# A Study of Dirichlet's Class Number Formula And Its Applications

**Mahinshi**

***A dissertation submitted for the partial fulfilment of MS degree in Science***


**Indian Institute of Science Education and Research Mohali**
**Sector 81,SAS Nagar,Mohali, Punjab-140306**
**April,2019**

# Certificate of Examination

This is to certify that the dissertation titled **A study of Dirichlet's Class Number Formula And Its Applications** submitted by **Mahinshi**(MP16011) for the partial fulfilment of MS degree programme of the IISER,Mohali , has been examined by the thesis committee duly appointed by the IISER, Mohali. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Amit Kulshrestha  Dr. Tanusree Khandai  Dr. Abhik Ganguli

(Supervisor)

Prof. Sudesh Kaur Khanduja

(Supervisor)

Dated: April 22, 2019

# Declaration

The work presented in this dissertation has been carried out by me under the guidance of **Dr. Abhik Ganguli** and **Prof. Sudesh Kaur Khanduja** at Indian Institute of Science Education and Research Mohali. This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. This is a bonafied record of original study done by me and all sources listed within have been detailed in the bibliography.

Mahinshi
(Candidate)
Dated: April 22,2019

In my capacity as the supervisor of the candidate's project work, I certify that the above statements made by the candidate are true to the best of my knowledge.

Dr. Abhik Ganguli
(Supervisor)

Prof. Sudesh Kaur Khanduja
(Supervisor)

# Acknowledgement

I would like to thank firstly my thesis supervisors Dr. Abhik Ganguli and Prof. Sudesh Kaur Khanduja in the department of Mathematical Sciences at Indian Institute of Science Education and Research Mohali, for their constant support and guidance throughout my thesis. A special thanks to Prof. Sudesh Kaur Khanduja for believing in me to execute this project successfully. She was extremely supportive, helpful and always there for me in every kind of problems I faced till the completion of my thesis. She never took step back from me as sometimes I was not able to perform with my true potential and even she tried to get me learn to stand up for doing the work better as possible as I can do.

I would also like to thank the committee, including Dr. Amit Kulshrestha and Dr. Tanusree Khandai who were involved for the validation of my thesis. I especially acknowledge Dr. Amit Kulshrestha for his supportive and delightful behaviour with me during the thesis.

I would like to show gratitude to the entire community of the institute: the director, faculty, staff and students for maintaining an intellectual environment which helped me to work in my comfort zone. I especially thanks to MHRD, Government of India for providing scholarship and institute for the facilities as library and computer labs.

I also acknowledge my seniors Dr. Anuj Jakhar, Miss. Neha Nanda, Miss. Gargi Lather and my friends for their support and consistent faith within me during every crucial time till now. I would be very thankful for their helpful nature and the strength I have received from them which really helped me keep going during this one year course of my thesis.

# Contents

# Abstract

Class number is an important invariant associated to an algebraic number field $K$. In this thesis, our main aim is to prove Dirichlet's Class Number Formula and some of its applications. For stating this formula, we need to know the structure of the group of units of the ring $\mathcal{O}_K$ of algebraic integers of $K$. In the first chapter, we prove Dirichlet's Unit Theorem which describes the structure of group of units of $\mathcal{O}_K$. The second chapter contains a proof of the finiteness of class number of an algebraic number field $K$. The third chapter contains a proof of Dirichlet's Class Number Formula and Dirichlet's Density Theorem besides some applications of this formula. In the fourth chapter, we describe simplified version of Dirichlet's Class Number Formula for cyclotomic fields and quadratic fields.

# Index of Notation

| | |
|---|---|
| $\mathbb{Z}$ | The set of Integers |
| $\mathbb{Q}$ | The set of Rational Numbers |
| $\mathbb{R}$ | The set of Real Numbers |
| $\mathbb{C}$ | The set of Complex Numbers |
| $\overline{z}$ | Complex Conjugate of $z$ |
| $\iota$ | iota $= \sqrt{-1}$ |
| $B'$ | Transpose of a matrix $B$ |
| $K$ | Algebraic Number Field |
| $\mathcal{O}_K$ | Ring of algebraic integers of $K$ |
| $d_K$ | Discriminant of $K$ |
| $N_{K/\mathbb{Q}}(\alpha)$ | Norm of $\alpha$ w.r.t. $K/\mathbb{Q}$ |
| $N(I)$ | Absolute norm of a non-zero ideal $I$ of $\mathcal{O}_K$ |
| $D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n)$ | Discriminant of a basis $\{w_1, w_2, \ldots, w_n\}$ of $K/\mathbb{Q}$ |
| $\phi(n)$ | Euler Totient Function evaluated at a number $n$ |
| $\left(\frac{a}{p}\right)$ | Legendre Symbol |
| $\|\|x\|\|$ | length of a vector $x$ in $\mathbb{R}^n$ |

# Chapter 1

# Units of $\mathcal{O}_K$

Let $K$ be an algebraic number field and $\mathcal{O}_K$ denote the ring of algebraic integers of $K$. This chapter is devoted to the study of units of the ring $\mathcal{O}_K$. We first recall some basic definitions.

**Definition.** An element $\alpha$ of $\mathcal{O}_K$ is said to be a unit of $\mathcal{O}_K$ if there exists $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$.

**Definition.** A non-zero non-unit element $\alpha$ of $\mathcal{O}_K$ is said to be irreducible element of $\mathcal{O}_K$ if whenever $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathcal{O}_K$, then either $\beta$ or $\gamma$ is a unit.

**Definition.** A non-zero non-unit element $\alpha$ of $\mathcal{O}_K$ is said to be a prime element of $\mathcal{O}_K$ if whenever $\alpha$ divides $\beta\gamma$ with $\beta, \gamma \in \mathcal{O}_K$, then either $\alpha$ divides $\beta$ or $\alpha$ divides $\gamma$.

**Definition.** A field isomorphism $\sigma$ of $K$ into $\mathbb{C}$ will be called a real isomorphism if $\sigma(K) \subseteq \mathbb{R}$ otherwise it will be called non-real isomorphism.

## 1.1 Statement of Dirichlet's Unit Theorem and Some Preliminary Results

In this chapter we shall prove a famous theorem of Dirichlet which describes the structure of the group of units of $\mathcal{O}_K$ and was proved in 1846. It is known as Dirichlet's Unit Theorem.

**Dirichlet's Unit Theorem.** *Let $K$ be an algebraic number field of degree $n = r+2s$ where $r$ is the number of real isomorphisms of $K$ and $2s$ is the number of non-real isomorphisms of $K$, $\mathcal{O}_K$ denotes the ring of algebraic integers of $K$. Then $\exists$ units $\epsilon_1, \epsilon_2, \ldots, \epsilon_t$ with $t = r + s - 1$ of $\mathcal{O}_K$ such that every unit $\epsilon$ of $\mathcal{O}_K$ can be uniquely written as*

$\epsilon = \zeta\epsilon_1^{a_1} \dots \epsilon_t^{a_t}$ *where* $a_1, \dots, a_t$ *are in* $\mathbb{Z}$ *and* $\zeta$ *is a root of unity in* $K$.

To prove this theorem we shall give some definitions and preliminary results.

**Proposition 1.1.1.** *Let* $K$ *be an algebraic number field. An element* $\alpha$ *of* $\mathcal{O}_K$ *is a unit if and only if* $|N_{K/\mathbb{Q}}(\alpha)| = \pm 1$.

*Proof.* Suppose first that $\alpha$ is a unit of $\mathcal{O}_K$. Then there exists $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. So $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta) = 1$. As norm of an algebraic integer with respect to the extension $K/\mathbb{Q}$ belongs to $\mathbb{Z}$, we see that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

Conversely, suppose that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$, $\alpha \in \mathcal{O}_K$. Let $\alpha_1 = \alpha, \alpha_2, \dots, \alpha_n$ be all the roots(counting multiplicity, if any) of the characteristic polynomial of $\alpha$ with respect to $K/\mathbb{Q}$. Then $N_{K/\mathbb{Q}}(\alpha) = \alpha_1\alpha_2 \dots \alpha_n = \pm 1$. Write $\beta = \prod_{i=2}^{n} \alpha_i$. Clearly $\beta$ is an algebraic integer; also $\beta = \frac{\pm 1}{\alpha} \in \mathbb{Q}(\alpha) \subseteq K$. So $\beta \in \mathcal{O}_K$ and $\alpha\beta = \pm 1$. Thus $\alpha$ is a unit of $\mathcal{O}_K$.

□

**Corollary 1.1.2.** *If* $\alpha$ *is an element of* $\mathcal{O}_K$ *with* $|N_{K/\mathbb{Q}}(\alpha)|$ *a prime number , then* $\alpha$ *is an irreducible element of* $\mathcal{O}_K$.

*Proof.* Suppose that $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathcal{O}_K$. Then $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\beta)N_{K/\mathbb{Q}}(\gamma) = \pm p$, where $p$ is a prime. As $N_{K/\mathbb{Q}}(\beta)$ and $N_{K/\mathbb{Q}}(\gamma)$ are integers, atleast one of these must be $+1$ or $-1$. So by the above proposition, either $\beta$ or $\gamma$ is a unit of $\mathcal{O}_K$.

□

*Remark.* If $\alpha$ is as in the above corollary then $\alpha$ is in fact a prime element of $\mathcal{O}_K$, because it is known that $N(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$ (see Chapter 5 [Ta-St]); consequently $\alpha\mathcal{O}_K$ is a prime ideal as its norm is a prime number.

We now prove that $\mathcal{O}_K$ is a Factorization Domain for each algebraic number field $K$. Recall that an integral domain $R$ is a factorization domain if every non-zero non-unit element of $R$ can be expressed as a product of finitely many irreducible elements of $R$.

**Theorem 1.1.3.** *Let* $K$ *be an algebraic number field. Any non-zero non-unit element* $\alpha \in \mathcal{O}_K$ *can be written as a product of finitely many irreducible elements of* $\mathcal{O}_K$.

*Proof.* We prove the theorem by induction on $|N_{K/\mathbb{Q}}(\alpha)|$. When $|N_{K/\mathbb{Q}}(\alpha)| = 1$, then $\alpha$ is a unit by Proposition 1.1.1. When $|N_{K/\mathbb{Q}}(\alpha)| = 2$, then $\alpha$ is irreducible by the above corollary. Suppose the theorem holds for all $\alpha \in \mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(\alpha)| < n$. Let $\alpha$ be an element of $\mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(\alpha)| = n$. If $\alpha$ is irreducible element of $\mathcal{O}_K$, then we are done, otherwise we can write $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathcal{O}_K$, where $\beta, \gamma$ are non-units. So $|N_{K/\mathbb{Q}}(\beta)| > 1$, $|N_{K/\mathbb{Q}}(\gamma)| > 1$ in view of Proposition 1.1.1. Therefore $|N_{K/\mathbb{Q}}(\beta)| < n$, $|N_{K/\mathbb{Q}}(\gamma)| < n$. By induction hypothesis $\beta, \gamma$ can written as a product of finitely many irreducible elements of $\mathcal{O}_K$ and hence so can be $\alpha = \beta\gamma$.

□

**Corollary 1.1.4.** *For an algebraic number field $K$, $\mathcal{O}_K$ has infinitely many non-associate irreducible elements.*

*Proof.* For any rational prime $p$, there exists an irreducible element $\pi_p$ (say) of $\mathcal{O}_K$ dividing $p$ by virtue of Theorem 1.1.3. If $p \neq q$ are prime numbers, then $\pi_p$, $\pi_q$ cannot be associates because otherwise $|N_{K/\mathbb{Q}}(\pi_p)| = |N_{K/\mathbb{Q}}(\pi_q)|$ which is impossible because $|N_{K/\mathbb{Q}}(\pi_p)|$ divides $N_{K/\mathbb{Q}}(p) = p^n$ and $N_{K/\mathbb{Q}}(\pi_q)$ divides $q^n$ and $|N_{K/\mathbb{Q}}(\pi_p)| > 1$.

□

*Remark.* Let $K = \mathbb{Q}(\sqrt{d}\ )$ be an imaginary quadratic field with $d$ a negative square free integer. In 1801, Gauss proved that $\mathcal{O}_K$ is a Unique Factorisation Domain (UFD) for $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. He also conjectured that these are the only imaginary quadratic fields $K$ for which $\mathcal{O}_K$ is a $UFD$. This conjecture remained open until 1966 when it was proved by Baker[Bak] and Stark[Sta]. Gauss has conjectured that there are infinitely many real quadratic fields whose ring of algebraic integers are $UFD$. This is not proved as yet.

**Definition.** Let $R$ be a commutating ring with identity. Let $c$ be a non-zero element of $R$; for $\alpha, \beta \in R$ we say that $\alpha \equiv \beta \bmod(c)$ if there exists $\gamma \in R$ such that $\alpha - \beta = c\gamma$.

This is an equivalence relation on $R$ and partitions $R$ into union of equivalence classes called congruence classes modulo $c$. The following lemma gives information about the congruence classes in $\mathcal{O}_K$ modulo a positive integer $c$.

Recall that a $\mathbb{Z}$-basis of the free abelian group $\mathcal{O}_K$ is called an integral basis of $K$.

**Lemma 1.1.5.** *Let $K$ be an algebraic number field of degree $n$ over $\mathbb{Q}$. Let $c$ be a positive integer. Then there are atmost $c^n$ congruence classes modulo $c$ in $\mathcal{O}_K$.*

*Proof.* Let $w_1, w_2, \ldots, w_n$ be integral basis of $K$. Let $\alpha$ be any element of $\mathcal{O}_K$, then we can write

$$\alpha = a_1 w_1 + \cdots + a_n w_n, a_i \in \mathbb{Z}$$

Write $a_i = cq_i + r_i, 0 \leq r_i < c$, $q_i, r_i \in \mathbb{Z}$. So

$$\alpha = c \sum_{i=1}^{n} q_i w_i + \sum_{i=1}^{n} r_i w_i$$

and hence $\alpha = \sum_{i=1}^{n} r_i w_i \bmod(\mathrm{c})$
Therefore every $\alpha \in \mathcal{O}_K$ is congruent to one member of the set

$$S = \{\sum_{i=1}^{n} b_i w_i | 0 \leq b_i < c, b_i \in \mathbb{Z}\}$$

Clearly $|S| = c^n$. Hence lemma is proved.

□

**Theorem 1.1.6.** *Let $K$ be an algebraic number field. Then for every positive integer $c$, there are only finitely many non-associate elements $\alpha \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\alpha)| = c$.*

*Proof.* First we will show that for any $\alpha \in \mathcal{O}_K$, $\frac{|N_{K/\mathbb{Q}}(\alpha)|}{\alpha} \in \mathcal{O}_K$. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the isomorphisms of $K$ into $\mathbb{C}$ with $\sigma_1(\alpha) = \alpha$, then

$$N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) = \alpha \prod_{i=2}^{n} \sigma_i(\alpha) = a(\text{say})$$

Then $a \in \mathbb{Z}$. So $\frac{a}{\alpha} = \prod_{i=2}^{n} \sigma_i(\alpha)$ is an algebraic integer.

In view of Lemma 1.1.5, the theorem is proved once we show that whenever $\alpha, \beta \in \mathcal{O}_K$ are in same congruence class modulo $c$ and $|N_{K/\mathbb{Q}}(\alpha)| = c = |N_{K/\mathbb{Q}}(\beta)|$, then $\alpha$ and $\beta$ are associates. Let $\alpha$ and $\beta$ be in the same congruence class mod $c$, then there exists $\gamma \in \mathcal{O}_K$ such that $\alpha - \beta = c\gamma$. As shown in the above paragraph $\frac{N_{K/\mathbb{Q}}(\beta)}{\beta} \in \mathcal{O}_K$. Therefore

$$\frac{\alpha}{\beta} = 1 + \frac{c\gamma}{\beta} = 1 \pm \frac{N_{K/\mathbb{Q}}(\beta)\gamma}{\beta} \in \mathcal{O}_K$$

Similarly $\frac{\beta}{\alpha} \in \mathcal{O}_K$. So $\frac{\alpha}{\beta}$ is a unit of $\mathcal{O}_K$. This proves that $\alpha$ and $\beta$ are associates as desired. As total number of congruence classes modulo $c$ is finite by Lemma 1.1.5, so there are only finitely many non-associate elements of $\mathcal{O}_K$ having $\pm c$ as norm.

□

**Proposition 1.1.7.** *Let $K$ be an algebraic number field of degree $n$ and $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the isomorphisms of $K$ into $\mathbb{C}$. Prove that for any constant $c > 0$, there are only finitely many $\alpha \in \mathcal{O}_K$ such that $|\sigma_i(\alpha)| \leq c$ for $1 \leq i \leq n$.*

*Proof.* Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of $K$. let $\alpha$ be any element of $\mathcal{O}_K$. We can write $\alpha = x_1w_1 + x_2w_2 + \cdots + x_nw_n$ with $x_i \in \mathbb{Z}$. Taking the image under $\sigma_i$, we have

$$\sigma_i(\alpha) = x_1\sigma_i(w_1) + \cdots + x_n\sigma_i(w_n),\ 1 \leq i \leq n$$

The above equations in the matrix form can be rewritten as $PX = B$, where

$$B = \begin{bmatrix} \sigma_1(\alpha) \\ \vdots \\ \sigma_n(\alpha) \end{bmatrix}, P = \begin{bmatrix} \sigma_1(w_1) & \cdots & \sigma_1(w_n) \\ \vdots & \ddots & \vdots \\ \sigma_n(w_1) & \cdots & \sigma_n(w_n) \end{bmatrix} \text{ and } X = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}.$$

By definition $det(P)^2$ is the discriminant of $K$. So $P$ is invertible. Therefore we have

$$X = P^{-1}B \tag{1.1}$$

Let $q_{i,j}$ denote the $(i,j)th$ entry of $P^{-1}$ and $c_1$ denote the $\max_{i,j} |q_{i,j}|$. If $|\sigma_i(\alpha)| \leq c$ for every $i$, then by Equation (1.1), $|x_j| \leq ncc_1$ for each $j$. So the integers $x_j$ will have only finitely many choices. The same holds for $\alpha \in \mathcal{O}_K$ with $|\sigma_i(\alpha)| \leq c$ for each $i$ and hence the proposition is proved.

□

**Corollary.** The group of roots of unity in any algebraic number field $K$ is finite.

*Proof.* If $\alpha$ is a root of unity in $K$, then so is $\sigma_i(\alpha)$ for any isomorphism

$$\sigma_i \ : \ K \to \mathbb{C}$$

So $|\sigma_i(\alpha)| = 1$. The corollary now follows from the above proposition.

□

**Definition.** A subset $S$ of $\mathbb{R}^n$ is called discrete if every bounded subset of $\mathbb{R}^n$ contains only finitely many points of $S$.

It can be easily seen that a free abelian group of finite rank contained in $\mathbb{R}^n$ is discrete.

**Proposition 1.1.8.** *A discrete subgroup $\Gamma$ of $\mathbb{R}^n$ is a free abelian group of rank not exceeding $n$.*

*Proof.* Let $V$ be the smallest subspace of $\mathbb{R}^n$ containing $\Gamma$ and $s$ its dimension over $\mathbb{R}$. We can choose $s$ vectors in $\Gamma$, say $v_1, v_2, \ldots, v_s \in \Gamma$ such that $v_1, v_2, \ldots, v_s$ form a basis of vector space $V$. Let $\Gamma_0$ denote the subgroup of $\Gamma$ defined by $\Gamma_0 = \mathbb{Z}v_1 + \mathbb{Z}v_2 + \cdots + \mathbb{Z}v_s$. We first show that $[\Gamma : \Gamma_0]$ is finite. Let $v = \sum_{i=1}^{s} a_i v_i$, $a_i \in \mathbb{R}$, be any element of $\Gamma$. Write $a_i = [a_i] + \delta_i$, where $[a_i]$ stands for the largest integer not exceeding $a_i$, $0 \leq \delta_i < 1$. Therefore

$$v = \sum_{i=1}^{s} [a_i] v_i + \sum_{i=1}^{s} \delta_i v_i = w + z, \ w \in \Gamma_0, z \in \Gamma \cap Y, \tag{1.2}$$

where Y is defined by

$$Y = \{(y_1, y_2, \ldots, y_n) \in \mathbb{R}^n \mid |y_j| \leq \sum_{i=1}^{s} ||v_i||, 1 \leq j \leq n\},$$

$||v_i||$ stands for the length of vector $v_i$ in $\mathbb{R}^n$. Equation 1.2 shows that $[\Gamma : \Gamma_0] \leq |\Gamma \cap Y|$. Since $Y$ is a bounded set and $\Gamma$ is discrete , $\Gamma \cap Y$ is a finite set. This proves that $[\Gamma : \Gamma_0]$ is finite, say $j$. By, Lagrange's Theorem of finite groups, $j\Gamma \subseteq \Gamma_0$ which implies that $\Gamma \subseteq \frac{1}{j}\Gamma_0$. As $\frac{1}{j}\Gamma_0$ is a free abelian group of rank $s$ so is $\Gamma$ of rank $l \leq s$ (cf. Theorem 2, Chapter-2, Sec-2 of [Bo-Sh]).

□

## 1.2 Minkowski's Lemma on Linear Forms and its Modifications

**Minkowski's Lemma**[1] **on real linear forms.** Let $L_i(x) = \sum_{j=1}^{n} a_{ij}x_j$ be real linear forms for $1 \leq i \leq n$ with $det(a_{ij}) \neq 0$. Let $c_1, \ldots, c_n$ be positive real numbers such that $\prod_{i=1}^{n} c_i > |det(a_{ij})|$ then there exists rational integers $u_1, u_2, \ldots, u_n$ not all zero such that $|L_i(u_1, u_2, \ldots, u_n)| < c_i$ for $1 \leq i \leq n$.

*Proof.* We show that $\exists$ integers $z_1, \ldots, z_n$ not all zero such that

$$|L_i(z_1, \ldots, z_n)| < c_i \ for \ 1 \leq i \leq n \qquad (*)$$

Suppose the lemma is false. For $g = (g_1, \ldots, g_n) \in \mathbb{Z}^n$, let $\pi_{(g_1,\ldots,g_n)}$ denote the subset called parallelotope of $\mathbb{R}^n$ defined by :

$$\pi_{(g_1,\ldots,g_n)} = \{\ x = (x_1, \ldots, x_n) \mid \ |L_i(x - g)| < \frac{c_i}{2} \text{ for } 1 \leq i \leq n \ \}$$

Note that if $g \neq g'$ are in $\mathbb{Z}^n$, then $\pi_{(g_1,\ldots,g_n)} \cap \pi_{(g'_1,\ldots,g'_n)} = \emptyset$, because if $x$ belongs to their intersection, then $|L_i(g - g')| \leq |L_i(g - x)| + |L_i(x - g')| < c_i$ for $1 \leq i \leq n$ which shows that the vector $g - g'$ satisfies (*), contrary to their assumption.
Let $J$ denote the volume of any parallelotope $\pi_{(g_1,\ldots,g_n)}$ and $d$ be the real number such that the co-ordinates of all points of $\pi_{(0,\ldots,0)}$ are less than $d$ in absolute value. Let $L$ be a positive integer. Consider the family $\mathbb{T}$ of all those $\pi_{(g_1,\ldots,g_n)}$ for which $|g_i| \leq L \ \forall \ i, \ g_i \in \mathbb{Z}$. Clearly $\mathbb{T}$ consists of $(2L+1)^n$ parallelotopes $\pi_{(g_1,\ldots,g_n)}$. If $x$ belongs to a member $\pi_{(g_1,\ldots,g_n)}$ of $\mathbb{T}$, then $|x_i| \leq |x_i - g_i| + |g_i| \leq d + |g_i| \leq d + L$. Since the members of $\mathbb{T}$ are pairwise disjoint, we see that $(2L + 1)^n J \leq (2d + 2L)^n$ On dividing by $(2L)^n$ and taking limit as

[1]This was established by H.Minkowski in 1896. Minkowski's lemma on linear forms is a corollary of more general theorem of Minkowski on convex bodies which is proved in Chapter 2( Section 2.2). The lemma on real linear forms goes back to Dirichlet.

$L \longrightarrow \infty$, we see that $J \leq 1$.
On the other hand, we have:

$$J = \int \cdots \int_{|L_i(x)|<\frac{c_i}{2} \ \forall \ i} dx_1 \dots dx_n = \frac{1}{|det(A)|} \int \cdots \int_{|y_i|<\frac{c_i}{2} \ \forall \ i} dy_1 ... dy_n = \frac{\prod_{i=1}^{n} c_i}{|det(A)|}$$

The above equation together with $J \leq 1$ implies that $\prod_{i=1}^{n} c_i \leq |det(A)|$ contrary to the hypothesis.

