DOKUZ EYLÜL UNIVERSITY
GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

PRIME IDEAL THEOREM ON NUMBER FIELDS

by
Hikmet Burak ÖZCAN

July, 2020
İZMİR

PRIME IDEAL THEOREM ON NUMBER FIELDS

A Thesis Submitted to the
Graduate School of Natural And Applied Sciences of Dokuz Eylül University
In Partial Fulfillment of the Requirements for the Degree of Master of
Science in Mathematics

by
Hikmet Burak ÖZCAN

July, 2020
İZMİR

M.Sc THESIS EXAMINATION RESULT FORM

We have read the thesis entitled "**PRIME IDEAL THEOREM ON NUMBER FIELDS**" completed by **HIKMET BURAK ÖZCAN** under supervision of **ASST. PROF. DR. HAYDAR GÖRAL** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

....

Asst. Prof. Dr. Haydar GÖRAL

Supervisor

....

Prof. Dr. Noyan Fevzi ER

Jury Member

....

Dr. Öğr. Üyesi Neslihan GÜGÜMCÜ

Jury Member

Prof. Dr. Özgür ÖZÇELİK
Director
Graduate School of Natural and Applied Sciences

ACKNOWLEDGEMENTS

First, I would like to offer my most sincere thankfulness to my supervisor Asst. Prof. Dr. Haydar GÖRAL for his encouragement for number theory, endless patience from the moment I started studying with him and precious guidance. It would be impossible without his help.

I am thankful to Prof. Dr. Noyan Fevzi ER and Asst. Prof. Dr. Neslihan GÜGÜMCÜ for their welcome to take part in the thesis defense jury. In particular, I would like to thank Prof. Dr. Noyan Fevzi ER for watching my progress in mathematics closely and for encouraging me to study what I like.

I would like to express my deepest thanks to Sedef TAŞKIN for spending her time to talk not only my thesis but almost everything. She was with me from the first to the last moment of my thesis.

I would like to thank my friends Çağatay ALTUNTAŞ and Mustafa Kutay KUTLU, who always gave me motivation when I was very overwhelmed. When I had problems, they were ready to help.

I sincerely thank Doğa Can SERTBAŞ for reading my thesis line by line and making critical corrections and valuable comments.

I would like to thank my grandparents Aynur ÖZCAN and Rifat ÖZCAN not only for my graduate education but also for supporting me during all my education.

Finally, I must emphasize that I am very grateful to my mother Leyla ÖZCAN and my father Murat ÖZCAN for supporting me over the years. They were always with me in any difficulties.

Hikmet Burak ÖZCAN

PRIME IDEAL THEOREM ON NUMBER FIELDS

ABSTRACT

In this study, our aim is to present a proof of the prime ideal theorem. It states that there is an asymptotic formula for the function $\pi_K(n)$ defined as the number of prime ideals with norm at most n in the ring of integers of a number field. In fact, it is a number field generalization of the prime number theorem. The prime ideal theorem was proved by Edmund Landau in 1903. In Landau's original proof, he gave an asymptotic formula with an error term for the number of prime ideals whose norms are less than or equal to n. In this thesis, using a weak version of the Wiener Ikehara Tauberian Theorem we will give another proof for the prime ideal theorem without an error term.

Keywords: Prime ideal theorem, number field, ring of integers, Wiener Ikehara Tauberian theorem

SAYI CİSİMLERİ ÜZERİNDEKİ ASAL İDEAL TEOREMİ

ÖZ

Bu çalışmada amacımız, bir sayı cisminin tam sayılar halkasında normu en fazla n olan asal ideallerin sayısını veren fonksiyona asimtotik bir formül veren asal ideal teoremini kanıtlamaktır. Aslında, bu teorem asal sayı teoreminin sayı cisimlerine bir genellemesi olarak görülür. Asal ideal teoremi, 1903'te Edmund Landau tarafından kanıtlanmıştır. Landau, orijinal kanıtında normları n'ye eşit veya daha az olan asal ideallerin sayısı için hata terimini de içeren bir asimtotik formül verir. Bu tezde ise biz Wiener Ikehara Tauberian Teoremi'nin zayıf bir versiyonunu kullanarak hata terimi olmadan asal ideal teoremi için orijinal kanıttan farklı başka bir kanıt vereceğiz.

Anahtar kelimeler: Asal ideal teoremi, sayı cismi, tam sayılar halkası, Wiener Ikehara Tauberian teoremi

CONTENTS

CHAPTER ONE
INTRODUCTION

Algebraic theory of numbers is a branch of the number theory dealing with the generalizations of the usual arithmetic of natural numbers in a more general setting. At heart, we want to study number theory in extended structures of the set of rational numbers, called number fields. In general, in order to deal with the theory of numbers we figure out the properties of integers rather than rational numbers. Therefore, we discover the set of integers of number fields satisfying algebraic properties similar to those of integers in rational numbers. In number fields, we call it the ring of integers. Then, we study analogues of the fundamental subjects of number theory in the ring of integers such as theory of prime numbers, divisibility, fundemental theorem of arithmetic, arithmetic (or number-theoretic) functions and so on. In addition to this, we are interested in some generalizations of significant results of number theory including the prime number theorem.

The prime number theorem provides an asymptotic formula for the function $\pi(n)$ that equals the number of prime numbers less than some positive n. In history, many famous mathematicians were closely interested in the question of counting primes. For instance, Gauss observed that $\pi(n)$ is asymptotic to the function $n/\log n$ when he was only 15. After that, he conjectured that the prime counting function $\pi(n)$ and the logarithmic integral $Li(n) = \int_2^n \frac{dt}{\log t}$ are asymptotic. In 1896, Charles Jean de la Vallée Poussin and Jacques Hadamard proved Gauss' claim independently. In mathematics, this is a well-known result called the prime number theorem. Furthermore, de la Vallée Poussin showed in his subsequent paper that

$$\pi(n) = Li(n) + O\big(n \exp\big(-c\sqrt{\log n}\big)\big), \tag{1.1}$$

where c is positive. Both proofs are based on the analytic features of the Riemann zeta function. In particular, the non-vanishing of the Riemann zeta function $\zeta(s)$ for any $s \in \mathbb{C}$ with $\Re(s) \geq 1$ is a crucial step of the proofs. For more detailed information about the prime number theorem we refer the reader to Davenport (2000).

In this thesis, we are concerned with a generalization of the prime number theorem. In algebraic theory of numbers, the generalization is a well-known result, called the prime ideal theorem. In 1903, Edmund Landau gave an asymptotic formula for the function $\pi_K(n)$, which equals the number of prime ideals with norm at most n in the ring of integers of a number field. He showed in his paper that

$$\pi_K(n) = Li(n) + O_K\big(n \exp\big(-b\sqrt{\log n}\big)\big), \tag{1.2}$$

where $b = b(K)$ is a constant. We can directly notice that it is the same formula for the function $\pi(n)$ in the prime number theorem. Thus, the prime number theorem can be generalized as the prime ideal theorem on number fields.

This thesis consists in two main parts. In the former part, we study the algebraic structure of the ring of integers, introduce the notion of the norm of an ideal of the ring of integers, and prove that it is always a finite number and a completely multiplicative function on the set of ideals of the ring of integers.

The latter part contains analytic tools for the prime ideal theorem. First, we shall mention a few of its equivalent statements. They involve analogues of the functions $\psi(x)$ and $\theta(x)$ known as Chebyshev auxilary functions. Then, for a given number field we will define its Dedekind zeta function. In fact, this generalizes the Riemann zeta function, too. We will investigate some analytic properties of the Dedekind zeta function. For instance, we will prove that it doesn't take the value 0 for any s with $\Re(s) = 1$. These analytic properties have a vital place in the proof of our main result. After showing the Wiener-Ikehara Tauberian theorem in its weaker form, we will obtain the proof of the prime ideal theorem.

CHAPTER TWO
PRELIMINARIES

2.1 Dedekind Domains

The major purpose of the first section is to prove that an arbitrary non-zero ideal of a Dedekind domain is expressed as a product of prime ideals in a unique way. For more details about Dedekind domains the reader might consult Samuel (1970).

Definition 2.1.1. *We say that an integral domain R is a Dededind domain if it satisfies the following properties:*

1. *R is Noetherian, namely, every non-empty subset of ideals of R has a maximal element.*
2. *R is integrally closed, that is, every element of the field of fractions of R which is a root of a monic polynomial with coefficients in R is an element of R.*
3. *R has a Krull dimension 1, which means that non-zero prime ideals of R are maximal.*

For instance, $\mathbb{Z}$ is a Dedekind domain.

Definition 2.1.2. *Let R be an integral domain and K denote its field of fractions. An R-submodule $\mathfrak{a}$ of K is called a fractional ideal of R if there is a non-zero $r \in R$ such that $r\mathfrak{a} \subseteq R$.*

Definition 2.1.3. *An ideal $\mathfrak{a}$ of R is said to be invertible if $\mathfrak{a}\mathfrak{a}^{-1} = R$, where $\mathfrak{a}^{-1} = \{k \in K \mid k\mathfrak{a} \subseteq R\}$.*

Lemma 2.1.1 (Samuel (1970))**.** *Assume that R is a Dedekind domain, which is not a field. Then, each prime ideal $\mathfrak{p}$ of R is an invertible ideal and $\mathfrak{p}^{-1}$ is a fractional ideal of R.*

Theorem 2.1.2. *All non-zero ideals of a Dedekind domian R can be factored into prime ideals in a unique way.*

Proof. We define S as the set of non-zero ideals of R which do not factor into prime ideals. We claim that S is empty. Suppose to the contrary that S is not empty. We have a maximal element in S due to the noetherianity of R. Let us call it $\mathfrak{a} \neq R$, since R can be seen as an empty factorization of primes. Choose a maximal ideal $\mathfrak{m}$ which contains $\mathfrak{a}$. As $\mathfrak{m}$ is also a prime ideal, $\mathfrak{m}\mathfrak{m}^{-1} = R$. Hence, multiplying both sides of $\mathfrak{a} \subseteq \mathfrak{m}$ by the fractional ideal $\mathfrak{m}^{-1}$, we obtain that $\mathfrak{a}\mathfrak{m}^{-1} \subseteq R$. As $\mathfrak{m}^{-1} \supsetneq R$, we have that $\mathfrak{a}\mathfrak{m}^{-1} \supsetneq \mathfrak{a}$. If we had $\mathfrak{a} = \mathfrak{a}\mathfrak{m}^{-1}$, this would imply $\mathfrak{a}\mathfrak{m} = \mathfrak{a}\mathfrak{m}^{-1}\mathfrak{m} = \mathfrak{a}R$. Thus, $\mathfrak{a}\mathfrak{m}^{-1}$ does not belong to S. Therefore, we obtain that

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n \mathfrak{m}, \tag{2.1}$$

where $\mathfrak{p}_i$ is a prime ideal in R for all $i = 1, \ldots, n$. As maximal ideals are also prime, $\mathfrak{a}$ factors into prime ideals. It is a contradiction.

Now, we will show the uniqueness part. Assume that $\mathfrak{a}$ is able to be written as a product of prime ideals in two ways :

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_n = \mathfrak{q}_1 \cdots \mathfrak{q}_m, \tag{2.2}$$

where $n \leq m$ and $\mathfrak{p}_i, \mathfrak{q}_j$ are all prime ideals. Since $\mathfrak{p}_1 \mid \mathfrak{q}_1 \cdots \mathfrak{q}_m$, we have $\mathfrak{p}_1 \mid \mathfrak{q}_j$ for some j. This means that $\mathfrak{p}_i \supseteq \mathfrak{q}_j$ for some j. Let us suppose $\mathfrak{p}_1 \supseteq \mathfrak{q}_1$ without loss of generality. However, R is of Krull dimension 1. Thus, we deduce that $\mathfrak{p}_1 = \mathfrak{q}_1$. After removing the same factors, we obtain that

$$\mathfrak{p}_2 \cdots \mathfrak{p}_n = \mathfrak{q}_2 \cdots \mathfrak{q}_m. \tag{2.3}$$

Similarly, we can obtain that $\mathfrak{p}_2 = \mathfrak{q}_2$ and $\mathfrak{p}_3 \cdots \mathfrak{p}_n = \mathfrak{q}_3 \cdots \mathfrak{q}_m$. Continuing in that manner, we eventually arrive at

$$R = \mathfrak{q}_{n+1} \cdots \mathfrak{q}_m. \tag{2.4}$$

This is a contradiction. Therefore, $n = m$ which makes the two factorization of $\mathfrak{a}$ unique. □

Note that the converse is also valid. Hence, this is a characterization of Dedekind domains.

Theorem 2.1.3 (Samuel (1970))**.** *For an integral domain R, TFAE:*

1. *R is a Dedekind domain.*
2. *All non-zero proper ideals $\mathfrak{a}$ of R are expressed as a product of prime ideals in a unique way.*

Note that there are several characterizations of Dedekind domains. For more details the reader might consult Samuel (1970).

2.2 Extension Fields

Definition 2.2.1. *We say that L is an extension field of a field K if K is subfield of L.*

We define $K(\alpha) = \{p(\alpha) : p(X) \in K(X)\}$, where K is a field. It is an extension field of K. For instance, the field $\mathbb{Q}(i)$ is an extension field of rational numbers $\mathbb{Q}$, whereas $\mathbb{C}$ is an extension field of both $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$. The reader may find the following results and more about extension fields in Fraleigh (2003).

Definition 2.2.2. *Suppose that L is an extension field of a field K. We say that $\alpha \in L$ is algebraic over K provided that $K[X]$ contains a non-zero polynomial $q(X)$ so that $q(\alpha) = 0$. If α is no algebraic, we call α transcendental over K.*

Let us illustrate the definition with an example. As $i \in \mathbb{C}$ is a root of $X^2 + 1$, we see that i is algebraic over $\mathbb{Q}$. In contrast, the real numbers π and e are transcendental.

Lemma 2.2.1. *Suppose that L is an extension field of a field K and $\alpha \in L$. If α is algebraic over K, then we can find a unique monic polynomial $q(X) \in K[X]$ having smallest degree with $q(\alpha) = 0$.*

Proof. As α is algebraic over K, there is a non-zero polynomial $f(X) \in K[X]$

$$f(X) = a_n X^n + \cdots + a_1 X + a_0, \tag{2.5}$$

so that $f(\alpha) = 0$. Since $a_n \neq 0$, we obtain a polynomial by dividing left hand side by a_n:

$$X^n + \cdots + \frac{a_1}{a_n} X + \frac{a_0}{a_n} \tag{2.6}$$

Note that α is a root of this non-zero monic polynomial, as well. Now, let $q(X)$ be a monic polynomial with smallest degree such that $q(\alpha) = 0$. We will show that $q(X)$ is unique. Assume to the contrary that $h(X)$ is another monic polynomial of the degree of $q(X)$ so that $h(\alpha) = 0$. Since both $q(X)$ and $h(X)$ are monic, the degree of the difference $(q - h)(X)$ is smaller than the degrees of $q(X)$ and $h(X)$ and we also have $(q-h)(\alpha) = 0$. Dividing by its leading coefficient again, we obtain a monic polynomial having α as a root and its degree is smaller than that of $q(X)$. It contradicts the choice of $q(X)$. Therefore, $q(X)$ is the unique monic polynomial such that $q(\alpha) = 0$. □

Definition 2.2.3. *The polynomial $q(X)$ in Lemma 2.2.1 is called the minimal polynomail of α.*

Definition 2.2.4. *An extension field L of a field K is said to be a simple extension if $L = K(\gamma)$ for some $\gamma \in L$.*

Theorem 2.2.2. *Suppose that $L = K(\gamma)$ for some $\gamma \in L$ and γ is algebraic over K. Then, we can express an element α of L in a unique way as follows:*

$$\alpha = a_{n-1}\gamma^{n-1} + \cdots + a_1\gamma + a_0, \tag{2.7}$$

where the minimal polynomial of γ over K has degree n and $a_i \in K$ for all $i = 0, \ldots, n-1$.

