime p in F is directly related to the factorization of $x^3 - x - 1 \pmod{p}$. Therefore, we have obtained a generating function which describes how $x^3 - x - 1$ splits modulo any prime.

References

[1] Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier. *The 1-2-3 of modular forms: lectures at a summer school in Nordfjordeid, Norway*. Springer Science & Business Media, 2008.

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

[3] David A Cox. *Primes of the form x2+ ny2: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[4] Fred Diamond and Jerry Michael Shurman. *A first course in modular forms*, volume 228. Springer, 2005.

[5] Andrew Granville. Binary quadratic forms. `https://dms.umontreal.ca/~andrew/Courses/Chapter4.pdf`. [Online; accessed 25-September-2020].

[6] Henryk Iwaniec. *Topics in classical automorphic forms*, volume 17. American Mathematical Soc., 1997.

[7] Daniel A Marcus. *Number fields*, volume 8. Springer, 1977.

[8] Marc Masdeu. Modular forms (ma4h9), 2015.

[9] Andrew Ogg. *Modular forms and Dirichlet series*. WA Benjamin New York, 1969.

[10] Corentin Perret-Gentil and Philippe Michel. The correspondence between binary quadratic forms and quadratic fields. `https://corentinperretgentil.gitlab.io/static/documents/correspondence-bqf-qf.pdf`, 2012. [Online; accessed 25-September-2020].

Appendix: SageMath code

We include the SageMath code that was used to check the transformation property of the eta product of Section 8.2.

Since the functional equations presented in Section 8.1 show the transformation property of the eta function by the matrices S and T, and they generate the full group $\mathrm{SL}_2(\mathbb{Z})$, we compute first the decomposition of any matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ as a product of matrices S and T. To write this as a recursive function, it is easier to assume that the input is in fact γ^{-1}.

```
T=SL2Z([1,1,0,1])
S=SL2Z([0,-1,1,0])

def inverse_matrix_as_S_T(mat):
    product=[] #stores a list of matrices with prod(product)*mat = id
    indices=[] #stores a list with k or 0 if the facor of the decomposition is T^k or S.

    if mat.c()==0 and mat.a() == 1:                        # if mat == [[1,b],
        product = [T^(-mat.b())]  if mat.b() != 0  else [] #            [0,1]]
        indices = [-mat.b()] if mat.b() != 0  else []

    elif (mat.c()==0 and mat.a() == -1) or abs(mat.a()) < abs(mat.c()) :  # if mat == [[-1,*],
        new_index, new_product= inverse_matrix_as_S_T(S*mat )             #             [0,-1]]
        product = new_product + [S]
        indices = new_index + [0]
    else:                                                   # if mat == [[ a+k*c, *],
        frac=mat.a()/(mat.c())                              #            [     c, *]]
        exp = floor(frac) if frac>0  else ceil(frac)
        new_index, new_product = inverse_matrix_as_S_T(T^(-exp)*mat )
        product =  new_product +[T^(-exp)]
        indices = new_index + [-exp]

    assert(prod(product,SL2Z([1,0,0,1]))*mat==SL2Z([1,0,0,1])),"matrix product is not the identity"
    product_form_indices = [(T^i if i!= 0 else S) for i in indices]
    assert(product_form_indices==product), "error computing indices"
    return (indices, product)
```

Let $\gamma \in \Gamma_0(\mathbb{Z})$ and $z \in \mathbb{H}$. We want to compute the transformation property of f for γ at z. We use a decomposition of γ with matrices S and T^k, to compute the automorphy factor of the eta function, $\frac{\eta(\gamma z)}{\eta(z)}$. Since there is a square root, and we want to do the computations symbolically, we compute the square of the automorphy factor.

```
def automorphy_factor_squared(mat,zz):
    ind,product = inverse_matrix_as_S_T(mat^-1)
    automorphy_sq=1

    for k in range(len(ind)):
        if ind[k] == 0:
            automorphy_sq *= -I*(prod(product[k+1:],SL2Z([1,0,0,1])).acton(zz))
        else:
            automorphy_sq *= (e^(2*I*pi*ind[k]/12))
    return automorphy_sq
```

For every generator γ of Γ_0, we compute the product of the automorphy factors for γ and $\tilde{\gamma}$,

```
z=var('z')
G=Gamma0(23)
for m in G.gens():
    m_1=SL2Z([m.a(), 23*m.b(),m.c()/23,m.d()])
    automorphy_sq = automorphy_factor_squared(m,z)
    automorphy_sq_1 = automorphy_factor_squared(m_1,23*z)
    show(m, (automorphy_sq*automorphy_sq_1/(m.c()*z+m.d())^2).full_simplify())
```

Using this code, we check that for each generator γ of $\Gamma_0(23)$ we have

$$\left(\frac{f(\gamma z)}{f(z)(cz+d)}\right)^2 = \frac{\eta(\gamma z)\eta(\gamma 23z)}{\eta(z)\eta(23z)(cz+d)^2} = 1.$$

Since $\frac{f(\gamma z)}{f(z)(cz+d)}$ is continuous, for any $\gamma \in \Gamma_0(23)$, it is either 1 or -1.

Now we compute $\frac{f(\gamma z)}{f(z)(cz+d)}$. We start with $\frac{\eta(\gamma z)}{\eta(z)}$ for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

```
def sqrt_upper_half_plane(zz):
    roots = zz.sqrt(all=true)
    return roots[0] if roots[0].imag()>=0 else roots[0]
def automorphy_factor(mat,zz):
    ind,product = inverse_matrix_as_S_T(mat^-1)
    automorphy = 1
    for k in range(len(ind)):
        if ind[k] == 0:
            automorphy*= sqrt_upper_half_plane(-QQbar(I)*(prod(product[k+1:],SL2Z([1,0,0,1])).acton(zz)))
        else:
            automorphy *= QQbar(e^(pi*(I)*ind[k]/12))
    return automorphy
```

Using this, we finally compute $\frac{f(\gamma i)}{f(i)(ci+d)}$,

```
for m in G.gens():
    automorphy = automorphy_factor(m,QQbar(I))
    m_1=SL2Z([m.a(), 23*m.b(),m.c()/23,m.d()])
    automorphy_1 = automorphy_factor(m_1,23*QQbar(I))
    show(m, real(QQbar((cocyc*cocyc_1/(m.c()*QQbar(I)+m.d())))))
```

We obtain the following results, which coincide with $\left(\frac{a}{23}\right)$.

γ	$\frac{f(\gamma i)}{f(i)(ci+d)}$	γ	$\frac{f(\gamma i)}{f(i)(ci+d)}$
$\begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}$	1	$\begin{pmatrix}19 & -5\\23 & -6\end{pmatrix}$	1
$\begin{pmatrix}17 & -3\\23 & -4\end{pmatrix}$	-1	$\begin{pmatrix}18 & -11\\23 & -14\end{pmatrix}$	1
$\begin{pmatrix}9 & -2\\23 & -5\end{pmatrix}$	1	$\begin{pmatrix}-1 & 0\\0 & -1\end{pmatrix}$	-1

Table 2: Values of $f(\gamma z)/f(z)(cz+d)$, that confirm the transformation property given in Section 8.2.