□

**Modified Minkowski's Lemma on real linear forms**
Let $L_i(x) = \sum_{i=1}^{n} a_{ij}x_j$ be $n$ real linear forms for $1 \leq i \leq n$ with $det(a_{ij}) \neq 0$. Let $c_1, c_2, \dots, c_n$ be positive constants such that $|det(a_{ij})| = \prod_{i=1}^{n} c_i$, then there exist rational integers $u_1, \dots, u_n$ not all zero such that $|L_i(u_1, \dots, u_n)| < c_i$ for $1 \leq i \leq n-1$ and $|L_n(u_1, u_2, \dots, u_n)| \leq c_n$.

*Proof.* For any real number $\epsilon > 0$ we define a subset $K_\epsilon$ of $\mathbb{R}^n$ by

$$K = \{(x_1, \dots, x_n) \ : \ |L_i(x_1, x_2, \dots, x_n)| < c_i, \ 1 \leq i \leq n-1, \ |L_n(x_1, x_2, \dots, x_n)| < c_n(1+\epsilon)\}$$

As $(\prod_{i=1}^{n} c_i)(1+\epsilon) > |det(a_{ij})|$ and $det(a_{ij}) \neq 0$, so by Minkowski's Lemma on real linear forms, we have $K_\epsilon \cap \mathbb{Z}^n \neq (0, 0, \dots, 0)$ i.e.,

$$K_\epsilon \cap (\mathbb{Z}^n \setminus (0, 0, \dots, 0)) \neq \emptyset$$

But $K_\epsilon$ is a bounded set for any $\epsilon > 0$. Therefore $K_\epsilon \cap \mathbb{Z}^n$ must be finite. In particular,if we take $\epsilon = 1$, then $K_\epsilon \cap (\mathbb{Z}^n \setminus (0, 0, \dots, 0))$ is a finite non-empty set $\{A_1, A_2, \dots, A_k\}$ (say). Suppose if possible the lemma is false. In view of this supposition, if $(u_1, u_2, \dots, u_n) \in K_\epsilon \cap \mathbb{Z}^n$ is a non-zero vector, then $|L_n(u_1, u_2, \dots, u_n)| > c_n$. This implies that there exists $\epsilon_0$ with $0 < \epsilon_0 < 1$ such that $|L_n(A_i)| \geq c_n(1+\epsilon_0)$ for $1 \leq i \leq k$. Consider the set $K_{\epsilon_0}$. Then $K_{\epsilon_0} \subseteq K_\epsilon$. Since no $A_i$ belongs to $K_{\epsilon_0}$, we conclude that $K_{\epsilon_0} \cap \mathbb{Z}$ consists of only zero vector which contradicts the fact that $K_\epsilon \cap \mathbb{Z}^n$ contains a non-zero vector for any $\epsilon > 0$ as shown above.

□

**Modified Minkowski's lemma on complex linear forms**

Let $L_i(x) = \sum_{j=1}^{n} a_{ij}x_j$ be linear forms for $1 \leq i \leq n$ with $det(a_{ij}) \neq 0$ such that $L_1, \ldots, L_r$ are real linear forms and $L_{r+1}, \ldots, L_{r+2s}$ are complex linear forms satisfying $\overline{L}_{r+j} = L_{r+s+j}$, $1 \leq j \leq s$. Let $c_1, c_2, \ldots, c_n$ be positive constants such that $\prod_{i=1}^{n} c_i = |det(a_{ij})|$ and $c_{r+j} = c_{r+s+j}$, $1 \leq j \leq s$, then there exist rational integers $u_1, u_2, \ldots, u_n$ not all zero such that $|L_i(u_1, u_2, \ldots, u_n)| < c_i$ for $1 \leq i \leq n-1$ and $|L_n(u_1, u_2, \ldots, u_n)| \leq c_n$.

*Proof.* We define $n$ real linear forms $L'_1, L'_2, \ldots, L'_n$ as follows:
Set $L'_j = L_j$ if $1 \leq j \leq r$,
$L'_{r+j} = \frac{1}{2}(L_{r+j} + L_{r+s+j})$ and $L'_{r+s+j} = \frac{1}{2\iota}(L_{r+j} - L_{r+s+j})$ if $1 \leq j \leq s$.
The absolute value $D'$ of the determinant of the matrix of the forms $L'_1, L'_2, \ldots, L'_n$ is $2^{-s}|det(a_{ij})|$. We now apply modified Minkowski's lemma on real linear forms to $L'_1, L'_2, \ldots, L'_n$ with constants $c'_1, c'_2, \ldots, c'_n$, where $c'_i = c_i$ for $1 \leq i \leq r$ and $c'_i = \frac{c_i}{\sqrt{2}}$ for $r+1 \leq i \leq r+2s = n$. Clearly $\prod_{i=1}^{n} c'_i = \left(\prod_{i=1}^{n} c_i\right)/2^s = \frac{|det(a_{ij})|}{2^s} = D'$. Hence by modified Minkowski's lemma on real linear forms, we can find integers $z_1, z_2, \ldots, z_n$ not all zero such that $|L_i(z_1, z_2, \ldots, z_n)| < c'_i$ for $1 \leq i \leq n-1$ and $|L'_n(z_1, z_2, \ldots, z_n)| \leq c'_n$. Thus $|L_i(z_1, z_2, \ldots, z_n)| < c_i$ for $1 \leq i \leq r$ and for $r+1 \leq i \leq r+s-1$, we have

$$\begin{aligned} |L_i(z_1, z_2, \ldots, z_n)| &= |L_{i+s}(z_1, z_2, \ldots, z_n)| \\ &= \sqrt{L'_i(z_1, \ldots, z_n)^2 + L'_{i+s}(z_1, \ldots, z_n)^2} \\ &< \sqrt{c_i'^2 + c_i'^2} = \sqrt{2}c'_i = c_i. \end{aligned}$$

Also,

$$\begin{aligned} |L_n(z_1, z_2, \ldots, z_n)| &= |L'_{r+s}(z_1, z_2, \ldots, z_n) + \iota L'_{r+2s}(z_1, z_2, \ldots, z_n)| \\ &\leq \sqrt{c'^2_{r+s} + c'^2_{r+2s}} = \sqrt{\frac{c^2_{r+s}}{2} + \frac{c^2_{r+2s}}{2}} = c_n \end{aligned}$$

So, $|L_n(z_1, z_2, \ldots, z_n)| \leq c_n$.

□

**Notation.**In what follows, for an algebraic number field $K$ of degree $n = r + 2s$, the isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$ of $K$ into $\mathbb{C}$ are arranged so that $\sigma_1, \ldots, \sigma_r$ are real isomorphisms and $\sigma_{r+1}, \ldots, \sigma_{r+s}$ are non-real and $\sigma_{r+s+j} = \overline{\sigma}_{r+j}$ for $1 \leq j \leq s$ and we denote

$\sigma_i(\alpha)$ by $\alpha^{(i)}$.

Using modified Minkowski's Lemma on complex linear forms, we now prove a lemma which plays a significant role in the proof of Dirichlet's Theorem on units.

**Lemma 1.2.1.** *Let $K$ be an algebraic number field of degree $n = r + 2s$. Prove that for each $k$, $1 \leq k \leq r + s$, there exists a unit $\eta$ of $\mathcal{O}_K$ such that $|\eta^{(k)}| > 1$ and $|\eta^{(j)}| < 1$ for $j \neq k,\ 1 \leq j \leq r + s$.*

*Proof.* Let $d_K$ denote the discriminant of $K$ . Let $b_1, \ldots, b_n$ be positive real numbers satisfying $b_{r+j} = b_{r+s+j}$, for $1 \leq j \leq s$ and $\prod_{i=1}^{n} b_i = \sqrt{|d_K|}$. Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of $K$. Now apply modified Minkowski's Lemma of complex linear forms to the forms $L_1, \ldots, L_n$ given by $L_i(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{n} w_j^{(i)} x_j$ and contains $b_1, \ldots, b_n$, we shall obtain rational integers $z_1, z_2, \ldots, z_n$ not all zero such that

$$|L_i(z_1, z_2, \ldots, z_n)| \leq b_i \tag{1.3}$$

Set $\gamma = \sum_{j=1}^{n} z_j w_j$, then $\gamma$ is non-zero element of $\mathcal{O}_K$ and equation (1.3) says that $|\gamma^{(i)}| \leq b_i$ for $1 \leq i \leq n$. In particular,

$$|N_{K/\mathbb{Q}}(\gamma)| = \prod_{i=1}^{n} |\gamma^{(i)}| \leq \prod_{i=1}^{n} b_i = \sqrt{|d_K|}$$

Take a fixed $k,\ 1 \leq k \leq r + s$; choose $b_j < 1$ for $1 \leq j \leq r + s$, when $j \neq k$ and $b_{r+j} = b_{r+s+j}$ for $1 \leq j \leq s$; determine $b_k$ such that $\prod_{i=1}^{n} b_i = \sqrt{|d_K|}$. So by the above process there exists a non-zero element $\gamma_0 \in \mathcal{O}_K$ such that $|\gamma_0^{(j)}| \leq b_j < 1$ for $j \neq k,\ 1 \leq j \leq r + s$ and $N_{K/\mathbb{Q}}(\gamma_0)| \leq \sqrt{|d_K|}$. Keeping in mind that $N_{K/\mathbb{Q}}(\gamma_0)| \geq 1$, we see that $|\gamma_0^{(k)}| > 1$. Set

$$m_0 = \min\{\ |\gamma_0^{(j)}|,\ 1 \leq j \leq r + s\ \}$$

Take new set of $b_j$'s such that $b_j < m_0,\ 1 \leq j \leq r + s,\ j \neq k$ and $b_{r+s} = b_{r+s+j}$ for $1 \leq j \leq s$ and $\prod_{i=1}^{n} b_i = \sqrt{|d_K|}$. Again by previous description, there exist $0 \neq \gamma_1 \in \mathcal{O}_K$ such that $|\gamma_1^{(j)}| < m_0$ for $1 \leq j \leq r + s,\ j \neq k$. In particular, $|\gamma_1^{(j)}| < |\gamma_0^{(j)}|,\ 1 \leq j \leq r + s,\ j \neq k$. We may continue this process indefinitely and find $\gamma_0, \gamma_1, \ldots$ in $\mathcal{O}_K$ such that for $1 \leq j \leq r + s,\ j \neq k$,

$$|\gamma_0^{(j)}| > |\gamma_1^{(j)}| > |\gamma^{(j)}| > \cdots$$

and $|N_{K/\mathbb{Q}}(\gamma_i)| \leq \sqrt{|d_K|}$ for each $i$. Now by Theorem 1.1.6 only finitely many $\gamma_i$'s can be non-associates. So there exist natural number $l$ and $m$, $m > l$ such that $\gamma_l$ and $\gamma_m$ are associates. Therefore $\exists$ a unit $\eta$ of $\mathcal{O}_K$ such that $\gamma_m = \eta\gamma_l$.
By choice of sequence $|\gamma_m^{(j)}| < |\gamma_l^{(j)}|,\ 1 \leq j \leq r+s,\ j \neq k$
$\implies |\eta^{(j)}| < 1$ for $1 \leq j \leq r+s,\ j \neq k$
Since $|N_{K/\mathbb{Q}}(\eta)| = 1$, this implies $|\eta^{(k)}| > 1$.

□

## 1.3 Proof of Dirichlet's Unit Theorem

*Proof.* Let $\mathcal{O}_K^\times$ denote the group of units of $\mathcal{O}_K$ and $W_K$ the group of roots of unity contained in $K$. Set $t = r + s - 1$. We define a group homomorphism

$$\lambda \ : \ \mathcal{O}_K^\times \to \mathbb{R}^t$$

defined by

$$\lambda(\varepsilon) = (\log|\varepsilon^{(1)}|, \ldots, \log|\varepsilon^{(t)}|).$$

Clearly, $\lambda$ is a group homomorphism. We divide the proof into four steps.

**Step I.** First we will prove that Kernel of $\lambda = W_K$.
If $\varepsilon$ is a root of unity in $K$, then $\varepsilon^{(j)}$ is also a root of unity.
So $|\varepsilon^{(j)}| = 1\ \forall j,\ 1 \leq j \leq t$
$\Rightarrow \log|\varepsilon^{(j)}| = 0$, which shows that $W_K \subseteq$ Kernel($\lambda$).
Conversely suppose that $\epsilon \in$ Kernel($\lambda$). So $|\epsilon^{(j)}| = |\epsilon^{(j+s)}| = 1$ for $1 \leq j \leq r+s-1$. As $|N_{K/\mathbb{Q}}(\epsilon)| = 1$ by Proposition 1.1.1, we see that

$$1 = \prod_{i=1}^{n} |\epsilon^{(i)}| = |\epsilon^{(r+s)}|^l,$$

where $l = 1$ or 2 according as $s = 0$ or not; consequently $|\epsilon^{(r+s)}| = 1$. Applying Proposition 1.1.7, we see that $\epsilon$ has finitely many choices. So Kernel($\lambda$) is a finite group. Hence each element of Kernel($\lambda$) is a root of unity.

**Step II.**In this step, we show that the theorem is proved once we prove that image of $\lambda$ is a free abelian group of rank $t$. In this situation if $\lambda(\mathcal{O}_K^\times)$ has a $\mathbb{Z}$- basis $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$, then $\varepsilon_1, \ldots, \varepsilon_t$ will be a desired set of units. If $\epsilon$ is any unit of $\mathcal{O}_K$, then we shall have

$$\lambda(\varepsilon) = a_1\lambda(\varepsilon_1) + \cdots + a_t\lambda(\varepsilon_t) \text{ for some } a_i \in \mathbb{Z} \Rightarrow \varepsilon\varepsilon_1^{-a_1} \ldots \varepsilon_t^{-a_t} \in \text{ Kernel}(\lambda).$$

By Step I, we shall have $\varepsilon\varepsilon_1^{-a_1}\dots\varepsilon_t^{-a_t} = \zeta \in W_K$. It implies that $\varepsilon = \zeta\varepsilon\varepsilon_1^{a_1}\dots\varepsilon_t^{a_t}$ as asserted in the theorem.

**Step III.** In this step we will prove that $\lambda(\mathcal{O}_K^\times)$ is a discrete subset of $\mathbb{R}^t$, then by using Proposition 1.1.8, $\lambda(\mathcal{O}_K^\times)$ will be a free group of rank $\leq t$. To check discreteness, let $c$ be any positive real number. We will show that there are only finitely many $\varepsilon$ in $\mathcal{O}_K^\times$ such that $-c \leq \log|\varepsilon^{(j)}| \leq c$ for $1 \leq j \leq t$, i.e.,

$$e^{-c} \leq |\varepsilon^{(j)}| \leq e^c \text{ for } 1 \leq j \leq t. \tag{1.4}$$

Let $\varepsilon$ be any unit in $\mathcal{O}_K$ satisfying (1.4). Now

$$1 = |N_{K/\mathbb{Q}}(\varepsilon)| = \prod_{j=1}^{n} |\varepsilon^{(j)}| \geq e^{-(n-l)c}|\varepsilon^{(n)}|^l$$

where $l = 1$ or 2 according as $s = 0$ or not. The above inequality implies $|\varepsilon^{(n)}| \leq e^{\frac{(n-l)c}{l}} \leq e^{nc}$. So all the conjugates of $\varepsilon$ are bounded in absolute value by $e^{nc}$. By Proposition 1.1.7, $\varepsilon$ has only finitely many choices. Hence $\lambda(\mathcal{O}_K^\times)$ is a discrete subset of $\mathbb{R}^t$.

**Step IV.** We have to show that the rank of $\lambda(\mathcal{O}_K^\times)$ is $t$. For this it is enough to prove that $\lambda(\mathcal{O}_K^\times)$ contains a set of $t$ vectors which are linearly independent over $\mathbb{R}$. We introduce a new notation.

**Notation.** For $\alpha \in K^\times$, we set

$$l^{(j)}(\alpha) = \begin{cases} \log|\alpha^{(j)}| & \text{for } 1 \leq j \leq r \\ 2\log|\alpha^{(j)}| & \text{for } r+1 \leq j \leq r+s \end{cases}$$

Note that

$$\log|N_{K/\mathbb{Q}}(\alpha)| = \log(\prod_{j=1}^{r} |\alpha^{(j)}| \prod_{j=r+1}^{r+s} |\alpha^{(j)}|^2) = \sum_{j=1}^{r+s} l^{(j)}(\alpha). \tag{1.5}$$

By the virtue of Lemma 1.2.1 applied $t$ times, there exists units $\eta_1, \dots, \eta_t$ of $\mathcal{O}_K$ such that $|\eta_i^{(i)}| > 1$, $|\eta_i^{(j)}| < 1$ if $i \neq j$, $1 \leq i, j \leq t$. We shall prove that $\lambda(\eta_1), \dots, \lambda(\eta_t)$ are linearly independent over $\mathbb{R}$ or we can say that $t \times t$ matrix formed by taking these vectors as row vectors has determinant non-zero. For this, it is enough to prove that the matrix $A = (a_{ij})_{t\times t} = (l^{(j)}(\eta_i))_{t\times t}$ is non-singular. The matrix $A$ clearly satisfies the first two

conditions of the following proved Lemma 1.3.1 . Also by using equation (1.5), we have

$$\sum_{j=1}^{r+s} l^{(j)}(\eta_i) = \log|N_{K/\mathbb{Q}}(\eta_i)| = 0$$

$$\Rightarrow \sum_{j=1}^{t} l^{(j)}(\eta_i) = -l^{(r+s)}(\eta_i);$$

the right hand side of the above equation is positive in view of the choice of $\eta_i$ and the fact that $i \neq r+s$ as $1 \leq i \leq t$. So the third condition of Lemma 1.3.1 is also satisfied and hence $det(A) \neq 0$. This completes the proof of Dirichlet's Unit Theorem.

□

**Lemma 1.3.1.** *Suppose $A = (a_{ij})_{t\times t}$ is a matrix with real entries satisfying the following three properties.*
$(i) a_{ii} > 0.$
$(ii) a_{ij} \leq 0 \ if \ i \neq j.$
$(iii) \sum_{j=1}^{t} a_{ij} > 0 \ \forall i, \ 1 \leq i \leq t.$
*Then $det(A) \neq 0$.*

*Proof.* Suppose to the contrary $det(A) = 0$. Then there exists a non-zero column vector $C = (c_1, \ldots, c_t)'$ such that $AC$ is the zero vector . Let $k$ be an index such that $|c_k| = \max_{1\leq i\leq t} |c_i|$. Then $AC = 0$ implies

$$\sum_{j=1}^{t} a_{kj}c_j = 0 \ \Rightarrow \ a_{kk} = -\sum_{j=1, j\neq k}^{t} \frac{a_{kj}c_j}{c_k} \ \Rightarrow \ |a_{kk}| = \left|\sum_{j=1, j\neq k}^{t} \frac{a_{kj}c_j}{c_k}\right|$$

Keeping in mind the hypothesis $(i)$ and $(ii)$,we have

$$a_{kk} = |a_{kk}| \leq \sum_{j=1, j\neq k}^{t} |a_{kj}| \left|\frac{c_j}{c_k}\right| \leq \sum_{j\neq k} |a_{kj}| = -\sum_{j\neq k} a_{kj}$$

$\Longrightarrow \sum_{j=1}^{t} a_{kj} \leq 0$ which contradicts condition $(iii)$.

□

*Remark.* It is clear from Dirichlet's Unit Theorem that the group of units of $\mathcal{O}_K$ is finite if and only if $t = 0$, i.e., if and only if either $K = \mathbb{Q}$, or $K$ is an imaginary quadratic field. When $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, then by Dirichlet's Unit Theorem there exists

a unique unit $\varepsilon > 1$ of $\mathcal{O}_K$ such that every unit of $\mathcal{O}_K$ can be uniquely written as $\pm\varepsilon^n$ for some $n \in \mathbb{Z}$; such a unit is called **Fundamental Unit of $\mathcal{O}_K$ or of $K$**. We shall prove in section 1.5 of this chapter that if $x + y\omega > 1$ is a fundamental unit of $\mathbb{Q}(\sqrt{d})$,$d \neq 5$ with $\omega = \frac{1+\sqrt{d}}{2}$ or $\omega = \sqrt{d}$ according as $d \equiv 1 \bmod 4$ or not, then $x$ and $y$ are smallest positive integers for which $N_{K/\mathbb{Q}}(x + y\omega) = \pm 1$. This paves the way for an interesting relation between units of real quadratic fields and solution of Pell's equation[2].

## 1.4 Fundamental System of Units and Regulator

**Definition.** If $\varepsilon_1, \ldots, \varepsilon_t$ is as in the statement of Dirichlet's Unit Theorem, then $\{\varepsilon_1, \ldots, \varepsilon_t\}$ is called a fundamental system of units of $\mathcal{O}_K$ or of $K$. As shown in Step II of the proof of Dirichlet's Unit Theorem $\varepsilon_1, \ldots, \varepsilon_t$ is a fundamental system of units if and only if $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$ is a basis of the group $\lambda(\mathcal{O}_K^\times)$. Another system of units $\eta_1, \ldots, \eta_t$ is a fundamental system of units if and only if the transition matrix from the basis $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$ to $\lambda(\eta_1), \ldots, \lambda(\eta_t)$ is unimodular. So if $C$ denotes the $t \times t$ matrix whose row vectors are $\lambda(\eta_1), \ldots, \lambda(\eta_t)$ and $B$ denotes the $t \times t$ matrix whose row vectors are $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_t)$ and if both $\{\varepsilon_1, \ldots, \varepsilon_t\}$ and $\{\eta_1, \ldots, \eta_t\}$ are fundamental system of units of $\mathcal{O}_K$ then $B = AC$ where $A$ is a unimodular matrix. Therefore $|detB| = |detC|$. So $|detB|$ does not depend on the choice of fundamental system. The **Regulator of K** is defined to be $|detB|$ or $2^{s-1}|detB|$ according as $s = 0$ or $s > 0$. In view of Step IV, regulator of an algebraic number field is never zero.

## 1.5 Explicit Calculation of Units in Quadratic Fields

Firstly we shall prove the following proposition which describes $\mathcal{O}_K^\times$ when $K$ is an imaginary quadratic field.

**Proposition 1.5.1.** *Let $K = \mathbb{Q}(\sqrt{d})$, where $d$ is a square free negative integer. Then $\mathcal{O}_K^\times = \{+1, -1\}$ except in the following two cases:*

[2]An equation of the type $x^2 - my^2 = 1$ where $m$ is a given positive non square integer is called Pell's Equation. Euler(1701-1783) attributed to the English mathematician John Pell (1611-1685) a method of finding a solution of the equation $x^2 - my^2 = 1$ in integers $x$ and $y$. Thus the equation has become known as the Pell equation. However, such a method had been found by another English mathematician, William Brouncker (1620-1684), in a series of letters (1657-1658) to Pierre Fermat(1601-1665). Lagarange(1736-1813) was the first mathematician to prove that the equation $x^2 - my^2 = 1$ has infinitely many solutions in integers $x$ and $y$. These solutions $x$ and $y$ may be used to accurately approximate the square root of $m$ by rational numbers $x/y$.The equation was first studied extensively in India, starting with Brahmagupta, who developed the Chakravala method to solve Pell's equation in his Brahma Sphuta Siddhanta in 628, about a thousand years before Pell's time.

(*i*) *when* $d = -1,\ \mathcal{O}_K^\times = \{1, -1, \iota, -\iota\},\ \iota = \sqrt{-1}$
(*ii*) *when* $d = -3,\ \mathcal{O}_K^\times = \{\pm 1, \pm\zeta, \pm\zeta^2\},\ \zeta = \frac{-1+\sqrt{-3}}{2}$.

*Proof.* Suppose first that $d$ is not congruent to 1 modulo 4. Let $x + y\sqrt{d}$ be a unit of $\mathcal{O}_K,\ x, y \in \mathbb{Z}$. So $x^2 - dy^2 = 1$. If $d < -1,\ x^2 - dy^2 = 1$ is possible only if $x = \pm 1,\ y = 0$. When $d = -1$, this equation becomes $x^2 + y^2 = 1$ whose only solutions are $x = \pm 1,\ y = 0$ and $x = 0,\ y = \pm 1$. In this case $\mathcal{O}_K^\times$ has four units $\pm 1, \pm\iota$.

