FACTORING OF PRIME IDEALS IN THE RING OF INTEGERS OF ALGEBRAIC EXTENSIONS OF □

by

Dursun ÇALIŞKAN

A thesis submitted to

The Graduate Institute of Sciences and Engineering

of

Fatih University

in partial fulfillment of the requirements for the degree of

Master of Science

in

Mathematics

June 2005
Istanbul, Turkey

FACTORING OF PRIME IDEALS IN THE RING OF INTEGERS OF ALGEBRAIC EXTENSIONS OF □

Dursun ÇALIŞKAN

M. S. Thesis - Mathematics
June 2005

Supervisor: Prof. Dr. Barış KENDİRLİ

ABSTRACT

In this thesis, factoring of prime ideals in the ring of integers of an algebraic extension of □ is investigated. Especially, quadratic and cyclotomic extensions are considered and their essentials are presented. Fundamental concepts and theorems of algebraic number fields, domains and ideals are given. The relationship between these concepts are stated, proved and supported by examples. Some techniques for proving if a domain is Euclidean are given. A quick technique for factoring of prime ideals in quadratic extensions of □ is given. The theoretical statements for factorization of ideals in a given extension are supported by examples.

Keywords: Factorization, unique factorization, ideal, domain, algebraic number field, the ring of integers of an algebraic number field, norm, trace, discriminant.

RASYONEL SAYILAR CİSMİNİN GENİŞLEMELERİNİN TAMSAYILAR HALKASINDA İDEALLERİN ÇARPANLARA AYRILMASI

Dursun ÇALIŞKAN

Yüksek Lisans Tezi – Matematik
Haziran 2005

Tez Yöneticisi: Prof. Dr. Barış KENDİRLİ

ÖZ

Bu tezde, Rasyonel Sayılar Cisminin genişlemelerinin tamsayılar halkasında ideallerin çarpanlara ayrılması araştırıldı. Özellikle, quadratik ve birimin primitif kökleriyle oluşturulan genişlemeler ele alındı ve bunlarla ilgili esas teoremler ispatlarıyla birlikte sunuldu. Genişlemelerin, halkaların ve ideallerin temel teoremleri ele alınarak, bunlar arasındaki ilişkiler örneklerle desteklenerek gösterildi. Bir cebirsel alanın öklid alanı olmasının ispat edilmesinde bazı teknikler gösterildi. Rasyonel sayılar cisminin quadratik genişlemelerinin tamsayılar halkasında ideallerin çarpanlara ayrılmasının bir pratik tekniği verildi. İdeallerin çarpanlara ayrılmasının teorisi örneklerle desteklendi.

Anahtar Kelimeler: Çarpanlara ayırma, çarpanlara ayırmanın tekliği, ideal, cebirsel alan, cebirsel sayı cismi, bir cebirsel sayı cisminde tamsayı halkası, norm, iz, diskirminant.

DEDICATION

To my parents

ACKNOWLEDGEMENT

I express sincere appreciation to Prof. Dr. Barış KENDİRLİ for his guidance and insight throughout the research.

Thanks go to the other faculty members, Ast. Prof. Tevfik BİLGİN, Prof. Dr. Allaberen ASHYRALYEV, Ast. Prof. Ali ŞAHİN, Ast. Prof. İbrahim ABU-ALSAİKH and Bülent KÖKLÜCE, for their valuable suggestions and comments.

Lastly, I am glad to thank to my parents for their encouragement, understanding and motivation.

TABLE OF CONTENTS

LIST OF SYMBOLS

$\mathbb{N}$	The Set of Natural Numbers
$\mathbf{Z}$	The Ring of Integers
$\mathbb{Q}$	The Field of Rational Numbers
$\mathbb{R}$	The Field of Real Numbers
$\mathbb{C}$	The Field of Complex Numbers
ζ_n	n'th primitive root of unity
$\mathbf{Z}[\alpha]$	The ring generated by α
$F[x]$	The ring of polynomials over the field F
$\mathbb{Q}(\alpha)$	The algebraic number field generated by α
$m_{\alpha,F}(x)$	The minimal polynomial of α over the field F
deg(f)	The degree of the polynomial f
$\lvert F(\alpha):F\rvert$	The degree of extension field $F(\alpha)$ over the field F
$F \subseteq K$	F is a subfield of the field K
$N_F(\alpha)$	The norm of α from the field F
$T_F(\alpha)$	The trace of α from the field F
$\mathbb{A}_F$	The ring of integers in the algebraic number field F
disc(B)	The discriminant of the integral basis B
Δ_F	The discriminant of the algebraic number field F
$\binom{n}{r}$	The number of r-combinations of n
disc(f)	The discriminant of the polynomial F
$U(R)$	The group of units of the ring R
$a\lvert b$	a divides b
$\Phi_n(x)$	The n'the cyclotomic polynomial
$\phi(n)$	The number of positive integers less then n which are relatively prime to n
R/I	The quotient ring
$I \supseteq J$	The ideal I contains the ideal J
$I \subset J$	The ideal I is contained by different ideal J
(α)	The ideal generated by α
(α,β)	The ideal generated by α and β
$(\alpha_1,\alpha_2,...,\alpha_r)$	The ideal generated by $\alpha_1,\alpha_2,...,\alpha_r$
$I\lvert J$	The ideal I divides the ideal J
det(A)	The determinant of the matrix A
$p\mathbb{A}_F$	The lifting of the prime ideal p to $\mathbb{A}_F$
$N(I)$	The norm of ideal I

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

Factorization takes important place in many areas of mathematics. For example, it is very powerful technique to use factorization for solving Diophantine equations in number theory. Moreover, recently it has important applications in some areas such as cryptography, computer science and mathematical biology.

As far as factorization is considered, uniqueness of the factorization has to be discussed. In some domain an element may have more then one factorizations. For instance, consider $D = \left\{ a + b\sqrt{10} : a, b \in \mathbb{Z} \right\}$. In this domain,

$$6 = 2 \times 3 = (4 + \sqrt{10})(4 - \sqrt{10}),$$

where each factor can not be factorized any more. So, 6 has at least two factorizations in *D*. *D is* said to be not unique factorization domain. Domains and related concepts will be discussed in chapter 3.

When one deals with factorization he/she has to remember the famous problem,

$$\textit{There is no } x, y, z \in \mathbb{Z} \textit{ such that } x^n + y^n = z^n$$

$$\textit{with } xyz \neq 0, \textit{ for any natural number } n \geq 3.$$

This is known as *Fermat's Last Theorem* (FLT), it could not be proven for centuries.

A proof of FLT for $n = 3$ was published in 1770 by Leonhard Euler, the most prolific mathematicians of all time. Euler's proof involved using numbers of the form $a + b\sqrt{-3}$ where $a, b \in \mathbb{Z}$. At one point in this argument, he made a claim about these numbers which was apparently based on tacit assumption that they obey unique factorization. His claim was correct, but the tacit assumption behind it was not, and this proof remained incomplete until the missing justification was supplied by Legendre some time later.

A proof for $n = 5$ was given by Legendre and independently by Dirichlet around 1825. The case n = 7 was handled by Lame in 1840. The first general -and by far the most significant- attack on the problem was made by E. Kummer in 1843. Kummer's basic idea was to consider numbers of the form

$$a_0 + a_1\zeta_p + a_2\zeta_p^{\,2} + \ldots + a_{p-1}\zeta_p^{\,p-1}$$

where p is prime, $a_0, a_1, a_2, \ldots, a_{p-1} \in \mathbb{Z}$ and ζ_p is the primitive p'th root of unity. These numbers form a sub ring of $\mathbb{C}$, denoted by $\mathbb{Z}[\zeta_p]$.Using them it is possible to factor $x^p + y^p$ completely and the equation $x^p + y^p = z^p$ becomes

$$(x+y)(x+\zeta_p y)(x+\zeta_p{}^2 y)...(x+\zeta_p{}^{p-1} y) = z^p .$$

Assuming that factorization of any number in $\mathbb{Z}[\zeta_p]$ is unique, Kummer used this form of the equation to prove that $x^p + y^p = z^p$ is impossible if $xyz \neq 0$. Kummer presented his proof to Dirichlet and Dirichlet pointed out that Kummer had neglected to verify the assumption that factorization into irreducibles is unique in $\mathbb{Z}[\zeta_p]$. (Kummer was later to point out a similar flaw in an attempt by Lame.) In 1847, Cauchy (after having made the same mistake himself) pointed out that factorization is not unique in $\mathbb{Z}[\zeta_{23}]$. Thus, Fermat's last theorem remained unproved.

Kummer was undaunted and set about trying to modify $\mathbb{Z}[\zeta_p]$ so as to restore the uniqueness of factorization. He introduced what he called ideal numbers, and the theory he developed was a precursor of the modern theory of ideals [1] and also see [2],[3]. Theory of ideals will be discussed in chapter 5.

Hundreds of mathematicians have tried to prove *FLT*. Common idea in their works was factorization and common mistake was assuming the factorization is unique in the domain that they work Tens of books have been written and thousands of theorems have been stated about *FLT* .The most essentially, tens of methods and two important approaches (algebraic and analytic approaches) have been developed in the way of proving *FLT*. Behind all these, two areas of mathematics have been systemized. They are Algebraic Number Theory and Analytic Number Theory see [2-8].

In this thesis, essentials of factorization with the view of algebraic approach are discussed; all facts in the road of understanding of factorization are considered. I have studied on theory of factorization, not on application. Application desires different kind of study.

For more basic facts, see [1] and [9-15].

In chapter 1, the thesis has been introduced and supported by history.

In chapter 2, definitions of algebraic numbers, algebraic number fields, the ring of integers of an algebraic number field, norm of an algebraic number field, and trace of an algebraic number field and discriminant of an algebraic number field; essential theorems related with them which take important place in development of factorization are given.

In chapter 3, definitions of domains and some theorems that give relations between domains and essential concepts to understand these relations are given.

In this thesis, mainly two important algebraic number fields are considered: First one quadratic fields and second one cyclotomic fields. Their essentials are discussed in chapter 4.

In chapter 5, theory of ideals and Dedekind domain are given.

In chapter 6, methods of factorization of an ideal into prime ideals and related theorems are given.

In chapter 2-6, theory is supported by examples.

In chapter 7, a short conclusion of the thesis is made.

CHAPTER 2

ALGEBRAIC NUMBER FIELDS AND SOME ARITHMETIC IN THEM

Facts and techniques of Abstract Algebra have been applied to solve problems of Number Theory for centuries. For example, many great mathematicians have used algebraic approach to try to prove Fermat's Last Theorem (*FLT*) which is very famous in number theory. And also, it is proven by Andrew Wiles by using combination of algebraic and analytic approaches.

In this study, we deal with algebraic approach to understand factorization of prime ideal in domains which takes important place in solving many problems of Number Theory.

To roughly understand the idea of algebraic approach let us start with an example.

Proposition 2.1 Let p be an odd prime. There exists a unique pair (a, b) of integers up to sign and order such that $p = a^2 + b^2$ if and only if $p \equiv 1 \pmod 4$.

Proof. Assume that $p \equiv 1 \pmod 4$, i.e. $p = 4n + 1$ for some natural number n.
By Wilson's Theorem, $(p-1)! \equiv -1 \pmod p$

$\Rightarrow$ 1 x 2 x 3 x... x 2n x $(2n+1)$ x $(2n+2)$ x ...x $(4n-1)$ x $4n \equiv -1 \pmod p$

$\Rightarrow$ 1 x 2 x 3 x... x 2n x $(-2n)$ x (-(2n -1)) x ...x (-2) x (-1) $\equiv -1 \pmod p$

$\Rightarrow$ $(-1)^{2n} 1^2 2^2 3^2 ... (2n)^2 \equiv -1 \pmod p$

$\Rightarrow$ $(1x2x3x...x2n)^2 \equiv -1 \pmod p$

So, there exists an integer m such that $m^2 \equiv -1 \pmod p$ or $m^2 + 1 \equiv 0 \pmod p$, implying that $(m-i)(m+i) = kp$ for some integer k. This means, p divides $(m-i)(m+i)$ in $\mathbb{Z}[i]$. It is clear that p divides neither $(m-i)$ nor $(m+i)$; so p is not prime; hence not irreducible in $\mathbb{Z}[i]$ since $\mathbb{Z}[i]$ is Principle Ideal Domain (*PID*). Thus, $p = \alpha\beta$ for some nonunit elements α and β of $Z[i]$. Let $\alpha = a + bi$ and $\alpha = a + bi$ for some integers a, b, c and d.
Since $N(p) = N(\alpha)N(\beta)$, $p^2 = (a^2 + b^2)(c^2 + d^2)$. On the other hand, neither $a^2 + b^2$ or $c^2 + d^2$ is 1 because α and β are not unit. Since Z is Unique Factorization Domain (*UFD*), $a^2 + b^2 = p = c^2 + d^2$. Being *UFD* of $\mathbb{Z}[i]$ requires uniqueness of the pair (a,b).

Assume that $p \equiv 3 \pmod 4$. Since square of an integer is equivalent to either 0 or 1 mod 4, the sum of two squares is equivalent to 0, 1 or 2 mod 4. Therefore, p can not be written as sum of two squares.

In this proof; some terms such as *PID* and *UFD*, some symbols such as $N(\alpha)$ and $\mathbb{Z}[i]$ have been occurred. They are concepts and symbols of Abstract Algebra; we are going to discuss them later.

2.1 Extensions

Definition 2.2 (Algebraic Numbers and Algebraic Number Fields)

A complex number which is a root of a polynomial of degree *d* and not a root of any polynomial of degree less then *d* is called an algebraic number of degree *d.*

Let α be an algebraic number of degree *d*. The field containing $\mathbb{Q}$ and α is called an algebraic number field of degree *d*. An algebraic number field is extension of $\mathbb{Q}$ generated by α and denoted by $\mathbb{Q}(\alpha)$.

For example; $\sqrt{2}$, *i* and $\sqrt{-5}$ are algebraic numbers of degree 2. $\mathbb{Q}(\sqrt{2}), \mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-5})$ are algebraic number fields. They are quadratic extensions of $\mathbb{Q}$. Here, $\mathbb{Q}(\sqrt{-5})$ can be explicitly written as $\left\{ q_1 + q_2\sqrt{-5} \,/\, q_1, q_2 \in \mathbb{Q} \right\}$.

$\sqrt[3]{3}$ is an algebraic number of degree 3, and $\mathbb{Q}(\sqrt[3]{3}) = \left\{ q_1 + q_2\sqrt[3]{3} + q_3\sqrt[3]{9} \,/\, q_1, q_2, q_3 \in \mathbb{Q} \right\}$ is a cubic extension of $\mathbb{Q}$.

$\alpha = e^{\frac{2\pi i}{5}}$ (fifth root of unity) is an algebraic number of degree 4 and $\mathbb{Q}(\alpha) = \left\{ q_1 + q_2\alpha + q_3\alpha^2 + q_4\alpha^3 \,/\, q_1, q_2, q_3, q_4 \in \mathbb{Q} \right\}$ is an extension of $\mathbb{Q}$ with degree of extension 4.

Definition 2.3 (Simple Extensions and Polynomials)

Let *F* be field and *E* be extension field of *F* and $\alpha \in E$. If there exists a nonzero $f(x) \in F[x]$ such that $f(\alpha) = 0$ then α is said to be algebraic over *F*. *E* is called algebraic extension of *F* if every element of *E* is algebraic over *F*.

The polynomial $f(x) \in F[x]$ such that ***i)*** $f(\alpha) = 0$ ***ii)*** $f(x)$ is monic ***ii)*** for any nonzero polynomial $g(x) \in F[x]$ with $g(\alpha) = 0$, $\deg(f) \le \deg(g)$ is called the minimal polynomial of α over *F*, denoted by $m_{\alpha,F}(x)$.

Let *F* be an algebraic number field and α be algebraic over *F*. The smallest field containing both α and *F* is called simple algebraic extension of *F* generated by α, denoted by $F(\alpha)$.

Theorem 2.4 (Existence and Uniqueness of the Minimal Polynomial)

Let *F* be an algebraic number field and α be algebraic over *F*. Then α has a unique minimal polynomial over *F*.

Proof. Existence is coming from being α algebraic over *F* (Definition 2.2). Let $f(x) \in F[x]$ be a minimal polynomial of α over *F* and there exists a nonzero polynomial $g(x) \in F[x]$ with $g(x) \neq f(x)$ and $g(\alpha) = 0$. By division Algorithm for polynomials there exist $q(x), r(x) \in F[x]$ such that

$$g(x) = f(x)q(x) + r(x) \text{ with } \deg(r) < \deg(f) \text{ or } r(x) = 0.$$

By substituting $x = \alpha$, we have $r(\alpha) = 0$. Since $f(x)$ is a minimal polynomial of α over $F, r(x) = 0$. So $g(x) = f(x)q(x)$, $g(x) \neq f(x) \Rightarrow q(x) \neq 1$. If $q(x)$ is constant, then $g(x)$ is not monic, hence can not be the minimal polynomial of α over *F*. Otherwise, $\deg(g) > \deg(f)$ and so $g(x)$ can not be the minimal polynomial of α over *F which* requires uniqueness of the minimal polynomial.

Example 2.5 Let's find the minimal polynomial of $\alpha = \sqrt{1+\sqrt{-3}}$ over $\mathbb{Q}$.

$\alpha^2 = 1+\sqrt{-3} \Rightarrow \alpha^2 - 1 = \sqrt{-3} \Rightarrow (\alpha^2-1)^2 = -3 \Rightarrow \alpha^4 - 2\alpha^2 + 4 = 0$

So, $m_{\alpha,\mathbb{Q}}(x) = x^4 - 2x^2 + 4$.

Corollary 2.6 Let $f(x) \in F[x]$ be a minimal polynomial of α over *F* and $g(\alpha) = 0$ for some $g(x) \in F[x]$. Then $f(x)$ divides $g(x)$ in $F[x]$.

Proof. In the proof of Theorem 2.4 we obtained $g(x) = f(x)q(x)$ for some $q(x) \in F[x]$ which directly implies desired result.

Corollary 2.7 Any irreducible polynomial over an algebraic number field has no repeated roots in $\mathbb{C}$.

Proof. Let $f(x) \in F[x]$ be irreducible. Assume that $f(x)$ has repeated root of $\alpha \in F$. Then,

$$f(x) = (x-\alpha)^2 g(x) \text{ For some } g(x) \in F[x].$$

Therefore, $m_{\alpha,F}(x)$ divides $f(x)$ by Corollary 2.6.Since $f(x)$ is irreducible, $f(x) = \beta m_{\alpha,F}(x)$ for some $\beta \in F$, i.e. $\deg(f) = \deg(m_{\alpha,F})$. However,

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x).$$

So, $f'(\alpha) = 0$, implying that $m_{\alpha,F}(x)$ divides $f'(x)$ which is a contradiction since $\deg(f') < \deg(f) = \deg(m_{\alpha,F})$. Thus, f has no repeated roots in $\mathbb{C}$.

Example 2.8 Let $F = \mathbb{Q}(i)$ and $\alpha = e^{\frac{2\pi i}{8}}$ (eighth root of unity).

Although $m_{\alpha,\mathbb{Q}}(x) = x^4 + 1$, $m_{\alpha,F}(x) = x^2 + i$.

Corollary 2.9 Let *F* be an algebraic number field, α be algebraic over *F* with $\deg(m_{\alpha,F}) = d$ and $F(\alpha)$ be the simple extension of *F* generated by α.

Every element $\beta \in F(\alpha)$ can be written uniquely in the form

$$\beta = \sum_{k=1}^{d} a_k \alpha^{k-1} \text{ For some } a_1, a_2, ..., a_d \in F .$$

Proof. Let $\beta \in F(\alpha)$. Then $\beta = \dfrac{f(\alpha)}{g(\alpha)}$ for some $f(x), g(x) \in F[x]$ such that $g(\alpha) \neq 0$. By Corollary 2.6, $m_{\alpha,F}(x)$ does not divide $g(x)$. Hence, $m_{\alpha,F}(x)$ and $g(x)$ are relatively prime. So, there exist $p(x), q(x) \in F[x]$ such that $p(x)m_{\alpha,F}(x) + q(x)g(x) = 1$.

$$m_{\alpha,F}(\alpha) = 0 \Rightarrow \frac{1}{g(\alpha)} = q(\alpha) \Rightarrow \beta = f(\alpha)q(\alpha) .$$

Let $h(x) = f(x)q(x)$. By division algorithm for polynomials, there exist unique $a(x), r(x) \in F[x]$ such that $h(x) = a(x)m_{\alpha,F}(x) + r(x)$ with $\deg(r) < \deg(m_{\alpha,F})$ or $r(x) = 0$. Since $m_{\alpha,F}(\alpha) = 0$, $\beta = f(\alpha)q(\alpha) = h(\alpha) = r(\alpha)$. Letting

$$r(x) = a_1 + a_2\alpha + ... + a_d\alpha^{d-1},$$

we have $\beta = \sum_{k=1}^{d} a_k \alpha^{k-1}$ for some $a_1, a_2, ..., a_d \in F$.

