UNITEXT 135

$$\lim_{s\to 1^+}(s-1)\zeta_K(s)=h\frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{|d_K|}}$$

Sudesh Kaur Khanduja

A Textbook of Algebraic Number Theory

Springer

UNITEXT

La Matematica per il 3+2

Volume 135

The **UNITEXT - La Matematica per il 3+2** series is designed for undergraduate and graduate academic courses, and also includes advanced textbooks at a research level.

Originally released in Italian, the series now publishes textbooks in English addressed to students in mathematics worldwide.

Some of the most successful books in the series have evolved through several editions, adapting to the evolution of teaching curricula.

Submissions must include at least 3 sample chapters, a table of contents, and a preface outlining the aims and scope of the book, how the book fits in with the current literature, and which courses the book is suitable for.

For any further information, please contact the Editor at Springer: francesca.bonadei@springer.com

THE SERIES IS INDEXED IN SCOPUS

More information about this subseries at https://link.springer.com/bookseries/5418

Sudesh Kaur Khanduja

A Textbook of Algebraic Number Theory

Springer

Sudesh Kaur Khanduja
Department of Mathematics
Panjab University
Chandigarh, India

ISSN 2038-5714 ISSN 2532-3318 (electronic)
UNITEXT
ISSN 2038-5722 ISSN 2038-5757 (electronic)
La Matematica per il 3+2
ISBN 978-981-16-9149-2 ISBN 978-981-16-9150-8 (eBook)
https://doi.org/10.1007/978-981-16-9150-8

Mathematics Subject Classification: 11R04, 11R11, 11R16, 11R18, 11R21, 11R27, 11R29, 11R42, 11Y40

This Springer imprint is published by the registered company Springer Nature Singapore Pte Ltd.
The registered company address is: 152 Beach Road, #21-01/04 Gateway East, Singapore 189721, Singapore

To my teacher Prof. R. P. Bambah who
initiated me into Algebraic Number Theory

Preface

This book is an outcome of teaching a two-semester course on Algebraic Number Theory several times and carrying out research work for many years in this area. Our main aim is to present the core course contents of Algebraic Number Theory for post-graduate students in a comprehensive and lucid manner. We follow the classical approach of Dedekind's theory of ideals. The prerequisite for this book is basic knowledge of abstract algebra and Elementary Number Theory including the Legendre symbol, the law of quadratic reciprocity and continued fractions. Some simple results regarding infinite series and infinite products are used in the proof of Dirichlet's Class Number Formula in Chap. 9. We have tried to make the book as self-contained as possible.

Chapter 1 gives the notions of the characteristic polynomial, norm and trace together with their properties and introduces the reader to algebraic numbers and algebraic integers. Formulae for discriminant and integral bases of quadratic, pure cubic and cyclotomic fields are derived in Chap. 2. In Chap. 3, the ideals of the ring $\mathcal{O}_K$ of algebraic integers in an algebraic number field K are studied. Chapter 4 contains a proof of Dedekind's Theorem on splitting of primes and its applications. In Chap. 5, Dirichlet's Unit Theorem is proved and a method to compute units of real quadratic fields using continued fractions is also explained. Chapter 6 deals with relative extensions of algebraic number fields, and a proof of the fundamental equality involving relative index of ramification and residual degree is given. In Chap. 7, the notions of relative different and relative discriminant are introduced and their properties are studied. This chapter culminates with the proof of Dedekind's Theorem on ramified primes. Chapter 8 establishes the finiteness of class number and proves Minkowski's Convex Body Theorem. A slight variation of this theorem is applied to obtain Minkowski's bound which has been used for computing class number of some algebraic number fields. Hermite's Theorem on discriminant has also been proved in this chapter. A self-contained proof of the first case of Fermat's Last Theorem for regular primes is also given in this chapter. In Chap. 9, we prove Dirichlet's Class Number Formula and give some of its applications. In Chap. 10, a simplified version of Dirichlet's Class Number Formula is derived for cyclotomic and quadratic fields using numerical characters and L-functions. We also deduce

Dirichlet's Theorem for primes in arithmetic progressions. At the end, an appendix has been added which contains the basics of field theory, the fundamental theorem of the Galois theory and a new proof of the classical Eisenstein-Dumas Irreducibility Criterion which has been published in 2020. Historical comments are added at several places in the book and a couple of open problems are also stated in certain remarks. Every chapter culminates with a set of exercises. At the end of the book, we provide "Hints and Answers to Selected Exercises" where answers to all numerical exercises are given, and moreover, elaborate hints to challenging exercises are also given.

We also aim to arouse readers' interest in research in Algebraic Number Theory. For this purpose, we have cited some recent results which are directly related to the basic results proved in the book and mentioned a few research problems arising out of these results together with the progress made in the direction of each problem. For example, in Chap. 2, we have remarked that a formula for the discriminant of nth degree fields of the type $\mathbb{Q}(a^{1/n})$ involving only the prime powers dividing a and n with a, n coprime or a squarefree, was given in 2017; an explicit integral basis for such fields has been constructed in 2020 but the problem is still open when a, n are arbitrary. Similarly, in Chap. 4, we introduce the reader to the simple criterion known as the Dedekind Criterion proved in 1878 which gives a necessary and sufficient condition on the minimal polynomial of θ over $\mathbb{Q}$ for a prime p to divide the group index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, where $\mathcal{O}_K$ is the ring of algebraic integers of an algebraic number field $K = \mathbb{Q}(\theta)$; this index is usually called the index of θ. We also refer to a result proved in 2017 which characterizes all primes dividing the index of θ when $K = \mathbb{Q}(\theta)$ with θ satisfying an irreducible trinomial $F(X) = X^n + aX^m + b$ belonging to $\mathbb{Z}[X]$. However, it is an open problem to determine the exact power of a prime p dividing the index of θ even in the simpler case when $F(X) = X^n + aX + b$ for $n \geq 7$; this problem is completely solved for all choices of a, b when $n \leq 6$ and solved for many choices of a, b when n is prime power.

It is hoped that this book will be of great use to students and researchers. I would appreciate receiving comments and suggestions for improvement of the book.

Chandigarh, India Sudesh Kaur Khanduja

Acknowledgements

It is a pleasure to express my gratitude to my students Amrit Pal Singh Virk, Anuj Jakhar, Neeraj Sangwan and Mahinshi Singla who helped me in typing the manuscript of the book. Words fail me to express my gratitude to Professor Sudhir Ghorpade from IIT Bombay with whom I had several discussions on the contents of the book and who gave valuable suggestions for the improvement of exposition. I am also thankful to my colleagues Professor Dinesh Khurana and Dr. Yashonidhi Pandey who proofread some parts of the book. My special thanks to Miss Mahinshi Singla who proofread the whole manuscript and corrected the misprints. I am highly grateful to my alma mater (Department of Mathematics, Panjab University Chandigarh) where I learnt Algebraic Number Theory from my teachers Prof. Ram Prakash Bambah and the late Prof. Indar Singh Luthar. Particular thanks to my family members for their constant inspiration and support. Thanks are also due to IISER Mohali for providing me necessary facilities and a congenial atmosphere to carry out this work. The financial assistance by the Indian National Science Academy in the form of senior scientistship is duly acknowledged. Finally, I would like to thank the publishers for their cooperation in the realization of the book.

Sudesh Kaur Khanduja
Emeritus Professor, Department of
Mathematics, Panjab University
Chandigarh, Chandigarh, India

INSA Honorary Scientist, IISER
Mohali, Punjab, India

Contents

About the Author

Sudesh Kaur Khanduja is Emeritus Professor at the Department of Mathematics, Panjab University, Chandigarh, India, and INSA Honorary Scientist at the Indian Institute of Science Education and Research (IISER) Mohali, India. A PhD and master's degree from Panjab University, India, her primary research interests are in algebraic number theory and valuation theory. With over 40 years of teaching experience at Panjab University and IISER Mohali, she has guided 12 PhD students and published over 90 research papers in reputed international journals.

A fellow of The World Academy of Sciences, the Indian Academy of Sciences, the National Academy of Sciences, India, and the Indian National Science Academy, she was awarded the Professor V.V. Narlikar Memorial Lecture Award of INSA in 2015. She has visited and delivered lectures at various universities including Ohio State University, Columbus; University of Missouri, Columbia; University of Michigan, Ann Arbor; University of Saskatchewan, Canada; Nihon University, Japan; State University of Campinas, Brazil, and University of Konstanz, Germany.