Suppose now that $d \equiv 1 \bmod 4$. Let $\frac{x+y\sqrt{d}}{2}$ be any unit of $\mathcal{O}_K,\ x, y \in \mathbb{Z}$. Then $x^2 - dy^2 = 4$. If $d < -3$, then $d \leq -7$; in this situation $x^2 - dy^2 = 4$ has only two solutions $x = \pm 2, y = 0$. So when $d < -3$, there are only two units, viz., $+1, -1$. If $d = -3$, we have the equation $x^2 + 3y^2 = 4$ which has six solutions viz., $x = \pm 1, y = \pm 1, x = \pm 2, y = 0$. In this case $\mathcal{O}_K^\times$ has six units. □

In order to describe $\mathcal{O}_K^\times$ for real quadratic fields, we prove some simple lemmas.

**Lemma 1.5.2.** *Let* $K = \mathbb{Q}(\sqrt{d})$ *be a real quadratic field with* $d$ *a square free integer. Let* $\omega$ *stands for* $\frac{1+\sqrt{d}}{2}$ *or* $\sqrt{d}$ *according as* $d \equiv 1 \bmod 4$ *or not. If* $\eta = x + y\omega > 1$ *is any unit of* $\mathcal{O}_K$*, then* $x \geq 1,\ y \geq 1$ *except when* $d = 5$ *in which case* $x \geq 0,\ y \geq 1$ *and if* $x = 0$*, then* $y = 1$.

*Proof.* Let $\omega'$ and $\eta'$ denote conjugates of $\omega$ and $\eta$ respectively. Since $N_{K/\mathbb{Q}}(\eta) = \eta\eta' = \pm 1$ and $\eta > 1$, so $\eta - \eta' = y(\omega - \omega') > 0$. As $\omega - \omega' > 0$, we see that $y > 0$. Note that

$$|x + y\omega'| = |\eta'| = \left|\frac{1}{\eta}\right| < 1 \tag{1.6}$$

and $\omega' < -1$ except when $d = 5$. So $y\omega' < -1$ when $d \neq 5$; in this situation (1.6) implies that $x \geq 1$. When $d = 5,\ \omega' = \frac{1-\sqrt{5}}{2}$. As $y \geq 1$, in this case (1.6) implies that $x \geq 0$. Further if $x = 0$, (1.6) becomes $\left|\frac{y(1-\sqrt{5})}{2}\right| < 1$ which is possible only when $y = 1$. □

**Lemma 1.5.3.** *Let* $K = \mathbb{Q}(\sqrt{d})$ *and* $\omega$ *be as in Lemma 1.5.2. Let* $\varepsilon = x + y\omega > 1$ *be a unit of* $\mathcal{O}_K$ *with* $x \neq 0$*. For any* $n \geq 1$*, if* $\varepsilon^n$ *is written as* $x_n + y_n\omega,\ x_n, y_n \in \mathbb{Z}$*, then* $x_{n+1} > x_n,\ y_{n+1} > y_n$ *for all* $n \geq 1$.

*Proof.* In view of Lemma 1.5.2, $x \geq 1, y \geq 1$. We prove the result by induction on $n$. Using $\omega^2 = d$ or $\omega^2 = \frac{d-1}{4} + \omega$, a simple calculation shows that

$$\varepsilon^2 = (x + y\omega)^2 = \begin{cases} x^2 + y^2 d + 2xy\sqrt{d} & \text{if } \omega = \sqrt{d} \\ x^2 + y^2\frac{d-1}{4} + \omega(y^2 + 2xy) & \text{if } \omega = \frac{1+\sqrt{d}}{2} \end{cases}$$

So $x_2 > x,\ y_2 > y$. Suppose that the result is true for $n$, we verify it for $n+1$.

$$\varepsilon^{n+1} = (x_n + y_n\omega)(x + y\omega) = \begin{cases} xx_n + yy_nd + \sqrt{d}(xy_n + yx_n) & \text{if } \omega = \sqrt{d} \\ xx_n + yy_n\frac{d-1}{4} + \omega(xy_n + yx_n + yy_n) & \text{if } \omega = \frac{1+\sqrt{d}}{2} \end{cases}$$

Clearly $x_{n+1} > x_n,\ y_{n+1} > y_n$. □

*Remark.* Lemma 1.5.3 does not hold when $x = 0$. For example, consider $d = 5,\ \epsilon = \frac{1+\sqrt{5}}{2} = \omega$, then $\epsilon^2 = 1 + \omega,\ \epsilon^3 = 1 + 2\omega$.

The following corollary is an immediate consequence of Lemmas 1.5.2 and 1.5.3.

**Corollary 1.5.4.** *When $d \neq 5$, the fundamental unit greater than 1 of $\mathbb{Q}(\sqrt{d})$ is $x + y\omega$, where $x$ and $y$ are smallest positive integers such that $N_{K/\mathbb{Q}}(x + y\omega) = \pm 1$.*

In order to be able to compute smallest positive integers $x, y$ for which $N_{K/\mathbb{Q}}(x+y\omega) = \pm 1$, we shall use simple continued fractions defined below.

**Definition.** A multiple decked expression of the type

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \frac{1}{a_n}}}$$

with $a_i > 0$ for $i \geq 1$ is called a finite continued fraction. If $a_i \in \mathbb{Z}$, then it is called a simple continued fraction. In symbols it will be expressed as $[a_0; a_1, \ldots, a_n]$. Every rational number can be written as a finite simple continued fraction. Any irrational number can be written as an infinite simple continued fraction(see[Niv]).

**Definition.** For any finite or infinite simple continued fraction $[a_0; a_1, \ldots]$, the continued fraction upto the $k^{th}$ stage $[a_0; a_1, \ldots, a_k]$ is called the $k^{th}$ convergent and will be denoted by $\frac{p_k}{q_k}$. So $a_0 = \frac{p_0}{q_0},\ a_0 + \frac{1}{a_1} = \frac{a_0a_1+1}{a_1} = \frac{p_1}{q_1},\ a_0 + \frac{1}{a_1+\frac{1}{a_2}} = \frac{a_2(a_0a_1+1)+a_0}{a_2a_1+1} = \frac{a_2p_1+p_0}{a_2q_1+q_0} = \frac{p_2}{q_2}$. One can prove by induction that $p_k = a_kp_{k-1} + p_{k-2},\ q_k = a_kq_{k-1} + q_{k-2},\ k \geq 2$. Note that $q_i > 0$ for every $i$. We shall consider continued fractions of positive real numbers. So $a_0 \geq 0$ and $p_{i+1} > p_i,\ q_{i+1} > q_i$ for every $i \geq 1$. The name convergent is appropriate because the infinite sequence $\left\{\frac{p_n}{q_n}\right\}$ of convergents of the continued fraction expansion of an irrational number $\xi$ converges to $\xi$.

*Remark.* The name convergent in the above definition is appropriate because the infinite sequence $\left\{\frac{p_n}{q_n}\right\}$ of convergents of the continued fraction expansion of an irrational number $\xi$ converges to $\xi$.

We shall use the following theorem about continued fractions (see [Ch.7. Niv]).

**Theorem.** Let $\xi$ be any irrational number. If there is a rational number $\frac{a}{b}$ with $b \geq 1$ such that $\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}$, then $\frac{a}{b}$ equals one of the convergents of the simple continued fraction expansion of $\xi$.

**Lemma 1.5.5.** *Let $K = \mathbb{Q}(\sqrt{d})$ and $\omega$ be as in Lemma 1.5.2. Assume that $d \neq 5$. Let $x + y\omega > 1$ be a unit of $\mathcal{O}_K$, $x, y \in \mathbb{Z}$. Then $\frac{x}{y}$ is a convergent to the continued fraction expansion of $-\omega'$, where $\omega'$ is the conjugate of $\omega$.*

*Proof.* Since $N_{K/\mathbb{Q}}(x + y\omega) = (x + y\omega)(x + y\omega') = \pm 1$. So

$$\left|\frac{x}{y} + \omega'\right| = \frac{1}{y(x + y\omega)}. \tag{1.7}$$

We split the proof into two cases.
**Case I.** $d \equiv 2$ or $3 \bmod 4$. In this case, we have $x^2 = dy^2 \pm 1 \geq dy^2 - 1 \geq y^2(d-1)$ and hence $\frac{x}{y} \geq \sqrt{d-1}$. It now follows from (1.7) that

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{1}{y^2(\frac{x}{y} + \sqrt{d})} \leq \frac{1}{y^2(\sqrt{d-1} + \sqrt{d})} < \frac{1}{2y^2}.$$

So by the theorem stated above, $\frac{x}{y}$ is a convergent to the continued fraction expansion of $-\omega' = \sqrt{d}$ by the previous theorem.
**Case II.** $d \equiv 1 \bmod 4$. Recall that $d \neq 5$, so $d \geq 13$ and $\frac{\sqrt{d}+1}{2} > 2$; consequently by virtue of (1.7), we have

$$\left|\frac{x}{y} + \omega'\right| = \frac{1}{y^2(\frac{x}{y} + \frac{1+\sqrt{d}}{2})} < \frac{1}{2y^2}$$

So again $\frac{x}{y}$ is a convergent to the continued fraction expansion of $-\omega'$. □

**Corollary 1.5.6.** *Let $K = \mathbb{Q}(\sqrt{d})$ be as in Corollary 1.5.4. The fundamental unit greater than 1 of $K$ is $p_n + q_n\omega$, where $n$ is the smallest non negative integer for which $N_{K/\mathbb{Q}}(p_n + q_n\omega) = \pm 1$; $\frac{p_n}{q_n}$ being the $n^{th}$ convergent to the continued fraction expansion of $-\omega'$.*

*Proof.* This follows immediately from the above lemma and Corollary 1.5.4. □

**Example.** $K = \mathbb{Q}(\sqrt{22})$.
**Solution.** Since $22 \equiv 2 \bmod 4$. Therefore, $\{1, \sqrt{22}\}$ is an integral basis of $K$. We know by Corollary 1.5.6 that fundamental unit greater than 1 of $\mathbb{Q}(\sqrt{22}\,)$ is $p_n + q_n(\sqrt{22})$, where $n$ is the smallest non-negative integer for which $N_{K/\mathbb{Q}}(p_n + q_n(\sqrt{22})) = \pm 1$ and $\frac{p_n}{q_n}$ is the

$n^{th}$ convergent to the continued fraction expansion of $\sqrt{22}$.
$N_{K/\mathbb{Q}}(p_n + q_n(\sqrt{22})) = p_n^2 - 22q_n^2$.
Now from the continued fraction expansion of $\sqrt{22}$, we get :

| $k$ | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| $a_k$ | 4 | 1 | 2 | 4 | 2 | 1 |
| $p_k$ | 4 | 5 | 14 | 61 | 136 | 197 |
| $q_k$ | 1 | 1 | 3 | 13 | 29 | 42 |
| $p_k^2 - 22q_k^2$ | $-6$ | 3 | $-2$ | 3 | $-6$ | 1 |

Thus we see that the fundamental unit is $197 + 42\sqrt{22}$.

**Example.** $K = \mathbb{Q}(\sqrt{41})$.
**Solution.** Since $41 \equiv 1 \bmod 4$. Therefore, $\{1, \frac{1+\sqrt{41}}{2}\}$ is an integral basis of $K$. We know by corollary 1.5.6 that fundamental unit greater than 1 of $\mathbb{Q}(\sqrt{41}\ )$ is $p_n + q_n(\frac{1+\sqrt{41}}{2})$, where $n$ is the smallest non-negative integer for which $N_{K/\mathbb{Q}}(p_n + q_n(\frac{1+\sqrt{41}}{2})) = \pm 1$ and $\frac{p_n}{q_n}$ is the $n^{th}$ convergent to the continued fraction expansion of $\frac{-1+\sqrt{41}}{2}$.
$N_{K/\mathbb{Q}}(p_n + q_n(\frac{1+\sqrt{41}}{2})) = p_n^2 + p_n q_n - 10q_n^2$.
Now from the continued fraction expansion of $\frac{-1+\sqrt{41}}{2}$, we get :

| $k$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| $a_k$ | 2 | 1 | 2 | 2 | 1 |
| $p_k$ | 2 | 3 | 8 | 19 | 27 |
| $q_k$ | 1 | 1 | 3 | 7 | 10 |
| $p_k^2 + p_k q_k - 10q_k^2$ | $-4$ | 2 | $-2$ | 4 | -1 |

Thus we see that the fundamental unit is $27 + 10\left(\frac{1+\sqrt{41}}{2}\right)$.

# Chapter 2

# Class Number

It is well known that for an algebraic number field $K$, $\mathcal{O}_K$ is a unique factorization domain if and only if it is a principal ideal domain. Our main aim is to find a way of measuring how far prime factorization fails to be unique in the case where $\mathcal{O}_K$ contains non-principal ideals for which we define the concept of ideal class group and class number.

## 2.1 Ideal Class Group and Class Number

Recall that an $\mathcal{O}_K$-module $I$ contained in $K$ is called a fractional ideal[1] of $\mathcal{O}_K$ if there exists $\alpha(\neq 0)$ in $\mathcal{O}_K$ such that $\alpha I \subseteq \mathcal{O}_K$. We assume that the set of all non-zero fractional ideals of $\mathcal{O}_K$ is an abelian group under multiplication of ideals(see Sec 8.3 of [Al-Wi]). This group will be denoted by $G(K)$. The subset of $G(K)$ consisting of all non-zero principal fractional ideals is a subgroup of $G(K)$ and will be denoted by $P(K)$. The group $G(K)/P(K)$ is called the **Ideal Class Group** or **Class Group** of $K$ and its members are be called **Ideal Classes** of $K$. The order of the class group of $K$ is called the **Class Number** of $K$. It is an important result that the class group is always a finite group. This result was first proved by Dedekind in 1871 in his first account of Ideal Theory. We shall prove it in the next section using modified Minkowski's lemma on complex linear forms which has been proved in Sec 1.2 .

Note that class number of an algebraic number field $K$ is 1 if and only if $\mathcal{O}_K$ is a principal ideal domain. Leonard Carlitz (1907-1999) has shown that class number of an algebraic number field $K$ is 1 or 2 if and only if whenever a non-zero non-unit element $\alpha \in \mathcal{O}_K$ can be written as $\alpha = u\pi_1 \dots \pi_s = u'\pi'_1 \dots \pi'_t$ with $u, u'$ units and $\pi_1, \dots, \pi_s, \pi'_1, \dots, \pi'_t$ prime elements of $\mathcal{O}_K$ then $s = t$(cf. [Car]).

[1] An ideal $I$ of $\mathcal{O}_K$ contained in $\mathcal{O}_K$ will sometimes be called an integral ideal of $\mathcal{O}_K$

## 2.2 Finiteness of Ideal Class Group

Let $K$ be an algebraic number field of degree $n = r + 2s$. As in previous chapter, the isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_n$ of $K$ into $\mathbb{C}$ are arranged so that $\sigma_1, \ldots, \sigma_r$ are real isomorphisms, $\sigma_{r+1}, \ldots, \sigma_{r+s}$ are non-real and $\sigma_{r+s+j} = \overline{\sigma}_{r+j}$ for $1 \leq j \leq s$ we denote $\sigma_i(\alpha)$ by $\alpha^{(i)}$. For a vector space basis $\{w_1, \ldots, w_n\}$ of $K$ over $\mathbb{Q}$, $D_{K/\mathbb{Q}}(w_1, \ldots, w_n)$ will stand for the square of the determinant of $n \times n$ matrix $[w_i^{(j)}]_{ij}$ ; if all $w_i \in \mathcal{O}_K$ and $A$ denotes the group $\mathbb{Z}w_1 + \cdots + \mathbb{Z}w_n$, then it can be easily proved that

$$D_{K/\mathbb{Q}}(w_1, \ldots, w_n) = [\mathcal{O}_K : A]^2 d_K \tag{2.1}$$

where $d_K$ denotes the discriminant of $K$ (see Thm 7.1.3 of [Al-Wi]).

We first prove the following theorem from which finiteness of class group will be deduced.

**Theorem 2.2.1.** *Let $K$ be an algebraic number field distinct from $\mathbb{Q}$. Then in every ideal class of $K$, there exists an ideal $B$ of $\mathcal{O}_K$ such that $N(B) < \sqrt{|d_K|}$, where $N(B)$ stands for the norm of $B$.*

*Proof.* Let $\mathcal{C}$ any ideal class of $K$, let $C$ be a fixed ideal belonging to $\mathcal{C}$. There exists an integral ideal $A$ such that $AC$ is a principal ideal. Let $\alpha_1, \ldots, \alpha_n$ be $\mathbb{Z}$-basis of $A$. Let $\sigma_1, \ldots, \sigma_r$ be all the real isomorphisms from $K$ to $\mathbb{C}$. Let $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ be the non-real isomorphisms of $K$ to $\mathbb{C}$ such that

$$\overline{\sigma}_{r+j} = \sigma_{r+s+j}, \ 1 \leq j \leq s.$$

Define the linear forms $L_1, L_2, \ldots, L_n$ by

$$L_i(x_1, x_2, \ldots, x_n) = \sigma_i(\alpha_1)x_1 + \sigma_i(\alpha_2)x_2 + \cdots + \sigma_i(\alpha_n)x_n$$

The absolute value of the determinant of these linear forms is

$$|det(\sigma_i(\alpha_j))| = \sqrt{|D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n)|}$$

which in view of equation (2.1) equals $[\mathcal{O}_K : A]\sqrt{|d_K|}$. Applying modified Minkowski's Lemma on complex linear forms (proved in section 1.2 ) taking

$$c_i = ([\mathcal{O}_K : A]\sqrt{|d_K|})^{\frac{1}{n}} \text{ for each } i, \tag{2.2}$$

we see that there exists rational integers $u_1, u_2, \ldots, u_n$ not all zero such that

$$|L_i(u_1, u_2, \ldots, u_n)| < c_i \text{ for all } i, \ 1 \leq i \leq n-1. \tag{2.3}$$

and

$$|L_n(u_1, u_2, \ldots, u_n)| \leq c_n \tag{2.4}$$

Now take $\alpha = u_1\alpha_1 + \cdots + u_n\alpha_n \in A,\ \alpha \neq 0$. So from (2.3) and (2.4), we obtain $|\sigma_i(\alpha)| < c_i$ , for $1 \leq i \leq n-1$ and $|\sigma_n(\alpha)| \leq c_n$; consequently keeping in mind that $K \neq \mathbb{Q}$ and using (2.2), we have

$$|N_{K/\mathbb{Q}}(\alpha)| < \prod_{i=1}^{n} c_i = [\mathcal{O}_K : A]\sqrt{|d_K|} = N(A)\sqrt{|d_K|} \tag{2.5}$$

Since $\alpha \in A$, there exist an integral ideal $B$ such that $\alpha\mathcal{O}_K = AB$. Recalling that $AC$ is a principal ideal we conclude that $C$ and $B$ lie in the same ideal class $\mathcal{C}$. In view of a basic result $|N_{K/\mathbb{Q}}(\alpha)| = N(\alpha\mathcal{O}_K)$(see Chapter 5 [Ta-St]), therefore we have $|N_{K/\mathbb{Q}}(\alpha)| = N(\alpha\mathcal{O}_K) = N(A)N(B)$. It follows (2.5) that $N(A)N(B) < N(A)\sqrt{|d_K|}$. So $N(B) < \sqrt{|d_K|}$. □

**Corollary 2.2.2.** *The group of ideal classes of an algebraic number field is finite.*

*Proof.* We know that for any integral ideal $B$, $N(B) \in B$ which implies that $B$ divides $N(B)\mathcal{O}_K$. Now by Theorem2.2.1, in every ideal class of $K$ there exists an ideal $B$ such that $N(B) < \sqrt{|d_K|}$. Thus $N(B)$ has only finitely many choices $1, 2, \ldots, \sqrt{|d_K|} - 1$ and $B$ being a divisor of $N(B)$ has only finitely many choices as every non-zero ideal of $\mathcal{O}_K$ can be uniquely written as a product of finitely many prime ideals (cf [Al-Wi]). So the number of ideal classes is finite. □

The following corollary is an immediate consequence of Theorem 2.2.1.

**Corollary 2.2.3.** *If $K \neq \mathbb{Q}$, then $|d_K| > 1$.*

Theorem 2.2.1 can be used to compute class number of $K$ for fields of small degree with small discriminant as is done in the solution of the following example.

**Example.** Find the class number of $\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-11})$.

**Solution.** We know that in every ideal class of $\mathbb{Q}(\sqrt{-1}$, there exists an integral ideal $B$ such that $N(B) < \sqrt{|d_K|}$. As $-1 \equiv 3 \bmod 4$, $d_K = -4$. So $N(B) = 1$ which implies that $B = \mathcal{O}_K$. Thus there is only one ideal class namely $P(K)$ i.e., class number of $K$ is 1.

When $K = \mathbb{Q}(\sqrt{-3})$, as $-3 \equiv 1 \bmod 4$, so $d_K = -3$. By Theorem 2.2.1 , in every ideal class of $K$ there exists an integral ideal $B$ such that $N(B) < \sqrt{3} < 2$. So $N(B) = 1$ which implies that $B = \mathcal{O}_K$. So there is only one ideal class namely $P(K)$ i.e., $|G(K)/P(K)| = 1$.

When $K = \mathbb{Q}(\sqrt{-7})$, as $-7 \equiv 1 \bmod 4$, so $d_K = -7$. So by Theorem 2.2.1 , in every ideal class of $K$ there exists an integral ideal $B$ such that $N(B) < \sqrt{7} < 3$. So $N(B) = 1$

or 2. If $N(B) = 1$, then $B = \mathcal{O}_K$ and class of $B$ is $P(K)$. Now we consider the possibility when $N(B) = 2$. Since $-7 \equiv 1 \bmod 8$.. By result Theorem 10.2.1 in [Al-Wi], 2 factorizes as $2\mathcal{O}_K = \wp_2\wp_2'$ with $N(\wp_2) = N(\wp_2') = 2$. So $B = \wp_2$ or $\wp_2'$. To check whether $\wp_2$ (and hence $\wp_2'$) is principal or not, i.e., whether there exist $a, b \in \mathbb{Z}$ such that

$$2 = \left(a + \frac{b}{2}(1 + \sqrt{-7})\right)\left(a + \frac{b}{2}(1 - \sqrt{-7})\right).$$

Therefore $8 = (2a + b)^2 + 7b^2$ where $a = 0$ and $b = 1$ work. We may take $\wp_2 = \frac{1+\sqrt{-7}}{2}\mathcal{O}_K$ and $\wp_2' = \frac{1-\sqrt{-7}}{2}\mathcal{O}_K$. So $\wp_2$ and $\wp_2'$ are principal ideals. Thus in every ideal class of $K$ lies a principal ideal. So $|G(K)/P(K)| = 1$.

When $K = \mathbb{Q}(\sqrt{-11})$, as $-11 \equiv 1 \bmod 4$, so $d_K = -11$. So by Theorem 2.2.1, in every ideal class of $K$ there exists an integral ideal $B$ such that $N(B) < \sqrt{11} < 4$. So $N(B) = 1$ or 2 or 3. If $N(B) = 1$, then $B = \mathcal{O}_K$ and class of $B$ is $P(K)$. Since $-11 \equiv 5 \bmod 8$. In view of basic result (see Theorem 2.2.1 in [Al-Wi]) $2\mathcal{O}_K = \wp_2$ with $N(\wp_2) = 4$ with $\wp_2$ prime ideal. So in case $K = \mathbb{Q}(\sqrt{-11})$, there is no integral ideal of norm 2. Now we consider the possibility when $N(B) = 3$. Since $-11 \equiv 1 \bmod 3$. So 3 factorizes as $3\mathcal{O}_K = \wp_3\wp_3'$ with $N(\wp_3) = N(\wp_3') = 3$. Since there exists an ideal of norm 3, we now try to see whether $\wp_3$ is principal or not i.e., whether there exists integers $a, b \in \mathbb{Z}$ such that $N(a + b(\frac{1+\sqrt{-11}}{2})) = 3$. Thus $(a + \frac{b}{2})^2 + (\frac{\sqrt{-11}b}{2})^2 = 3$. We can rewrite this as $12 = (2a + b)^2 + 11b^2$. Note that $b = 1$ and $a = 0$ works. We may take $\wp_3 = \frac{1+\sqrt{-11}}{2}\mathcal{O}_K$ and $\wp_3' = \frac{1-\sqrt{-11}}{2}\mathcal{O}_K$. So in every ideal class of $\mathbb{Q}(\sqrt{-11})$ there exists a principal ideal. Hence class number is 1.

## 2.3 Minkowski's Convex Body Theorem

Next our aim is to give an improvement of Theorem 2.2.1. It will be shown that given an algebraic number field $K$ of degree $n = r+2s$, there exists a constant $C_K = \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|d_K|}$ such that in every ideal class of $K$, there exists an integral ideal $B$ with $N(B) \leq C_K$. This constant will be useful for computing quickly the class number of some algebraic number fields and is known as Minkowski's constant. This constant will be obtained using Minkowski's theorem on complex bodies which will be proved in this section after giving some definitions and a couple of lemmas.

