The Dedekind Zeta Function and The Analytic Class Number Formula

by

Çağatay Altuntaş

A Dissertation Submitted to the
Graduate School of Sciences and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Mathematics

June 27, 2018

The Dedekind Zeta Function and The Analytic Class Number Formula

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

Çağatay Altuntaş

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

_____

Assoc. Prof. Kazım Büyükboduk

_____

Prof. Dr. Tolga Etgü

_____

Assoc. Prof. Ayhan Günaydın

Date: _____

to my family

ABSTRACT

In this thesis, we first introduce number fields and their rings of integers. We show that ring of integers $\mathcal{O}_K$ of a number field K is an integrally closed, Noetherian ring such that its prime and maximal ideals coincide. Namely, $\mathcal{O}_K$ is a Dedekind domain. To study $\mathcal{O}_K$ in details, we present a geometric approach so that K is embedded inside a finite dimensional real vector space. By doing so, we show that *the class number* h_K of K is finite. In addition, we characterize the group of units of $\mathcal{O}_K$ via geometric methods. After that, we define the Dedekind zeta function $\zeta_K(s)$ of a number field K. It is a generalization of the Riemann zeta function $\zeta(s)$. Moreover, we present the *Analytic Class Number Formula* which states that $\zeta_K(s)$ converges for any $Re(s) > 1$ and has a simple pole at $s = 1$. Moreover, its residue is given by $\dfrac{2^{r_1+r_2}\pi^{r_2}R_K}{|\mu(K)|\sqrt{|\Delta_K|}}\ h_K$ where r_1 is the number of real embeddings of K, r_2 is the number of non-conjugate complex embeddings, R_K is the regulator of K, Δ_K is the discriminant of K and $\mu(K)$ is the group of roots of unity in K. Lastly, we present various arguments to evaluate h_K for various number fields.

ÖZETÇE

Bu çalışmada ilk olarak sayı cisimleri ve bu sayı cisimlerinin cebirsel tamsayı halkalarına değineceğiz. Herhangi bir sayı cisminin cebirsel tamsayılar halkasının tamsayıca kapalı bir Noether halkası olduğunu ve asal ile maksimal ideallarinin örtüştüğünü göstereceğiz. Bu halkayı detaylıca çalışmak için geometrik bir metod kullanacağız. Böylelikle, bu sayı cisminin ideal sınıf grubunun sonlu olduğunu göstereceğiz. Ek olarak, geometrik yöntemler ile herhangi bir cebirsel tamsayılar halkasının tersinir elemanlarını karakterize edeceğiz. Sonrasında ise, sayı cisimleri için karmaşık sayılar üzerinde tanımlı Dedekind zeta fonksiyonunu tanımlayıp bu fonksiyonun 1 noktasında basit bir kutbu olduğunu göstereceğiz. Dahası, fonksiyonun bu noktadaki kalıntısının ilgili sayı cisminin değişmezleri tarafından verildiğini göreceğiz. Son olarak, sayı cisimlerinin ideal sınıf sayısının farklı yollarla hesaplama yollarından bahsedeceğiz.

ACKNOWLEDGMENTS

I would like to express my sincere gratitude to my advisors Haydar Göral and Kazım Büyükboduk for giving me the opportunity to write about an intriguing subject. It would not be possible without them. Especially, without Haydar Göral's valuable guidance and tremendous patience I could be lost. Day by day, I realise the value of precious times we have spent and still learn from them. I am deeply indebted to him for everything he taught, his willingness to teach and his support from the beginning.

I am grateful to Ayhan Günaydın and Tolga Etgü for accepting to be a part my thesis defence jury.

I would like to thank Doğa Can Sertbaş for his support as a friend and sparing his time to answer my various questions inside and outside the office.

I would also like to thank my dear friend Hikmet Burak Özcan for devoting his time to discuss not only my thesis but almost everything.

Lastly, my very special thanks go to my mother Neslihan Altuntaş who introduced me Nesin Mathematics Village almost 10 years ago and my beautiful sister Berfin Altuntaş for their limitless support.

TABLE OF CONTENTS

INTRODUCTION

In this thesis, we study finite extensions of the field of rational numbers, called *number fields*. Since the degree of the extension is finite, every element of a number field is a root of a non-zero polynomial with coefficients in $\mathbb{Q}$. The elements which satisfy a non-zero, monic polynomial with integer coefficients constitute a subring of the number field called *ring of integers of* K. The ring of integers $\mathcal{O}_K$ is a Noetherian, integrally closed ring such that its prime and maximal ideals coincide. In general, the unique factorization in $\mathcal{O}_K$ fails. On the other hand, the unique factorization property is preserved in the set of ideals of $\mathcal{O}_K$.

In the first chapter, we introduce the notion of *integrality*, and define *Noetherian rings* together with *Dedekind rings*. In particular, we develop the necessary background in order to understand $\mathcal{O}_K$ and to show that it is a Dedekind domain.

In Chapter 2, we begin to study number fields and their rings of integers. Note that if the degree of the number field over $\mathbb{Q}$ is 2, we call it *quadratic* and if the degree is 3, it is called *cubic*. In this chapter, we study their rings of integers briefly. We see that $\mathcal{O}_K$ is a Dedekind domain. In addition, we introduce the *norm* of an ideal and recall the class group $Cl(K)$ of K. However, we are not able to show that *the class number* of K is finite, yet.

Next, we study the geometry of number fields in Chapter 3. We introduce *lattices* and develop geometrical techniques to understand the structure of $\mathcal{O}_K$. To do so, we embed $\mathcal{O}_K$ inside a finite dimensional real vector space. First, we prove that $Cl(K)$, namely *the class number* h_K *of* K is finite. After that, we prove **Dirichlet's Unit Theorem**:

Let K be a number field of degree n over $\mathbb{Q}$. Then,

$$\mathcal{O}_K^{\times} \cong \mu(K) \times \mathbb{Z}^{r_1+r_2-1}.$$

where $n = r_1 + 2r_2$ such that r_1 is the number of real embeddings of K, r_2 is the number of non-conjugate complex embeddings of K and $\mu(K)$ is the finite group of roots of unity in K.

Thus, we characterize the unit group of $\mathcal{O}_K$.

In Chapter 4, we introduce the *Dedekind zeta function* which is named for *Julius Wilhelm Richard Dedekind*. Then, we present the main result of this thesis, the *Analytic Class Number Formula*, which consists of important invariants of a number field K.

Theorem. *The Dedekind zeta function $\zeta_K(s)$ converges for any s with $Re(s) > 1$, has a simple pole at $s = 1$ and*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}R_K}{|\mu(K)|\sqrt{|\Delta_K|}}\ h_K.$$

where h_K is the class number of K and R_K is the regulator of K.

The positive integer h_K measures how far is $\mathcal{O}_K$ being a PID. Loosely speaking, Δ_K measures the size of $\mathcal{O}_K$ and R_K measures the density of units in $\mathcal{O}_K$.

The formula was first introduced by *Peter Gustav Lejeune Dirichlet* in 1839. His work was not a residue calculation but he studied the limit $\dfrac{T(x)}{x}$ as x goes to infinity, where $T(x)$ is the number of ideals with norm bounded by x. By doing so, Dedekind proved that $\lim_{s\to 1^+}(s-1)\zeta_K(s)$ exists and given by the formula above for any number field K.

Notice that on the left-hand side, we have an analytic object and on the right-hand side we have arithmetic objects. So, we can say that *aritmetic information can be encoded by analytic objects.*

In Chapter 5, we introduce different techniques to calculate the class number of K. We present binary quadratic forms to calculate the class number of an imaginary quadratic field. We continue with *continued fractions*, which can be useful to solve

Pell's Equation. As a consequence, we find the *fundamental unit* of a real quadratic number field. Then, via *Minkowski's bound*, we study the structure of the ideal class group and based on our knowledge on ideals of $\mathcal{O}_K$. Finally, we evaluate the class number of a quadratic number field via $L-$functions.

Chapter 1

PRELIMINARIES

1.1 Integrality

We first introduce the integrality of elements over a ring. In this thesis, a ring always be a commutative ring with unity. Detailed arguments on the context can be found in [1], [2] and [3].

Let B be a ring and A a subring of B.

Definition 1.1. An element $\alpha \in B$ is integral over A if for some monic non-zero polynomial $f(X) \in A[X]$ we have $f(\alpha) = 0$.

The following theorem states equivalent conditions for an element to be *integral*.

Theorem 1.2. *[1, Chapter 2.1, Theorem 1] Let α be an element of B. Then the following statements are equivalent:*

1. $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ *for some* $a_{n-1}, \ldots, a_0 \in A$ *and* $n \in \mathbb{Z}^{\geq 1}$.

2. $A[\alpha]$ *is a finitely generated A-module.*

3. B *has a subring containing A and α which is finitely generated as an A-module.*

Proof. (1) $\implies$ (2). Assume that y is an element of $A[\alpha]$ such that

$$y = \sum_{i=0}^{m} a_i \alpha^i$$

for some $a_i \in A$ for any $i = 0, \ldots, m$.

It is enough to show that for any $i \geq n$, α^i can be written as a linear combination of $1, \ldots, \alpha^{n-1}$ with coefficients in A.

We continue by induction on $i \geq n$. Suppose first that $i = n$. Then,

$$\alpha^i = \alpha^n = -a_0 - a_1\alpha - \cdots - a_{n-1}\alpha^{n-1}.$$

Let $i > n$ and for any $j \leq i-1$, suppose that α^j can be written in terms of $1, \alpha, \ldots, \alpha^{n-1}$. Then,

$$\alpha^i = -a_0\alpha^{i-n} - a_1\alpha^{i-n+1} - \cdots - a_{n-1}\alpha^{i-1}$$

and we are done.

(2) $\implies$ (3). Taking B as $A[\alpha]$ gives the result.

(3) $\implies$ (1). Let B is generated by $s_1, \ldots, s_n$ as an A-module. Since $\alpha s_i \in B$ for any $i = 1, \ldots, n$, we can write

$$\alpha s_i = \sum_{j=1}^{n} m_{ij} s_j$$

for some $m_{ij} \in A$ and $1 \leq i, j \leq n$. Define the matrix $M = (m_{ij})_{1 \leq i,j \leq n}$ and let S be the matrix $(s_1, \ldots, s_n)^T$. Then, $\alpha S = MS$ or $(\alpha Id - M)S = 0$. However, S is non-trivial therefore $(\alpha Id - M)$ must have a non-trivial kernel.

Thus, $\det(\alpha Id - M) = \alpha^n + \sum_{i=0}^{n-1} a_i\alpha^i = 0$ where each $a_i \in A$ since the coefficients of M belong to A. Therefore, we find the desired equation. □

An equation $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some $a_{n-1}, \ldots, a_0 \in A$, $n \in \mathbb{Z}^{\geq 1}$ is called *an equation of integral depence of α over A.*

Proposition 1.3. *[1, Chapter 2.1, Proposition 1] Let $\{x_1, \ldots, x_n\} \subseteq B$ be a finite set of elements which are integral over A. If for any i, the element x_i is integral over $A[x_1, \ldots, x_{i-1}]$ then $A[x_1, \ldots, x_n]$ is a finitely generated A-module.*

By Theorem 1.2 and Proposition 1.3 we conclude the following:

Corollary 1.4. *If $\alpha, \beta \in B$ are integral over A, then so are $\alpha \pm \beta$ and $\alpha\beta$.*

The corollary above states that the set of integral elements over a ring constitutes a ring. In particular, if we set $A' := \{\alpha \in B | \alpha \text{ is integral over } A\}$, then A' is a subring of B containing A.

Definition 1.5. Let B be a ring and A a subring of B.

The set of elements $A' = \{\alpha \in B | \alpha \text{ is integral over } A\}$ is called the *integral closure* of A over B. If every element of B is integral over A, then B is said to be *integral over* A. In this case, we also say that B is an *integral extension* of A.

Naturally, the following proposition arises:

Proposition 1.6. *[1, Chapter 2.1, Proposition 2] Let A be a subring of a ring B and B a subring of a ring C so that B is integral over A and C is integral over B. Then, C is integral over A.*

Now, let us see what happens in an integral extension when we have a field instead of a ring.

Proposition 1.7. *Suppose that B is a domain, A is a subring of B such that B is integral over A. Then, A is a field if and only if B is a field.*

Proof. Let A be a field and take any non-zero element $\beta \in B$. Since B is integral over A, $A[\beta]$ is a finite dimensional vector space over A by Theorem 1.2. Note that the transformation $a \mapsto \beta a$ is an $A - linear$ transformation on $A[\beta]$. Since $\beta \neq 0$ and A is a domain, the kernel of the transformation is trivial and the map is injective. Also, since $A[\beta]$ is a finite dimensional vector space, the map is surjective. Thus, there exists some $\beta' \in A[\beta]$ such that $\beta\beta' = 1$. Therefore, B is a field.

On the other hand, if B is a field, take any non-zero $\alpha \in A$. Then, there exist $\alpha^{-1} \in B$ and it is integral over A so we can write

$$\alpha^{-n} + a_{n-1}\alpha^{-n+1} + \cdots + a_1\alpha^{-1} + a_0 = 0$$

for some $a_{n-1}, \ldots, a_0 \in A$. If we multiply both sides with α^{n-1} we get

$$\alpha^{-1} = -(a_0\alpha^{n-1} + a_1\alpha^{n-2} + \cdots + a_{n-1}) \in A$$

and we are done.

□

Definition 1.8. Let A be a domain and K be its field of fractions. We call the integral closure of A in K simply as *integral closure of A*. In addition, A is called integrally closed if its integral closure is equal to itself.

For instance, any unique factorization domain is integrally closed. Let us prove it.

Example 1.9. If A is a unique factorization domain then it is integrally closed.

Proof. Let $K = Frac(A)$ and $\alpha \in K$. Then $\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_1\alpha + c_0 = 0$ for some $c_{n-1}, \ldots c_0 \in A$.

Since $\alpha = \frac{a}{b}$ for some $a, b \in A, b \neq 0$ we have $(\frac{a}{b})^n + c_{n-1}(\frac{a}{b})^{n-1} + \cdots + c_1(\frac{a}{b}) + c_0 = 0$. Multiplying both sides with b^n results in $a^n + bc_{n-1}a^{n-1} + \cdots + b^{n-1}c_1a + b^nc_0 = 0$. Therefore, $a^n = b\gamma$ for some $\gamma \in A$ and b divides a^n implies b divides a since A is a UFD. As a conclusion, b is a unit and $\frac{a}{b} = \alpha \in A$. □

Now, let R be a ring and $K \subseteq R$ be a field.

Definition 1.10. Let $\alpha \in R$. We say that α is algebraic over K if

$$a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_n, \ldots, a_0 \in K$, not all equal to 0.

Let us say that $a_n \neq 0$, so, since K is a field $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ implies that $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$ for some $b_{n-1}, \ldots, b_0 \in K$. Thus, for an algebraic element $\alpha \in R$ there exists a non-zero, monic polynomial $f(X) \in K[X]$ satisfying $f(\alpha) = 0$.

In addition, $a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ in which not all the coefficients are zero, it can be said that $\alpha^n, \ldots, \alpha, 1$ are linearly dependent. If $\beta \in R$ is not

algebraic over K then it is called transcendental over K. In this case, for any $n \in \mathbb{Z}^{\geq 0}$ the elements $\{1, \beta, \ldots, \beta^n\}$ are linearly independent.

Let $\alpha \in R$ be an element which is algebraic over K.

Write $\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ for some $a_{n-1}, \ldots, a_0 \in K$. By Theorem 1.2, $K[\alpha]$ is finitely generated, therefore, $K[\alpha]$ is a vector space over K of finite dimension.

Definition 1.11. R is algebraic over K if every element of R is algebraic over K. In particular, if R is a field then it is called an algebraic extension of K

Definition 1.12. Let L be a field and $K \subseteq L$ a subfield of L. The field L is a K-vector space and its dimension over K is denoted by $[L : K]$.

Let $\alpha \in R$ be an algebraic element over K. Define the following homomorphism:

$$\varphi : K[X] \to R$$

$$f(X) \mapsto f(\alpha)$$

$$a \mapsto a, \forall a \in K$$

Let us make some observations. Since K is a field, $K[X]$ is a principal ideal domain. Therefore, $Ker(\varphi) \subseteq K[X]$ is a principal ideal so that it is generated by a single element. Also if α is algebraic over K, then we have a non-trivial element in $Ker(\varphi)$, so $Ker(\varphi) \neq (0)$. Therefore, there exists a monic, nonzero polynomial $f(X) \in K[X]$ such that $Ker(\varphi) =< f(X) >$. Here, $f(X)$ is determined by K and α uniquely. Lastly, image of φ is $K[\alpha]$ and we have the canonical isomorphism $K[X]/ < f(X) > \cong K[\alpha]$.