Notation

$\mathbb{Z}$	The set of integers (also called rational integers)
$\mathbb{Q}$	The set of rational numbers
$\mathbb{R}$	The set of real numbers
$\mathbb{C}$	The set of complex numbers
$\mathbb{Z}^n$	The set of n-tuples with integer entries
$\mathbb{R}^n$	The set of n-tuples with entries from $\mathbb{R}$
$\|\|x\|\|$	The norm $\sqrt{x_1^2 + \cdots + x_n^2}$ of a vector $x = (x_1, \ldots, x_n)$ in $\mathbb{R}^n$
$\underline{0}$	Zero Vector in $\mathbb{R}^n$
$\mathrm{vol}(S)$	Volume of a subset S of $\mathbb{R}^n$
ι	iota $= \sqrt{-1}$
$\bar{z}$	Complex conjugate of a complex number z
$Re(z)$	Real part of a complex number z
$Im(z)$	Imaginary part of a complex number z
$\mathbb{Z}[\alpha_1, \ldots, \alpha_n]$	The smallest subring of $\mathbb{C}$ containing $\mathbb{Z}$ and $\alpha_1, \ldots, \alpha_n$
$\langle a_1, \ldots, a_n \rangle$	The ideal generated by elements $a_1, \ldots, a_n$ of a commutative ring
$\deg h(X)$	degree of the polynomial $h(X)$
$[G : H]$	The index of a subgroup H of a group G in G
$[L : K]$	The degree of a field extension L/K
$N_{L/K}(\alpha)$	The norm of α w.r.t. L/K
$Tr_{L/K}(\alpha)$	The trace of α w.r.t. L/K
$\mathrm{Gal}(L/K)$	The Galois group of a Galois extension L/K
$I_{n\times n}$	The $n \times n$ identity matrix
A^t	Transpose of a matrix A
det A or $\|A\|$	Determinant of a matrix A
$(a_{ij})_{i,j}$	The matrix whose (i, j)th entry is a_{ij}
$\|S\|$	Cardinality of a set S
S_n	Symmetric group of degree n
A_n	Alternating group of degree n
$\ker(\psi)$	Kernel of map ψ

$\psi\|_H$	map ψ restricted to H
PID	Principal Ideal Domain
UFD	Unique Factorization Domain
$R^\times$	The group of units of a commutative ring R with identity
gcd	Greatest common divisor
lcm	Least common multiple
(a, b)	gcd of a and b
$\mathcal{O}_K$	The ring of algebraic integers of an algebraic number field K
d_K	The discriminant of an algebraic number field K
h_K	The class number of K
R_K	The Regulator of K
$\mathrm{ind}\,\theta$	index of θ
$N(I)$	The absolute norm of a non-zero ideal I of $\mathcal{O}_K$
$N_{K'/K}(I')$	The relative norm of a non-zero ideal I' of $\mathcal{O}_{K'}$
$D_{K'/K}(w_1, \ldots, w_n)$	The Discriminant of a basis $\{w_1, \ldots, w_n\}$ of K'/K
$\phi(n)$	Euler totient function evaluated at a number n
$\emptyset$	The empty set
$\lfloor \lambda \rfloor$	Greatest integer not exceeding a real number λ
$\left(\frac{a}{p}\right)$	Legendre symbol where p is an odd prime
$\left(\frac{a}{2}\right)$	Kronecker symbol where $a \equiv 0$ or $1 \pmod 4$
$\left(\frac{m}{n}\right)$	Jacobi symbol defined for integers m, n with n odd
$\left(\frac{a}{n}\right)$	Jacobi-Kronecker symbol defined for $a \equiv 0$ or $1 \pmod 4$ and n non-zero.

Chapter 1
Algebraic Integers, Norm and Trace

1.1 Historical Background

The origin of Algebraic Number theory is attributed to Fermat's Last Theorem which was conjectured by a French mathematician Pierre de Fermat in 1637. It states that the equation $X^n + Y^n = Z^n$ has no solution in non-zero integers x, y, z, when n is an integer greater than 2. Fermat himself proved the case $n = 4$ of the theorem (see [Ded2, 0.3.1]). If $n = pm$, then the relation $x^n + y^n = z^n$ implies that $(x^m)^p + (y^m)^p = (z^m)^p$ which gives a solution of the equation $X^p + Y^p = Z^p$. Since any integer greater than 2 is either a multiple of 4 or has an odd prime factor, for proving Fermat's Last Theorem it is enough to show that $X^p + Y^p = Z^p$ has no solution in non-zero integers for all odd prime exponents p. This celebrated theorem motivated a general study of the theory of algebraic numbers. History reveals that in 1770, Leonhard Euler used the field $\mathbb{Q}(\omega)$ with ω a complex cube root of unity to prove Fermat's Last Theorem for the case $n = 3$ (cf. [Ded2, 0.5.1]). The first major step towards a general proof of Fermat's Last Theorem was by a French woman[1] Sophie Germain. In a letter dated May 12, 1819 to the greatest number theorist of that time Carl Friedrich Gauss, she explained her idea of the proof. She had proved that if p is an odd prime such that $q = 2kp + 1$ is also a prime for some number k satisfying the following conditions: (i) $x^p \equiv p \pmod{q}$ has no solution (ii) the set of pth powers modulo q contains no consecutive non-zero integers, then the first case of Fermat's Last Theorem holds for the exponent p, i.e., the equation $X^p + Y^p = Z^p$ has no

[1] It may be pointed out that women were not allowed to enroll themselves as members of École Polytechnique which was opened in Paris in 1794 when Germain was 18 years old. Germain managed to obtain lecture notes from this institute under the pseudonym Monsieur Le Blanc. A couple of months later, the supervisor of the course Joseph-Louis Lagrange could no longer ignore the brilliance of Monsieur Le Blanc's answer sheets and Germain was forced to reveal her identity. Lagrange recognised her abilities and became her mentor. She wrote several letters discussing mathematical problems to the well known number theorist Carl Friedrich Gauss under the same pseudonym.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_1

solution in integers x, y, z with p not dividing xyz. In particular, for an odd prime p if $2p + 1$ is also a prime, then the first case of Fermat's Last Theorem holds for the exponent p. In this way she was able to show that the same holds for all odd primes $p \leq 197$. In 1825, her method claimed its first complete success when the famous mathematicians Peter Gustav Lejeune Dirichlet and Adrien-Marie Legendre (one German and the other French) working independently were able to prove the case $n = 5$ of Fermat's Last Theorem. In fact, they acknowledged that their proofs were based on the method of Sophie Germain. Fourteen years later, the French mathematician Gabriel Lamé proved the case $n = 7$ of the theorem using Germain's results. Her results related to Fermat's Last Theorem remained most important until the contribution of Eduard Kummer in 1847.

The German mathematician Ernst Eduard Kummer contributed a lot towards the subject. While trying to prove Fermat's Last Theorem, he was studying arithmetic of the ring $\mathbb{Z}[\zeta_p]$ where ζ_p is a primitive pth root of unity, p prime and realized that unique factorization into prime elements may not hold in such rings. While tackling the above problem, he made a remarkable achievement discovering that the unique factorization property could be salvaged if we replace role of elements of $\mathbb{Z}[\zeta_p]$ by what he called ideal numbers. Richard Dedekind extended Kummer's work by using ideals in place of ideal numbers; in fact the concept of an ideal of a ring was thus born in the work of Kummer and Dedekind. By using the theory of ideal numbers, Kummer proved Fermat's Last Theorem for a wide range of prime exponents - the so called 'regular' primes.[2] He also evolved a powerful approach with applications to many other problems. In fact, a large part of classical number theory can be expressed in the framework of Algebraic Number Theory. This theory now has a wealth of applications to several topics in mathematics such as Diophantine equations, cryptography, factorizations into prime ideals, primality testing etc. It is this wider link that led to the final proof of Fermat's Last Theorem. After seven years of single minded efforts, an English mathematician Andrew John Wiles completed a proof of Fermat's Last Theorem by May 1993. He outlined the proof in three lectures in a conference held at Sir Issac Newton Institute in Cambridge in June 1993. The title of Wiles' lecture series was "Modular forms, Elliptic curves and Galois representations". At the end of his third lecture on 23rd June 1993, when he concluded Fermat's Last Theorem, he became the most famous mathematician in the world. In September 1993, Nick Katz, a referee of the paper containing this proof noticed a gap in one of the arguments. Wiles corrected the proof with the help of his former student Richard Taylor and the revised proof was published in 1995 (cf. [Wil, Ta-Wi]). In the words of Cambridge Professor John Coates (Ph.D. supervisor of Andrew Wiles) "A proof of Fermat's Last Theorem is a great intellectual triumph and one shouldn't lose sight of the fact that it has revolutionised number theory in one fell swoop. For me the charm and beauty of Andrew's work has been that it has been a tremendous step for algebraic number theory". For solving this problem, he was knighted in 2000 and

[2] A prime p is said to be regular if the class number of the field $\mathbb{Q}(e^{2\pi\iota/p})$ is not divisible by p.

received other awards such as 2016 Abel[3] prize. A detailed outline of Wiles' proof along with all other necessary preliminary results is fairly well explained in [St-Ta]. Simon Singh in his book "Fermat's Last Theorem" [Sin] takes us through a journey of more than 330 years of the struggle of Math world to prove this theorem. His narrative fold is very interesting which includes Pythagoras, Euclid, Fermat, Euler, Germain, Gauss, Cauchy, Lamé, Kummer, Taniyama, Shimura, Ribet, Faltings[4] and eventually Andrew Wiles whose legacy will remain as long as Mathematics rules our lives.

1.2 Algebraic Numbers and Algebraic Integers

We begin by introducing some basic notions of algebraic number theory.
Definition A complex number α is said to be an algebraic number if α is a root of a non-zero polynomial with coefficients from the field $\mathbb{Q}$ of rational numbers. A complex number which is not an algebraic number is called a transcendental number.

Note that if α is an algebraic number, then the degree of the extension $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$ is finite and vice versa.