Proof. Note that we are able to consider an element of $K(\gamma)$ as a linear combination of powers of γ with coefficients in K by using the evaluation homomorphism

$$\begin{aligned}\phi_\gamma : & K[X] \longrightarrow K(\gamma)\\ & q(X) \mapsto q(\gamma).\end{aligned}$$

Suppose that

$$m(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0 \tag{2.8}$$

is the minimal polynomial of γ over K, where $c_i \in K$ for all $i = 0, \ldots, n-1$. As $m(\gamma) = 0$, we see that

$$\gamma^n = -c_{n-1}\gamma^{n-1} - \cdots - c_1\gamma - c_0. \tag{2.9}$$

Multiply the equation (2.9) by γ. Then, we obtain that

$$\begin{aligned}\gamma^{n+1} &= -c_{n-1}\gamma^n - c_{n-2}\gamma^{n-1} \cdots - c_0\gamma && (2.10)\\ &= -c_{n-1}(-c_{n-1}\gamma^{n-1} - \cdots - c_1\gamma - c_0) - c_{n-2}\gamma^{n-1} \cdots - c_0\gamma. && (2.11)\end{aligned}$$

Using this argument repeatedly, we see that for $m \geq n$ every monomial γ^m can be represented as a linear combinations of $1, \gamma, \ldots, \gamma^{n-1}$ with coefficients in K. Therefore, each $\alpha \in K(\gamma)$ has a form as follows:

$$\alpha = a_{n-1}\gamma^{n-1} + \cdots + a_1\gamma + a_0, \tag{2.12}$$

$a_i \in K$ for every $i = 0, \ldots, n-1$.

It remains to show the uniqueness part. Suppose that

$$a_{n-1}\gamma^{n-1} + \cdots + a_1\gamma + a_0 = a'_{n-1}\gamma^{n-1} + \cdots + a'_1\gamma + a'_0, \tag{2.13}$$

where $a'_i \in F$ for every $i = 0, \ldots, n-1$. Then, we obtain that

$$f(X) = (a_{n-1} - a'_{n-1})X^{n-1} + \cdots + (a_1 - a'_1)X + (a_0 - a'_0) \tag{2.14}$$

so that $f(\gamma) = 0$. Now, deg $f(X) <$ deg $m(X)$. This forces a_i to be equal a'_i for every $i = 0, \ldots, n-1$. Hence, we get the uniqueness. □

Definition 2.2.5. *An extension field L of a field K is called finite degree provided that the dimension of L as a vector space over K is finite. In this case,* $\dim(L_K)$ *is called the degree of L over K and denoted by $[L : K]$.*

Theorem 2.2.3. *Suppose that $K \subseteq L$ and $L \subseteq T$ are finite degree extensions. Then, $K \subseteq T$ is a finite degree extension and*

$$[T : K] = [T : L][L : K]. \tag{2.15}$$

Proof. Assume that $n = [L : K]$ and $m = [T : L]$ so that $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of L over K, while $\{\beta_1, \ldots, \beta_m\}$ is a basis of T over L. We claim that

$$\{\alpha_i\beta_j \mid i = 1, \cdots, n \text{ and } j = 1, \cdots, m\} \tag{2.16}$$

forms a basis of T over L and it is immediately seen that

$$[T : K] = [T : L][L : K]. \tag{2.17}$$

Take an arbitray element $\gamma \in T$. Then, we have that

$$\gamma = \sum_{j=1}^{m} b_j\beta_j \tag{2.18}$$

for some $b_j \in L$. As $\{\alpha_1, \ldots, \alpha_n\}$ is a basis of L over K, we obtain that

$$b_j = \sum_{i=1}^{n} a_{ij}\alpha_i \tag{2.19}$$

for some $a_{ij} \in K$. Thus, we see that

$$\gamma = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} a_{ij}\alpha_i \right) \beta_j = \sum_{i,j} a_{ij}(\alpha_i\beta_j). \tag{2.20}$$

Therefore, the mn elements $\alpha_i\beta_j$ span T over K.

For linear independency, suppose that

$$\sum_{i,j} c_{ij}(\alpha_i\beta_j) = 0, \tag{2.21}$$

where $c_{ij} \in K$. Then, we have that

$$\sum_{j=1}^{m}\left(\sum_{i=1}^{n} c_{ij}\alpha_i\right)\beta_j = 0. \tag{2.22}$$

Since $\{\beta_1, \ldots, \beta_m\}$ is a basis of T over L and $\sum_{i=1}^{n} c_{ij}\alpha_i$ belongs to L, we obtain that

$$\sum_{i=1}^{n} c_{ij}\alpha_i = 0. \tag{2.23}$$

Using the same argument for the basis $\{\alpha_1, \ldots, \alpha_n\}$ of L over K, we conclude that $c_{ij} = 0$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, m$. Thus, the claim follows. □

Corollary 2.2.3.1. *Let γ be an algebraic element of L over K and $m(X)$ be its minimal polynomial. If $L = K(\gamma)$, then $[L : K] = \deg m(X)$.*

Proof. By Thereom 2.2.2, the corollary is straight-forward. □

2.3 Free Abelian Groups

We define a basis B of an abelian group G as a subset of G such that every element of G can be uniquely expressed as a linear combination of elements of B with integer coefficients.

Definition 2.3.1. *A free abelian group G is an abelian group provided that it possess a basis.*

Note that every basis of a free abelian group is of the same cardinality, which we call the rank of the group.

Theorem 2.3.1 (Jarvis (2014))**.** *Any subgroup of a free abelian group of finite rank n is a free abelian group of rank $\leq n$.*

Proof. Assume that $H \subseteq G$ are groups satisfying the assumptions of theorem. We might suppose that H is non-trivial. If H were trivial, there would be nothing to prove. We use induction on the rank n. The initial case $n = 1$; clearly $G \simeq \mathbb{Z}$. We know that every subgroup of $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some $m \in \mathbb{Z}$. Hence, the assertion is satisfied.

Suppose that the assertion is true when the rank is $n - 1$. Now, assume that G has rank n. Then, G contains elements $g_1, \ldots, g_n$ such that

$$G = g_1\mathbb{Z} + \cdots + g_n\mathbb{Z}. \tag{2.24}$$

Let π denote the canonical projection mapping

$$\begin{aligned} \pi \ &: G \longrightarrow \mathbb{Z} \\ g \ &\mapsto \ a_1. \end{aligned}$$

Then, $\ker \pi = g_2\mathbb{Z} + \cdots + g_n\mathbb{Z}$ has rank $n - 1$. If $H \subseteq \ker \pi$, then the proof is done by the induction hypothesis. Otherwise, $\pi(H)$ is a non-trivial subgroup of $\mathbb{Z}$ and that's why $\pi(H)$ is of rank 1. Let $\pi(h)$ be the basis of $\pi(H)$. Then, we obtain that

$$H = h\mathbb{Z} + (H \cap \ker \pi). \tag{2.25}$$

so that $H \cap \ker \pi$ is a free abelian group of rank at most $n-1$ by the induction hypothesis. Therefore, we conclude that H is a free abelian group of rank at most n. □

2.4 Dirichlet Series and Abel's Summation Formula

The aim of the this section is to mention some significant properties of Dirichlet series and show Abel's summation formula. For the results mentioned below and more about Dirichlet series, we refer the reader to Apostol (1998).

Definition 2.4.1. *A function $f : \mathbb{Z}^+ \longrightarrow \mathbb{C}$ is called an arithmetic function.*

The following are some arithmetic functions of interest.

Example 1.

1. *The unit function $u(n) = 1$ for any $n \in \mathbb{Z}^+$.*
2. *The Möbius function* $\mu(n) = \begin{cases} (-1)^t, & \text{if} \quad \text{n is a product of } t \text{ distinct primes.} \\ 1, & \text{if} \quad n = 1. \\ 0, & otherwise. \end{cases}$
3. *The von Mangoldt function* $\Lambda(n) = \begin{cases} \log p, & \text{if} \quad \text{n is a power of a prime } p \\ 0, & otherwise. \end{cases}$
4. *The Euler ϕ-function* $\phi(n) = \big|\{k \leq n \mid \text{gcd}(k, n) = 1\}\big|$.

We may refer the reader to Apostol (1998) for more examples of arithmetic functions.

Definition 2.4.2. *Let $s \in \mathbb{C}$ and $f(n)$ denote an arithmetic function. Then, the series*

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} \tag{2.26}$$

is said to be a Dirichlet series of $f(n)$.

For instance, if we choose $f(n) = u(n)$ in Example 1, then the Dirichlet series yields the Riemann zeta function $\zeta(s)$, given by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{2.27}$$

for $\Re(s) > 1$.

Throughout the thesis, we will assume for historical reasons that $s = \sigma + it$, where $\sigma, t \in \mathbb{R}$. This is the Riemann's notation in his famous paper. Then, we have that

$$n^s = n^{\sigma+it} = n^\sigma n^{it} = n^\sigma e^{it\log n}. \tag{2.28}$$

Thus, $|n^s| = n^\sigma$, because $|e^{it\log n}| = 1$. This observation gives us that

$$\left|\sum_{n=1}^{\infty} \frac{f(n)}{n^s}\right| \leq \sum_{n=1}^{\infty} \left|\frac{f(n)}{n^s}\right| = \sum_{n=1}^{\infty} \frac{|f(n)|}{n^\sigma}. \tag{2.29}$$

If c is a complex number with $\Re(c) > \sigma$, then $n^{-\Re(c)} < n^{-\sigma}$ and hence

$$\sum_{n=1}^{\infty} \frac{|f(n)|}{n^{\Re(c)}} < \sum_{n=1}^{\infty} \frac{|f(n)|}{n^\sigma}. \tag{2.30}$$

By the comparison test, $\sum_{n=1}^{\infty} f(n)n^{-s}$ is converges absolutely for all c with $\Re(c) > \sigma$ provided that it is absolutely convergent for all $s = \sigma + it$.

Theorem 2.4.1 (Apostol (1998)). *Suppose that the series $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ is neither convergent nor divergent on the whole complex plane. Then, there is a real value $\sigma_a \in \mathbb{R}$ so that $\sum_{n=1}^{\infty} f(n)n^{-s}$ is absolutely convergent if $\sigma > \sigma_a$. It is not absolutely convergent whenever $\sigma < \sigma_a$. The number σ_a is said to be the "abscissa of absolute convergence".*

Proof. Assume that

$$D_f = \left\{ \sigma \in \mathbb{R} \,\middle|\, \sum_{n=1}^{\infty} \frac{f(n)}{n^s} \text{ diverges absolutely} \right\}. \tag{2.31}$$

As $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ diverges for some s, the set D_f is not empty. Also, there are complex values s for which the series $\sum_{n=1}^{\infty} |f(n)n^{-s}|$ is convergent. Hence, D_f is bounded above. Therefore, D_f has a supremum, call it σ_a. We can see that $\sigma \in D_f$ for all $\sigma < \sigma_a$, whereas $\sigma \notin D_f$ for all $\sigma > \sigma_a$. This proves the theorem. □

Definition 2.4.3. *An arithmetic function f is said to multiplicative provided that the* *equality*

$$f(mn) = f(m)f(n) \tag{2.32}$$

is satisfied for any relatively prime positive integers m and n. If the equality is satisfied for all postive integers m and n, then we say that f is completely multiplicative.

Theorem 2.4.2 (Apostol (1998))**.** *If f is multiplicative and the series $\sum f(n)$ converges absolutely, then we can express the series as an infinite product*

$$\sum_{n=1}^{\infty} f(n) = \prod_{p\in\mathbb{P}} \big(1 + f(p) + f(p^2) + \cdots\big), \tag{2.33}$$

where $\mathbb{P}$ is the set of primes. If f is also completely multiplicative, then we have

$$\sum_{n=1}^{\infty} f(n) = \prod_{p\in\mathbb{P}} \frac{1}{1 - f(p)}. \tag{2.34}$$

This theorem was proved by Euler in 1737, and so we call (2.34) the Euler product for f. In fact, it is the analytic version of the fundamental theorem of arithmetic.

Proof. Suppose that f is multiplicative and the series $\sum f(n)$ converges absolutely. Let us set $P(x)$ as follows:

$$P(X) = \prod_{p\leq x} \big(1 + f(p) + f(p^2) + \cdots\big). \tag{2.35}$$

As the series $\sum f(n)$ converges absolutely, we get that

$$\left|\sum_{n=1}^{\infty} f(n) - P(x)\right| \leq \sum_{n>x} |f(n)| \to 0, \tag{2.36}$$

as $x \to \infty$. The rest can be immediately shown by using the definition of completely multiplicative functions and the property of convergent geometric series. □

For instance, if we take $f(n) = u(n)$, then we get the Euler product of the Riemann zeta function $\zeta(s)$

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathbb{P}} \frac{1}{1 - p^{-s}} \quad \text{if} \quad \sigma > 1. \tag{2.37}$$

Definition 2.4.4. *Let $g(x)$ be a positive function for all $x \geq a$. We write*

$$f(x) = O(g(x)) \tag{2.38}$$

provided that there is a positive number $B > 0$ such that

$$|f(x)| \leq Bg(x) \tag{2.39}$$

for every $x \geq a$.

Definition 2.4.5. *Two functions $f(x)$ and $g(x)$ are called asymptotic, which we denote by $f(x) \sim g(x)$, if*

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 1. \tag{2.40}$$

In 1826, Niels Henrik Abel discovered the following dexterous theorem. We often apply Abel's summation formula in analytic number theory to compute series. By means of this formula, we are able to represent partial sums as integrals. For instance, using Abel's summation formula we can obtain integral representations of harmonic numbers, the Riemann zeta function and so on.

Theorem 2.4.3 (Abel's Summation Formula, Apostol (1998)**).** *Assume that $a(n)$ is an arithmetic function and $f(t)$ is a function which has a continuous derivative on the interval $[x, y]$. Then,*

$$\sum_{x < n \leq y} a(n)f(n) = A(y)f(y) - A(x)f(x) - \int_x^y A(t)f(t)dt, \tag{2.41}$$

where $A(x) = \sum_{n \leq x} a(n)$ and $A(x) = 0$ whenever $x < 1$.

Note that the reader can easily follow the proof of Abel's summation formula step by step in Apostol (1998).

CHAPTER THREE
ALGEBRAIC PART OF THE PRIME IDEAL THEOREM

Let us note that the reader might consult Jarvis (2014) for the results in the algebraic part of the prime ideal theorem. We tried to rewrite the proofs more clearly (adhering to Jarvis (2014)).