Definition 1.13. $f(X) \in K[X]$ in the argument above is called the minimal polynomial of α over K and will be denoted as $m_\alpha(X)$.

The minimal polynomial $m_\alpha(X)$ is irreducible and for any $g(X) \in K[X]$ satisfying $g(\alpha) = 0$, we have $m_\alpha(X) | g(X)$.

Proposition 1.14. *If $f(X) \in K[X]$ is a non-constant polynomial, then there exists some finite extension L of K such that $f(X)$ splits into linear factors over L.*

Definition 1.15. K is called *algebraically closed* if any non-constant $f(X) \in K[X]$ can be written as a product of linear factors in K.

It can be shown via *Zorn's Lemma* that any field can be embedded into an algebraically closed field.

Definition 1.16. An extension L of K is called an algebraic closure of K if every polynomial over K splits into linear factors over L. We will denote L by $\overline{K}$.

Now, let L_1 and L_2 be two fields containing K.

Definition 1.17. Suppose that $\varphi : L_1 \to L_2$ is a field isomorphism. If, $\varphi(a) = a$ for any $a \in K$ then φ is called a $K - isomorphism$ of L_1 onto L_2. In this case, they are called *conjugate over K* or $K - isomorphic$.

Definition 1.18. Let α_1, α_2 belong to L_1 and L_2 respectively. If there exists a $K - isomorphism$ $\varphi : K(\alpha_1) \to K(\alpha_2)$ such that $\varphi(\alpha_1) = \alpha_2$ then, α_1 and α_2 are called *conjugate over K*.

Before closing this subsection, we will give the following theorems without proofs. They will be quietly used in Chapter 2 and Chapter 3. (See [1, Chapter 2.4] for the proofs).

Theorem 1.19. *[1, Chapter 2.4, Theorem 1] Let L be an extension of K of degree n. Then, there exist $n-$many distinct $K-$isomorphisms from L to any field containing $\overline{K}$.*

Theorem 1.20 (Primitive Element Theorem)**.** *[1, Chapter 2.4, Corollary 1] Suppose that K is finite or of characteristic 0 and L is an extension of K of degree n. Then, there exists an element $\gamma \in L$ such that $L = K(\gamma)$.*

1.2 Norm and Trace

In this section, let us say that B be a ring and $A \subseteq B$ a subring where B is a free A-module of finite rank n unless otherwise is stated.

Now, let α be an element of B.

Define the following map, an A-module endomorphism:

$$\mu_\alpha : B \to B$$

$$x \mapsto \alpha x$$

If we choose a base for B, then μ_α can be represented by an $n \times n$ matrix. By *trace* and *determinant* of μ_α, we mean the trace and determinant of this matrix, respectively. It is important to note that they are independent of the choice of base for B.

Definition 1.21. The trace of μ_α is called the *trace of α relative to B and A* and is denoted by $Tr_{B/A}(\alpha)$. Determinant of μ_α is called the *norm of α relative to B and A* and is denoted by $N_{B/A}(\alpha)$.

Also, we can define the *characteristic polynomial* of α relative to B and A, $\chi_{B/A}(X)$. It is defined as the characteristic polynomial of μ_α, namely, $\det(X \cdot I - \mu_\alpha)$.

After doing some matrix arithmetic we can show that if $\alpha, \beta \in B$,
then $Tr_{B/A}(\alpha+\beta) = Tr_{B/A}(\alpha)+Tr_{B/A}(\beta)$. Also, we have $N_{B/A}(\alpha\beta) = N_{B/A}(\alpha)N_{B/A}(\beta)$.
In particular, for any $a \in A$, $Tr_{B/A}(a\alpha) = aTr_{B/A}(\alpha)$ and $N_{B/A}(a\alpha) = a^n N_{B/A}(\alpha)$.

Proposition 1.22. *[1, Chapter 2.6, Proposition 1] Assume that F is a finite field or a field of characteristic 0, E an algebraic extension of F with $[E : F] = n$ and $\alpha \in E$. Furthermore, assume that $\alpha_1, \ldots, \alpha_n$ are the roots of $m_\alpha(X)$, the minimal polynomial of α over K, such that α_i is repeated $[E : F[\alpha_i]]$ times. Then, $\chi_{E/F}(X) = \prod_{i=1}^{n}(X - \alpha_i)$, $Tr_{E/F}(\alpha) = \sum_{i=1}^{n} \alpha_i$ and $N_{E/F}(\alpha) = \prod_{i=1}^{n} \alpha_i$.*

Therefore, $\chi_{L/K}(X) = (m_\alpha(X))^{[L:K[\alpha]]}$.

Proposition 1.23. *[1, Chapter 2.6, Proposition 1] Given an extension L/K of degree n where K is of characteristic 0, $\alpha \in L$ that is algebraic over K with minimal polynomial $m_\alpha(X)$ we have $\chi_{L/K}(X) = (m_\alpha(X))^{[L:K[\alpha]]}$.*

Proposition 1.24. *Let A be a domain, $K = Frac(A)$ and of characteristic 0, L a finite extension of K. Suppose that $\alpha \in L$ is an integral element over A with characteristic polynomial relative to L and K: $\chi_{L/K}(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$. Then, $c_{n-1}, \ldots c_0$ and both $Tr_{L/K}(\alpha)$ and $N_{L/K}(\alpha)$ are integral over A.*

Proof. By Proposition 1.22, we can say that $\chi_{L/K}(X) = (X-\alpha_1)\ldots(X-\alpha_n)$. Therefore, the coefficients of the polynomial are sums of products of $\alpha_i's$. We also know that each α_i is a conjugate of α so that there exists a $K-isomorphism$ φ_i from $K[\alpha]$ into $K[\alpha_i]$ such that $\varphi_i(\alpha) = \alpha_i$. Furthermore, since α is integral over A, $\alpha^m + a_{m-1}\alpha^{m-1} + \cdots + a_1\alpha + a_0 = 0$ is satisfied for some $a_{m-1}, \ldots, a_0 \in A$. Applying φ_i to this equation, we conclude that α_i is integral over A. Then by Corollary 1.4, we get the result. □

As a consequence, we have the following corollary:

Corollary 1.25. *In addition, if A is integrally closed, then*

$$a_{n-1}, \ldots, a_0 \text{ and } Tr_{L/K}(\alpha), N_{L/K}(\alpha) \in A.$$

Now, we define the *discriminant* of a collection elements of B. It is quite important because it can be used to check whether a collection of elements give a base or not.

Definition 1.26. Let B be a ring, A a subring of B such that B is a free A-module of finite rank n and let $x_1, \ldots, x_n \in B$. We define the discriminant of $(x_1, \ldots, x_n) \subseteq B^n$ as $\det(Tr_{B/A}(x_ix_j))$. We denote it by $D(x_1, \ldots, x_n)$ and it is an element of A.

Proposition 1.27. *[1, Chapter 2.7, Proposition 3] Let F be a finite field or of characteristic 0, E an extension of F of degree n and let $\sigma_1, \ldots, \sigma_n$ be the distinct $F-isomorphisms$ from E to $\overline{F}$. Then, for any $x_1, \ldots, x_n \in E$, $D(x_1, \ldots, x_n) = \det(\sigma_i(x_j))^2_{1\leq i,j\leq n}$. If $\{x_1, \ldots, x_n\}$ is a base for E over F, then $D(x_1, \ldots, x_n) \neq 0$.*

Proof. Let $M = (\sigma_i(x_j))_{1\leq i,j\leq n}$. Then, $(M^TM)_{ij} = \sigma_1(x_i)\sigma_1(x_j)+\cdots+\sigma_n(x_i)\sigma_n(x_j) = \sigma_1(x_ix_j) + \cdots + \sigma_n(x_ix_j) = Tr_{B/A}(x_ix_j)$.

For the second part, see [1, Chapter 2.7, Proposition 3]. □

The following theorem gives an important property of the integral closure of a ring inside a field extension. Before the proof, we give a remark:

Remark 1.28. Considering L as a finite dimensional K-vector space, we can say that the bilinear form $(\alpha, \beta) \mapsto Tr_{L/K}(\alpha\beta)$ is non-degenerate: *if* $Tr_{L/K}(\alpha\beta) = 0$ *for any* $\beta \in L$ *then* $\alpha = 0$. In addition, if $(x_1, \ldots, x_n)$ is a base of L over K, then there exists a base $(y_1, \ldots, y_n)$ of L over K where

$$Tr_{L/K}(x_iy_j) = \delta_{ij}, (1 \leq i, j, \leq n).$$

Theorem 1.29. *[1, Chapter 2.7, Theorem 1] Suppose that A is an integrally closed ring, $K = Frac(A)$, L an extension of K of degree n, A' the integral closure of A in L and K has characteristic 0. Then, for some free A-module C of rank n, A' is an $A-$submodule of C.*

Proof. Assume that $(e_1, \ldots, e_n)$ is a base of L over K. Every e_i satisfies an equation of the form $a_ne_i^n + a_{n-1}e_i^{n-1} + \cdots + a_1e_i + a_0 = 0$ with $a_j \in A$ for every $j = 0, \ldots, n$ and a_n can be chosen to be non-zero. Multiplying the equation by a_n^{n-1} gives us $(a_ne_i)^n + a_{n-1}(a_ne_i)^{n-1} + \cdots + a_1a_{n-1}^{n-2}(a_ne_i) + a_n^{n-1}a_0 = 0$. Therefore, a_ne_i is integral over A. Set $e_i^{'} = a_ne_i$. Then we have that $(e_1^{'}, \ldots, e_n^{'})$ is a base of L over K and $e_i^{'} \in A'$ for any i.

Now, by the remark above, we have a basis

$(f_1, \ldots, f_n)$ of L over K and $Tr_{L/K}(e_i^{'}f_j) = \delta_{ij}, (1 \leq i, j, \leq n)$. Take any $z \in A'$. z can be written as $\sum_{j=1}^{n} b_jf_j$ for some $b_j \in K$. Since $e_i^{'} \in A$ for any i, $e_i^{'}z \in A'$, thus, $Tr_{L/K}(e_i^{'}z) \in A$ by Corollary 1.25. Therefore, $Tr_{L/K}(e_i^{'}z) = Tr_{L/K}(\sum_{j=1}^{n} b_je_i^{'}f_j) =$

$\sum_{j=1}^{n} b_j Tr_{L/K}(e_i' f_j) = \sum_{j=1}^{n} b_j \delta_{ij} = b_i$. In conclusion, $b_i \in A$ for any i, therefore A' is a submodule of $\sum_{j=1}^{n} Af_j$ which is a free A-module. □

Corollary 1.30. *In addition, if A is PID then A' is a free A-module of rank n.*

Proof. We know by [1, Chapter 1.5, Theorem 1] that A' is a free A-module of rank q, $0 \leq q \leq n$. However, we know by Theorem 1.29 above that A' contains a base of L over K. Thus, A' is a free A-module of rank exactly n. □

1.3 Noetherian Rings

Let A be a ring and M an A-module. Then, the following statements are equivalent:

Theorem 1.31. *[1, Chapter 1.4, Theorem 1]*

1. *Any collection of submodules of M that is non-empty contains a maximal element.*

2. *Any increasing sequence of submodules of M is stationary.*

3. *Any submodule of M is finitely generated.*

Proof. (1) $\implies$ (3). Let $N \leq M$ and $C = \{E \leq N | E \text{ is finitely generated}\}$. C contains 0 so that it is non-empty. Then, it has a maximal element, say E. If $E \not\subseteq N$ then for some $x \in N - E$, (E, x) is a finitely generated submodule of N and $E \not\subseteq (E, x)$. This contradicts with the maximality of E.

(3) $\implies$ (2). Let $(E_i)_{i \in \mathbb{N}}$ be an increasing sequence of submodules of M. Let us say that $E = \bigcup_{i \in \mathbb{N}} E_i$. We can say that E is generated by elements $\{e_1, \ldots, e_k\}$ where $e_i \in E_{n_i}$ for $i = 1, \ldots, k$. Now, set $n = \max_{1 \leq i \leq k}(n_i)$.

Then, $\bigcup_{i \in \mathbb{N}} E_i \subseteq E_n \subseteq E_{n+1} \subseteq \cdots \subseteq \bigcup_{i \in \mathbb{N}} E_i$. Therefore, $E_{n+j} = E_n$ for any $j \in \mathbb{N}$ so the sequence is stationary.

(2) $\implies$ (3). Suppose that $N \leq M$ is not finitely generated so we can find elements $x_i \in N$ for some $i \in I$ where I is a countable index set. Now, consider the sequence of submodules $(x_1) \subseteq (x_1, x_2) \subseteq \dots$. The sequence does not terminate because otherwise N would be finitely generated, thus, we are done. □

Definition 1.32. M is called a Noetherian A-module if one of the statements above holds. A is called a Noetherian ring if it is Noetherian as an A-module.

Now let us give the following proposition without a proof.

Proposition 1.33. *[1, Chapter 3.1, Proposition 1] Assume that A is a ring, M an A-module and $M' \leq M$. Then, M is Noetherian if and only if M' and M/M' is Noetherian.*

Corollary 1.34. *Assume that $M_1, \dots, M_n$ are Noetherian A-modules. Then, $\prod_{i=1}^{n} M_i$ is a Noetherian A-module.*

Proof. We have $M_1 \cong M_1 \times \{0\} \leq M_1 \times M_2$ and the quotient $M_1 \times M_2 / M_1 \times \{0\} \cong M_2$. Then, by above proposition $M_1 \times M_2$ is Noetherian. By induction on n, we conclude the result. □

Corollary 1.35. *If A is Noetherian and M is a finitely generated A-module, then M is Noetherian.*

Proof. Let us say that the A-module M is generated by n elements.

Then, we know by [1, Chapter 1.4] that M is isomorphic to a quotient of a free module, namely A^n/M'. By Corollary 1.34, A^n is Noetherian. Then, by Proposition 1.33 we conclude the result. □

We will close this section with the proposition below.

Proposition 1.36. *Suppose that A is Noetherian and integrally closed in its field of fractions K. Suppose also that K has characteristic 0 and L is a finite extension of K of degree n. Define A' to be the integral closure of A in L. Then, A' is a Noetherian ring and finitely generated as an A-module.*

Proof. By Theorem 1.29, we can say that A' is a submodule of a free A-module of rank n. In addition, A' is a finitely genetared A-module and by the corollary above, it is Noetherian as an A-module. Lastly, the ideals of A' correspond to A-submodules of A' so that they satisfy the conditions to be Noetherian given in Theorem 1.31. □

Lemma 1.37. *[1, Chapter 3.3, Lemma 3] If A is Noetherian and I is an ideal of A, then for some prime ideals $\mathfrak{p}_1, ..., \mathfrak{p}_n$ we have $\mathfrak{p}_1 ... \mathfrak{p}_n \subseteq I$. If A is a Noetherian domain and $0 \neq I$ is an ideal of A, then $\mathfrak{q}_1 ... \mathfrak{q}_n \subseteq I$ for some non-zero prime ideals $\mathfrak{q}_1, ..., \mathfrak{q}_n$.*

Proof. We will prove the second part of the theorem since the first part follows from the same argument. Suppose that A is a Noetherian domain. Let C be the collection of non-zero ideals of A that does not contain a product of non-zero prime ideals. Let C be non-empty. A is Noetherian, therefore we have a maximal element $I \in C$. I is not prime because otherwise it would lie in C, so that for some $x, y \in A$, $x \notin I$ and $y \notin I$, $xy \in I$. Now, (I, x) and (I, y) are two ideals that properly contain I and they do not belong to C since I is maximal. Therefore, $\mathfrak{p}_1 \dots \mathfrak{p}_r \subseteq (I, x)$ and $\mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq (I, y)$, for some prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ and $\mathfrak{q}_1, \dots, \mathfrak{q}_s$.

Finally, since $xy \in I$ we have $\mathfrak{p}_1 \dots \mathfrak{p}_r \mathfrak{q}_1 \dots \mathfrak{q}_s \subseteq (I, x)(I, y) \subseteq I$, a contradiction. □

1.4 Dedekind Domains

Definition 1.38. Let A be an integral domain. A is called a Dedekind domain if the following statements are satisfied:

1. A is Noetherian.

2. A is integrally closed.

3. Every non-zero prime ideal of A is maximal.

For instance, any PID is Dedekind.

Now, we give a crucial theorem on the structure of Dedekind domains. The theorem allows us to say that for any number field K, $\mathcal{O}_K$ is a Dedekind domain.