**Definition.** A set $S$ contained in $\mathbb{R}^n$ is said to be convex if whenever $x, y \in S$, then $\lambda x + (1 - \lambda)y \in S$ for all $\lambda \in \mathbb{R}$ such that $0 \leq \lambda \leq 1$.

**Definition.** A set $S$ contained in $\mathbb{R}^n$ is said to be centrally symmetric whenever $x \in S$, then $-x \in S$.

**Example 1.** We know that a sphere S in $\mathbb{R}^n$ is always convex, i.e., the set $S = \{\ x \in \mathbb{R}^n\ :\ ||x-a|| < r\ \}$ is convex because if $||x-a|| < r$ and $||y-a|| < r$, we obtain $||\lambda x + (1-\lambda)y - a|| \leq \lambda||x-a|| + (1-\lambda)||y-a|| < \lambda r + (1-\lambda)r = r$.

**Example 2.** Let $A = (a_{ij})_{n\times n}$ be a non-singular matrix. The set $P = \{x\ :\ |a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n| < c_1,\ \ldots\ , |a_{n1}x_1 + \cdots + a_{nn}x_n| < c_n\ \}$ where $c_1, c_2, \ldots, c_n$ are fixed positive constants, is a convex set.

*Proof.* Define $L_i(x_1, x_2, \ldots, x_n) = \sum_{j=1}^{n} a_{ij}x_j,\ 1 \leq i \leq n$. Suppose $x, y \in P$ and $\lambda$ such that $0 \leq \lambda \leq 1$. We have $|L_i(x)| < c_i$ and $|L_i(y)| < c_i$ for $1 \leq i \leq n$. Now

$$\begin{aligned} |L_i(\lambda x + (1-\lambda)y)| &= |\lambda L_i(x) + (1-\lambda)L_i(y)| \\ &\leq \lambda|L_i(x)| + (1-\lambda)|L_i(y)| \\ &< \lambda c_i + (1-\lambda)c_i = c_i \end{aligned}$$

for all $i$. Thus $\lambda x + (1-\lambda)y \in P$. □

**Definition.** By an $n$-dimensional lattice in $\mathbb{R}^n$ we mean a subgroup of $\mathbb{R}^n$ which is generated as a group by $n$ linearly independent vectors over $\mathbb{R}$. Such a set of generators is called a basis of the lattice. If $\{A_1, A_2, \ldots, A_n\}$ and $\{B_1, B_2, \ldots, B_n\}$ are two basis of the lattice $\mathfrak{L}$, then there exists a unimodular matrix $U$ such that

$$\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{bmatrix} = U_{n\times n} \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{bmatrix}$$

So the absolute value of the determinant of the matrix with row vectors $A_1, A_2, \ldots, A_n$ is well defined. It is called the determinant of $\mathfrak{L}$.

For example $\mathfrak{L}_0 = \{\ (a_1, \ldots, a_n)\ :\ a_i \in \mathbb{Z}\}$ is a lattice in $\mathbb{R}^n$ called the Fundamental lattice or integral lattice and has got basis $(1, 0, \ldots, 0), (0, 1, 0, \ldots, 0),\ \ldots\ , (0, 0, \ldots, 1)$. Clearly $det(\mathfrak{L}_0) = 1$.

**Definition.** Let $\mathfrak{L}$ be a lattice in $\mathbb{R}^n$ with basis $\{u_1, u_2, \ldots, u_n\}$. The set $T$ of points of the form $\{a_1u_1 + \cdots + a_nu_n \mid 0 \leq a_i < 1 \text{ for } 1 \leq i \leq n\ \}$ is called a fundamental parallelepiped of the lattice $\mathfrak{L}$.

*Remark.* A fundamental parallelepiped $T$ of a lattice $\mathfrak{L}$ is not uniquely determined by $\mathfrak{L}$. It depends on the choice of basis of $\mathfrak{L}$. Observe that determinant of a lattice $\mathfrak{L}$ equals the volume of a fundamental parallelepiped $T$ of $\mathfrak{L}$.

**Minkowski's Theorem on Convex bodies for general lattice.** Let $\mathfrak{L}$ be an $n$-dimensional lattice in $\mathbb{R}^n$ with the volume of a fundamental parallelepiped of $\mathfrak{L}$ given by $\Delta$. Let $S$ be a bounded, centrally symmetric convex subset of $\mathbb{R}^n$ with $Vol(S) > 2^n\Delta$. Then $S$ contains at least one non-zero vector of $\mathfrak{L}$.

For proving Minkowski's theorem on convex bodies, we first prove some lemmas.

**Lemma 2.A.** Every bounded subset of $\mathbb{R}^n$ contains only finitely many points of a lattice $\mathfrak{L}$.

*Proof.* It is enough to prove the lemma when $\mathfrak{L}$ is an $n$-dimensional lattice in $\mathbb{R}^n$. Let $\{u_1, u_2, \ldots, u_n\}$ be a basis of $\mathfrak{L}$. Consider the linear transformation $\psi : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ defined by $\psi((x_1, x_2, \ldots, x_n)) = x_1u_1 + \cdots + x_nu_n$. Since $\{u_1, u_2, \ldots, u_n\}$ is linearly independent over $\mathbb{R}$, $\psi$ is invertible. its inverse is continuous. Let $S$ be a bounded set in $\mathbb{R}^n$. Then $S$ is contained in a compact set $S_0$. But $\psi^{-1}(S_0)$ is compact and hence bounded. So $\psi^{-1}(S)$ is also bounded. Hence $\psi^{-1}(S)$ contains only finitely many points in $\mathbb{Z}^n$; so $S$ contains only finitely many points of $\psi(\mathbb{Z}^n) = \mathfrak{L}$. □

**Lemma 2.B.** If $T$ is a fundamental parallelepiped of an $n$-dimensional lattice $\mathfrak{L}$, then the sets $T_z = T + z$, where $z$ runs through all the points of $\mathfrak{L}$, are pairwise disjoint and fill the entire space $\mathbb{R}^n$.

*Proof.* Let $\{u_1, u_2, \ldots, u_n\}$ be a basis of $\mathfrak{L}$ used to construct the parallelepiped $T$. Let $x = c_1u_1 + \cdots + c_nu_n, c_i \in \mathbb{R}$, be any vector in $\mathbb{R}^n$. Write $c_i = k_i + \alpha_i,\ k_i \in \mathbb{Z},\ \alpha_i \in \mathbb{R},\ 0 \leq \alpha_i < 1$. Set $z = \sum_{i=1}^{n} k_iu_i,\ u = \sum_{i=1}^{n} \alpha_iu_i$, we have $x = z + u$ with $z \in \mathfrak{L}$ and $u \in T$. It can be easily seen that if $z \neq z'$ are in $\mathfrak{L}$, then $T_z \cap T_{z'} = \emptyset$. □

**Lemma 2.C.** Let $T$, $\mathfrak{L}$ be as in the above lemma. Then for any given bounded set $B \subseteq \mathbb{R}^n$, there are only finitely many translates $T_z, z \in \mathfrak{L}$, whose intersection with $B$ is non-empty.

*Proof.* Let $\{u_1, u_2, \ldots, u_n\}$ be a basis of $\mathfrak{L}$ used to construct $T$. Set $d = ||u_1|| + \cdots + ||u_n||$, then for any vector $u = \alpha_1u_1 + \cdots + \alpha_nu_n \in T$, we have

$$||u|| \leq \alpha_1||u_1|| + \cdots + \alpha_n||u_n|| < d \tag{2.6}$$

Since $S$ is bounded, there exists $r > 0$ such that $||x|| \leq r$ for all $x \in S$. Let $z \in \mathfrak{L}$ be such that $T_z \cap S \neq \emptyset$, say $x \in T_z \cap S$. So $x = z + u,\ u \in T$ implies that $||z|| \leq ||x|| + ||u|| \leq r + d$ by (2.6). This shows that $z$ belongs to a bounded set which is a sphere with centre at origin and radius $r + d$. So by Lemma 2.A, there are only finitely many choices of $z$. □

**Proof of Minkowski's Theorem on Convex Bodies.**
The proof is divided into two steps.
**Step 1.** In this step, we prove that when a bounded subset $Y$ of $\mathbb{R}^n$ has the property that all of its translates $Y + z$ by vectors of $\mathfrak{L}$ are pairwise disjoint, then $Vol(Y) \leq \Delta$. Let $T$ be a fundamental parallelepiped of $\mathfrak{L}$. By Lemma 2.B,

$$Vol(Y) = \sum_{z \in \mathfrak{L}} Vol(Y \cap T_{-z}); \tag{2.7}$$

the sum on right hand side of above equation contains only a finitely number of non-zero terms by virtue of Lemma 2.C. Rewrite (2.7) as

$$Vol(Y) = \sum_{z \in \mathfrak{L}} Vol((Y + z) \cap T). \tag{2.8}$$

By assumption of Step 1, the translates $Y + z,\ z \in \mathfrak{L}$ are pairwise disjoint. Therefore the sum on the right hand side of (2.8) is $\leq Vol(T) = \Delta$ and hence the assertion of Step 1 is proved.
**Step 2.** We now prove the theorem. By hypothesis $Vol(\frac{1}{2}S) = \frac{Vol(S)}{2^n} > \Delta$. By Step 1, there exist at least two translations $\frac{1}{2}S + z,\ \frac{1}{2}S + z'$ with non-empty intersection, say there exist $x, x'$ in $S$ such that $\frac{1}{2}x + z = \frac{1}{2}x' + z'$. So $\frac{1}{2}(x - x') = z - z' \in \mathfrak{L}$. Since $S$ is centrally symmetric $-x' \in S$. Also $S$ being convex $\frac{1}{2}(x - x') \in S$. So $S$ contains a non-zero vector of $\mathfrak{L}$.

**Modified Minkowski's Theorem for Convex bodies.** Let $\mathfrak{L}$ be an $n$-dimensional lattice in $\mathbb{R}^n$ with determinant $\Delta$. Let $S$ be a bounded, convex centrally symmetric subset of $\mathbb{R}^n$ with $Vol(S) = 2^n\Delta$. Then the closure of $S$ contains a non-zero vector of $\mathfrak{L}$.

*Proof.* Let $\overline{S}$ denote the closure of $S$. For $y \in \mathbb{R}^n$, let $d(y, S)$ denote the distance of $y$ from $S$ defined by $d(y, S) = Inf\{\ ||y-x|| \mid x \in S\ \}$. Suppose to the contrary $\overline{S}$ does not contain any non-zero vector of $\mathfrak{L}$. Let $r$ be a positive real number such that $||x|| < r$ for all $x \in S$. Fix any $\epsilon > 0$. Consider the set $(1 + \epsilon)S$. Since $Vol((1 + \epsilon)S) = (1 + \epsilon)^n Vol(S) > 2^n\Delta$, it follows that $(1 + \epsilon)S$ contains a non-zero vector of $\mathfrak{L}$ by Minkowski's Theorem. Write

$$(1 + \epsilon)S \cap L\backslash\{0\} = \{y_1, y_2, \ldots, y_k\}. \tag{2.9}$$

Since $y_i \notin \overline{S}$ n view of our assumption, it follows that the distance $d(y_i, S) > 0$. So there exist $\epsilon_0 > 0$ such that

$$d(y_i, S) > \epsilon_0 \text{ for } 1 \leq i \leq k. \tag{2.10}$$

Choose $\epsilon_1 > 0$ such that $\epsilon_1 < \epsilon$ and $\epsilon_1 < \frac{\epsilon_0}{r}$. then $(1 + \epsilon_1)S \subseteq (1 + \epsilon)S$ in view of the fact that $\lambda S \subseteq S$ for $0 < \lambda < 1$ which can be verified keeping in mind that $S$ is convex

and $0 \in S$. In view of Minkowski's Theorem $(1+\epsilon_1)S \cap \mathfrak{L}\backslash\{0\} \neq \emptyset$ and it is a subset of $\{y_1, y_2, \ldots, y_k\}$ by (2.9). So there exists $i$ such that $y_i = (1+\epsilon_1)x$ for some $x \in S$. Then $d(y_i, S) = d(1+\epsilon_1)x,\ x) = \epsilon_1||x|| \leq \epsilon_1 r < \epsilon_0$ which contradicts (2.10) and proves the theorem. □

## 2.4 Minkowski's Bound

We now give an improvement of Theorem 2.2.1.

**Theorem 2.4.1.** *Let $K$ be an algebraic number field of degree $n = r + 2s$, where $r$ is the number of real isomorphisms of $K$ and $2s$ is the number of non-real isomorphisms of $K$. Then in every ideal class of $K$ there exists an integral ideal $B$ such that*

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

For proving the above theorem , we need the following lemmas.

**Lemma 2.4.2.** *Let $X = X_t = \{\ (x_1, \ldots, x_r, y_{r+1}, z_{r+1}, \ldots, y_{r+s}, z_{r+s}) \ : \ \sum_{i=1}^{r} |x_i| + 2\sum_{j=r+1}^{r+s} \sqrt{y_j^2 + z_j^2} < t\ \}$ where $t$ is a fixed positive real number then $X_t$ is a bounded open convex subset of $\mathbb{R}^n$, $n = r + 2s$.*

*Proof.* All co-ordinates are bounded by $t$, so the boundedness is clear. Since the inverse image of an open set under a continuous map is open, $X_t$ is open. Now we prove convexity. Let $\lambda$ be any real number $0 \leq \lambda \leq 1$. Let $x, x' \in X$. We need to show that $\lambda x(1-\lambda)x' \in X$ i.e., to prove

$$\sum_{i=1}^{r} |\lambda x_i + (1-\lambda)x_i'| + 2\sum_{j=r+1}^{r+s} \sqrt{(\lambda y_j + (1-\lambda)y_j')^2 + (\lambda z_j + (1-\lambda)z_j')^2} < t. \qquad (2.11)$$

The left hand side of (2.11) is less than or equal to

$$\sum_{i=1}^{r} |\lambda x_i + (1-\lambda)x_i'| + 2\sum_{j=r+1}^{r+s} \sqrt{(\lambda^2(y_j^2 + z_j^2) + (1-\lambda)^2({y_j'}^2 + {z_j'}^2) + 2\lambda(1-\lambda)(y_j y_j' + z_j z_j')}.$$

By Cauchy- Schwartz inequality

$$|y_j y_j' + z_j z_j'| \leq \sqrt{y_j^2 + z_j^2}\sqrt{{y_j'}^2 + {z_j'}^2}.$$

So left hand side of (2.11) $\leq \sum_{i=1}^{r} |\lambda x_i + (1-\lambda)x_i'| + 2\sum_j \left(\lambda\sqrt{y_j^2+z_j^2} + (1-\lambda)\sqrt{{y_j'}^2+{z_j'}^2}\right)$

$= \lambda\left(\sum_{i=1}^{r}|x_i| + 2\sum_j\sqrt{y_j^2+z_j^2}\right) + (1-\lambda)\left(\sum_{i=1}^{r}|x_i'| + 2\sum_j\sqrt{{y_j'}^2+{z_j'}^2}\right) < \lambda t + (1-\lambda)t = t.$

Therefore $\lambda x + (1-\lambda)x' \in X$ and hence $X$ is convex. □

**Lemma 2.4.3.** *If $X = X_t$ is as in Lemma 2.4.2, then $Vol(X_t) = 2^r(\frac{\pi}{2})^s\frac{t^n}{n!}$.*

**Lemma 2.4.4.** ***( Arithmetic-O-Geometric Inequality)*** *If $a_1, \ldots, a_n$ are positive real numbers, then*

$$\sqrt[n]{a_1.\ldots.a_n} \leq \frac{a_1 + \cdots + a_n}{n} \tag{2.12}$$

These lemmas shall be proved after proving Theorem 2.4.1.

**Proof of Theorem 2.4.1** Let $\mathcal{C}$ be any ideal class in $K$. Let $C$ be any fixed ideal in class $\mathcal{C}$. There exists an integral ideal $A$ of $\mathcal{O}_K$ such that $AC$ is a principal ideal. Let $\sigma_1, \ldots, \sigma_r$ be all the real isomorphisms of $K$ and $\sigma_{r+1}, \ldots, \sigma_{r+2s}$ be non-real isomorphisms of $K$ arranged so that $\overline{\sigma_{r+j}} = \sigma_{r+s+j},\ 1 \leq j \leq s$. Consider the homomorphism

$$F : \mathcal{O}_K \longrightarrow \mathbb{R}^n,\ n = r + 2s$$

defined by

$$F(\alpha) = (\,\sigma_1(\alpha)\,, \ldots,\, \sigma_r(\alpha)\,,\, Re(\sigma_{r+1}(\alpha))\,,\, Im(\sigma_{r+1}(\alpha))\,, \ldots,\, Re(\sigma_{r+s}(\alpha))\,,\, Im(\sigma_{r+s}(\alpha))\,).$$

Clearly $F$ is a homomorphism of additive groups and is one-one. So $F(A)$ is a subgroup of $\mathbb{R}^n$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be $\mathbb{Z}$-basis of $A$. So $F(\alpha_1), \ldots, F(\alpha_n)$ form a $\mathbb{Z}$-basis of $F(A)$. Therefore $F(A)$ will be a lattice in $\mathbb{R}^n$ once we show that $F(\alpha_1), \ldots, F(\alpha_n)$ form a linearly independent set over $\mathbb{R}$. This is verified if we show that the matrix with row vectors $F(\alpha_1), \ldots, F(\alpha_n)$ has determinant non-zero. The absolute value of the determinant will be the determinant of the lattice $F(A)$.

Let $d$ denote the determinant of the matrix $P$ with row vectors $F(\alpha_1), \ldots, F(\alpha_n)$. We write $\sigma_i(\alpha_j) = x_j^{(i)},\ 1 \leq i \leq r$ and $\sigma_{r+i}(\alpha_j) = y_j^{(r+i)} + \iota z_j^{(r+i)}$ for $1 \leq i \leq s$, where $\iota$ stands for $\sqrt{-1}$.

$$P = \begin{bmatrix} x_1^{(1)} & \cdots & x_1^{(r)} & y_1^{(r+1)} & z_1^{(r+1)} & \cdots & y_1^{(r+s)} & z_1^{(r+s)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n^{(1)} & \cdots & x_n^{(r)} & y_n^{(r+1)} & z_n^{(r+1)} & \cdots & y_n^{(r+s)} & z_n^{(r+s)} \end{bmatrix}$$

To the $(r+1)^{th}$ column of $P$ add $\iota(r+2)^{th}$ column, then in the new matrix multiply the $(r+2)^{th}$ column by $-2\iota$ and to it add the $(r+1)^{th}$ column. Repeating this process with

successive pairs of columns, we obtain

$$(-2\iota)^s d = det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_r(\alpha_1) & \sigma_{r+1}(\alpha_1) & \sigma_{r+s}(\alpha_1) & \overline{\sigma_{r+1}(\alpha_1)} & \cdots & \overline{\sigma_{r+s}(\alpha_1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_r(\alpha_n) & \sigma_{r+1}(\alpha_n) & \sigma_{r+s}(\alpha_n) & \overline{\sigma_{r+1}(\alpha_n)} & \cdots & \overline{\sigma_{r+s}(\alpha_n)} \end{bmatrix}$$

Taking square on both sides of the above equation and in view of equation (2.1), we have $(-2\iota)^{2s}d^2 = D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = d_K[\mathcal{O}_K : A]^2 = d_K N(A)^2$. Therefore $|d| = \frac{\sqrt{|d_K|}N(A)}{2^s} \neq 0$. This is the determinant of the lattice $F(A)$. Now we shall choose a real number $t_0 > 0$ in such a way that

$$V(X_{t_0}) = 2^n|d| = \frac{2^n\sqrt{|d_K|}N(A)}{2^s} \tag{2.13}$$

In view of Lemma 2.4.3, $t_0$ is such that $2^s(\frac{\pi}{2})^s\frac{{t_0}^n}{n!} = \frac{2^n\sqrt{|d_K|}N(A)}{2^s}$. Thus

$${t_0}^n = \left(\frac{4}{\pi}\right)^s n!\sqrt{|d_K|}N(A) \tag{2.14}$$

So by modified Minkowski's theorem, there exists a non-zero vector (say) $F(\alpha)$ in the lattice $F(A)$ such that $F(\alpha)$ belongs to the closure $\overline{X_{t_0}}$ of $X_{t_0}$, i.e., there exists a non-zero $\alpha \in A$ such that the vector

$( \sigma_1(\alpha), \ldots, \sigma_r(\alpha), Re(\sigma_{r+1}(\alpha)), Im(\sigma_{r+1}(\alpha)), \ldots, Re(\sigma_{r+s}(\alpha)), Im(\sigma_{r+s}(\alpha)) )$

belongs to $\overline{X_{t_0}}$. It implies that $\sum_{i=1}^{r}|\sigma_i(\alpha)| + 2\sum_{j=r+1}^{r+s}|\sigma_j(\alpha)| \leq t_0$. By Arithmetic-O-Geometric inequality (proved in Lemma 2.4.4)

$$\left(\prod_{i=1}^{r}|\sigma_i(\alpha)|\prod_{j=r+1}^{r+s}|\sigma_j(\alpha)|^2\right)^{\frac{1}{n}} \leq \frac{\sum_{i=1}^{r}|\sigma_i(\alpha)| + 2\sum_{j=r+1}^{r+s}|\sigma_j(\alpha)|}{n} \leq \frac{t_0}{n}.$$

The above inequality implies by virtue of equation (2.14) that

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{{t_0}^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}N(A) \tag{2.15}$$

Recall that $\alpha \in A$. So there exists an integral ideal $B$ such that $\alpha\mathcal{O}_K = AB$. Also $AC$ is principal. Therefore $B$ and $C$ belong to the same ideal class. By virtue of (2.15), $N(A)N(B) = |N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}N(A)$. So $N(B) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^s\sqrt{|d_K|}$.

**Proof of Lemma 2.4.3.** We shall prove that

$$Vol(X_t) = 2^r \left(\frac{\pi}{2}\right)^s \frac{t^n}{n!} \tag{2.16}$$

by induction on $r+s$. In the case of $r=1, s=0$ and $r=0, s=1$, (2.16) can be easily verified. Assume now that (2.16) holds for $r=a, s=b$, $a$ and $b$ are non-negative integers. Then for $r=a+1, s=b$, we have

$$\begin{aligned} V(X_t) &= 2\frac{2^{a-b}\pi^b}{(a+2b)!}\int_0^t (t-x_{a+1})^{a+2b}\, dx_{a+1} \\ &= -\frac{2^{a-b+1}\pi^b}{(a+2b)!}\frac{(t-x_{a+1})^{a+2b+1}}{a+2b+1}\Big|_0^t \\ &= \frac{2^{a-b+1}\pi^b}{(a+2b+1)!}t^{a+2b+1} \end{aligned}$$

Similarly for $r=a, s=b+1$, we get $V(X_t) = \frac{2^{a-b}\pi^b}{(a+2b)!}\int\int_{y^2+z^2\le\frac{t^2}{4}} (\, t-2\sqrt{(y^2+z^2)}\,)^{a+2b}\, dydz$.

Put $y = \mathrm{r}\cos\theta,\ z = \mathrm{r}\sin\theta$.

$$\begin{aligned} V(X_t) &= \frac{2^{a-b}\pi^b}{(a+2b)!}\int_0^{2\pi}\int_0^{\frac{t}{2}} (t-2\mathrm{r})^{a+2b}\mathrm{r}d\mathrm{r}d\theta \\ &= (-1)^{a+2b}\frac{2^{a-b}\pi^b}{(a+2b)!}2\pi\int_0^{\frac{t}{2}} (2\mathrm{r}-t)^{a+2b}\mathrm{r}d\mathrm{r}d\theta \\ &= (-1)^{a+2b}\frac{2^{a-b}\pi^b}{(a+2b)!}2\pi\left\{\frac{(2\mathrm{r}-t)^{a+2b+1}}{2(a+2b+1)}\mathrm{r} - \int\frac{(2\mathrm{r}-t)^{a+2b+1}}{2(a+2b+1)}d\mathrm{r}\right\}\Big|_o^{\frac{t}{2}} \\ &= (-1)^{a+2b}\frac{2^{a-b}\pi^b}{(a+2b)!}2\pi\frac{(-t)^{a+2b+2}}{4(a+2b+1)(a+2b+2)} \\ &= \frac{2^{a-b-1}\pi^{1+b}}{(a+2b+2)!}t^{a+2b+2} \end{aligned}$$

So the formula follows by induction.