Corollary 2.10 Let F be an algebraic number field and E be an extension field of F, and let $\alpha \in E$. $F(\alpha)$ is a finite extension of F if and only if α is algebraic over F. Moreover, if α is algebraic over F, then $|F(\alpha) : F| = \deg(m_{\alpha,F})$.

Proof. Assume that α is algebraic over F. By Corollary 2.9, every element $\beta \in F(\alpha)$ can be written uniquely in the form $\beta = \sum_{k=1}^{d} a_k \alpha^{k-1}$ for some $a_1, a_2, ..., a_d \in F$. So $|F(\alpha) : F|$ is finite. Conversely assume that, $|F(\alpha) : F| = d$ for some $d \in N$. Therefore, $F(\alpha)$ is a vector space with the base $\{1, \alpha, \alpha^2, \alpha^3, ..., \alpha^{d-1}\}$. From here, $\alpha^d = q_1 + q_2\alpha + q_3\alpha^2 + ... + q_d\alpha^{d-1}$ for some $q_1, q_2, q_3, ..., q_d \in F \Rightarrow q_1 + q_2\alpha + q_3\alpha^2 + ... + q_d\alpha^{d-1} - \alpha^d = 0$. Thus, α is algebraic over F with $\deg(m_{\alpha,F}) = d$.

Example 2.11 Let $\alpha = e^{\frac{2\pi i}{8}}$ (eighth root of unity).
If $F = \mathbb{Q}(i)$, then $|F(\alpha) : F| = 2$. But if $F = \mathbb{Q}$, then $|F(\alpha) : F| = 4$.

Proposition 2.12 Let $F \subseteq K \subseteq E \subseteq \mathbb{C}$, where F, K and E are fields then,

$$|E : F| = |E : K|.|K : F| .$$

Proof. Let $\{\alpha_1, \alpha_2, ..., \alpha_k\}$ and $\{\beta_1, \beta_2, ..., \beta_l\}$ be basis for *K* over *F* and *E* over *K* respectively. If $\alpha \in E$ then it has a unique representation

$$\alpha = \sum_{i=1}^{l} a_i \beta_i \text{ , where } a_i \in K \text{ for every } i \in \{1,2,...,l\}.$$

On the other hand for every $i \in \{1,2,...,l\}$ $a_i \in K$ has unique representation

$$a_i = \sum_{i=1}^{k} b_i \alpha_i \text{ , where } b_i \in F \text{ for every } i \in \{1,2,...,k\}.$$

Thus, $\alpha \in E$ has a unique representation

$$\alpha = \sum_{i=1}^{l} a_i \beta_i = \sum_{j=1}^{l} \beta_j \sum_{i=1}^{k} b_i \alpha_i = \sum_{j=1}^{l} \sum_{i=1}^{k} b_i \alpha_i \beta_j$$

This yields

$$|E : F| = |E : K| . |K : F| .$$

Proposition 2.13 Let *p* be a prime and ζ_p be *p*'th root of unity.
$m_{\zeta_p, Q}(x) = x^{p-1} + x^{p-2} + x^{p-3} + ... + 1$.

Proof. It is easy to see that $(\zeta_p)^{p-1} + (\zeta_p)^{p-2} + (\zeta_p)^{p-3} + ... + 1 = 0$. For the minimality it is enough to prove that $m_{\zeta_p, Q}(x) = x^{p-1} + x^{p-2} + x^{p-3} + ... + 1$ is irreducible over $\mathbb{Q}$.

Assume that $\frac{x^p - 1}{x - 1} = (x^n + a_{n-1}x^{n-1} + ... + a_0)(x^m + b_{m-1}x^{m-1} + ... + b_0)$.

Then

$$\frac{(x+1)^p - 1}{(x+1) - 1} = ((x+1)^n + a_{n-1}(x+1)^{n-1} + ... + a_0)((x+1)^m + b_{m-1}(x+1)^{m-1} + ... + b_0).$$

So, $\frac{(x+1)^p - 1}{(x+1) - 1}$ is irreducible over $\mathbb{Q}$. But

$$\frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + \binom{p}{1} x^{p-2} + ... + \binom{p}{p-2} x + p$$

which is irreducible over $\mathbb{Q}$ by Eisenstein Criterion. This is a contradiction.
Therefore, $m_{\zeta_p, Q}(x) = x^{p-1} + x^{p-2} + x^{p-3} + ... + 1$ is irreducible over $\mathbb{Q}$.

Proposition 2.14 Let *p* be an odd prime and ζ_p be p'th root of unity.
$F = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ is an algebraic number field of degree $(p-1)/2$.

Proof. By Proposition 2.12 and Corollary 2.10 $|\mathbb{Q}(\zeta_p) : \mathbb{Q}| = p - 1$. It is easy to see that $|\mathbb{Q}(\zeta_p) : \mathbb{Q}(\zeta_p + \zeta_p^{-1})| = 2$. So, $|\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}| = (p-1)/2$.

Thus, $F=\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ is an algebraic number field of degree $(p-1)/2$.

Example 2.15 Let g be the golden ratio and ζ_3 be third root of unity. By some simple calculations it can be prove that

$$\zeta_3=\frac{1}{4}(g+\zeta_3)+\frac{1}{4}(g+\zeta_3)^3+\frac{1}{2}.$$

So, $\zeta_3\in Q(g+\zeta_3)$.

Example 2.16 Let ζ_8 be primitive eighth root of unity. Factorize x^4+1 in $\mathbb{Q}(\zeta_8)$.

$$\zeta_8^{\,8}=1\Rightarrow(\zeta_8^{\,4})^2=1\Rightarrow\zeta_8^{\,4}=1\text{ or }\zeta_8^{\,4}=-1.$$

Since ζ_8 is primitive eight root of unity, $\zeta_8^{\,4}=-1$. So,

$$\begin{aligned}
\zeta_8+\zeta_8^{\,3}+\zeta_8^{\,5}+\zeta_8^{\,7}&=0,\\
\zeta_8^{\,2}+\zeta_8^{\,6}&=0,\\
\zeta_8\zeta_8^{\,3}+\zeta_8\zeta_8^{\,5}+\zeta_8\zeta_8^{\,7}+\zeta_8^{\,3}\zeta_8^{\,5}+\zeta_8^{\,3}\zeta_8^{\,7}+\zeta_8^{\,5}\zeta_8^{\,7}&=0,\\
\zeta_8\zeta_8^{\,3}\zeta_8^{\,5}+\zeta_8\zeta_8^{\,3}\zeta_8^{\,7}+\zeta_8\zeta_8^{\,5}\zeta_8^{\,7}+\zeta_8^{\,3}\zeta_8^{\,5}\zeta_8^{\,7}&=0\text{ and}\\
\zeta_8\zeta_8^{\,3}\zeta_8^{\,5}\zeta_8^{\,7}&=1.
\end{aligned}$$

Thus,

$$\begin{aligned}
x^4+1=\;&x^4-(\zeta_8+\zeta_8^{\,3}+\zeta_8^{\,5}+\zeta_8^{\,7})x^3\\
&+(\zeta_8\zeta_8^{\,3}+\zeta_8\zeta_8^{\,5}+\zeta_8\zeta_8^{\,7}+\zeta_8^{\,3}\zeta_8^{\,5}+\zeta_8^{\,3}\zeta_8^{\,7}+\zeta_8^{\,5}\zeta_8^{\,7})x^2\\
&-(\zeta_8\zeta_8^{\,3}\zeta_8^{\,5}+\zeta_8\zeta_8^{\,3}\zeta_8^{\,7}+\zeta_8\zeta_8^{\,5}\zeta_8^{\,7}+\zeta_8^{\,3}\zeta_8^{\,5}\zeta_8^{\,7})x\\
&+\zeta_8\zeta_8^{\,3}\zeta_8^{\,5}\zeta_8^{\,7}\\
=\;&(x-\zeta_8)(x-\zeta_8^{\,3})(x-\zeta_8^{\,5})(x-\zeta_8^{\,7}).
\end{aligned}$$

Definition 2.17 (Embeddings) Let F be a number field. Any one to one ring homomorphism (ring monomorphism) of θ from F to $\mathbb{C}$ is called an embedding of F in C. Let F be extension of $\mathbb{Q}$ and θ be an embedding of F in $\mathbb{C}$ such that $\theta(l)=l$ for all $l\in\mathbb{Q}$ (fixes $\mathbb{Q}$ point wise), then θ is called a $\mathbb{Q}$-isomorphism of F. Let θ be $\mathbb{Q}$-isomorphism and $F=\mathbb{Q}(\alpha)$, then $\theta(\alpha)$ is called conjugate of α over $\mathbb{Q}$.

For example, if $F=\mathbb{Q}(\sqrt{D})$, D is square free integer (quadratic extension), then conjugate of $a+b\sqrt{D}$ is $a-b\sqrt{D}$ which is some times called algebraic conjugate of $a+b\sqrt{D}$.

Properties 2.18 Any embedding θ of a number field F in $\mathbb{C}$ is a $\mathbb{Q}$-isomorphism of F.

Proof. Let $q=\frac{a}{b}\in\mathbb{Q}$ with $a,b\in\mathbb{Z}$. Since θ is ring monomorphism

$$b\theta(q)=\theta(bq)=\theta(a)=a.$$

So,

$$\theta(q) = q$$

Which means θ is a $\mathbb{Q}$-isomorphism of F.

Theorem 2.19 (The Number of Embeddings of a Number Field) Let $F = \mathbb{Q}(\alpha)$ be an algebraic number field of degree d over $\mathbb{Q}$. Then, there are exactly d embeddings $\theta_1, \theta_2, ..., \theta_d$ of F in $\mathbb{C}$. Moreover, all conjugates of α over $\mathbb{Q}$ are $\theta_1(\alpha) = \alpha_1, \theta_2(\alpha) = \alpha_2, ..., \theta_d(\alpha) = \alpha_d$ with $\alpha_1 = \alpha$ and these are roots of minimal polynomial $m_{\alpha,Q}(x)$ of α over $\mathbb{Q}$.

Proof. Assume that θ is an embedding of F in $\mathbb{C}$ with $\theta(\alpha) = \beta$. Since

$$0 = m_{\alpha,Q}(\alpha) = \sum_{i=0}^{d-1} q_i \alpha^i \text{ with } q_i \in \mathbb{Q},$$

which implies

$$0 = \theta(0) = \theta(\sum_{i=0}^{d-1} q_i \alpha^i) = \sum_{i=0}^{d-1} q_i \theta(\alpha)^i = \sum_{i=0}^{d-1} q_i \beta^i .$$

Therefore, $\beta = \alpha_j$ for some $j \in \{1,2,...,d\}$, implying there are at most d embeddings of F in $\mathbb{C}$. Let θ_j be defined by $\theta_j(f(\alpha)) = f(\alpha_j)$ for some $j \in \{1,2,...,d\}$ where $f(x) \in F[x]$. We have to prove that θ_j is also an embedding of F in $\mathbb{C}$ .For this reason we are going to show that θ_j is well-defined. Let $f(x), g(x) \in F[x]$ such that $f(\alpha) = g(\alpha)$, then there exists $h(x) \in F[x]$ such that $f(x) - g(x) = h(x) m_{\alpha,\mathbb{Q}}(x)$. Therefore,

$$f(\alpha_j) - g(\alpha_j) = h(\alpha_j) m_{\alpha,\mathbb{Q}}(\alpha_j) = 0.$$

Hence,

$$\theta_j(f(\alpha)) = f(\alpha_j) = g(\alpha_j) = \theta_j(g(\alpha)).$$

So, θ_j is well-defined and conjugates of α are α_j's, which are roots of $m_{\alpha,\mathbb{Q}}(x)$.

Example 2.20 Let $F = \mathbb{Q}(\sqrt{5})$. There are 2 embeddings of F in $\mathbb{C}$ which are

$$\theta_1 : \sqrt{5} \to \sqrt{5}$$

and

$$\theta_2 : \sqrt{5} \to -\sqrt{5} .$$

Example 2.21 Let $F = \mathbb{Q}(\sqrt{-5})$. There are 2 embeddings of F in $\mathbb{C}$ which are

$$\theta_1 : \sqrt{-5} \to \sqrt{-5}$$

and

$$\theta_2 : \sqrt{-5} \to -\sqrt{-5} .$$

Example 2.22 Let $F=\mathbb{Q}(\sqrt[3]{5})$. There are 3 embeddings of F in $\mathbb{C}$ which are

$$\theta_1 : \sqrt[3]{5} \to \sqrt[3]{5},$$

$$\theta_2 : \sqrt[3]{5} \to \zeta_3 \sqrt[3]{5}$$

and

$$\theta_3 : \sqrt[3]{5} \to \zeta_3^2 \sqrt[3]{5}$$

where ζ_3 is the third primitive root of unity.

2.2 Norms and Traces

Here are some concepts which take important place in the development of factorization. They are discriminants norms and traces.

Definition 2.23 Let F be an algebraic number field of degree d over $\mathbb{Q}$ and θ_j for $j \in \{1,2,...,d\}$ be the embeddings of F in $\mathbb{C}$. For each element $\alpha \in F$ the product

$$\prod_{j=1}^{d} \theta_j(\alpha)$$

is called norm of α from F, denoted by $N_F(\alpha)$.

Example 2.24 Let $F=\mathbb{Q}(\sqrt{7})$ and $\alpha = \frac{1}{2}(11+3\sqrt{7})$. The embeddings of F in $\mathbb{C}$ are

$$\theta_1 : \sqrt{7} \to \sqrt{7}$$

and

$$\theta_2 : \sqrt{7} \to -\sqrt{7}.$$

So,

$$N_F(\alpha) = \theta_1(\alpha)\theta_2(\alpha) = \frac{1}{2}(11+3\sqrt{7})\frac{1}{2}(11-3\sqrt{7}) = \frac{29}{2}.$$

Definition 2.25 Let F be an algebraic number field of degree d over $\mathbb{Q}$ and θ_j for $j \in \{1,2,...,d\}$ be the embeddings of F in $\mathbb{C}$. For each element $\alpha \in F$ the sum

$$\sum_{j=1}^{d} \theta_j(\alpha)$$

is called trace of α from F, denoted by $T_F(\alpha)$.

Example 2.26 Let $F=\mathbb{Q}(\sqrt{-3})$ and $\alpha = \frac{1}{2}(1+\sqrt{-3})$. The embeddings of F in $\mathbb{C}$ are

$$\theta_1 : \sqrt{-3} \to \sqrt{-3}$$

and

$$\theta_2 : \sqrt{-3} \to -\sqrt{-3}\,.$$

So,

$$N_F(\alpha) = \theta_1(\alpha)\theta_2(\alpha) = \frac{1}{2}(1+\sqrt{-3})\frac{1}{2}(1-\sqrt{-3}) = 1$$

and

$$T_F(\alpha) = \theta_1(\alpha) + \theta_2(\alpha) = \frac{1}{2}(1+\sqrt{-3}) + \frac{1}{2}(1-\sqrt{-3}) = 1\,.$$

Note that, if $F = \mathbb{Q}(\sqrt{D})$ where D is a square free integer and $\alpha = a + b\sqrt{D}$ with $a,b \in \mathbb{Q}$, then

$$N_F(\alpha) = a^2 - b^2 D$$

and

$$T_F(\alpha) = 2a\,.$$

Moreover, $\alpha = a + b\sqrt{D} \Rightarrow \alpha - a = b\sqrt{D}$

$$\Rightarrow (\alpha - a)^2 = b^2 D$$
$$\Rightarrow \alpha^2 - 2a\alpha + a^2 - b^2 D = 0$$
$$\Rightarrow \alpha^2 - T_F(\alpha)\alpha + N_F(\alpha) = 0\,.$$

So the minimal polynomial is

$$m_{\alpha,\mathbb{Q}}(x) = x^2 - T_F(\alpha)x + N_F(\alpha)\,.$$

Proposition 2.27 Let F be an algebraic number field of degree d over $\mathbb{Q}$ and $\alpha, \beta \in F$. Then,

$$N_F(\alpha\beta) = N_F(\alpha)\ N_F(\beta)\,,$$

for any $q \in F$

$$N_F(q\alpha) = q^d N_F(\alpha)$$

and for any $a,b \in F$

$$T_F(a\alpha + b\beta) = aT_F(\alpha) + bT_F(\beta)\,.$$

Proof. Let θ_j for $j \in \{1,2,...,d\}$ be the embeddings of F in C. Since each of θ_j for $j \in \{1,2,...,d\}$ is a ring homomorphism;

$$\begin{aligned} N_F(\alpha\beta) &= \prod_{j=1}^{d} \theta_j(\alpha\beta) \\ &= \prod_{j=1}^{d} \theta_j(\alpha)\theta_j(\beta) \\ &= \prod_{j=1}^{d} \theta_j(\alpha) \prod_{j=1}^{d} \theta_j(\beta) \\ &= N_F(\alpha)\ N_F(\beta)\,, \end{aligned}$$

for any $q \in F$

$$N_F(q\alpha)=\prod_{j=1}^{d}\theta_j(q\alpha)$$
$$=\prod_{j=1}^{d}q\theta_j(\alpha)$$
$$=q^d\prod_{j=1}^{d}\theta_j(\alpha)$$
$$=q^d N_F(\alpha)$$

and for any $a,b\in F$

$$T_F(a\alpha+b\beta)=\sum_{j=1}^{d}\theta_j(a\alpha+b\beta)$$
$$=\sum_{j=1}^{d}(a\theta_j(\alpha)+b\theta_j(\beta))$$
$$=a\sum_{j=1}^{d}\theta_j(\alpha)+b\sum_{j=1}^{d}\theta_j(\beta)$$
$$=aT_F(\alpha)+bT_F(\beta).$$

Example 2.28 Let $F=\mathbb{Q}(\sqrt{-1})$. Let us prove that there is no $\alpha\in F$ such that $N_F(\alpha)=3$. Let $\alpha=a+b\sqrt{-1}$ with $a,b\in\mathbb{Q}$. Assume that

$$N_F(\alpha)=3\Rightarrow\ a^2+b^2=3\,,a,b\in\mathbb{Q}. \tag{2.1}$$

By using definition of rational number, last equation can be written as

$$c^2+d^2=3l^2\,,\ c,d,l\in\mathbb{Z}. \tag{2.2}$$

So, $c^2+d^2\equiv 0 \pmod 3$; implying that both $c\equiv 0 \pmod 3$ and $d\equiv 0 \pmod 3$. So, by using this result in (2.2)**,** we get $l\equiv 0 \pmod 3$. Let $c=3c_1$, $d=3d_1$ and $l=3l_1$, $c_1,d_1,l_1\in\mathbb{Z}$ applying them in (2.2) we get $c_1^{\,2}+d_1^{\,2}=3l_1^{\,2}$. By the above manner c_1,d_1,l_1 are all divisible by 3, which means c,d,l are all divisible by 9. By induction it can be concluded that c,d,l are all divisible by 3^n for every natural number *n*. So, c,d,l are all 0.But *l*=0 contradicts with (2.1). Thus, there is no $\alpha\in F$ such that $N_F(\alpha)=3$.

Proposition 2.29 Let *p* be a prime number and ζ_p be a primitive *p*'th root of unity and let $F=\mathbb{Q}(\zeta_p)$. Then,

$$T_F(\zeta_p)=-1\ \text{ and }N_F(1-\zeta_p)=p\,.$$

Proof. By Proposition 2.13, we know that

$$m_{\zeta_p,\mathbb{Q}}(x)=x^{p-1}+x^{p-2}+\ldots+x+1=\prod_{j=1}^{p-1}(x-\zeta_p{}^{j})\,. \tag{2.3}$$

So,

$$\zeta_p{}^{p-1}+\zeta_p{}^{p-2}+\ldots+\zeta_p+1=0\,.$$

Therefore,

$$T_F(\zeta_p) = \sum_{j=1}^{p-1} \zeta_p{}^j = -1 .$$

And also by letting $x = 1$ in (2.3) we get,

$$N_F(1-\zeta_p) = \prod_{j=1}^{p-1}(1-\zeta_p{}^j) = p .$$

Proposition 2.30 Let *p* is a prime number and ζ_p be a primitive *p*'th root of unity and let $F = \mathbb{Q}(\zeta_p)$. Then, for every natural number *n* which is relatively prime to *p*

$$T_F(1-\zeta_p{}^n) = p .$$

Proof. $\{1,2,3,...,p-1\}$ is a reduced residue system of mod p. Since *n* and *p* are relatively prime $\{n,2n,3n,...,(p-1)n\}$ is also a reduced residue system of mod *p*. So, for every $r \in \{1,2,3,...,p-1\}$ there exists $j \in \{1,2,3,...,p-1\}$ such that $\zeta_p{}^{rn} = \zeta_p{}^j$ and for every $r_1, r_2 \in \{1,2,3,...,p-1\}$ if $r_1 \neq r_2$ then $\zeta_p{}^{r_1 n} \neq \zeta_p{}^{r_2 n}$. Thus,

$$T_F(1-\zeta_p{}^n) = \sum_{j=1}^{p-1}(1-\zeta_p{}^{jn}) = \sum_{j=1}^{p-1}1 - \sum_{j=1}^{p-1}\zeta_p{}^{jn} = p-1-\sum_{j=1}^{p-1}\zeta_p{}^j = p-1-(-1) = p .$$

2.3 Discriminants, Algebraic Integers and Integral Bases

Definition 2.31 Let *R* be a commutative ring and *A* be sub ring of *R*. Let $x \in R$ be a root of monic polynomial *f* with coefficients in *A*, *x* is said to be integral over *A*. The equation *f* (*x*)=0 is said to be equation of integral dependence of *x* over *A*. If *x* is complex number that is integral over $\mathbb{Z}$, then *x* is called an algebraic integer.