Theorem 1.39. *[1, Chapter 3.4, Theorem 1] Suppose that A is a Dedekind domain with $Frac(A) = K$, L is a finite extension of K of degree n and A' is the integral closure of A in L. Suppose also that the characteristic of K is 0. Then, A' is a finitely generated A-module and a Dedekind domain.*

Proof. First of all, A' is integrally closed by definition. Also, by Proposition 1.36, we can say that A' is a Noetherian ring and finitely generated as an A-module. We show that every non-zero prime ideal of A' is maximal and we are done.

Let $P \neq (0)$ be a prime ideal of A' and take a non-zero element $\alpha \in P$. Since α is integral over A, we can write an equation of integral depence of α over A with a smallest degree possible as:

$$\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$$

for some $a_{n-1}, \ldots, a_1, a_0 \in A$.

We can say that $a_0 \neq 0$ because otherwise we would have an equation of degree $n-1$. Let us denote the ideal generated by α inside A' with $A'\alpha$. Then, by the equation above $a_0 \in A'\alpha \cap A \subseteq P \cap A$, therefore, $P \cap A \neq (0)$. It can be verified that $P \cap A$ is a prime ideal of A and since A is a Dedekind domain, it is maximal. Thus, $A/(P \cap A)$ is a field. Now, since A' is integral over A, we can say that A'/P is integral over $A/(P \cap A)$. This is because if we take an element $\bar{\beta}$ from A'/P then we can write an equation of integral depence of β over A and re-write the equation modulo $P \cap A$. To add, we can say that $A/(P \cap A)$ can be identified with a subring of A'/P. Then by Proposition 1.7, we conclude that A'/P is a field and P is a maximal ideal of A'. □

Let us call the ideals of A as *integral ideals*. Suppose that I is an $A-$*submodule* of K so that for some $0 \neq \alpha \in A$, $\alpha I \subseteq A$. In this case I is called a *fractional ideal* of A. Any integral ideal is a fractional ideal. Ideal operations on fractional ideals are defined similarly. Fractional ideals give a monoid under multiplication with the identity element A.

Theorem 1.40. *[1, Chapter 3.4, Theorem 2] Suppose that A is a Dedekind Domain. If A is not a field, then every prime ideal of A is invertible and inverse of a prime ideal is a fractional ideal of A.*

Proof. Let $\mathfrak{p}$ be a prime ideal of A. Since A is not a field and $\mathfrak{p}$ is maximal, $\mathfrak{p} \neq (0)$.

Define $\mathfrak{p}' = \{\alpha \in K | \alpha\mathfrak{p} \subseteq A\}$. $\mathfrak{p}$ is a fractional ideal of A.

Now, $A \subseteq \mathfrak{p}'$ since for any $x \in A, x\mathfrak{p} \subseteq A$. We have $\mathfrak{p}\mathfrak{p}' \subseteq A$ and $\mathfrak{p} = \mathfrak{p}A \subseteq \mathfrak{p}'\mathfrak{p}$. Thus, $\mathfrak{p} \subseteq \mathfrak{p}\mathfrak{p}' \subseteq A$ but A is a Dedekind domain so we have either $\mathfrak{p}\mathfrak{p}' = A$ or $\mathfrak{p}\mathfrak{p}' = \mathfrak{p}$.

If the latter holds, take an arbitrary element $\alpha \in \mathfrak{p}'$. For any $n \in \mathbb{N}$,

$$\alpha^n\mathfrak{p} \subseteq \cdots \subseteq \alpha\mathfrak{p} \subseteq \mathfrak{p}.$$

Therefore, for any $0 \neq p \in \mathfrak{p}'$, and $n \in \mathbb{N}$, $p \in (\alpha^n\mathfrak{p})$. So, for any non-zero $\gamma \in \mathfrak{p}$, $x^n\gamma \in \mathfrak{p} \subseteq A$. Thus, $A[\alpha]$ is a fractional ideal of A and recall that A is Noetherian, therefore $A[\alpha]$ is a finitely generated A-module. Thus, α is integral over A. In addition, A is integrally closed so that $\alpha \in A$. As a conclusion, $\mathfrak{p}'\mathfrak{p} = \mathfrak{p}$ implies that $\mathfrak{p}' = A$.

Now, take $0 \neq \beta \in \mathfrak{p}$. By Lemma 1.37, for some prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, we have $\mathfrak{q}_1 \ldots \mathfrak{q}_s \subseteq A\beta = (\beta)$. Choose smallest possible s, so we have $\mathfrak{p} \supseteq A\beta \supseteq \mathfrak{q}_1 \ldots \mathfrak{q}_s$ which implies that $\mathfrak{p} \supseteq \mathfrak{q}_i$ for some i. Maximality of $\mathfrak{p}$ implies that $\mathfrak{p} = \mathfrak{q}_i$. Without loss of generality, say $\mathfrak{q}_i = \mathfrak{q}_1$

Let us define an ideal $\mathfrak{a} = \mathfrak{q}_2 \ldots \mathfrak{q}_s$. Then, $A\beta \supseteq \mathfrak{p}\mathfrak{a}$ and since s is chosen to be the smallest number as possible, $A\beta \not\supseteq \mathfrak{a}$. Therefore, there exists $a \in \mathfrak{a}$ where $a \notin A\beta$. Lastly, since $A\beta \supseteq \mathfrak{p}\mathfrak{a}$ we have $A\beta \supseteq \mathfrak{p}a$ so that $\mathfrak{p}a\beta^{-1} \subseteq A$ but then, $a\beta^{-1}$ must be in $\mathfrak{p}'$ by the definition of $\mathfrak{p}'$. However, we know that $a \notin A\beta$ and this implies that $a\beta^{-1} \notin A$. Therefore, $\mathfrak{p}' \neq A$. □

Theorem 1.41. *[1, Chapter 3.4, Theorem 3] Suppose that A is a Dedekind domain. Then, every non-zero fractional ideal of A can be uniquely written as a product of prime ideals of A with integer exponents. Moreover, the monoid of non-zero fractional ideals of A is a group.*

Proof. Let us start with an observation. Let J be any fractional ideal so that we have $\alpha J \subseteq A$ for some non-zero $\alpha \in A$. Therefore, $J = (\alpha J)(\alpha A)^{-1}$. Thus, if we prove the statement for any integral ideal of A, we conclude the result.

Now, let S be the set of non-zero integral ideals of A which does not admit a prime ideal factorization and suppose that it is not empty. Since A is Noetherian, S has a maximal element, say I. We have $I \neq A$ since A is the empty product of prime ideals. Then, I is contained in a maximal ideal $\mathfrak{m}$ of A. Let $\mathfrak{m}'$ be the inverse of $\mathfrak{m}$. We have $I \subseteq \mathfrak{m}$, which implies that $I\mathfrak{m}' \subseteq \mathfrak{m}\mathfrak{m}' = A$. Moreover, $\mathfrak{m}' \supsetneq A$ thus $I\mathfrak{m}' \supsetneq I$ Now, since $\mathfrak{m}' \neq A$, $I\mathfrak{m}'$ is an ideal that does not lie in S. Thus, $I\mathfrak{m}' = \mathfrak{p}_1 \dots \mathfrak{p}_l$ for some prime ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_l$. Therefore, $I = I\mathfrak{m}'\mathfrak{m} = \mathfrak{p}_1 \dots \mathfrak{p}_l\mathfrak{m}$ and we conclude that every ideal is a product of prime ideals.

Now, assume that an ideal I has two prime factorizations $\prod_{i=1}^{s} \mathfrak{p}_i^{e_i} = \prod_{j=1}^{t} \mathfrak{q}_j^{f_j}$ for some integers $e_1, \dots, e_s, f_1, \dots, f_t$. Then, for any $i = 1, \dots, s$ we have $\mathfrak{p}_i \supseteq \prod_{j=1}^{t} \mathfrak{q}_j^{f_j}$. As a conclusion, $\mathfrak{p}_i \supseteq \mathfrak{q}_j$ for some $\mathfrak{q}_j$, $j = 1, \dots, t$. However, since prime ideals are maximal we have $\mathfrak{p}_i = \mathfrak{q}_j$. By cancelling out the factors, we conclude that the prime factorization is unique.

Finally, if we have $I = \prod_{i=1}^{s} \mathfrak{p}_i^{e_i}$ then the inverse of I is written as $\prod_{i=1}^{s} \mathfrak{p}_i^{-e_i}$. Therefore, non-zero fractional ideals form a group under ideal multiplication. □

Let us denote the group of fractional ideals by I_K. As we define principal ideals, we define principal fractional ideals. I is a *principal fractional ideal* if it is of the form Ax for some $x \in K^{\times}$. The set of principal fractional ideals are denoted as P_K and actually P_K is a subgroup of I_K. Then, define the quotient group $Cl(K) = I_K/P_K$. It is called the *ideal class group of* A and we will work on this group in details in the following chapters.

Chapter 2

NUMBER FIELDS

Number fields are the main *objects* of this thesis. A *number field* K is a finite degree extension of $\mathbb{Q}$. They always have characteristic 0. In this chapter, we make a brief introduction to number fields and most importantly, we will notice that the *ring of integers* of a number field is a *Dedekind domain*.

Now, let K be a number field of degree n over $\mathbb{Q}$.

Definition 2.1. The set of elements $\{\alpha \in K | \alpha \text{ is integral over } \mathbb{Z}\}$ is called the ring of integers of K. It is denoted by $\mathcal{O}_K$.

By Corollary 1.4, $\mathcal{O}_K$ is a ring.

Any element $\alpha \in \mathbb{C}$ that is integral over $\mathbb{Z}$ is called an algebraic integer.

Now, let us give a proposition, which states that for any $\alpha \in K$, we can find some $z \in \mathbb{Z}$ so that $z\alpha \in \mathcal{O}_K$.

Proposition 2.2. $\mathbb{Q}\mathcal{O}_K = K$.

Proof. If we show that $K \subseteq \mathbb{Q}O_K$, we are done. The aim is, for any element $\alpha \in K$, to find some $z \in \mathbb{Z}, \beta \in \mathcal{O}_K$ such that $\alpha = \frac{\beta}{z}$.

So let $\alpha \in K$, there exists $f(X) \in \mathbb{Q}[X]$, the minimal polynomial of α. Let us say that

$$f(X) = X^n + \frac{a_{n-1}}{b_{n-1}}X^{n-1} + \cdots + \frac{a_1}{b_1}X + \frac{a_0}{b_0}$$

and we have $f(\alpha) = \alpha^n + \frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \cdots + \frac{a_1}{b_1}\alpha + \frac{a_0}{b_0} = 0$. Our aim is to find a non-zero, monic polynomial $g(X) \in \mathbb{Z}[X]$ such that $g(\beta) = 0$ where $\beta = z\alpha$ for some $z \in \mathbb{Z}$, so $\beta \in \mathcal{O}_K$.

Since the polynomial $f \in \mathbb{Q}[X]$, we have to get rid of the rational coefficients and get integer ones.

The most natural idea is to multiply these coefficients with least common multiples of denominators of them, set $D = lcm(b_0, b_1, \ldots, b_{n-1})$. Then, $Df \in \mathbb{Z}[X]$.

Notice that $f(\alpha) = \alpha^n + \frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \cdots + \frac{a_1}{b_1}\alpha + \frac{a_0}{b_0} = 0$.

Therefore $D^n f(\alpha) = D^n\alpha^n + D^n\frac{a_{n-1}}{b_{n-1}}\alpha^{n-1} + \cdots + D^n\frac{a_1}{b_1}\alpha + D^n\frac{a_0}{b_0} = 0$, thus

$$(D\alpha)^n + D\frac{a_{n-1}}{b_{n-1}}(D\alpha)^{n-1} + \cdots + D^{n-1}\frac{a_1}{b_1}(D\alpha) + D^n\frac{a_0}{b_0} = 0$$

Now say $g(X) = X^n + D\frac{a_{n-1}}{b_{n-1}}X^{n-1} + \cdots + D^{n-1}\frac{a_1}{b_1}X + D^n\frac{a_0}{b_0} \in \mathbb{Z}[X]$.
Finally, set $z = D$ and we have $\beta = z\alpha = D\alpha$. Thus,

$$g(\beta) = g(D\alpha) = (D\alpha)^n + D\frac{a_{n-1}}{b_{n-1}}(D\alpha)^{n-1} + \cdots + D^{n-1}\frac{a_1}{b_1}(D\alpha) + D^n\frac{a_0}{b_0} = 0.$$

□

Corollary 2.3. *$\mathcal{O}_K$ spans K over $\mathbb{Q}$.*

By Chapter 1, we can state some results on $\mathcal{O}_K$. In particular, we can say that $\mathcal{O}_K$ is integrally closed by Theorem 1.39.

Moreover, by Corollary 1.30, we have the following proposition:

Proposition 2.4. *$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n.*

Now, let us define an important invariant of a number field:

Definition 2.5. Let K be a number field of degree n and let $(x_1, \ldots, x_n)$ be a $\mathbb{Z}$ basis for $\mathcal{O}_K$. Then, the discriminant of K is defined as the discriminant $D(x_1, \ldots, x_n)$ and it is denoted by Δ_K.

It is important to note that Δ_K is independent from the choice of basis. To show that, let us take two bases for $\mathcal{O}_K$, $(x_1, \ldots, x_n)$ and $(y_1, \ldots, y_n)$. We can find some

$a_{ij}, b_{st} \in \mathbb{Z}$ so that $y_i = \sum_{j=1}^{n} a_{ij}x_j$ and $x_s = \sum_{t=1}^{n} b_{st}x_t$ for $1 \leq i, j, s, t \leq n$. Then $D(y_1, \ldots, y_n) = (\det(a_{ij}))^2 D(x_1, \ldots, x_n)$ and $D(x_1, \ldots, x_n) = (\det(b_{st}))^2 D(y_1, \ldots, y_n)$. Thus, $D(y_1, \ldots, y_n) = (\det(a_{ij}))^2(\det(b_{st}))^2 D(y_1, \ldots, y_n)$. Therefore, $(\det(a_{ij}))^2 = 1$ and we conclude that $D(x_1, \ldots, x_n) = D(y_1, \ldots, y_n)$.

2.1 Ideals in $\mathcal{O}_K$

In this section, we will study the ideals of $\mathcal{O}_K$ but first, let us start with the following crucial observation.

Theorem 2.6. *$\mathcal{O}_K$ is a Dedekind Domain.*

Proof. Observe that $\mathbb{Z}$ is a PID, thus, a Dedekind domain. The field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$ and K is a finite extension of $\mathbb{Q}$. The integral closure of $\mathbb{Z}$ in K is $\mathcal{O}_K$ and K has characteristic 0. Therefore, by Theorem 1.39, we conclude that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module and a Dedekind domain. □

Therefore, $\mathcal{O}_K$ is a Noetherian ring, integrally closed and its prime ideals are maximal.

Recall that we define the norm of an element in the previous chapter. It can be seen that if $\eta \in {\mathcal{O}_K}^{\times}$, then $N_{K/\mathbb{Q}}(\eta) = \pm 1$. We will characterize the units of $\mathcal{O}_K$ later.

We can also define a norm on the ideals of $\mathcal{O}_K$. $\mathcal{O}_K$ is a free abelian group of rank n and any ideal $I \subseteq \mathcal{O}$ is of rank n too, therefore we expect that $|\mathcal{O}_K/I|$ is finite. Let us proceed by defining the norm of an ideal.

Proposition 2.7. *[1, Chapter 3.5, Proposition 1] Let I be a non-zero ideal of $\mathcal{O}_K$. Then, $|\mathcal{O}_K/I|$ is finite and for any non-zero $\alpha \in \mathcal{O}_K$, $N_{K/\mathbb{Q}}(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$.*

We define the norm of I as $N_{K/\mathbb{Q}}(I) = |\mathcal{O}/I|$. Also, note that for any non-zero ideals I, J of $\mathcal{O}_K$, $N_{K/\mathbb{Q}}(I)N_{K/\mathbb{Q}}(J) = N_{K/\mathbb{Q}}(IJ)$ is satisfied ([1, Chapter 3.5, Proposition 2]).

We can see the prime ideals of $\mathcal{O}_K$ as prime numbers in some sense. Since $\mathcal{O}_K$ is a Dedekind domain, non-zero prime ideals are maximal and every non-zero ideal has a prime ideal decomposition.

Also, we have the ideal class group $Cl(K)$ of $\mathcal{O}_K$. The equivalence relation $\sim$ on $Cl(K)$ is given as $I \sim J$ whenever $\alpha I = J$ for some $\alpha \in K^\times$. The size of this group is finite and it will be proven in the next chapter.

Chapter 3

GEOMETRY OF NUMBER FIELDS

Let K be a number field. Recall that we defined the quotient group I_K/P_K, the ideal class group $Cl(K)$ of $\mathcal{O}_K$. In this chapter, we will show that the quotient group $Cl(K)$ is finite. The order of $Cl(K)$ is called *the class number* h_K of K. To add, we will characterize the structure of ${\mathcal{O}_K}^{\times}$. To do that, we need some geometric arguments.