3.1 Number Fields and the Ring of Integers

Definition 3.1.1. *We say that $\alpha \in \mathbb{C}$ is an algebraic number provided that it is an algebraic element over rational numbers $\mathbb{Q}$. Otherwise, it is called transcendental.*

According to the definition, the monic polynomial $q(X)$ in $\mathbb{Q}[X]$ of the lowest degree such that $q(\alpha) = 0$ is the minimal polynomial of an algebraic number α. One may easily observe that it is an irreducible polynomial over rational numbers $\mathbb{Q}$. Furthermore, this polynomial divides every $f(X) \in \mathbb{Q}[X]$ having α as a root.

Lemma 3.1.1. *Every element of a finite degree extension of rational numbers $\mathbb{Q}$ is algebraic over $\mathbb{Q}$.*

Proof. Assume that $\mathbb{Q} \subseteq K$ denotes a finite degree extension with $[K : \mathbb{Q}] = n$. Then, the $n + 1$ elements which are $1, \alpha, \ldots, \alpha^n$ are linearly dependent. Hence, we may find rational numbers $q_0, q_1, \ldots, q_n$, not all zero, such that

$$q_n\alpha^n + \cdots + q_1\alpha + q_0 = 0. \tag{3.1}$$

This shows that there exists a polynomial with rational coefficients

$$p(X) = q_nX^n + \cdots + q_1X + q_0 \tag{3.2}$$

such that $p(\alpha) = 0$. Therefore, α is algebraic over $\mathbb{Q}$. □

Definition 3.1.2. *Any finite degree extension field K of $\mathbb{Q}$ in $\mathbb{C}$ is said to be a number field.*

For instance, the cyclotomic field $\mathbb{Q}(\eta_n)$ is a number field of degree $\phi(n)$, where η_n is a primitive n-th root of unity and the field $\mathbb{Q}(i)$ is a number field of degree 2.

Unless otherwise stated in the rest of the thesis, K will denote a number field and n will denote the degree of K over $\mathbb{Q}$.

Lemma 3.1.2. *Any irreducible polynomial $q(X) \in \mathbb{Q}[X]$ admits distinct roots in the field of complex numbers $\mathbb{C}$.*

Proof. Suppose to the contrary that β is a complex number which is a zero of $q(X)$ of order $m > 1$. That is, we have

$$q(X) = (X - \beta)^m f(X). \tag{3.3}$$

Then, $(X - \beta)^{m-1}$ is also a factor of the formal derivative $q'(X)$. As $q'(\beta) = 0$ and $q'(X) \in \mathbb{Q}[X]$, we have $q(X)|q'(X)$. But, $q'(X)$ is a non-zero polynomial and we have the inequality deg(q') $<$ deg(q). Therefore, $q(X)$ can not have a multiple root $\beta \in \mathbb{C}$. □

Theorem 3.1.3 (Fraleigh (2003))**.** *$K = \mathbb{Q}(\gamma)$ for some $\gamma \in K$.*

In abstract algebra, this is a well-known theorem which is called “primitive element theorem”.

Proof. We use induction on the degree n. First, we consider the initial case $n = 2$. Assume that α, β are bases elements of K over $\mathbb{Q}$. We denote the minimal polynomials of α and β by $f(X)$ and $g(X)$, respectively. Note that they are irreducible polynomials over $\mathbb{Q}$. Thus, by Lemma 3.1.2 $f(X)$ and $g(X)$ admit distinct roots in $\mathbb{C}$. Suppose that $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_s$ and $\beta_1 = \beta, \beta_2, \ldots, \beta_t$ denote the roots of $f(X)$ and $g(X)$ in $\mathbb{C}$, respectively. Choose an element $k \in K$ such that

$$k \neq \frac{\alpha_i - \alpha}{\beta - \beta_j} \tag{3.4}$$

for any i, j with $j \neq 1$. Let $\gamma = \alpha + k\beta$. We claim that $K = \mathbb{Q}[\gamma]$. Hence, it is enough to verify that $\alpha, \beta \in \mathbb{Q}[\gamma]$. We have that

$$\gamma \neq \alpha_i + k\beta_j, \tag{3.5}$$

because $\frac{\alpha_i - \alpha}{\beta - \beta_j}$ is a unique solution of the equation

$$\alpha_i + X\beta_j = \alpha + X\beta. \tag{3.6}$$

Now, consider the following two polynomials

$$g(X), f(\gamma - kX) \in (\mathbb{Q}(\gamma))[X]. \tag{3.7}$$

Observe that β satisfies both $g(X)$ and $f(\gamma - \delta X)$. Furthermore, they have no other common roots, since the remaining ones of $g(X)$ are $\beta_2, \dots, \beta_t$ and $\gamma - k\beta_j \neq \alpha_i$ unless $j = 1$. Therefore, $g(X)$ and $f(\gamma - \delta X)$ admits the only common factor $X - \beta$. Since they have coefficients in $\mathbb{Q}(\gamma)$, the common factor $X - \beta$ is a polynomial having coefficients in $\mathbb{Q}(\gamma)$. Thus, $\beta \in \mathbb{Q}[\gamma]$ which immediately implies $\alpha = \gamma - k\beta \in \mathbb{Q}[\gamma]$. Hence, we conclude that $K = \mathbb{Q}[\gamma]$ in the case $n = 2$. Now, suppose that the assertion is valid for the case $n = m - 1$. We will prove for $n = m$. Assume that $n = m$ and $\alpha_1, \dots, \alpha_m$ denotes the bases elements of K over $\mathbb{Q}$, that is,

$$K = \mathbb{Q}(\alpha_1, \dots, \alpha_m). \tag{3.8}$$

Since we can consider K as $\mathbb{Q}(\alpha_1, \dots, \alpha_{m-1})(\alpha_m)$, using the induction hypothesis, one may find an element $\gamma_1 \in K$ so that $K = \mathbb{Q}(\gamma_1, \alpha_m)$. But, we have shown that $K = \mathbb{Q}(\gamma)$ for the case $n = 2$. Therefore, the result easily follows. □

Our major purpose is to do number theory in finite degree extensions of the rational numbers. In other words, we would like to study prime numbers, divisibility, arithmetic (or number-theoretic) functions and some of the most significant theorems. Actually, number theory is a branch of mathematics devoted to the study of the properties of integers $\mathbb{Z}$ rather than rational numbers $\mathbb{Q}$. Thus, in order to do number theory in a number field K, we should discover the set of integers in K. Furthermore, these integers need to satisfy the same algebraic properties of integers $\mathbb{Z}$. For instance, we need to have a ring structure so that it is possible to add and multiply the integers in K. In order to be consistent, the integers in rational numbers $\mathbb{Q}$ should turn out to be integers $\mathbb{Z}$. Then, we are going to check whether there exists a unique factorization or not. Note that the proofs of the following lemmas and theorems can be found in Jarvis (2014). For details, we direct the reader to "Algebraic Number Theory" by Frazer Jarvis.

Definition 3.1.3. *An algebraic number α is said to be an algebraic integer provided that its minimal polynomial possesses coefficients from $\mathbb{Z}$.*

Lemma 3.1.4. *Suppose that α is an algebraic number which satisfies a monic polynomial with integer coefficients. Then, α is an algebraic integer.*

Proof. Assume that α is an algebraic number whose minimal polynomial is $m(X)$. Let $p(X)$ be a monic polynomial with integer coefficients such that $p(\alpha) = 0$. So, $m(X)|p(X)$ which means that

$$p(X) = m(X)f(X), \tag{3.9}$$

where $f(X) \in \mathbb{Q}[X]$. As $m(X)$ and $p(X)$ are both monic, $f(X)$ should be monic, too. Thus, we have

$$p(X) = m(X)f(X) \in \mathbb{Z}[X], \tag{3.10}$$

where $m(X), f(X)$ are monic in $\mathbb{Q}[X]$. By Gauss' Lemma (the reader might consult Fraleigh (2003)), in fact, the polynomials $m(X), f(X)$ have coefficients from $\mathbb{Z}$. It yields that α is an algebraic integer. □

Using above lemma, when we investigate whether an algebraic number is an algebraic integer or not, we don't have to look at the coefficients of the minimal polynomial anymore. From now on, it suffices to find a polynomial which admits integer coefficients and is monic, in order to show if an algebraic number is an algebraic integer.

Let's take two algebraic integers α and β. It is not clear that their sums and products are again algebraic integers. Consider that $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. Let us attempt to show that $\alpha + \beta$ is an algebraic integer. Assume that $X = \sqrt{2} + \sqrt{3}$. Taking the square we have that

$$X^2 - 5 = 2\sqrt{6}.$$

Taking the square one more time, we obtain that

$$X^4 - 10X^2 + 1 = 0.$$

This means that $\alpha + \beta$ is an algebraic integer. However, this proof may not work immediately for other algebraic integers. For this we need the following lemma.

Lemma 3.1.5. *For $\alpha \in K$, TFAE:*

1. *α is an algebraic integer.*
2. *$\mathbb{Z}[\alpha]$ is a finitely generated abelian group.*

Proof. Assume (1). Let $m(X)$ denote the minimal polynomial of α:

$$m(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0, \tag{3.11}$$

where $a_{n-1}, \ldots, a_0 \in \mathbb{Z}$. Then, we have that

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0. \tag{3.12}$$

That is, we can represent α^n as a $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. Thus, we deduce that

$$\begin{aligned}
\alpha^{n+1} &= \alpha \cdot \alpha^n && (3.13)\\
&= \alpha \cdot (-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0) && (3.14)\\
&= -a_{n-1}\alpha^n - a_{n-2}\alpha^{n-1} - \cdots - a_1\alpha^2 - a_0\alpha && (3.15)\\
&= -a_{n-1}(-a_{n-1}\alpha^{n-1} - \cdots - a_1\alpha - a_0) - a_{n-2}\alpha^{n-1} - \cdots - a_1\alpha^2 - a_0\alpha && (3.16)\\
&= (a_{n-1}^2 - a_{n-2})\alpha^{n-1} + \cdots + (a_{n-1}a_1 - a_0)\alpha + a_{n-1}a_0 && (3.17)
\end{aligned}$$

which shows that α^{n+1} is able to be also written as a $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. Continuing in this manner, we obtain that

$$\mathbb{Z}[\alpha] = \mathbb{Z}\alpha^{n-1} \oplus \cdots \oplus \mathbb{Z}\alpha \oplus \mathbb{Z}, \tag{3.18}$$

which means that $\{1, \alpha, \ldots, \alpha^{n-1}\}$ generates $\mathbb{Z}[\alpha]$ as an abelian group. Therefore, $\mathbb{Z}[\alpha]$ is a finitely generated abelian group.

Conversely, let $a_1, \ldots, a_n$ be generators of $\mathbb{Z}[\alpha]$, where $a_i = f_i(\alpha)$ for some $f_i(X) \in \mathbb{Z}[X]$. Choose an integer N so that $N >$ deg(f_i) for any $i = 1, \ldots, n$. Note that $\alpha^N \in \mathbb{Z}[\alpha]$ and hence

$$\alpha^N = c_n a_n + \cdots + c_1 a_1, \tag{3.19}$$

where $c_1, \ldots, c_n \in \mathbb{Z}$. Thus, we obtain that

$$\alpha^N - \big(c_n f_n(\alpha) + \cdots + c_1 f_1(\alpha)\big) = 0. \tag{3.20}$$

Now, we define

$$p(X) = X^n - \sum_{i=1}^{n} c_i f_i(X) \tag{3.21}$$

Since $N >$ deg(f_i) for any $i = 1, \ldots, n$, then $p(X)$ has integer coefficients and is monic such that $p(\alpha) = 0$. Therefore, α is an algebraic integer. □

Theorem 3.1.6. *The set of algebraic integers in K is a ring.*

Proof. Let us take two algebraic integers α and β from K. Then, $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated abelian groups and hence so too is $\mathbb{Z}[\alpha, \beta]$. By Theorem 2.3.1, $\mathbb{Z}[\alpha \pm \beta]$ and $\mathbb{Z}[\alpha\beta]$ are finitely generated abelian subgroups. Using Lemma 3.1.5, we see that $\alpha \pm \beta$ and $\alpha\beta$ are algebraic integers. This completes the proof. □

Definition 3.1.4. *Let K be a number field and $\mathcal{O}_K$ be the set of all algebraic integers in K. The set $\mathcal{O}_K$ is called the ring of integers of K.*

Let us illustrate this definition with two examples in which the former is trivial whereas the latter is non-trivial:

Proposition 1 (Jarvis (2014)). *1. $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.*

2. (a) $\mathcal{O}_{\mathbb{Q}(\sqrt{r})} = \mathbb{Z}[\sqrt{r}]$ if r is square-free integer with $r \equiv 2$ or 3 $(mod\ 4)$.

(b) $\mathcal{O}_{\mathbb{Q}(\sqrt{r})} = \mathbb{Z}[\frac{1+\sqrt{r}}{2}]$ if $r \equiv 1$ $(mod\ 4)$.

Lemma 3.1.7. $\mathbb{Q}\mathcal{O}_K = K$.

Proof. It is clear that $\mathbb{Q}\mathcal{O}_K \subseteq K$. Now, consider an algebraic number $\alpha \in K$. We need to find a non-zero integer $u \in \mathbb{Z}$ such that $u\alpha \in \mathcal{O}_K$. Let

$$m(X) = X^n + \cdots + a_1 X + a_0 \tag{3.22}$$

be the minimal polynomial of α, where $a_i = v_i/u_i$ with $u_i \neq 0$ for all $i = 0, 1, \ldots n-1$. Choose u to be ℓcm of the denominators u_i. After that we obtain a monic polynomial $f(X)$:

$$f(X) = u^n m\left(\frac{X}{u}\right) = X^n + \cdots + u^{n-1}\frac{v_1}{u_1}X + u^n\frac{v_0}{u_0}. \tag{3.23}$$

Since $u = \ell cm(u_0, \ldots u_{n-1})$, we deduce that $f(X)$ has integer coefficients such that $f(u\alpha) = 0$. Therefore, $u\alpha \in \mathcal{O}_K$ which implies that $\alpha \in \mathbb{Q}\mathcal{O}_K$ and we conclude that $\mathbb{Q}\mathcal{O}_K = K$. □

3.2 Algebraic Structure of the Ring of Integers

Throughout this section, we will prove that $\mathcal{O}_K$ is a free abelian group of rank $n = [K : \mathbb{Q}]$ and $\mathcal{O}_K$ is a Dedekind domain. We may refer the reader to Jarvis (2014) for more details about the algebraic structure of the ring of integers.

We have seen that an element α of K can be expressed as a $\mathbb{Q}$-linear combination

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n, \tag{3.24}$$

where $\alpha_1, \ldots, \alpha_n \in K$ are $\mathbb{Q}$-basis elements and $a_1, \ldots, a_n \in \mathbb{Q}$. It is natural to try to prove the same for $\mathcal{O}_K$. That is, are there algebraic integers $\alpha_1, \ldots, \alpha_n$ in $\mathcal{O}_K$ so that each element of $\mathcal{O}_K$ can be represented as a $\mathbb{Z}$-linear combination

$$a_1\alpha_1 + \cdots + a_n\alpha_n, \tag{3.25}$$

where $a_1, \ldots, a_n \in \mathbb{Z}$? Although this question is somewhat harder than for K, the answer is affirmative. In order to prove this fact, we need some materials. Now, we will introduce them.