The subfields of all algebraic numbers in $\mathbb{C}$ is denoted by $\overline{\mathbb{Q}}$ and all algebraic integers in $\overline{\mathbb{Q}}$ is denoted by $\overline{A}$.

Definition 2.32 Let *F* be an algebraic number field. The intersection $F \cap \overline{A}$ is a ring which is called the ring of integers in *F*, denoted by $\mathfrak{A}_F$.

So, in any algebraic extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$, the ring of integers of $\mathbb{Q}(\alpha)$ is the set of elements of $\mathbb{Q}(\alpha)$ whose minimal polynomials are in $\mathbb{Z}[x]$.

The ring of integers of $\mathbb{Q}$ is $\mathfrak{A}_{\mathbb{Q}} = \mathbb{Z}$.

Let $F = \mathbb{Q}(\sqrt{D})$ where *D* is a square free integer. Then,

$$\mathfrak{A}_F = \begin{cases} \mathbb{Z}[\frac{1+\sqrt{D}}{2}] \ \textit{if}\ D \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{D}] \ \textit{if}\ D \equiv 2 \ \textit{or}\ 3 \pmod 4 \end{cases} \quad [16].$$

Example 2.33 Let $F = \mathbb{Q}(\sqrt{7})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{7}]$.

If $F = \mathbb{Q}(\sqrt{13})$, then $\mathfrak{A}_F = \mathbb{Z}[\frac{1+\sqrt{13}}{2}]$.

Definition 2.34 Let F be an algebraic number field and $\mathfrak{A}_F$ be the ring of integers of F. A basis for $\mathfrak{A}_F$ over $\mathbb{Z}$ is called an integral basis for F.

Example 2.35 Let $F=\mathbb{Q}(\sqrt{7})$, then $\mathfrak{A}_F=\mathbb{Z}[\sqrt{7}]$ and an integral basis is $\left\{1,\sqrt{7}\right\}$. If $F=\mathbb{Q}(\sqrt{13})$, then $\mathfrak{A}_F=\mathbb{Z}[\frac{1+\sqrt{13}}{2}]$ and an integral basis $\left\{1,\frac{1+\sqrt{13}}{2}\right\}$.

Definition 2.36 Let $F=\mathbb{Q}(\alpha)$ be an algebraic number field with $\left|F:\mathbb{Q}\right|=d$, $B=\{\alpha_1,\alpha_2,...,\alpha_d\}$ be a basis for F and $\theta_1,\theta_2,\ldots,\theta_d$ be all embeddings of F in $\mathbb{C}$. Then, The square of determinant of the matrix A is called the discriminant of the basis B, where

$$A=\begin{pmatrix}\theta_1(\alpha_1)\ldots\theta_d(\alpha_1)\\ \vdots\quad\ddots\quad\vdots\\ \theta_1(\alpha_d)\cdots\theta_d(\alpha_d)\end{pmatrix}$$

denoted by disc(B). So, disc(B) = $\det(\theta_j(\alpha_i))^2$, where $\det(\theta_j(\alpha_i))^2$ is the square of determinant of the matrix with entry $\theta_j(\alpha_i)$ in i'th row and j'th column. If $B=\{1,\alpha,\alpha^2,...,\alpha^{d-1}\}$ then we have $\text{disc}(B)=\det(\theta_j(\alpha^{i-1}))^2$. Here, $\det(\theta_j(\alpha^{i-1}))$ is called Vandermonde determinant and has value $\prod_{1\le i<j\le d}(\alpha_i-\alpha_j)$ and so, in this case

$$\text{disc}(B)=\prod_{1\le i<j\le d}(\alpha_i-\alpha_j)^2.$$

Example 2.37 Let $F=\mathbb{Q}(\sqrt{7})$. The embeddings of F in $\mathbb{C}$ are

$$\theta_1:\sqrt{7}\to\sqrt{7}$$

and

$$\theta_2:\sqrt{7}\to-\sqrt{7}.$$

So,

$$B=\{1,\sqrt{7}\}$$

and

$$\text{disc}(B)=\det\begin{pmatrix}1 & 1\\ \sqrt{7} & -\sqrt{7}\end{pmatrix}^2=28.$$

Example 2.38 $F=\mathbb{Q}(\sqrt{-3})$. The embeddings of F in $\mathbb{C}$ are

$$\theta_1 : \sqrt{-3} \to \sqrt{-3}$$

and

$$\theta_2 : \sqrt{-3} \to -\sqrt{-3}\,.$$

So,

$$B=\{1,\frac{1+\sqrt{-3}}{2}\}$$

and

$$\text{disc}(B)=\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{-3}}{2} & \frac{1-\sqrt{-3}}{2} \end{pmatrix}^2 = -3$$

Definition 2.39 Let F be an algebraic number field and B be an integral basis for F. Then, disc(B) is said to be discriminant of F, denoted by Δ_F .

Example 2.40 Let $F=\mathbb{Q}(\sqrt{23})$. Then $B=\{1,\sqrt{23}\}$ is an integral basis for F. So,

$$\Delta_F=\text{disc}(B)=\det\begin{pmatrix} 1 & 1 \\ \sqrt{23} & -\sqrt{23} \end{pmatrix}^2 = 92.$$

Example 2.41 Let $F=\mathbb{Q}(\sqrt{5})$. Then $B=\{1,\frac{1+\sqrt{5}}{2}\}$ is an integral basis for F. So,

$$\Delta_F=\text{disc}(B)=\det\begin{pmatrix} 1 & 1 \\ \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \end{pmatrix}^2 = 5.$$

Note that if $F=\mathbb{Q}(\sqrt{D})$ where D is a square free integer, then

$$\Delta_F=\begin{cases} D \ \textit{if}\ D\equiv 1 \pmod 4 \\ 4D \ \textit{if}\ D\equiv 2 \textit{or} 3 \pmod 4. \end{cases}$$

See [16].

Proposition 2.42 Discriminant of a totally real number field is positive.

Proof. Let $F=\mathbb{Q}(\alpha)$ be a totally real number field with the degree of extension d. Then an integral basis of F is $\{1,\alpha,\alpha^2,...,\alpha^{d-1}\}$. And so,

$$\Delta_F = \text{disc}(\,B\,) = \prod_{1\le i<j\le d}(\alpha_i-\alpha_j)^2 > 0.$$

Proposition 2.43 Let $F=\mathbb{Q}(\sqrt{D})$ where D is a square free integer. F is norm-Euclidean with Euclidean function $f(\alpha)=N_F(\alpha)$ if and only if whenever any $\sigma\in F$ is given there exists $\beta\in\mathfrak{A}_F$ such that $\left|N_F(\sigma-\beta)\right|<1$.

Proof. Suppose that F is norm-Euclidean with Euclidean function $f(\alpha)=N_F(\alpha)$. Given any $\sigma\in F$, there is $z\in\mathbb{Z}$ such that $z\sigma\in\mathfrak{A}_F$. So, $\sigma=\alpha/\beta$, where $\alpha,\beta\in\mathfrak{A}_F$. Since F is norm-Euclidean with Euclidean function $f(\alpha)=N_F(\alpha)$, there are $\gamma,\delta\in\mathfrak{A}_F$ such that $\alpha=\beta\gamma+\delta$, where $\delta=0$ or $\left|N_F(\delta)\right|<\left|N_F(\beta)\right|$. Therefore,

$$\left|N_F(\sigma-\beta)\right|=N_F(\delta/\beta)=N_F(\delta)/N_F(\beta)<1.$$

Conversely, given any $\sigma\in F$ there exists $\beta\in\mathfrak{A}_F$ such that $\left|N_F(\sigma-\beta)\right|<1$. Set $\sigma=\alpha/\beta$, for some $\alpha,\beta\in\mathfrak{A}_F$; then $\left|N_F(\delta)\right|<\left|N_F(\beta)\right|$ where $\delta=\alpha-\gamma\beta$. Thus, F is norm-Euclidean with Euclidean function $f(\alpha)=N_F(\alpha)$.

Definition 2.44 Let $F\subseteq\mathbb{C}$ be a field and $f(x)\in F[x]$ with deg (f) = d > 1 such that

$$f(x)=a\prod_{i=1}^{d}(x-\alpha_i),\ a\in F \text{ and } \alpha_1,\alpha_2,...,\alpha_d\in\mathbb{C}.$$

Then the product $a^{2d-2}\prod_{1\le i<j\le d}(\alpha_i-\alpha_j)^2$ is called discriminant of f, denoted by disc(f).

Note that if $F=\mathbb{Q}(\alpha)$ and B be an integral basis for f, then disc ($m_{\alpha,\mathbb{Q}}$) = disc (B) see [2].

Example 2.45 Let $\alpha=\zeta_3$ be primitive third root of unity. Consider $F=\mathbb{Q}(\zeta_3)$. One can check that $m_{\alpha,\mathbb{Q}}(x)=x^2+x+1=(x-\zeta_3)(x-\zeta_3^{\,2})$. So,

$$\text{disc}\,(m_{\alpha,\mathbb{Q}})=\prod_{1\le i<j\le 2}(\zeta_3^{\,i}-\zeta_3^{\,j})^2=(\zeta_3-\zeta_3^{\,2})^2=\zeta_3^{\,2}-2+\zeta_3. \qquad (2.4)$$

Since $\zeta_3^{\,2}+\zeta_3+1=0$, we have $\zeta_3^{\,2}+\zeta_3=-1$. If we put this value in (2.4), then we get

$$\text{disc}\,(m_{\alpha,\mathbb{Q}})=-3.$$

In generally, if $F=\mathbb{Q}(\zeta_p)$ where $\alpha=\zeta_p$ be primitive p'th root of unity for odd prime p. Then,

$$m_{\alpha,\mathbb{Q}}(x)=\sum_{i=0}^{p-1}x^i=\prod_{i=1}^{p-1}(x-\zeta_p^{\,i}),$$

and

$$\text{disc}\,(m_{\alpha,\mathbb{Q}})=\prod_{1\le i<j\le p-1}(\zeta_p^{\,i}-\zeta_p^{\,j})^2=(-1)^{(p-1)/2}p^{p-2}\quad [2].$$

Theorem 2.46 Let $F=\mathbb{Q}(\alpha)$ be an algebraic number field of degree *d* over $\mathbb{Q}$ and $\alpha_1,\alpha_2,...,\alpha_d$ be conjugates of α over $\mathbb{Q}$. Then,

$$\text{disc}\,(m_{\alpha,\mathbb{Q}}) = (-1)^{\binom{d}{2}}\prod_{i=1}^{d} m'_{\alpha,\mathbb{Q}}(\alpha_i) = (-1)^{\binom{d}{2}} N_F(m'_{\alpha,\mathbb{Q}}(\alpha)),$$

where $m'_{\alpha,\mathbb{Q}}$ is derivative of $m_{\alpha,\mathbb{Q}}$.

Proof. $m_{\alpha,\mathbb{Q}}(x)=\prod_{i=1}^{d}(x-\alpha_i)$. So, $m'_{\alpha,\mathbb{Q}}(x)=\sum_{k=1}^{d}\prod_{\substack{i=1\\ i\neq k}}^{d}(x-\alpha_i)$.

Therefore,

$$m'_{\alpha,\mathbb{Q}}(\alpha_k)=\prod_{\substack{i=1\\ i\neq k}}^{d}(\alpha_k-\alpha_i),$$

for all k = 1,2,3,…,*d*. So,

$$N_F(m'_{\alpha,\mathbb{Q}}(\alpha))=\prod_{i=1}^{d} m'_{\alpha,\mathbb{Q}}(\alpha_i)=\prod_{1\le i<k\le d}(\alpha_i-\alpha_k)\prod_{1\le i<k\le d}(\alpha_i-\alpha_k),$$

Since there are $\binom{d}{2}$ pairs of (*i*,*k*) with $1\le i<k\le d$, we have

$$N_F(m'_{\alpha,\mathbb{Q}}(\alpha))=(-1)^{\binom{d}{2}}\prod_{1\le i<k\le d}(\alpha_i-\alpha_k)^2.$$

On the other hand, by definition 2.44 we have,

$$\text{disc}\,(m_{\alpha,\mathbb{Q}})=\prod_{1\le i<k\le d}(\alpha_i-\alpha_k)^2.$$

Thus. combining last two results, one gets

$$\text{disc}\,(m_{\alpha,\mathbb{Q}}) = (-1)^{\binom{d}{2}}\prod_{i=1}^{d} m'_{\alpha,\mathbb{Q}}(\alpha_i) = (-1)^{\binom{d}{2}} N_F(m'_{\alpha,\mathbb{Q}}(\alpha)).$$

Example 2.47 Let $F=\mathbb{Q}(\sqrt[3]{2})$. There are 3 embeddings of *F* in $\mathbb{C}$ which are

$$\theta_1:\sqrt[3]{2}\to\sqrt[3]{2},$$

$$\theta_2:\sqrt[3]{2}\to\zeta_3\sqrt[3]{2}$$

and

$$\theta_3:\sqrt[3]{2}\to\zeta_3^{\,2}\sqrt[3]{2},$$

where ζ_3 is the primitive third root of unity. On the other hand,

$$m_{\sqrt[3]{2},\mathbb{Q}}(x)=x^3-2 \quad\text{and}\quad m'_{\sqrt[3]{2},\mathbb{Q}}(x)=3x^2.$$

Thus, by Theorem 2.46

$$\text{disc}\,(m_{\sqrt[3]{2},\mathbb{Q}}) = (-1)^{\binom{3}{2}} N_F(m'_{\sqrt[3]{2},\mathbb{Q}}(\sqrt[3]{2})) = -3(\sqrt[3]{2})^2 3(\zeta_3\sqrt[3]{2})^2 3(\zeta_3^{\,2}\sqrt[3]{2})^2 = -108.$$

Corollary 2.48 Let $F=\mathbb{Q}(\alpha)$ be an algebraic number field and $m_{\alpha,\mathbb{Q}}(x)$ be the minimal polynomial α over $\mathbb{Q}$. Then,

$$\text{disc}\,(m_{\alpha,\mathbb{Q}}) = \pm\, N_F(m'_{\alpha,\mathbb{Q}}(\alpha)).$$

Proof. Let deg ($m_{\alpha,\mathbb{Q}}$) = *d*. By Theorem 2.46

$$\text{disc}\,(m_{\alpha,\mathbb{Q}}) = (-1)^{\binom{d}{2}} N_F(m'_{\alpha,\mathbb{Q}}(\alpha)).$$

If $d \equiv 0$ *or* $1 \pmod 4$, then

$$\text{disc}\,(m_{\alpha,\mathbb{Q}}) = + N_F(m'_{\alpha,\mathbb{Q}}(\alpha)).$$

If $d \equiv 2$ *or* $3 \pmod 4$, then

$$\text{disc}\,(m_{\alpha,\mathbb{Q}}) = - N_F(m'_{\alpha,\mathbb{Q}}(\alpha)).$$

Thus,

$$\text{disc}\,(m_{\alpha,\mathbb{Q}}) = \pm N_F(m'_{\alpha,\mathbb{Q}}(\alpha)).$$

Proposition 2.49 Let F be an algebraic number field with $\mathfrak{A}_F = \mathbb{Z}[\alpha]$. Then,

$$\Delta_F = \text{disc}\,(m_{\alpha,\mathbb{Q}}).$$

Proof. Let degree of extension of F over $\mathbb{Q}$ be d. Since $\mathfrak{A}_F = \mathbb{Z}[\alpha]$, $B = \{1, \alpha, \alpha^2, ..., \alpha^{d-1}\}$ be integral basis for F. So,

$$\text{disc}\,(B) = \text{disc}\,(m_{\alpha,\mathbb{Q}}).$$

Thus,

$$\Delta_F = \text{disc}\,(m_{\alpha,\mathbb{Q}}).$$

CHAPTER 3

THEORY OF DOMAINS

If R is a commutative ring with unity and without zero-divisor, then such a ring is called a *domain*. Throughout the study, R will denote a domain unless the converse is stated. $U(R)$ will denote unit group. Prior to talk about a factorization in a domain, first of all, we need several concepts. Now let us define them.

Definition 3.1 Let a and b be non-zero elements of the domain R. We say that a *divides* b and denoted by $a \mid b$ if there exists an element c in R such that $b = a\,c$.

Proposition 3.2 Let $u \in R$. $u \in U(R)$ if and only if $u \mid 1$**.**

Prof. Let $u \in U(\mathrm{R})$ then $\exists\ v \in R$ such that $u.v=1$ so $u \mid 1$**.** Conversely, let $u \mid 1$ then by Definition 1.1 we write $1= u.r$ for some $r \in R$, so $u \in U(R)$.

Corollary 3.3 For all $r \in R$, $u \in U(R)$

i)$1 \mid r$,

ii) $u \mid r$ and

iii)in a field F there is no division problem (any non-zero elements divide each other).

Definition 3.4 Let $a, b \in R$. b is said to be *associate of* a if there exists $u \in R$ such that $b = au$.

Proposition 3.5 The relation of being associate in R is an equivalence relation.

(for $r, s \in R$ $r \sim s \Leftrightarrow s = r.u$ for some $u \in U(R)$)

Prof. *i*) For all $r \in \mathrm{R}$, we have $r = r \times 1$. So, $\sim$ is reflexive.

ii) Let $r \sim \mathrm{s}$ in R, then for some $u \in U(R)$ we write

$s = r.u \Rightarrow r = s.u^{-1}$ since $u \in U(R)$. So, $\sim$ is symmetric.

iii) Let $r \sim \mathrm{s}$ and $s \sim t$ in R, then for some $u,v \in U(R)$ we write

$$\left.\begin{array}{l} s = r.u \\ t = s.v \end{array}\right\} \Rightarrow t = (r.u).v = r.(uv), \text{ for } uv \in U(R).$$ So, $\sim$ is transitive.

Consequently, since the relation is equivalence relation, we can say that a and b are associates in R .

Proposition 3.6 a and b are non-zero associates in R if and only if $a \mid b$ and $b \mid a$.

Proof. ($\Rightarrow$)Let a and b be associate in R . Then we write $b = au$ and $a = bv$ for some $u,v \in U(R)$ so $a \mid b$ and $b \mid a$.

($\Leftarrow$) For $a,b \in R$ let $a \mid b$ and $b \mid a$. We have $b = a.s$ and $a = b.t$ for some $s,t \in R$. Then, $b = a.s = (b.t).s = b.(ts) \Rightarrow b.(1-ts)=0$. Since b is non-zero, $st=1$. So, $s,t \in U(R)$. Thus, a and b are associate.

Definition 3.7 A non-zero element a of an integral domain R is called *an irreducible element* if i) $a \notin U(R)$ and ii) $a = bc$ implies either $b \in U(R)$ or $c \in U(R)$, for $b,c \in R$.

Definition 3.8 A non-zero element p of an integral domain R is called a *prime element* if

i) $p \notin U(R)$ and ii) $p \mid bc$ implies either $p \mid b$ or $p \mid c$, for $b,c \in R$.

3.1 Unique Factorization Domain (*UFD*)

Definition 3.9 A domain R is called a Unique Factorization Domain (in short, a *UFD*) if the following two conditions hold :

i) Every nonunit of R is a finite product of irreducible factors.

ii) Every irreducible element is prime

Theorem 3.10 If R is a *UFD,* then the factorization of any element in R as a finite product of irreducible factors is a unique within order and unit factors.

Proof. Assume that R is *UFD*. Let a be an element of R , $p_1 p_2 ... p_n$ and $q_1 q_2 ... q_m$ be two factorizations of a, in which p_i's and q_i's are irreducible. We have to prove that $m = n$ and in one arrangement of q_i's p_i and q_i are associates for every i = 1,2,3,...,n. For this purpose we are going to use induction.