**Proof of Lemma 2.4.4.** We first prove (2.12) when $n$ is a power of 2. For $n=2$, the

inequality (2.12) is clear because $(\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$. Now we verify it for $n = 4$.

$$\sqrt[4]{a_1 \dots a_4} \leq \frac{\sqrt{a_1 a_2} + \sqrt{a_3 a_4}}{2} \leq \frac{a_1 + a_2 + a_3 + a_4}{4}$$

Suppose (2.12) is true for $2^{k-1}$. To verify for $n = 2^k$, we have by induction

$$\begin{aligned} \sqrt[2^k]{a_1 \dots a_{2^k}} &\leq \frac{\sqrt{a_1 a_2} + \dots + \sqrt{a_{2^k-1} a_{2^k}}}{2^{k-1}} \\ &\leq \frac{a_1 + a_2 + \dots + a_{2^k-1} + a_{2^k}}{2^k} \end{aligned}$$

To prove (2.12) for general $n$, clearly it is enough to prove that if $b_1, \dots, b_n$ are positive real numbers such that $\prod_{i=1}^{n} b_i = 1$, then $b_1 + \dots + b_n \geq n$. This has been proved in above paragraph when $n$ is a power of 2. Let $k$ be such that $n < 2^k$. Set

$$b_{n+1} = \dots = b_{2^k} = 1$$

Therefore, $\sum_{i=1}^{2^k} b_i \geq 2^k$ and hence $\sum_{i=1}^{n} b_i \geq 2^k - (2^k - n) = n$.

We now give some applications of Theorem 2.4.1.

**Example.** Prove that the class number of $K = \mathbb{Q}(\theta)$ where $\theta$ satisfies the equation $x^3 - x - 1$ is one.
**Solution.** One can easily check that $D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -23$. So $d_K = -23$ and $\{1, \theta, \theta^2\}$ is an integral basis of $K$ in view of equation (2.1). Since the discriminant is negative, all the isomorphisms of $K$ into complex numbers can't be real. So $r = 1, s = 1$. By Theorem 2.4.1, in every ideal class of $K$, there exists an integral ideal $B$ such that $N(B) \leq \left(\frac{4}{\pi}\right)^s \frac{3!}{3^3}\sqrt{23}$. So $N(B) \leq \frac{4}{\pi}\frac{6}{27}\sqrt{23} < 2$. So $N(B) = 1$ then $B = \mathcal{O}_K$. Hence there is only one ideal class namely $P(K)$. Therefore $|G(K)/P(K)| = 1$.

**Example.** Prove that the class number of $\mathbb{Q}(\sqrt{-23})$ is 3.
**Solution.** Let $K = \mathbb{Q}(\sqrt{-23})$. Note that $r = 0$ and $s = 1$. As $-23 \equiv 1 \bmod 4$, $d_K = -23$. By Theorem 2.4.1, in every ideal class of $K$, there exists an integral ideal $B$ with $N(B) \leq \left(\frac{4}{\pi}\right)\frac{2!}{2^2}\sqrt{23} < 4$. If $N(B) = 1$ then $B = \mathcal{O}_K$. Now for $N(B) = 2$, we first check whether there is an ideal of norm 2 or not. Consider the splitting of prime 2 in $K$. As $-23 \equiv 1 \bmod 8$, $2\mathcal{O}_K = \wp_2\wp_2'$ with $N(\wp_2) = N(\wp_2') = 2$. Now we check if $\wp_2$ is

principal or not. Let it is principal. Then $\wp_2 = \alpha\mathcal{O}_K$, where $\alpha = a + b(\frac{1+\sqrt{-23}}{2}),\ a, b \in \mathbb{Z}$. Thus $2 = N(\wp_2) = |N_{K/\mathbb{Q}}(\alpha)|$ which implies that $8 = (2a+b)^2 + 23b^2$ which does not have any solution in $\mathbb{Z}$. Therefore $\wp_2, \wp_2'$ are not principal.

Now for $N(B) = 3$, firstly we check that whether there is an ideal of norm 3 or not. Consider the splitting of prime 3, firstly we check that whether there is an ideal of norm 3 or not. Consider the splitting of prime 3 in $\mathcal{O}_K$ as $-23 \equiv 1 \bmod 3$, $3\mathcal{O}_K = \wp_3\wp_3'$ with $N(\wp_3) = N(\wp_3') = 3$. If $\wp_3$ is principal, then $\wp_3 = \alpha\mathcal{O}_K$, where $\alpha = a+b(\frac{1+\sqrt{-23}}{2}),\ a'b \in \mathbb{Z}$. Thus $3 = N(\wp_2) = |N_{K/\mathbb{Q}}(\alpha)|$ which implies that $12 = (2a + b)^2 + 23b^2$ which does not have any solution in $\mathbb{Z}$. Therefore $\wp_3, \wp_3'$ are not principal.

Since $N(\frac{1+\sqrt{-23}}{2}) = 6$, it follows that $\left\langle \frac{1+\sqrt{-23}}{2} \right\rangle = \wp_3\wp_2'$(say). So $\wp_2$ and $\wp_3$ lie in the same class and hence $\wp_2'$ and $\wp_3'$ lie in the same ideal class. Now we show that $\wp_2$ and $\wp_2'$ lie in the different classes for otherwise $\wp_2^2 = \left\langle c + d(\frac{1+\sqrt{-23}}{2}) \right\rangle$ which on taking norm show that $16 = (2c+d)^2 + 23d^2$; this is possible only when $c = \pm 1$ and $d = 0$, i.e., $\wp_2^2$ is an ideal generated by 2 which is not so. Therefore there are three classes $P(K), \wp_2P(K), \wp_2'P(K)$.

# Chapter 3

# Dirichlet's Class Number Formula and its Applications

The class number $h_K$ of an algebraic number field $K$ plays an important role in the arithmetic of $K$. Thus one would like to have an explicit formula in terms of simpler values which depend on the field $K$. Since all ideals of $\mathcal{O}_K$ are products of prime ideals and number of prime ideals of $\mathcal{O}_K$ is infinite, to compute $h_K$ in finite number of steps, one has to use some infinite processes for e.g. infinite series, infinite products and another analytic concepts as has been done in the present chapter.

## 3.1 Statement of Dirichlet's Class Number Formula and Ideal Theorem

Consider the series $\sum_A \frac{1}{N(A)^s}$ where $A$ runs over all non-zero ideals of $\mathcal{O}_K$. We shall prove that this series converges uniformly on compact subsets of $(1, \infty)$. The sum function will be denoted by $\zeta_K(s)$ and is called Dedekind Zeta function of $K$.

With the above notations, we shall prove the following theorem which is usually attributed to Dirichlet, although he originally proved it only for quadratic fields. The formula for the limit in the theorem below was proved by Dedekind.

**Theorem 3.1.1.** *Let $K$ be an algebraic number field of degree $n = r + 2s$ with class number $h$, where $r$ is the number of real isomorphisms of $K$ and $2s$ is the number of non-real isomorphisms of $K$ into $\mathbb{C}$. Let $R$ stand for regulator of $K$ and $d_K$ stand for discriminant of $K$. The series $\sum_A \frac{1}{N(A)^s}$ converges uniformly for all compact subset of $(1, \infty)$ and represents a continuous function of $s$ in $(1, \infty)$, where $A$ runs over all non-*

*zero integral ideals of $\mathcal{O}_K$. If we denote $\zeta_K(s) = \sum_A \frac{1}{N(A)^s}$ then*

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = h\frac{2^{r+s}\pi^s R}{m\sqrt{|d_K|}} \tag{3.1}$$

*where $m$ is the number of roots of unity in $K$.*
*The above formula is called* ***Dirichlet Class Number Formula****.*

For proving the above theorem, we shall first prove the following ideal theorem by Dedekind.

**Theorem 3.1.2. (Ideal Theorem)** *Let $K$ be an algebraic number field of degree $n$ and $r, s, R, d_K, m$ be as in the above theorem. Let $\mathcal{C}$ be an ideal class of $K$. Let $\mathcal{Z}(T, \mathcal{C})$ be number of integral ideals of $\mathcal{C}$ whose norm is less than or equal to $T$. Then*

$$\lim_{T\to\infty}\frac{\mathcal{Z}(T,\mathcal{C})}{T} = \frac{2^{r+s}\pi^s R}{m\sqrt{|d_K|}}$$

## 3.2 Proof of Ideal Theorem

For a subset $S$ of $\mathbb{R}^n$ and for any real number $T$, we denote by $S(T)$ the set $\{(Tx_1, \ldots, Tx_n) | (x_1, \ldots, x_n) \in S\}$ contained in $\mathbb{R}^n$.

We first prove a lemma.

**Lemma 3.2.1.** *Let $S$ be a bounded subset of $\mathbb{R}^n$. Suppose volume of $S$ (denoted by $V$) exists. For any real number $T > 0$, let $N(T)$ be a number of points in $S(T)$ with integral co-ordinates. Then $\lim_{T\to\infty}\frac{N(T)}{T^n} = V$*

*Proof.* Clearly a point $(y_1, y_2, \ldots, y_n) \in S(T)$ if and only if $(\frac{y_1}{T}, \ldots, \frac{y_n}{T}) \in S$. A family $F_T$ of all cubes $C_T$ of the type $C_T = \{(y_1, \ldots, y_n) | \frac{z_i}{T} \leq y_i \leq \frac{z_i+1}{T}$ for $1 \leq i \leq n, z_i \in \mathbb{Z}\}$ forms a net in $\mathbb{R}^n$. Each cube in the family $F_T$ has volume $1/T^n$. Let $\overline{V_T}$ be the sum of volume of all those cubes of the family $F_T$ whose intersection with $S$ is not empty and let $\underline{V_T}$ be the sum of volumes of those cubes of $F_T$ which are fully contained in the set $S$. Since volume of $S$ exists, we have

$$\lim_{T\to\infty}\overline{V_T} = \lim_{T\to\infty}\underline{V_T} = V$$

But $\underline{V_T} \leq \frac{N(T)}{T^n} \leq \overline{V_T}$. By squeeze principle $\lim_{T\to\infty}\frac{N(T)}{T^n} = V$. □

**Proof of Theorem 3.1.2.**

The proof is divided into four steps.

**Step I.** Let $B$ be any fixed integral ideal in the class $\mathcal{C}^{-1}$. If $A$ is integral ideal in the class $\mathcal{C}$, then $AB$ is principal ideal say $AB = w\mathcal{O}_K$. Also if $B$ divides a principal ideal $w_1\mathcal{O}_K = BA_1$, then $A_1 \in \mathcal{C}$. Hence to every ideal $A \in \mathcal{C}$ with $N(A) \leq T$. Also observe that two principal ideals $w\mathcal{O}_K$ and $w_1\mathcal{O}_K$ are equal if and only if $w_1 = \epsilon w$, where $\epsilon$ is unit of $\mathcal{O}_K$. (In the following paragraph, we try to fix the choice of $w$ upto some extent.) We shall denote $N_{K/\mathbb{Q}}(w)$ by $N(w)$.

Let $\epsilon_1, \epsilon_2, \ldots, \epsilon_t$ be a fundamental system of units where $t = r + s - 1$ and let $\zeta$ be a primitive $m^{th}$ root of unity. We arrange the isomorphisms $\sigma_i$ of $K \longrightarrow \mathbb{C}$ in such a manner that $\sigma_1, \ldots, \sigma_r$ are real isomorphisms and $\sigma_{r+s+j} = \overline{\sigma_{r+j}}$ ,$1 \leq j \leq s$. For $\alpha \in K$ , denote $\sigma_i(\alpha)$ by $\alpha^i$. Recall that the regulator $R$ of field $K$ is the absolute value of determinant of $t \times t$ matrix $(C_{ij})$, where $C_{ij} = e_j b_{ij} = \log|\epsilon_i^{(j)}|$, $e_j$ equals 1 or 2 according as $1 \leq j \leq r$ or $j > r$. Since $R \neq 0$, it follows that determinant of the matrix $(b_{ij})$is non-zero. So given non-zero $w \in \mathcal{O}_K$, the vector $\log|\frac{w^{(1)}}{\sqrt[n]{N(w)}}|, \ldots, \log|\frac{w^{(t)}}{\sqrt[n]{N(w)}}|$, can be written as a combination of the row vectors of the matrix $(\log|\epsilon_i^{(j)}|), 1 \leq i, j \leq t$. So given $0 \neq w \in \mathcal{O}_K$, there exists real numbers $c_1, c_2, \ldots, c_t$ satisfying

$$\log\left|\frac{w^{(i)}}{\sqrt[n]{N(w)}}\right| = c_1 \log|\epsilon_1^{(i)}| + \cdots + c_t \log|\epsilon_t^{(i)}|, \quad 1 \leq i \leq t. \tag{3.2}$$

We now show that (3.2) holds for $i = t + 1$ also. Since $\sum_{i=1}^{t+1} e_i \log|\frac{w^{(i)}}{\sqrt[n]{N(w)}}| = \log|\frac{N(w)}{N(w)}| = \log 1 = 0$ and $\sum_{i=1}^{t+1} e_i \log|\epsilon_j^{(i)}| = \log|N(\epsilon_j)| = \log 1 = 0$, we have by virtue of (3.2) that

$$e_{t+1} \log|\frac{w^{(t+1)}}{\sqrt[n]{N(w)}}| = -\sum_{i=1}^{t} e_i \log|\frac{w^{(i)}}{\sqrt[n]{N(w)}}|$$

Cancelling $e_{t+1}$ on both sides, we get

$$\log|\frac{w(i)}{\sqrt[n]{N(w)}}| = c_1 \log|\epsilon_1^{(i)}| + \cdots + c_t \log|\epsilon_t^{(i)}|, \quad 1 \leq i \leq t+1. \tag{3.3}$$

If $w$ and $w_1$ are non-zero elements of $\mathcal{O}_K$ which are associates, then there exists unique integers $s_1, s_2, \ldots, s_t$ and a non-negative integer $k < m$ such that $w_1^{(i)} = w^{(i)}(\mathcal{C}^{(i)})^k(\epsilon_1^{(i)})^{s_1} \ldots (\epsilon_t^{(i)})^{s_t}$,

$1 \leq i \leq t+1$. So we have

$$\log|\frac{w_1^{(i)}}{\sqrt[n]{N(w_1)}}| = \log|\frac{w^{(i)}}{\sqrt[n]{N(w)}}| + s_1\log|\epsilon_1^{(i)}| + \cdots + s_t\log|\epsilon_t^{(i)}|, \quad 1 \leq i \leq t+1.$$

Using equation (3.3), we see that above equation gives

$$\log|\frac{w_1^{(i)}}{\sqrt[n]{N(w_1)}}| = (c_1+s_1)\log|\epsilon_1^{(i)}| + \cdots + (c_t+s_t)\log|\epsilon_t^{(i)}|, \quad 1 \leq i \leq t+1.$$

Hence the last equation shows that in every class of non-zero associate elements of $\mathcal{O}_k$, there are exactly $m$ elements $w$ which satisfies the inequalities $0 \leq c_j < 1$ for $j = 1, 2, \ldots t$ in equation (3.3). This shows that $m\mathcal{Z}(T, \mathcal{C})$ is the number of those algebraic integers $w$ lying in the ideal $B$ for which the following two conditions are satisfied :

$$0 < |N(w)| \leq TN(B), \tag{3.4}$$

if we write for $1 \leq i \leq t+1$

$$\log\left|\frac{w^{(i)}}{\sqrt[n]{N(w)}}\right| = \sum_{j=1}^{t} c_j \log|\epsilon_j^{(i)}|, \text{ then } 0 \leq c_j < 1 \text{ for} j = 1, \ldots, t. \tag{3.5}$$

**STEP II.** Let $\beta_1, \ldots, \beta_n$ be a $\mathbb{Z}$-basis for the ideal $B$. If $w \in B$, we can write $w = \sum_{q=1}^{n} \beta_q x_q, x_q \in \mathbb{Z}$. So we have $w^{(i)} = \sum_{q=1}^{n} \beta_q^{(i)} x_q$. Hence $m\mathcal{Z}(T, \mathcal{C})$ is the number of points with integral co-ordinates in the subset $S'$ of $\mathbb{R}^n$ consisting of points $(x_1, x_2, \ldots, x_n)$ defined by the following conditions:
If $y_i = \sum_{q=1}^{n} \beta_q^{(i)} x_q, \quad 1 \leq i \leq n$, then

$$0 < \left|\prod_{i=1}^{n}\sum_{q=1}^{n} \beta_q^{(i)} x_q\right| = \left|\prod_{i=1}^{n} y_i\right| \leq N(B).T$$

and

$$\log\left|\frac{y_i}{\sqrt[n]{\prod y_i}}\right| = \sum_{q=1}^{t} c_q \log|\epsilon_q^{(i)}| \text{ for } 1 \leq i \leq n,$$

then $0 \leq c_q < 1$ for $q = 1, \ldots, t$.
Note that if $K$ is imaginary quadratic field, then $r = 0, s = 1$. So $t = 0$. In this case, the last condition stated above is trivially satisfied.

We now verify that $S'$ is bounded subset of $\mathbb{R}^n$. We shall denote by $S$, the subset of $\mathbb{R}^n$ defined so as $S' = S(T^{\frac{1}{n}})$. In fact the set $S(T^{\frac{1}{n}})$ results from the set $S$ by multiplying all co-ordinates by $T^{\frac{1}{n}}$. So, $S$ is a subset of $\mathbb{R}^n$ consisting of all those $(x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ such that if $y_i = \sum_{q=1}^{n} \beta_q^{(i)} x_q, \quad 1 \leq i \leq n$, then $0 \leq c_q < 1$. . We shall prove that S is bounded and that its volume exists. Therefore by Lemma 3.2.1,

$$\lim_{T \to \infty} \frac{m\mathcal{Z}(T, \mathcal{C})}{T} = \text{volume of } S.$$

So the theorem is proved once we show that $S$ is bounded and

$$\text{volume of } S = \frac{2^{r+s}\pi^s R}{\sqrt{|d_K|}} \tag{3.6}$$

We first verify that $S$ is a bounded set. We shall find a constant $c$ such that all $|x_i| \leq c$ for every vector $x_1, x_2, \ldots, x_n \in S$. For this consider the mapping $L : \mathbb{C}^n \longmapsto \mathbb{C}^n$ defined by

$$[x_1, x_2, \ldots, x_n] \to [x_1, x_2, \ldots, x_n] \begin{bmatrix} \beta_1^{(1)} & \beta_1^{(2)} & \cdots & \beta_1^{(n)} \\ \beta_2^{(1)} & \beta_2^{(2)} & \cdots & \beta_2^{(n)} \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \beta_n^{(1)} & \beta_n^{(2)} & \cdots & \beta_n^{(n)} \end{bmatrix}$$

which is a non-singular linear transformation, as the absolute value of its determinant is $\sqrt{|D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)|} \neq 0$. Therefore a subset $V$ of $\mathbb{C}^n$ is bounded if and only if $L(V)$ is bounded subset of $\mathbb{C}^n$. So it is enough to prove that the set $L(S)$ is bounded, where $L(S) = \{(y_1, \ldots, y_n) \in \mathbb{C}^n,\ 0 < |\prod_{i=1}^{n} y_i| \leq N(B)\ \}$, and

$$\log |\frac{y_i}{\sqrt[n]{\prod_{j=1}^{n} y_j}}| = \sum_{q=1}^{t} c_q \log |\epsilon_q^{(i)}|, \quad 1 \leq i \leq n,\ 0 \leq c_q < 1.$$

Taking exponential in above equality, we see that

$$\begin{aligned} |y_i| &= \sqrt[n]{\prod_{j=1}^{n} y_j} \prod_{q=1}^{t} |\epsilon_q^{(i)}|^{c_q} \\ &\leq (N(B))^{\frac{1}{n}} \exp(\sum_{q=1}^{t} c_q \log |\epsilon_q^{(i)}|) \leq (N(B))^{\frac{1}{n}} \exp(m_0 t), \end{aligned}$$

where $m_0 = \max_{1\le q\le t,\ 1\le i\le n} |\log \epsilon_q^{(i)}|$. So $S$ is a bounded set.

**STEP III.** In this step, we proceed to calculate the volume of $S$. Put

$$z_i = \begin{cases} y_j, & \text{for } j = 1, 2, \ldots, r \\ \frac{y_j + y_{j+s}}{2}, & \text{for } j = r+1, r+2, \ldots, r+s \\ \frac{y_j - y_{j+s}}{2\iota}, & \text{for } j = r+s+1, r+s+2, \ldots, r+2s \end{cases}$$

Then $z_1, \ldots, z_n$ are real numbers. The Jacobian

$$\begin{aligned} \left|\frac{\partial(z_1, \ldots, z_n)}{\partial(x_1, \ldots, x_n)}\right| &= \left|\frac{\partial(z_1, \ldots, z_n)}{\partial(y_1, \ldots, y_n)}\right| \left|\frac{\partial(y_1, \ldots, y_n)}{\partial(x_1, \ldots, x_n)}\right| \\ &= \left|\det \begin{bmatrix} I_r & 0 \\ 0 & M_{2s} \end{bmatrix}\right| \det|\beta_j^{(i)}| \end{aligned}$$

where $M_{2s}$ is a $2s \times 2s$ matrix of the type

$$\begin{bmatrix} \frac{1}{2} & 0 & \cdots & 0 & \frac{1}{2} & 0 & \cdots & 0 \\ 0 & \frac{1}{2} & \cdots & 0 & 0 & \frac{1}{2} & \cdots & 0 \\ . & . & \cdots & . & . & . & \cdots & . \\ . & . & \cdots & . & . & . & \cdots & . \\ 0 & 0 & \cdots & \frac{1}{2} & 0 & 0 & \cdots & \frac{1}{2} \\ \frac{1}{2\iota} & 0 & \cdots & 0 & -\frac{1}{2\iota} & 0 & \cdots & 0 \\ 0 & \frac{1}{2\iota} & \cdots & 0 & 0 & -\frac{1}{2\iota} & \cdots & 0 \\ . & . & \cdots & . & . & . & \cdots & . \\ . & . & \cdots & . & . & . & \cdots & . \\ 0 & 0 & \cdots & \frac{1}{2\iota} & 0 & -\frac{1}{2\iota} & \cdots & -\frac{1}{2\iota} \end{bmatrix}$$

and $[0\ 0\ \ldots\ \frac{1}{2}\ 0\ 0\ \ldots\ \frac{1}{2}]$, $[\frac{1}{2}\ 0\ \ldots\ 0\ -\frac{1}{2\iota}\ 0\ \ldots\ 0]$ stands for the $s^{th}$ row and $(s+1)^{th}$ column of the matrix $M_{2s}$ respectively. Multiply $(s+1)^{th}$ row by $\iota$, where $\iota = \sqrt{-1}$ and adding it to $2^{nd}$ row and continue this process, we see that det $M_{2s}$ = determinant of lower triangular matrix whose first $s$ diagonal entries are 1 and next $s$ diagonal entries are $-\frac{1}{2\iota}$. Therefore $\det|M_{2s}| = 2^{-s}$.

.

$$\begin{aligned} |detB_j^{(i)}| &= \sqrt{|D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)|} \\ &= [\mathcal{O}_K : B]\sqrt{|d_K|} \\ &= N(B)\sqrt{|d_K|} \end{aligned}$$

So, $\left|\frac{\partial(z_1,\ldots,z_n)}{\partial(x_1,\ldots,x_n)}\right| = 2^{-s}N(B)\sqrt{|d_K|}$.

Therefore $I = \underbrace{\int\cdots\int}_{S} dx_1\cdots dx_n = \left(\underbrace{\int\cdots\int}_{S^*} dz_1\cdots dz_n\right)\frac{2^s}{N(B)\sqrt{|d_K|}}$

where $S^*$ is subset of $\mathbb{R}^n$ consisting $(z_1,\cdots,z_n)$ such that

$$0 < \prod_{j=1}^{r}|z_j| \prod_{j=r+1}^{r+s}(z_j^2+z_{j+s}^2) = z^*(\text{say}) \le N(B),$$

$$\log\left|\frac{z_i}{\sqrt[n]{z^*}}\right| = \sum_{q=1}^{t} c_q \log|\epsilon_q^{(i)}|, \quad 1 \le i \le r, \tag{3.7}$$

$$\log\left|\frac{\sqrt{z_j^2+z_{j+s}^2}}{\sqrt[n]{z^*}}\right| = \sum_{q=1}^{t} c_q \log|\epsilon_q^{(i)}|, \ j = r+1,\cdots,r+s; \ 0 \le c_q < 1.$$

For an imaginary quadratic field, the last two conditions of (3.7) have no meaning. For an imaginary quadratic field, the (3.6) and hence the theorem is proved because

$$I = \frac{2}{N(B)\sqrt{|d_K|}}\underbrace{\int\int}_{S^*} dz_1dz_2, \quad 0 < (z_1^2+z_2^2) \le N(B)$$
$$= \frac{2\pi N(B)}{N(B)\sqrt{|d_K|}} = \frac{2\pi}{\sqrt{|d_K|}}.$$

Now we come back again to general case. Clearly on replacing $z_i$ by $\frac{z_i}{(N(B)^{1/n})}$, one can easily see that

$$I = \frac{2^s2^rN(B)}{N(B)\sqrt{|d_K|}}\underbrace{\int\cdots\int}_{S^*} dz_1\cdots dz_n,$$

where $S^{**}$ is a subset of $\mathbb{R}^n$ consisting of all points $(z_1,\ldots,z_n)$ which satisfy the three conditions of (3.7) with $N(B)$ replaced by 1 in first condition and with extra condition that $z_i > 0, 1 \le i \le r$.