Let us begin with a definition.

Definition 3.1. Let $\Gamma \subseteq \mathbb{R}^n$ be an additive subgroup. Γ is called discrete if for any compact set S, $\Gamma \cap S$ is finite.

Theorem 3.2. *[1, Chapter 4.1 Theorem 1] If $\Gamma \subseteq \mathbb{R}^n$ is discrete, then Γ is generated as a $\mathbb{Z}$-module by at most n vectors linearly independent over $\mathbb{R}$.*

Now, let us define a *lattice*.

Definition 3.3. A discrete subgroup $\Gamma \subseteq \mathbb{R}^n$ which is a $\mathbb{Z}$-module of rank n is called a lattice.

Definition 3.4. Let Γ be a lattice with a $\mathbb{Z}$ basis $v = \{v_1, \ldots, v_n\}$. Define the set $\Phi_\Gamma = \{x \in \mathbb{R}^n | x = \sum_{i=1}^{n} \alpha_i v_i, 0 \leq \alpha_i < 1\}$. Then, Φ_Γ is called a fundamental domain for Γ. The volume of Γ is defined as the Lebesgue measure $\mu(\Phi_\Gamma)$ of $\Phi_\Gamma \subseteq \mathbb{R}^n$.

Let us make some observations. As a side note, let Γ be a lattice which has two $\mathbb{Z}$ bases $\{v_1, \ldots, v_n\}$ and $\{w_1, \ldots, w_n\}$ and let the volume of the corresponding fundamental domains be $\mu(\Phi_{\Gamma_v})$ and $\mu(\Phi_{\Gamma_w})$ respectively. Then, $\mu(\Phi_{\Gamma_v}) = \mu(\Phi_{\Gamma_w})$. (See, [1, Chapter 4.1, lemma 1]).

Therefore, the volume of a lattice is independent from the choice of a basis.

Next, let us find the volume of a lattice.

Proposition 3.5. *[2, Chapter 7, Proposition 7.5] Let* $\Gamma = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_n$ *be a lattice in* $\mathbb{R}^n$*, where* $v_i = (a_{i1}, \ldots, a_{in})$*. Then,* $vol(\Gamma) = |\det(a_{ij})|$*.*

Proof. Let $\{e_1, \ldots, e_n\}$ be the standard basis for $\mathbb{R}^n$. We have $v_i = \sum_{i=1}^{n} a_{ij}e_j$ and let us say that an arbitrary point in the space has coordinates $(x_1, \ldots, x_n)$ with respect to the standard basis. Then,

$$vol(\Gamma) = \int_{\Phi_\Gamma} 1 dx_1 \ldots dx_n.$$

Let us change the standard basis to $\{v_1, \ldots, v_n\}$. Since any vector v_i is given as $v_i = \sum_{i=1}^{n} a_{ij}e_j$, the change of basis matrix is $A = (a_{ij})_{1 \leq i,j \leq n}$.

For any arbitrary element $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, it can be written that $x = \sum_{i=1}^{n} x_i e_i = \sum_{i=1}^{n} y_i v_i$ where $0 \leq y_i < 1$. That is because the coordinates of Φ_Γ with respect to the basis $\{v_1, \ldots, v_n\}$ are $0 \leq y_i < 1$.

So,

$$vol(\Gamma) = \int_{\Phi_\Gamma} 1 dx_1 \ldots dx_n = \int_{\Phi_\Gamma} |\det(A)| dy_1 \ldots dy_n,$$

since the Jacobian of the transformation is $|\det(A)|$. Then, we have

$$\int_{\Phi_\Gamma} |\det(A)| dy_1 \ldots dy_n = \int_0^1 \cdots \int_0^1 |\det(A)| dy_1 \ldots dy_n = |\det(A)|.$$

□

Theorem 3.6 (Minkowski)**.** *[1, Chapter 4.1, Theorem 2] Assume that* Γ *is a lattice in* $\mathbb{R}^n$ *and* S *a measurable subset with* $\mu(S) > v(\Gamma)$*. Then, for some* $x \neq y \in S$*,* $x - y$ *belongs to* Γ*.*

Proof. Let $s = (s_1 \ldots, s_n) \in S$. For any $s_i, i = \{1, \ldots, n\}$, $s_i = [s_i] + \alpha_i$ with $\alpha_i \in [0, 1)$ so that $s = p + h$ for some $p \in \Phi_\Gamma$ and $h \in \Gamma$. Therefore, $S = \bigcup_{h \in \Gamma} \Phi_\Gamma + h$. Since the union is disjoint, $\mu(S) = \sum_{h \in \Gamma} \mu(S \cap (\Phi_\Gamma + h))$.

For any h, it can be written that $\mu(S \cap (\Phi_\Gamma + h)) = \mu((S - h) \cap (\Phi_\Gamma + h - h)) = \mu((S - h) \cap \Phi_\Gamma)$.

Since $v(\Gamma) = \mu(\Phi_\Gamma) \geq \sum_{h\in\Gamma} \mu((S-h)\cap\Phi_\Gamma) = \sum_{h\in\Gamma} \mu(S\cap(\Phi_\Gamma+h)) = \mu(S)$, which contradicts with the assumption, $\sum_{h\in\Gamma} \mu((S-h)\cap\Phi_\Gamma)$ cannot be a disjoint sum. Then, for some distinct $h_1, h_2 \in \Gamma$, $(S-h_1)\cap(S-h_2)\cap\Phi_\Gamma \neq \emptyset$. If z belongs to the intersection, $z = z_1 - h_1 = z_2 - h_2$ for some $z_1, z_2 \in S, h_1, h_2 \in \Gamma$ so that $z_1 - z_2 = h_2 - h_1 \in H$ and $z_1 \neq z_2$ since h_1, h_2 are distinct. □

Corollary 3.7 (Minkowski's Convex Body Theorem)**.** *[1, Chapter 4.1, Corollary 1] Assume that Γ is a lattice in $\mathbb{R}^n$ and S a measurable subset of $\mathbb{R}^n$ where S is convex and symmetric with respect to 0. If S satisfies at least one of*

1. $\mu(S) > 2^n v(\Gamma)$
2. $\mu(S) \geq 2^n v(\Gamma)$, *$S$ is compact.*

then $S\cap\Gamma$ contains a non-zero element.

Proof. 1. $\mu(S) > 2^n v(\Gamma)$ implies that $2^{-n}\mu(S) = \mu(\frac{1}{2}S) = \mu(S') > v(\Gamma)$. Applying Minkowski's theorem yields there exist distinct $x', y' \in S'$ and $x'-y' \in H$ where $x' = \frac{1}{2}x$ and $y' = \frac{1}{2}y$ for some $x, y \in S$. The set S is symmetric with respect to 0, thus, $-y \in S$ and convexity of S implies that $\frac{1}{2}x + \frac{1}{2}(-y) = x' - y' \in S$. In conclusion, $0 \neq x' - y' \in S\cap\Gamma$.

2. The proof is similar and can be found in [1, Chapter 4.1, Corollary (b)]

□

Minkowski's theorem and the arguments on lattices provide the tools that we can implement on number fields and their ring of integers. Now, we will embed number fields inside vector spaces to get information about the corresponding ring of integers.

Let K be a number field with ring of integers $\mathcal{O}_K$ and $[K:\mathbb{Q}] = n$. Recall that $\epsilon \in \mathcal{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(\epsilon) = \pm 1$ and there are $n-$many embeddings of K into $\mathbb{C}$ -or into any field containing $\bar{K}$-.

If $\sigma : K \hookrightarrow \mathbb{C}$ is any of these embeddings, it is called *real* when $\sigma(K) \subseteq \mathbb{R}$ holds. Otherwise, it is called *complex*. Given a complex embedding τ, its conjugate is given by $\overline{\tau}(x) = \overline{\tau(x)}$ which is an embedding of K. Complex embeddings come in pairs, so if we have r_1-many real and r_2-many conjugate pair of complex embeddings, then $n = r_1 + 2r_2$ holds.

Let us fix some notation. ρ denotes any real embedding and τ denotes any complex embedding. Then, the embeddings of K are given as

$\{\rho_1, \ldots, \rho_{r_1}, \tau_1, \ldots, \tau_{r_2}, \tau_{r_2+1}, \ldots, \tau_{2r_2}\}$. If we let $\tau, \overline{\tau}$ to denote a complex pair of embeddings, the embeddings of K is then given as $\{\rho_1, \ldots, \rho_{r_1}, \tau_1, \overline{\tau_1}, \ldots, \tau_{r_2}, \overline{\tau_{r_2}}, \}$ since the complex embeddings come in pairs.

Then, K can be embedded into an $n-$dimensional vector space as follows:

$$\Psi : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

$$\alpha \mapsto (\rho_1(\alpha), \ldots, \rho_{r_1}(\alpha), \tau_1(\alpha), \ldots, \tau_{r_2}(\alpha))$$

Remark 3.8. The map Ψ is called the canonical embedding of K in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and it is generally identified with $\mathbb{R}^n$ as $\mathbb{C} \cong \mathbb{R}^2$ as a vector space.

Another identification may be done as follows:

For any $y \in K$, $y \mapsto (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

Then, $(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mapsto (x_1, \ldots, x_{r_1}, Re(z_1), Im(z_1), \ldots, Re(z_{r_2}), Im(z_{r_2}))$.

Proposition 3.9. *If H is a free $\mathbb{Z}$-submodule of K of rank n with a $\mathbb{Z}$ base $\{e_1, \ldots, e_n\}$, then $\Psi(H)$ is a lattice in $\mathbb{R}^n$ so that its volume $vol(\Psi(H)) = 2^{-r_2} |\det_{1 \leq i,j, \leq n} (\psi_i(e_j))|$.*

Proof. Let $A_{n \times n}$ be the matrix whose i^{th} column is

$$[\psi_1(e_i), \ldots, \psi_{r_1}(e_i), Re(\psi_{r_1+1}(e_i)), Im(\psi_{r_1+1}(e_i)) \ldots, Re(\psi_{r_2}(e_i)), Im(\psi_{r_2}(e_i))]$$

such that the column vector is the coordinates of $\Psi(e_i)$ with respect to the canonical basis of $\mathbb{R}^n$.

For any $z \in \mathbb{C}$, $Re(z) = \frac{z+\bar{z}}{2}$ and $Im(z) = \frac{z-\bar{z}}{2i}$ holds.

Using the equalities and applying column operations we conclude that

$$\det(A) = (2i)^{-r_2} \det_{1\leq i,j,\leq n} (\psi_i(e_j)).$$

The set $\{e_1, \ldots, e_n\}$ form a basis for K over $\mathbb{Q}$. By Proposition 1.27, we have $\det_{1\leq i,j\leq n} (\psi_i(e_j)) \neq 0$, thus, $\det(A) \neq 0$. Furthermore, $\det(A) \neq 0$ implies that the vectors $\Psi(e_i)$ are linearly independent over $\mathbb{R}$. Therefore, $\Psi(H)$ gives a lattice in $\mathbb{R}^n$. By Proposition 3.5, its volume is

$$|\det(A)| = |(2i)^{-r_2} \det_{1\leq i,j\leq n} (\psi_i(e_j))| = 2^{-r_2} |\det_{1\leq i,j\leq n} (\psi_i(e_j))|.$$

□

Corollary 3.10. *$\Psi(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ with volume $vol(\Psi(\mathcal{O}_K)) = 2^{-r_2}|\Delta_K|^{\frac{1}{2}}$.*

In addition, if $0 \neq I \subseteq \mathcal{O}_K$ is an ideal, $\Psi(I)$ is a lattice with volume

$$vol(\Psi(I)) = 2^{-r_2}|\Delta_K|^{\frac{1}{2}} N_{K/\mathbb{Q}}(I)$$

(See, [1, Chapter 4.2, Proposition 2]).

So far, we embed a number field into an $n-$dimensional vector space. Now, let us give an important proposition on the ideals of $\mathcal{O}_K$.

Proposition 3.11. *Let $I \subseteq \mathcal{O}_K$ be a non-zero integral ideal. Then, there exists an element $0 \neq x \in I$ such that*

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |\Delta_K|^{\frac{1}{2}} N_{K/\mathbb{Q}}(I).$$

Proof. Assume that $c \in \mathbb{R}^{>0}$ and define

$$D_c := \{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} : \sum_{i=1}^{r_1} |x_i| + 2\sum_{j=1}^{r_2} |z_j| \leq c\}.$$

The set D_c is compact, convex and symmetric with respect to 0. By a calculation given in [1, Chapter 4, Appendix] we have $\mu(D_c) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{c^n}{n!}$.

Choose c so that $\mu(D_c) = 2^n v(\Psi(I))$. Therefore, we have

$$2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{c^n}{n!} = 2^{n-r_2}|\Delta_K|^{\frac{1}{2}}N_{K/\mathbb{Q}}(I).$$

Note that the equality above yields $c^n = 2^{n-r_1}\pi^{-r_2}n!|\Delta_K|^{\frac{1}{2}}N_{K/\mathbb{Q}}(I)$. By Corollary 3.7, there exist an element $0 \neq x \in I$ such that $\Psi(x) \in D_c$ and

$$|N_{K/\mathbb{Q}}(x)| = \prod_{i=1}^{r_1}|\rho_i(\alpha)|\prod_{j=1}^{r_2}|\tau_j(\alpha)|^2.$$

For any n positive numbers $a_1, \ldots, a_n$, $\sqrt[n]{a_1 a_2 \ldots a_n} \leq \frac{a_1+\cdots+a_n}{n}$ holds. Therefore,

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{1}{n}\sum_{i=1}^{r_1}|\rho_i(x)| + \frac{2}{n}\sum_{j=1}^{r_2}|\tau_j(x)|\right)^n \leq \frac{c^n}{n^n}$$

since $\Psi(x) \in D_c$. Finally, recall that we have $c^n = 2^{n-r_1}\pi^{-r_2}n!|\Delta_K|^{\frac{1}{2}}N_{K/\mathbb{Q}}(I)$. Thus, we conclude that

$$|N_{K/\mathbb{Q}}(x)| \leq \frac{1}{n^n}2^{n-r_1}\pi^{-r_2}n!|\Delta_K|^{\frac{1}{2}}N_{K/\mathbb{Q}}(I).$$

Using the equality $n = r_1 + 2r_2$, we have

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\Delta_K|^{\frac{1}{2}}N_{K/\mathbb{Q}}(I).$$

□

Corollary 3.12. *In the ideal class group of $\mathcal{O}_K$, each class contains an integral ideal I with*

$$N_{K/\mathbb{Q}}(I) \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\Delta_K|^{\frac{1}{2}}.$$

Proof. Let $\mathfrak{C}$ be a class in $Cl(K)$ and $J \in \mathfrak{C}$. We know that J^{-1} is a fractional ideal and for some non-zero $\alpha \in \mathcal{O}_K$ we have $\alpha J^{-1} = \tilde{J} \subseteq \mathcal{O}_K$. By Proposition 3.11, there exists a non-zero element $x \in \tilde{J}$ such that

$$|N_{K/\mathbb{Q}}(x)| \leq \left(\frac{4}{\pi}\right)^{r_2}\frac{n!}{n^n}|\Delta_K|^{\frac{1}{2}}N_{K/\mathbb{Q}}(\tilde{J}).$$

Then, we can say that

$$\frac{|N_{K/\mathbb{Q}}(x)|}{N_{K/\mathbb{Q}}(\tilde{J})} = \frac{N_{K/\mathbb{Q}}(x\mathcal{O}_K)}{N_{K/\mathbb{Q}}(\tilde{J})} = N_{K/\mathbb{Q}}(x\tilde{J}^{-1}) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|\Delta_K|^{\frac{1}{2}}.$$

Thus, $I = x\tilde{J}^{-1}$ is the desired ideal. □

This bound is called *Minkowski's Bound* in the literature. We are almost done.