Every thing is obvious if a is irreducible. Assume that it is true if a can be factored into s irreducible factors. That is, if $p_1 p_2 ... p_s$ and $q_1 q_2 ... q_m$ be two factorizations of a, in which p_i's and q_i's are irreducible, then $m = s$ and in one arrangement of q_i's p_i and q_i are associates for every i = 1,2,3,...,s. Now suppose that, a can be factored into s + 1 irreducible factors. Let

$$a = p_1 p_2 ... p_{s+1} = q_1 q_2 ... q_m \qquad (3.1)$$

where p_i's and q_i's are irreducible. We have that p_1 divides the product $q_1 q_2 ... q_m$. Since p_1 prime , p_1 divides q_k for some $k \in \{1,2,3,...,m\}$. But q_k is irreducible so p_1 and q_k are associates. Therefore, $q_k = up_1$ for some unit element of R. After substitution up_1 instead of q_k and cancellation, (3.1) gives

$$p_2 p_3 ... p_{s+1} = u q_1 q_2 ... q_{k-1} q_{k+1} ... q_m \qquad (3.2)$$

Thus, by induction hypothesis, two factorizations in (3.2) can differ only in the order of factors and by unit factors. We know that p_1 and q_k are not unit factors, this completes the proof.

Definition 3.11 An element d in an integral domain R is called *a greatest common divisor* of elements a and b in R if the following two conditions hold:

i) $d|a$ and $d|b$,

ii) if for c in R, $c|a$ and $c|b$ implies $c|d$.

Theorem 3.12 Let R be a *UFD* and $a,b \in R$. Then there exists a greatest common divisor of a and b that is uniquely determined to within an arbitrary unit factor.

Proof. Let $a = p_1^{e_1} p_2^{e_2} ... p_n^{e_n}$ and $b = p_1^{f_1} p_2^{f_2} ... p_n^{f_n}$, where p_i are irreducible, e_i's and f_i's are nonnegative integers; here by p_i^0 we mean a unit. Set $g_i = \min(e_i, f_i)$ for all $i = 1,2,...,n$ and $d = p_1^{g_1} p_2^{g_2} ... p_n^{g_n}$.

Clearly, d divides a and d divides b. Let $c = p_1^{h_1} p_2^{h_2} ... p_n^{h_n}$ where h_i's are nonnegative integers, such that c divides a and c divides b. Obviously, $h_i \le e_i$ and $h_i \le f_i$

for every $i = 1,2,...,n$; implying that $h_i \le g_i$ for every $i = 1,2,...,n$. Then, c divides d as desired.

Now, suppose d and d' are two greatest common divisor. Then, d divides d' and d' divides d.

Since R is commutative integral domain, d and d' are associates which completes the proof.

The uniquely determined greatest common divisor of a and b is denoted by (a, b). (a, b) is a set in which any two elements are associates. That is, if d is one of the greatest common divisor of a and b, then $(a, b) = \{ du : u \in U(R) \}$.

Definition 3.13 In a *UFD,* two elements a and b are called *relatively prime* if $(a, b) = 1$.

Proposition 3.14 Let R be a domain and $a, b, c \in R$. Then the following properties hold:

i) $c(a, b)$ and (ca, cb) are associates

ii) if $(a, b)=1$, $a \mid c$ and $b \mid c$ then $ab \mid c$.

iii) if $(a, b)=1$, $a \mid bc$ then $a \mid c$.

iv) if $(a, b)=1$ and $(a, c)=1$ then $(a, bc)=1$.

v) $(a, b)=1 \Leftrightarrow (a^n, b^n)=1$, for all positive integer n.

Proof.

i) Let $(a, b) = d$ and $(ca, cb) = e$. We want to show that $e = dx$, for some $x \in U(R)$.

$$\begin{aligned} (a,b) = d &\Rightarrow d \mid a \quad \text{and} \quad d \mid b \\ &\Rightarrow cd \mid ca \text{ and } cd \mid cb \\ &\Rightarrow cd \mid (a,b) \\ &\Rightarrow cd \mid e \\ &\Rightarrow e = (cd)x, \ (x \in R) \end{aligned} \tag{3.3}$$

On the other hand,

$$(ca,cb) = e \Rightarrow \left.\begin{matrix} e \mid ca \\ e \mid cb \end{matrix}\right\} \Rightarrow \left.\begin{matrix} ca = eu \\ cb = ev \end{matrix}\right\} \text{ for some } u,v \in R. \tag{3.4}$$

By (3.3) and (3.4) we obtain

$$\begin{aligned} ca = eu &\Rightarrow ca = (cdx)u \\ &\Rightarrow c(a - dxu) = 0 \\ &\Rightarrow a = dxu. \end{aligned} \tag{3.5}$$

$$\begin{aligned} cb = ev &\Rightarrow cb = (cdx)v \\ &\Rightarrow c(b - dxv) = 0 \\ &\Rightarrow b = dxv. \end{aligned} \tag{3.6}$$

If we combine (3.5) and (3.6) we have

$$\begin{aligned} (dx) \mid a \text{ and } (dx) \mid b &\Rightarrow (dx) \mid (a,b) = d \\ &\Rightarrow d = (dx)z, \quad (z \in R) \\ &\Rightarrow d(1 - xy) = 0 \\ &\Rightarrow xy = 1 \\ &\Rightarrow x, y \in U(R). \end{aligned}$$

$$ii)\ \left.\begin{array}{l}(a,b)=1\Rightarrow ax+by=1\\ a|c \quad\Rightarrow\quad c=au\\ b|c \quad\Rightarrow\quad c=bv\end{array}\right\}\ \text{for some } x,y,u,v\in R.$$

That's why we get

$$\begin{aligned}c=c.1&=c(ax)+c(by)\\&=(bv)(ax)+(au)(by)\\&=ab(vx+uy)\\&=ab(vx+uy)\end{aligned}$$

$So,(ab)|c,\quad \text{Since } vx+uy\in R$

$$iii)\ \left.\begin{array}{l}(a,b)=1\Rightarrow ax+by=1\\ a|bc\Rightarrow\ \ bc=az\end{array}\right\}\text{for some } x,y,z\in R.$$

Therefore we have

$$\begin{aligned}c=c.1&=c(ax+by)\\&=(ca)x+(cb)y\\&=a(cx)+(az)y\\&=a(cx+zy)\end{aligned}$$

$So,\ a|c,\quad \text{Since } cx+zy\in R$

$$iv)\ \left.\begin{array}{l}(a,b)=1\Rightarrow ax+by=1\\ (a,c)=1\Rightarrow au+cv=1\end{array}\right\}\text{for some } x,y,u,v\in R. \text{ And so,}$$

$$\begin{aligned}1&=(ax+by)(au+cv)\\&=(ax+by)au+(ax+by)cv\\&=a(ax+by)u+ax(cv)+(bc)(yv)\\&=a\left[(ax+by)u+x(cv)\right]+bc(yv)\end{aligned}$$

$$Thus,\ (a,bc)=1,\quad \text{Since } (ax+by)u+x(cv),yv\in R$$

3.2 Principle Ideal Domain (*PID*)

Definition 3.15 Let R be a domain. R is called Principle Ideal Domain if each ideal of R is generated by a single element in R, i.e. for each ideal $I=(a)=aR$, $(a\in R)$.

Theorem 3.16 An irreducible element in a principle ideal domain is always prime.

Proof. Let R be a *PID* and let $p \in R$ be an irreducible element. Assume that for $a,b \in R$ $p \mid ab$. Suppose p does not divide a, then we will show that $p \mid b$. Since R is a *PID*, there exist $c \in R$ such that

$$pR + aR = cR .$$

So $p \in cR$, which means $p = cd$, for some $d \in R$. But because of irreducibility of p, there are two cases, either $c \in U(R)$ or $d \in U(R)$.

Claim : Suppose $d \in U(R)$. Then we have $pR = cR$ which implies

$$pR + cR = pR.$$

This means that $a \in pR$, which contradicts the assumption p does not divide a. Hence, $c \in U(R)$. That's why, $cR = R$ which implies $pR + aR = R$. Then there exist $x, y \in R$ such that

$$px + ay = 1 \Rightarrow (px)b + (ab)y = b \Rightarrow p(bx) + (pz) = b, \quad (p \mid ab \Rightarrow ab = pz, \ p \in R) .$$

Therefore $p \mid b$.

Theorem 3.17 Every *PID* is a *UFD*.

Proof. First of all, let us show the following claim

Claim 1) If R is a principle ideal ring, then R can not have any infinite properly ascending chain of ideals in R.

Let $A = \bigcup a_i R$ and $a, b \in A$, $r \in R$. Then we can write $a \in a_i R$, $b \in a_j R$ for some natural numbers i, j. Since either $a_i R \subset a_j R$ or $a_j R \subset a_i R$, a, b must be contained one of these two ideals. Let us say $a, b \in a_i R$. So we have

$$a - b, \ ar \in a_i R \subset A .$$

Hence, A is an ideal in R. Since R is a principle ideal domain, $A = aR$ for some $a \in R$. Thus, $a \in A \Rightarrow a \in a_k R$ for some natural number k. For this reason,

$$A = aR \subset a_k R \subset A \Rightarrow aR = a_k R \Rightarrow a_k R = a_{k+1} R = a_{k+2} R = ...$$

Consequently, this proves that a principle ideal ring can not have any infinite properly ascending chain of ideals.

Claim 2) each element $a \in R$ can be written as a finite product of irreducible elements.

If a is irreducible, then we are done. If not, we write $a = bc$, where $a, b \notin U(R)$. If b, c are irreducible, then we are done. If not, one of them (say b) can be written as a product of two non-unit elements. That is, $b = xy$, where $x, y \notin U(R)$. If x, y are irreducible, then we are done. If not, one of them (say x)

can be written as a product of two non-unit elements. This process leads to properly ascending chain ideals

$$(a) = (b) = (x) = \ldots$$

that will continue infinitely if a is not a finite product of irreducible elements. Yet, in Claim1 we have shown that R has such property. That's why, a must be written as a finite product of irreducible elements.

By Theorem 3.16, since every irreducible element in a *PID* is prime, any *PID* is a *UFD*.

3.3 Euclidean Domain (*EUD*)

Definition 3.18 A domain E is called a Euclidean domain if there exists a function $\phi : E \to Z$ satisfying the following axioms:

i) If $a, b \in E^* = E - \{0\}$ and $b \mid a$, then $\phi(b) \le \phi(a)$

ii) for each pair of elements $a, b \in E, b \neq 0, \ \exists \ q, r \in E$ such that $a = bq + r$ then

$\phi(\mathrm{r}) < \phi(\mathrm{b})$.

Some well-known Euclidean domains are ring of integers and polynomial rings over a field. If we define $\phi(n) = |n| \ (n \in \mathbb{Z})$, $\mathbb{Z}$ becomes Euclidean domain. Similarly, If we define $\phi : F[x] \to \mathbb{Z}$ as $\phi(f) =$ degree of f, (for non-zero $f \in F[x]$) and $\phi(0) = -1$, then $F[x]$ turns out Euclidean domain. Now, let us give less-known two Euclidean domains.

Proposition 3.19 Gaussian Integers ($\mathbb{Z}[i] = \{\alpha = a + bi : a, b \in \mathbb{Z}\}$) is a Euclidean domain.

Proof. Let us define a function from Gaussian Integers to $\mathbb{Z}$ as follows

$$\begin{aligned} \phi : \mathbb{Z}[i] &\longrightarrow \mathbb{Z} \\ a + bi &\to a^2 + b^2 \end{aligned}$$

First of all, let us observe ϕ is multiplicative. For any $\alpha = a + bi, \beta = c + di \in \mathbb{Z}[i]$

$$\begin{aligned} \phi(\alpha\beta) = \phi((a + bi)(c + di)) &= \phi((ac - bd) + (ad + bc)i) \\ &= (ac - bd)^2 + (ad + bc)^2 \\ &= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 \\ &= a^2(c^2 + d)^2 + b^2(c^2 + d^2) \\ &= \phi(a + bi)\phi(c + di) \end{aligned}$$

$$= \phi(\alpha)\phi(\beta)\,. \qquad (3.7)$$

There are two cases for non-zero $\alpha, \beta \in \mathbb{Z}[i]$, either $\beta|\alpha.$ or β doesn't divide α.

i)Let us assume that for non zero $\alpha, \beta \in \mathbb{Z}$, $\beta|\alpha.$ Then we write
$\alpha = \beta\gamma$, for some $\gamma \in \mathbb{Z}[i]$

$$\begin{aligned}\phi(\alpha) &= \phi(\beta\gamma)\\ &= \phi(\beta)\phi(\gamma), \quad \text{(by (3.7))}\\ &\geq \phi(\beta).1\\ So, (\beta) &\leq \phi(\alpha),\end{aligned}$$

ii) Now let us assume β does not divide α. Then $\frac{\alpha}{\beta} \in \mathbb{Q}(i)$ not in $\mathbb{Z}[i]$.

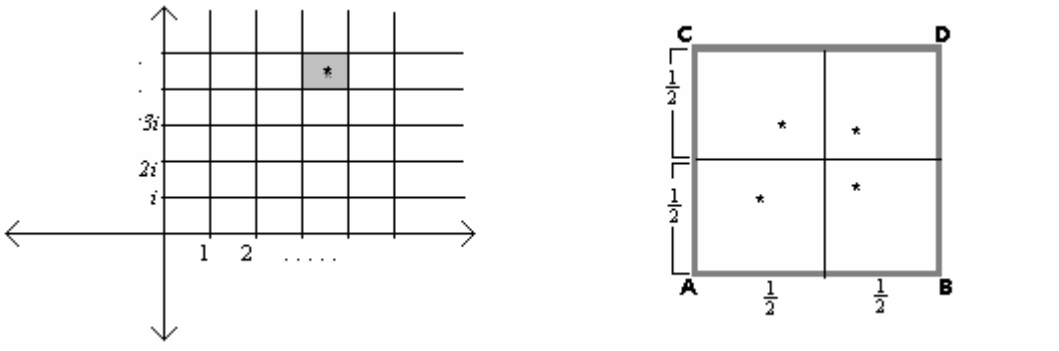

Figure 3.1 Illustrated lattice diagram for $\mathbb{Z}[i]$

If we choose the shortest corner $m+ni \in \mathbb{Z}[i]$, then

$$\frac{\alpha}{\beta} = (m+ni)+(p+qi), \text{ where } p,q \in \mathbb{Q}\text{, such that } |p|,|q| \leq \frac{1}{2}.$$

Thus if we choose $(m+ni)$ as a quotient then the remainder is $\rho = \alpha - (m+ni)\beta$.
Now, let us check the value of ρ.

$$\begin{aligned}\phi(\rho) &= \phi(\alpha - (m+ni)\beta)\\ &= \phi((p+qi)\beta)\\ &= \phi(\beta)\phi(p+qi)\\ &= \phi(\beta)(p^2+q^2)\\ &\leq \phi(\beta)\tfrac{1}{2}\\ &< \phi(\beta).\end{aligned}$$

Proposition 3.20 $\mathbb{Z}[\sqrt{2}]=\left\{\alpha=a+b\sqrt{2}:a,b\in\mathbb{Z}\right\}$ is a Euclidean domain.

Proof. Let us define a function from $\mathbb{Z}[\sqrt{2}]=\left\{\alpha=a+b\sqrt{2}:a,b\in\mathbb{Z}\right\}$ to $\mathbb{Z}$ as follows

$$\begin{aligned}\phi:\mathbb{Z}[\sqrt{2}]&\longrightarrow\mathbb{Z}\\ a+b\sqrt{2}&\rightarrow\left|a^2-2b^2\right|\end{aligned}$$

First of all, let us observe ϕ is multiplicative, too . For any $\alpha=a+b\sqrt{2},\beta=c+d\sqrt{2}\in\mathbb{Z}[\sqrt{2}]$

$$\begin{aligned}\phi(\alpha\beta)=\phi((a+b\sqrt{2})(c+d\sqrt{2}))&=\phi((ac+2bd)+(ad+bc)\sqrt{2})\\ &=\left|(ac+2bd)^2-2(ad+bc)^2\right|\\ &=\left|(ac)^2+4(bd)^2-2(ad)^2-2(bc)^2\right|\\ &=\left|a^2(c^2-2d^2)+2(2d^2-c^2)\right|\\ &=\left|a^2-2b^2\right\|c^2-2d^2\left|\right.\\ &=\phi(a+b\sqrt{2})\phi(c+d\sqrt{2})\\ &=\phi(\alpha)\phi(\beta).\end{aligned}\qquad(3.8)$$

There are two cases for non-zero $\alpha,\beta\in\mathbb{Z}\left[\sqrt{2}\right]$, either $\beta|\alpha.$ or β does not divide α.

i)Let us assume that for non zero $\alpha,\beta\in\mathrm{Z}$, $\beta|\alpha.$ Then we write

$\alpha=\beta\gamma,$ for some $\gamma\in\mathbb{Z}\left[\sqrt{2}\right]$

$$\begin{aligned}\phi(\alpha)&=\phi(\beta\gamma)\\ &=\phi(\beta)\phi(\gamma),\quad\text{(by (3.8))}\\ &\geq\phi(\beta).1\\ So,\phi(\beta)&\leq\phi(\alpha),\end{aligned}$$

ii) Now let us assume β does not divide α. Then $\frac{\alpha}{\beta}\in\mathbb{Q}(\sqrt{2})$ not in $\mathbb{Z}\left[\sqrt{2}\right]$.

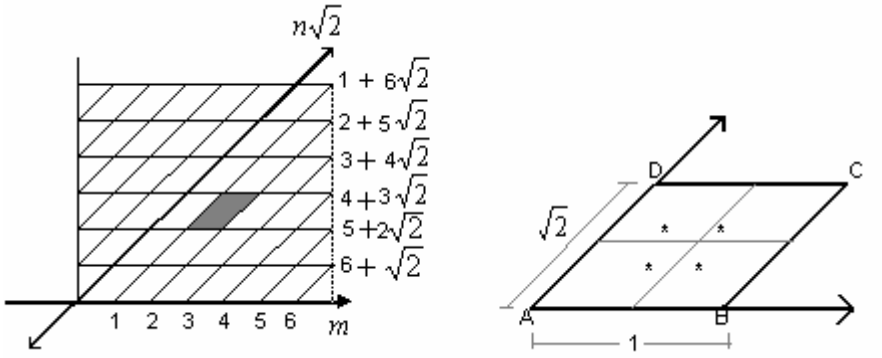

Figure 3.2 Illustrated lattice diagram for $\mathbb{Z}\left[\sqrt{2}\right]$

If we choose the shortest corner $(m+n\sqrt{2}) \in \mathbb{Z}\left[\sqrt{2}\right]$, then

$$\frac{\alpha}{\beta} = (m+n\sqrt{2}) + (p+q\sqrt{2}), \text{ where } p,q \in \mathbb{Q}, \text{ such that } |p|,\ |q| \le \frac{1}{2}.$$

Thus if we choose $(m+n\sqrt{2})$ as a quotient then the remainder is $\rho = \alpha - (m+n\sqrt{2})\beta$. Now, let us check the value of ρ.

$$\begin{aligned}
\phi(\rho) &= \phi(\alpha - (m+n\sqrt{2})\beta) \\
&= \phi((p+q\sqrt{2})\beta) \\
&= \phi(\beta)\phi(p+q\sqrt{2}) \\
&= \phi(\beta)\left|p^2 - 2q^2\right| \\
&\le \phi(\beta)(p^2 + 2q^2) \\
&\le \phi(\beta).\tfrac{3}{4} \\
So, \phi(\rho) &< \phi(\beta)
\end{aligned}$$

Theorem 3.21 Every Euclidean domain is a *PID*.

Proof. Let R be a Euclidean domain and I be its non-zero ideal. Since for all $a \in I, \phi(1) \le \phi(a)$, Then we have

$$\phi(1) \le \{\phi(a) : 0 \ne a \in I\} \subseteq \mathbb{Z}.$$

Because of the principle of well-ordering of $\mathbb{Z}$, there exists $c \in I$ such that the smallest of this set is $\phi(c)$. That is

$$\phi(c) \le \phi(a),\ \forall a \in I - \{0\} \tag{3.9}$$

Claim : $I = (c)$ Since R is a Euclidean domain, if $a \in I \Rightarrow a = cq + r$, for some $q, r \in R$. If we assume that $r \ne 0$ then we say $\phi(r) < \phi(c)$. On the other hand, since $r = a - cq \in I$,

by (3.9) we get $\phi(c) \le \phi(r) < \phi(c)$ a contradiction. So, $r = 0$. Thus, $I = (c)$.

Proposition 3.22 Let $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ where D is a square free integer. If $a^2 - b^2 D = \pm 1$, then α is unit in $\mathbb{Z}[\sqrt{D}]$.

Proof. $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ implies $\alpha' = a - b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$. Since

$$a^2 - b^2 D = \alpha\alpha' \pm 1$$

α' is an inverse of α in $\mathbb{Z}[\sqrt{D}]$. So, α is unit in $\mathbb{Z}[\sqrt{D}]$.