Theorem 1.1 *The set of all algebraic numbers is a subfield of* $\mathbb{C}$, *the field of complex numbers.*

Proof Suppose that α, β are algebraic numbers with $\beta \neq 0$. We have to show that $\alpha \pm \beta$, $\alpha\beta$ and $\dfrac{\alpha}{\beta}$ are algebraic numbers. The extensions $\mathbb{Q}(\alpha)/\mathbb{Q}$ and $\mathbb{Q}(\beta)/\mathbb{Q}$ are finite, say of degree m and n respectively. Since

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)] \leq [\mathbb{Q}(\beta) : \mathbb{Q}] = n,$$

it follows from Tower theorem (cf. Theorem A.1) that

$$[\mathbb{Q}(\alpha, \beta) : \mathbb{Q}] = [\mathbb{Q}(\alpha, \beta) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] \leq mn.$$

As the elements $\alpha \pm \beta$, $\alpha\beta$ and $\dfrac{\alpha}{\beta}$ belong to $\mathbb{Q}(\alpha, \beta)$, therefore the degree of the extension obtained by adjoining any of these elements to $\mathbb{Q}$ is finite and hence the theorem is proved. □

[3] This prize is named after the Norwegian Mathematician Niels Henrik Abel (1802-1829) and directly modeled after the Nobel Prize. It comes with a monetary award of 7.5 million Norwegian Kroner.

[4] Gerd Faltings has been closely linked with the work leading to the final proof of Fermat's Last Theorem by Andrew Wiles. In 1983, he proved that for every $n > 2$, there are at most a finite number of coprime integers x, y, z with $x^n + y^n = z^n$. In 1986, he received the highest honour that a young mathematician can receive when he was awarded a Fields Medal at the International Congress of Mathematicians at Berkeley.

Theorem 1.2 *The field $\mathbb{A}$ of all algebraic numbers is a countable set.*

Proof We know that a complex number α is an algebraic number if and only if it is a root of a non-zero polynomial with coefficients from the ring $\mathbb{Z}$ of integers. For a non-constant polynomial $f(X) = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0$ belonging to $\mathbb{Z}[X]$, we define the rank of $f(X)$ by

$$\text{rank}(f) = n + |a_n| + |a_{n-1}| + \cdots + |a_0|;$$

note that $\text{rank}(f) \geq 2$. Also observe that for any given positive integer s, the number of polynomials with coefficients from $\mathbb{Z}$ having rank s is finite. Consequently if P_s denotes the set of all those algebraic numbers which are roots of polynomials with integer coefficients having rank s, then P_s is a finite set. Since $\mathbb{A} = \bigcup_{s=2}^{\infty} P_s$ and countable union of finite sets is countable, it follows that $\mathbb{A}$ is countable. □

Remark 1.3 The above theorem implies that the set of all transcendental numbers is uncountable. It was Joseph Liouville who first constructed in 1853 a large number of transcendental numbers by proving that real algebraic numbers cannot be too well approximated by rationals.[5] However the question whether some familiar real numbers were transcendental still persisted. The first success in this direction was by Charles Hermite. In 1873, Hermite proved that e is transcendental and in 1882 Ferdinand Lindemann proved the transcendence of π; in fact he proved that for any non-zero algebraic number α, e^α is transcendental, which implies that π is transcendental because $e^{\pi\iota} = -1$ is algebraic. In 1934, working independently Alexander Gelfond and Theodor Schneider proved that if α, β are algebraic numbers (real or complex) with $\alpha \neq 0, 1$ and β irrational, then each value of α^β is transcendental. This answered in affirmative the question raised by David Hilbert, whether $2^{\sqrt{2}}$ is transcendental.

Definition A complex number α is said to be an algebraic integer if α is a root of a monic polynomial with integer coefficients. To avoid confusion, elements of $\mathbb{Z}$ will sometimes be called rational integers and a prime number will sometimes be referred to as a rational prime.

Note that $\sqrt{2}$ is an algebraic integer but $1/\sqrt{2}$ is not in view of the following theorem.

Theorem 1.4 *A complex number α is an algebraic integer if and only if the minimal polynomial of α over $\mathbb{Q}$ has all its coefficients in $\mathbb{Z}$.*

Proof Suppose that α is an algebraic integer and $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ is a monic polynomial with coefficients in $\mathbb{Z}$ of which α is a root. We can write $f(X) = f_1(X)f_2(X)\cdots f_r(X)$, where each $f_i(X)$ belonging to $\mathbb{Q}[X]$ is irreducible. For $1 \leq i \leq r$, write

[5] For precise statement of Liouville's Theorem and its applications, see Sect. 3.2 of [Es-Mu].

$$f_i(X) = \frac{d_i}{b_i} g_i(X), \quad d_i, b_i \in \mathbb{Z}^+,$$

where $g_i(X) \in \mathbb{Z}[X]$ is primitive.[6] Then

$$b_1 b_2 \cdots b_r f(X) = d_1 d_2 \cdots d_r g_1(X) g_2(X) \cdots g_r(X).$$

Since product of primitive polynomials is primitive by Gauss' lemma, on taking content, the above equation implies that $b_1 b_2 \cdots b_r = d_1 d_2 \cdots d_r$. In view of the fact that $f(X)$ is monic, the equality $f(X) = g_1(X) g_2(X) \cdots g_r(X)$ shows that the leading coefficient of each $g_i(X)$ belongs to $\{+1, -1\}$. Recall that α is a root of $f(X)$, so $g_i(\alpha) = 0$ for some i. But $g_i(X)$ is irreducible over $\mathbb{Q}$ and has coefficients in $\mathbb{Z}$ with leading coefficient ± 1. Therefore the minimal polynomial of α over $\mathbb{Q}$ is $\pm g_i(X)$, which proves the desired assertion. The converse part is trivial. □

The following theorem gives some more characterizations of an algebraic integer.

Theorem 1.5 *For a complex number α, the following statements are equivalent:*

(i) *α is an algebraic integer.*
(ii) *The subring $\mathbb{Z}[\alpha]$ of $\mathbb{C}$ generated by $\mathbb{Z}$ and α is a finitely generated $\mathbb{Z}$-module.*
(iii) *There exists a non-zero finitely generated $\mathbb{Z}$-submodule M of $\mathbb{C}$ such that $\alpha M \subseteq M$.*

Proof (i) $\Longrightarrow$ (ii). Let $g(X) \in \mathbb{Z}[X]$ be a monic polynomial satisfied by α. Let $h(\alpha) \in \mathbb{Z}[\alpha]$ be any element with $h(X)$ belonging to $\mathbb{Z}[X]$. By division algorithm, we can write $h(X) = g(X)q(X) + r(X)$ where $q(X), r(X) \in \mathbb{Z}[X]$ and $\deg r(X) < \deg g(X) = n$ (say). So $h(\alpha) = g(\alpha)q(\alpha) + r(\alpha) = r(\alpha)$, which shows that $h(\alpha)$ is a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ with coefficients from $\mathbb{Z}$. Thus $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a system of generators of $\mathbb{Z}[\alpha]$ as $\mathbb{Z}$-module.
(ii) $\Longrightarrow$ (iii) is trivial.
(iii) $\Longrightarrow$ (i). Let $\{w_1, \ldots, w_n\}$ be a system of generators of a non-zero finitely generated $\mathbb{Z}$-module $M \subseteq \mathbb{C}$ such that $\alpha M \subseteq M$. By hypothesis, $\alpha w_i \in M$ for each i. So there exist integers a_{ij} such that

$$\alpha w_i = a_{i1} w_1 + \cdots + a_{in} w_n, \ 1 \leq i \leq n.$$

On denoting the $n \times n$ matrix $(a_{ij})_{i,j}$ by A and the identity matrix by I, the above n equations can be rewritten as

$$(\alpha I - A) \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}.$$

[6] The content of a polynomial $f(X) \in \mathbb{Z}[X]$ is the gcd of its coefficients; $f(X)$ is said to be primitive if its content is 1.

Multiplying the above equation on the left by the transpose of the cofactor matrix of $(\alpha I - A)$, we obtain

$$\det(\alpha I - A)\begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{1.1}$$

Since $\{w_1, w_2, \ldots, w_n\}$ generates M, (1.1) implies that $\det(\alpha I - A)M = \{0\}$. As M is a non-zero submodule of $\mathbb{C}$, we conclude that $\det(\alpha I - A) = 0$ which proves that α satisfies the monic polynomial $\det(XI - A)$ with coefficients from $\mathbb{Z}$. □

The following theorem relates the sets of algebraic numbers and algebraic integers.

Theorem 1.6 *(i) The set of all algebraic integers is a subring of the field of all algebraic numbers.*

(ii) If ξ is an algebraic number, then there exists an integer $c \neq 0$ such that $c\xi$ is an algebraic integer.

(iii) The field of algebraic numbers is the quotient field of the ring of algebraic integers.

Proof (i) Suppose that α and β are algebraic integers which satisfy monic polynomials having degrees m and n over $\mathbb{Z}$. We have to prove that $\alpha - \beta, \alpha\beta$ are algebraic integers. As shown in the proof of the previous theorem, we have

$$\mathbb{Z}[\alpha] = \mathbb{Z} + \mathbb{Z}\alpha + \cdots + \mathbb{Z}\alpha^{m-1}$$

and

$$\mathbb{Z}[\beta] = \mathbb{Z} + \mathbb{Z}\beta + \cdots + \mathbb{Z}\beta^{n-1}.$$

Therefore

$$\mathbb{Z}[\alpha, \beta] = \sum_{i=0}^{m-1}\sum_{j=0}^{n-1} \mathbb{Z}\alpha^i\beta^j;$$

so $\mathbb{Z}[\alpha, \beta]$ is a finitely generated $\mathbb{Z}$-module. Since $(\alpha - \beta)\mathbb{Z}[\alpha, \beta] \subseteq \mathbb{Z}[\alpha, \beta]$, it follows from assertion (iii) of the previous theorem that $\alpha - \beta$ is an algebraic integer. Arguing similarly, we see that $\alpha\beta$ is an algebraic integer.