Proposition 3.13. *Fix a number $b \in \mathbb{N}$. Then, there are only finitely many ideals with norm bounded by b.*

Proof. Let $I \subseteq \mathcal{O}_K$ be a non-zero integral ideal with $N_{K/\mathbb{Q}}(I) < b$. Then, we have $I = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_m^{e_m}$ for some prime ideals $\mathfrak{p}_i$ and $e_i \in \mathbb{Z}^{>0}$. Note that each prime factor $\mathfrak{p}_i$ comes from a prime number p such that $\mathfrak{p}_i | p\mathcal{O}_K$. Also, we have

$$N_{K/\mathbb{Q}}(I) = N_{K/\mathbb{Q}}(\mathfrak{p}_1)^{e_1} \dots N_{K/\mathbb{Q}}(\mathfrak{p}_m)^{e_m}$$

where $\mathfrak{p}_i$ has norm p^k for some prime number p and $k \in \mathbb{Z}^{>0}$ such that k is bounded by n. Since the possible prime numbers p are bounded by b and the possible prime ideals that can appear in a factorization are also bounded, there can be only finitely many ideals with bounded norm. □

We are ready to prove the main theorem of this section:

Theorem 3.14 (Dirichlet)**.** *[1, Chapter 4.3, Theorem 2] The ideal class group $Cl(K)$ of $\mathcal{O}_K$ is finite.*

Proof. By Corollary 3.12, an integral ideal can be chosen from each ideal class of K so that its norm is bounded by Minkowski's bound. It is known by Proposition 3.13 that the ideals with a bounded norm is a finite set. Thus, $Cl(K)$ is finite. □

We can say that h_K measures how far is $\mathcal{O}_K$ of being a principal ideal domain.

Proposition 3.15. *$\mathcal{O}_K$ is a principal ideal domain if and only if $\mathcal{O}_K$ is a unique factorization domain.*

Proof. We only need to prove the necessity part. Since any integral ideal has a prime ideal decomposition, if we show that the prime ideals are principal, we are done. Now, suppose that $\mathcal{O}_K$ is a UFD and let $\mathfrak{p}$ be any non-zero prime ideal of $\mathcal{O}_K$. Take any non-zero element $p \in \mathfrak{p}$. Since $\mathcal{O}_K$ is UFD, we can write $p = \pi_1^{e_1} \dots \pi_m^{e_m}$ for some irreducible elements π_i. Then, $\pi_i \in \mathfrak{p}$ for some $i \in \{1, \dots, m\}$. In a UFD, irreducible elements are prime and $(\pi_i) \subseteq \mathfrak{p}$ is a prime ideal. Also, since prime ideals are maximal, we have $\mathfrak{p} = (\pi_i)$. □

3.1 Units in $\mathcal{O}_K$ and Dirichlet's Unit Theorem

Our aim is to study units of $\mathcal{O}_K$ which have a multiplicative structure. Minkowski's theorem works on vector spaces and they have an additive structure. In order to relate these two concepts, we need to find a way that translates multiplicative structures to additive ones.

Recall that K is embedded into an $n-$dimensional vector space as follows:

$$\Psi : K \hookrightarrow \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

$$\alpha \mapsto (\rho_1(\alpha), \dots, \rho_{r_1}(\alpha), \dots, \tau_1(\alpha), \dots, \tau_{r_2}(\alpha)).$$

To add, recall that for any $\alpha \in K$, norm map $N_{K/\mathbb{Q}}$ sends α to

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{r_1} \rho_i(\alpha) \prod_{j=1}^{2r_2} \tau_j(\alpha) = \prod_{i=1}^{r_1} \rho_i(\alpha) \prod_{j=1}^{r_2} \tau_j(\alpha)\overline{\tau_j(\alpha)} = \prod_{i=1}^{r_1} \rho_i(\alpha) \prod_{j=1}^{r_2} |\tau_j(\alpha)|^2.$$

A similar map N' can be defined on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as follows:

$$N' : \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \to \mathbb{R}$$

$$(x_1, \dots, x_{r_1}, z_1, \dots, z_{r_2}) \mapsto \prod_{i=1}^{r_1} x_i \prod_{j=1}^{r_2} |z_j|^2.$$

Actually, as $N_{K/\mathbb{Q}}(\alpha)$ being the determinant of the map, multiplication by α on the $\mathbb{Q}$-vector space K, the map $N'(\alpha)$ is the determinant of the multiplication by α map on $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$.

As a result, we have the following commutative diagram:

$$\begin{array}{ccc} K & \xrightarrow{\Psi} & \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N'} \\ \mathbb{Q} & \longrightarrow & \mathbb{R} \end{array}$$

Remark 3.16. For any $\alpha \in K$, $N'(\Psi(\alpha)) = N_{K/\mathbb{Q}}(\alpha)$.

Now, let us expand the diagram. Define the following maps:

$$l' : (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times \to \mathbb{R}^{r_1+r_2}$$

$$(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \mapsto (\log(|x_1|), \ldots, \log(|x_{r_1}|), \log(|z_1|^2), \ldots, \log(|z_{r_2}|^2))$$

and

$$l : \mathbb{R}^\times \to \mathbb{R}$$

$$x \mapsto \log(|x|).$$

In addition, define t on $\mathbb{R}^{r_1+r_2}$ as follows:

$$t : \mathbb{R}^{r_1+r_2} \to \mathbb{R}$$

$$(y_1, \ldots, y_{r_1+r_2}) \mapsto y_1 + \cdots + y_{r_1+r_2}.$$

Together with Remark 3.16, we have the following diagram which is also commutative:

$$\begin{array}{ccccc} K^\times & \xrightarrow{\Psi} & (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times & \xrightarrow{l'} & \mathbb{R}^{r_1+r_2} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N'} & & \downarrow{\scriptstyle t} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \xrightarrow[l]{} & \mathbb{R} \end{array}$$

We know that the units of $\mathcal{O}_K$ is given as ${\mathcal{O}_K}^\times = \{\epsilon \in \mathcal{O}_K : N_{K/\mathbb{Q}}(\epsilon) = \pm 1\}$.

Let us define $B = \{v \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times | N'(v) = \pm 1\}$ and $T = \{w \in \mathbb{R}^{r_1+r_2} | t(w) = 0\}$.

Note that $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ consists of elements that has non-zero coordinates. We define addition and multiplication on $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ coordinate-wise. Therefore, for any $v \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$ we have $v^{-1} \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$.

Then, ${\mathcal{O}_K}^\times$ is mapped into B via Ψ and the map l' takes B into $T \subseteq \mathbb{R}^{r_1+r_2}$. Therefore, we have the composite map $\varphi = l' \circ \Psi : K \to \mathbb{R}^{r_1+r_2}$ such that

$$\varphi\big|_{\mathcal{O}_K{}^\times} : \mathcal{O}_K{}^\times \to B \to T \subseteq \mathbb{R}^{r_1+r_2}.$$

Note that the subspace T has dimension $r_1 + r_2 - 1$. Finally, set $\Gamma = \varphi(\mathcal{O}_K{}^\times)$. We will understand the structure of Γ. Now, let us denote *the group of roots of unity in* K by $\mu(K)$. The group $\mu(K)$ is finite because otherwise we could find elements which have arbitrarily large degree over $\mathbb{Q}$.

Proposition 3.17. *[2, Chapter 7, Proposition 7.26] The kernel of the map φ is $\mu(K)$.*

Proof. If $\alpha \in \mu(K)$ then $|\rho_i(\alpha)| = |\tau_j(\alpha)| = 1$ for any $1 \leq i \leq r_1$ and $1 \leq j \leq r_2$. Therefore, $l'(\Psi(\alpha)) = 0$ and $\mu(K) \subseteq \ker(\varphi)$. On the other hand, if $\alpha \in ker(\varphi)$ then $|\rho_i(\alpha)| = |\tau_j(\alpha)| = 1$ for any embedding ρ_i and τ_j. So, we can say that $\Psi(\alpha)$ is contained in a bounded region inside $(\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$. Furthermore, $\Psi(\alpha)$ is also contained inside the lattice $\Psi(\mathcal{O}_K)$. There are finitely many possible $\Psi(\alpha)$'s since lattices are discrete, therefore, $ker(\varphi)$ is finite. It is also true that $ker(\varphi)$ is a multiplicative group. Then, by [1, Chapter 1.6, Theorem 1], it consists of roots of unity so any element of $ker(\varphi)$ is a root of unity. □

Now, we can also say that Γ is a subgroup of T. That is because φ is a homomorphism from $(\mathcal{O}_K{}^\times, \cdot)$ into $(T, +) \subseteq \mathbb{R}^{r_1+r_2}$.

We continue to understand the structure of Γ with the following proposition.

Proposition 3.18. *[2, Chapter 7, Proposition 7.28] Γ is a discrete subgroup of T.*

Proof. Take any ball C of radius $c \geq 0$ inside T.

We have $(l')^{-1}(\Gamma \cap C) = (l')^{-1}(\Gamma) \cap (l')^{-1}(C) = \Psi((\mathcal{O}_K)^\times) \cap (l')^{-1}(C)$. Now, since $(l')^{-1}(C) \subseteq B$, $(l')^{-1}(C)$ lies inside a bounded region in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. Thus, it lies inside a ball of some radius.

In addition, since $\Psi(\mathcal{O}_K)$ is discrete, $\Psi(\mathcal{O}_K{}^\times) \cap (l')^{-1}(C) \subseteq \Psi(\mathcal{O}_K) \cap (l')^{-1}(C)$ is finite. Then, if we apply l' again, we conclude that $\Psi(\mathcal{O}_K{}^\times) \cap C = \Gamma \cap C$ is finite. □

By the above proposition, we see that Γ is discrete. Now, our aim is to show that Γ is a lattice. We start with the following proposition.

Proposition 3.19. *Assume that* Γ *is a lattice in* $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ *and for some* $b_1, \ldots, b_{r_1}, B_1, \ldots, B_{r_2} \in \mathbb{R}^{>0}$,

$$b_1 \ldots b_{r_1} (B_1, \ldots, B_{r_2})^2 > \left(\frac{4}{\pi}\right)^{r_2} vol(\Gamma)$$

is satisfied. Then, there exist an element $v = (v_1, \ldots, v_{r_1}, \tilde{v}_1, \ldots, \tilde{v}_{r_2}) \neq 0$ *in* Γ *such that* $|v_s| < b_s$ *for any* $1 \leq s \leq r_1$ *and* $|\tilde{v}_j| < B_j$ *for any* $1 \leq j \leq r_2$.

Proof. Let us define the subset C of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ such that for any

$$v = (v_1, \ldots, v_{r_1}, c_1 + id_1, \ldots, c_{r_2} + id_{r_2}) \in C,$$

$|v_s| < b_s$ for any $s = 1, \ldots, r_1$ and $|c_j + id_j|^2 < {B_j}^2$ for any $j = 1, \ldots, r_2$.

The set C is a cartesian product of r_1- many intervals of length $2b_s$ and r_2- many circles of radius B_j. Therefore,

$$vol(C) = (2b_1) \ldots (2b_{r_1})(\pi {B_1}^2) \ldots (\pi {B_{r_2}}^2) = 2^{r_1} \pi^{r_2} b_1 \ldots b_{r_1} (B_1 \ldots B_{r_2})^2.$$

Thus, by hypothesis, $vol(C) > 2^{r_1} \pi^{r_2} \left(\frac{4}{\pi}\right)^{r_2} vol(\Gamma) = 2^{r_1} 2^{2r_2} vol(\Gamma) = 2^n vol(\Gamma)$ since we have $r_1 + 2r_2 = n$.

Note that C is convex and symmetric with respect to 0. Now, by Corollary 3.7, *Minkowski's Convex Body Theorem*, this inequality gives us that there exists a non-zero element $v \in C$ such that $v \in \Gamma$. □

Proposition 3.20. *There exist a bounded region*

$$C_B \subseteq B = \{v \in (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times | N'(v) = \pm 1\}$$

such that

$$B = \bigcup_{\eta \in {\mathcal{O}_K}^\times} i(\eta) C_B.$$

Proof. Take any element $v \in B$. We know by Corollary 3.10 that the lattice $\Psi(\mathcal{O}_K)$ has volume $vol(\Psi(\mathcal{O}_K)) = 2^{-r_2} |\Delta|^{1/2}$. We can say that the lattice $v\Psi(\mathcal{O}_K)$ has volume

$2^{-r_2}|\Delta_K|^{1/2}$ too since, the determinant of the multiplication by v is $N'(v) = \pm 1$. Now, find $b_1, \ldots, b_{r_1}, B_1, \ldots, B_{r_2} \in \mathbb{R}^{>0}$ such that

$$b_1 \ldots b_{r_1}(B_1 \ldots B_{r_2})^2 > \left(\frac{2}{\pi}\right)^{r_2} |\Delta_K|^{1/2} = \left(\frac{4}{\pi}\right)^{r_2} 2^{-r_2}|\Delta_K|^{1/2} = \left(\frac{4}{\pi}\right)^{r_2} vol(\Psi(\mathcal{O}_K)).$$

Define $C = \{(x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \big| |x_i| < b_i, |z_j| < B_j\}$.

Then, by Proposition 3.19 above, there exists a non-zero element $x \in C$ such that $x \in v\Psi(\mathcal{O}_K)$.

Now, we can write $x = y\Psi(\gamma)$ for some $\gamma \in \mathcal{O}_K$. If we apply N' to the equality, we get $N'(x) = N'(v)N'(\Psi(\gamma)) = \pm N_{K/\mathbb{Q}}(\gamma)$. Thus, $N_{K/\mathbb{Q}}(\gamma)$ is bounded. Let us say that $|N_{K/\mathbb{Q}}(\gamma)| < m$. We know by Proposition 3.13 that there are finitely many integral ideals with a given norm. To add, note that $|N_{K/\mathbb{Q}}(\gamma)|$ is the norm of the principal ideal $\gamma\mathcal{O}_K$. Thus, up to units, we can say that there are finitely many elements with bounded norm.

Now, let $\{\gamma_1, \ldots, \gamma_s\}$ be the set of non-associate elements of norm at most m. Let us write $\gamma = \eta^{-1}\gamma_k$ for some unit η and $\gamma_k \in \{\gamma_1, \ldots, \gamma_s\}$. Thus, $x = y\Psi(\gamma)$ implies that $y = x\Psi(\gamma)^{-1} = x\Psi(\eta^{-1}\gamma_k)^{-1} = x\Psi(\gamma_k)^{-1}\Psi(\eta)$.

Next, let us define C_B as $\{c \in B | c \in \Psi(\gamma_k)^{-1}C \text{ for some } k\}$. It is known that C is bounded. Furthermore, C_B is the union of finitely many translates of C. Therefore, C_B is also bounded. Lastly, for any element $y \in B$, we have $y = x\Psi(\eta)$ for some $x \in C_B$ and $\eta \in \mathcal{O}_K$.

Thus,

$$B = \bigcup_{\eta \in \mathcal{O}_K{}^\times} i(\eta)C_B.$$

□

Corollary 3.21. Γ *is a lattice in* T.

Proof. Proposition 3.20 above says that there is a bounded region

$$C_B \subseteq B \subseteq (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times$$

such that

$$B = \bigcup_{\eta \in {\mathcal{O}_K}^\times} i(\eta) C_B.$$

Now, let us say that $C_H = l'(C_B)$. By definition of C, for any

$v = (x_1, \ldots, x_{r_1}, z_1, \ldots, z_{r_2}) \in C \subseteq B$, we have $N'(v) = \pm 1$. Also, each component x_i, z_j is bounded; since $N'(v) = \prod_{i=1}^{r_1} |x_i| \prod_{j=1}^{r_2} |z_j| = 1$. Therefore, $l'(C)$ is bounded in T.

Similarly, for every γ_k, the translate $l'(\Psi(\gamma_k)^{-1} C)$ is bounded in T.

Thus, $C_H = l'(C_B)$ is bounded in T.

Now, recall that we have

$$B = \bigcup_{\eta \in {\mathcal{O}_K}^\times} i(\eta) C_B.$$

Then,

$$l'(B) = T = \bigcup_{\eta \in {\mathcal{O}_K}^\times} (\varphi(\eta) + C_H).$$

On the other hand, we know that $\Gamma = \varphi({\mathcal{O}_K}^\times)$ so that we can write

$$T = \bigcup_{h \in \Gamma} (h + C_H).$$

Since C_H is bounded, we can say that the distance between 0 and any element of C_H is at most m. Therefore, there cannot be any element in $\{h + C_H : h \in \Gamma\}$ that has distance greater than m to any point of Γ. So, in the case that the span of Γ has strictly smaller dimension than T, we could find a point of T that is arbitrarily far from the span of Γ.

Thus, we conclude that Γ is a lattice. □

Now, we are ready to give the striking *Dirichlet's Unit Theorem.* Let us set $r = r_1 + r_2 - 1$.

Theorem 3.22 (Dirichlet's Unit Theorem)**.** *[2, Chapter 7, Theorem 7.31] Let K be a number field of degree n over $\mathbb{Q}$ where $n = r_1 + 2r_2$. Then,*

$$\mathcal{O}_K^\times \cong \mu(K) \times \mathbb{Z}^r.$$

In other words, there exist $\eta_1, \ldots, \eta_r \in {\mathcal{O}_K}^\times$ *such that any* $\eta \in {\mathcal{O}_K}^\times$ *can be written uniquely as*

$$\eta = \zeta \eta_1^{e_1} \ldots \eta_r^{e_r}$$

for some $\zeta \in \mu(K)$ *and* $e_i \in \mathbb{Z}$.