Proposition 3.23 Let $\alpha = a + b\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ where D is a square free integer. If $\left|a^2 - b^2 D\right|$ is prime, then α is irreducible in $\mathbb{Z}[\sqrt{D}]$.

Proof. Assume that $\alpha = \beta_1\beta_2$ for some $\beta_1, \beta_2 \in \mathbb{Z}[\sqrt{D}]$. Then,

$$\left|N(\alpha)\right| = \left|N(\beta_1)\right|\left|N(\beta_2)\right| = p,$$

where p is prime. So, either $\left|N(\beta_1)\right|$ or $\left|N(\beta_2)\right|$ is 1. Thus, by proposition 3.20, either β_1 or β_2 is unit in $\mathbb{Z}[\sqrt{D}]$, implying that α is irreducible in $\mathbb{Z}[\sqrt{D}]$.

Proposition 3.24 Let $\alpha = a + bi \in \mathbb{Z}[i]$. $a^2 + b^2$ is prime in $\mathbb{Z}$ if and only if α is prime in $\mathbb{Z}[i]$.

Proof. If $a^2 + b^2$ is prime in $\mathbb{Z}$, by Proposition 3.23 α is irreducible in $\mathbb{Z}[i]$. On the other hand, by Proposition 3.19 $\mathbb{Z}[i]$ is a *EUD* and by Theorem 3.21 it is *PID*. So, by Theorem 3.16 α is prime in $\mathbb{Z}[i]$.

Conversely assume that α is prime in $\mathbb{Z}[i]$, it follows immediately that *gcd*(*a*,*b*) = 1. Let $a^2 + b^2 = pn$ where p is prime and $n \in \mathbb{N}$. So, p divides neither a nor b. But then, either $a + bi$ or $a - bi$ divides p; since otherwise $a^2 + b^2$ divides n which means $p(n/(a^2 + b^2) = 1$, a contradiction. Without loss of generality suppose that $a + bi$ divides p. Thus,

$$p = (a + bi)(c + di) = ac - bd + (ad + bc)i, \text{ for some } c, d \in \mathbb{Z}. \tag{3.9}$$

By comparing coefficients in (3.9) we get

$$ac - bd = p \tag{3.10}$$

and

$$ad + bc = 0. \tag{3.11}$$

Multiplying (3.10) by c and adding the result to d times (3.11) yields

$$a(c^2 + d^2) = pc. \tag{3.12}$$

Since p does not divide a, (3.12) implies a divides c. If gcd (c,d) = p, (3,9) requires $1=(a+bi)(c/p+id/p)=\alpha(c/p+id/p)$, forcing α to be unit in $\mathbb{Z}[i]$, a contradiction with primality of α in $\mathbb{Z}[i]$. So, gcd (c,d) = 1, which implies c divides a. Hence $c=a$. Similarly, $d=b$. Thus, $a^2+b^2=p$.

3.4 Polynomial Rings over *UFD*

First of all, let us remember polynomial rings. Let R be a ring, then the set $R[x]=\{f(x): f(x)=a_0+a_1x+a_2x^2+...+a_nx^n; a_i\in R, n\in\mathbb{N}\}$, where x is an indeterminate. The set is a ring under the sum and the product of two polynomials. Here, n is called *degree* of f and a_n is called *leading coefficient* of f.

Let R be a ring let S=R[x] be a polynomial ring over R. If we start with S and the construct the polynomial ring S[y] over S in indeterminate y, then S[y] is called a polynomial ring in two variables x,y over R. We write this ring as R[x,y]. It follows from the definition that R[x,y]= R[y,x]. A typical element of R[x,y] is of the form

$$\sum_{i=0}^{m}\sum_{j=0}^{n}a_{ij}x^iy^j, a_{ij}\in R.$$

Theorem 3.25 Let R[x] be a polynomial ring over a domain R. Let $f(x)$ and $g(x)$ be non-zero polynomial of R[x] of degree n and m respectively. Let $k=\max\{m-n+1,0\}$ and let 'a' be the leading coefficient of g(x). Then there exist unique polynomials $q(x)$ and $r(x)$ in R[x] such that

$$a^kf(x)=q(x)g(x)+r(x),$$

where r(x)=0, or r(x) has degree less than the degree of g(x).

Proof. If $m < n$, we take q(x)=0 and r(x)=f(x). Hence, let $m > n$ and k=m-n+1. We prove the theorem by induction on m. We assume that it is true for all polynomials of degree < m, and we prove it for polynomials of degree m.

Now the polynomial $af(x)-bx^{m-n}.g(x)$ has degree at most m-1, where b is the leading coefficient of f. By induction hypothesis there exist polynomials $q_1(x)$ and $r_1(x)$ such that

$$a^{(m-1)-n+1}(af(x)-bx^{m-n}g(x))=q_1(x)g(x)+r_1(x).$$

Then

$$a^kf(x)=(ba^{m-n}x^{m-n}+q_1(x))g(x)+r_1(x),$$

as desired. Uniqueness follows immediately.

In order to show that polynomial rings over a *UFD* are *UFD*, too. To do this we need some preliminaries.

Definition 3.26 Let *R* be a *UFD*. Then $f(x) \in R[x]$ is called *primitive* if the greatest common divisor of its coefficients is a unit.

Corollary 3.27 For any nonzero $f(x) \in R[x]$ can be written in the form $f(x) = cf_1(x)$, where c is the greatest common divisor of the coefficients of *f*(x) and f_1(x) is primitive.

Definition 3.28 Let *R* be a *UFD* and $0 \neq f(x) \in R[x]$. If we write $f(x) = cf_1(x)$, where f_1(x) is primitive, then '*c*' is called content of *f* and denoted by *c*(*f*).

Corollary 3.29 For any nonzero $f(x) \in R[x]$, *f*(*x*) is a primitive if and only if *c*(*f*) is a unit.

Lemma 3.30 (Gauss) If $f(x), g(x) \in R[x]$, then *c*(*fg*)=*c*(*f*)*c*(*g*). In particular, the product of two primitive polynomials is primitive.

Proof. Let $c = c(f)$ and $d = c(g)$, then we write $f(x) = cf_1(x)$ and $g(x) = dg_1(x)$ where $f_1(x)$ and $g_1(x)$ are primitive. Since $f(x)g(x) = (cf_1(x))(dg_1(x))$, we need to prove that $f_1(x)g_1(x)$ is primitive. Assume that $f_1(x)g_1(x)$ is not primitive and let *p* be an irreducible element of *R* that divides all the coefficients of $f_1(x)g_1(x)$. If $f_1(x) = \sum a_i x^i$ and $g_1(x) = \sum b_j x^j$ $(a_i, b_j \in R)$. Let a_s, b_t be the first coefficients of $f_1(x)g_1(x)$, respectively, that is not divisible by *p*. The coefficient of x^{s+t} in $f_1(x)g_1(x)$ is

$$\ldots + a_{s-1}b_{t+1} + a_s b_t + a_{s+1}b_{t-1} + \ldots$$

Since *R* is a *UFD*, $p \nmid a_s b_t$. Therefore we obtained a contradiction. Hence, $f_1(x)g_1(x)$ is primitive.

Theorem 3.31 Let *R* be a *UFD*. Then The polynomial ring *R*[*x*] over *R* is also a *UFD* [10].

3.5 Construction of Counterexamples

Example 3.32 An irreducible element may not be prime in a domain.

Let $R=\mathbb{Z}\left[i\sqrt{5}\right]$ and $\alpha=2+i\sqrt{5},\beta=2-i\sqrt{5},\gamma=3\in R$. Now let us consider norms of these elements :

$N(\alpha)=N(\beta)=N(\gamma)=9$. If α,β,γ were reducible, then there could be a non-unit $\delta\in R$ such that $N(\delta)\big|9$ properly, i.e., $N(\delta)=3\Rightarrow a^2+5b^2=3$ in Z. There is no such solution. That's why, α,β,γ are irreducible elements. Now, let us demonstrate that they are not prime.

$$\alpha\beta=(2+i\sqrt{5})(2-i\sqrt{5})=9=3.3=\gamma^2\Rightarrow\alpha\big|\gamma^2.$$

Does this case imply $\alpha\big|\gamma$?

If we have an affirmative answer, we can write $\gamma=\alpha\delta,$ for some $\delta\in R$, which means

$$\gamma=(2+i\sqrt{5})\delta\Rightarrow\delta=\frac{3}{2+i\sqrt{5}}=\frac{2+i\sqrt{5}}{3}\notin R\,.$$

Thus, α is not a prime element.

Consequently we have shown that in an arbitrary domain an irreducible element may not be prime.

Example 3.33 Every element can not be factorized uniquely in a domain.

Let $R=\mathbb{Z}\left[i\sqrt{5}\right]$ and $\alpha=2+i\sqrt{5},\beta=2-i\sqrt{5},\gamma=3\in R$ again. In the previous example we have seen that α,β,γ are irreducible elements. $9\in R$ has two different factorizations as follows:

$$9=3.3=(2+i\sqrt{5})(2-i\sqrt{5})=\gamma^2=\alpha\beta$$

where α,β,γ are irreducible elements.

Example 3.34 In a domain the greatest common divisor may not exist.

Let $R=\mathbb{Z}\left[i\sqrt{3}\right]$ and $\alpha=4,\beta=2+2i\sqrt{3}\in R$. First of all, let us write down the divisors of α and β :

$$\delta\big|\alpha\Rightarrow\delta=\pm1,\ \pm2,\ \pm(1\pm i\sqrt{3}),\ \pm4\ \text{ and}$$

$$\delta\big|\beta\Rightarrow\delta=\pm1,\ \pm2,\ \pm(1\pm i\sqrt{3}),\ \pm2(1\pm i\sqrt{3})\,.$$

So common divisors of α and β are

$$\pm 1,\ \pm 2,\ \pm(1 \pm i\sqrt{3}).$$

If we exclude units of $R = U(\mathbb{Z}\left[i\sqrt{3} \right]) = \{\pm 1\},$ then the common divisors are

$$2,\ 1 + i\sqrt{3} \text{ and } 1 - i\sqrt{3}.$$

Now let us check if there is a greatest common divisor. By definition 3.10

i) 2 can not be a *g.c.d* since

$$\begin{aligned}(1 \pm i\sqrt{3}) \mid \alpha \text{ and } (1 \pm i\sqrt{3}) \mid \beta &\Rightarrow (1 \pm i\sqrt{3}) \mid (\alpha, \beta) \\ &\Rightarrow (1 \pm i\sqrt{3}) \mid 2 \\ &\Rightarrow 2 = (1 \pm i\sqrt{3})\delta,\ (\delta \in R) \\ &\Rightarrow \delta = \frac{2}{1 \pm i\sqrt{3}} \\ &\Rightarrow \delta = \frac{1 \mp i\sqrt{3}}{2}.\end{aligned}$$

ii) neither $1 - i\sqrt{3}$ nor $1 + i\sqrt{3}$ can not be a *g.c.d* since

$$\begin{aligned}2 \mid \alpha \text{ and } 2 \mid \beta &\Rightarrow 2 \mid (\alpha, \beta) \\ &\Rightarrow 2 \mid (1 \pm i\sqrt{3}) \\ &\Rightarrow (1 \pm i\sqrt{3}) = 2\delta,\ (\delta \in R) \\ &\Rightarrow \delta = \frac{1 \mp i\sqrt{3}}{2}.\end{aligned}$$

As a result α and β have a few common divisors but they haven't any g.c.d.

Example 3.35 *UFD* may not be *PID*.

Let us consider the polynomial ring $R = F[x, y]$ over a field F in two variables; x and y. Then by Theorem 3.28, R is a *UFD*. On the other hand, The ideal $A = (x) + (y)$ in $F[x, y]$ can not be of the form ($f(x, y)$) for any polynomial $f(x, y) \in F[x, y]$, Since

$$(x) + (y) = (f(x, y)) \Rightarrow x = cf(x, y) \text{ and } y = df(x, y),$$

where c, d are non-zero constants in F. It means that

$$\frac{x}{c} = \frac{y}{d} \Rightarrow dx - cy = 0,$$

which contradicts with independency of the variables x and y. So, $F[x, y]$ is not a *PID*.

Example 3.36 *PID* may not a *EUD*.

$R = \{a + \frac{b}{2}(1 + \sqrt{-19}) : a, b \in \mathbb{Z}\}$ is a PID but not EUD. But demonstration needs tedious computations. For proof see [17] .

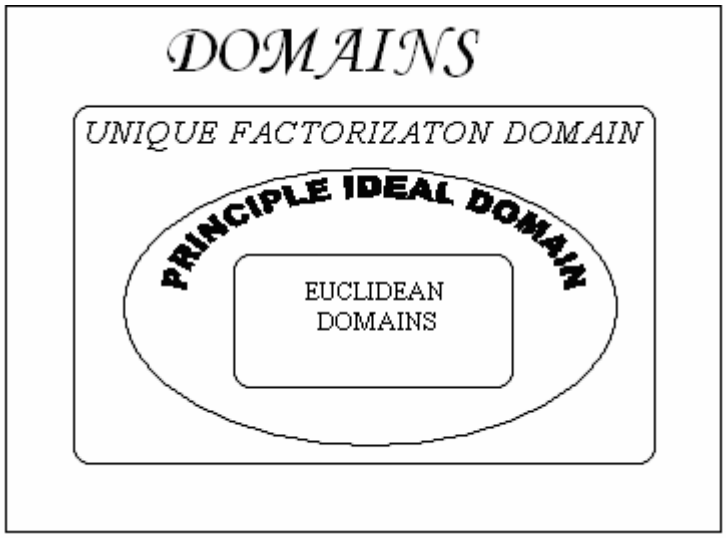

Figure 3.3 Containing- relations between domains

CHAPTER 4

ESSENTIALS OF QUADRATIC AND CYCLOTOMIC FIELDS

4.1 Quadratic Fields

Definition 3.1 Let $F = \mathbb{Q}(\sqrt{D})$ where D is a square free integer. Then, F is said to be a quadratic extension of $\mathbb{Q}$. Obviously, degree of extension of a quadratic field is 2.

We have already learned many things about quadratic fields in Chapter 2.We completely determined the ring of integers $\mathfrak{A}_F$, and the discriminant Δ_F for any quadratic field F.

Theorem 4.2 (No More Complex Quadratic Euclidean Domains) Let F be a complex quadratic field with discriminant $\Delta_F < -12$, then $\mathfrak{A}_F$ is not a Euclidean domain.

Proof. Assume f be a Euclidean function on $\mathfrak{A}_F$. Suppose that $\alpha \in \mathfrak{A}_F$ is a nonzero, nonunit element such that $f(\alpha)$ is minimal. This means that for any $\beta \in \mathfrak{A}_F$, there is a $\gamma \in \mathfrak{A}_F$ such that $\beta - \alpha\gamma = \delta = 0, \pm 1$, since either $\delta = 0$ or $f(\delta) < f(\alpha)$, $\left|\mathfrak{A}_F / \langle \alpha \rangle\right| \leq 3$. Therefore,

$$N_F(\alpha) \leq 3. \tag{4.1}$$

If $\Delta_F \equiv 0 \pmod 4$. In this case, $\alpha = a + b\sqrt{D}$ for $a, b \in \mathbb{Z}$, where $D = \Delta_F / 4$ is the radicand of F. Thus, by Equation (4.1),

$$N_F(\alpha) = a^2 - b^2 D \leq 3.$$

On the other hand, $\Delta_F < -12$ implies $-D > 3$ .. Hence, for $\alpha \neq 0, \pm 1$, $a^2 - b^2 D > 3$, which is a contradiction.

If $\Delta_F \equiv 1 \pmod 4$. In this case, $\alpha = (a + b\sqrt{D}) / 2$ for $a, b \in \mathbb{Z}$. If both a,b are even, then for a $\neq 0, \pm 1$, we get $3 \leq (a/2)^2 - D(b/2)^2 - D(b/2)^2 \leq 3$, so $D = \Delta_F = -3$, contradicting the hypothesis of the theorem. So, we assume that both a and b are odd. And so,$(a^2 - b^2 D)/4 \leq 3$. Hence, for α a $\neq 0, \pm 1$,

$$12 \leq a^2 + 11b^2 < a^2 - b^2 \ \Delta_F = a^2 - b^2 D \leq 12,$$

which is a contradiction. Therefore, $\mathfrak{A}_F$ is not a Euclidean domain.

Theorem 4.2 demonstrates that all Euclidean complex quadratic fields are necessarily norm - Euclidean. However, there are known to exist Euclidean real quadratic fields that are not norm - Euclidean. Also, there are known to exist exactly sixteen real quadratic fields that are norm - Euclidean. These are the fields $\mathbb{Q}(\sqrt{D})$ where

$$D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 55, 73\} \quad [6].$$

Theorem 4.3 (Some Norm – Euclidean Real Quadratic Fields)

If $D \in \{2, 3, 5, 6, 7, 13, 17, 21, 29\}$, then $F = \mathbb{Q}(\sqrt{D})$ is norm -Euclidean.

Proof. Let

$$\varepsilon = \begin{cases} 2 & \text{if } D \equiv 1 \pmod 4, \\ 1 & \text{if } D \equiv 2 \text{ or } 3 \pmod 4, \end{cases}$$

and one can easily observe that any $\sigma \in F$ can be written as

$$\sigma = r_1 + (r_2/\varepsilon)\sqrt{D},$$

where $r_1, r_2 \in \mathbb{Q}$.

By Proposition 2.43 we have for any

$$\sigma = r_1 + (r_2/\varepsilon)\sqrt{D}, \text{ for } r_1, r_2 \in \mathbb{Q}$$

there exists a

$$\beta = (x + y\sqrt{D})/\varepsilon \in \mathfrak{A}_F, \text{ where } x, y \in \mathbb{Z}$$

such that

$$|N_F(\sigma - \beta)| = |(r_1 - x/\varepsilon)^2 - (r_2 - y)^2 D/\varepsilon^2| < 1. \tag{4.2}$$

Assume that Equation (4.2) fails for some $r_1, r_2 \in \mathbb{Q}$ and $x, y \in \mathbb{Z}$. Without loss of generality we may suppose that $0 \le r_j \le 1/2$, for j = 1,2. To prove this; first, for j = 1,2 we set,

$$z_j = \begin{cases} [r_j] & \text{if } 0 \le r_j - [r_j] \le 1/2, \\ [r_j] + 1 & \text{if } 1 \ge r_j - [r_j] \ge 1/2, \end{cases}$$

where $[r_j]$ is the greatest integer less than or equal to r_j. Let $x = \varepsilon z_1 + \delta_1 x_1$, and $y = z_2 + \delta_2 y_1$, for any integers x_1, y_1, where $\delta_j = 1$ if $z_j = [r_j]$ and $\delta_j = -1$ otherwise for $j = 1,2$. Thus,

$$\left| (r_1 - x/\varepsilon)^2 - (r_2 - y)^2 D/\varepsilon^2 \right| = \left| (s_1 - x_1/\varepsilon)^2 - (s_2 - y_1)^2 D/\varepsilon^2 \right|,$$

for any $x_1, y_1 \in \mathbb{Z}$., where $0 \le s_j = |r_1 - z_j| \le 1/2$. $j = 1,2$.

Thus ,without loss of generality we may suppose that $0 \le r_j \le 1/2$, for $j = 1,2$.

So, for all $x, y \in \mathbb{Z}$, one of the following inequalities must hold for some $0 \le r_j \le 1/2$, $j = 1.2$,

$$(r_1 - x/\varepsilon)^2 \ge 1 + (r_2 - y)^2 D/\varepsilon^2, \tag{4.3}$$

or

$$(r_2 - y)^2 D/\varepsilon^2 / \ge 1 + (r_1 - x/\varepsilon)^2. \tag{4.4}$$

If $r_j = 0$ for $j = 1,2$, then (4.3) and (4.4) both fail for $x = 0 = y$. Thus, at least one of the r_j is nonzero. Therefore, if $x = 0 = y$, or $x = 1$, and $y = 0$, then (3.3) fails to hold. Thus, by (3.4) both

$$r_2^{\,2} D/\varepsilon^2 \ge 1 + r_1^{\,2} \tag{4.5}$$

and

$$r_2^{\,2} D/\varepsilon^2 \ge 1 + (r_1 - 1/\varepsilon)^2 \tag{4.6}$$

hold. If $x = -\varepsilon$, $y = 0$, and (4.3) holds, then

$$(r_1+1)^2 \ge 1 + r_2^{\,2} D/\varepsilon^2 \ge 2 + (r_1 - 1/\in)^2 \ge 2 + (r_1 - 1)^2 \tag{4.7}$$

Hence $2r_1 \ge 1$, from which $r_1 = 1/2$.

Thus, from (4.7),

$$(1/2+1)^2 \ge 1 + r_2^{\,2} D/\varepsilon^2 \ge 2 + (r_1 - 1/\varepsilon)^2 \ge 2 + (1/2 - 1)^2,$$

which implies $r_1^{\,2} D/\varepsilon^2 = 5/4$. Let $r_2 = a/b$, where $a, b \in \mathbb{Z}$ are relatively prime.