**Step IV.** In this step, we complete the calculation of volume of $S$. We have shown that

$$I = \frac{2^s2^r}{\sqrt{|d_K|}}\underbrace{\int\cdots\int}_{S^*} dz_1\cdots dz_n,$$

where $S^{**}$ is a subset of $\mathbb{R}^n$ consisting of all points $(z_1, \ldots, z_n)$ which satisfy the following three conditions:

$$0 < \prod_{j=1}^{r} |z_j| \prod_{j=r+1}^{r+s} (z_j^2 + z_{j+s}^2) = z^*(\text{say}) \leq 1,$$

$$\log \left| \frac{z_i}{\sqrt[n]{z^*}} \right| = \sum_{q=1}^{t} c_q \log |\epsilon_q^{(i)}|, \quad 1 \leq i \leq r,$$

$$\log \left| \frac{\sqrt{z_j^2 + z_{j+s}^2}}{\sqrt[n]{z^*}} \right| = \sum_{q=1}^{t} c_q \log |\epsilon_q^{(i)}|, j = r+1, \cdots, r+s; 0 \leq c_q < 1.$$

We now take new variables $\rho_1, \ldots, \rho_{r+s}, \phi_{r+1}, \ldots, \phi_{r+s}$ and put

$$z_i = \begin{cases} \rho_i, & \text{for } 1 \leq i \leq r \\ \rho_i \cos \phi_i, & \text{for } i = r+1, r+2, \ldots, r+s \end{cases}$$

$$z_{i+s} = \rho_i \sin \phi_i \quad i = r+1, \ldots, \phi_{r+s}.$$

$$dz_i dz_{i+s} = \rho_i d\rho_i d\phi_i \quad \text{for} \quad i = r+1, \ldots, \phi_{r+s}.$$

So

$$I = \frac{2^s 2^r}{\sqrt{|d_K|}} \times (2\pi)^s \underbrace{\int \cdots \int}_{U} (\prod_{i=r+1}^{r+s} \rho_i) d\rho_1, \ldots, d\rho_{r+s}, \tag{3.8}$$

where U is a subset of $\mathbb{R}^{r+s}$ consisting of all vectors $(\rho_1, \ldots, \rho_{r+s})$ which satisfy following two conditions

$$0 < \prod_{i=1}^{r+s} \rho_i^{\epsilon_i} \leq 1, \rho_i > 0 \text{ with } \epsilon_i = 1 \text{ or } 2 \text{ according as } i \leq r \text{ or not}, \tag{3.9}$$

$$\log \left( \frac{\rho_i}{\sqrt[n]{\rho}} \right) = \sum_{q=1}^{t} c_q \log |\epsilon_q^{(i)}|, \quad 1 \leq i \leq r+s; \ 0 \leq c_q < 1.$$

Finally we introduce $\rho$ and $c_q$ as new variables. Rewriting the second condition of (3.9), we see that

$$\log \rho_i = \frac{1}{n} \log \rho + \sum_{q=1}^{t} c_q \log |\epsilon_q^{(i)}|.$$

Differentiating the above equation $\rho$ and $c_q$, we obtain

$$\frac{1}{\rho_i} \frac{\partial \rho_i}{\partial \rho} = \frac{1}{n\rho},$$

$$\frac{1}{\rho_i}\frac{\partial \rho_i}{\partial c_q} = \log|\epsilon_q^{(i)}|.$$

Let us calculate the Jacobian,

$$\left|\frac{\partial(\rho_1,\ldots,\rho_{t+1})}{\partial(\rho,c_1,\ldots,c_t)}\right| = \det\begin{bmatrix} \frac{\rho_1}{n\rho} & \frac{\rho_2}{n\rho} & \cdots & \frac{\rho_{t+1}}{n\rho} \\ \rho_1\log|\epsilon_1^{(1)}| & \rho_2\log|\epsilon_1^{(2)}| & \cdots & \rho_{t+1}\log|\epsilon_1^{(t+1)}| \\ . & . & \cdots & . \\ . & . & \cdots & . \\ \rho_1\log|\epsilon_t^{(1)}| & \rho_2\log|\epsilon_t^{(2)}| & \cdots & \rho_{t+1}\log|\epsilon_t^{(t+1)}| \end{bmatrix}$$
$$= \frac{\prod_{i=1}^{t+1}\rho_i}{n\rho}$$

Since $\sum_{t=1}^{t+1}\epsilon_i\log|\epsilon_q^{(i)}| = 0$, multiplying $i$-th column by $\epsilon_i, 1 \le i \le t+1$ and adding them to last column and then expanding by last column, we see that

$$\left|\frac{\partial(\rho_1,\ldots,\rho_{t+1})}{\partial(\rho,c_1,\ldots,c_t)}\right| = \frac{\prod_{i=1}^{t+1}\rho_i}{n\rho}\frac{n}{e_{t+1}}\det|\log|\epsilon_i^{(j)}||,\ 1 \le i,j \le t$$
$$= \frac{\prod_{i=1}^{t+1}\rho_i}{\rho e_{t+1}}\frac{R}{2^{s-1}}.$$

Therefore using (3.8) and (3.9), we have

$$I = \frac{(2\pi)^s 2^{r+s}}{\sqrt{|d_K|2^s}}R\int\cdots\int\frac{\prod_{i=1}^{t+1}\rho_i}{\rho}\prod_{i=r+1}^{r+s}\rho_i d\rho dc_1\cdots dc_t$$
$$= \frac{\pi^s 2^{r+s}}{\sqrt{|d_K|}}R\int_0^1\cdots\int_0^1 d\rho dc_1\cdots dc_t = \frac{\pi^s 2^{r+s}R}{\sqrt{|d_K|}}.$$

This proves (3.6), which completes the proof of the theorem.

The following corollary is an immediate consequence of Ideal Theorem.

**Corollary 3.2.2.** *Let $K$ be an algebraic number field and let notations be as in the above theorem. If $\mathcal{Z}(T)$ denotes the number of ideals of $\mathcal{O}_K$ whose norm does not exceed $T$ and*

*h the class number of K, then*

$$\lim_{T\to\infty}\frac{\mathcal{Z}(T)}{T}=\lim_{T\to\infty}\left[\frac{\sum_{i=1}^{h}\mathcal{Z}(T,\mathcal{C}_i)}{T}\right]=h\kappa.$$

$$\textit{where}\quad \kappa=\frac{2^{r+s}\pi^s R}{m\sqrt{|d_K|}} \tag{3.10}$$

## 3.3 Derivation of Dirichlet's Class Number Formula

For deriving Dirichlet's Class Number Formula from Ideal Theorem, we first prove couple of results dealing with mathematical analysis.

**Definition.** A series of the form $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$, where $a_n$ are complex numbers, is called Dirichlet series. In particular when $a_n = 1\ \forall n$, this was introduced by Riemann and is called Riemann Zeta Function.

**Proposition 3.3.1.** *The series $\sum_{n=1}^{\infty}\frac{1}{n^s}$ converges for $s>1$. Its sum function denoted by $\mathcal{C}(s)$ (Riemann zeta function) for $s>1$ is continuous function of $s$ and $\lim_{s\to1^+}(s-1)\zeta(s)=1$.*

*Proof.* Since the function $\frac{1}{x^s}$ is monotonically decreasing function for $x\in(0,\infty)$ when $s>1$. Therefore

$$\int_n^{n+1}\frac{dx}{x^s}<\frac{1}{n^s}<\int_{n-1}^{n}\frac{dx}{x^s},$$

where inequality holds for $n\geq1$ on LHS and for $n\geq2$ on RHS of the above equation. Hence for $N>1$,

$$\int_1^{N+1}\frac{dx}{x^s}<\sum_{n=1}^{N}\frac{1}{n^s}<1+\int_1^{N}\frac{dx}{x^s}.$$

Since we know $\int_1^{\infty}\frac{dx}{x^s}$ converges for $s>1$. So taking limit as $N\to\infty$, we have

$$\int_1^{\infty}\frac{dx}{x^s}\leq\zeta(s)\leq1+\int_1^{\infty}\frac{dx}{x^s}$$

$$\frac{1}{s-1} \leq \zeta(s) \leq 1 + \frac{1}{s-1}.$$

Multiply throughout by $(s-1)$ and taking limit $s \to 1^+$, we obtain

$$1 \leq \lim_{s\to 1^+} (s-1)\zeta(s) \leq \lim_{s\to 1^+} s.$$

By Squeeze Principal, we have $\lim_{s\to 1^+} (s-1)\zeta(s) = 1$. We now verify that $\zeta(s)$ is a continuous function of $s$ in the region $s > 1$. Fix a positive real number $\delta$. Then $s \geq 1+\delta$ and we have $\sum_{n=1}^{\infty} \frac{1}{n^s} \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}}$. Since RHS of the last inequality converges, by Weierstrass M-test, $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges uniformly in $[1+\delta, \infty)$. Each term of series is continuous function of $s$. So its sum function is continuous function of $s$ in interval $(1, \infty)$. □

**Proposition 3.3.2.** *Let $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series. Let $P_n$ stand for $\sum_{j=1}^{n} a_j$. If there exists $\sigma_0 \geq 0$ such that $|\frac{P_n}{n^{\sigma_0}}| \leq A \ \forall\ n \geq 1$. Then the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges uniformly on each compact subset on the $(\sigma_0, \infty)$ and represent a continuous function of $s$ in $(\sigma_0, \infty)$.*

*Proof.* Recall that a series is uniformly convergent in the set $F$ if and only if the sequence of its partial sum is uniformly Cauchy in $F$. So, let $F$ be compact subset of the interval $(\sigma_0, \infty)$. So $F$ is closed and bounded. If $f_0$ is the greatest lower bound of $F$ then $f_0 \in F$. Hence $f_0 > \sigma_0$. So there exists real number $r > 0$ such that $f_0 \geq \sigma_0 + r$. We now show that the sequence of partial sums of the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is uniformly Cauchy on $F$. Let $M > N$ be any natural number. Then

$$\sum_{n=N}^{M} \frac{a_n}{n^s} = \sum_{n=N}^{M} \frac{P_n - P_{n-1}}{n^s} = \frac{P_M}{M^s} - \frac{P_{N-1}}{N^s} + \sum_{n=N}^{M-1} P_n \left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right].$$

But $\int_n^{n+1} \frac{dx}{x^{s+1}} = \frac{1}{s}\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)$ provided $s > 0$. So for $s \in F$,

$$\begin{aligned}\left|\sum_{n=N}^{M} \frac{a_n}{n^s}\right| &\leq \frac{AM^{\sigma_0}}{M^s} + \frac{A(N-1)^{\sigma_0}}{N^s} + \sum_{n=1}^{M-1} An^{\sigma_0}\left[\frac{1}{n^s} - \frac{1}{(n+1)^s}\right] \\ &\leq \frac{AM^{\sigma_0}}{M^s} + \frac{A(N-1)^{\sigma_0}}{N^s} + \sum_{n=1}^{M-1} An^{\sigma_0} s \int_n^{n+1} \frac{dx}{x^{s+1}}\end{aligned}$$

$$\leq \frac{A}{M^{f_0-\sigma_0}} + \frac{A}{N^{f_0-\sigma_0}} + A\sum_{n=1}^{M-1} s\int_n^{n+1} \frac{dx}{x^{s+1}} x^{\sigma_0}$$
$$\leq \frac{2A}{N^{f_0-\sigma_0}} + sA\int_N^{\infty} \frac{dx}{x^{s-\sigma_0+1}} = \frac{2A}{N^{f_0-\sigma_0}} + \frac{sA}{s-\sigma_0}\frac{1}{N^{s-\sigma_0}}$$
$$\leq \frac{2A}{N^r} + \frac{BA}{r}\frac{1}{N^r} \to \infty, \text{ where } s \leq B \ \forall \ s \in F$$

We have shown that sequence of partial sum of the series $\sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ is uniformly Cauchy in any compact subset $F$ in the interval $(\sigma_0, \infty)$. So $\sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ is uniformly convergent in $F$. Since each term of the series is continuous, the sum $\sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ is continuous function. □

**Theorem 3.3.3.** *Let $\sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series whose sum is denoted by $f(s)$. Let $P_n = \sum\limits_{j=1}^{n} a_j$. If there is constant $c$ such that $\lim\limits_{m\to\infty} \frac{P_n}{n} = c$, then $\lim\limits_{s\to 1^+} (s-1)f(s) = c$.*

*Proof.* First observe that $\sum\limits_{n=1}^{\infty} \frac{a_n}{n^s}$ is uniformly convergent on compact subsets of $(1, \infty)$; this is so in view of Proposition 3.3.2 because $\frac{P_n}{n}$ is convergent and hence a bounded sequence. Write $P_n = cn + n\epsilon_n$, then $\epsilon_n \to 0$ as $n \to \infty$. Now for $s > 1$

$$\begin{aligned}
\left|\sum_{n=1}^{M} \frac{a_n}{n^s} - c\sum_{n=1}^{M} \frac{1}{n^s}\right| &= \left|\sum_{n=1}^{M} \frac{P_n - P_{n-1}}{n^s} - c\sum_{n=1}^{M} \frac{1}{n^s}\right| \\
&= \left|\sum_{n=1}^{M} \frac{[P_n - P_{n-1} - c]}{n^s}\right| \\
&= \left|\sum_{n=1}^{M} \frac{[cn + n\epsilon_n - cn + c - n\epsilon_{n-1} + \epsilon_{n-1} - c]}{n^s}\right| \\
&= \left|\sum_{n=1}^{M} \frac{n\epsilon_n - (n-1)\epsilon_{n-1}]}{n^s}\right| \\
&\leq \left|\sum_{n=1}^{M} n\epsilon_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right)\right| + \frac{M|\epsilon_M|}{M^s}
\end{aligned}$$

$$= \left| \sum_{n=1}^{M} n\epsilon_n s \int_n^{n+1} \frac{dx}{x^{s+1}} \right| + \frac{|\epsilon_M|}{M^{s-1}}$$
$$\leq s \sum_{n=1}^{M} |\epsilon_n| \int_n^{n+1} \frac{dx}{x^s} + \frac{|\epsilon_M|}{M^{s-1}}$$

Our aim is to show that for any given $\epsilon > 0$,

$$\lim_{s \to 1^+} |(s-1)f(s) - c(s-1)\zeta(s)| < \epsilon.$$

Consequently, $\lim_{s \to 1^+} |(s-1)f(s) - c(s-1)\zeta(s)| = 0$. But by Proposition 3.3.1, $\lim_{s \to 1^+} (s-1)\zeta(s) = 1$, and hence we shall deduce that $\lim_{s \to 1^+} (s-1)f(s) = c$.

Let $\epsilon > 0$ be any given real number. Since the sequence $\{\epsilon_n\} \to 0$ as $n \to \infty$, so there exists a natural number $N$ such that $|\epsilon_n| < \frac{\epsilon}{3}$, $\forall n \geq N$. Also every convergent sequence is bounded. So there exists $k$ such that $|\epsilon_n| < k$ for all $n$. By what we have shown in first paragraph, if $M > N$, then for $s > 1$

$$\left| \sum_{n=1}^{M} \frac{a_n}{n^s} - c \sum_{n=1}^{M} \frac{1}{n^s} \right| \leq s \sum_{n=1}^{M-1} |\epsilon_n| \int_n^{n+1} \frac{dx}{x^s} + \frac{\epsilon}{3}.$$

Letting $M \to \infty$, we see that

$$|f(s) - c\zeta(s)| \leq s \sum_{n=1}^{\infty} |\epsilon_n| \int_n^{n+1} \frac{dx}{x^s} + \frac{\epsilon}{3} \text{ for } s > 1. \tag{3.11}$$

$$\text{RHS of (3.11)} = s \sum_{n=1}^{N} |\epsilon_n| \int_n^{n+1} \frac{dx}{x^s} + s \sum_{n=N+1}^{\infty} |\epsilon_n| \int_n^{n+1} \frac{dx}{x^s} + \frac{\epsilon}{3}$$
$$\leq sk \sum_{n=1}^{N} \int_n^{n+1} \frac{dx}{x^s} + \frac{s\epsilon}{3} \int_{N+1}^{\infty} \frac{dx}{x^s} + \frac{\epsilon}{3}$$
$$\leq sk \int_1^{N+1} \frac{dx}{x} + \frac{s\epsilon}{3} \int_{N+1}^{\infty} \frac{dx}{x^s} + \frac{\epsilon}{3}$$
$$= sk \log(N+1) + \frac{s\epsilon}{3(s-1)} \frac{1}{(N+1)^{s-1}} + \frac{\epsilon}{3}.$$

$$\text{Thus} |f(s) - c\zeta(s)| \leq sk \log(N+1) + \frac{s\epsilon}{3(s-1)} \frac{1}{(N+1)^{s-1}} + \frac{\epsilon}{3}. \tag{3.12}$$

Multiply the above inequality by $s-1$ on both sides, we see that for $s > 1$,

$$|(s-1)f(s) - c(s-1)\zeta(s)| \leq (s-1)sk \log(N+1) + \frac{s\epsilon}{(N+1)^{s-1}} + \frac{\epsilon(s-1)}{3} \tag{3.13}$$

Taking limits as $s \to 1^+$, RHS of (3.13) will tend to $\frac{\epsilon}{3}$. Since it is true for every $\epsilon > 0$, we get desired result.

□

**Proof of Theorem 3.1.1** For any number $j$, let $f(j)$ denote the number of integral ideals having norm $j$. With this notation, the series $\sum\limits_{A} \frac{1}{N(A)^s}$, where $A$ running over all non-zero ideals of $\mathcal{O}_K$, can be rewritten as $\sum\limits_{j=1}^{\infty} \frac{f(j)}{j^s}$. If $\mathcal{Z}(T)$ stands for the number of integral ideals of $\mathcal{O}_K$ whose norm does not exceed $T$, then $\sum\limits_{j=1}^{T} f(j) = \mathcal{Z}(T)$. By Corollary 3.2.2, $\lim\limits_{n\to\infty} \frac{\mathcal{Z}(n)}{n} = h\kappa$. So by Proposition 3.3.2, the series $\sum\limits_{j=1}^{\infty} \frac{f(j)}{j^s} = \sum\limits_{A} \frac{1}{N(A)^s}$ converges on all compact subsets of $(1, \infty)$. Further using Corollary 3.2.2 and Theorem 3.3.3 , we conclude that

$$\lim_{s\to 1^+} (s-1)\zeta_K(s) = h\kappa$$

## 3.4 Applications of Dirichlet's Class Number Formula

Dirichlet's class number formula becomes valuable because the function $\zeta_K(s)$ also has a representation as an infinite product $\prod_{\wp} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1}$ given by the following proposition. If for a field $K$, we have a good knowledge of prime ideals of $\mathcal{O}_K$, then we can obtain explicit expression for $h_K$ from Dirichlet's class number formula (3.1). Using this method, we shall give simpler formulas for $h_K$ in the next chapter when $K$ is cyclotomic or quadratic field.

**Proposition 3.4.1.** *(**Euler's Product Formula for** $\zeta_K(s)$) Let $K$ be an algebraic number field. Prove that for $s > 1$,*

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

*where* $\mathfrak{p}$ *runs over all non-zero prime ideal of* $\mathcal{O}_K$.

*Proof.* Let $x$ be any natural number.

$$\left| \prod_{\mathfrak{p} \text{ prime } N(\mathfrak{p}) \leq x} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} - \sum_{N(A) \leq x} \frac{1}{N(A)^s} \right| \leq \sum_{A^*} \frac{1}{N(A^*)^s}, \tag{3.14}$$

where $A^*$ runs over those integral ideals of $\mathcal{O}_K$ whose norm is strictly greater than $x$ but which are divisible by only those prime ideals whose norm is less than or equals to $x$. Now RHS of (3.14), being dominated by the tail of convergent series (namely the series for $\zeta_K(s)$ tends to 0 as $x \to \infty$. Hence the result is proved. □

The proof of the Proposition 3.4.1 can be imitated to proof of the following proposition which will be used later.

**Proposition 3.4.2.** *Let* $a_n$ *be sequence of complex numbers such that* $a_1 = 1$, $a_{mn} = a_m a_n$ *and* $|a_m| < 1 \ \forall \ m > 1$. *If* $\sum\limits_{m=1}^{\infty} |a_m| < \infty$, *then prove that* $\sum\limits_{m=1}^{\infty} |a_m| = \prod\limits_{p} (1 - a_p)^{-1}$, *where* $p$ *runs over all rational primes.*

*Proof.* Let $x$ be any natural number.

$$\left| \prod_{p \text{ prime } p \leq x} (1 - a_p)^{-1} - \sum_{m \leq x} a_m \right| \leq \sum_{m^*} |a_m^*|, \tag{3.15}$$

where $m$ runs over rational integers and $m^*$ runs over all those rational integers which are strictly greater than $x$ but which are divisible by only primes $p \leq x$. Observe that $\sum\limits_{m^*} |a_m^*|$ is dominated by tail of series $\sum\limits_{m=1}^{\infty} |a_m|$ which is convergent and hence $\sum |a_m^*| \to 0$ as $x \to \infty$. Therefore we have $\prod\limits_{p} (1 - a_p)^{-1} = \sum\limits_{m=1}^{\infty} |a_m|$, where $p$ runs over rational primes. □

The following theorem is an application of Dirichlet class number formula.

**Theorem 3.4.3.** *An algebraic number field* $K$ *has infinite number of prime ideals* $\wp$ *such that the absolute residual degree of* $\wp$ *is* 1.

*Proof.* We know by Euler's product formula, for $s > 1$

$$\zeta_K(s) = \prod_{\wp} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1}$$

Taking log both sides in the above equation, we obtain for $s > 1$

$$\log \zeta_K(s) = \sum_{\wp} \sum_{m=1}^{\infty} \frac{1}{mN(\wp)^{ms}} \tag{3.16}$$

We isolate the sum on RHS of the above equation into two parts. Denote

$$P(s) = \sum_{\wp_1} \frac{1}{N(\wp)^s}, \tag{3.17}$$

where $\wp_1$ runs over all those prime ideals of $K$ whose absolute residual degree is 1. We denote sum of remaining terms of(3.16) by $G(s)$. So we rewrite (3.16) as

$$\log \zeta_K(S) = P(s) + G(s).$$

If $f$ denotes absolute residual degree of prime ideal $\wp$ of $K$, then $N(\wp) = p^f$ and when $f \geq 2$, we have

$$\begin{aligned} \sum_{m=1}^{\infty} \frac{1}{mN(\wp)^{ms}} &\leq \sum_{m=1}^{\infty} \frac{1}{p^{2sm}} \\ &= \frac{1}{p^{2s}-1} < \frac{2}{p^{2s}}. \end{aligned}$$

If $f = 1$, then

$$\sum_{m=2}^{\infty} \frac{1}{mN(\wp)^{ms}} \leq \sum_{m=2}^{\infty} \frac{1}{p^{sm}} = \frac{1}{p^s(p^s-1)} < \frac{2}{p^{2s}} \tag{3.18}$$

Therefore we have

$$\begin{aligned} G(s) &= \sum_{\wp,\ f_\wp \geq 2} \sum_{m=1}^{\infty} \frac{1}{mN(\wp)^{ms}} + \sum_{\wp,\ f_\wp = 1} \sum_{m=2}^{\infty} \frac{1}{mN(\wp)^{ms}} \\ &\leq \sum_{\wp | p} \sum_{p} \frac{2}{p^{2s}}, \end{aligned}$$

where $p$ runs over all rational primes and $\wp$ runs over all prime ideals of $\mathcal{O}_K$. Now again for any rational prime $p$, there exist atmost $n$ = degree of $K/\mathbb{Q}$ prime ideals $\wp$ of $\mathcal{O}_K$ which lie over $p$. Therefore

$$G(s) \leq 2n \sum_{p} \frac{1}{p^{2s}} \leq 2n\zeta(2s) \tag{3.19}$$

We know that $\zeta(s)$ is a continuous function of $s$ in the interval $(1, \infty)$. Therefore $G(s)$ is bounded when $s \to 1^+$. By Dirichlet Class Number Formula, we know that $\lim_{s \to 1^+}(s-1)\zeta_K(s) = h\kappa \neq 0$, which implies $\zeta_K(s) \to \infty$ as $s \to 1^+$, i.e.,$\log \zeta_K(s) \to \infty$ as $s \to 1^+$. But $\log \zeta_K(s) = P(s) + G(s)$, and $G(s)$ is bounded as $s \to 1^+$. So $P(s) \to \infty$ as $s \to 1^+$ and hence there are infinitely many terms in the sum for $P(s)$ and therefore infinitely many prime ideals with residual degree 1. □

For an odd prime $p$ and an integer $a$ not divisible by $p$, denote by $\left(\frac{a}{p}\right)$ the Legendre Symbol defined to be $+1$ or $-1$ according as the congruence $x^2 \equiv a \bmod p$ is solvable or not. With the above notation, we prove the following corollary.