(ii) Since ξ is an algebraic number, it satisfies a polynomial $\frac{a_0}{b_0}X^s + \frac{a_1}{b_1}X^{s-1} + \cdots + \frac{a_s}{b_s}$ with a_i, b_i integers, a_0 non-zero. Clearing the denominators, we see that

$$c_0\xi^s + c_1\xi^{s-1} + \cdots + c_s = 0 \tag{1.2}$$

for some c_i's in $\mathbb{Z}$. Multiplying (1.2) by c_0^{s-1}, we have

$$(c_0\xi)^s + c_1(c_0\xi)^{s-1} + \cdots + c_s c_0^{s-1} = 0,$$

which shows that $c_0\xi$ satisfies the monic polynomial $X^s + c_1X^{s-1} + \cdots + c_s c_0^{s-1}$ with integral coefficients. Hence (ii) is proved. Assertion (iii) follows from (ii). □

Definition A subfield K of $\mathbb{C}$ is called an algebraic number field if K is a finite extension of $\mathbb{Q}$.
Notation For an algebraic number field K, we shall denote by $\mathcal{O}_K$ the set consisting of all algebraic integers belonging to K. In view of Theorem 1.6, $\mathcal{O}_K$ is a subring of K having quotient field K.

The following theorem gives an important property of the ring of algebraic integers.

Theorem 1.7 *If a complex number α is a root of a monic polynomial whose coefficients are algebraic integers, then α is an algebraic integer.*

Proof Let α be a root of the polynomial $P(X) = X^m + \alpha_1X^{m-1} + \cdots + \alpha_m$ of degree m, where each α_i is an algebraic integer. Suppose that α_i satisfies a monic polynomial over $\mathbb{Z}$ of degree n_i for $1 \le i \le m$. Then as shown in the proof of Theorem 1.5, we have

$$\mathbb{Z}[\alpha_i] = \mathbb{Z} + \mathbb{Z}\alpha_i + \cdots + \mathbb{Z}\alpha_i^{n_i-1}, \quad 1 \le i \le m.$$

Therefore

$$\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_m] = \sum_{j_1=0}^{n_1-1} \sum_{j_2=0}^{n_2-1} \cdots \sum_{j_m=0}^{n_m-1} \mathbb{Z}\alpha_1^{j_1}\alpha_2^{j_2} \cdots \alpha_m^{j_m}. \tag{1.3}$$

Note that α satisfies the monic polynomial $P(X)$ with coefficients from the ring $\mathbb{Z}[\alpha_1, \alpha_2, \ldots, \alpha_m] = R$ (say). Therefore arguing as in the first paragraph of the proof of Theorem 1.5, we see that

$$R[\alpha] = R + R\alpha + \cdots + R\alpha^{m-1}.$$

It now follows from (1.3) and the above equation that

$$R[\alpha] = \sum_{j=0}^{m-1} \sum_{j_1=0}^{n_1-1} \cdots \sum_{j_m=0}^{n_m-1} \mathbb{Z}\alpha_1^{j_1} \cdots \alpha_m^{j_m}\alpha^j.$$

Thus $R[\alpha]$ is a finitely generated $\mathbb{Z}$-module with $\alpha R[\alpha] \subseteq R[\alpha]$. Therefore by Theorem 1.5(iii), α is an algebraic integer. □

The next definition extends the notion of an algebraic integer.

Definition Let R be an integral domain with quotient field F and let F' be an extension of F. We say that α belonging to F' is integral over R if α satisfies a monic polynomial with coefficients from R.

Arguing as for the proof of Theorem 1.5, the following theorem can be easily proved.

Theorem 1.8 *Let α, R, F and F' be as in the above definition. Then the following statements are equivalent:*

(i) *α is integral over R.*
(ii) *$R[\alpha]$ is a finitely generated R-module.*
(iii) *There exists a non-zero finitely generated R-submodule M of F' such that $\alpha M \subseteq M$.*

The theorem stated below can be proved similarly as Theorem 1.6.

Theorem 1.9 *Let R be an integral domain with quotient field F and let F' be an extension of F. The following hold:*

(i) *The set of all elements of F' which are integral over R is a subring of F'.*
(ii) *If ξ belonging to F' is algebraic over F, then there exists a non-zero element r belonging to R such that $r\xi$ is integral over R.*
(iii) *If F'/F is an algebraic extension, then the quotient field of R' is F', where R' is the set of those elements of F' which are integral over R. The ring R' is called the integral closure of R in F'.*

Definition An integral domain R is said to be integrally closed if the integral closure of R in its quotient field coincides with R.

The following corollary is an immediate consequence of Theorems 1.6 and 1.7.

Corollary 1.10 *For an algebraic number field K, if $\mathcal{O}_K$ denotes the ring of algebraic integers of K, then $\mathcal{O}_K$ is an integrally closed domain with quotient field K.*

It may be pointed out that the analogue of Theorem 1.4 does not hold for an arbitrary integral domain, i.e., if R is an integral domain with quotient field F and α is an element of an extension of F such that α is integral over R, then the minimal polynomial of α over F may not have coefficients in R. For example, if $R = \mathbb{Z}[\sqrt{5}]$ and $\alpha = \dfrac{1+\sqrt{5}}{2}$, then α being a root of the polynomial $X^2 - X - 1$ is integral over R, but the minimal polynomial of α over F is $X - \alpha$, which does not belong to $R[X]$. The following simple lemma shows that the analogue of Theorem 1.4 holds for integrally closed domains.

Lemma 1.11 *If R is an integrally closed domain with quotient field F and α is an element of an extension of F such that α is integral over R, then the minimal polynomial of α over F has coefficients in R.*

Proof Let $f(X)$ be a monic polynomial belonging to $R[X]$ of which α is a root and $g(X)$ be the minimal polynomial of α over F. Since $g(X)$ divides $f(X)$, each root of $g(X)$ is integral over R. So the coefficients of $g(X)$, being elementary symmetric functions of the roots of $g(X)$, are also integral over R in view of Theorem 1.9(i). The lemma now follows as $g(X) \in F[X]$ and R is an integrally closed domain. □

1.3 Norm and Trace

In this section, the notions of norm and trace[7] are introduced and some important results related to these are proved which are used in the subsequent chapters.

Definition Let K/F be a finite extension of fields, then K is a finite-dimensional vector space over F. For α belonging to K, consider the F-linear transformation T_α of K defined by $T_\alpha(\xi) = \alpha\xi$ for every $\xi \in K$. The characteristic polynomial of this linear transformation is called the characteristic polynomial of α relative to the extension K/F. Thus if $\{v_1, v_2, \ldots, v_n\}$ is a (vector space) basis of the extension K/F and $\alpha v_i = \sum_{j=1}^{n} a_{ij} v_j$, $a_{ij} \in F$, then the characteristic polynomial of α relative to K/F is determinant of the matrix $(XI - A)$, where $A = (a_{ij})_{i,j}$ and I is the $n \times n$ identity matrix.

Remark 1.12 With notations as in the above definition, it may be pointed out that the characteristic polynomial of α relative to K/F is independent of the choice of the basis $\{v_1, v_2, \ldots, v_n\}$ of K/F. If $\{v_1', v_2', \ldots, v_n'\}$ is another basis of K/F, then the matrix $B = (b_{ij})_{i,j}$ of the linear transformation T_α with respect to $\{v_1', v_2', \ldots, v_n'\}$ defined by $\alpha v_i' = \sum_{j=1}^{n} b_{ij} v_j'$ is similar to the matrix A. In fact, $B = PAP^{-1}$, where P is the transition matrix from $\{v_1, v_2, \ldots, v_n\}$ to $\{v_1', v_2', \ldots, v_n'\}$, because

$$\begin{bmatrix} \alpha v_1 \\ \alpha v_2 \\ \vdots \\ \alpha v_n \end{bmatrix} = A \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}, \begin{bmatrix} \alpha v_1' \\ \alpha v_2' \\ \vdots \\ \alpha v_n' \end{bmatrix} = B \begin{bmatrix} v_1' \\ v_2' \\ \vdots \\ v_n' \end{bmatrix}, \begin{bmatrix} v_1' \\ v_2' \\ \vdots \\ v_n' \end{bmatrix} = P \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix}$$

and hence

[7] The definitions of norm and trace were first given by Richard Dedekind in his book *Über die Theorie der ganzen algebraischen Zahlen,* published in 1879. Its English translation is now available with the title *Theory of Algebraic Integers* (cf. [Ded2]).

$$\begin{bmatrix} \alpha v_1' \\ \alpha v_2' \\ \vdots \\ \alpha v_n' \end{bmatrix} = P \begin{bmatrix} \alpha v_1 \\ \alpha v_2 \\ \vdots \\ \alpha v_n \end{bmatrix} = PA \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{bmatrix} = PAP^{-1} \begin{bmatrix} v_1' \\ v_2' \\ \vdots \\ v_n' \end{bmatrix}.$$

which shows that $B = PAP^{-1}$.

Definition Let K/F be a finite extension of fields. For an element α of K, let T_α denote the F-linear transformation of K defined by $T_\alpha(\xi) = \alpha\xi$ for all $\xi \in K$. Let A be the matrix of T_α with respect to a fixed basis $\{v_1, v_2, \ldots, v_n\}$ of K/F. The norm and trace of α with respect to K/F are defined to be the determinant of A and the trace of A; these will be denoted by $N_{K/F}(\alpha)$, $Tr_{K/F}(\alpha)$ respectively. In view of Remark 1.12, these are independent of the choice of a basis of K/F.