Proof. By Proposition 3.17, the kernel of φ is $\mu(K)$ and $\varphi({\mathcal{O}_K}^\times) = \Gamma \cong \mathbb{Z}^r$ by Corollary 3.21 since the dimension of T is $r_1 + r_2 - 1 = r$.

□

Lastly, we close this section with one last definition.

Definition 3.23. The units $\eta_1, \ldots, \eta_r \in {\mathcal{O}_K}^\times$ are called a set of fundamental units.

Chapter 4

THE ANALYTIC CLASS NUMBER FORMULA

In this chapter, we give the analytic class number formula which consists of important invariants of a ring of integers. Some statements will be given without proofs and the details can be found in [1],[2] and [5].

The Riemann zeta function $\zeta(s)$ is defined for any $s \in \mathbb{C}$ as

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

provided that $Re(s) > 1$. Now, let us define the Dedekind zeta function of a number field, which is a generalization of $\zeta(s)$.

Definition 4.1. Let K be a number field. Then, the Dedekind zeta function of K is defined as

$$\zeta_K(s) = \sum_{0 \neq I \subseteq \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(I)^s}$$

for $s \in \mathbb{C}$. Recall that we can factorize the ideals of $\mathcal{O}_K$ uniquely. The Dedekind zeta function is absolutely convergent for $s \in \mathbb{C}$ with $Re(s) > 1$ and it has the following Euler product :

$$\zeta_K(s) = \prod_{0 \neq \mathfrak{p} \subseteq \mathcal{O}_K, \text{ prime}} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}}.$$

Remark 4.2. If we take $K = \mathbb{Q}$, we have $N_{K/\mathbb{Q}}(I)^s = n^s$ since any ideal $0 \neq I \subseteq \mathbb{Z}$ is of the form $n\mathbb{Z}$ for some positive $n \in \mathbb{Z}$. Thus, $\zeta_{\mathbb{Q}}(s) = \zeta(s)$.

To add, let us take $K = \mathbb{Q}(i)$. We have $\mathcal{O}_K = \mathbb{Z}[i]$. It is known that $\mathcal{O}_K$ is a Euclidean domain, thus, a PID. Therefore, the integral ideals are of the form

$(a+bi)\mathcal{O}_K$ for some $a, b \in \mathbb{Z}$. Also, we have $N_{\mathbb{Q}(i)/\mathbb{Q}}((a+bi)\mathcal{O}_K) = a^2+b^2$. By *Dirichlet's Unit Theorem* we have that $\mathcal{O}_K \cong \mu(K) = \{\pm 1, \pm i\}$.

Notice that, for any $0 \neq I = (a+bi) \subseteq \mathcal{O}_K$ and $\epsilon \in {\mathcal{O}_K}^\times$ we have

$(a+bi)\mathcal{O}_K = \epsilon(a+bi)\mathcal{O}_K$. Thus, $(a+bi), (-a-bi), (-b+ai)$ and $(-a-bi)$ generate the same ideal. Therefore, we only consider the pairs $(a,b) \in \mathbb{Z}^{>0} \times \mathbb{Z}^{>0}$.

Thus,

$$\zeta_{\mathbb{Q}(i)}(s) = \sum_{0 \neq I \subseteq \mathbb{Z}[i]} \frac{1}{N_{K/\mathbb{Q}}(I)^s} = \sum_{(a,b) \in \mathbb{Z}^{>0} \times \mathbb{Z}^{>0}} \frac{1}{(a^2+b^2)^s}.$$

Given a number field K of degree n, recall that we have $n = r_1 + 2r_2$ many embeddings of K into $\mathbb{C}$ with real embeddings $\rho_1, \ldots, \rho_{r_1}$ and non-conjugate complex embeddings $\sigma_1, \ldots, \sigma_{r_2}$. By Dirichlet's Unit Theorem, we see that

$$\mathcal{O}_K{}^\times \cong \mu(K) \times \mathbb{Z}^r$$

where $r = r_1 + r_2 - 1$.

Recall that we have a commutative diagram:

$$\begin{array}{ccccc} K^\times & \xrightarrow{\Psi} & (\mathbb{R}^{r_1} \times \mathbb{C}^{r_2})^\times & \xrightarrow{l'} & \mathbb{R}^{r_1+r_2} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N'} & & \downarrow{\scriptstyle t} \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \xrightarrow[l]{} & \mathbb{R} \end{array}$$

So, ${\mathcal{O}_K}^\times$ is mapped into r-dimensional subspace T of $\mathbb{R}^{r_1+r_2}$ via φ. The image $\varphi(\mathcal{O}_K^\times)$ is a lattice Γ inside $T = \{w \in \mathbb{R}^{r_1+r_2} | t(w) = 0\} \subseteq \mathbb{R}^{r_1+r_2}$.

Finally, by Dirichlet's Unit Theorem, we can say that any element $\eta \in {\mathcal{O}_K}^\times$ can be written as $\zeta \eta_1^{e_1} \ldots \eta_r^{e_r}$ for some $\zeta \in \mu(K)$ and $e_1 \ldots, e_r \in \mathbb{Z}$ uniquely.

Thus, the vectors $\varphi(\eta_1), \ldots, \varphi(\eta_r)$ give a basis for the lattice Γ and they span T.

So, we have

$$\varphi : K \to \mathbb{R}^{r_1+r_2}$$

$$x \mapsto (\log(|\rho_1(x)|), \ldots, \log(|\rho_{r_1}(x)|), \log(|\tau_1(x)|^2), \ldots, \log(|\tau_{r_2}(x)|^2)).$$

For simplicity, say that $\varphi(x) = (\varphi_1(x), \ldots, \varphi_{r_1+r_2}(x))$. Define the matrix $A_{ij} = (\varphi_i(\eta_j))$ where $1 \leq i \leq r_1 + r_2$ and $1 \leq j \leq r_1 + r_2 - 1$ so that η_j's are the fundamental

units. Take any $(r_1+r_2-1)\times(r_1+r_2-1)$-minor of this matrix and take determinant. *Regulator of* K, R_K, is defined as the absolute value of the resulting determinant.

In this section, our goal is to prove the following theorem, the *Analytic Class Number Formula*:

Theorem 4.3 (Analytic Class Number Formula)**.** *[2, Chapter 10, Theorem 10.9]*

The Dedekind zeta function $\zeta_K(s)$ *converges for any* s *with* $Re(s) > 1$ *with a simple pole at* $s = 1$ *and*

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}R_K}{|\mu(K)|\sqrt{|\Delta_K|}}\ h_K$$

where h_K *is the class number of* K *and* R_K *is the regulator of* K*.*

To prove the theorem, we need some arguments from geometry. We begin by defining a *cone*.

Definition 4.4. Given a subset $X \subseteq \mathbb{R}^n$, if $x \in X$ and $c \in \mathbb{R}^{>0}$ implies that $cx \in X$, then it is called a cone.

A cone can be defined similarly in $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, namely, in any real vector space.

Now, let us start the proof of our main theorem with the following proposition:

Proposition 4.5. *[2, Chapter 10, Proposition 10.11] Let* $X \subseteq \mathbb{R}^n$ *be a cone. Assume that* $f : X \to \mathbb{R}^{>0}$ *is a function satisfying* $f(cx) = c^n f(x)$ *for any* $x \in X$ *and* $c \in \mathbb{R}^{>0}$*. Let the set* $U = \{x \in X | f(x) \leq 1\}$ *be bounded with volume* $\omega = vol(U)$ *such that* $\omega \neq 0$ *and let* Γ *be a lattice in* $\mathbb{R}^n$ *with volume* $\upsilon = vol(\Gamma)$*. Then,*

$$z(s) = \sum_{\Gamma\cap X} \frac{1}{f(x)^s}$$

converges for $Re(s) > 1$ *and we have* $\lim_{s\to 1}(s-1)z(s) = \dfrac{\omega}{\upsilon}$.

Proof. For any positive real number m, we can say that $vol(\frac{1}{m}\Gamma) = \frac{\upsilon}{r^n}$ since we work in an n-dimensional real vector space.

Now, define $G(m)$ to be $|\{x \in \frac{1}{m}\Gamma \cap U\}|$. Then,

$$\omega = vol(U) = \lim_{m\to\infty} G(m)\frac{\upsilon}{m^n} = \upsilon \lim_{m\to\infty} \frac{G(m)}{m^n}.$$

Furthermore, we can say that $G(m)$ is the number of elements in

$$\{x \in \Gamma \cap X | f(x) \leq m^n\}.$$

That is because these elements are the elements x' of $\frac{1}{m}X$ satisfying $f(x') \leq 1$.

Moreover, since Γ is a lattice and U is bounded, $G(m)$ is finite. Therefore, we can order the elements of $\Gamma \cap X$ as

$$0 < f(x_1) \leq f(x_2) \leq \dots$$

Now, set m_i to be $f(x_i)^{\frac{1}{n}}$. By our observation on the function $G(m)$, we have $G(m_i - m') < i \leq G(m_i)$ for any $m' \in \mathbb{R}^{>0}$. If we multiply the inequality by $\frac{1}{(m_i)^n}$, we get

$$\frac{G(m_i - m')}{(m_i - m')^n}\left(\frac{m_i - m'}{m_i}\right)^n < \frac{i}{{m_i}^n} \leq \frac{G(m_i)}{{m_i}^n}.$$

Note that if we take limit as m_i goes to ∞, then outer fractions go to $\dfrac{\omega}{\upsilon}$ by our limit calculation in the beginning. Therefore, taking limit as m_i goes to ∞ gives us

$$\lim_{m_i\to\infty} \frac{i}{{m_i}^n} = \lim_{i\to\infty} \frac{i}{f(x_i)} = \frac{vol(U)}{vol(\Gamma)} = \frac{\omega}{\upsilon}.$$

Thus, we can say that for any positive real number m, there exists i_m such that for any $i \geq i_m$ we have

$$\left(\frac{\omega}{\upsilon} - m\right)\frac{1}{i} < \frac{1}{f(x_i)} < \left(\frac{\omega}{\upsilon} + m\right)\frac{1}{i}.$$

Taking s^{th} power of the terms and summing over i starting from i_m gives us

$$\left(\frac{\omega}{\upsilon}-m\right)^s\sum_{i=i_m}^{\infty}\frac{1}{i^s}<\sum_{i=i_m}^{\infty}\frac{1}{f(x_i)^s}<\left(\frac{\omega}{\upsilon}+m\right)^s\sum_{i=i_m}^{\infty}\frac{1}{i^s}.$$

Now, let us make an observation on $\sum_{i=i_m}^{\infty}\frac{1}{i^s}$.

It can be seen that $\zeta(s)=\sum_{i=1}^{\infty}\frac{1}{i^s}=\sum_{i=1}^{i_m-1}\frac{1}{i^s}+\sum_{i=i_m}^{\infty}\frac{1}{i^s}$. So, for $Re(s)>1$, $\zeta(s)$ converges, its residue at $s=1$ is 1. Therefore,

$$\lim_{s\to1}(s-1)\zeta(s)=\lim_{s\to1}(s-1)\left(\sum_{i=i_m}^{\infty}\frac{1}{i^s}\right)=1.$$

Similarly, notice that $z(s)$ converges for any s with $Re(s)>1$.

Now, let us multiply the terms in the inequality with $(s-1)$ and take limit as s goes to 1:

$$\lim_{s\to1}(s-1)\left(\frac{\omega}{\upsilon}-m\right)^s\sum_{i=i_m}^{\infty}\frac{1}{i^s}<\lim_{s\to1}(s-1)\sum_{i=i_m}^{\infty}\frac{1}{f(x_i)^s}<\lim_{s\to1}(s-1)\left(\frac{\omega}{\upsilon}+m\right)^s\sum_{i=i_m}^{\infty}\frac{1}{i^s}$$

which yields

$$\frac{\omega}{\upsilon}-m\le\lim_{s\to1}(s-1)z(s)\le\frac{\omega}{\upsilon}-m$$

by our observation above.

Thus, since $m>0$ is arbitrary, we conclude that

$$\lim_{s\to1}(s-1)z(s)=\frac{\omega}{\upsilon}\ .$$

□

This theorem is a crucial part of proving the *Analytic Class Number Formula*. We will construct a cone X and a lattice Γ. Then, by taking $|N'|$ as f, we will be able to use this proposition.

Now, let us work on the Dedekind zeta function of K. For each class $C \in Cl(K)$ define the following function:

$$z_C(s) = \sum_{I \in C} \frac{1}{N_{K/\mathbb{Q}}(I)^s} \ .$$

Then, we can write $\zeta_K(s)$ as:

$$\zeta_K(s) = \sum_{C \in Cl(K)} z_C(s).$$

We will re-write z_C in a different way by manipulating the sum. So, let us make some observations.

In the previous chapter, it is mentioned that $Cl(K)$ is a finite group of order h_K. Therefore, the class C has its inverse C^{-1} inside $Cl(K)$ such that $CC^{-1} = P_K$. Take any integral ideal $J \in C^{-1}$. Then, for any $I \in C$, IJ is principal, call it $< \alpha >$ for some $\alpha \in \mathcal{O}_K$. Taking norm on the both sides yields

$$N_{K/\mathbb{Q}}(IJ) = N_{K/\mathbb{Q}}(< \alpha >) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Since the norm is multiplicative, we get $N_{K/\mathbb{Q}}(I)N_{K/\mathbb{Q}}(J) = |N_{K/\mathbb{Q}}(\alpha)|$. Also, since $IJ =< \alpha >$ we can say that J divides $< \alpha >$.

Therefore, we can write the sum running over the elements α as:

$$z_C(s) = \sum_{J|<\alpha>} \frac{N_{K/\mathbb{Q}}(J)^s}{|N_{K/\mathbb{Q}}(\alpha)|^s} = N_{K/\mathbb{Q}}(J)^s \sum_{J|<\alpha>} \frac{1}{|N_{K/\mathbb{Q}}(\alpha)|^s}.$$

Moreover, J divides $< \alpha >$ which means that $< \alpha > \subseteq J$. Thus, $\alpha \in J$.

Note that if α and $\tilde{\alpha}$ are associates then $< \alpha >=< \tilde{\alpha} >$. Therefore, we consider only non-associate elements α. So, we can say that the elements α runs over the non-associate elements of J. Let us say that these elements belong to the subset $J^* \subseteq J$.

We will manipulate the sum once more, so, let us define the following lattice:

$$\Gamma = \Psi(J) = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} | x = \Psi(\alpha) \text{ for some } \alpha \in J\}$$

and the subset Ω of $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ as

$$\Omega = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} | x = \Psi(\alpha) \text{ for some } \alpha \in J^*\}.$$

Finally, recall that we have $N_{K/\mathbb{Q}} = N'(\Psi)$. Since we count the non-associate members α of J and by the equality above, our sum can be re-written as:

$$z_C(s) = N_{K/\mathbb{Q}}(J)^s \sum_{x \in \Omega} \frac{1}{|N'(x)|^s}.$$

Our next step is to define a particular cone $X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$. X will contain elements x such that $x = \Psi(\alpha)$ for some α and $x \neq \Psi(\alpha')$ for any associate α' of α. In conclusion, we write Ω as $\Gamma \cap X$ and writing $|N'(x)|$ instead of $f(x)$ will make Proposition 4.5 a crucial tool.

Now, recall that the vectors $\varphi(\eta_1), \ldots, \varphi(\eta_r)$ span $T \subseteq \mathbb{R}^{r_1+r_2}$ where $\eta_1, \ldots, \eta_r$ are fundamental units. Our aim is to span $\mathbb{R}^{r_1+r_2}$ so we need one additional linearly independent vector. For this reason, let us define a vector

$$\hat{\varphi} = (\hat{\varphi}_1, \ldots, \hat{\varphi}_{r_1}, \hat{\varphi}_{r_1+1}, \ldots, \hat{\varphi}_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2}$$

such that for every $i = 1, \ldots, r_1$ we have $\hat{\varphi}_i = 1$ and for every $j = r_1 + 1, \ldots, r_1 + r_2$ we have $\hat{\varphi}_j = 2$. So $\hat{\varphi}$ is of the form $(1, \ldots, 1, 2, \ldots, 2)$ where each of the r_1-many real components is equal to 1 and each of the r_2-many complex components is equal to 2.

Then, we can say that the vectors $\hat{\varphi}, \varphi(\eta_1), \ldots, \varphi(\eta_r)$ give a basis for $\mathbb{R}^{r_1+r_2}$. Therefore, for any $l'(x) \in \mathbb{R}^{r_1+r_2}$ we can write

$$l'(x) = \hat{c}\hat{\varphi} + c_1\varphi(\eta_1) + \cdots + c_r\varphi(\eta_r)$$

for some $\hat{c}, c_1, \ldots, c_r \in \mathbb{R}$.