**Corollary 3.4.4.** *Given any integer $a$ which is not a perfect square, there exists infinitely many rational primes $p$ such that $\left(\frac{a}{p}\right) = 1$.*

*Proof.* Write $a = b^2 d$, where $d$ is square free integer and $b \geq 1$. For any prime $p$ does not divide $a$, $p \neq 2$, we know that

$$\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right).$$

It is known that if $p$ does not divide $d$ and $p \neq 2$, then $\left(\frac{d}{p}\right) = 1$ if and only if there exists two prime ideals $\wp_1, \wp_2$ of $\mathbb{Q}(\sqrt{d})$ lying over $p$ if and only if $f(\wp/p) = 1$ for a prime ideal $\wp$ of $\mathbb{Q}(\sqrt{d})$ lying over $p$. By Theorem 3.4.3, there exist infinitely many prime ideals $\wp$ of $\mathcal{O}_K$ whose absolute residual degree is 1.

□

The next theorem is another application of Dirichlet's class number formula.

**Theorem 3.4.5.** *Given any non-zero integer $a$ not a perfect square, there exist infinitely many rational primes $p$ such that $\left(\frac{a}{p}\right) = -1$.*

*Proof.* Write $a = b^2 d$, where $b \geq 1$ and $d$ is a square free integer. So we have to prove that there exist infinitely many rational primes $p$ such that $\left(\frac{d}{p}\right) = -1$. Suppose the result is false. Let $D$ denote the discriminant of the field $K = \mathbb{Q}(\sqrt{d})$ and $F$ denote the finite set of primes for which $\left(\frac{D}{p}\right) = -1$. For $s > 1$, we have $\zeta_K(s) = \prod_{\wp} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1}$ which can be rewritten as

$$\zeta_K(s) = \prod_{p \in F} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{p \notin F,\ p \nmid D} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \mid D} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{3.20}$$

$$\begin{aligned}\text{RHS of (3.20)} &= \prod_{\text{all } p}\left(1-\frac{1}{p^s}\right)^{-1}\prod_{p\in F}\left(1+\frac{1}{p^s}\right)^{-1}\prod_{p\notin F,\ p\nmid D}\left(1-\frac{1}{p^s}\right)^{-1}\\ &= \zeta(s)\prod_{p\in F}\left(1+\frac{1}{p^s}\right)^{-1}\prod_{p\in F}\left(1-\frac{1}{p^s}\right)\prod_{p|D}\left(1-\frac{1}{p^s}\right)\prod_{\text{all } p}\left(1-\frac{1}{p^s}\right)^{-1}\\ &= \zeta(s)^2\prod_{p\in F}\left(1+\frac{1}{p^s}\right)^{-1}\prod_{p\in F}\left(1-\frac{1}{p^s}\right)\prod_{p|D}\left(1-\frac{1}{p^s}\right).\end{aligned}$$

So by Proposition 3.3.1 $\lim_{s\to 1^+}(s-1)\zeta(s)=1$, the above expression for $\zeta_K(s)$ shows that

$$\lim_{s\to 1^+}(s-1)^2\zeta_K(s)=\prod_{p\in F}\left(1+\frac{1}{p}\right)^{-1}\prod_{p\in F}\left(1-\frac{1}{p}\right)\prod_{p|D}\left(1-\frac{1}{p}\right),$$

which is non-zero being a product of finitely many non-zero terms. But in view of Dirichlet class number formula $\lim_{s\to 1^+}(s-1)^2\zeta_K(s)=0$. This contradiction proves the theorem. □

# Chapter 4

# Simplified Dirichlet's Class Number Formula for Quadratic and Cyclotomic Fields

To obtain simplified Dirichlet's Class Number Formula for quadratic and cyclotomic fields, we first introduce the terms numerical characters and their L-functions and prove some results regarding characters of finite abelian groups.

## 4.1 Numerical Characters and L-Functions

**Definition.** Let $G$ be a finite abelian group. By a character $\chi$ of $G$, we mean a homomorphism $\chi : G \to \{z : |z| = 1,\ z \in \mathbb{C}\}$. If $G$ has order $n$ and $x \in G$, $x^n = e$(where $e$ is the identity of $G$) implies that $\chi(x)^n = \chi(x^n) = \chi(e) = 1$. So $\chi(G) \subset$ Group of $n^{th}$ roots of unity.

*Remark.* If $G$ is a cyclic group of order $m$ generated by $a$, then $G$ has exactly $m$ characters $\chi_0, \ldots, \chi_{m-1}$, where $\chi_i(a) = \epsilon^i$, where $\epsilon$ is a fixed primitive $m^{th}$ roots of unity. In fact this is true for every finite abelian group.

**Proposition 4.1.1.** *The number of characters of a finite abelian group equals the order of a group.*

*Proof.* We can write $G$ as $G_1 \times G_2 \times \cdots \times G_s$ as product of cyclic groups. Suppose $G_i = \langle a_i \rangle$ and $G_i$ has order $m_i$. Any element $x \in G$ is of the form

$$x = a_1^{k_1} a_2^{k_2} \ldots a_s^{k_s}. \tag{4.1}$$

So a character of $G$ is completely determined if we define $\chi(a_1), \ldots, \chi(a_s)$. Since $a_i^{m_i} = e$, so, $\chi(a_i)$ is an $m_i^{th}$ root of unity. Conversely, let $\epsilon_i$ be any $m_i^{th}$ root of unity, then, for any $x \in G$ given by (4.1), we can define

$$\chi(x) = \epsilon_1^{k_1} \epsilon_2^{k_2} \ldots \epsilon_s^{k_s} \tag{4.2}$$

and this is well defined because the value of (4.1) is independent of the choice of $k_i$ (which are unique modulo $m_i$). Each root $\epsilon_i$ can be chosen in $m_i$ ways, so, there are $m_1 m_2 \ldots m_s$ characters of $G$. □

*Remark.* The set of all characters of a finite abelian group is a group under multiplication.

*Proof.* Let $\chi_1, \chi_2$ be characters of $G$. We have to show that $\chi_1\chi_2$ is a character of $G$. As

$$\chi_1\chi_2(gh) = \chi_1(gh)\chi_2(gh) = \chi_1(g)\chi_1(h)\chi_2(g)\chi_2(h) = \chi_1\chi_2(g)\chi_1\chi_2(h)$$

which implies that $\chi_1\chi_2$ is a character of $G$. Let the identity character be $\chi_0$, then $\chi\chi_0(g) = \chi(g)$ for all $g \in G$ since $\chi_0(g) = 1$ for all $g \in G$. For a character $\chi$ the inverse character is $\chi'(x) = \frac{1}{\chi(x)}$ for any $x \in G$. □

**Proposition 4.1.2.** *If $G$ is a finite abelian group and $H$ is a subgroup, then any character of $H$ can be extended to a character of $G$ and the number of such extensions equals the index of $H$ in $G$, i.e., $[G : H]$.*

*Proof.* Let $G$ be of order $n$ and $H$ be of order $m$. If we restrict a character $\chi$ of $G$ to $H$, we obtain a character of $H$. We denote this restriction by $\hat{\chi}$. It is clear that the map $\lambda$ sending $\chi \longrightarrow \hat{\chi}$ is a homomorphism from the group $X$ of characters of $G$ into the group $Y$ of characters of $H$. Let $A =$ krnel of the map $\lambda$, then $\chi \in A$ if and only if $\chi(g) = 1$ for all $g \in H$. It can be easily verified that the group $A$ is in one-one correspondence with the group of characters of $G/H$. Thus by previous proposition $|A| = |G/H| = \frac{n}{m}$. Now $\lambda : X \longrightarrow Y$ and $\ker(\lambda)$ has order $\frac{n}{m}$. By first Isomorphism Theorem, $X/A \cong \lambda(X)$. So order of $\lambda(X) = m$. But $Y$ has order $m$. Thus $\lambda(X) = Y$ which implies that $\lambda$ is onto. So in other words, given any character of $H$, it can be extended to a character of $G$ and the number of such extensions equals order$(A)= \frac{n}{m}$. □

**Corollary 4.1.3.** *Let $G$ be a finite abelian group. If $g \neq e$, $g \in G$, then there exists a character $\chi$ of $G$ such that $\chi(g) \neq 1$.*

*Proof.* Let $H$ be a subgroup of $G$ generated by $g$, $H \neq \{e\}$. Let $\psi$ be a non trivial character $\chi$ of $G$ such that $\psi(g) \neq 1$. By Proposition 4.1.2, we can extend character $\psi$ of $H$ to a character $\chi$ of $G$. So $\chi(g) = \psi(g) \neq 1$. □

**Proposition 4.1.4.** *Let $G$ be a finite abelian group of order $n$. Let $X$ be the group of characters of $G$, then*
*(i)* $\sum_{g\in G}\chi(g)$ *equals* $n$ *if* $\chi=\chi_0$ *and* $0$ *if* $\chi\neq\chi_0$.
*(ii)* $\sum_{\chi\in X}\chi(g)$ *equals* $n$ *if* $g=e$ *and* $0$ *if* $g\neq e$.

*Proof.* If $\chi=\chi_0$ then $\sum_{g\in G}\chi(g)=n$. Suppose $\chi\neq\chi_0$. Therefore there exists $z\in G$ such that $\chi(z)\neq 1$. As $g$ runs over all the elements of $G$ so does $gz$. Thus $\sum_{g\in G}\chi(g)=\sum_{g\in G}\chi(gz)=\chi(z)\sum_{g\in G}\chi(g)$. Since $\chi(z)\neq 1$ we see that $\sum_{g\in G}\chi(g)=0$.

If $g=e$, $\sum_{\chi\in X}\chi(g)=1+1+\cdots+1=n$. If $g\neq e$, then by Corollary 4.1.3, there exists a character $\chi'$ of $G$ such that $\chi'(g)\neq 1$. As $\chi$ runs over all the elements of $X$, so does $\chi\chi'$. Thus $\sum_{\chi\in X}\chi(g)=\sum_{\chi\in X}\chi\chi'(g)=\chi'(g)\sum_{\chi\in X}\chi(g)$. Since $\chi'(g)\neq 1$, we have $\sum_{\chi\in X}\chi(g)=0$. □

**Notation.** For any natural number $m$, let $G_m$ denote the multiplicative group of all residue classes modulo $m$, i.e., those cosets of group $\mathbb{Z}/m\mathbb{Z}$ which are of the form $m\mathbb{Z}+a$, $(a,m)=1$. $G_m$ is a group of order $\phi(m)$. The residue class mod $m$ which contains an integer $a$ will be denoted by $\bar{a}$. To every character $\chi$ of $G_m$, one can associate a function $\chi^*:\mathbb{Z}\longrightarrow\mathbb{C}$ defined by

$$\chi^*(a)=\begin{cases}\chi(\bar{a}) & if\ \ (a,m)=1\\ 0 & if\ \ (a,m)>1\end{cases}$$

Such a function is defined on $\mathbb{Z}$ is called a numerical character mod $m$. So a function $\chi^*:\mathbb{Z}\longrightarrow\mathbb{C}$ is called a numerical character modulo $m$ if it has the following properties
(i) $\chi^*(ab)=\chi^*(a)\chi^*(b)$ for all $a,b\in\mathbb{Z}$,
(ii) $\chi^*(a)=0$ if and only if $(a,m)>1$,
(iii) $\chi^*(a)=\chi^*(a')$ if $a\equiv a'(\text{mod } m)$.
So the number of numerical characters mod $m$ is $\phi(m)$. In future, we shall denote numerical character $\chi^*$ corresponding to a character $\chi$ of $G_m$ by $\chi$ again. So corresponding to the trivial character $\chi_0$ of $G_m$, we shall denote again by $\chi_0$, the numerical character mod $m$ which is defined by

$$\chi_0=\begin{cases}1 & if\ \ (a,m)=1\\ 0 & if\ \ (a,m)>1\end{cases}$$

It will be called the principal character mod $m$.

*Remark.* If $\chi$ is a numerical character mod $m$ and $\chi\neq\chi_0$, the principal character, then $\sum_g\chi(g)=0$ where $g$ runs over a reduced residue system or complete residue system mod $m$ by the first assertion of Proposition 4.1.4.

**Proposition 4.1.5.** *Let $\chi \neq \chi_0$ be a numerical character mod $m$, then the series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges uniformly on all the compact subsets of $(0,\infty)$ and represents a continuous function of $s$ in $(0,\infty)$. The convergence is absolute when $s \in (1,\infty)$.*

*Proof.* In view of Proposition 3.3.2 of the Chapter 3, it is enough to show that the sequence $P_n$ defined by $P_n = \sum_{j=1}^{n} \chi(j)$ is bounded. Fix any $n \geq 1$. By division algorithm, write $n = mq + r,\ 0 \leq r < m$. Each of the sets $T_0 = \{1, 2, \ldots, m\},\ T_1 = \{m+1, m+2, \ldots, 2m\},\ \ldots\ , T_i = \{im+1, im+2, \ldots, (i+1)m\},\ \ldots\ , T_{q-1}$ represents a complete residue system mod $m$, so by the remark before this proposition, $\sum_{x \in T_i} \chi(x) = 0$. Thus $\sum_{x=1}^{mq} \chi(x) = \sum_{i=0}^{q-1} \sum_{x \in T_i} \chi(x) = 0$. Therefore $P_n = \sum_{j=1}^{n} \chi(j) = \sum_{j=mq+1}^{mq+r} \chi(j)$. Hence $|P_n| \leq \sum_{j=mq+1}^{mq+r} |\chi(j)| \leq r \leq m-1$ for any $n \geq 1$. So by Proposition 3.3.2, $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges uniformly on compact subsets of $(0,\infty)$ and represents a continuous function of $s$ in $(0,\infty)$. Since the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges for $s > 1$ by Proposition 3.3.1, so the series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges absolutely for $s > 1$. □

**Definition.** For a numerical character $\chi$ mod $m$, we denote $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ by $L(s,\chi)$ and is called L-function attached with character $\chi$. Applying Proposition 3.4.2 ( with $a_n = \frac{\chi(n)}{n^s}$ for $s > 1$ ), we see that

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$$

In particular $L(s,\chi)$ does not vanish for $s > 1$.

## 4.2 Simplification of Dirichlet's Class Number Formula for Cyclotomic Fields

Let $K = \mathbb{Q}(\zeta)$, where $\zeta$ is a primitive $m^{th}$ root of unity, $m > 2$. It can be easily seen that the number of roots of unity in $K$ to be denoted by $w$ is $m$ or $2m$ according as $m$ is even or odd. We want to simplify class number formula for $K$. Keeping in mind that $K$ has no real isomorphisms, by Dirichlet's class number formula

$$\lim_{s \to 1^+} (s-1)\zeta_K(s) = \frac{h(2\pi)^{\frac{\phi(m)}{2}} R}{w\sqrt{|d_K|}}$$

where $R$ is the regulator of $K$. By Euler's Product Formula, $\zeta_K(s) = \prod_{\wp} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1}$. We shall write, the product of right hand side in a clear manner.

Let $K = \mathbb{Q}(\zeta)$, where $\zeta$ is a primitive $m^{th}$ root of unity. Then for $s > 1, \zeta_K(s) = \prod_{p} \prod_{\wp|p} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1}$. For $s > 0$, define $G(s) = \prod_{p|m} \prod_{\wp|p} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1}$.

Suppose $p$ is a rational prime that does not divide $m$. If $\wp$ is a prime ideal of $\mathcal{O}_K$ lying over $p$, then we denote the absolute residual degree of $\wp$ by $f_p$, it is independent of the choice of $\wp$ lying over $p$. In fact $f_p$ is the smallest positive integer such that $p^{f_p} \equiv 1 (\text{mod } m)$ . Also the number of distinct prime ideals $\wp$ of $\mathcal{O}_K$ lying over $p$ is $\frac{\phi(m)}{f_p}$.

$$\zeta_K(s) = G(s) \prod_{p \nmid m} \left(1 - \frac{1}{p^{s f_p}}\right)^{-\frac{\phi(m)}{f_p}} \tag{4.3}$$

We now make use of the following interesting device to write $1 - p^{-s f_p}$ in a convenient form. Let $\epsilon$ be primitive $f_p^{th}$ root of unity, $1 - x^{f_p} = \prod_{k=0}^{f_p - 1} (1 - \epsilon^k x)$. Thus for $x = p^{-s}$, we get, $1 - p^{-s f_p} = \prod_{k=0}^{f_p - 1} (1 - \epsilon^k p^{-s})$ and hence

$$(1 - p^{-s f_p})^{\frac{\phi(m)}{f_p}} = \prod_{k=0}^{f_p - 1} (1 - \epsilon^k p^{-s})^{\frac{\phi(m)}{f_p}} \tag{4.4}$$

Clearly the number of factors on the right hand side of the above equation is $\phi(m)$, which is independent of $p$. Thus, if we wish to combine terms corresponding to different rational primes $p$, then we have the same number of terms available to us. Let $\chi$ be any character of the group $G_m$ of reduced residue classes mod $m$. Since the class $\bar{p}$ has order $f_p$, $\chi(\bar{p})$ is an $f_p^{th}$ root of unity, and hence $\chi(\bar{p}) = \epsilon^k,\ 0 \leq k \leq f_p - 1,\ \epsilon = e^{\frac{2\pi\iota}{f_p}}$. Conversely if $\epsilon^k$ is taken then there exists exactly one character $\chi_1$ of the cyclic group generated by $\bar{p}$ such that $\chi_1(\bar{p}) = \epsilon^k$. Extend $\chi_1$ to $G_m$ and this can be done in exactly $\frac{\phi(m)}{f_p}$ ways by Proposition 4.1.2. Thus as $\chi$ runs through all characters of $G_m$, $\chi(\bar{p})$ takes each value $\epsilon^k,\ 0 \leq k \leq f_p - 1$, exactly $\frac{\phi(m)}{f_p}$ times. Therefore it follows from ( 4.3) , (4.4) that

$$\begin{aligned} \zeta_K(s) &= G(s) \prod_{p \nmid m} \prod_{k=0}^{f_p - 1} (1 - \epsilon^k p^{-s})^{\frac{\phi(m)}{f_p}} \\ &= G(s) \prod_{p \nmid m} \prod_{\chi} \left(1 - \frac{\chi(\bar{p})}{p^s}\right)^{-1}, \end{aligned}$$

where $\chi$ runs over all the characters of $G_m$. Now let us denote the numerical character mod $m$ which corresponds to $\chi$ again by $\chi$. Since $\chi(p) = 0$, if $p$ divides $m$ by definition of numerical character, so $\zeta_K(s) = G(s) \prod_{all\ p} \prod_{\chi} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, where $\chi$ runs over all numerical characters mod $m$. Therefore for $s > 1$

$$\zeta_K(s) = G(s) \prod_{\chi} \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} = G(s) \prod_{\chi} L(s, \chi) \tag{4.5}$$

where $\chi$ runs over all numerical characters mod $m$. If $\chi = \chi_0$ is the principal character mod $m$, then

$$L(s, \chi_0) = \prod_{all\ p} \left(1 - \frac{\chi_0(p)}{p^s}\right)^{-1} = \prod_{p \nmid m} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right)$$

because $\zeta(s) = \prod_{all\ p} \left(1 - \frac{1}{p^s}\right)^{-1}$ by Euler's Product formula. Thus we have shown that

$$\zeta_K(s) = F(s)\zeta(s) \prod_{\chi \neq \chi_0} L(s, \chi) \tag{4.6}$$

where $F(s) = \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \prod_{p|m} \prod_{\wp|p} \left(1 - \frac{1}{N(\wp)^s}\right)^{-1}$. Multiplying both sides of (4.6) by $s - 1$ and take limit as $s \to 1^+$, we see that $h\kappa = F(1) \prod_{\chi \neq \chi_0} L(1, \chi)$, where $L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n}$. This gives the following class number formula for cyclotomic fields.

$$h = \frac{F(1) \prod_{\chi \neq \chi_0} L(1, \chi)}{\kappa} = \frac{w\sqrt{|d_K|}}{2^{r+s}\pi^s R} F(1) \prod_{\chi \neq \chi_0} L(1, \chi) = \frac{w\sqrt{|d_K|}}{2^{\frac{\phi(m)}{2}}\pi^{\frac{\phi(m)}{2}} R} F(1) \prod_{\chi \neq \chi_0} L(1, \chi). \tag{4.7}$$

**Corollary 4.2.1.** *If $\chi$ is a non principal numerical character mod $m$, then $L(1, \chi) \neq 0$.*

## 4.3 Derivation of Dirichlet's Theorem for Primes in Arithmetic Progressions

Using the above corollary we prove the well known theorem by Dirichlet.

**Dirichlet's Theorem for primes in arithmetic progressions.** Let $m \geq 2$ be an integer. If $(a, m) = 1$, then there exists infinitely many primes $p \equiv a \bmod m$.

*Proof.* We need to prove when $m \geq 3$. Let $a, b \in \mathbb{Z}$. Let $\chi$ run over all the numerical characters modulo $m$. We first show that

$$\sum_{\chi} \bar{\chi}(a)\chi(b) = \begin{cases} \phi(m) & \text{if } a \equiv b \bmod m \\ 0 & \text{otherwise} \end{cases}$$

Let $a'$ be an integer such that $aa' \equiv 1 \bmod m$. Then $\bar{\chi}(a) = \frac{1}{\chi(a)} = \chi(a')$. So by Proposition 4.1.4,

$$\sum_{\chi} \bar{\chi}(a)\chi(b) = \sum_{\chi} \chi(a'b) = \begin{cases} \phi(m) & if \quad a'b \equiv 1 \bmod m \\ 0 & otherwise \end{cases}$$

Let $K = \mathbb{Q}(\zeta)$, $\zeta$ primitive $m$-th root of unity. We know that for $s > 1$,

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

Taking log on both sides, we see that

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

$$\begin{aligned} \sum_{\chi} \overline{\chi}(a) \log L(s, \chi) &= \sum_{p} \sum_{n=1}^{\infty} \sum_{\chi} \frac{\bar{\chi}(a)\chi(p^n)}{np^{ns}} \\ &= \sum_{p} \sum_{n} \frac{\phi(m)}{np^{ns}} \end{aligned}$$

where the second sum is over those $n$ for which $p^n \equiv a \bmod m$. So

$$\sum_{\chi} \overline{\chi}(a) \log L(s, \chi) = \phi(m) \sum_{p \,\equiv\, a \bmod m} \frac{1}{p^s} + \phi(m) \sum_{p} \sum_{n \geq 2,\ p^n \,\equiv\, a \bmod m} \frac{1}{np^{ns}}.$$

We show that the second sum on R.H.S. remains bounded for $s > 1$ and the sum on the L.H.S. $\to \infty$ as $s \to 1^+$. Therefore $\sum_{p \,\equiv\, a \bmod m} \frac{1}{p^s} \to \infty$ as $s \to 1^+$ and hence the theorem will be proved. For $s > 1$,

$$\sum_{p} \sum_{n \geq 2,\ p^n \,\equiv\, a \bmod m} \frac{1}{np^{ns}} \leq \sum_{p} \sum_{n=2}^{\infty} \frac{1}{np^{ns}} \leq \sum_{p} \frac{1}{p(p-1)}. \tag{4.8}$$

Recall that by Proposition 4.1.5 for $\chi \neq \chi_0$, $L(s,\chi)$ is continuous in $(0,\infty)$ and $L(s,\chi)$ does not vanish in $(0,\infty)$. So $\lim_{s\to 1^+} \log L(s,\chi) = \log L(1,\chi)$. Also in view of Corollary 4.2.1, $L(1,\chi) \neq 0$ for a non-principal character $\chi$ mod $m$; consequently $\lim_{s\to 1^+} \log L(s,\chi)$ is finite. In view of Euler product formula $L(s,\chi_0) = \prod_{p|m} \left(1 - \frac{1}{p^s}\right) \zeta(s)$. So $\log L(s,\chi_0) = \sum_{p|m} \log\left(1 - \frac{1}{p^s}\right) + \log \zeta(s)$ which tends to $\infty$ when $s \to 1^+$ as $\log \zeta(s)$ does so.