Some Simple Properties of Norm and Trace

Let K be an extension of degree n of a field F. Let α, β be in K and $a \in F$. Then the following hold:

(i) $Tr_{K/F}(a) = na$ and $N_{K/F}(a) = a^n$.
(ii) $Tr_{K/F}(\alpha + \beta) = Tr_{K/F}(\alpha) + Tr_{K/F}(\beta)$.
(iii) $N_{K/F}(\alpha\beta) = N_{K/F}(\alpha)N_{K/F}(\beta)$.

Proof The first two assertions follow immediately from the definition of norm and trace. We prove (iii). For an element α belonging to K, let T_α be as in the above definition and $M(T_\alpha)$ denote its matrix with respect to a fixed basis $\{v_1, v_2, \ldots, v_n\}$ of K/F. Note that $T_{\alpha\beta} = T_\alpha \circ T_\beta$. Therefore

$$M(T_{\alpha\beta}) = M(T_\alpha \circ T_\beta) = M(T_\beta)M(T_\alpha).$$

Consequently

$$N_{K/F}(\alpha\beta) = \det(M(T_{\alpha\beta})) = \det(M(T_\beta)M(T_\alpha)) = N_{K/F}(\alpha)N_{K/F}(\beta)$$

as desired. □

Remark 1.13 For a finite extension K/F, the mapping $\alpha \mapsto N_{K/F}(\alpha)$ is a homomorphism of the multiplicative group $K^\times$ consisting of non-zero elements of the field K into the multiplicative group $F^\times$ and the mapping $\alpha \mapsto Tr_{K/F}(\alpha)$ is an F-linear functional on K.

The following lemma will be used in the proof of the next theorem.

Lemma 1.14 *Let* $B_n = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-2} & -c_{n-1} \end{pmatrix}$.

Then the characteristic polynomial of the matrix [8] B_n *is* $f(X) = c_0 + c_1 X + \cdots + c_{n-1}X^{n-1} + X^n$.

Proof We prove the lemma by induction on n. For $n = 2$, clearly

$$\det(XI - B_2) = \begin{vmatrix} X & -1 \\ c_0 & X + c_1 \end{vmatrix} = c_0 + c_1 X + X^2.$$

Now assume that the result is true when $n = k - 1$. We prove it for $n = k$. Expanding determinant of the matrix $(XI - B_k)$ by the first column and applying induction hypothesis, we see that

$$\begin{vmatrix} X & -1 & 0 & \cdots & 0 & 0 \\ 0 & X & -1 & \cdots & 0 & 0 \\ 0 & 0 & X & \cdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & X & -1 \\ c_0 & c_1 & c_2 & \cdots & c_{k-2} & X + c_{k-1} \end{vmatrix} = X(c_1 + c_2 X + \cdots + c_{k-1}X^{k-2} + X^{k-1}) + c_0.$$

Hence the lemma is proved. □

Theorem 1.15 *The characteristic polynomial* $f_\alpha(X)$ *of an element* $\alpha \in K$ *relative to the extension* K/F *is a power of the minimal polynomial of* α *over* F.

Proof Let $\phi_\alpha(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_0$ be the minimal polynomial of α over F. Then $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis of the extension $F(\alpha)/F$. Let $\{\theta_1, \theta_2, \ldots, \theta_r\}$ be a basis of $K/F(\alpha)$. Fix the basis

$$\{\theta_1, \alpha\theta_1, \ldots, \alpha^{n-1}\theta_1 \ ; \ \theta_2, \alpha\theta_2, \ldots, \alpha^{n-1}\theta_2 \ ; \ \ldots \ ; \ \theta_r, \alpha\theta_r, \ldots, \alpha^{n-1}\theta_r\}$$

of the extension K/F. The matrix of the linear transformation T_α defined by $T_\alpha(\xi) = \alpha\xi$ with respect to this basis will be a block diagonal matrix with r blocks down the main diagonal, each block being equal to

[8] In Linear Algebra, the transpose of the matrix B_n is called the companion matrix of the polynomial $f(X)$.

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-2} & -c_{n-1} \end{pmatrix}.$$

So the characteristic polynomial of T_α is the rth power of the characteristic polynomial of A. By Lemma 1.14, the characteristic polynomial of the matrix A is $\phi_\alpha(X)$ and hence $f_\alpha(X) = \phi_\alpha(X)^r$. □

It may be pointed out that basic notions and results about separable, normal and Galois extensions are given in Appendix A. The following simple result of field theory will be used in the sequel.

Lemma 1.16 *Let $F(\theta)$ be a separable extension of a field F of degree n and $f(X) = (X - \theta^{(1)}) \cdots (X - \theta^{(n)})$ be the minimal polynomial of θ over F. If $g(X_1, \ldots, X_n)$ is a polynomial with coefficients in F such that $g(\theta^{(1)}, \ldots, \theta^{(n)})$ remains unchanged under all the permutations of $\theta^{(1)}, \ldots, \theta^{(n)}$, then $g(\theta^{(1)}, \ldots, \theta^{(n)}) \in F$.*

Proof Let $L = F(\theta^{(1)}, \ldots, \theta^{(n)})$. Then L is a Galois extension of F. Let σ be an F-automorphism of L. Applying σ to the equality

$$f(X) = (X - \theta^{(1)}) \cdots (X - \theta^{(n)}),$$

we have

$$f(X) = (X - \sigma(\theta^{(1)})) \cdots (X - \sigma(\theta^{(n)})).$$

So $\sigma(\theta^{(1)}), \ldots, \sigma(\theta^{(n)})$ is a permutation of $\theta^{(1)}, \ldots, \theta^{(n)}$. Therefore in view of the hypothesis, we see that

$$\sigma(g(\theta^{(1)}, \ldots, \theta^{(n)})) = g(\sigma(\theta^{(1)}), \ldots, \sigma(\theta^{(n)})) = g(\theta^{(1)}, \ldots, \theta^{(n)}).$$

Consequently by the fundamental theorem of Galois theory (Theorem A.44), the element $g(\theta^{(1)}, \ldots, \theta^{(n)}) \in F$. □

The theorem stated below describes all roots of a characteristic polynomial.

Theorem 1.17 *Let K/F be a separable extension of degree n and let $\tau_1, \tau_2, \ldots, \tau_n$ be all the F-isomorphisms of K into a normal extension of F containing K. Then the characteristic polynomial of an element $\alpha \in K$ relative to the extension K/F is $(X - \tau_1(\alpha)) \cdots (X - \tau_n(\alpha))$.*

Proof By primitive element theorem (Theorem A.28), there exists $\theta \in K$ such that $K = F(\theta)$. Let $\alpha = h(\theta)$ be an element of K where $h(X) \in F[X]$. Denote the

polynomial $(X - \tau_1(\alpha)) \cdots (X - \tau_n(\alpha))$ by $H(X)$ and $\tau_i(\theta)$ by $\theta^{(i)}$. We first show that $H(X) \in F[X]$. Keeping in mind that $\alpha = h(\theta)$, we see that the coefficients of $H(X)$ are polynomial expressions say $g_i(\theta^{(1)}, \ldots, \theta^{(n)})$ with $g_i(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$. Since $H(X)$ remains unchanged when $\tau_1(\alpha), \ldots, \tau_n(\alpha)$ are permuted, so the coefficients $g_i(\theta^{(1)}, \ldots, \theta^{(n)})$ of $H(X)$ remain unchanged under all permutations of $\theta^{(1)}, \ldots, \theta^{(n)}$. Consequently in view of Lemma 1.16, the coefficients of $H(X)$ belong to F. It can be easily seen that each root of $H(X)$ is a root of the minimal polynomial $\phi_\alpha(X)$ of α over F and hence $H(X)$ belonging to $F[X]$ is a power of $\phi_\alpha(X)$. Also the characteristic polynomial $f_\alpha(X)$ of α relative to the extension K/F is a power of $\phi_\alpha(X)$ by Theorem 1.15. Since $f_\alpha(X)$ and $H(X)$ have the same degree, it now follows that they are equal. □

The following theorem and its corollary provide another definition of norm and trace.

Theorem 1.18 *Let K/F be an extension of fields and let $\alpha \in K$ have characteristic polynomial $f_\alpha(X)$ relative to the extension K/F. Suppose that $f_\alpha(X)$ factors into linear factors as $f_\alpha(X) = (X - \alpha_1) \cdots (X - \alpha_n)$ over an extension of K. Then $N_{K/F}(\alpha) = \alpha_1 \alpha_2 \cdots \alpha_n$ and $Tr_{K/F}(\alpha) = \alpha_1 + \alpha_2 + \cdots + \alpha_n$.*

Proof Let A denote the matrix of linear transformation T_α defined on K by $T_\alpha(\xi) = \alpha\xi$ with respect to a fixed basis of K/F. Then

$$f_\alpha(X) = \det\left(XI - A\right) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \quad \text{(say)}.$$

Substituting $X = 0$ in the above equation, we obtain

$$\det(-A) = a_0;$$

consequently

$$N_{K/F}(\alpha) = \det A = (-1)^n a_0 = \alpha_1 \alpha_2 \cdots \alpha_n.$$

When we expand the determinant of the matrix $(XI - A)$, the coefficient of X^{n-1} is $-\sum_{i=1}^{n} a_{ii}$. So

$$\alpha_1 + \alpha_2 + \cdots + \alpha_n = \sum_{i=1}^{n} a_{ii} = Tr_{K/F}(\alpha).$$

This proves the theorem. □

The theorem stated below follows immediately from the above theorem and Theorem 1.17.