If $\varepsilon = 1$, then $4a^2 D = 5b^2$, so $a^2 | 5$. Thus, $a = 1$. Since D is square free, then $b = 2$, so $r_2 = ½$, and $D = 5$, which is on the list.

If $\varepsilon = 2$, then $a^2 D = 5b^2$, so $a = b = 1$ is forced, contradicting that $r_2 \le 1/2$.

Therefore, when $x = -\varepsilon$, and $y = 0$, (4.3) cannot hold, unless $D = 5$ (in which case (4.3) becomes an equality). Therefore, we may assume that (4.4) holds in this case, namely

$$r_2^{\,2} D/\varepsilon^2 \ge 1 + (r_1 - 1)^2 \ge 2.$$

Since $r_2^{\,2} \le 1/4$, hen the last inequality implies that $D \ge 8\varepsilon^2$.

Hence, if $D < 8\varepsilon^2$, then F is norm – Euclidean. For $D \equiv 1 \pmod 4$, this means that $D < 32$, and if $D \ne 1 \pmod 4$, then $D < 8$. This yields the values of D listed in the statement of the theorem.

Theorem 4.4 (Finitely Many Norm – Euclidean Quadratic Fields)

Let , $F = \mathbb{Q}(\sqrt{D})$, where D > 0 and is a square free integer , and $\Delta_F \equiv 0 \pmod 4$, then the number of such fields that are norm – Euclidean is finite in number.

Proof. Let F be a norm – Euclidean field of the given type. By proposition 2.43, there exists $x + y\sqrt{D} \in \mathbb{Z}[\sqrt{D}]$ such that for any $t \in \mathbb{Z}$,

$$|x^2 - D(y - t/D)^2| < 1.$$

which implies,

$$|Dx^2 - (Dy - t)^2| < D.$$

Since

$$(Dy - t)^2 - Dx^2 \equiv t^2 \pmod D,$$

there exist $x, z \in \mathbb{Z}$ such that

$$x^2 - Dx^2 \equiv t^2 \pmod D, \text{ and } |z^2 - Dx^2| < D. \tag{4.8}$$

Assume $D \equiv 3 \pmod 4$.

Let $t = 2[(\sqrt{6D} - 1)/2] + 1$. One can easily verify that for $D \geq 88$,

$$5D < t^2 < 6D.$$

Therefore, by (4.8), either $z^2 - Dx^2 = t^2 - 5D$, or $z^2 - Dx^2 = t^2 - 6D$. Therefore,

$$D(5 - x^2) = t^2 - z^2 , \text{ or } D(6 - x^2) = t^2 - z^2. \tag{4.9}$$

Assume that $D \equiv 2 \pmod 4$.

Let $t = 2[(\sqrt{3D} - 1)/2] + 1$. Again, one can easily verify that if $D \geq 40$, then

$$2D < t^2 < 3D.$$

So, by (4.8) , as above,

$$D(2 - x^2) = t^2 - x^2 , \text{ or } D(3 - x^2) = t^2 - x^2 . \tag{4.10}$$

By some number theoretical manipulations it can be proven that Equations (4.9) and (4.10) are impossible. Hence, for sufficiently large D with $\Delta_F \equiv 0 \pmod 4$, we have that F cannot be norm-Euclidean.

Example 4.5 Let's prove that $\mathbb{Q}(\sqrt{23})$ is not norm-Euclidean.
If $D = 23$, $r_1 = 0$ and $r_2 = 7/23$; then (3.2) becomes

$$\left|23x^2 - (7-23y)^2\right| < 23.$$

Since $23x^2 - (7-23y)^2 \equiv -3 \pmod{23}$, we have

$$23x^2 - (7-23y)^2 = -3 \text{ or } 20. \tag{4.11}$$

Let $z = 7-23y$, then (11) becomes $23x^2 - z^2 = -3$ *or* 20.
If $23x^2 - z^2 = -3$, then neither *x* nor *z* is divisible by 3. So, $x^2 \equiv z^2 \equiv 1 \pmod 3$, implying that $23-1 \equiv 0 \pmod 3$ which is a contradiction.
If $23x^2 - z^2 = 20$, then neither *x* nor *z* is divisible by 5. So, $x^2 \equiv z^2 \equiv \pm 1 \pmod 5$, implying that $20 = 23x^2 - z^2 \equiv 1,2,3 \text{ or } 4 \pmod 5$ which is again a contradiction. Therefore, there is no solution for equation (4.11). Thus, $\mathbb{Q}(\sqrt{23})$ is not norm-Euclidean

4.2 Cyclotomic Fields

Definition 3.6 Let *n* be a natural number and ζ_n be primitive *n*'th root of unity. The extension field $\mathbb{Q}(\zeta_n)$ is called the *n*'th cyclotomic field.
The ring of integers the *n*'th cyclotomic field is $\mathbb{Z}[\zeta_n]$. Namely,

$$\text{if } F = \mathbb{Q}(\zeta_n), \text{then } \mathfrak{A}_F = \mathbb{Z}[\zeta_n] \quad [7].$$

Definition 4.6 (Cyclotomic Polynomials) Let $n \in \mathbb{N}$ and ζ_n be primitive *n*'th root of unity. Then, the polynomial

$$\Phi_n(x) = \prod_{\substack{\gcd(n,\, j) = 1 \\ 1 \le j < n}} (x - \zeta_n^{\,j})$$

is called the *n*'th cyclotomic polynomial .The degree of $\Phi_n(x)$ is $\phi(n)$
where $\phi(n) = n\prod(1 - \frac{1}{p_i})$, p_i 's are prime divisors of *n*.

Theorem 4.7 (Irreducibility of the Cyclotomic Polynomial) For any $n \in \mathbb{N}$

$$\Phi_n(x) = m_{\zeta_n, \mathbb{Q}}(x)$$

where ζ_n be primitive *n*'th root of unity. So $\Phi_n(x)$ is irreducible in $\mathbb{Z}[x]$.

Proof. Let us prove first that $\Phi_n(x) \in \mathbb{Z}[x]$. We use induction on n.
If $n = 1$ $\Phi_1(x) = x\text{-}1 \in \mathbb{Z}[x]$. Assume that $\Phi_k(x) \in \mathbb{Z}[x]$ for all $k < n$. Now we have

$$\Phi_n(x) = \frac{x^n - 1}{f(x)}$$

where, by induction hypothesis, $f(x) \in \mathbb{Z}[x]$ is a monic polynomial. So, by dividing out we have $\Phi_n(x) \in \mathbb{Z}[x]$.
Also, $m_{\zeta_n,\mathbb{Q}}(x) \in \mathbb{Z}[x]$ since all powers of ζ_n are integral over $\mathbb{Z}$.

Claim: $m_{\zeta_n,\mathbb{Q}}(\zeta_n{}^j) = 0$ for any $j \in \mathbb{Z}$ such that gcd $(j, n) = 1$,
Proof. We first prove the result for a prime $j = p$ which does not divide n. Since

$$x^n - 1 = m_{\zeta_n,\mathbb{Q}}(x)\, f(x),$$

for some $f(x) \in \mathbb{Z}[x]$, we may let the image of $x^n - 1$ under the natural map

$$\mathbb{Z}[x] \to (\mathbb{Z}/p\mathbb{Z})[x]$$

be given by the bar notation

$$x^n - \overline{1} = \overline{m}\zeta_n, \mathbb{Q}(x)\overline{f}(x).$$

Since

$$(x^n - 1)/(x - 1) = \sum_{j=0}^{n-1} x^j = \prod_{j-1}^{n-1} (x - \zeta_n^{\,j}),$$

and setting $x = 1$

$$n = \prod_{j=1}^{n-1} (1 - \zeta_n^{\,j}).$$

Since p does not divide n, we have

$$\bar{n} = \prod_{j=1}^{n-1} \overline{(1 - \zeta_n^{\,j})}.$$

Thus, $\overline{\zeta_n^{\,j}} \neq \bar{1}$ for any $j = 1,2, \ldots, n-1$. Hence $\overline{\zeta_n^{\,j}} \neq \overline{\zeta_n^{\,i}}$ for any such $i \neq j$, so the roots of $x^n - \bar{1}$ are distinct in $(\mathbb{Z}/\mathrm{p}\mathbb{Z})[x]$. Hence, $\overline{m}\zeta_n,\mathbb{Q}(x)$ and $\overline{f}(x)$ have no common roots. Assume $m_{\zeta_n,\mathbb{Q}}(\zeta_n^{\,p}) \neq 0$, then $f(\zeta_n{}^p) = 0$, so $\overline{f}(\zeta_n{}^p) = 0$. Hence, using the Binomial Theorem $\overline{f}(\zeta_n)^p = \bar{0}$, so $\overline{f}(\zeta_n) = \bar{0}$. Therefore, $\overline{m}\zeta_n,\mathbb{Q}(\zeta_n) \neq 0$ which contradicts with $m_{\zeta_n,\mathbb{Q}}(\zeta_n) = 0$. Thus, claim is true for prime $j = p$ which does not divide n.

On the other hand, if j is a product of primes each of which does not divide n, then ζ_n^j is also a root of $m_{\zeta_n,\mathbb{Q}}(x)$ which means claim is true for any $j \in \mathbb{Z}$ such that gcd (j, n) = 1.Hence,

$$\Phi_n(x) \text{ divides } m_{\zeta_n,\mathbb{Q}}(x). \tag{4.12}$$

So,

$$\deg(\Phi_n(x)) \leq \deg(m_{\zeta_n,\mathbb{Q}}(x)). \tag{4.13}$$

Since ζ_n is a root of $\Phi_n(x)$, minimality of $m_{\zeta_n,\mathbb{Q}}(x)$ implies

$$\deg(\Phi_n(x)) \geq \deg(m_{\zeta_n,\mathbb{Q}}(x)). \tag{4.14}$$

(4.13) and (4.14) implies

$$\deg(\Phi_n(x)) = \deg(m_{\zeta_n,\mathbb{Q}}(x)) = \phi(n). \tag{4.15}$$

(4.12) and (4.15) implies

$$\Phi_n(x) = m_{\zeta_n,\mathbb{Q}}(x). \tag{4.16}$$

Corollary 4.8 The degree of extension of the cyclotomic field generated by the primitive n'th root of unity is $\phi(n)$. Namely, for any $n \in \mathbb{N}$

$$\left|\mathbb{Q}(\zeta_n) : \mathbb{Q}\right| = \phi(n).$$

Proof. This follows from direct result of Theorem 4.7

Theorem 4.9 (Discriminant Divisibility)

Let $F = \mathbb{Q}(\zeta_n)$. Then, Δ_F divides $n^{\phi(n)}$.

Proof. We have $x^n - 1 = \Phi_n(x) f(x)$, for some $f(x) \in \mathbb{Z}[x]$. After differentiating both sides, we get

$$n\, x^{n-1} = \Phi_n'(x) f(x) + \Phi_n(x) f'(x)$$

By setting $x = \zeta_n$, we obtain

$$n\zeta_n^{n-1} = \Phi_n'(\zeta_n) f(\zeta_n).$$

By taking the norm of both sides,

$$\pm n^{\phi(n)} = N_F(n\zeta_n^{n-1}) = N_F(\Phi_n'(\zeta_n))\, N_F(f(\zeta_n)).$$

By corollary 2.48 and proposition 2.49, we get

$$\Delta_F = \pm N_F(\Phi'_n(\zeta_n)).$$

Thus, last two equations imply Δ_F divides $n^{\phi(n)}$.

Theorem 4.10 (The Ring of Integers of a Cyclotomic Field) Let $n \in \mathbb{N}$ and ζ_n be primitive n'th root of unity.

$$\text{If } F = \mathbb{Q}(\zeta_n) \text{ then } \mathfrak{A}_F = \mathbb{Z}[\zeta_n] \quad [2].$$

Theorem 4.11 (Discriminants of Prime-Power Cyclotomic Fields) Let p be a prime number,

$n = p^a$ for a natural number a and $F = \mathbb{Q}(\zeta_n)$. Then,

$$\Delta_F = (-1)^{\phi(p^a)/2} p^{p^{a-1}(a(p-1)-1)} \quad [2].$$

Example 4.12 Let $\alpha = \zeta_8$ be pirimitive eighth root of unitiy and $F = \mathbb{Q}(\alpha)$. Since $8 = 2^3$ and $\phi(8) = 4$, by theorem 3.11 $\Delta_F = (-1)^2 2^{2^2(3(2-1)-1)} = 256$.

We can find Δ_F also as follws. By example 2.16 and theorem 4.7

$$m_{\alpha,\mathbb{Q}}(x) = x^4 + 1 \text{ and } m'_{\alpha,\mathbb{Q}}(x) = 4x^3.$$

Embeddings of F in $\mathbb{C}$ are

$$\theta_1 : \zeta_8 \to \zeta_8,$$

$$\theta_2 : \zeta_8 \to \zeta_8^3,$$

$$\theta_3 : \zeta_8 \to \zeta_8^5$$

and

$$\theta_4 : \zeta_8 \to \zeta_8^7.$$

Thus, by theorem 2.46 and proposition 2.49

$$\Delta_F = (-1)^{\binom{4}{2}} N_F(m'_{\alpha,\mathbb{Q}}(\alpha)) = (4\zeta_8^3)(4(\zeta_8^3)^3)(4(\zeta_8^5)^3)(4(\zeta_8^7)^3) = 256.$$

CHAPTER 5

THEORY OF IDEALS

5.1 Properties of Ideals

The primary goal of this chapter is to achieve the Unique Factorization Theorem for Ideals. First, we develop the basic properties of ideals, which will include wide variety of results in arithmetic of ideal theory.

Definition 5.1 Let *R* be a commutative ring. A nonempty subset *I* of *R* is called an ideal of *R*, if it satisfies following two conditions:

(i) If $\alpha, \beta \in I$, then $\alpha - \beta \in I$.

(ii) For every $r \in R$ and for every $\alpha \in I$, $r\alpha \in I$.

Note that, first condition makes *I* be an additive subgroup of *R* and second one makes *I* be a sub ring of *R*.

Ideals may be defined over noncommutative rings, but for our purposes the commutative case is sufficient.

Ideals in a commutative ring *R* with identity are called *R*-ideals for convenience sake. We are primarily interested in $\mathfrak{A}_F$-ideals for a given number field *F*.

And two ideals are equal if they are equal as sets. Any ideal *I* in a commutative ring with identity having a finite set of generators is said to be finitely generated. When there is exactly one such generator α we call *I* principal, and write

$$I = (\alpha)$$

Example 5.2 Let $R = \mathbb{Z}[\sqrt{10}]$. One can check that

$$I_1 = (2) = \left\{ 2a + 2b\sqrt{10} : a, b \in \mathbb{Z} \right\} \text{ and}$$

$$I_2 = (3) = \left\{ 3a + 3b\sqrt{10} : a, b \in \mathbb{Z} \right\}$$

are two ideals of *R*. I_1 is generated by 2 and I_2 is generated by 3. These are examples of principle ideals, namely ideals which are generated by a single element. Consider the ideal generated by 6. It is product of two ideals as it is seen below,

$$(6) = \left\{ 6a + 6b\sqrt{10} : a, b \in \mathbb{Z} \right\} = (2)(3).$$

Observe that, $(6) \subset (2)$ and $(6) \subset (3)$.

Definition 5.3 Let R be a commutative ring and I ,J be two ideals of R. If there exists an ideal H of R such that $J = HI$, then I is said to divide J .

For example, according to example 5.2 (2) divides (6) and (3) divides (6) in $\mathbb{Z}[\sqrt{10}]$.

Lemma 5.4 Let R be a commutative ring with identity and I, J be two R- ideals. If I divides J, then I contains J.

Proof. If I divides J, then by definition 5.3 there exists an R-ideal H such that $J = HI$. By definition of ideal I contains HI. So, I contains J.

Converse of this lemma is also true. That is, Let R be a commutative ring with identity and I ,J be two R- ideals. If I contains J, then I divides J. We are going to discuss the proof later.

An ideal may be generated by more than one element. If I is generated by $\alpha_1, \alpha_2, ..., \alpha_r$; then we write $I = (\alpha_1, \alpha_2, ..., \alpha_r)$ This is illustrated by the following example.

Example 5.5 Let $R = \mathbb{Z}[\sqrt{10}]$. Consider the ideal generated by 4 and 6 which is denoted by (4,6)**.**

$$(4,6) = \{4x + 6y : x, y \in R\}.$$

Let $x = a + b\sqrt{10}$ and $y = c + d\sqrt{10}$, $a, b, c, d \in \mathbb{Z}$; then

$$4x + 6y = (4a + 6c) + (4b + 6d)\sqrt{10} \text{ , } a, b, c, d \in \mathbb{Z}.$$

Since gcd (4,6) = 2, numbers of the form $4p + 6q, p, q \in \mathbb{Z}$ are multiples of 2.

So,

$$(4,6) = \left\{2n + 2m\sqrt{10} : n, m \in \mathbb{Z}\right\} = (2).$$

Note that, although (4,6) seems to be generated by two members this example shows that it can be generated by a single element; therefore it is a principle ideal of R.

Proposition 5.6 Let F be an algebraic number field and $I = (\alpha)$ and $J = (\beta)$ be principal $\mathfrak{A}_F$ -ideals. Then, $I = J$ if and only if α and β are associates.

Proof. By proposition 3.6 α and β are associates if and only if $\alpha \mid \beta$ and $\beta \mid \alpha$ if and only if $\alpha \subseteq \beta$ and $\beta \subseteq \alpha$ if and only if $(\alpha) = (\beta)$. Thus, $I = J$ if and only if α and β are associates.

Proposition 5.7 (Generalization of Proposition 5.4) Let F be an algebraic number field and $I=(\alpha_1,\alpha_2,...,\alpha_n)$ and $J=(\beta_1,\beta_2,...,\alpha_n)$ be $\mathfrak{A}_F$-ideals. Then, $I=J$ if and only if there exists an invertible $n\times n$ matrix $A\in GL_n(\mathbb{Z})$ such that

$$\begin{pmatrix}\alpha_1\\ .\\ \alpha_n\end{pmatrix}= A\begin{pmatrix}\beta_1\\ .\\ \beta_n\end{pmatrix}$$ [2].

Example 5.8 Let $F=\mathbb{Q}(\sqrt{10})$. Then $\mathfrak{A}_F=\mathbb{Z}[\sqrt{10}]$. Consider

$$I=(3,1+\sqrt{10}) \text{ and } J=(-3,2-\sqrt{10}).$$

$I=J$, since the following matrix equation holds,

$$\begin{pmatrix}3\\ 1+\sqrt{10}\end{pmatrix}=\begin{pmatrix}-1 & 0\\ -1 & -1\end{pmatrix}\begin{pmatrix}-3\\ 2-\sqrt{10}\end{pmatrix} \text{ with } \begin{pmatrix}-1 & 0\\ -1 & -1\end{pmatrix}\in GL_2(\mathbb{Z}).$$

There is an other notation to represent $\mathfrak{A}_F$-ideals. It is $\mathbb{Z}$-module notation. We know that every $\mathfrak{A}_F$-ideal I is a subgroup of the free abelian group $\mathfrak{A}_F$ of rank

$$|F:\mathbb{Q}|=d.$$

So, I is a free abelian group of rank at most d. Therefore I has $\mathbb{Z}$-basis $\{\alpha_1,\alpha_2,...,\alpha_r\}\subseteq\mathfrak{A}_F$, for $r\le d$. Thus, I can be written in $\mathbb{Z}$-module structure as

$$I=[\alpha_1,\alpha_2,...,\alpha_r]. \tag{5.1}$$

Proposition 5.9 Let $F=\mathbb{Q}(\alpha)$ be an algebraic number field with $|F:\mathbb{Q}|=d$ and $I=[\alpha_1,\alpha_r,...,\alpha_r]$ be a $\mathfrak{A}_F$-ideal. Then, $r=d$.

Proof. We know that $r\le d$. Let $\{\beta_1,\beta_2,...,\beta_d\}$ be a $\mathbb{Z}$-basis for $\mathfrak{A}_F$. If $\alpha\in I$ is nonzero, then $\alpha\beta_1,\alpha\beta_2,...,\alpha\beta_d$ are linearly independent and $\alpha\beta_1,\alpha\beta_2,...,\alpha\beta_d\in I$. So, $\{\alpha\beta_1,\alpha\beta_2,...,\alpha\beta_d\}$ is a $\mathbb{Z}$-basis for F. So, for every $j\in\{1,2,...,d\}$ there exist $z_{1,j},z_{2,j},...,z_{r,j}\in\mathbb{Z}$ such that

$$\alpha\beta_j=\sum_{i=1}^{r}z_{i,j}\beta_i.$$

Assume that $d>r$. Then here exist $w_1,w_2,...,w_d\in\mathfrak{A}_F$, not all zero such that

$$\sum_{j=1}^{d}z_{i,j}w_j=0.$$

Therefore, for each $j\in\{1,2,...,d\}$

$$0=\sum_{i=1}^{r}z_{i,j}w_j\beta_i=w_j\sum_{i=1}^{r}z_{i,j}\beta_i=w_j\alpha\beta_j.$$

Thus,

$$\sum_{j=1}^{d} w_j \alpha \beta_j = 0$$

which is impossible , because $\{\beta_1, \beta_2, ..., \beta_d\}$ is a $\mathbb{Z}$-basis for *F*.
Hence $d \le r$, implying that $r = d$.