Recall that the set T is given as $\{w \in \mathbb{R}^{r_1+r_2} | t(w) = 0\}$ where the function t is given as

$$t : \mathbb{R}^{r_1+r_2} \to \mathbb{R}$$

$$(y_1, \ldots, y_{r_1+r_2}) \mapsto y_1 + \cdots + y_{r_1+r_2}.$$

Notice also that for any fundamental unit η_j, we have $\varphi(\eta_j) \in T$ and $t(\varphi(\eta_j)) = \log 1 = 0$.

Therefore,

$$t(l'(x)) = \hat{c}t(\hat{\varphi}) + c_1 t(\varphi(\eta_1)) + \cdots + c_r t(\varphi(\eta_r)) = \hat{c}t(\hat{\varphi}).$$

Thus, $t(l'(x)) = \hat{c}(1 + \cdots + 1 + 2 \cdots + 2) = \hat{c}n$. Lastly, notice that

$$t(l'(x)) = \log |N'(x)|$$

so $\hat{c} = \frac{1}{n} \log |N'(x)|$. We are ready to define the desired cone.

Let $X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ be the set of elements x satisfying the following properties:

1. $N'(x) \neq 0$.

2. for any coefficient c_i of $l'(x)$ we have $0 \leq c_i < 1$ for each $i = 1, \ldots, r$.

3. If x_1 is the first component of x, we have $0 \leq arg(x_1) < \dfrac{2\pi}{|\mu(K)|}$.

We claim that the set X is a cone. Let us show that.

For any $c \in \mathbb{R} > 0$, $N'(cx) = c^n N'(x) \neq 0$. Also, $l'(cx) = (\log c)\hat{\varphi} + l'(x)$ and since $l'(x) = \hat{c}\hat{\varphi} + c_1\varphi(\eta_1) + \cdots + c_r\varphi(\eta_r)$, the coefficients $\varphi(\eta_j)$ do not change and satisfy the condition.

To add, $arg(cx_1) = arg(x_1)$ since *streching* the vector does not affect the argument.

Therefore, for any $x \in X$ and $c \in \mathbb{R}^{>0}$, $cx \in X$. Thus, we conclude that

$$X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$$

is a cone.

Lemma 4.6. *If $y \in \mathbb{R}^n$ and $N'(y) \neq 0$, then y can be written uniquely as $x \cdot \Psi(\eta)$ for some $x \in X \subseteq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ and $\eta \in {\mathcal{O}_K}^{\times}$.*

Proof. Let us write $l'(y)$ as $\hat{d}\hat{\varphi} + d_1\varphi(\eta_1) + \cdots + d_r\varphi(\eta_r)$ for some $\hat{d}, d_1, \ldots, d_r \in \mathbb{R}$. For any $j = 1, \ldots, r$, we can write $d_j = m_j + f_j$ where $m_j \in \mathbb{Z}$ and $f_j \in [0, 1)$, the fractional part of d_j. Now, let us write a unit u as $u = \eta_1^{m_1} \ldots \eta_r^{m_r}$ and set $z = y \cdot \Psi(u^{-1})$.

Assume that the argument of the first component of z, $arg(z_1) = \theta$. Then, we can find an integer $\bar{m}$ such that

$$0 \leq \theta - \frac{2\pi\bar{m}}{|\mu(K)|} < \frac{2\pi}{|\mu(K)|}.$$

Next, take $\zeta \in \mu(K)$ such that the first component of the image of ζ under the map $\Psi : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{\times}$ is $\Psi_1(\zeta) = e^{\frac{2\pi i}{|\mu(K)|}}$.

Now, set $x = y \cdot \Psi(u^{-1}) \cdot \Psi(\zeta^{\bar{m}})$. We will show that $x \in X$.

By assumption $N'(y) \neq 0$ and we have $y \cdot \Psi(u^{-1}) \cdot \Psi(\zeta^{\bar{m}}) = N'(x) \neq 0$.

The coefficients f_j $(j = 1, \ldots, r)$ of x satisfy $0 \leq f_j < 1$ by our construction. Finally, argument $arg(x_1)$ of the first component of x lies inside $[0, \frac{2\pi}{|\mu(K)|})$ by our choice of ζ. Thus, x lies in the cone X.

The equality $x = y \cdot \Psi(u^{-1}) \cdot \Psi(\zeta^{\bar{m}})$ implies that $y = \Psi(\eta)$ for some unit $\eta \in \mathcal{O}_K$. In addition, the decomposition of y is unique by the construction. □

So, we prove that if $\alpha \in \mathcal{O}_K$ then there is a unique element $\tilde{\alpha}$ of $\{\tilde{\alpha} \in \mathcal{O}_K | \tilde{\alpha}$ is associate to $\alpha\}$ such that $\Psi(\tilde{\alpha}) \in X$.

Recall that we have the lattice

$$\Gamma = \Psi(J) = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} | x = \Psi(\alpha) \text{ for some } \alpha \in J\}$$

and J^* is defined as the non-associate member of J so that we also have

$$\Omega = \{x \in \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} | x = \Psi(\alpha) \text{ for some } \alpha \in J^*\}.$$

Thus, we can write Ω as $\Gamma \cap X$.

Then,

$$z_C(s) = N_{K/\mathbb{Q}}(J)^s \sum_{x \in \Omega} \frac{1}{|N'(x)|^s}$$

can be written as

$$z_C(s) = N_{K/\mathbb{Q}}(J)^s \sum_{x \in \Gamma \cap X} \frac{1}{|N'(x)|^s}.$$

Now, to evaluate this sum via Proposition 4.5 we have to find $vol(U) = \omega$ and $vol(\Gamma) = \upsilon$ where $U = \{x \in X \big| |N'(x)| \leq 1\}$.

By Corollary 3.10, the volume of the lattice $\Gamma = \Psi(J)$ is $2^{-r_2}|\Delta_K|^{\frac{1}{2}} N_{K/\mathbb{Q}}(J)$.

Therefore, we only need the volume of U.

Proposition 4.7. *The volume of ω of U is* $\dfrac{2^{r_1}\pi^{r_2}R_K}{|\mu(K)|}$.

Proof. See, [2, Chapter 10, Proposition 10.14] □

Let us put everything together:

$$\lim_{s\to 1}(s-1)z_C(s) = N_{K/\mathbb{Q}}(J)\frac{\omega}{\upsilon} = N_{K/\mathbb{Q}}(J)\frac{2^{r_1}\pi^{r_2}R_K}{|\mu(K)|}\frac{1}{2^{-r_2}|\Delta_K|^{\frac{1}{2}}N_{K/\mathbb{Q}}(J)}$$
$$= \frac{2^{r_1+r_2}\pi^{r_2}R_K}{|\mu(K)|\sqrt{|\Delta_K|}}.$$

Note that the sum is independent from the class C.

Recall that we write $\zeta_K(s)$ as $\displaystyle\sum_{C\in Cl(K)} z_C(s)$ and there are only finitely many ideal classes. The number of these classes is the class number h_K of K, thus:

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1+r_2}\pi^{r_2}R_K}{|\mu(K)|\sqrt{|\Delta_K|}}\ h_K.$$

Chapter 5

APPLICATIONS

In this chapter, we briefly cover various concepts in order to compute the class number of a number field. We mainly focus on the *quadratic number fields*, number fields of degree 2 over $\mathbb{Q}$. A quadratic number field K is given by $K = \mathbb{Q}(\sqrt{d})$ for some square-free integer d.

Let us state some results on quadratic number fields first.

Remark 5.1. Let $K = \mathbb{Q}[\sqrt{d}]$ be a quadratic number field. Then, we have the following:

1. $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and $\Delta_K = 4d$, if $d \equiv 2, 3 \pmod 4$.

2. $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and $\Delta_K = d$ if $d \equiv 1 \pmod 4$.

Now take any prime number p. The ideal $p\mathcal{O}_K$ is an ideal of $\mathcal{O}_K$ generated by p, so it can be written as a product of prime ideals. We have 3 cases:

1. p *splits* in K if $p\mathcal{O}_K = P'Q'$ for some distinct prime ideals P', Q' of norm p.

2. p is inert in K if $p\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ of norm p^2.

3. p is ramifed in K if $p\mathcal{O}_K = P^2$ for some prime ideal P of $\mathcal{O}_K$ of norm p.

Now, let us begin with *Binary Quadratic Forms*.

5.1 Binary Quadratic Forms

Definition 5.2. A binary quadratic form is a homogeneous polynomial of degree 2 and of the form $p(x, y) = ax^2 + bxy + cy^2$ for some integers a, b and c.

The *discriminant* of the binary quadratic form $ax^2+bxy+cy^2$ is defined as b^2-4ac.

We will write (a, b, c) for the binary quadratic form $ax^2 + bxy + cy^2$ in short.

Definition 5.3. A quadratic form $p(x, y)$ is called *positive definite* if for any $x, y \in \mathbb{R}$, we have $f(x, y) \geq 0$ and $f(x, y) = 0$ implies that $(x, y) = 0$.

Now, let us we have a quadratic form (a, b, c). We look for the conditions that is needed to have a positive definite form.

$$ax^2 + bxy + cy^2 = a\left(x + \frac{b}{2a}y\right)^2 + \left(c - \frac{b^2}{4a}\right)y^2.$$

First of all, a must be greater than 0, in order to say that (a, b, c) is positive definite because taking $(x, y) = (1, 0)$ gives a negative value. The same is valid for c by symmetry. To add, if we look at the equation above, $(c - \frac{b^2}{4a})$ must be positive to have a positive definite form. Equivalently, we must have $b^2 - 4ac < 0$. Thus, we have the following corollary:

Corollary 5.4. *[2, Chapter 6, Corollary 6.10] The quadratic form (a, b, c) is positive definite if and only if $a > 0$ and $b^2 - 4ac < 0$.*

Remark 5.5. Let K be an imaginary quadratic number field. So, $K = \mathbb{Q}(\sqrt{d})$ for some negative square-free integer d. Then, the norm $N_{K/\mathbb{Q}}(x + y\sqrt{d})$ of any element $x + y\sqrt{d}$ is a positive definite quadratic form: $x^2 + (-d)y^2$.

Now, we make an observation and after that, we define an equivalence relation on the set of quadratic forms.

Let v be the vector $(x, y)^T$ and say $A = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$. Then, the form

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

can be written as $p(x, y) = v^T Av$.

Definition 5.6. The quadratic forms $p(x, y)$ and $q(x, y)$ are said to be equivalent if $q(x, y) = p(m_{11}x + m_{12}y, m_{21}x + m_{22}y)$ for some invertible matrix $M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}$ in $GL_2(\mathbb{Z})$.

Equivalently, since M is invertible, $\det(M) = \pm 1$ so that $p(x, y)$ and $q(x, y)$ are equivalent if the substitution $(x, y) \mapsto (m_{11}x + m_{12}y, m_{21}x + m_{22}y)$ transforms one to another for some $m_{11}, m_{12}, m_{21}, m_{22} \in \mathbb{Z}$ with $m_{11}m_{22} - m_{12}m_{21} = \pm 1$.

They are called properly equivalent if $m_{11}m_{22} - m_{12}m_{21} = 1$ which is the case that when $M \in SL_2(\mathbb{Z})$.

Let us take a form $p(x, y)$ as $v^T Av$ as above.

Notice that

$$Mv = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} m_{11}x + m_{12}y \\ m_{21}x + m_{22}y \end{pmatrix}$$

.

Thus, we can write $p(m_{11}x+m_{12}y, m_{21}x+m_{22}y) = (Mv)^T A(Mv) = v^T(M^T AM)v$.

Now, let us say that the form $q(x, y)$ corresponds to a matrix B. Then, it can be said that p and q are equivalent if $B = M^T AM$ for some $M \in GL_2(\mathbb{Z})$ and properly equivalent if $M \in SL_2(\mathbb{Z})$.

In some cases, writing a form in terms of matrices *makes things easier* and help one to come up with various conclusions. For instance, one can prove the following theorem:

Theorem 5.7. $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ *generate* $SL_2(\mathbb{Z})$ *(For the proof, see [2, Chapter 6, Corollary 6.18]).*

Now, let us give a remark and continue with *reduced* quadratic forms.

Remark 5.8. Equivalent forms have the same discriminant.

Both equivalences give an equivalence relation on the quadratic forms. In fact, on the set of binary quadratic forms of fixed discriminant, we have these equivalence relations.

Definition 5.9. The binary quadratic form (a, b, c) is called reduced if either

$$-a < b \leq c \text{ or } 0 \leq b \leq a = c.$$

Now, let us take a positive-definite form $p(x, y) = (a, b, c)$ and define the following transformations:

1. $T_1 : (x, y) \mapsto (x + y, y)$ which gives $(a, b, c) \mapsto (a, 2a + b, a + b + c)$.

2. $T_2 : (x, y) \mapsto (x, y - x)$ which gives $(a, b, c) \mapsto (a, b - 2a, a - b + c)$.

3. $T_3 : (x, y) \mapsto (y, -x)$ which gives $(a, b, c) \mapsto (c, -b, a)$.

The transformations T_1, T_2, T_3 generate properly equivalent forms. If we start with a positive definite quadratic form and apply the algorithm in [2, Chapter 6.4] we get a reduced form after finitely many steps and they are properly equivalent. We actually have more than that:

Theorem 5.10. *[2, Chapter 6, Theorem 6.14] Assume that $p(x, y)$ is a positive definite binary quadratic form. Then, there exist a unique reduced form $r(x, y)$ such that $p(x, y)$ is properly equivalent to $r(x, y)$.*

Now, recall that if $K = \mathbb{Q}(\sqrt{d})$ for some square-free $d \in \mathbb{Z}^{<0}$ with discriminant Δ_K. Then, we have

$$\Delta_K = \begin{cases} d & \text{if } d \equiv 1 \pmod 4 \\ 4d & \text{if } d \equiv 2, 3 \pmod 4 \end{cases}$$

Also, we mentioned that *discriminant* of a form can be defined too. Let us say that (a, b, c) is a quadratic form with discriminant $\tilde{d}$. So, we focus on the forms (a, b, c) with discriminant $\tilde{d} = \Delta_K$ that is negative.

Moreover, we define bijective functions between the set proper equivalence classes of quadratic forms of discriminant $\tilde{d} = \Delta_K$ and the set of ideal classes in $\mathcal{O}_K$. Briefly, for any representative (a, b, c) we send it to an ideal class such that the ideal representing the class has $\mathbb{Z}$-basis α, β consisting of a, b and c. Conversely, for any ideal $I \subseteq \mathcal{O}_K$ we can find two generators such that I is of the form $a\mathbb{Z} + (b + c\gamma)\mathbb{Z}$ for some $\gamma \in K$. Thus, we can send I to a form (a, b, c). It is important to mention that either case, the maps are well-defined (For details, see [2, Chapter 6.5]).

Proposition 5.11. *The number of reduced quadratic forms with fixed discriminant is finite.*

Proof. Let (a, b, c) be a reduced form with discriminant $\tilde{d}$ so we have $0 \leq |b| \leq a \leq c$. Thus, $0 \leq b^2 \leq ac$ and this implies that $-4ac \leq b^2 - 4ac \leq ac - 4ac = -3ac$. Therefore, $-4ac \leq \tilde{d} \leq -3ac$ and we can bound ac as

$$\frac{-\tilde{d}}{4} \leq ac \leq \frac{-\tilde{d}}{3}.$$

Since (a, b, c) is reduced, $0 \leq a \leq c$ so that $a^2 \leq ac$. Thus,

$$a^2 \leq ac \leq \frac{-\tilde{d}}{3}.$$

Therefore, a is bounded and since $|b| \leq a$, b is bounded too. There are finitely many choices for a and b. Thus, together with the equality $b^2 - 4ac = \tilde{d}$, we can say that there are finitely many choices for c. □

We see that the collection of positive definite binary quadratic forms with fixed discriminant is finite, thus, we prove that the ideal class group of an imaginary quadratic field is finite. Moreover, we can evaluate the class number of an imaginary quadratic field by counting the related reduced forms.

Now, we give the main theorem of this section:

Theorem 5.12. *[2, Chapter 6, Theorem 6.19]*

Assume that the number of reduced quadratic forms with discriminant Δ_K is p_K. Then, the class number h_K of an imaginary quadratic field $\mathbb{Q}(\sqrt{d})$ is equal to p_K .

We will finish this section with the following example:

Example 5.13. Let $K = \mathbb{Q}(-\sqrt{13})$, so $\Delta_K = -52$. We look for reduced forms (a, b, c) of discriminant $b^2 - 4ac = -52$. We mentioned in the proof of Proposition 5.11 that $\frac{52}{4} \leq ac \leq \frac{52}{3}$, equivalently, $13 \leq ac \leq 17$ must be satisfied.