Theorem 1.19 *If K/F is a separable extension of degree n and $\tau_1, \tau_2, \ldots, \tau_n$ are all the F-isomorphisms of K into a normal extension of F containing K, then for every $\alpha \in K$, we have $Tr_{K/F}(\alpha) = \sum_{i=1}^{n} \tau_i(\alpha)$ and $N_{K/F}(\alpha) = \prod_{i=1}^{n} \tau_i(\alpha)$.*

The following theorem is an immediate consequence of Theorems 1.15 and 1.18.

Theorem 1.20 *Let K/F be an extension of degree n and α be an element of K with $[F(\alpha) : F] = d$. Let $\alpha_1, \alpha_2, \ldots, \alpha_d$ be the roots of the minimal polynomial of α over F counting multiplicities (if any) in some extension of F. Then*

$$Tr_{K/F}(\alpha) = \frac{n}{d}\sum_{i=1}^{d}\alpha_i = \frac{n}{d}Tr_{F(\alpha)/F}(\alpha) \text{ and } N_{K/F}(\alpha) = \left(\prod_{i=1}^{d}\alpha_i\right)^{n/d} = \left(N_{F(\alpha)/F}(\alpha)\right)^{n/d}.$$

The corollary stated below follows immediately from Theorem 1.20 and Lemma 1.11.

Corollary 1.21 *Let R be an integrally closed domain with quotient field F and K be a finite extension of F. If an element α of K is integral over R, then $Tr_{K/F}(\alpha)$ and $N_{K/F}(\alpha)$ belong to R.*

The following special case of the above corollary will be used quite often.

Corollary 1.22 *If α is an algebraic integer belonging to an algebraic number field K, then $Tr_{K/F}(\alpha)$ and $N_{K/F}(\alpha)$ belong to $\mathbb{Z}$.*

We now prove the following theorem which asserts that norm and trace are transitive.

Theorem 1.23 *Let $F \subseteq K \subseteq L$ be a tower of finite extensions. Then $Tr_{L/F}(\gamma) = Tr_{K/F}(Tr_{L/K}(\gamma))$ and $N_{L/F}(\gamma) = N_{K/F}(N_{L/K}(\gamma))$ for each element $\gamma \in L$.*

Proof Let $\{w_1, w_2, \ldots, w_n\}$ and $\{\theta_1, \theta_2, \ldots, \theta_m\}$ be bases of the extensions K/F and L/K respectively. Let γ be an element of L. Write

$$\gamma\theta_i = \sum_{j=1}^{m}\alpha_{ij}\theta_j,\ \alpha_{ij} \in K,\ \ \alpha_{ij}w_r = \sum_{s=1}^{n}a_{ijrs}w_s,\ a_{ijrs} \in F.$$

By definition

$$\begin{aligned}
Tr_{L/K}(\gamma) &= \alpha_{11} + \alpha_{22} + \cdots + \alpha_{mm},\\
Tr_{K/F}(\alpha_{11}) &= a_{1111} + a_{1122} + \cdots + a_{11nn},\\
Tr_{K/F}(\alpha_{22}) &= a_{2211} + a_{2222} + \cdots + a_{22nn},\\
\vdots &= \vdots \qquad\quad \vdots \qquad\quad \vdots\\
Tr_{K/F}(\alpha_{mm}) &= a_{mm11} + a_{mm22} + \cdots + a_{mmnn}.
\end{aligned}$$

We compute the matrix of the F-linear transformation $T_\gamma : L \to L$ defined by $T_\gamma(\xi) = \gamma\xi$ with respect to the basis

$$\mathcal{B} := \{\theta_1 w_1, \ldots, \theta_1 w_n \ ; \ \theta_2 w_1, \ldots, \theta_2 w_n \ ; \ \ldots \ ; \ \theta_m w_1, \ldots, \theta_m w_n\}$$

of the extension L/F. Write the equation

$$T_\gamma(\theta_1 w_1) = \gamma\theta_1 w_1 = (\alpha_{11}\theta_1 + \alpha_{12}\theta_2 + \cdots + \alpha_{1m}\theta_m)w_1$$

as

$$T_\gamma(\theta_1 w_1) = \sum_{i=1}^{n} a_{111i}\theta_1 w_i + \sum_{j=1}^{n} a_{121j}\theta_2 w_j + \cdots + \sum_{r=1}^{n} a_{1m1r}\theta_m w_r.$$

Similarly write

$$T_\gamma(\theta_1 w_2) = \gamma\theta_1 w_2 = (\alpha_{11}\theta_1 + \alpha_{12}\theta_2 + \cdots + \alpha_{1m}\theta_m)w_2 \ \ as$$

$$T_\gamma(\theta_1 w_2) = \sum_{i=1}^{n} a_{112i}\theta_1 w_i + \sum_{j=1}^{n} a_{122j}\theta_2 w_j + \cdots + \sum_{r=1}^{n} a_{1m2r}\theta_m w_r.$$

Continuing in this way, it can be seen that the matrix of T_γ with respect to the basis $\mathcal{B}$ is an $mn \times mn$ matrix given by

$$\begin{bmatrix} A_{11} & A_{12} & \cdots & A_{1m} \\ A_{21} & A_{22} & \cdots & A_{2m} \\ \vdots & \vdots & \vdots & \vdots \\ A_{m1} & A_{m2} & \cdots & A_{mm} \end{bmatrix},$$

where each A_{ij} is an $n \times n$ matrix with (r, s)th entry a_{ijrs}. So

$$Tr_{L/F}(\gamma) = \sum_{i=1}^{m}\sum_{j=1}^{n} a_{iijj} = \sum_{i=1}^{m} Tr_{K/F}(\alpha_{ii}) = Tr_{K/F}\Big(\sum_{i=1}^{m}\alpha_{ii}\Big) = Tr_{K/F}(Tr_{L/K}(\gamma))$$

and hence the first assertion of the theorem is proved.

We now prove that

$$N_{L/F}(\gamma) = N_{K/F}(N_{L/K}(\gamma)). \tag{1.4}$$

Keeping in mind Theorem 1.20, it can be quickly seen that the left hand side of (1.4) equals $[N_{K(\gamma)/F}(\gamma)]^{[L:K(\gamma)]}$ and its right hand side equals $[N_{K/F}(N_{K(\gamma)/K}(\gamma))]^{[L:K(\gamma)]}$. So it is enough to prove (1.4) when $L = K(\gamma)$. Let $\{w_1, \ldots, w_n\}$ be a basis of K/F and m denote the degree of $K(\gamma)/F$. Consider the basis

$$\mathcal{B}' := \{w_1, \ldots, w_n \,;\, \gamma w_1, \ldots, \gamma w_n \,;\, \ldots \,;\, \gamma^{m-1} w_1, \ldots, \gamma^{m-1} w_n\}$$

of $K(\gamma)/F$. Let $X^m + \alpha_1 X^{m-1} + \cdots + \alpha_m$ denote the minimal polynomial of γ over K. Then by Theorem 1.20, $N_{K(\gamma)/K}(\gamma) = (-1)^m \alpha_m$. Let A_i denote the matrix of the F-linear transformation $T_{\alpha_i} : K \to K$ (which is multiplication by α_i) with respect to the basis $\{w_1, w_2, \ldots, w_n\}$. Then it can be easily verified that the $mn \times mn$ matrix M of the F-linear transformation $T_\gamma : K(\gamma) \to K(\gamma)$ defined by $T_\gamma(\xi) = \gamma\xi$ with respect to the basis $\mathcal{B}'$ is given by

$$M = \begin{bmatrix} O_{n\times n} & I_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} \\ O_{n\times n} & O_{n\times n} & I_{n\times n} & \cdots & O_{n\times n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -A_m & -A_{m-1} & -A_{m-2} & \cdots & -A_1 \end{bmatrix}.$$

In order to evaluate determinant of M, interchange the first block of n columns of the matrix M with the second block of n columns; in the new matrix interchange second block of n columns with the third block of n columns. Repeating the process $m-1$ times, we see that

$$N_{K(\gamma)/F}(\gamma) = \det M = (-1)^{n(m-1)} \det \begin{bmatrix} I_{n\times n} & O_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} \\ O_{n\times n} & I_{n\times n} & O_{n\times n} & \cdots & O_{n\times n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ -A_{m-1} & -A_{m-2} & -A_{m-3} & \cdots & -A_m \end{bmatrix}$$

$$= (-1)^{n(m-1)} \det(-A_m) = (-1)^{nm} \det(A_m) = (-1)^{nm} N_{K/F}(\alpha_m)$$
$$= N_{K/F}((-1)^m \alpha_m) = N_{K/F}(N_{K(\gamma)/K}(\gamma)).$$

This proves the second assertion of the theorem. □

Exercises

1. Prove by induction on n that the determinant of the Vandermonde matrix

$$\begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_n & \alpha_n^2 & \cdots & \alpha_n^{n-1} \end{bmatrix}$$

equals $\prod_{1 \le j < i \le n} (\alpha_i - \alpha_j)$.

2. Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial and α be an algebraic number. Show that if $f(\alpha)$ is an algebraic integer, then α is an algebraic integer.
3. If a complex number α is not an algebraic integer, then show that α^{ϵ} with ϵ a positive rational number can not be an algebraic integer.
4. Prove that $\cos \dfrac{\pi}{12}$ is an algebraic number. Is it an algebraic integer? Justify your answer.
5. Which of the following polynomials are irreducible over $\mathbb{Q}$. Give justification for your answer.

   (a) $X^3 + X + 1$;
   (b) $X^3 - 4$;
   (c) $X^3 - 4X + 2$.