Suppose that $K = \mathbb{Q}(\gamma)$ for some $\gamma \in K$. Note that using the primitive element theorem, we may to find such an element $\gamma \in K$. Suppose that $m(X)$ denote the minimal polynomial of γ. Then, deg$(m) = n$. We are able to factor $m(X)$ completely over $\mathbb{C}$

$$m(X) = \prod_{i=1}^{n}(X - \gamma_i), \tag{3.26}$$

where $\gamma_1 = \gamma, \gamma_2, \ldots, \gamma_n$ are the roots of $m(X)$. We say that the zeros $\gamma_1, \ldots, \gamma_n$ are the conjugates of γ. We can notice that $m(X)$ is the minimal polynomial of conjugate elements $\gamma_1, \ldots, \gamma_n$, as well. Remember that the roots of an irreducible polynomial are distinct. Thus, the conjugates of an algebraic number are distinct. For instance, the conjugates of $i \in \mathbb{Q}(i)$ are $\pm i$, since its minimal polynomial $X^2 + 1$ has two complex zeros $\pm i$.

An embedding of K into $\mathbb{C}$ is a non-zero field homomorphism from K to $\mathbb{C}$, which necessarily leaves the elements of $\mathbb{Q}$ unchanged.

Because $K = \mathbb{Q}(\gamma)$ for some $\gamma \in K$, every element of K can be considered as a polynomial of γ with rational coefficients. Then, we define embeddings of K into $\mathbb{C}$ as follows

$$\sigma_i : \ K = \mathbb{Q}(\gamma) \hookrightarrow \mathbb{Q}(\gamma_i) \ \subseteq \ \mathbb{C} \tag{3.27}$$

$$\sum_{j=0}^{n-1} a_j \gamma^j \mapsto \sum_{j=0}^{n-1} a_j \gamma_i^j. \tag{3.28}$$

Lemma 3.2.1. *A number field K of degree n has n distinct embeddings $\sigma_1, \ldots, \sigma_n$ into $\mathbb{C}$.*

Proof. It is immediately seen that the maps $\sigma_1, \ldots, \sigma_n$ are embeddings.

Conversely, consider an embedding $\sigma : K \hookrightarrow \mathbb{C}$. As $K = \mathbb{Q}(\gamma)$ for some $\gamma \in K$, the map σ is determined by its effect on γ, that is,

$$\sigma \left(\sum_{j=0}^{n-1} a_j \gamma^j \right) = \sum_{j=0}^{n-1} a_j \sigma(\gamma)^j. \tag{3.29}$$

Note that $m(X)$ is the minimal polynomial of γ and so $m(\gamma) = 0$. Applying σ to both sides of the equation, we obtain that

$$\sigma(m(\gamma)) = m(\sigma(\gamma)) = \sigma(0) = 0. \tag{3.30}$$

Since $\sigma(\gamma)$ is a root of $m(X)$, it must be γ_i for some i. This shows that $\sigma = \sigma_i$. □

Unless otherwise stated, $\sigma_1, \ldots, \sigma_n$ denote all the embeddings of the number field K of degree n.

Now, let's consider an element $\alpha \in K$ so that $m(X)$ is its minimal polynomial. Note that $\mathbb{Q}(\alpha)$ is a subfield of K and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d = \deg(m)$. If we consider the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$, then Theorem 2.2.3 gives that

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}]. \tag{3.31}$$

Therefore, we obtain that $d|n$ and let $r = n/d$.

Lemma 3.2.2. *Let $\sigma_1, \ldots, \sigma_n$ be all the embeddings of K into $\mathbb{C}$ and $\alpha \in K$ be as above. Then, each of the conjugates of α occurs precisely r times in the sequence $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$.*

Proof. By Lemma 3.2.1, we have exactly d distinct embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$. Let $\tau_1, \ldots, \tau_d$ denote the embeddings of $\mathbb{Q}(\alpha)$. We have seen that the embedding has the property $\tau_i(\alpha) = \alpha_i$. As $r = n/d = [K : \mathbb{Q}(\alpha)]$, the embedding $\tau_i : \mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ can be extended to an embedding of K into $\mathbb{C}$ in r ways. Hence, we get $dr = n$ embeddings of K into $\mathbb{C}$. In fact, these are all the embeddings $\sigma_1, \ldots, \sigma_n$ of K into $\mathbb{C}$. Therefore, each of the conjugates $\alpha_1, \ldots, \alpha_d$ of α occurs precisely r times in the sequence $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$. □

Using Lemma 3.2.2, we might observe that

$$m(X)^r = \prod_{i=1}^{n} (X - \sigma_i(\alpha)), \tag{3.32}$$

where $m(X)$ is the minimal polynomial of α.

For an element $\alpha \in K$, let

$$\mu_\alpha : K \longrightarrow K \tag{3.33}$$

$$x \mapsto \alpha x \tag{3.34}$$

be the multiplication map by α. As μ_α is $\mathbb{Q}$-linear map and the degree of K is n, this map can be represented by an $n \times n$ matrix.

Definition 3.2.1. *We define the norm $N(\alpha)$ and the trace $Tr(\alpha)$ of α to be the determinant and trace of μ_α, respectively.*

We can notice that the trace is additive while the norm is multiplicative, because

$$N(\alpha\beta) = \det(\mu_{\alpha\beta}) = \det(\mu_\alpha \mu_\beta) = \det(\mu_\alpha)\det(\mu_\beta) = N(\alpha)N(\beta), \tag{3.35}$$

$$Tr(\alpha + \beta) = Tr(\mu_{\alpha+\beta}) = Tr(\mu_\alpha + \mu_\beta) = Tr(\mu_\alpha) + Tr(\mu_\beta) = Tr(\alpha) + Tr(\beta). \tag{3.36}$$

It is easy to see that $N(\alpha)$ and $Tr(\alpha)$ are both in $\mathbb{Q}$, as they are the determinant and trace of a matrix with rational entries.

Proposition 2 (Jarvis (2014)). *For any $\alpha \in K$, we have that*

$$N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha). \tag{3.37}$$

Corollary 3.2.2.1. *If $\alpha \in \mathcal{O}_K$, then the norm $N(\alpha)$ and trace $Tr(\alpha)$ belong to $\mathbb{Z}$.*

Proof. Suppose that $m(X)$ is the minimal polynomial of α. Then, $m(X)$ is the monic polynomial with integer coefficients. We have observed that

$$m(X)^r = \prod_{i=1}^{n} (X - \sigma_i(\alpha)), \tag{3.38}$$

where $r = [K : \mathbb{Q}(\alpha)]$. It gives that

$$\prod_{i=1}^{n} (X - \sigma_i(\alpha)) \in \mathbb{Z}[X]. \tag{3.39}$$

Note that the constant coefficient of this polynomial is $(-1)^n \prod_{i=1}^{n} \sigma_i(\alpha)$ and the coefficent of X^{n-1} is $-\sum_{i=1}^{n} \sigma_i(\alpha)$. By Proposition 2, we deduce that $N(\alpha)$ and $Tr(\alpha)$ belong to $\mathbb{Z}$. □

Given arbitrary elements $\omega_1, \dots, \omega_n$ in K, consider the matrix:

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \dots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \dots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \dots & \sigma_n(\omega_n) \end{pmatrix}, \tag{3.40}$$

where $\sigma_1, \dots, \sigma_n$ are all the embeddings of K into $\mathbb{C}$.

Definition 3.2.2. *The discriminant of* $\{\omega_1, \dots, \omega_n\}$*, denoted by* $\Delta\{\omega_1, \dots, \omega_n\}$*, is defined as follows:*

$$\Delta\{\omega_1, \dots, \omega_n\} = (\det M)^2. \tag{3.41}$$

Lemma 3.2.3. *Let* $\omega_1, \dots, \omega_n$ *be arbitrary elements in* K*. If* T *is a matrix with* $T_{ij} = Tr(\omega_i \omega_j)$*, then* $\Delta\{\omega_1, \dots, \omega_n\} = \det T$*.*

Proof. We have that

$$\Delta\{\omega_1, \dots, \omega_n\} = (\det M)^2 = \det(M^t M), \tag{3.42}$$

where M^t is the transpose of M. We claim that $T = M^t M$. Then,

$$(M^t M)_{ij} = \sum_{\ell=1}^{n} M^t_{i\ell} M_{\ell j} = \sum_{\ell=1}^{n} M_{\ell i} M_{\ell j} = \sum_{\ell=1}^{n} \sigma_\ell(\omega_i)\sigma_\ell(\omega_j) = \sum_{\ell=1}^{n} \sigma_\ell(\omega_i \omega_j) = Tr(\omega_i \omega_j). \tag{3.43}$$

Thereby, we conclude that $T = M^t M$ and hence $\Delta\{\omega_1, \dots, \omega_n\} = \det T$. □

In particular, choose $\omega_1, \dots, \omega_n$ from the ring of integers $\mathcal{O}_K$. Then, $\omega_i \omega_j \in \mathcal{O}_K$. We showed $Tr(\alpha) \in \mathbb{Z}$ for all $\alpha \in \mathcal{O}_K$. Thus, we obtain that $Tr(\omega_i \omega_j) \in \mathbb{Z}$ and hence $\Delta\{\omega_1, \dots, \omega_n\} \in \mathbb{Z}$.

Lemma 3.2.4 (Jarvis (2014))**.** *Let* K *be a number field of degree* n*. The set* $\{\omega_1, \dots, \omega_n\}$ *is a basis for* K *over* $\mathbb{Q}$ *if and only if* $\Delta\{\omega_1, \dots, \omega_n\} \neq 0$*.*

Proof. ($\Rightarrow$) We know that all number fields are simple extensions, that is, $K = \mathbb{Q}(\gamma)$ for some $\gamma \in K$. Then, $1, \gamma, \dots, \gamma^{n-1}$ constitude a basis of K over $\mathbb{Q}$. Suppose that

$\gamma_1, \ldots, \gamma_n$ denote the conjugates of γ. Thus, we obtain that

$$\Delta\{1, \gamma, \ldots, \gamma^{n-1}\} = \begin{vmatrix} 1 & \gamma_1 & \ldots & \gamma_1^{n-1} \\ 1 & \gamma_2 & \ldots & \gamma_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \gamma_n & \ldots & \gamma_n^{n-1} \end{vmatrix}^2 . \tag{3.44}$$

Notice that it is the determinant of a Vandermonde matrix. Hence, we see that

$$\Delta\{1, \gamma, \ldots, \gamma^{n-1}\} = \prod_{i<j} (\gamma_i - \gamma_j)^2. \tag{3.45}$$

As the conjugates $\gamma_1, \ldots, \gamma_n$ are all distinct, we deduce that $\Delta\{1, \gamma, \ldots, \gamma^{n-1}\} \neq 0$. Now, let us write $\omega_1, \ldots, \omega_n$ as a $\mathbb{Q}$-linear combination of $1, \gamma, \ldots, \gamma^{n-1}$:

$$\omega_1 = a_{11}1 + a_{21}\gamma + \cdots + a_{n1}\gamma^{n-1}, \tag{3.46}$$

$$\omega_2 = a_{12}1 + a_{22}\gamma + \cdots + a_{n2}\gamma^{n-1}, \tag{3.47}$$

$$\vdots \quad \vdots \quad \vdots \quad \vdots \quad \vdots \tag{3.48}$$

$$\omega_n = a_{1n}1 + a_{2n}\gamma + \cdots + a_{nn}\gamma^{n-1}, \tag{3.49}$$

where $a_{ij} \in \mathbb{Q}$. We claim that if $A = (a_{ij})$ denotes the change of basis matrix, we have

$$\Delta\{\omega_1, \ldots, \omega_n\} = (\det A)^2 \Delta\{1, \gamma, \ldots, \gamma^{n-1}\}. \tag{3.50}$$

Let M denote the matrix in (3.40)

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \ldots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \ldots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \ldots & \sigma_n(\omega_n) \end{pmatrix}, \tag{3.51}$$

where $\sigma_1, \ldots, \sigma_n$ are all the embeddings of K into $\mathbb{C}$. We have that

$$\Delta\{\omega_1, \ldots, \omega_n\} = (\det M)^2. \tag{3.52}$$

Note that

$$\sigma_k(\omega_i) = a_{1i}1 + a_{2i}\gamma_k + \cdots + a_{ni}\gamma_k^{n-1}. \tag{3.53}$$

Thus, we obtain that $\Delta\{\omega_1, \ldots, \omega_n\} = (\det A)^2\Delta\{1, \gamma, \ldots, \gamma^{n-1}\}$. However, A is an invertible matrix and hence $\det A \neq 0$. We saw above that $\Delta\{1, \gamma, \ldots, \gamma^{n-1}\} \neq 0$. Therefore, we conclude that $\Delta\{\omega_1, \ldots, \omega_n\} \neq 0$.

($\Leftarrow$) Conversely, assume that $\Delta\{\omega_1, \ldots, \omega_n\} \neq 0$. If $\{\omega_1, \ldots, \omega_n\}$ is not a basis, then $\omega_1, \ldots, \omega_n$ are linearly dependent. Hence, we have that

$$a_1\omega_1 + \cdots + a_n\omega_n = 0 \tag{3.54}$$

for some $a_1, \ldots, a_n \in \mathbb{Q}$, not all zero. Applying the embedding σ_k to both sides of the equation, we obtain that

$$a_1\sigma_k(\omega_1) + \cdots + a_n\sigma_k(\omega_n) = 0. \tag{3.55}$$

This implies the dependency of the columns of M. Thus, $\det M = 0$ which implies that $\Delta\{\omega_1, \ldots, \omega_n\} = 0$, a contradiction. Thereby, $\{\omega_1, \ldots, \omega_n\}$ constitute a basis. □

Theorem 3.2.5. *$\mathcal{O}_K$ is a free abelian group of rank n.*

Proof. By Lemma 3.1.7 for a given basis of K we can replace each basis element with a non-zero multiple such that it belongs to $\mathcal{O}_K$. Now, suppose that $\omega_1, \ldots, \omega_n$ are basis elements of K in $\mathcal{O}_K$. In particular, we choose $\{\omega_1, \ldots, \omega_n\}$ such that $|\Delta\{\omega_1, \ldots, \omega_n\}|$ is the smallest among the discriminants of the other basis elements in $\mathcal{O}_K$. We claim that they generate $\mathcal{O}_K$ as an abelian group. Suppose to the contrary that there exists an element $\omega \in \mathcal{O}_K$ so that

$$\omega = a_1\omega_1 + \cdots + a_n\omega_n. \tag{3.56}$$

for some coefficient $a_i \in \mathbb{Q} \setminus \mathbb{Z}$. We may suppose without loss of generality that $a_1 \in \mathbb{Q} \setminus \mathbb{Z}$. Then, we can find an integer b_1 such that $|a_1 - b_1| \leq 1/2$. Now, we will construct new basis elements whose discriminant is strictly less than that of $\omega_1, \ldots, \omega_n$. This will contradict the minimality of $|\Delta\{\omega_1, \ldots, \omega_n\}|$.