□

# 4.4 Simplification of Dirichlet's Class Number Formula for Quadratic Fields

For simplification of Dirichlet's Class Number Formula for Quadratic Fields, we recall the notions of Legendre Symbol, Kronecker Symbol and Jacobi Symbol and study their properties.

Recall that for an odd prime $p$ and an integer $n$, the Legendre Symbol $\left(\frac{n}{p}\right)$ is defined by

$$\left(\frac{n}{p}\right) = \begin{cases} 0 & if \;\; p|n \\ 1 & if \;\; x^2 \equiv n \bmod p \text{ is solvable and } \;\; p \nmid n, \\ -1 & if \;\; x^2 \equiv n \bmod p \text{ is not solvable} \end{cases}$$

The following are immediate consequences :

(i). If $m \equiv n (\text{mod } p)$, then $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right)$.

(ii). If $a, b \in \mathbb{Z}$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

**Definition.** We define Kronecker Symbol by

$$\left(\frac{n}{2}\right) = \begin{cases} 0 & \text{if } n \equiv 0 (\text{mod } 4) \\ 1 & \text{if } n \equiv 1 (\text{mod } 8) \\ -1 & \text{if } n \equiv 5 (\text{mod } 8) \end{cases}$$

This symbol is defined for $n \equiv 0, 1 (\text{mod } 4)$.

**Definition.** Let $m$ be a positive odd integer and $n \in \mathbb{Z}$. We define Jacobi Symbol $\left(\frac{n}{m}\right) = \prod_{i=1}^{r} \left(\frac{n}{p_i}\right)^{a_i}$, where $m = \prod_{i=1}^{r} p_i^{a_i}$, $p_i$ are distinct rational primes. The immediate consequences are

(i). If $n_1 \equiv n_2 (\text{mod } m)$, then $\left(\frac{n_1}{m}\right) = \left(\frac{n_2}{m}\right)$.

(ii). If $m_1, m_2$ are odd positive integers, then $\left(\frac{n}{m_1 m_2}\right) = \left(\frac{n}{m_1}\right)\left(\frac{n}{m_2}\right)$.

(iii). If $n_1, n_2$ are any integers, then $\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right)$.

(iv). If the congruence $x^2 \equiv n (\text{mod } m)$ is solvable and $(n, m) = 1$ then $\left(\frac{n}{m}\right) = 1$. The converse is false e.g. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1$ but $x^2 \equiv 2 (\text{mod } 15)$ is not solvable.

**Lemma 4.A.** If $n_1, n_2, \ldots, n_k$ are odd integers, then $\left(\prod_{i=1}^{k} n_i\right) - 1 \equiv \sum_{i=1}^{k} (n_i - 1) (\text{mod } 4)$.
(Can be easily proved by using induction on $k$.)

**Lemma 4.B.** If $n_1, n_2, \ldots, n_k$ are odd integers, then $\left(\prod_{i=1}^{k} n_i^2\right) - 1 \equiv \sum_{i=1}^{k} (n_i^2 - 1) (\text{mod } 16)$.
(Can be easily proved by using induction on $k$.)

Now we shall prove the following results using the above two lemmas and the standard formula $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{(p^2-1)}{8}}$ for odd primes $p$ and the Gauss reciprocity law [1] $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$ for distinct odd primes $p, q$.

(i). If $m > 0$ is odd, then $\left(\frac{-1}{m}\right) = (-1)^{\frac{(m-1)}{2}}$

(ii). Let $m$ be an odd positive integer, then $\left(\frac{2}{m}\right) = (-1)^{\frac{(m^2-1)}{8}}$

(iii). If $m, n$ are positive odd integers, then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$.

(see Theorem 5.9 [LeV]).

**Proof of (i).** Write $m = \prod p_i^{a_i}$. By definition $\left(\frac{-1}{m}\right) = \prod_i \left(\frac{-1}{p_i}\right)^{a_i} = (-1)^{\frac{\sum a_i (p_i - 1)}{2}}$. We have to prove that

$$\sum a_i (p_i - 1) \equiv m - 1 (\text{mod } 4). \qquad (*)$$

[1] Gauss Reciprocity Law is a relation connecting the values of the Legendre symbols $\left(\frac{p}{q}\right)$, $\left(\frac{q}{p}\right)$ for different odd prime numbers p and q. The reciprocity law for quadratic residues was first stated in 1772 by L. Euler. A. Legendre in 1785 formulated the law in modern form and proved a part of it. C.F. Gauss in 1801 was the first to give a complete proof of the law(cf. [Gau]) , which for this reason is called the Gauss reciprocity law.

Now by Lemma 4.A applied to $(p_i-1)+\cdots+(p_i-1) = a_i(p_i-1)$, we have $a_i(p_i-1) \equiv p_i^{a_i}-1 \mod 4$. Again applying the same lemma with $n_i = p_i^{a_i} - 1$, we see that

$$\sum a_i(p_i - 1) \equiv \sum (p_i^{a_i} - 1) \equiv (\prod p_i^{a_i}) - 1 \mod 4,$$

which proves the desired congruence.
**(ii).** It can be simply proved using Lemma 4.B.
**(iii).** It can be easily proved using (*).

**Definition. (Generalized Jacobi Symbol).** If $n$ is a negative integer, $n$ odd, we define for any integer $a$ coprime to $n$, $\left(\frac{a}{n}\right) = \left(\frac{a}{|n|}\right)$.

**Properties of Generalized Jacobi Symbol.** Let $m, n$ be odd integers which are coprime. Let $sgn(m)$ stands for $+1$ or $-1$ according as $m > 0$ or $m < 0$. Then the following can be quickly deduced from the above results.

(i). $\left(\frac{-1}{m}\right) = (-1)^{\frac{(m-1)}{2}+\frac{sgn(m)-1}{2}}$.

(ii). $\left(\frac{2}{m}\right) = (-1)^{\frac{(m^2-1)}{8}}$.

(iii). $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)}{2}\frac{(n-1)}{2}+\frac{sgn(m)-1}{2}\frac{sgn(n)-1}{2}}$.

Note that Jacobi reciprocity law for Generalized Jacobi symbol remains the same as for the Jacobi symbol when at least one of $m$ or $n$ is positive.

*Remark.* (i). If $a \equiv 1(\mod 4)$, then $\left(\frac{a}{2}\right) = \left(\frac{2}{a}\right)$.

(ii). $\left(\frac{aa'}{2}\right) = \left(\frac{a}{2}\right)\left(\frac{a'}{2}\right)$.

**Proof of (i).**If $a \equiv 1(\mod 8)$, then $\left(\frac{a}{2}\right) = 1$ and $\left(\frac{2}{a}\right) = (-1)^{\frac{(a^2-1)}{8}} = 1$. If $a \equiv 5(\mod 8)$, then $\left(\frac{a}{2}\right) = -1$, $\left(\frac{2}{a}\right) = -1$.

**Proof of (ii).** If any of $a, a' \equiv 0(\mod 4)$, both sides of (ii) are zero. So we can assume that both $a, a' \equiv 1(\mod 4)$. We have $\left(\frac{a}{2}\right) = \left(\frac{2}{a}\right) = (-1)^{\frac{(a^2-1)}{8}}$ and $\left(\frac{a'}{2}\right) = \left(\frac{2}{a'}\right) = (-1)^{\frac{(a'^2-1)}{8}}$. Also $(aa')^2 - 1 \equiv (a^2-1)(a'^2-1)(\mod 16)$ by Lemma 4.B. Therefore $(-1)^{\frac{(a^2a'^2-1)}{8}} = (-1)^{\frac{(a^2-1)+(a'^2-1)}{8}}$.

**Definition.** Let $a \equiv 0, 1(\mod 4)$ be any integer and let $n$ be any non-zero integer. We write $n = n_1 2^c$, where $2 \nmid n_1$, we define Jacobi-Kronecker symbol by $\left(\frac{a}{n}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{2}\right)^c$.

**Definition.** Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with discriminant $d_K$. We define a numerical character $\chi$ mod $|d_K|$ by setting $\chi(x) = 0$ if $(x, d_K) > 1$ and

$$\chi(x) = \begin{cases} \left(\frac{x}{|d|}\right) & \text{if } d \equiv 1 (\text{mod } 4) \\ (-1)^{\frac{(x-1)}{2}} \left(\frac{x}{|d|}\right) & \text{if } d \equiv 3 (\text{mod } 4) \\ (-1)^{\frac{(x^2-1)}{8} + \frac{x-1}{2}\frac{d'-1}{2}} \left(\frac{x}{|d'|}\right) & \text{if } d = 2d' \end{cases},$$

then $\chi$ is called a character of the field $K = \mathbb{Q}(\sqrt{d})$ .

It will be proved that $\chi$ is a numerical character mod $|d_K|$. We have to show that

(i). $\chi(xy) = \chi(x)\chi(y)$, for all $x, y \in \mathbb{Z}$.

(ii). If $x \equiv x' (\text{mod } |d_K|)$, then $\chi(x) = \chi(x')$.

**(i).** Clearly (i) needs to be verified only when $(xy, |d_K|) = 1$. We distinguish three cases.
**Case 1.** When $d \equiv 1 (\text{mod } 4)$, then

$$\chi(xy) = \left(\frac{xy}{|d|}\right) = \left(\frac{x}{|d|}\right)\left(\frac{y}{|d|}\right) = \chi(x)\chi(y).$$

**Case 2.** When $d \equiv 3 (\text{mod } 4)$, then $\chi(xy) = (-1)^{\frac{(xy-1)}{2}} \left(\frac{xy}{|d|}\right)$. By Lemma 4.A, $\frac{(xy-1)}{2} \equiv \frac{(x-1)}{2} + \frac{(y-1)}{2} (\text{mod } 2)$. It implies that $(-1)^{\frac{(xy-1)}{2}} = (-1)^{\frac{(x-1)}{2}}(-1)^{\frac{(y-1)}{2}}$. Thus $\chi(xy) = (-1)^{\frac{(x-1)}{2}}(-1)^{\frac{(y-1)}{2}} \left(\frac{x}{|d|}\right)\left(\frac{y}{|d|}\right) = \chi(x)\chi(y)$.
**Case 3.** When $2|d,\ d = 2d'$, then

$$\chi(xy) = (-1)^{\frac{(x^2y^2-1)}{8} + \frac{xy-1}{2}\frac{d'-1}{2}} \left(\frac{xy}{|d'|}\right) = (-1)^{\frac{(x^2y^2-1)}{8} + \frac{xy-1}{2}\frac{d'-1}{2}} \left(\frac{x}{|d'|}\right)\left(\frac{y}{|d'|}\right).$$

By Lemma 4.B, $\frac{(x^2y^2-1)}{8} \equiv \frac{(x^2-1)}{8} + \frac{(y^2-1)}{8} (\text{mod } 2)$. By Lemma 4.A, $\frac{xy-1}{2} \equiv \frac{x-1}{2} + \frac{y-1}{2} (\text{mod } 2)$. Therefore

$$\chi(xy) = (-1)^{\frac{(x^2-1)}{8} + \frac{(x-1)(d'-1)}{4}} \left(\frac{x}{|d'|}\right)(-1)^{\frac{(y^2-1)}{8} + \frac{(y-1)(d'-1)}{4}} \left(\frac{y}{|d'|}\right) = \chi(x)\chi(y).$$

**(ii).** To verify (ii), we again distinguish three cases and assume that $(x, d_K) = 1$.
**Case 1.** When $d \equiv 1 (\text{mod } 4)$, then $d_K = d$ and $\chi(x') = \left(\frac{x'}{|d|}\right) = \left(\frac{x'}{|d_K|}\right) = \left(\frac{x}{|d_K|}\right) =$

$\left(\frac{x}{|d|}\right) = \chi(x)$.

**Case 2.** When $d \equiv 3(\text{mod } 4)$, then $d_K = 4d$ and $\chi(x') = (-1)^{\frac{x'-1}{2}} \left(\frac{x'}{|d|}\right)$. Since $x \equiv x'(\text{mod } |d_K|)$ we have $x \equiv x'(\text{mod } 4)$. Thus $\frac{x-1}{2} \equiv \frac{x'-1}{2}(\text{mod } 2)$. Also $x \equiv x'(\text{mod } |d_K|)$ implies that $x \equiv x'(\text{mod } |d|)$ which in turn implies that $\left(\frac{x}{|d|}\right) = \left(\frac{x'}{|d|}\right)$. Thus $\chi(x') = (-1)^{\frac{x'-1}{2}} \left(\frac{x'}{|d|}\right) = (-1)^{\frac{x-1}{2}} \left(\frac{x}{|d|}\right) = \chi(x)$.

**Case 3.** If $d = 2d'$, then $d_K = 4d = 8d'$, $d'$ is odd. Since $x \equiv x'(\text{mod } |d_K|)$ we have $x \equiv x'(\text{mod } |d'|)$. Therefore $\left(\frac{x}{|d'|}\right) = \left(\frac{x'}{|d'|}\right)$. Also $x \equiv x'(\text{mod } 8)$ implies that $x - 1 \equiv x' - 1 \text{ (mod } 4)$ which implies that $\frac{x-1}{2} \equiv \frac{x'-1}{2} \text{ (mod } 2)$. Therefore $(-1)^{\frac{x-1}{2}} = (-1)^{\frac{x'-1}{2}}$ and $x, x'$ are both odd. Also $x^2 - x'^2 \equiv (x + x')(x - x') \equiv 0(\text{mod } 16)$. It implies that $\frac{x^2-1}{8} \equiv \frac{x'^2-1}{8} \text{ (mod } 2)$. Thus $\chi(x) = \chi(x')$.

**Lemma 4.4.1.** *Let $\mathbb{Q}(\sqrt{d})$ and $\chi$ be as above. Then prove that $\chi(x) = \left(\frac{d_K}{x}\right) \ \forall\ x > 0$.*

*Proof.* We only need to prove it when $(x, d_K) = 1$.

**Case 1.** When $d \equiv 1(\text{mod } 4)$. This case is split in three subcases :

**Subcase (i).** Let $x$ be odd. By Generalized Jacobi's reciprocity law,

$$\chi(x) = \left(\frac{x}{|d|}\right) = \left(\frac{x}{d}\right) = \left(\frac{d}{x}\right)(-1)^{\frac{(x-1)(d-1)}{4}} = \left(\frac{d}{x}\right) = \left(\frac{d_K}{x}\right).$$

**Subcase (ii).** Let $x = 2^r y$ with $r$ even and $y$ odd. Then

$$\left(\frac{d_K}{x}\right) = \left(\frac{d}{x}\right) = \left(\frac{d}{2}\right)^r \left(\frac{d}{y}\right) = \left(\frac{d}{y}\right) = (-1)^{\frac{(y-1)(d-1)}{4}} \left(\frac{y}{d}\right) = \left(\frac{y}{d}\right).$$

And $\left(\frac{y}{d}\right) = \left(\frac{y}{d}\right)\left(\frac{2}{d}\right)^r = \left(\frac{x}{d}\right) = \left(\frac{x}{|d|}\right) = \chi(x)$.

**Subcase (iii).** Let $x = 2^r y$, with $y$ odd and $r$ odd. We have

$$\begin{aligned}\left(\frac{d_K}{x}\right) = \left(\frac{d}{x}\right) = \left(\frac{d}{2}\right)^r \left(\frac{d}{y}\right) &= (-1)^{\frac{d^2-1}{8}r} \left(\frac{d}{y}\right) \\ &= (-1)^{\frac{d^2-1}{8}} (-1)^{\frac{(y-1)(d-1)}{4}} \left(\frac{y}{d}\right) \\ &= (-1)^{\frac{d^2-1}{8}} \left(\frac{y}{d}\right) = \left(\frac{2}{d}\right)\left(\frac{y}{d}\right) = \left(\frac{2y}{d}\right) = \left(\frac{2^r y}{d}\right)\end{aligned}$$

because $\left(\frac{2^{r-1}}{d}\right) = 1$.

**Case 2.** Let $d \equiv 3(\text{mod } 4)$ with $x$ odd. We have

$$\left(\frac{d_K}{x}\right) = \left(\frac{4d}{x}\right) = \left(\frac{d}{x}\right) = (-1)^{\frac{(x-1)(d-1)}{4}} \left(\frac{x}{d}\right) = (-1)^{\frac{(x-1)}{2}} \left(\frac{x}{d}\right) = \chi(x).$$

**Case 3.** Let 2 divides $d$ i.e., $d = 2d'$. We have

$$\left(\frac{d_K}{x}\right) = \left(\frac{8d'}{x}\right) = \left(\frac{2d'}{x}\right) = \left(\frac{2}{x}\right)\left(\frac{d'}{x}\right)$$
$$= (-1)^{\frac{x^2-1}{8}+\frac{(x-1)(d'-1)}{4}}\left(\frac{x}{d'}\right) = \chi(x)$$

□

The above lemma together with result of factoring primes in quadratic number fields (see Theorem 10.2.1 of [Al-Wi] ) yields the following result.

**Proposition 4.4.2.** *Let $\mathbb{Q}(\sqrt{d})$ be a quadratic field with discriminant $d_K$ and let $\chi$ be the character associated with $\mathbb{Q}(\sqrt{d})$. Then $\chi(p) = \left(\frac{d_K}{p}\right)$ for all primes $p$ and the following holds :*

$$\chi(p) = \begin{cases} 1 & \text{if } p\mathcal{O}_K = \wp\wp',\ N(\wp) = N(\wp') = p \\ -1 & \text{if } p\mathcal{O}_K = \wp,\ N(\wp) = p^2 \\ 0 & \text{if } p\mathcal{O}_K = \wp^2 \end{cases}$$

**Dirichlet's Class Number Formula for Quadratic Fields.**
Let $K$ be a quadratic field with discriminant $d_K$. For $s > 1$,

$$\begin{aligned}\zeta_K(s) &= \prod_p \prod_{\wp|p}\left(1 - \frac{1}{N(\wp)^s}\right)^{-1} \\ &= \prod_{p|d_K}\prod_{\wp|p}\left(1 - \frac{1}{N(\wp)^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=1}\prod_{\wp|p}\left(1 - \frac{1}{N(\wp)^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=-1}\prod_{\wp|p}\left(1 - \frac{1}{N(\wp)^s}\right)^{-1} \\ &= \prod_{p|d_K}\left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=1}\left(1 - \frac{1}{p^s}\right)^{-2} \prod_{\left(\frac{d_K}{p}\right)=-1}\left(1 - \frac{1}{p^{2s}}\right)^{-1}.\end{aligned}$$

By Proposition 4.4.2,we have $\chi(p) = \left(\frac{d_K}{p}\right)$. Thus for $s > 1$, we have

$$\zeta_K(s) = \prod_{p|d_K}\left(1 - \frac{1}{p^s}\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=1}\left((1 - \frac{\chi(p)}{p^s})(1 - \frac{1}{p^s})\right)^{-1} \prod_{\left(\frac{d_K}{p}\right)=-1}\left((1 - \frac{\chi(p)}{p^s})(1 - \frac{1}{p^s})\right)^{-1}$$

So

$$\zeta_K(s) = L(s,\chi)\zeta(s) \tag{4.9}$$

in view of the fact that $\chi(p) = 0$ when $p|d_K$ and $L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$. Multiply both sides of (4.9) by $s-1$ and take the limits as $s \to 1^+$, we see in view of Dirichlet's class number formula that $h\kappa = L(1,\chi)$ because $L(s,\chi)$ is a continuous function in $(0,\infty)$ by Proposition 4.1.5 and $\chi$ is a non-trivial character in view of Lemma 4.4.4. So

$$h = \frac{L(1,\chi)}{\kappa} = \begin{cases} \frac{L(1,\chi)\sqrt{d_K}}{2\log\epsilon} & \text{if } d_K > 0 \\ \frac{mL(1,\chi)\sqrt{|d_K|}}{2\pi} & \text{if } d_K < 0 \end{cases} \tag{4.10}$$

where $m$ is the number of roots of unity in $K$ and $\epsilon > 1$ is the fundamental unit of $\mathcal{O}_K$ when $d_K$ is positive.

The corollary stated below is an immediate consequence of (4.10).

**Corollary 4.4.3.** *Let $\chi$ be the character associated with quadratic field having discriminant $d_K$. Then $L(1,\chi) > 0$ i.e., $\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{d_K}{n}\right) > 0$.*

Now, we shall give the following important result for the character of a quadratic field.

**Lemma 4.4.4.** *The character $\chi$ of a quadratic field $\mathbb{Q}(\sqrt{d})$ is always non-trivial.*

*Proof.* The proof is split into three cases.
**Case 1.** When $d \equiv 1 (\text{mod } 4)$. Choose a prime $p$ such that $p|d$, $p$ an odd prime. Choose an integer $s$ such that $\left(\frac{s}{p}\right) = -1$. By Chinese Remainder Theorem, there exists an integer $x$ such that $x \equiv s (\text{mod } p)$ and $x \equiv 1 (\text{mod } \frac{d}{p})$. Claim is that $\chi(x) = -1$. This happens since

$$\chi(x) = \left(\frac{x}{|d|}\right) = \left(\frac{x}{p}\right)\left(\frac{x}{\frac{|d|}{p}}\right) = \left(\frac{s}{p}\right) = -1.$$

**Case 2.** When $d \equiv 3 (\text{mod } 4)$, $d_K = 4d$. By Chinese remainder theorem, there exists an integer $x$ such that

$$x \equiv 1 (\text{mod } d),\ x \equiv 3 (\text{mod } 4),$$

then $\chi(x) = (-1)^{\frac{x-1}{2}}\left(\frac{x}{|d|}\right) = -1$.
**Case 3.** When $d = 2d'$. By Chinese remainder theorem, there exists an integer $x$ such that

$$x \equiv 5 (\text{mod } 8),\ x \equiv 1 (\text{mod } d'),$$

then, $\chi(x) = (-1)^{\frac{x^2-1}{8} + \left(\frac{x-1}{2}\right)\left(\frac{d'-1}{2}\right)}\left(\frac{x}{|d'|}\right) = -1$ □

# Bibliography


[Al-Wi] Saban Alaca and Kenneth S. Williams, *Introductory Algebraic Number Theory*, Cambridge University Press, Cambridge, 2004.

[Bo-Sh] A. I. Borevich and I. R. Shafarevich, *Number Theory*, Translated from the Russian by Newcomb Greenleaf. Pure and Applied Mathematics, Vol.20 Academic Press, New York-London, 1966.

[Bak] A. Baker, *Linear Forms in the Logarithms of Algebraic Numbers*. Mathematika, Vol.13, 1966, 204-216.

[Bur] David M. Burton, *Elementary Number Theory*,(Sixth Edition). McGraw-Hill Higher Education, New York, 2007.

[Car] L.Cartlitz, *A characterization of algebraic number fields with class number two*, Proceedings of the American Mathematical Society 11 (1960), 391-392.

[Ded] R. Dedekind, *Theory of Algebraic Integers*, Cambridge University Press, Cambridge, 1996.

[Es-Mu] M. Ram Murty and Jody Esmonde, *Problems in Algebraic Number Theory*, Graduate Texts in Mathematics, 190. Springer-Verlag, New York, 1999.

[Gau] C.F. Gauss, *Disquisitiones Arithmeticae*(1801), English Translation, Yale Univ. Press (1966).

[Ir-Ro] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, (Second Edition). Graduate Texts in Mathematics, 84. Springer-Verlag, New York, 1990.

[Kha] S. K. Khanduja, *Notes of Algebraic Number Theory*.

[LeV] William J. LeVeque, *Fundamentals of Number Theory*. Addison Wesley Publishing, 1977.

[Lu-Pa] I. S. Luthar, I. B. S. Passi. *Algebra Volume 2 Rings*, (First Edition). Narosa Publishing House, 2002.

[Nar] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, (Third Edition). Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2004.

[Niv] I.Niven, H.S. Zukerman, H.L. Montgomery, *An introduction to the theory of numbers*, John Wiley and Sons, Canada, 1991.

[Sta] H. M. Stark, *A Complete Determination of the Complex Quadratic Fields of Class-Number One.* Michigan Math.J. , Vol.14, 1967, 1-27.

[Ta-St] David Tall, Ian Stewart, *Algebraic Number Theory and Fermat's Last Theorem*, (Fourth Edition). CRC Press, 2016.