6. Suppose that $\zeta = e^{\frac{2\pi\iota}{5}}$ where $\iota = \sqrt{-1}$. Write the minimal polynomial of ζ over $\mathbb{Q}$.
7. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Compute the characteristic polynomial of $\sqrt{2} + \sqrt{3}$ with respect to $K/\mathbb{Q}$. Is this polynomial the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$? Give justification for your answer.
8. Let $K = \mathbb{Q}(\sqrt{-1}, \sqrt{2})$. Compute the characteristic polynomial of $\sqrt{-1} + \sqrt{2}$ with respect to $K/\mathbb{Q}$ and its minimal polynomial over $\mathbb{Q}$.
9. Let $K = \mathbb{Q}(\zeta)$ where $\zeta = e^{\frac{2\pi\iota}{5}}$. Compute $N_{K/\mathbb{Q}}(\alpha)$ and $Tr_{K/\mathbb{Q}}(\alpha)$ for the following values of α:

   (a) $\alpha = \zeta^3$;
   (b) $\alpha = \zeta + \zeta^2$;
   (c) $\alpha = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$.

10. Let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive (p^r)th root of unity, p prime. Compute $N_{K/\mathbb{Q}}(1 - \zeta^{p^{r-1}})$.
11. Write down a 3×3 matrix whose characteristic polynomial is $X^3 - 2X^2 + 3X - 1$.
12. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field where θ is a root of $X^3 - 4$. Calculate $Tr_{K/\mathbb{Q}}(\theta^2 + \theta)$ and $N_{K/\mathbb{Q}}(\theta^2 - \theta)$.
13. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field where θ is a root of $X^3 + X + 1$. Calculate $Tr_{K/\mathbb{Q}}(\theta^2 + 2)$ and $N_{K/\mathbb{Q}}(3\theta^2 + 1)$.
14. Let $F \subseteq K \subseteq L$ be a tower of finite extensions of degrees 3 and 2 respectively. Prove that $Tr_{L/F}(\gamma) = Tr_{K/F}(Tr_{L/K}(\gamma))$ for each $\gamma \in L$.
15. Let $F \subseteq K \subseteq L$ be a tower of finite extensions of degrees 2 and 3 respectively. Given $\gamma \in L$, prove that $N_{L/F}(\gamma) = N_{K/F}(N_{L/K}(\gamma))$.
16. Let K/F be a finite extension and σ be an F-isomorphism of K into an extension of F. For $\alpha \in K$, prove that $Tr_{K/F}(\alpha) = Tr_{\sigma(K)/F}(\sigma(\alpha))$ and $N_{K/F}(\alpha) = N_{\sigma(K)/F}(\sigma(\alpha))$.

17. Let A, B be $m \times m$ and $n \times n$ matrices with entries from $\mathbb{C}$. Prove that the determinant of the following $mn \times mn$ matrix (called the Kronecker product of A and B)

$$\begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \cdots & \cdots & \cdots & \\ \cdots & \cdots & \cdots & \\ a_{m1}B & a_{m2}B & \cdots & a_{mm}B \end{bmatrix}$$

is $(\det A)^n (\det B)^m$.

Chapter 2
Integral Basis and Discriminant

Discriminant whose notion is due to Dedekind, is a basic invariant associated with an algebraic number field. Its computation is one of the most important problems in algebraic number theory. For an algebraic number field $K = \mathbb{Q}(\theta)$ with θ in the ring $\mathcal{O}_K$ of algebraic integers of K having $f(X)$ as its minimal polynomial over the field $\mathbb{Q}$ of rational numbers, the discriminant d_K of K and the discriminant[1] of the polynomial $f(X)$ are related by the formula $discr(f) = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 d_K$. So computation of d_K is closely connected with that of the index of the group $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$. It will be shown that $\mathcal{O}_K$ is a free abelian group of rank equal to the degree of the extension $K/\mathbb{Q}$. A $\mathbb{Z}$-basis of the group $\mathcal{O}_K$ is called an integral basis of K. We shall describe explicit integral basis for quadratic, pure cubic[2] and cyclotomic extensions of $\mathbb{Q}$. The problem of computation of discriminant as well as an integral basis of an infinite family of algebraic number fields which are defined over $\mathbb{Q}$ by certain types of irreducible polynomials has attracted the attention of several mathematicians. We shall cite some recent results in this direction and mention a few related open problems.

2.1 Notions of Integral Basis and Discriminant

Definition For an algebraic number field K, the degree of the extension $K/\mathbb{Q}$ is called the degree of K and will be denoted by $[K : \mathbb{Q}]$.

[1] The discriminant of a monic polynomial of degree n having roots $\theta_1, \ldots, \theta_n$ is defined to be the product $\prod_{1 \le i < j \le n} (\theta_i - \theta_j)^2$.

[2] By a pure cubic extension of $\mathbb{Q}$, we mean an algebraic number field $\mathbb{Q}(\theta)$ where θ is a root of an irreducible polynomial $X^3 - a$ over $\mathbb{Z}$.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_2

An algebraic number field of degree 2 is called a quadratic field and one of degree 3 is called a cubic field. Algebraic number fields of degrees 4, 5 and 6 are respectively referred to as quartic, quintic and sextic fields. A quadratic field K is called real or imaginary according as $K \subseteq \mathbb{R}$ or not. A subfield $\mathbb{Q}(\zeta)$ of $\mathbb{C}$, where ζ is a primitive nth root of unity is called the nth cyclotomic field.

The following notation will be used throughout the chapter.

Notation. Let K be an algebraic number field of degree n and $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the distinct $\mathbb{Q}$-isomorphisms (to be called isomorphisms) of K into $\mathbb{C}$. For an element α belonging to K, we shall denote $\sigma_i(\alpha)$ by $\alpha^{(i)}$. Note that if $K = \mathbb{Q}(\alpha)$, then $\alpha^{(1)}, \ldots, \alpha^{(n)}$ are distinct.

Definition Let K be an algebraic number field of degree n and let $\{w_1, \ldots, w_n\}$ be a basis of $K/\mathbb{Q}$ as a vector space. The square of the determinant of $n \times n$ matrix $\left(w_i^{(j)}\right)_{i,j}$ is called discriminant of the basis $\{w_1, \ldots, w_n\}$ and will be denoted by $D_{K/\mathbb{Q}}(w_1, \ldots, w_n)$.

The following lemma gives another expression for the discriminant of a basis.

Lemma 2.1 *If $\{w_1, \ldots, w_n\}$ is a basis of an algebraic number field K as a vector space over $\mathbb{Q}$, then*

$$D_{K/\mathbb{Q}}(w_1, \ldots, w_n) = \det\left(Tr_{K/\mathbb{Q}}(w_i w_j)\right)_{i,j}.$$

Proof Let P denote the $n \times n$ matrix $\left(w_i^{(j)}\right)_{i,j}$ and P^t denote its transpose. By Theorem 1.19, $Tr_{K/\mathbb{Q}}(\alpha) = \alpha^{(1)} + \cdots + \alpha^{(n)}$ for α belonging to K. Keeping this in mind, one can check that $PP^t = \left(Tr_{K/\mathbb{Q}}(w_i w_j)\right)_{i,j}$. On taking determinant, the lemma is proved. □

Remark 2.2 If $\{w_1, \ldots, w_n\}$ is as in the above lemma and if all w_i's belong to $\mathcal{O}_K$, then $D_{K/\mathbb{Q}}(w_1, \ldots, w_n)$ is in $\mathbb{Z}$, because $Tr_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$ for α belonging to $\mathcal{O}_K$ in view of Corollary 1.22.

The next lemma relates the discriminant of two bases.

Lemma 2.3 *Let K be an algebraic number field of degree n. If $\{w_1, w_2, \ldots, w_n\}$ and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ are two bases of $K/\mathbb{Q}$ and C is the transition matrix from $\{w_1, w_2, \ldots, w_n\}$ to $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, then*

$$D_{K/\mathbb{Q}}(\alpha_1, \alpha_2, \ldots, \alpha_n) = (\det C)^2 D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n).$$

Proof Write $C = (c_{ij})_{n\times n}$, then $\alpha_i = \sum_{j=1}^{n} c_{ij} w_j$; consequently

$$\alpha_i^{(r)} = \sum_{j=1}^{n} c_{ij} w_j^{(r)}, \quad 1 \le i \le n, \ 1 \le r \le n. \tag{2.1}$$

Denote the $n \times n$ matrices $\left(w_i^{(j)}\right)_{i,j}$ and $\left(\alpha_i^{(j)}\right)_{i,j}$ by P and Q respectively. We can rewrite the n^2 equations given by (2.1) in the matrix form as $Q = CP$. Taking determinant on both sides and then squaring, we obtain the desired equality. □

Lemma 2.4 *Let $f(X) \in \mathbb{Q}[X]$ be a monic irreducible polynomial of degree n having a root θ in $\mathbb{C}$. If $K = \mathbb{Q}(\theta)$, then $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = discr(f)$.*

Proof Let $\sigma_1, \ldots, \sigma_n$ be all the distinct isomorphisms of K into $\mathbb{C}$. Then $\theta^{(i)} := \sigma_i(\theta)$ is a root of $f(X)$ for $1 \leq i \leq n$. Since these roots are distinct, $f(X) = \prod_{i=1}^{n} \left(X - \theta^{(i)}\right)$. By definition of discriminant of a basis,