Let $\omega_1' = \omega - b_1\omega_1$ and $\omega_i' = \omega_i$ for all $i = 2, \dots, n$. Note that

$$\omega_1' = (a_1 - b_1)\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n. \tag{3.57}$$

Observe that

$$\omega_1 = \frac{1}{a_1 - b_1}\omega_1' - \frac{a_2}{a_1 - b_1}\omega_2' - \cdots - \frac{a_n}{a_1 - b_1}\omega_n' \tag{3.58}$$

and recall that $\omega_i = \omega_i'$ for all $i = 2, \dots, n$ and $a_1 - b_1 \neq 0$. We see that the basis elements $\omega_1, \dots, \omega_n$ might be seen as a $\mathbb{Q}$-linear combination of $\omega_1', \dots, \omega_n'$. Therefore, they are also basis elements of K in $\mathcal{O}_K$. Then, we obtain that

$$\Delta\{\omega_1', \dots, \omega_n'\} = (\det A)^2 \Delta\{\omega_1, \dots, \omega_n\}, \tag{3.59}$$

where A denotes the change of basis matrix from $\{\omega_1, \dots, \omega_n\}$ to $\{\omega_1', \dots, \omega_n'\}$, i.e.

$$A = \begin{pmatrix} a_1 - b_1 & a_2 & a_3 & \dots & a_n \\ 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}. \tag{3.60}$$

Thus, we have that

$$\Delta\{\omega_1', \dots, \omega_n'\} = (a_1 - b_1)^2 \Delta\{\omega_1, \dots, \omega_n\}. \tag{3.61}$$

As $|a_1 - b_1| \leq 1/2$, we obtain that

$$|\Delta\{\omega_1', \dots, \omega_n'\}| < |\Delta\{\omega_1, \dots, \omega_n\}| \tag{3.62}$$

which is a contradiction, as desired. Therefore, we conclude that $\omega_1, \dots, \omega_n$ generate $\mathcal{O}_K$ as an abelian group. □

Definition 3.2.3. *A ring R is said to be a Noetherian ring if all ideals in R are finitely generated.*

For instance, principal ideal rings are Noetherian. We claim that $\mathcal{O}_K$ is a Noetherian ring for any number fields K.

Theorem 3.2.6 (Jarvis (2014))**.** *$\mathcal{O}_K$ is Noetherian.*

Proof. We have already proved that $\mathcal{O}_K$ is a free abelian group of rank n. As all ideals $\mathfrak{a}$ of $\mathcal{O}_K$ are its subgroups out of the gate, they are free abelian groups of finite rank. Then, we have

$$\mathfrak{a} = \alpha_1\mathbb{Z} + \cdots + \alpha_r\mathbb{Z}. \tag{3.63}$$

for some $\alpha_1, \ldots, \alpha_r \in \mathfrak{a}$. Additionally, we claim that they are finitely generated as an ideal. Note that $r \leq n$ and it is clear that $\alpha_i\mathbb{Z} \subseteq \alpha_i\mathcal{O}_K$ for all $i = 1, \ldots, r$. Thus, we obtain that

$$\mathfrak{a} = \alpha_1\mathbb{Z} + \cdots + \alpha_r\mathbb{Z} \subseteq \alpha_1\mathcal{O}_K + \cdots + \alpha_r\mathcal{O}_K \subseteq \mathfrak{a}. \tag{3.64}$$

This implies that

$$\mathfrak{a} = \alpha_1\mathcal{O}_K + \cdots + \alpha_r\mathcal{O}_K. \tag{3.65}$$

Therefore, $\mathfrak{a}$ is a finitely generated ideal which means that $\mathcal{O}_K$ is Noetherian. □

Theorem 3.2.7. *If an element α in K is a root of a monic polynomial with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$.*

Proof. Let $\alpha \in K$ and $p(X)$ be monic polynomial whose coefficients are in $\mathcal{O}_K$ with $p(\alpha) = 0$. Assume that

$$p(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_0, \tag{3.66}$$

where $a_i \in \mathcal{O}_K$ for all $i = 0, \ldots, m-1$. Since $\mathcal{O}_K$ is a free abelian group of rank n and

$$\alpha^m = -a_{m-1}\alpha^{m-1} - \cdots - a_0, \tag{3.67}$$

$\mathcal{O}_K[\alpha]$ is finitely generated as an abelian group. As $\mathbb{Z}[\alpha] \subset \mathcal{O}_K[\alpha]$, we deduce that $\mathbb{Z}[\alpha]$ is a finitely generated abelian group as well, which gives $\alpha \in \mathcal{O}_K$. □

In fact, we proved in the previous theorem that $\mathcal{O}_K$ is integrally closed.

Finally, in order to prove that $\mathcal{O}_K$ is a Dedekind domain, we will prove that prime ideals of $\mathcal{O}_K$ are maximal.

Lemma 3.2.8. *If $\mathfrak{p}$ is a non-zero prime ideal of $\mathcal{O}_K$, then $|\mathcal{O}_K/\mathfrak{p}|$ is finite.*

Proof. Consider a non-zero prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ and take a non-zero element $\alpha \in \mathfrak{p}$. Let $\alpha_1, \dots, \alpha_r$ denote all the conjugates of α and $\alpha_1 = \alpha$. As we showed in Corollary 3.2.2.1, the norm $N(\alpha) \in \mathbb{Z}$, since $\alpha \in \mathcal{O}_K$. Note that the product $\alpha_1 \dots \alpha_r \in \mathfrak{p}$. As we know that

$$N(\alpha) = \prod_{i=1}^{r} \alpha_i, \tag{3.68}$$

the norm $N(\alpha)$ belongs to $\mathfrak{p}$. As $\mathcal{O}_K$ is a free abelian group of rank n, we can express $\mathcal{O}_K$ as follows

$$\mathcal{O}_K = \omega_1\mathbb{Z} + \cdots + \omega_n\mathbb{Z}, \tag{3.69}$$

where $\omega_1, \dots, \omega_n \in \mathcal{O}_K$. Since $\mathfrak{p}$ is an ideal, we have that $N(\alpha)\omega_i \in \mathfrak{p}$ for every $i = 1, \dots, n$. Hence, we deduce that

$$a_1\omega_1 + \cdots + a_n\omega_n \equiv b_1\omega_1 + \cdots + b_n\omega_n \; (mod\, \mathfrak{p}) \tag{3.70}$$

such that $0 \leq b_i < N(\alpha)$. Now, one can easily observe that there are finitely many such elements. Therefore, $\mathcal{O}_K/\mathfrak{p}$ is finite. □

Theorem 3.2.9 (Jarvis (2014))**.** *All non-zero prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ are maximal.*

Proof. We have seen that $\mathcal{O}_K/\mathfrak{p}$ is finite. We know the fact from abstract algebra that every finite integral domain is a field. Since $\mathcal{O}_K/\mathfrak{p}$ is an integral domain and finite, it is a field. Therefore, $\mathfrak{p}$ is maximal. □

Now, we are ready to state our main theorem of this section.

Theorem 3.2.10 (Jarvis (2014))**.** *$\mathcal{O}_K$ is a Dedekind domain.*

Proof. By Theorems 3.2.7, 3.2.6 and 3.2.9, we can immediately obtain that $\mathcal{O}_K$ is a Dedekind domain. □

3.3 Norms of Ideals

First, we will introduce the norm of a non-zero ideal of $\mathcal{O}_K$ and show that it is always finite and a completely multiplicative function. For the following results and more details one may consult Jarvis (2014).

Definition 3.3.1. *The norm $N(\mathfrak{a})$ of a non-zero ideal $\mathfrak{a}$ of $\mathcal{O}_K$ is the index of $\mathfrak{a}$ in $\mathcal{O}_K$, i.e. $N(\mathfrak{a}) = |\mathcal{O}_K/\mathfrak{a}|$.*

Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_K$ are relatively prime provided that $\mathfrak{a} + \mathfrak{b} = \mathcal{O}_K$. Alternatively, $\mathfrak{a}$ and $\mathfrak{b}$ are relatively prime when there is no common prime ideal in their factorizations.

Recall that the "Chinese remainder theorem" states that if $a_1, \ldots, a_n$ are pairwise relatively prime positive integers, then the map

$$\phi : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_n\mathbb{Z} \tag{3.71}$$

$$\bar{x} \quad \mapsto \quad (\bar{x}, \ldots, \bar{x}) \tag{3.72}$$

defines a ring isomorphism. Given any K, this theorem might be generalized to $\mathcal{O}_K$ with a formulation involving ideals, see Jarvis (2014).

Theorem 3.3.1 (Chinese Remainder Theorem, Jarvis (2014)**).** *Suppose that $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ are mutually relatively prime ideals in $\mathcal{O}_K$. Then, we have that*

$$\mathcal{O}_K/(\mathfrak{a}_1 \ldots \mathfrak{a}_n) \simeq \mathcal{O}_K/\mathfrak{a}_1 \times \cdots \times \mathcal{O}_K/\mathfrak{a}_n. \tag{3.73}$$

Lemma 3.3.2. *Let $\mathfrak{a}$ be a non-zero ideal in $\mathcal{O}_K$ and $\mathfrak{p}$ be a non-zero prime ideal in $\mathcal{O}_K$. Then, $\mathcal{O}_K/\mathfrak{p}$ and $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ are isomorphic $\mathcal{O}_K$-modules.*

Proof. We guarantee that we may take a non-zero element $\beta \in \mathfrak{a} - \mathfrak{a}\mathfrak{p}$. Assume that $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, where $\mathfrak{p}_i$ is a prime ideal for each $i = 1, \ldots, r$. If we had $\mathfrak{a}\mathfrak{p} = \mathfrak{p}$, then we would have that

$$\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p} = \mathfrak{p} \quad \Rightarrow \quad \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{p}\mathfrak{p}^{-1} = R, \tag{3.74}$$

a contradiction. We define the following map

$$\phi : \mathcal{O}_K \longrightarrow \mathfrak{a}/\mathfrak{a}\mathfrak{p} \tag{3.75}$$

$$\alpha \;\mapsto\; \overline{\alpha\beta}. \tag{3.76}$$

We see that if $\mathfrak{a}\mathfrak{p} \subseteq \mathfrak{b} \subseteq \mathfrak{a}$, then multiplying through by $\mathfrak{a}^{-1}$ we obtain that

$$\mathfrak{p} \subseteq \mathfrak{a}^{-1}\mathfrak{b} \subseteq \mathcal{O}_K. \tag{3.77}$$

Since prime ideals in $\mathcal{O}_K$ are maximal, we have that either $\mathfrak{a}^{-1}\mathfrak{b} = \mathfrak{p}$ or $\mathfrak{a}^{-1}\mathfrak{b} = \mathcal{O}_K$. This gives $\mathfrak{b} = \mathfrak{a}$ or $\mathfrak{b} = \mathfrak{a}\mathfrak{p}$. Hence, one can easily deduce that ϕ is onto. Furthermore, we have that

$$\ker(\phi) = \{\alpha \in \mathcal{O}_K \mid \alpha\beta \in \mathfrak{a}\mathfrak{p}\}. \tag{3.78}$$

Remember that we have choosen β to be in $\mathfrak{a}$ but not in $\mathfrak{a}\mathfrak{p}$. Thus, $\alpha\beta \in \mathfrak{a}\mathfrak{p}$ means that $\alpha \in \mathfrak{p}$. This shows that $\ker(\phi) = \mathfrak{p}$. By using the first isomorphism theorem, we conclude that $\mathcal{O}_K/\mathfrak{p} \simeq \mathfrak{a}\mathfrak{p}$. □

Corollary 3.3.2.1. *Suppose that $\mathfrak{p}$ is a non-zero prime ideal in $\mathcal{O}_K$ and $n \geq 1$. Then, there is an $\mathcal{O}_K$-module isomorphism between $\mathcal{O}_K/\mathfrak{p}$ and $\mathfrak{p}^{n-1}/\mathfrak{p}^n$.*

Proof. If we take $\mathfrak{a} = \mathfrak{p}^{n-1}$ in the previous lemma, then the proof is done. □

Lemma 3.3.3. *Assume that $\mathfrak{p}$ is a prime ideal in $\mathcal{O}_K$. Then, $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$ for any positive integer n.*

Proof. By the third isomorphism theorem, we know that

$$\mathcal{O}_K/\mathfrak{p}^{n-1} \simeq \frac{\mathcal{O}_K/\mathfrak{p}^n}{\mathfrak{p}^{n-1}/\mathfrak{p}^n}. \tag{3.79}$$

Using Corollary 3.3.2.1, we obtain that

$$N(\mathfrak{p}^{n-1}) = |\mathcal{O}_K/\mathfrak{p}^{n-1}| = \left|\frac{\mathcal{O}_K/\mathfrak{p}^n}{\mathfrak{p}^{n-1}/\mathfrak{p}^n}\right| = \frac{|\mathcal{O}_K/\mathfrak{p}^n|}{|\mathfrak{p}^{n-1}/\mathfrak{p}^n|} = \frac{|\mathcal{O}_K/\mathfrak{p}^n|}{|\mathcal{O}_K/\mathfrak{p}|} = \frac{N(\mathfrak{p}^n)}{N(\mathfrak{p})} \tag{3.80}$$

which implies that $N(\mathfrak{p}^n) = N(\mathfrak{p}^{n-1})N(\mathfrak{p})$. Continuing in this way, we obtain the result $N(\mathfrak{p}^n) = N(\mathfrak{p})^n$ for any $n \in \mathbb{Z}^+$. □

Theorem 3.3.4. *For any non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$, its norm $N(\mathfrak{a})$ is always finite.*

Proof. Let's take a non-zero ideal $\mathfrak{a}$ in $\mathcal{O}_K$. We proved in Theorem 3.2.10 that $\mathcal{O}_K$ is a Dedekind domain. Thus, we can express $\mathfrak{a}$ uniquely as follows:

$$\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k}, \tag{3.81}$$

where $\mathfrak{p}_i$ is a prime ideal in $\mathcal{O}_K$ and m_i is a positive integer for all $i = 1, \dots, k$. The ideals $\mathfrak{p}_i^{m_i}$ and $\mathfrak{p}_j^{m_j}$ are relatively prime for all $i \neq j$. Thus, by the Chinese remainder theorem we have that

$$\mathcal{O}_K/\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k} \simeq \mathcal{O}_K/\mathfrak{p}_1^{m_1} \times \cdots \times \mathcal{O}_K/\mathfrak{p}_k^{m_k}. \tag{3.82}$$

Thus, by Lemma 3.3.3, we obtain that

$$N(\mathfrak{a}) = N(\mathfrak{p}_1)^{m_1} \dots N(\mathfrak{p}_k)^{m_k}. \tag{3.83}$$

Moreover, we showed that $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}|$ is finite for every prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. It follows that $N(\mathfrak{a})$ is finite, as well. □

Theorem 3.3.5. *For two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in $\mathcal{O}_K$, we have that*

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}). \tag{3.84}$$

Proof. It suffices to show the case $\mathfrak{b} = \mathfrak{p}$, i.e.

$$N(\mathfrak{a}\mathfrak{p}) = N(\mathfrak{a})N(\mathfrak{p}). \tag{3.85}$$

Since we have a unique factorisation $\mathfrak{b} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k}$, we see that

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a}\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k-1}\mathfrak{p}_k) = N(\mathfrak{a}\mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k-1})N(\mathfrak{p}_k). \tag{3.86}$$

Continuing in this way, we can obtain the result.