As a result of this proposition, in (5.1) $r = d$.

Note that proposition 5.5 is true for $\mathbb{Z}$-module structures [2].

Proposition 5.10 Let $R = \mathbb{Z}[\sqrt{D}] = \mathbb{Z} + \sqrt{D}\mathbb{Z} = [1, \sqrt{D}]$ where *D* be a square free integer. $a\mathbb{Z} + (b + c\sqrt{D})\mathbb{Z} = [a, b + c\sqrt{D}]$ with $a, b, c \in \mathbb{Z}$, $a > 0$ and $c > 0$ is an *R*-ideal if and only if *c* divides *a*, *c* divides *b* and ac divides $b^2 - c^2 D$.

Proof. Let $I = [a, b + c\sqrt{D}]$ and $A = \left\{ y : x + y\sqrt{10} \in I \; x, y \in \mathbb{Z}, \; y > 0 \right\}$. Clearly $c \in A$ because $b + c\sqrt{D} \in I$. *Claim* : c is the least element of *A*. If not, there exists $b_1 + c_1\sqrt{D} \in I$ such that $0 < c_1 < c$. So, $b_1 + c_1\sqrt{D} = ap + (b + c\sqrt{D})q$ for some $p, q \in \mathbb{Z}$. From here, $c_1 = cq$ which implies $c_1 \ge c$, a contradiction. Therefore, c is the least element of *A*. Similarly, it can be proven that *a* is the least positive integer in *I*.

If *I* is an ideal, then $a\sqrt{D} \in I$, so *c* divides *a* by minimality of *c*. Also $\pm\sqrt{D}(b + c\sqrt{D}) = cD \pm b\sqrt{D} \in I$, so *c* divides *b*. Moreover,

$$(b/c - \sqrt{D})(b + c\sqrt{D}) = (b^2 - c^2 D)/c \in I,$$

which implies *a* divides $(b^2 - c^2 D)/c$ by minimality of *a*. So,
ac divides $b^2 - c^2 D$.

Conversely, if *c* divides *a*, *c* divides *b* and ac divides $b^2 - c^2 D$, then

$$a\sqrt{D} = -(b/c)a + (a/c)(b + c\sqrt{D}) \in I$$

and

$$(b + c\sqrt{D})\sqrt{D} = b\sqrt{D} + cD = (-b^2 + c^2 D)/c + (b/c)(b + c\sqrt{D}) \in I.$$

Thus, *I* is an ideal.

Example 5.11 Let $F = \mathbb{Q}(\sqrt{10})$. Then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{10}]$. Consider

$$[1 + \sqrt{10}, 1 - \sqrt{10}] \text{ and } [2, 1 + \sqrt{10}].$$

$[1 + \sqrt{10}, 1 - \sqrt{10}] = [2, 1 + \sqrt{10}]$, since the following matrix equation holds,

$$\begin{pmatrix} 2 \\ 1+\sqrt{10} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1+\sqrt{10} \\ 1-\sqrt{10} \end{pmatrix} \text{ with } \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{Z}).$$

Note that, $[1+\sqrt{10}, 1-\sqrt{10}] \neq (1+\sqrt{10}, 1-\sqrt{10})$.
In order to see this, we have

$$1 = 5(1+\sqrt{10}) + (6+\sqrt{10})(1-\sqrt{10}) \in (1+\sqrt{10}, 1-\sqrt{10}).$$

So,

$$(1+\sqrt{10}, 1-\sqrt{10}) = \mathfrak{A}_F .$$

But, since 2 does not divide $N_F(1+\sqrt{10}) = -9$; by proposition 5.10 $[2, 1+\sqrt{10}]$ is not a $\mathfrak{A}_F$ - ideal .

By a product of two $\mathfrak{A}_F$ -ideals,

I = { $\alpha_1, \ldots, \alpha_r$) and $J = (\beta_1, \ldots \beta_s)$,

We mean the $\mathfrak{A}_F$ -ideal generated by all products $\alpha_j \beta_j$ namely,

$IJ = (\alpha_1\beta_1, \ldots, \alpha_1 b_s, \ldots, \alpha_i\beta_j, \ldots, \alpha_r\beta_1, \quad , \alpha_r\beta_s)$.

Definition 5.12 Let F be a number field. A prime $\mathfrak{A}_F$ -ideal is a nonzero ideal $P \neq \mathfrak{A}_F$ such that, whenever P divides IJ, where I and J are two $\mathfrak{A}_F$ -ideals , then P divides I or P divides J. We call the prime ideal (0) the trivial ideal.

Example 5.13 Let $F = \mathbb{Q}(i)$, then $\mathfrak{A}_F = \mathbb{Z}[i]$. Consider. $P = (5, 2+i)$. P is an $\mathfrak{A}_F$ -ideal by proposition 5.10. Also, by proposition 3.24, P is a prime ideal.

In the view of Lemma 5.4, by Definition 5.12 we can say that a prime ideal P is a $\mathfrak{A}_F$ -ideal satisfying the property that whenever $IJ \subseteq P$ where I and J are $\mathfrak{A}_F$ -ideals then either $I \subseteq P$ or $J \subseteq P$.

Definition 5.14 Let R be a commutative ring with unity, and $I \neq R$ an R-ideal, I is called a maximal ideal if whenever $I \subseteq J$ for any R-ideal J, then $I = J$, or $J = R$.

Thus, maximal R-ideals are proper R-ideals that are not contained in any other proper R-ideals.

A nonzero R-ideal I is called minimal if whenever $(0) \subseteq J \subseteq I$ for any R-ideal J, then J = (0) or $J = I$. In other words, a minimal R-ideal is a nonzero R-ideal that contains no other nonzero R-ideal.

Theorem 5.15 Let R be a commutative ring with unity. M is maximal ideal if and only if R/M is a field [9].

Example 5.16 Let $R = \mathbb{Z}$ and p be a prime number. Since $\mathbb{Z} / p\mathbb{Z}$ is isomorphic to $\mathbb{Z}_p$ which is a field, (p) = $p\mathbb{Z}$ is a maximal ideal.

Theorem 5.17 Let R be a commutative ring with unity and $N \neq R$ be an R-ideal. N is prime ideal if and only if R / N is an integral domain [9].

Corollary 5.18 Let R be a commutative ring with unity. Every maximal R-ideal is prime R-ideal.

5.2 Dedekind Domain

Definition 5.19 A Dedekind domain R is an integral domain satisfying the following three properties.

(i) Every ideal of R is finitely generated.
(ii) Every nonzero prime ideal of R is maximal.
(iii) R is integrally closed in its quotient field.

A principal ideal domain satisfies all three conditions, and is therefore a Dedekind domain.

$$F = \{\alpha / \beta : \alpha, \beta \in R, \beta \neq 0\}.$$

Observe that condition (iii) above says that if $\alpha / \beta \in F$ is the root of some monic polynomial over R, then $\alpha / \beta \in R$. In other words, $\beta \mid \alpha$ in R.

Definition 5.20 The sum of two R-ideals I and J in a commutative ring with identity R is given by

$$I + J = \{\alpha + \beta : \alpha \in I, \beta \in J\},$$

which is an ideal [8]. If there does not exist any proper ideal H such that H divides I and H divides J , then I and J are said to be relatively prime. If I and J are relatively prime R-ideals, then $I + J = R$.

Example 5.21 Let $F = \mathbb{Q}(\sqrt{10})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{10}]$. Consider the two principal $\mathfrak{A}_F$-ideals (2) and (3). One can easily prove that (2) and (3) are relatively prime. So,

$$(2) + (3) = \mathfrak{A}_F = \mathbb{Z}[\sqrt{10}].$$

Theorem 5.22 (Number Rings are Dedekind Domains)

If F is a number field, then $\mathfrak{A}_F$ is a Dedekind domain [2]..

Lemma 5.23 If R is a Dedekind domain and I is an R-ideal, then I contains a product of prime R-ideals.

Proof. Let *S* be the set of all *R*-ideals that do not contain a product of prime ideals. If S ≠ ∅, then S has a maximal element *M*, Therefore, *M* cannot be prime, since it would otherwise contain a product of primes, namely itself. Thus, there exist $r,s \in R$ such that $rs \in M$, but $r \notin M$ and $s \notin M$. Since *M* is contained in both of the ideals $M + (r)$ and $M + (s)$, then both of these latter ideals contain products of prime ideals. Therefore,

$$(M + (r))\,(M + (s)) \subseteq M,$$

a contradiction, so S is empty. This completes the proof.

Theorem 5.24 In any commutative ring with unity, every proper ideal is contained in a maximal ideal.

Proof. Let *R* be a commutative ring with unity. By Zorn's Lemma to family of proper *R*-ideals, it is enough to show that a nested union of proper *R*-ideals is another *R*-ideal. Now, if we have $I_1 \subset I_2 \subset \ldots \subset I_j \subset \ldots$, then $I = \bigcup_{j=1}^{\infty} I_j$ satisfies $rI \subseteq I$ since $rI_j \subseteq I_j$ for each *j*. Hence *I* is a *R*-ideal and since $1_R \notin I_j$ for each *j*; *I* is proper.

Lemma 5.25 Let *R* is a Dedekind domain with quotient field *F* and let $I \neq R$ be an *R*-ideal. Then there exists $\alpha\, \gamma \in F$ -*R* such that $\gamma I \subseteq R$.

Proof. Let $\alpha \in I$ be a fixed nonzero element. By Lemma 5.23, the principal *R*-ideal (α) contains a product of prime ideals $P_1 \ldots P_r$, . Suppose that *r* is minimal with respect to being a product of primes in (α). By Theorem 5.24 , every proper *R*-ideal is contained in a maximal ideal, which must be prime by Corollary 5.18.Thus, $I \subseteq P$ for some prime *R*-ideal *P*. By primality, $P_j \subseteq P$ for some *j*, which we may assume to be $j = 1$ without loss of generality, By condition (ii) of Definition 5.19, $P_1 = P$. Since (α) cannot contain a product of fewer than *r* prime ideals, there is a $\beta \in P_2 \ldots P_r - (\alpha)$. Therefore,

$$\beta/\alpha \in \frac{1}{(\alpha)}\ P_2\ \ldots P_r \text{ - } R \subseteq F \text{ - } R.$$

On the other hand,

$$\beta P \subseteq PP_2 \ldots P_r \subseteq (\alpha).$$

So if $\delta \in P$, then $\beta\delta \in (\alpha)$. In particular if $\delta \in I$, then $\beta\delta \in (\alpha)$, so

$$\frac{\beta}{\alpha}\delta \in R.$$

It means,

$$\gamma I = \frac{\beta}{\alpha} I \subseteq R,$$

which completes the proof.

Theorem 5.26 Let R be a Dedekind domain and let I be a nonzero R-ideal. Then there exists a nonzero R-ideal J such that IJ is principal.

Proof. Let I be a nonzero R-ideal with $\alpha \in$ I, and let

$$J = \{\beta \in R : \beta I \subseteq (\alpha)\}.$$

Therefore, J is a nonzero R-ideal containing α and

$$IJ \subseteq (\alpha).$$

Now let $L = \frac{1}{\alpha} IJ$, then $L \subseteq R$. Since I, J are ideals, then so is L. Assume that L is a proper R-ideal. By Lemma 5.25, there exists a $\gamma \in F$-R such that $\gamma L \subseteq R$.We will show that γ is the root of a monic polynomial over R. Since $J \subseteq L$, given that $\alpha \in$I, then $\gamma J \subseteq \gamma L \subseteq R$. Hence $\gamma JI \subseteq RI \subseteq I$, which implies that

$$\gamma J \subseteq J \ . \tag{5.1}$$

Let $\{\beta_1 \ldots\ldots, \beta_r\}$ be a generating set for the ideal J. From (5.1), there exist $z_{i,j} \in \mathbb{Z}$ such that for each $i = 1, \ldots\ldots, r$,

$$\gamma\beta_i = \sum_{j=1}^{r} z_{i,\,j}\beta_j \ .$$

This gives the homogeneous system of equations

$$\begin{aligned}
&\left(z_{1,1} - \gamma\right)x_1 + z_{1,2}x_2 + \ldots + z_{1,r}\,x_r = 0\\
&z_{2,1}x_1 + \left(z_{2,2} - \gamma\right)x_2 \ldots + z_{2,r}x_r = 0\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&z_{1,1}x_1 + z_{r,2}x_2 + \ldots + (z_{r,r} - \gamma)x_r = 0
\end{aligned}$$

which has the nontrivial solution $x_j = \beta_j$, so the determinant

$$\det\begin{pmatrix}
(z_{1,1} - \gamma) & z_{1,2} & \cdots & z_{r,1}\\
z_{2,1} & (z_{2,2} - \gamma) \ldots & & z_{2,r}\\
M & & \vdots & \vdots\\
z_{r,1} & z_{r,2} & \cdots (z_{r,r} - \gamma)
\end{pmatrix}$$

vanishes. Hence, γ satisfies the required monic polynomial over R, which contradicts the condition (iii) of Definition 5.19. So, L is a not proper R-ideal. Thus, $IJ = (\alpha)$ which requires desired result.

Corollary 5.27 Let I, J, L be ideals in a Dedekind domain such that I is nonzero, and $IJ = IL$, then $J = L$.

Proof. If H is an ideal such that $IH = (\alpha)$, then $J(\alpha) = L(\alpha)$. Since,

$$L \subseteq L(\alpha) = J(\alpha) \subseteq J,$$

And

$$J \subseteq J(\alpha) = L(\alpha) \subseteq L,$$

Then $L = J$.

Corollary 5.28 Let I and J be ideals in a Dedekind domain, then I divides J if and only if $I \supseteq J$.

Proof. First direction is Lemma 5.4, so was proven. Assume that $I \supseteq J$. Let L be an ideal such that LI is principal, say $LI = (\alpha)$. Then, $H = \frac{1}{\alpha} LJ$ is an ideal, and $IH = J$. Thus, I divides J.

Theorem 5.29 (Unique Factorization of Ideals) Every proper nonzero ideal in a Dedekind domain R is uniquely representable as a product of prime ideals. In other words, any R-ideal I has a unique expression (up to order of the factors) of the form

$$I = p_1^{e_1} p_2^{e_2} \ldots p_2^{e_n}$$

where the P_j are the distinct prime R-ideals containing I, and $e_j \in \mathbb{N}$ for j =1,2 . . . , n.

Proof. First we must show existence. In other words, we must show that every ideal is indeed representable as a product of primes. Let S be the set of all nonzero proper ideals that are not so representable. If $S \neq \varnothing$, then S has a maximal member M. Since $M \neq R$, then by Theorem 5.24 and Corollary 5.18, there exists a prime ideal P such that $M \subseteq P$. Thus, there is an R-ideal H such that $M = HP$, by Corollary 5.28. Thus, $H \supseteq M$. If $H = M$, then $H = HP$, so $P = R$, by Corollary 3.17, a contradiction. Hence, H strictly contains M. By the maximality of M, H must be a product of prime ideals. However, $M = H P$, contradicting that $M \in S$, so $S = \varnothing$, We have established existence. It remains to show uniqueness of representation.

Let P_j and Q_s be (not necessarily distinct) prime R -deals such that,

$$P_1 \ \ldots P_r = Q_1 \ \ldots Q_s \, .$$

Hence, $P_1 \supseteq Q_1 Q_2 \ldots Q_s$ which implies $P_1 \supseteq Q_i$ for some $i \in \{1, 2, \ldots, s\}$. Without loss of generality assume that $P_1 \supseteq Q_1$. So by Corollary 5.27, we get

$$P_2 \ \ldots P_r = Q_2 \ \ldots Q$$

Continuing in this way, we see that by induction, $r = s$ and $P_i = Q_i$ for each $i \in \{1, 2, ..., s\}$.

Corollary 5.30 Let F is a number field, then every proper, nonzero $\mathfrak{A}_F$-ideal is uniquely represent able as a product of prime ideals.

Proof. It is immediate result of Theorem 5.22 and Theorem 5.29.

Example 5. 31 Let $F = \mathbb{Q}(\sqrt{10})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{10}]$. Consider $P = (2, \sqrt{10})$, $Q = (3, 1+\sqrt{10})$ and $Q' = (3, 1-\sqrt{10})$. By Proposition 5.10 P, Q, Q' are all $\mathfrak{A}_F$-ideals; moreover they are prime ideals. One can easily check that

$$(2) = P^2 \text{ and } (3) = QQ'$$

So,

$$(6) = (2)(3) = P^2 QQ'.$$

This is the unique factorization of deal (6) in $\mathfrak{A}_F$.

Definition 5.32 Let R is a Dedekind domain, and I, J are R-ideals, then

$$\gcd(I, J) = I + J$$

and

$$\text{lcm}(I, J) = I \cap J.$$

Observe that Corollary 5.28 tells us that the lcm (I, J) is actually the largest ideal contained in both I and J, whereas gcd (I, J) is the smallest ideal containing both I and J. This is because a divisor of an ideal is a larger ideal, and a multiple of an ideal means a sub-ideal. If $I = (\alpha)$, we write gcd(α, J) and lcm(α, J). Also, if $J = (\beta)$ as well, we write

$$\gcd(I, J) = \gcd(\alpha, \beta), \text{ and } \text{lcm}(I, J) = \text{lcm}(\alpha, \beta).$$

Theorem 5.33 Let R be a Dedekind domain, and let I be an R-ideal. If $\alpha \in$ is any nonzero element, there exists $\beta \in I$ such that $I = (\alpha, \beta)$ [2].

CHAPTER 6

FACTORING OF PRIME IDEALS IN EXTENSIONS

6.1 Lifting of Prime Ideals

Let F be an algebraic number field, it is extension of $\mathbb{Q}$ with degree of extension n. In chapter 5 we have seen that the ring of integers of F, denoted by $\mathfrak{A}_F$, is Dedekind domain; and it is integral closure of $\mathbb{Z}$.

Definition 6.1 Let F be an algebraic number field and $\mathfrak{A}_F$ be the ring of integers of F. Let p be a nonzero prime ideal of $\mathbb{Z}$. The lifting (also called the extension) of p to $\mathfrak{A}_F$ is the ideal $p\mathfrak{A}_F$. Although $p\mathfrak{A}_F$ need not be a prime ideal of $\mathfrak{A}_F$, we can use the fact that $\mathfrak{A}_F$ is a Dedekind domain and the unique factorization theorem to write

$$p\mathfrak{A}_F = \prod_{i=1}^{g} P_i^{e_i}$$

Where the P_i are distinct prime ideals of $\mathfrak{A}_F$ and the e_i are positive integers . On the other hand, we can start with a nonzero prime ideal Q of $\mathfrak{A}_F$ and form a prime ideal of $\mathbb{Z}$ via.

$$p = Q \cap \mathbb{Z}.$$

We say that Q lies over p, or that p is the contraction of Q to $\mathbb{Z}$.
Now suppose that we start with a nonzero prime ideal p of $\mathbb{Z}$ and lift it to $\mathfrak{A}_F$. We will show that the prime ideals $P_1, \ldots, P_g$ that appear in the prime factorization of $p\mathfrak{A}_F$ are precisely the prime ideals of $\mathfrak{A}_F$ that lie over p.

Proposition 6.2 Let Q be a nonzero prime ideal of $\mathfrak{A}_F$. Then Q appears in the prime factorization of $p\mathfrak{A}_F$ if and only if $Q \cap \mathbb{Z} = p$.

Proof. If $Q \cap \mathbb{Z} = p$, then $p \subseteq Q$, hence $p\mathfrak{A}_F \subseteq Q$ because Q is a $\mathfrak{A}_F$- ideal. So, Q divides $p\mathfrak{A}_F$. Conversely, assume that Q divides (contains) $p\mathfrak{A}_F$ Then

$$p = p \cap \mathbb{Z} \subseteq p\mathfrak{A}_F \cap \mathbb{Z} \subseteq Q \cap \mathbb{Z}.$$

But in a Dedekind domain, every nonzero prime ideal is maximal, so $p = Q \cap \mathbb{Z}$.