Now, if $ac = 13$ and $b = 0$, then we must have $(1, 0, 13)$ since $0 \leq a \leq c$.

If $ac = 14$, then $b = \pm 2$ and we have four possibilites in this case:

1. (1,2,14): it is not reduced since $|b| > a$.

2. (1,-2,14): again it is not reduced since $|b| > a$.

3. (2,2,7): It is reduced.

4. (2,-2,7): It is not reduced since $b = -a$.

Now, if $ac = 15$, then $b^2 = 8$ and if $ac = 16$, then $b^2 = 12$ so we can not find such b.

Lastly, if $ac = 17$, then $b = \pm 4$ but we can not find such a, c to satisfy

$$4 = |b| \leq a \leq c.$$

Therefore, the only reduced forms of discriminant -52 are $(1, 0, 13)$ and $(2, 2, 7)$. Thus, the class number h_K of K is 2. So, it is not a UFD.

5.2 Continued Fractions

In the previous subsection, we worked on the imaginary quadratic fields and presented a way to find their class numbers. Now, we work on real quadratic fields. The most significant difference between these two quadratic number fields is that real ones have infinitely many units. To find their units, we must find the fundamental unit η of the real quadratic field since the units are of the form $\pm\eta^n$ for some $n \in \mathbb{Z}$ by *Dirichlet's Unit Theorem.*

Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field. For instance, let us assume that $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$ and take any unit $a + b\sqrt{d} \in {\mathcal{O}_K}^{\times}$. Then,

$$N_{K/\mathbb{Q}}(a + b\sqrt{d}) = a^2 - db^2 = \pm 1$$

so that the units are the solutions of a *Pell's equation*, $x^2 - dy^2 = \pm 1$. It is known that when $d \in \mathbb{Z}^{>0}$ and is square-free, the equation has infinitely many solutions and the general solution gives us the fundamental unit of the real quadratic field.

Now, observe that we can write $\sqrt{2}$ as:

$$\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + \frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2+\dots}}}.$$

The expression on the right hand side is called the *continued fraction* for $\sqrt{2}$. We use $[1; 2, 2, \dots] = [1; \overline{2}]$ for the expression in short.

Now, let $d \in \mathbb{Z}^{>0}$ be a square-free integer. We will give some facts without proofs.

Proposition 5.14. *The continued fraction for $\sqrt{d}$ is given as $[b_0; \overline{b_1 \dots b_k}]$ for some positive integers $b_0, \dots, b_k$ so that $b_k = 2b_0$.*

Now, let us say that we can write $\gamma = b_0 + \frac{1}{b_1 + \frac{1}{b_2 + \frac{1}{\dots}}} = b_0 + \frac{1}{\gamma_0} = b_0 + \frac{1}{b_1 + \frac{1}{\gamma_2}} = \dots$ such that there exists $k \in \mathbb{Z}^{>0}$ where $\gamma_j = \gamma_{j+k}$ for some j. The smallest possible k is called the period of $\sqrt{d}$.

Now, let us fix some notation.

Define $p_{-2} = 0, q_{-2} = 1, p_{-1} = 1, q_{-1} = 0, p_0 = \lfloor \gamma \rfloor$ and $q_0 = 1$. If $\gamma = [b_0; b_1 b_2 \dots]$, then $p_k = a_k p_{k-1} + p_{k-2}$ and $q_k = a_k q_{k-1} + q_{k-2}$. Set $A_0 = 0, C_0 = 1$, $\gamma_0 = \sqrt{d}$ and $b_0 = \lfloor \gamma_0 \rfloor$. Also, define $A_{n+1} = b_n C_n - A_n$, $C_{n+1} = \frac{d - {C_{n+1}}^2}{A_n}$, $\gamma_{n+1} = \frac{\sqrt{d} + C_{n+1}}{A_{n+1}}$ and $b_{n+1} = \lfloor \gamma_{n+1} \rfloor$. Then, $A_n, C_n \in \mathbb{Z}$ for any n and $\gamma_n = b_n + \frac{1}{\gamma_{n+1}}$, thus $\gamma = [b_0; b_1, b_2, \dots]$.

Lastly, we have that ${p_n}^2 - d{q_n}^2 = (-1)^{n+1} A_{n+1}$. (For the proofs, see [2, Chapter 8.2].)

The fraction $\frac{p_n}{q_n}$ is called n^{th} convergent to γ.

Now, we can give some results on solving *Pell's equation*.

Theorem 5.15. *Suppose that $d \in \mathbb{Z}^{>0}$ is square-free. Then, $x^2 - dy^2 = 1$ has infinitely many solutions and $x^2 - dy^2 = -1$ has infinitely many solutions if the period of $\sqrt{d}$ is odd.*

Proof. We have ${p_n}^2 - d{q_n}^2 = (-1)^{n+1} A_{n+1}$. The sequence (γ_n) repeats with some period k, therefore (A_n) repeats with the same period. We have $N_0 = 1$ so that $N_{ik} = 1$ for any $i \in \mathbb{Z}^{\geq 0}$. Then, for any $n = ik - 1$ where i or k even (p_n, q_n) solves $x^2 - dy^2 = 1$. Therefore, Pell's equation has infinitely many solutions. If k is odd and $n = ik - 1$ with i odd, (p_n, q_n) is a solution for $x^2 - dy^2 = -1$. □

Theorem 5.16. *Suppose that $d \in \mathbb{Z}^{>0}$ is square-free and say n^{th} convergent to $\sqrt{d}$ is $\frac{p_n}{q_n}$. Suppose also that $m \in \mathbb{Z}$ with $|m| < \sqrt{d}$. Then, for any solution (u, v) of $x^2 - dy^2 = m$ with $(u, v) = 1$ we have $s = p_n$ and $t = q_n$ for some n.*

To sum up, we can find the units $u + v\sqrt{d}$ with the convergents to $\sqrt{d}$. So, we look for convergents $\frac{p_n}{q_n}$ with ${p_n}^2 - d{q_n}^2 = \pm 1$. We see in the proof of Theorem 5.15 that the values of ${p_n}^2 - d{q_n}^2$ repeats with period k of $\sqrt{d}$.

So, if $d \equiv 2, 3 \pmod 4$, then the first pair (p_n, q_n) that satisfies ${p_n}^2 - d{q_n}^2 = \pm 1$ gives the fundamental unit of K, $p_n + q_n\sqrt{d}$. However, if $d \equiv 1 \pmod 4$ then we seek for $a + b\sqrt{d} = \pm 1$ for some $a, b \in \frac{1}{2}\mathbb{Z}$. Thus, we need to solve $(2a)^2 - d(2b)^2 = \pm 4$ and it has a solution by Theorem 5.16. So, in this case, the first pair of (p_n, q_n) satisfying ± 1 or ± 4 gives the fundamental unit of K.

5.3 Class Number Calculations via Minkowski's Bound

In this section, we introduce a method to find the class number of any number field. We will give an example on real quadratic fields since we presented a method for imaginary quadratic fields. Now, we give the main theorem of this section:

Theorem 5.17. *Let K be a number field of degree n and $c \in R$ be a constant such that every ideal class contains an ideal I with $N_{K/\mathbb{Q}}(I) \leq \upsilon$. Let $\{P_1, \ldots, P_m\}$ be the set of prime ideals of $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(P_i) \leq \upsilon$ for any $i = 1, \ldots, m$ and say that $C_i = [P_i]$ is the class of P_i in $Cl(K)$. Then, $\{C_1, \ldots, C_m\}$ generates $Cl(K)$. In addition, $h_K \leq \sum_{i=2}^{\lfloor \upsilon \rfloor} n^{\frac{\log i}{\log 2}}$.*

Proof. By Proposition 3.13, we can say that there are finitely many prime ideals P with $N_{K/\mathbb{Q}}(P) \leq \upsilon$. Let us say that they are $\{P_1, \ldots, P_m\}$. Now take any $C \in Cl(K)$ and an ideal $I \in C$ with $N_{K/\mathbb{Q}}(I) \leq \upsilon$. Let ${Q_1}^{e_1} \ldots {Q_l}^{e_l}$ be the decompositon of I for some prime ideals $Q_1, \ldots, Q_l$. Then, $\prod_{i=1}^{l} N_{K/\mathbb{Q}}(Q_i)^{e_i} \leq \upsilon$ implies that $N_{K/\mathbb{Q}}(Q_i) \leq \upsilon$ for any $i = 1, \ldots, l$. Thus, $\{Q_1, \ldots, Q_l\} \subseteq \{P_1, \ldots, P_m\}$ and $Cl(K)$ is generated by $C_1, \ldots, C_m$.

For the last part, see [3, Chapter 4, Corollary 4.2] □

We can take υ as Minkowski's bound $\left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}|\Delta_K|^{\frac{1}{2}}$ given in Corollary 3.12 since it satisfies the condition of the theorem.

Now, let us see an example:

Example 5.18. Let $K = \mathbb{Q}(\sqrt{82})$. Then, we have $n = 2, r_1 = 2, r_2 = 0, \Delta_K = 328$ and Minkowski's bound $M \approx 9.05$. Lastly, $\mathcal{O}_K = \mathbb{Z}[\sqrt{82}]$.

Prime ideals have norm p^m for some prime number p with $m \in \mathbb{N}$ and their norm must be less than M so we consider the primes less than M. Thus, we consider the factors of $p\mathcal{O}$ to find the prime ideals we are looking for.

By [2, Chapter 5.8, Proposition 5.42], $2\mathcal{O}_K = P_2^2, 3\mathcal{O}_K = P_3\tilde{P}_3$ and $5, 7$ are inert so we consider the prime ideals P_2, P_3 and $\tilde{P}_3$ only.

Note that $2\mathcal{O}_K = P_2^2 \sim (1)$ and since $3\mathcal{O}_K = P_3\tilde{P}_3 \sim (1)$, we can say that $Cl(K)$ is generated by P_2 and P_3.

Now let $\beta = 10 + \sqrt{82}$. We have $N_{K/\mathbb{Q}}(\beta\mathcal{O}_K) = 18$ so $\beta\mathcal{O}_K$ has a prime factor with norm 3. Since $3 \not| 10 + \sqrt{82}$, $\beta \notin 3\mathcal{O}_K = P_3\tilde{P}_3$, $\beta\mathcal{O}_K$ is divisible by one of P_3 and $\tilde{P}_3$. Let P_3 divides the ideal so we have $\beta\mathcal{O}_K = P_2{P_3}^2$, a principal ideal. Therefore, $P_2 \sim P_3^{-2}$ and we conclude that $Cl(K)$ is generated by the class of P_3. Now, we have $[P_2]^2 = 1$ and $[P_3]^2 = [P_2]$ therefore the order of $[P_3]$ divides 4. Let us show that P_2 is not principal.

Suppose that $P_2^2 = (\alpha)^2$ for some $\alpha = (a + b\sqrt{82}) \in \mathbb{Z}[\sqrt{82}]$.

Thus, $2\mathcal{O} =< (a + b\sqrt{82})^2 >$. Then, $2 = ((a + b\sqrt{82})^2)u$ for some $u \in {\mathcal{O}_K}^\times$. By Dirichlet's Unit Theorem (Theorem 3.22), $u = \pm\eta^n$ for some $n \in \mathbb{Z}$ where η is the fundamental unit of K. Let us find the fundamental unit by considering the continued fraction of $\sqrt{82}$. It is given as $[9; \overline{18}]$. By the method we introduced in the previous section we conclude that $\eta = 9 + \sqrt{82}$. Thus, $u = \pm(9 + \sqrt{82})^n$ for some $n \in \mathbb{Z}$. Then, $2 = (a + b\sqrt{82})^2 u = \pm(a + b\sqrt{82})^2(9 + \sqrt{82})^n$ implies that u must be positive. By taking the norm of both sides we conclude that $n = 2k$ for some $k \in \mathbb{Z}$. Finally, we have

$$2 = (a + b\sqrt{82})^2(9 + \sqrt{82})^{2k}.$$

Then, $\sqrt{2} = (a + b\sqrt{82})(9 + \sqrt{82})^k = a' + b'\sqrt{82}$ for some $a', b' \in \mathbb{Z}[\sqrt{82}]$ but this implies that $\sqrt{2} \in \mathbb{Z}[\sqrt{82}]$ which is a contradiction.

Thus, P_2 is not principal, so $[P_3]$ has order 4 and $Cl(K)$ is generated by $[P_3]$. Therefore, $Cl(K) \cong \mathbb{Z}/4\mathbb{Z}$ and $h_K = 4$.

5.4 Explicit Class Number Formula

A *Dirichlet character modulo n* is a group homomorphism

$$\chi : (\mathbb{Z}/n\mathbb{Z})^\times \to \mathbb{C} - \{0\}.$$

It can be extended to $\mathbb{Z}/n\mathbb{Z}$ by setting $\chi(a) = 0$ for any a with $(a, n) > 1$. We call χ as principal if it is the trivial homomorphism and non-principal otherwise. A character is primitive (mod k) if for any divisor $a < k$ of k, there exists $b \in \mathbb{Z}$ with $b \equiv 1 \pmod{k}$ provided that $(a, b) = 1$ and $\chi(b) \neq 1$.

We define the *Dirichlet L-function* with Dirichlet character χ as

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

for $Re(s) > 1$.

Now, suppose that K is a quadratic field. Recall that a prime number either splits, ramifies or is inert. Define

$$\chi(p) = \begin{cases} 1 & \text{if p splits} \\ -1 & \text{if p is inert} \\ 0 & \text{if p ramifies} \end{cases}$$

Then, χ gives a real primitive character modulo $|\Delta_K|$. Actually, this character is the Kronecker symbol $(|\Delta_K|, \cdot)$ (*We encourage the reader to see [5], [6], [7]*).

For this character, we have

$$\zeta_K(s) = \zeta(s)L(s,\chi).$$

Then, if we multiply both sides with $(s-1)$ and take limit as s goes to 1:

$$\frac{2^{r_1+r_2}\pi^{r_2}R_K}{|\mu(K)|\sqrt{|\Delta_K|}}\ h_K = L(1,\chi).$$

Now, if K is a real quadratic field, then we have $r_1 = 2, r_2 = 0$, $|\mu(K)| = 2$, and $R_K = \eta$ where η is a fundamental unit. Thus, we have:

$$h_K = \frac{\sqrt{|\Delta_K|}}{2\log\eta}\ L(1,\chi).$$

On the other hand, if K is an imaginary quadratic field, then we have $r_1 = 0, r_2 = 1$ and $R_K = 1$. Therefore, we conclude:

$$h_K = \frac{|\mu(K)|\sqrt{|\Delta_K|}}{2\pi}\ L(1,\chi).$$

Thus, the value of $L(1,\chi)$ can be useful to make assumptions on h_K. However, note that it is not easy to compute $L(1,\chi)$ sometimes. Lastly, in our case

$L(1,\chi) \neq 0$ and this plays a fundamental role on proving Dirichlet's theorem on arithmetic progressions:

Theorem 5.19 (Dirichlet's Theorem on Arithmetic Progressions)**.** *Let $a, b \in \mathbb{Z}^{>0}$ such that $(a,b) = 1$. Then, there exist infinitely many prime numbers p of the form $an + b$ for some $n \in \mathbb{Z}^{>0}$.*

Proof. [7, Chapter 4]. □

Example 5.20. Let $K = \mathbb{Q}(\sqrt{2})$ with fundamental unit $\eta = 1 + \sqrt{2}$. We have $\Delta_K = 8$. Thus,

$$h_K = \frac{\sqrt{8}}{2\log(1+\sqrt{2})}\ L(1,\chi) \approx 1.605\ \ L(1,\chi).$$

We have

$$L(1,\chi) = 1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \dots$$

However, the value of $L(1,\chi)$ is between $1 - \frac{1}{3}$ and $1 - \frac{1}{3} + \frac{1}{5}$ so that $L(1,\chi) < 1$. Thus, $h_K < 1.605$. Therefore, h_K must be 1.

BIBLIOGRAPHY

[1] P. Samuel, *Algebraic Theory of Numbers*, Hermann, 1970.

[2] F. Jarvis, *Algebraic Number Theory*, Springer, 2014.

[3] D. Lorenzini, *An Invitation to Arithmetic Geometry*, American Mathematical Society, 1996.

[4] Keith Conrad : Class Group Calculations
`http://www.math.uconn.edu/ kconrad/blurbs/gradnumthy/classgpex.pdf`

[5] T.M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1970.

[6] H. Cohen, *Number Theory*, Springer, 2007.

[7] H. Davenport, *Multiplicative Number Theory*, Springer-Verlag, 1980.