Now, suppose that $\mathfrak{b} = \mathfrak{p}$. It has been shown that $\mathcal{O}_K/\mathfrak{p}$ and $\mathfrak{a}/\mathfrak{a}\mathfrak{p}$ are isomorphic $\mathcal{O}_K$-modules. Thus, we deduce that

$$|\mathcal{O}_K/\mathfrak{a}| = \left|\frac{\mathcal{O}_K/\mathfrak{a}\mathfrak{p}}{\mathfrak{a}/\mathfrak{a}\mathfrak{p}}\right| = \frac{|\mathcal{O}_K/\mathfrak{a}\mathfrak{p}|}{|\mathcal{O}_K/\mathfrak{p}|}, \tag{3.87}$$

that is, $|\mathcal{O}_K/\mathfrak{a}\mathfrak{p}| = |\mathcal{O}_K/\mathfrak{a}||\mathcal{O}_K/\mathfrak{p}|$. By the definition of the ideal norm, we conclude that $N(\mathfrak{a}\mathfrak{p}) = N(\mathfrak{a})N(\mathfrak{p})$, as desired. □

Let's take a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$. It has been shown that the quotient $\mathcal{O}_K/\mathfrak{p}$ is a finite field. Hence, we can deduce that $\mathfrak{p}$ is associated with a prime number $p \in \mathbb{Z}$. We sometimes use the terminology that $\mathfrak{p}$ lies above p.

Lemma 3.3.6. $N(\mathfrak{a}) = N(\alpha)$ *for any ideal* $\mathfrak{a} = (\alpha) \subseteq \mathcal{O}_K$*, where* $\alpha \in \mathcal{O}_K$.

Proof. Let $\mathcal{O}_K = \omega_1\mathbb{Z} + \cdots + \omega_n\mathbb{Z}$. Then, we have that

$$\mathfrak{a} = \mathbb{Z}\alpha\omega_1 + \cdots + \mathbb{Z}\alpha\omega_n. \tag{3.88}$$

Assume that

$$\alpha\omega_i = \sum_{j=1}^{n} a_{ij}\omega_j, \tag{3.89}$$

where $a_{ij} \in \mathbb{Z}$ for every $i = 1, \ldots, n$. Then, $|\mathcal{O}_K/\mathfrak{a}| = |\det(a_{ij})|$. Thus, we obtain that $N(\mathfrak{a}) = |\det(a_{ij})|$. On the other hand, $N(\alpha) = \det(a_{ij})$ by the definition. Therefore, we conclude that $N(\mathfrak{a}) = N(\alpha)$. □

Theorem 3.3.7. *A prime number p admits at most n prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ that lie above it and $N(\mathfrak{p}) \geq p$.*

Proof. Let p be a prime number and $\mathfrak{a} \subseteq \mathcal{O}_K$ be a principal ideal generated by p. Since O_K is a Dedekind domain, we can express that

$$\mathfrak{a} = \mathfrak{p}_1^{m_1} \cdots \mathfrak{p}_k^{m_k}, \tag{3.90}$$

where $\mathfrak{p}_i$ is a prime ideal in $\mathcal{O}_K$ and m_i is a positive integer for all $i = 1, \ldots, k$. If we take the norm of (3.90), then

$$p^n = N(\mathfrak{p}_1)^{m_1} \ldots N(\mathfrak{p}_k)^{m_k}. \tag{3.91}$$

Using this equality, we can immediately complete the proof. □

CHAPTER FOUR
ANALYTIC PART OF THE PRIME IDEAL THEOREM

The function $\pi(x) = \#\{p \in \mathbb{P} \mid p < x\}$ is called the prime counting function in number theory. In c. 300 BC, Euclid offered a proof of the infinitude of primes in his work “Elements”. Euclid’s proof is the first known proof in mathematics. This result directly implies that

$$\lim_{x\to\infty} \pi(x) = \infty. \tag{4.1}$$

However, there were no any considerable information about the growth of $\pi(x)$. Legendre and Gauss conjectured independently that the following ratio

$$\frac{\pi(x)}{x/\log x}$$

approaches 1 as $x \to \infty$. This assertion has attracted the attention of many famous mathematicians over the years. In 1891, Chebyshev made a remarkable attack in order to prove this claim. He discovered that assuming the existence of the limit of the ratio proves the conjecture. In 1859, Riemann also attacked this conjecture using analytic methods, starting with the function which is discovered by Euler in 1737

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \tag{4.2}$$

for real $s > 1$. He regarded this function for complex values of s with $\sigma > 1$. He chalked out a magnificent method which connect the distribution of primes to properties of the function $\zeta(s)$. However, the techniques to prove his ideas were not fully developed in mathematics. Within 40 years new developments were made in complex analysis. In 1896, C.J. de la Vallée Poussin and J. Hadamard proved independently but almost at the same time that

$$\pi(x) \sim \frac{x}{\log x} \quad \text{as} \quad x \to \infty. \tag{4.3}$$

That is to say,

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1. \tag{4.4}$$

This is a very famous result called the “prime number theorem”.

In theory of algebraic numbers, we study the generalizations of the usual arithmetic of natural numbers in a more general setting. For instance, we define the function $\pi_K(x) = \#\{\mathfrak{p} \subset \mathcal{O}_K \mid N(\mathfrak{p}) \leq x\}$. We can easily see that $\pi_K(x) = \pi(x)$ whenever $K = \mathbb{Q}$. As $\mathcal{O}_\mathbb{Q} = \mathbb{Z}$ and all prime ideal $\mathfrak{p}$ in $\mathbb{Z}$ are of the form $p\mathbb{Z}$ for a prime p, then $N(\mathfrak{p}) = |\mathbb{Z}/p\mathbb{Z}| = p$. Hence, $\pi_K(x) = \pi(x)$.

In 1903, Edmund Landau proved for an arbitrary number field K that there exists an asymptotic formula for the function $\pi_K(x)$:

$$\pi_K(x) \sim \frac{x}{\log x} \quad \text{as} \quad x \to \infty. \tag{4.5}$$

In fact, he showed that

$$\pi_K(x) = \int_2^x \frac{dt}{\log t} + O_K\big(x \exp\big(-b\sqrt{\log x}\big)\big), \tag{4.6}$$

where $b = b(K)$ is a constant. One can immediately see that this is the same asymptotic formula in this prime number theorem. This remakable result is a number field generalization of the prime number theorem and known as the Landau’s prime ideal theorem.

In this thesis, our aim is to obtain the prime ideal theorem without an error term. But, the reader may check Landau (1903) for his original proof. First, we will obtain the equivalent statement of the prime ideal theorem

$$\psi_K(x) \sim x \quad \text{as} \quad x \to \infty, \tag{4.7}$$

where $\psi_K(x)$ is Chebyshev's function given by the formula

$$\psi_K(x) = \sum_{N(\mathfrak{a}) \leq x} \Lambda_K(\mathfrak{a}), \tag{4.8}$$

where the sum ranges over all ideals $\mathfrak{a}$ of $\mathcal{O}_K$ with $N(\mathfrak{a}) \leq x$ and $\Lambda_K(\mathfrak{a}) = \log N(\mathfrak{p})$ if $\mathfrak{a} = \mathfrak{p}^m$, otherwise it is zero.

Second, we will introduce the Dedekind zeta function $\zeta_K(s)$ given by the formula for $\sigma > 1$

$$\zeta_K(s) = \sum_{0 \neq \mathfrak{a} \subseteq \mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}. \tag{4.9}$$

The proof of the prime ideal theorem is predicated on the analytic features of the Dedekind zeta function. In this section, our main purposes are to make the continuation of the Dedekind zeta function $\zeta_K(s)$ meromorphically to $\sigma > 1 - \frac{1}{n}$ and to show that $\zeta_K(s)$ does not disappear for all s with $\sigma = 1$.

Third, we will mention the Wiener-Ikehara Tauberian theorem in its weaker form. It yields the proof of the prime ideal theorem. This theorem links the behavior of a real sequence to the analytic features of the associated Dirichlet series.

Finally, we will give the proof of the prime ideal theorem by making use of these three main parts.

4.1 Equivalent Statements of the Prime Ideal Theorem

Definition 4.1.1. *For a number field K and $x > 0$ we define Chebyshev's functions $\theta_K(x)$ and $\psi_K(x)$ by the formulas*

$$\theta_K(x) = \sum_{N(\mathfrak{p}) \leq x} \log N(\mathfrak{p}), \tag{4.10}$$

where $\mathfrak{p}$ *ranges over prime ideals in* $\mathcal{O}_K$ *with* $N(\mathfrak{p}) \leq x$*, and*

$$\psi_K(x) = \sum_{N(\mathfrak{a}) \leq x} \Lambda_K(\mathfrak{a}), \tag{4.11}$$

where $\mathfrak{a}$ *ranges over ideals in* $\mathcal{O}_K$ *with* $N(\mathfrak{a}) \leq x$ *and the von Mangoldt function* Λ_K *is defined by*

$$\Lambda_K(\mathfrak{a}) = \begin{cases} \log N(\mathfrak{p}), & \text{if} \quad \mathfrak{a} = \mathfrak{p}^m \\ 0, & otherwise. \end{cases} \tag{4.12}$$

Note that the definition of $\psi_K(x)$ is restated as follows:

$$\psi_K(x) = \sum_{N(\mathfrak{a}) \leq x} \Lambda_K(\mathfrak{a}) = \sum_{m} \sum_{N(\mathfrak{p}^m) \leq x} \log N(\mathfrak{p}) = \sum_{m} \sum_{N(\mathfrak{p}) \leq x^{1/m}} \log N(\mathfrak{p}). \tag{4.13}$$

In point of fact, that sum depending on m is finite. If $2 > x^{1/m}$, then $m > \frac{\log x}{\log 2}$ and the sum depending on $\mathfrak{p}$ is empty. Thus, we have that

$$\psi_K(x) = \sum_{m=1}^{\left\lfloor \frac{\log x}{\log 2} \right\rfloor} \sum_{N(\mathfrak{p}) \leq x^{1/m}} \log N(\mathfrak{p}) = \sum_{m=1}^{\left\lfloor \frac{\log x}{\log 2} \right\rfloor} \theta_K(x^{1/m}). \tag{4.14}$$

From this formula of $\psi_K(x)$, we obtain that

$$\psi_K(x) - \theta_K(x) = \sum_{m=2}^{\left\lfloor \frac{\log x}{\log 2} \right\rfloor} \theta_K(x^{1/m}). \tag{4.15}$$

As $N(\mathfrak{p})$ is a prime power, we can provide the following trivial bound for $\theta_K(x)$:

$$\theta_K(x) = \sum_{N(\mathfrak{p}) \leq x} \log N(\mathfrak{p}) \leq \sum_{N(\mathfrak{p}) \leq x} \log x \leq x \log x. \tag{4.16}$$

Therefore,

$$0 \leq \psi_K(x) - \theta_K(x) = \sum_{m=2}^{\left\lfloor \frac{\log x}{\log 2} \right\rfloor} \theta_K(x^{1/m}) \leq \sum_{m=2}^{\left\lfloor \frac{\log x}{\log 2} \right\rfloor} x^{1/m} \log x^{1/m} \leq \frac{\sqrt{x} \log^2 x}{2 \log 2}. \tag{4.17}$$

Dividing by x, we obtain that

$$0 \leq \frac{\psi_K(x)}{x} - \frac{\theta_K(x)}{x} \leq \frac{\log^2 x}{2\sqrt{x}\log 2}. \tag{4.18}$$

From the inequality (4.18), we deduce that

$$\lim_{x\to\infty}\left(\frac{\psi_K(x)}{x} - \frac{\theta_K(x)}{x}\right) = 0 \tag{4.19}$$

Put another way, $\theta_K(x) \sim x$ and $\psi_K(x) \sim x$ are equivalent statements.

Proposition 3. *For $x > 1$, we have*

1. $\theta_K(x) = \pi_K(x)\log x - \int_2^x \frac{\pi_K(t)}{t}dt.$
2. $\pi_K(x) = \frac{\theta_K(x)}{\log x} + \int_2^x \frac{\theta_K(t)}{t\log^2 t}dt.$

Proof. Let $\chi_K(\mathfrak{a})$ be the characteristic function of the prime ideals in $\mathcal{O}_K$. So,

$$\theta_K(x) = \sum_{N(\mathfrak{p})\leq x} \log N(\mathfrak{p}) = \sum_{N(\mathfrak{a})\leq x} \chi_K(\mathfrak{a})\log N(\mathfrak{a}). \tag{4.20}$$

By Abel's summation formula, one acquire that

$$\theta_K(x) = \pi_K(x)\log x - \int_2^x \frac{\pi_K(t)}{t}dt. \tag{4.21}$$

For (2), we have that

$$\pi_K(x) = \sum_{N(\mathfrak{p})\leq x} 1 = \sum_{N(\mathfrak{a})\leq x} \chi_K(\mathfrak{a}) = \sum_{N(\mathfrak{a})\leq x} \frac{\chi_K(\mathfrak{a})\log N(\mathfrak{a})}{\log N(\mathfrak{a})}. \tag{4.22}$$

Using Abel's summation formula, we acquire that

$$\pi_K(x) = \frac{\sum_{N(\mathfrak{a})\leq x}\chi_K(\mathfrak{a})\log N(\mathfrak{a})}{\log x} + \int_2^x \frac{\sum_{N(\mathfrak{a})\leq t}\chi_K(\mathfrak{a})\log N(\mathfrak{a})}{t\log^2 t}dt \tag{4.23}$$

$$= \frac{\theta_K(x)}{\log x} + \int_2^x \frac{\theta_K(t)}{t\log^2 t}dt. \tag{4.24}$$

□

Now, we can state more equivalent versions of the prime ideal theorem.

Theorem 4.1.1. *TFAE:*

1. $\pi_K(x) \sim \frac{x}{\log x}$.

2. $\theta_K(x) \sim x$.

3. $\psi_K(x) \sim x$.

Proof. We have already shown that the second and the third statements are equivalent. Thus, it suffices to show the equivalence of the first and the second. By Proposition 3,

$$\frac{\pi_K(x)\log x}{x} = \frac{\theta_K(x)}{x} + \frac{\log x}{x}\int_2^x \frac{\theta_K(t)}{t\log^2 t}dt, \tag{4.25}$$

$$\frac{\theta_K(x)}{x} = \frac{\pi_K(x)\log x}{x} - \frac{1}{x}\int_2^x \frac{\pi_K(t)}{t}dt. \tag{4.26}$$

Now, suppose that $\pi_K(x) \sim \frac{x}{\log x}$. Then, $\pi_K(t)/t = O(1/\log t)$ for $t \geq 2$. Thus, we obtain that

$$\frac{1}{x}\int_2^x \frac{\pi_K(t)}{t}dt = O\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\right). \tag{4.27}$$

As

$$\int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x-\sqrt{x}}{\log\sqrt{x}}, \tag{4.28}$$

we can obtain the limit

$$\lim_{x\to\infty}\left(\frac{1}{x}\int_2^x \frac{dt}{\log t}\right) = 0. \tag{4.29}$$

Therefore, by equation (4.26) we obtain that $\theta_K(x) \sim x$.