Definition 6.3 (Ramification and Relative Degree) Let F be an algebraic number field and $\mathfrak{A}_F$ be the ring of integers of F . Let p be a nonzero prime ideal of $\mathbb{Z}$ .Let

$$p\mathfrak{A}_F = \prod_{i=1}^{g} P_i^{e_i}$$

The positive integer e_i is called the ramification index of P_i over p(or over $\mathbb{Z}$). We say that p ramifies in $\mathfrak{A}_F$ (or in F) if $e_i > 1$ for at least one i. We will prove in a moment that $\mathfrak{A}_F/P_i$ is a finite extension of the field $\mathbb{Z}/p$. The degree f_i of this extension is called the relative degree (or the residue class degree, or the inertial degree) of P_i over p (or over $\mathbb{Z}$).

Proposition 6.4 We can identify $\mathbb{Z}/p$ as a subfield of $\mathfrak{A}_F/P_i$, and $\mathfrak{A}_F/P_i$ is a finite extension of $\mathbb{Z}/p$.

Proof. The map from $\mathbb{Z}/p$ to $\mathfrak{A}_F/P_i$ given by $a + p \to a + P_i$ is well-defined and injective, because $P = P_i \cap A$, and it is a homomorphism by direct verification. $\mathfrak{A}_F$ is a finite-dimensional vector space over $\mathbb{Z}/p$. It comletes the proof.

Theorem 6.5

$\sum_{i=1}^{g} e_i f_i = [\mathfrak{A}_F / p\mathfrak{A}_F : \mathbb{Z}/p] = n$ [16].

6.2 Norms of Ideals

Definition 6.6 Let F be an algebraic number field and $\mathfrak{A}_F$ be the ring of integers of F.The value $\left|\mathfrak{A}_F / I\right|$ for a $\mathfrak{A}_F$-ideal I is said to be norm of I, denoted by $N(I)$.

Proposition 6.7 Let α be any nonzero element of the ideal I of $\mathfrak{A}_F$, and let $m = N_F(\alpha) \in \mathbb{Z}$. Then $m \in I$ and $|\mathfrak{A}_F/m\mathfrak{A}_F| = m^n$, where $n = |F : \mathbb{Q}|$.

Proof. $m = \alpha\ \beta$ where β is a product of conjugates of α . But a conjugate of an algebraic integer is an algebraic integer. Thus $\beta \in \mathfrak{A}_F$, and since $\alpha \in I$, we have $m \in I$. Now, $\mathfrak{A}_F$ is the direct sum of n copies of $\mathbb{Z}$, hence by the first isomorphism theorem, $\mathfrak{A}_F/\mathrm{m}\mathfrak{A}_F$ is the direct sum of n copies of $\mathbb{Z}/m\mathbb{Z}$. Consequently, $|\mathfrak{A}_F/m\mathfrak{A}_F| = mn$.

Corollary 6.8 Let I be any nonzero ideal of $\mathfrak{A}_F$, then $N(I)$ is finite. Moreover, $N(I)$ divides m^n where $m = N_F(\alpha)$ for some α in I and $n = |F : \mathbb{Q}|$.

Proof. Observe that $(m) \subseteq I$, hence

$$\frac{\mathfrak{A}_F/(m)}{\mathfrak{A}_F/I} \cong I/(m).$$

Theorem 6.9 Let F be an algebraic number field and I be a nonzero $\mathfrak{A}_F$-ideal. Let $B = \{\alpha_1, \alpha_2, ..., \alpha_n\}$ be a $\mathbb{Z}$-basis for I. Then,

$$N(I) = \left(\frac{\text{disc}(B)}{\Delta_F}\right)^{1/2} \quad [2].$$

Corollary 6.10 Let $I = (\alpha)$ with $\alpha \neq 0$, then $N(I) = |N_F(\alpha)|$ [2].

Example 6.11 Let $F = \mathbb{Q}(\sqrt{10})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{10}]$. Consider $P = (2, \sqrt{10})$ and $Q = (3, 1-\sqrt{10})$. P and Q are $\mathfrak{A}_F$-ideals by Proposition 5.10. $B_1 = \{2, \sqrt{10}\}$ is a $\mathbb{Z}$-basis for P. Since $\Delta_F = 40$, then by Theorem 6.9

$$N(P) = \left(\frac{\det\begin{pmatrix} 2 & 2 \\ \sqrt{10} & -\sqrt{10} \end{pmatrix}^2}{40}\right)^{1/2} = 2.$$

And $B_2 = \{3, 1-\sqrt{10}\}$ is a $\mathbb{Z}$-basis for Q. Since $\Delta_F = 40$, then by Theorem 6.9

$$N(Q) = \left(\frac{\det\begin{pmatrix} 3 & 3 \\ 1-\sqrt{10} & 1+\sqrt{10} \end{pmatrix}^2}{40}\right)^{1/2} = 3.$$

Example 6.12 Let $F = \mathbb{Q}(\sqrt{10})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{10}]$. Consider $I = (1+\sqrt{10})$. It is clear that $N_F(1+\sqrt{10}) = -9$. So, by Corollary 6.10 $N(I) = 9$. Let us check this result by using Theorem 6.9. $B = \{1+\sqrt{10}, 10+\sqrt{10}\}$ be a $\mathbb{Z}$-basis for I. Thus,

$$N(I) = \left(\frac{\det\begin{pmatrix} 1+\sqrt{10} & 1-\sqrt{10} \\ 10+\sqrt{10} & 10-\sqrt{10} \end{pmatrix}^2}{40}\right)^{1/2} = 9.$$

Theorem 6.13 Let I and J be nonzero $\mathfrak{A}_F$-ideals , then $N(IJ) = N(I)N(J)$ [4].

Corollary 6.14 Let I be a nonzero $\mathfrak{A}_F$ ideal . If $N(I)$ is prime, then I is a prime ideal.

Proof. Suppose I is the product of two ideals I_1 and I_2. By Theorem 6.13, $N(I)=N(I_1)\,N(I_2)$, so by hypothesis, $N(I_1) = 1$ or $N(I_2) = 1$. Thus either I_1 or I_2 is a unit of $\mathfrak{A}_F$. Therefore, the prime factorization of I is I itself, in other words, I is a prime ideal.

Example 6.15 Let $F = \mathbb{Q}(\sqrt{10})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{10}]$. Consider $P = (2, \sqrt{10})$ and $Q = (3, 1-\sqrt{10})$.By Coroolary 6.14 and Example 6.11 P and Q prime $\mathfrak{A}_F$-ideals.

But, Corollary 6.14 does not say anything about primaty of the $\mathfrak{A}_F$-ideal $I = (1+\sqrt{10})$ given in the Example 6.12. It may be prime ideal may be not.

Remark 6.16 (The Norm of a Prime Ideal)

If we can compute the norm of every nonzero prime $\mathfrak{A}_F$ - ideal P, then by multiplicativity, we can calculate the norm of any nonzero ideal. Let p be the unique rational prime in P, and recall that the relative degree of P over p is $f(P) = |\mathfrak{A}_F/P : \mathbb{Z}/p\mathbb{Z}|$. Therefore

$$N(P) = \left|\mathfrak{A}_F / P\right| = p^{f(P)} \quad [2].$$

4.3 A Practical Way of Factorization

The following result, usually credited to Kummer but sometimes attributed to Dedekind, allows, under certain conditions, an efficient factorization of a rational prime in a number field.

Theorem 6.17 Let F be a number field of degree n over $\mathbb{Q}$, and assume that the ring $\mathfrak{A}_F$ of algebraic integers of F is $\mathbb{Z}[\alpha]$ for some $\alpha \in \mathfrak{A}_F$. Thus 1, α, α^2, ... , α^{n-1} form an integral basis of $\mathfrak{A}_F$. Let p be a rational prime, and let f be the minimal polynomial of α over $\mathbb{Q}$. Reduce the coefficients of f modulo p to obtain $\overline{f} \in \mathbb{Z}[X]$. Suppose that the factorization of $\overline{f}$ into irreducible polynomials over $\mathbb{F}_p$ is given by

$$\overline{f} = h_1^{e_1} \ldots h_r^r$$

Let f_i be any polynomial in $\mathbb{Z}$[X] whose reduction mod p is h_i. Then the ideal

$$Pi = (p, f_i(\alpha))$$

is prime, and the prime factorization of (p) in $\mathfrak{A}_F$ is

$$(p) = P_1^{e_1} \ldots P_r^{e_r} \quad [2].$$

Remark 6.18 (Prime Factorization in Quadratic Fields)

We consider $F = \mathbb{Q}(\sqrt{D})$, where D is a squarefree integer, and factor the ideal (p) in the ring $\mathfrak{A}_F$ of algebraic integers of F. By theorem 6.5, $\sum_{i=1}^{g} e_i f_i = 2$. So, there will be three cases:

(1) $g = 2$, $e_1 = e_2 = f_1 = f_2 = 1$. Then $(p) = P_1 P_2$, P_1 and P_2 are $\mathfrak{A}_F$-ideals and we say that p splits in F.

(2) $g = 1$, $e_1 = 1$, $f_1 = 2$. Then (p) is a prime ideal of $\mathfrak{A}_F$, and we say that p remains prime in F or that p is inert.

(3) $g = 1$, $e_1 = 2$, $f_1 = 1$. Then $(p) = P_1^2$ for some prime $\mathfrak{A}_F$ - ideal P_1, and we say that p ramifies in F.

We will examine all possibilities systematically.

(a) Assume p is an odd prime not dividing D. Then p does not divide the discriminant Δ_F, so p does not ramify.

(a1) If D is a quadratic residue (mod p), then p splits. Say $D \equiv n^2 \pmod{p}$. Then $x^2 - D$ factors mod p as $(x + n)(x - n)$, so $(p) = (p, n + \sqrt{D})(p, n - \sqrt{D})$.

(a2) If D is not a quadratic residue mod p, then $x^2 - D$ cannot be the product of two linear factors, hence $x^2 - D$ is irreducible mod p and p remains prime.

(b) Let p be any prime dividing D. Then p divides the discriminant, hence p ramifies.

Since $x^2 - D \equiv x^2 = xx \pmod{p}$, we have $(p) = (p, \sqrt{D})^2$

This takes care of all odd primes, and also $p = 2$ with D is even.

(c) Assume p = 2, D odd.

(c1) Let $D \equiv 3 \pmod 4$. Then 2 divides the discriminant $\Delta_F = 4D$, so 2 ramifies.

We have $x^2 - D \equiv (x + 1)^2 \pmod 2$, so $(2) = (2, 1 + \sqrt{D})^2$.

(c2) Let $D \equiv 1 \pmod 8$, hence $D \equiv 1 \bmod 4$.An integral basis is $\{1, (1 + \sqrt{D})/ 2\}$, and the discriminant is $\Delta_F = D$. Thus 2 does not divide Δ_F, so 2 does not ramify.

We claim that $(2) = (2, (1 + \sqrt{D}) / 2). (2, (1- \sqrt{D}) / 2)$.

To verify this note that the right side is $(2, 1 - \sqrt{D}, 1 + \sqrt{D}, (1 - D) / 4)$. This coincides with (2) because $(1 - D)/4$ is an even integer and $1 - \sqrt{D} + 1 + \sqrt{D} = 2$.

(c3) Let $D \equiv 5 \pmod 8$, hence $D \equiv 1 \bmod 4$, so $\Delta_F = D$ and 2 does not ramify.

Consider $f(x) = x^2 - x + (1 - D) / 4$ over $\mathfrak{A}_F / P$, where P is any prime ideal lying over (2). The roots of f are $(1 \pm \sqrt{D}) / 2$, so f has a root in $\mathfrak{A}_F$, hence in $\mathfrak{A}_F$/P.

But there is no root in $\mathbb{F}_2$, because $(1 - D) / 4 \equiv 1 \pmod 2$. Thus $\mathfrak{A}_F /P$ and $\mathbb{F}_2$ cannot be isomorphic. If (2) factors as Q_1Q_2, then the norm of (2) is 4, so Q_1 and Q_2 have norm 2, so the $\mathfrak{A}_F /Q_i$ are isomerphic to $\mathbb{F}_2$, which contradicts the argument just given. Therefore 2 remains prime .

Example 6.19 Let $\alpha = \sqrt[3]{2}$ and $F = \mathbb{Q}(\alpha)$. One can check that $\mathfrak{A}_F = \mathbb{Z}[\sqrt[3]{2}]$.

Obviously,

$$m_{\alpha,\mathbb{Q}}(x) = x^3 - 2 .$$

For $p = 7$, $x^3 - 2$ is irreducible moddulo 7. So, (7) $\mathfrak{A}_F$ be a $\mathfrak{A}_F$-prime ideal. In other words 7 remains prime in F or 7 is inert .

For $p = 29$, $x^3 - 2 \equiv (x+3)(x^2 + 26x - 20)$ modulo 29 where $(x^2 + 26x - 20)$ is irreducible modulo 29. So, (29) $\mathfrak{A}_F = P_1P_2$, P_1 and P_2 are $\mathfrak{A}_F$-prime ideals. $g = 2$, $e_1 = e_2 = 1$, $f_1 = 1$ and $f_2 = 2$. Thus, 29 is unramified .

For $p = 31$, $x^3 - 2 \equiv (x-4)(x-7)(x+11)$ modulo 31. So, (31) $\mathfrak{A}_F = P_1P_2P_3$, P_1, P_2 and P_3 are $\mathfrak{A}_F$-prime ideals. $g = 3$, $e_1 = e_2 = e_3 = 1$, $f_1 = f_2 = f_3 = 1$. Thus, 31 is completely split in $\mathfrak{A}_F$.

Example 6.20 Let $F = \mathbb{Q}(\sqrt{10})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{10}]$. Namely *F* is aquadratic field with *D* = 10 and $\Delta_F = 40$.

For *p* = 2; since 2 divides $\Delta_F = 40$, 2 ramifies and $(2) = (2, \sqrt{10})^2$.

For *p* = 3; since 3 does not divide $\Delta_F = 40$ and $10 \equiv 1^2 \pmod 3$, 3 splits and $(3) = (3, 1-\sqrt{10})(3, 1+\sqrt{10})$.

For *p* = 5; since 5 divides $\Delta_F = 40$, 5 ramifies and $(5) = (5, \sqrt{10})^2$.

For *p*=7; since 7 does not divide $\Delta_F = 40$ and 10 is not quadratic residu modulo 7, 7 remains prime or it is inert.

Example 6.21 Let $F = \mathbb{Q}(\sqrt{5})$, then $\mathfrak{A}_F = \mathbb{Z}[(1+\sqrt{5})/2]$. Namely *F* is aquadratic field with *D* = 5 and $\Delta_F = 5$.

For *p* = 2; since $D \equiv 5 \pmod 8$, 2 is inert.

For *p*=3; since 3 does not divide $\Delta_F = 5$ and 5 is not quadratic residu modulo 3, 3 remains prime or it is inert.

For *p* = 5; since 5 divides $\Delta_F = 5$, 5 ramifies and $(5) = (5, \sqrt{5})^2$.

For *p*=7; since 7 does not divide $\Delta_F = 5$ and 5 is not quadratic residu modulo 7, 7 remains prime or it is inert.

Example 6.22 Let $F = \mathbb{Q}(\sqrt{11})$, then $\mathfrak{A}_F = \mathbb{Z}[\sqrt{11}]$. Namely *F* is aquadratic field with *D* = 11 and $\Delta_F = 44$.

For *p* = 2; since 2 divides $\Delta_F = 44$, 2 ramifies and $(2) = (2, 1+\sqrt{11})^2$.

For *p*=3; since 3 does not divide $\Delta_F = 44$ and 11 is not quadratic residu modulo 3, 3 remains prime or it is inert.

For *p* = 5; since 5 does not divide $\Delta_F = 44$ and $11 \equiv 1^2 \pmod 5$, 5 splits and $(5) = (5, 1-\sqrt{11})(5, 1+\sqrt{11})$.

For p = 7; since 7 does not divide $\Delta_F = 44$ and $11 \equiv 2^2 \pmod 7$, 7 splits and $(7) = (7, 2-\sqrt{11})(7, 2+\sqrt{11})$.

For p = 11; since 11 divides $\Delta_F = 44$, 11 ramifies and $(11) = (11, \sqrt{11})^2$.

Example 6.22 Let $F = \mathbb{Q}(\sqrt{17})$, then $\mathfrak{A}_F = \mathbb{Z}[(1+\sqrt{17})/2]$. Namely F is aquadratic field with D = 17 and $\Delta_F = 17$.

For p = 2; since $17 \equiv 1 \pmod 8$, 2 splits and $(2) = (2, (1-\sqrt{17})/2)(2, (1+\sqrt{17})/2)$.

For p=3; since 3 does not divide $\Delta_F = 17$ and 17 is not quadratic residu modulo 3, 3 remains prime or it is inert.

For p=5; since 5 does not divide $\Delta_F = 17$ and 17 is not quadratic residu modulo 5, 5 remains prime or it is inert.

For p=7; since 7 does not divide $\Delta_F = 17$ and 17 is not quadratic residu modulo 7, 7 remains prime or it is inert.

For p=11; since 11 does not divide $\Delta_F = 17$ and 17 is not quadratic residu modulo 11, 11 remains prime or it is inert.

For p = 13; since 13 does not divide $\Delta_F = 17$ and $17 \equiv 2^2 \pmod{13}$, 13 splits and $(13) = (13, 2-\sqrt{17})(13, 2+\sqrt{17})$.

For p = 17; since 11 divides $\Delta_F = 17$, 17 ramifies and $(17) = (17, \sqrt{17})^2$.

.

CHAPTER 7

DISCUSSION AND CONCLUSION

Although, factorization was in theory for centuries, it takes place in application on some cricial areas recently. This makes it more important then before.

In this thesis, theory of factorization is studied. For application related to cryptography see [2]. In order to make an appropriate algorithm to solve Chords' Problem, factorization of polynomial is used [18]. To make algorithm more powerfull, techniques given in chapter 6 may be used. Note that, Chords' Problem is used in Bioinformatics in order to solve Digest Problem.

In this thesis, essential propositions which require to understand factorization of ideals in extensions correctly and allmost completely are given in the way of logical reasoning. It is allmost enough for the beginners to understand the subject. Moreover, there are important techniques to prove if a given domain is Euclidean or not, to test if a given prime remains prime in extension or not and some quick techniques of factoring prime ideals in quadratic extensions are given.

In this thesis, theory is based on simple extensions of $\mathbb{Q}$, generalization is not considered. Generalization is just analogy of facts in simple extensions. If one understand what is happining in simple extensions, he/she can understand facts of complex extensions and to understand what is happining in complex extensions, one should understand facts of simple extensions.

Lastly, the deficiency of the thesis is lack of techniques of factoring of prime ideals in cyclotomic extensions. In order to understand these techniques, more complicated theories such as Galaois Theory and theory of Frobenius Automorphisms are neded. So, it is required harder and longer sdudy. For more explicit information see [2], [4],[5],[19] and [20].

REFERENCES

1. Dan Saracino, Abstract Algebra, Waveland Press, Inc., Illinois,1992 .

2. Richard A. Mollin, Algebraic Number Theory, CRC Press LLC, New York, 1999.

3. Ian Stewart, David Tall, Algebraic Number Theory and Fermat's Last Theorem, A K Peters, Ltd., Natick, Massachusetts, 2002.

4. Geralg J.Janusz, Algebraic Number Fields, American Mathematical Society, 1996.

5. Jody Esmonde, M. Ram Murty, Problems In Algebraic Number Theory, Springer-Verlag, New York, 1999.

6. W.Narkiewicz, Elementary and Analytic Theory of Numbers, Polish Scientific Publishers, Warsaw,1974.

7. Tom M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York Inc. 1976.

8. M. Ram Murty, Problems in Analytic Number Theory, Springer-Verlag, New York, Inc. 2001.

9. John B. Fraleigh, A First Course In Abstract Algebra , Pearson Education Inc., London, 2003 .

10. P.B.Bhattacharya, S.K.Jain, S.R.Nagpaul, Basic Abstract Algebra, Cambridge University Press, New York,1994.

11. Thomas W. Hungerford, Abstract Algebra, Saunders College Publishing, London, 1997.

12. Kenneth H. Rosen, Elementary Number Theory and its Application, AT & T Laboratories, 2000.

13. William W. Adams, Larry Joel Goldstein, Introduction to Number Theory, Prentice-Hall, Inc. Englewood Cliffs, New Jersey, 1976.

14. Trygve Nagell, Introduction to Number Theory, Chelsea Publishing Company, New York, 1964.

15. Richard A. Mollin, Fundamental Number Theory with Applications, CRC Press LLC, New York, 1998.

16. Barış Kendirli, Lecture Notes on Algebraic Number Theory, İstanbul, 2004.

17. T.Motzkin, The Euclidean Algorithm, Bulletin of American Mathematical Society, vol.55, pp.1142-1146, 1949.

18. Alain Daurat, Yan Gerard, Maurice Nivat, The Chords' Problem, 2002.

19. Patrick Morandi, Field and Galois Theory, Springer-Verlag, New York, 1996.

20. Joseph Rotman, Galois Theory, Springer-Verlag, New York, 1998.