Conversely, assume that $\theta_K(x) \sim x$. Then, $\theta_K(t) = O(t)$ for $t \geq 2$. Thus, we see that

$$\frac{\log x}{x}\int_2^x \frac{\theta_K(t)}{t\log^2 t}dt = O\left(\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}\right). \tag{4.30}$$

Since

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x-\sqrt{x}}{\log^2\sqrt{x}}, \tag{4.31}$$

we can find the limit

$$\lim_{x\to\infty}\left(\frac{\log x}{x}\int_2^x \frac{dt}{\log^2 t}\right) = 0. \tag{4.32}$$

Therefore, by equation (4.25) we deduce that $\pi_K(x) \sim \frac{x}{\log x}$. □

4.2 The Dedekind Zeta Function

Definition 4.2.1. *The Dedekind zeta function of a number field K, denoted by $\zeta_K(s)$, is defined for all complex values s with $\sigma > 1$ as follows:*

$$\zeta_K(s) = \sum_{0\neq\mathfrak{a}\subseteq\mathcal{O}_K} \frac{1}{N(\mathfrak{a})^s}. \tag{4.33}$$

For example, we discussed that $\mathcal{O}_K = \mathbb{Z}$ when $K = \mathbb{Q}$. We also know that every ideal $\mathfrak{a} \subseteq \mathbb{Z}$ is of the form $n\mathbb{Z}$ for some positive $n \in \mathbb{Z}$. Hence, $N(\mathfrak{a}) = |\mathbb{Z}/n\mathbb{Z}| = n$ and we obtain that

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq\mathbb{Z}} \frac{1}{N(\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{1}{n^s} = \zeta(s). \tag{4.34}$$

We have seen in the algebraic part that if $K = \mathbb{Q}(i)$, then $\mathcal{O}_K = \mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is a PID, every ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is of the form $\mathfrak{a} = (a+ib)$ for some $a, b \in \mathbb{N}$. Then, the norm $N(\mathfrak{a}) = a^2 + b^2$ and hence we obtain that

$$\zeta_K(s) = \sum_{\mathfrak{a}\subseteq\mathbb{Z}[i]} \frac{1}{N(\mathfrak{a})^s} = \sum_{\substack{a,b\in\mathbb{N}\\(a,b)\neq(0,0)}} \frac{1}{(a^2+b^2)^s}. \tag{4.35}$$

In fact, the Dedekind zeta function is a generalization of the Riemann zeta function. Therefore, it is natural to ask the results about the Riemann zeta function $\zeta(s)$ to the Dedekind zeta function $\zeta_K(s)$. For instance, in which half plane does the Dedekind zeta function $\zeta_K(s)$ converge absolutely and does there any corresponding the Euler product of it?

Lemma 4.2.1. *For any $s \in \mathbb{C}$ with $\sigma > 1$,*

1. *There exists an Euler product for $\zeta_K(s)$*

$$\zeta_K(s) = \prod_{\mathfrak{p}\in\mathcal{P}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}, \tag{4.36}$$

where $\mathcal{P}$ is the set of prime ideals in $\mathcal{O}_K$, and the Euler product converges absolutely.

2. *The Dedekind zeta function $\zeta_K(s)$ is a holomorphic function with no zeros.*

Proof. 1. We proved that for a given number field K of degree n and a prime number p, there are at most n prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ lying above p and $N(\mathfrak{p}) \geq p$. Then,

$$\sum_{N(\mathfrak{p})\leq x} \left|\frac{1}{N(\mathfrak{p})^s}\right| \leq n \sum_{p\leq x} \frac{1}{p^\sigma}. \tag{4.37}$$

It gives the absolute convergence of the series $\sum_{\mathfrak{p}} N(\mathfrak{p})^{-s}$ provided that $\sigma > 1$. Hence, the Euler product is $\prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$ is absolutely convergent provided that $\sigma > 1$. Since every non-zero proper ideal $\mathfrak{a}$ in $\mathcal{O}_K$ factors uniquely into prime ideals $\mathfrak{p}$ and from the following geometric series

$$\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{k=0}^{\infty} \frac{1}{N(\mathfrak{p})^{ks}}, \tag{4.38}$$

we obtain that

$$\sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} \leq \prod_{\mathfrak{p}\in\mathcal{P}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} \tag{4.39}$$

for any real number $s > 1$. It follows that the Dedekind zeta function $\zeta_K(s)$ is absolutely convergent for all $s \in \mathbb{C}$ with $\sigma > 1$. Therefore,

$$\left|\sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s} - \prod_{N(\mathfrak{p})\leq x} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}\right| \leq \sum_{N(\mathfrak{a})>x} \frac{1}{N(\mathfrak{a})^\sigma} \to 0, \tag{4.40}$$

as $x \to \infty$, implying that

$$\zeta_K(s) = \prod_{\mathfrak{p}\in\mathcal{P}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}, \tag{4.41}$$

for all $s \in \mathbb{C}$ with $\sigma > 1$.

2. The convergence of $\zeta_K(s)$ is uniform on the compact subset in $\sigma > 1$, hence $\zeta_K(s)$ is holomorphic on this half plane. By the Euler product, we can easily see that $\zeta_K(s)$ has no roots there.

□

By the Euler product formula of $\zeta_K(s)$ for $s \in \mathbb{C}$ with $\sigma > 1$, we have that

$$\log \zeta_K(s) = \sum_{\mathfrak{p}} -\log\left(1 - \frac{1}{N(\mathfrak{p})^s}\right) = \sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{1}{nN(\mathfrak{p})^{ns}}. \tag{4.42}$$

If we taking the derivative (4.42), then

$$\frac{\zeta_K'}{\zeta_K}(s) = -\sum_{\mathfrak{p}} \sum_{n=1}^{\infty} \frac{\log N(\mathfrak{p})}{N(\mathfrak{p})^{ns}} = -\sum_{\mathfrak{a}} \frac{\Lambda_K(\mathfrak{a})}{N(\mathfrak{a})^s}, \tag{4.43}$$

where $\Lambda_K(\mathfrak{a}) = \log N(\mathfrak{a})$, if $\mathfrak{a} = \mathfrak{p}^m$, otherwise it is zero. We have proved in the algebraic part that the norm $N(\mathfrak{a})$ is always finite. Therefore, the Dedekind zeta function $\zeta_K(s)$ might be considered as an ordinary Dirichlet series

$$\zeta_K(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{4.44}$$

where a_n denotes the number of ideals $\mathfrak{a}$ with $N(\mathfrak{a}) = n$. Hence, the summatory function $A(x) = \sum_{n \leq x} a_n$ is equal to the number of ideals $\mathfrak{a}$ in $\mathcal{O}_K$ with $N(\mathfrak{a}) \leq x$. In the following lemma, we see an asymptotic formula of $A(x)$. For more details about the lemma, the reader might consult Lang (1994).

Lemma 4.2.2. *Suppose that K is a number field of degree n and $\mathcal{O}_K$ is the ring of integers of K. Then, the number $A(x)$ of ideals $\mathfrak{a}$ in $\mathcal{O}_K$ with $N(\mathfrak{a}) \leq x$ is*

$$A(x) = cx + O(x^{1-\frac{1}{n}}), \tag{4.45}$$

where $c = c(K)$ is a positive constant called the ***ideal density****.*

Now, we are ready to prove that the Dedekind zeta function $\zeta_K(s)$ has a meromorphic continuation to the half plane $\sigma > 1 - \frac{1}{n}$.

Lemma 4.2.3. *For any $s \in \mathbb{C}$ with $\sigma > 1 - \frac{1}{n}$,*

$$\zeta_K(s) = \frac{cs}{s-1} + s\int_1^\infty \frac{A(x) - cx}{x^{s+1}} dx \tag{4.46}$$

is an analytic function apart from a simple pole at $s = 1$ with residue c.

Proof. We apply Abel's summation formula to the partial sum of $\zeta_K(s)$. Then,

$$\sum_{n \leq x} \frac{a_n}{n^s} = \frac{A(x)}{x^s} + \int_1^x \frac{A(t)}{t^{s+1}} dt. \tag{4.47}$$

Keeping $\sigma > 1$ and letting $x \to \infty$, we obtain that

$$\zeta_K(s) = s\int_1^\infty \frac{A(t)}{t^{s+1}} dt = s\int_1^\infty \frac{c}{t^s} dt + \int_1^\infty \frac{A(t) - ct}{t^{s+1}} dt = \frac{cs}{s-1} + \int_1^\infty \frac{A(t) - ct}{t^{s+1}} dt. \tag{4.48}$$

But, we have that

$$\left| \int_1^\infty \frac{A(t) - ct}{t^{s+1}} dt \right| \leq \int_1^\infty \frac{Mt^{1-1/n}}{t^{\sigma+1}} dt = M\int_1^\infty \frac{dt}{t^{\sigma+1/n}} dt. \tag{4.49}$$

Note that the last integral is uniformly convergent for $\sigma > 1 - \frac{1}{n}$. Thus,

$$\zeta_K(s) = \frac{cs}{s-1} + s\int_1^\infty \frac{A(x) - cx}{x^{s+1}} dx \tag{4.50}$$

is an analytic function outside of a simple pole at $s = 1$ with residue c in $\sigma > 1 - \frac{1}{n}$. □

Lemma 4.2.4. *For $\sigma > 1$ and $t \in \mathbb{R}$,*

$$\Re\left(-3\frac{\zeta_K'}{\zeta_K}(\sigma) - 4\frac{\zeta_K'}{\zeta_K}(\sigma + it) - \frac{\zeta_K'}{\zeta_K}(\sigma + 2it) \right) \geq 0. \tag{4.51}$$

Proof. For $\sigma > 1$ and $t \in \mathbb{R}$,

$$-\frac{\zeta_K'}{\zeta_K}(s) = \sum_{\mathfrak{a}} \Lambda_K(\mathfrak{a}) N(\mathfrak{a})^{-s} \tag{4.52}$$

$$= \sum_{\mathfrak{a}} \Lambda_K(\mathfrak{a}) N(\mathfrak{a})^{-\sigma} e^{-it\log N(\mathfrak{a})} \tag{4.53}$$

$$= \sum_{\mathfrak{a}} \Lambda_K(\mathfrak{a}) N(\mathfrak{a})^{-\sigma} \Bigg(\cos(t \log N(\mathfrak{a})) - i \sin(t \log N(\mathfrak{a})) \Bigg). \tag{4.54}$$

Taking the real part of both sides, we obtain that

$$\Re\left(-\frac{\zeta_K'}{\zeta_K}(s) \right) = \sum_{\mathfrak{a}} \Lambda_K(\mathfrak{a}) N(\mathfrak{a})^{-\sigma} \cos(t \log N(\mathfrak{a})). \tag{4.55}$$

Thus, we have that

$$\Re\left(-3\frac{\zeta_K'}{\zeta_K}(\sigma) - 4\frac{\zeta_K'}{\zeta_K}(\sigma + it) - \frac{\zeta_K'}{\zeta_K}(\sigma + 2it) \right) \tag{4.56}$$

$$= \sum_{\mathfrak{a}} \Lambda_K(\mathfrak{a}) N(\mathfrak{a})^{-\sigma} \Bigg(3 + 4\cos(t \log N(\mathfrak{a})) + \cos(2t \log N(\mathfrak{a})) \Bigg). \tag{4.57}$$

On the other hand, we can easily observe that

$$3 + 4\cos x + \cos 2x = 2(1 + \cos x)^2 \geq 0. \tag{4.58}$$

Let us also note that $\Lambda(\mathfrak{a}) N(\mathfrak{a})^{-\sigma} \geq 0$ for every non-zero ideal $\mathfrak{a}$. Thus, it follows that

$$\Re\left(-3\frac{\zeta_K'}{\zeta_K}(\sigma) - 4\frac{\zeta_K'}{\zeta_K}(\sigma + it) - \frac{\zeta_K'}{\zeta_K}(\sigma + 2it) \right) \geq 0. \tag{4.59}$$

□

Lemma 4.2.5. *For all non-zero $t \in \mathbb{R}$, we have $\zeta_K(1 + it) \neq 0$.*

Proof. Let $1+it$ be a zero of $\zeta_K(s)$ of order $m \geq 1$ for some $t \in \mathbb{R}$. As $\zeta_K(s)$ possesses a simple pole at $s = 1$, the function

$$\zeta_K^3(\sigma)\zeta_K^4(\sigma + it)\zeta_K(\sigma + 2it)$$

has a zero of order $4m+k-3$ at $\sigma = 1$. Here, k denotes the order of zero of $\zeta_K(s)$ at $1+2it$. Then,

$$\zeta_K^3(\sigma)\zeta_K^4(\sigma+it)\zeta_K(\sigma+2it) = (\sigma-1)^{4m+k-3} f(\sigma), \tag{4.60}$$

where $f(1) \neq 0$. Thus, we deduce that

$$3\frac{\zeta_K'}{\zeta_K}(\sigma) + 4\frac{\zeta_K'}{\zeta_K}(\sigma+it) + \frac{\zeta_K'}{\zeta_K}(\sigma+2it) = \frac{4m+k-3}{\sigma-1} + \frac{f'}{f}(\sigma). \tag{4.61}$$

It follows that

$$\Re\left(3\frac{\zeta_K'}{\zeta_K}(\sigma) + 4\frac{\zeta_K'}{\zeta_K}(\sigma+it) + \frac{\zeta_K'}{\zeta_K}(\sigma+2it)\right) \to \infty, \tag{4.62}$$

as $\sigma \to 1^+$. However, it is a contradiction, because we have already proved in the previous lemma that

$$\Re\left(3\frac{\zeta_K'}{\zeta_K}(\sigma) + 4\frac{\zeta_K'}{\zeta_K}(\sigma+it) + \frac{\zeta_K'}{\zeta_K}(\sigma+2it)\right) \leq 0. \tag{4.63}$$

□

Lemma 4.2.6. *Suppose that $f(s)$ possesses a pole of order $m \geq 1$ at $s = \alpha$, then $\frac{f'}{f}(s)$ admits a simple pole at $s = \alpha$ with residue $-m$.*

Proof. As $f(s)$ possesses a pole of order $m \geq 1$ at $s = \alpha$, we have that

$$f(s) = \frac{g(s)}{(s-\alpha)^m}, \tag{4.64}$$

where $g(s)$ is analytic at $s = \alpha$ with $g(\alpha) \neq 0$. Thus, for any s with $|s-\alpha| < \varepsilon$,

$$\begin{aligned} f'(s) &= \frac{g'(s)(s-\alpha)^m - g(s)m(s-\alpha)^{m-1}}{(s-\alpha)^{2m}} && (4.65)\\ &= \frac{g'(s)}{(s-\alpha)^m} - \frac{g(s)m}{(s-\alpha)^{m+1}} && (4.66)\\ &= \frac{g(s)}{(s-\alpha)^m}\left(\frac{g'(s)}{g(s)} - \frac{m}{s-\alpha}\right). && (4.67) \end{aligned}$$

Thus, we obtain that

$$\frac{f'}{f}(s) = \frac{g'}{g}(s) - \frac{m}{s-\alpha}. \tag{4.68}$$

Since $\frac{g'}{g}(s)$ is analytic at $s = \alpha$, it follows that $\frac{f'}{f}(s)$ has a simple pole at $s = \alpha$ with residue $-m$. □

Corollary 4.2.6.1. *The logarithmic derivative* $-\frac{\zeta_K'}{\zeta_K}(s)$ *of* $\zeta_K(s)$ *has a simple pole at* $s = 1$ *with residue* 1.

Proof. We have seen that $\zeta_K(s)$ possesses a simple pole at $s = 1$. From above lemma, we acquire that $-\frac{\zeta_K'}{\zeta_K}(s)$ has a simple pole at $s = 1$ with residue 1. □

4.3 A Weak Version of the Wiener-Ikehara Tauberian Theorem

In this section, we shall see a proof of the Wiener-Ikehara Tauberian theorem in its weaker form. However, the reader might consult Montgomery & Vaughan (2007) for more details about the Wiener Ikehara Tauberian theorem. For a weak version of the Wiener Ikehara Tauberian theorem we based on the paper “Newman’s Short Proof of the Prime Number Theorem” written by Zagier (1997).

Lemma 4.3.1. *Let* $a_n \geq 0$ *and* $A(x) = \sum_{n \leq x} a_n$. *Suppose that*

$$\int_1^\infty \frac{A(x) - x}{x^2} dx$$

is a convergent integral. Then, $A(x) \sim x$ *as* $x \to \infty$.

Proof. In order to prove $A(x) \sim x$ as $x \to \infty$, we need to show that

$$\limsup_{x\to\infty} \frac{A(x)}{x} \leq 1 \leq \liminf_{x\to\infty} \frac{A(x)}{x}. \tag{4.69}$$

First, let us suppose that $\limsup \frac{A(x)}{x} > 1$. Then, there exist a constant $\lambda > 1$ and a sequence $(x_i) \to \infty$ such that $A(x_i) \geq \lambda x_i$. Since a_n is non-negative, the function

$A(x)$ is non-decreasing. Hence,

$$\int_{x_i}^{\lambda x_i} \frac{A(t)-t}{t^2}dt \geq \int_{x_i}^{\lambda x_i} \frac{A(x_i)-t}{t^2}dt \geq \int_{x_i}^{\lambda x_i} \frac{\lambda x_i - t}{t^2}dt. \tag{4.70}$$

Making the substitution, $u = t/x_i$ we obtain that

$$\int_{x_i}^{\lambda x_i} \frac{\lambda x_i - t}{t^2}dt = \int_1^{\lambda} \frac{\lambda - u}{u^2}du. \tag{4.71}$$

Since $\lambda > 1$, the integrand $(\lambda - u)/u^2$ is positive for any $u \in (1, \lambda)$. Therefore, we see that

$$\int_{x_i}^{\lambda x_i} \frac{A(t)-t}{t^2}dt = c(\lambda) > 0. \tag{4.72}$$

However, the tail of a convergent integral goes to 0 and that's why

$$\left| \int_{x_i}^{\lambda x_i} \frac{A(t)-t}{t^2}dt \right| = \left| \int_{x_i}^{\infty} \frac{A(t)-t}{t^2}dt - \int_{\lambda x_i}^{\infty} \frac{A(t)-t}{t^2}dt \right| \leq \varepsilon \tag{4.73}$$

for sufficiently large x_i. This contradicts the positivity of the integral $\int_{x_i}^{\lambda x_i} \frac{A(t)-t}{t^2}dt$. Thus, we have that

$$\limsup_{x\to\infty} \frac{A(x)}{x} \leq 1. \tag{4.74}$$

Similarly, one can see that

$$\liminf_{x\to\infty} \frac{A(x)}{x} \geq 1. \tag{4.75}$$

Therefore, we conclude that $A(x) \sim x$ as $x \to \infty$. □

Lemma 4.3.2 (Zagier (1997)). *For any $t \geq 0$, suppose that $Q(t)$ is a locally integrable and bounded function. Let the Laplace transform $L(s)$ of $Q(t)$ defined for $\sigma > 0$*

$$L(s) = \int_0^{\infty} \frac{Q(t)}{e^{st}}dt \tag{4.76}$$

extend to $\sigma \geq 0$ holomorphically. Then, $\int_0^{\infty} Q(t)dt$ converges and also

$$\int_0^{\infty} Q(t)dt = L(0). \tag{4.77}$$

Proof. Fix a large enough $T > 0$ and define $L_T(s)$ as follows:

$$L_T(s) = \int_0^T \frac{Q(t)}{e^{st}} dt. \tag{4.78}$$

In order to show that $\int_0^\infty f(t)dt$ converges and

$$\int_0^\infty Q(t)dt = L(0), \tag{4.79}$$

we need to prove that

$$\lim_{T\to\infty} L_T(0) = L(0). \tag{4.80}$$

Note that $L_T(s)$ is an entire function and

$$\frac{dL_T(s)}{ds} = \int_0^T (-t)Q(t)e^{-st}dt \tag{4.81}$$

which exists, since for $\sigma > 0$

$$\left| \int_0^T (-t)Q(t)e^{-st}dt \right| \leq \int_0^T T|Q(t)e^{-\sigma t}|dt \leq \int_0^T T|Q(t)|dt < \infty. \tag{4.82}$$

Choose a fixed sufficiently large R and let γ be the boundary of the domain $\{s \in \mathbb{C} : |s| \leq R, \sigma \geq -\delta\}$, where $\delta > 0$ is sufficiently small depending on R so that $L(s)$ is holomorphic inside and on the boundary γ. Let

$$h(s) = \big(L(s) - L_T(s)\big)e^{sT} \left(\frac{1}{s} + \frac{s}{R^2} \right). \tag{4.83}$$

As $h(s)$ possesses a simple pole only at $s = 0$ that lies inside γ, we have by residue theorem that

$$\frac{1}{2\pi i} \int_\gamma h(s)ds = Res_{s=0}h(s), \tag{4.84}$$

where the residue of $h(s)$ at $s = 0$ is

$$\lim_{s\to 0} sh(s) = \lim_{s\to 0} \big(L(s) - L_T(s)\big)e^{sT} \left(1 + \frac{s^2}{R^2}\right) = L(0) - L_T(0). \tag{4.85}$$

Thus, we obtain that

$$\frac{1}{2\pi i}\int_{\gamma} h(s)ds = L(0) - L_T(0). \tag{4.86}$$

Let $\gamma_+ = \gamma \cap \{s \in \mathbb{C} \, : \, \sigma > 0\}$. As $Q(t)$ be a bounded function, let $M = \sup_{t \geq 0} |Q(t)|$. Using ML-inequality, we obtain that

$$\left|\int_{\gamma_+} h(s)ds\right| \leq \frac{Me^{-\sigma T}}{\sigma} \cdot e^{\sigma T}\frac{2\sigma}{R^2} \cdot \pi R = \frac{2\pi M}{R}, \tag{4.87}$$

since

$$|L(s) - L_T(s)| = \left|\int_T^{\infty} Q(t)e^{-st}dt\right| \leq M\int_T^{\infty} e^{-\sigma t}dt = \frac{Me^{-\sigma T}}{\sigma} \tag{4.88}$$

and

$$\left|e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)\right| = e^{\sigma T}\left|\left(\frac{\sigma - it}{\sigma^2 + t^2} + \frac{\sigma + it}{R^2}\right)\right| = e^{\sigma T}\frac{2\sigma}{R^2}. \tag{4.89}$$

Now, let $\gamma_- = \gamma \cap \{s \in \mathbb{C} \; : \; \sigma < 0\}$ and γ' is the boundary of the domain $\{s \in \mathbb{C} \; : \; |s| \leq R, \sigma \leq 0\}$. As $g_T(s)$ is an entire function, we have by Cauchy's theorem that

$$\int_{\gamma'} L_T(s)ds = 0. \tag{4.90}$$

For that reason, we see that

$$\int_{\gamma_-} L_T(s)ds = \int_{\gamma'_-} L_T(s)ds, \tag{4.91}$$

where $\gamma'_- = \{s \in \mathbb{C} \, : \, |s| = R, \sigma < 0\}$. Then, we have that

$$|L_T(s)| = \left|\int_0^T Q(t)e^{-st}dt\right| \leq M\int_{-\infty}^{T} e^{-\sigma t}dt = \frac{Me^{-\sigma T}}{-\sigma}. \tag{4.92}$$

Hence, we obtain that

$$\left|\int_{\gamma_-} L_T(s)e^{sT}\left(\frac{1}{s} + \frac{s}{R^2}\right)ds\right| \leq \frac{Me^{-\sigma T}}{-\sigma} \cdot e^{\sigma T}\frac{-2\sigma}{R^2} \cdot \pi R = \frac{2\pi M}{R}. \tag{4.93}$$

It remains to show that

$$\left|\int_{\gamma^-} L(s)e^{sT}\left(\frac{1}{s}+\frac{s}{R^2}\right)ds\right| \to 0, \tag{4.94}$$

as $T \to \infty$. As $L(s)\left(\frac{1}{s}+\frac{s}{R^2}\right)$ isn't a function of T and e^{sT} converges uniformly to 0 on compact sets as $T \to \infty$ in $\sigma < 0$, we conclude that

$$\lim_{T\to\infty} |L(0) - L_T(0)| = \lim_{T\to\infty}\left|\frac{1}{2\pi i}\int_\gamma h(s)ds\right| \le \frac{2M}{R}. \tag{4.95}$$

Letting $R \to \infty$, we get the proof. □

Theorem 4.3.3 (A Weak Version of the Wiener-Ikehara Tauberian Thereom). *Suppose that $a_n \ge 0$ and $A(x) = \sum_{n\le x} a_n = O(x)$. If the Dirichlet series*

$$D(s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s} \tag{4.96}$$

is absolutely convergent in $\sigma > 1$ and it extends analytically to $\sigma \ge 1$ apart from a simple pole at $s = 1$ with residue 1, then $A(x) \sim x$, as $x \to \infty$.

Proof. By Abel's summation formula,

$$\sum_{n\le x}\frac{a_n}{n^s} = \frac{A(x)}{x^s} + s\int_1^x \frac{A(t)}{t^{s+1}}dt. \tag{4.97}$$

Because $A(x) = O(x)$, by letting $x \to \infty$ we obtain that

$$D(s) = s\int_1^\infty \frac{A(t)}{t^{s+1}}dt \tag{4.98}$$

for any $\sigma > 1$. Then, we see that

$$D(s) - \frac{s}{s-1} = s\int_1^\infty \frac{A(t)-t}{t^{s+1}}dt \tag{4.99}$$

is analytic for $\sigma \ge 1$. Putting $s+1$ in place of s and dividing both sides by $s+1$, we obtain that

$$\frac{D(s+1)}{s+1} - \frac{1}{s} = \int_1^\infty \frac{A(t)-t}{t^{s+2}} dt \tag{4.100}$$

is analytic for $\sigma \geq 0$. Making the substitution $u = \log t$, we deduce that

$$\frac{D(s+1)}{s+1} - \frac{1}{s} = \int_0^\infty \left(\frac{A(e^u)-e^u}{e^u}\right) e^{-su} du \tag{4.101}$$

is analytic for $\sigma \geq 0$. Moreover, the function

$$f(u) = \frac{A(e^u)-e^u}{e^u} \tag{4.102}$$

is bounded, locally integrable and

$$g(s) = \int_0^\infty \left(\frac{A(e^u)-e^u}{e^u}\right) e^{-su} du \tag{4.103}$$

is the Laplace transform of $f(u)$. Making the substitution $x = e^u$, we obtain by Lemma 4.3.2 that

$$\int_0^\infty \frac{A(e^u)-e^u}{e^u} du = \int_1^\infty \frac{A(x)-x}{x^2} dx \tag{4.104}$$

is a convergent integral. Then, Lemma 4.3.1 gives $A(x) \sim x$, as $x \to \infty$. □

4.4 Proof of the Prime Ideal Theorem

Remember that a prime number p admits at most n many prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ that lies above p and $N(\mathfrak{p}) \geq x$. Then, we obtain that

$$\theta_K(x) = \sum_{N(\mathfrak{p}) \leq x} \log N(\mathfrak{p}) \leq \sum_{p \leq x} n \log p^n = n^2 \theta(x) \ll_n x, \tag{4.105}$$

Hence,

$$\psi_K(x) = \sum_m \theta_K(x^{1/m}) = \theta_K(x) + \theta_K(\sqrt{x}) + \theta_K(\sqrt[3]{x}) + \cdots \ll_n x \tag{4.106}$$

which means that $\psi_K(x) = O(x)$. We also know from Section 4.2 that the Dirichlet series

$$-\frac{\zeta_K'}{\zeta_K}(s) = \sum_{\mathfrak{a}} \frac{\Lambda_K(\mathfrak{a})}{N(\mathfrak{a})^s} \tag{4.107}$$

is an analytic function in $\sigma \geq 1$ except for a simple pole at $s = 1$ with residue 1. These are all the assumptions of a weak version of the Wiener-Ikehara Tauberian theorem. Therefore, $\psi_K(x) \sim x$ which proves the prime ideal theorem. □

CHAPTER FIVE
CONCLUSION

In this dissertation, we aimed to give a different proof for the prime ideal theorem than Landau's original proof using the Wiener Ikehara Tauberian theorem in its weaker form. Firstly, in the algebraic part our main goal was to show that the ring of integers of a number field is a Dedekind domain. Besides, we proved that the norm of an ideal in the ring of integers is finite. We also showed that the norm is a completely multiplicative function. In the analytic part, we first stated two equivalent forms of the prime ideal theorem in terms of the analogues of Chebyshev's functions $\theta(x)$ and $\psi(x)$. Then, we examined some of the most important analytic properties of the Dedekind zeta function. We considered its behavior on the line $\sigma = 1$. We showed that it has no zero on this line. Finally, by combining non-vanishing of the Dedekind zeta function on the line $\sigma = 1$ and a weak version of the Wiener Ikehara-Tauberian theorem, we concluded the prime ideal theorem without an error term.

REFERENCES

Apostol, T. (1998). *Introduction to Analytic Number Theory*. Undergraduate Texts in Mathematics. New York: Springer.

Davenport, H. (2000). *Multiplicative Number Theory*. Graduate Texts in Mathematics. New York: Springer.

Fraleigh, J. (2003). *A First Course in Abstract Algebra*. Addison-Wesley series in mathematics. Boston: Addison-Wesley.

Jarvis, F. (2014). *Algebraic Number Theory*. Springer Undergraduate Mathematics Series. New York: Springer.

Landau, E. (1903). Neuer beweis des primzahlsatzes und beweis des primidealsatzes. *Mathematische Annalen*, *56*, 645-670.

Lang, S. (1994). *Algebraic Number Theory*. Graduate Texts in Mathematics. Verlag, New York: Springer.

Montgomery, H., & Vaughan, R. (2007). *Multiplicative Number Theory I: Classical Theory*. Cambridge Studies in Advanced Mathematics. New York: Cambridge University Press.

Samuel, P. (1970). *Algebraic Theory of Numbers*. Paris: Hermann.

Zagier, D. (1997). Newman’s short proof of the prime number theorem. *The American Mathematical Monthly*, *104*, 705-708.