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ \theta^{(1)} & \theta^{(2)} & \ldots & \theta^{(n)} \\ \vdots & \vdots & \ddots & \vdots \\ \left(\theta^{(1)}\right)^{n-1} & \left(\theta^{(2)}\right)^{n-1} & \ldots & \left(\theta^{(n)}\right)^{n-1} \end{vmatrix}^2.$$

Keeping in mind the determinant of the Vandermonde matrix, we see that the right hand side of the above equation equals $\prod_{1 \leq i < j \leq n} \left(\theta^{(i)} - \theta^{(j)}\right)^2$, which is the discriminant of $f(X)$. □

Lemma 2.5 *For an algebraic number field K, $D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n)$ is non-zero for any basis $\{w_1, w_2, \ldots, w_n\}$ of $K/\mathbb{Q}$.*

Proof Write $K = \mathbb{Q}(\theta)$. Then $\theta^{(1)}, \ldots, \theta^{(n)}$ are distinct. Let C denote the transition matrix from a basis $\{w_1, w_2, \ldots, w_n\}$ of $K/\mathbb{Q}$ to $\{1, \theta, \ldots, \theta^{n-1}\}$. By Lemma 2.3, we have

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = (\det C)^2 D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n).$$

The desired result follows from above equation and Lemma 2.4, because

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \prod_{1 \leq i < j \leq n} \left(\theta^{(i)} - \theta^{(j)}\right)^2,$$

which is different from zero. □

It may be pointed out that if $\beta_1, \beta_2, \ldots, \beta_n$ are elements of an algebraic number field K of degree n which are linearly dependent over $\mathbb{Q}$, then the determinant of the matrix $\left(\beta_i^{(j)}\right)_{i,j}$ is zero, because if β_k is a $\mathbb{Q}$-linear combination of $\beta_1, \ldots, \beta_{k-1}$, then the kth row of the matrix $\left(\beta_i^{(j)}\right)_{i,j}$ is a linear combination of its first $k-1$ rows.

Lemma 2.6 *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n and $f(X)$ be the minimal polynomial of θ over $\mathbb{Q}$. Then $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta))$.*

Proof Let $\sigma_1, \ldots, \sigma_n$ be all the distinct isomorphisms of K into $\mathbb{C}$. Then $\theta^{(i)} := \sigma_i(\theta)$ is a root of $f(X)$ for $1 \leq i \leq n$. Since these roots are distinct, $f(X) = \prod_{i=1}^{n} \left(X - \theta^{(i)}\right)$. By Theorem 1.19,

$$N_{K/\mathbb{Q}}(f'(\theta)) = \prod_{i=1}^{n} \sigma_i(f'(\theta)) = \prod_{i=1}^{n} f'(\theta^{(i)}). \tag{2.2}$$

In the equation $f'(X) = \sum_{j=1}^{n} \frac{f(X)}{(X - \theta^{(j)})}$, substituting $X = \theta^{(i)}$, we see that

$$f'(\theta^{(i)}) = \prod_{k=1, k\neq i}^{n} (\theta^{(i)} - \theta^{(k)}).$$

Therefore it follows from (2.2) that

$$N_{K/\mathbb{Q}}(f'(\theta)) = \prod_{i=1}^{n} \prod_{k=1, k\neq i}^{n} (\theta^{(i)} - \theta^{(k)}). \tag{2.3}$$

By Lemma 2.4, we have

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \prod_{1 \leq i < j \leq n} \left(\theta^{(i)} - \theta^{(j)}\right)^2.$$

On comparing the above equation with (2.3), we obtain the desired result. □

Definition Let K be an algebraic number field. A set $\{w_1, w_2, \ldots, w_n\}$ of algebraic integers in K is said to be an integral basis of K if every algebraic integer in K can be uniquely written as $a_1 w_1 + a_2 w_2 + \cdots + a_n w_n$ with a_i's in $\mathbb{Z}$.

The following theorem proves the existence of an integral basis.

Theorem 2.7 *Let K be an algebraic number field of degree n. Then the following hold:*

(i) K has an integral basis.
(ii) Any integral basis of K has n elements.

Proof Consider the set

$$S = \left\{ |D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)| \;\middle|\; \{\beta_1, \beta_2, \ldots, \beta_n\} \subseteq \mathcal{O}_K \text{ runs over bases of } K/\mathbb{Q} \right\}.$$

Observe that S is non-empty. By virtue of Lemma 2.5 and Remark 2.2, S is a subset of the set of natural numbers. Therefore S has a smallest element, say l. So there

exists a basis $\{w_1, w_2, \ldots, w_n\}$ of $K/\mathbb{Q}$ consisting of algebraic integers such that $\left|D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n)\right| = l$, i.e.,

$$D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n) = \pm l.$$

Claim is that $\{w_1, w_2, \ldots, w_n\}$ is an integral basis of K. To prove the claim, it is enough to show that each α belonging to $\mathcal{O}_K$ can be written as $a_1 w_1 + a_2 w_2 + \cdots + a_n w_n$, with a_i's in $\mathbb{Z}$, because uniqueness is already there. Suppose to the contrary, there exists $\alpha \in \mathcal{O}_K$ such that $\alpha = \sum_{i=1}^{n} b_i w_i$, where b_i's belong to $\mathbb{Q}$ and at least one $b_i \notin \mathbb{Z}$. Assume without loss of generality that $b_1 \notin \mathbb{Z}$. We can write $b_1 = \lfloor b_1 \rfloor + q$, where $\lfloor b_1 \rfloor$ is the largest integer not exceeding b_1 and $0 < q < 1$, $q \in \mathbb{Q}$. Consider the element β_1 of $\mathcal{O}_K$ given by

$$\beta_1 = \alpha - \lfloor b_1 \rfloor w_1 = q w_1 + b_2 w_2 + \cdots + b_n w_n.$$

Note that $\{\beta_1, w_2, \ldots, w_n\}$ is a basis of $K/\mathbb{Q}$ and consists of elements of $\mathcal{O}_K$. If C denotes the transition matrix from $\{w_1, w_2, \ldots, w_n\}$ to $\{\beta_1, w_2, \ldots, w_n\}$, then by virtue of Lemma 2.4, we have

$$D_{K/\mathbb{Q}}(\beta_1, w_2, \ldots, w_n) = \left(\det C\right)^2 D_{K/\mathbb{Q}}(w_1, w_2, \ldots, w_n) = \pm q^2 l$$

and hence $\left|D_{K/\mathbb{Q}}(\beta_1, w_2, \ldots, w_n)\right| = q^2 l < l$. This contradicts the definition of l and hence the claim is proved.

Assertion (ii) will be proved once we show that whenever $\mathcal{B}$ is an integral basis of K, then $\mathcal{B}$ is also a basis of the vector space $K/\mathbb{Q}$. It is enough to show that $\mathcal{B}$ generates K as a vector space over $\mathbb{Q}$. Let β be any element of K. Then by Theorem 1.6, there exists a non-zero integer r such that $r\beta \in \mathcal{O}_K$. So $r\beta$ can be written as a finite linear combination of elements of $\mathcal{B}$ with coefficients in $\mathbb{Z}$ and hence the result follows. □

Definition A square matrix with entries from $\mathbb{Z}$ is called unimodular if its determinant is ± 1. Equivalently a square matrix with entries in $\mathbb{Z}$ is called unimodular if its inverse has entries in $\mathbb{Z}$.

Definition Let K be an algebraic number field of degree n. Let $\{w_1, \ldots, w_n\}$ and $\{\alpha_1, \ldots, \alpha_n\}$ be two integral bases of K. Then there exist $n \times n$ matrices A and B with entries from $\mathbb{Z}$ such that

$$\begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix} = A \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} \quad \text{and} \quad \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = B \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix},$$

which implies that $AB = I$ and hence $\det A = \pm 1$. So by virtue of Lemma 2.3, $D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = \big(\det A\big)^2 D_{K/\mathbb{Q}}(w_1, \ldots, w_n) = D_{K/\mathbb{Q}}(w_1, \ldots, w_n)$. Therefore any two integral bases of K have the same discriminant. This common value of the discriminant is called the discriminant of the field K. We shall denote it by d_K.

The following basic lemma gives a criterion for a basis of $K/\mathbb{Q}$ to be an integral basis of K.

Lemma 2.8 *Let K be an algebraic number field of degree n and $\beta_1, \beta_2, \ldots, \beta_n$ be algebraic integers in K, which are linearly independent over $\mathbb{Q}$. Then the quotient $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)/d_K$ is the square of an integer. In particular, if $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = d_K$, then $\beta_1, \beta_2, \ldots, \beta_n$ form an integral basis of K.*

Proof Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of K and C be the transition matrix from $\{w_1, w_2, \ldots, w_n\}$ to $\{\beta_1, \beta_2, \ldots, \beta_n\}$. Then C has entries in $\mathbb{Z}$. In view of Lemma 2.3, $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = \big(\det C\big)^2 d_K$. So $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)/d_K$ is the square of an integer. If $D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = d_K$, then C is a unimodular matrix and hence $\beta_1, \beta_2, \ldots, \beta_n$ form an integral basis of K. □

First we determine explicitly the discriminant and an integral basis of a quadratic field. It can be easily seen that every quadratic field can be uniquely written as $\mathbb{Q}(\sqrt{d})$, where d is a squarefree integer.

Theorem 2.9 *For a quadratic field $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer, the following hold:*

(i) If $d \equiv 2$ or $3 \pmod 4$, then $\big\{1, \sqrt{d}\big\}$ is an integral basis of K and $d_K = 4d$.
(ii) If $d \equiv 1 \pmod 4$, then $\{1, (1 + \sqrt{d})/2\}$ is an integral basis of K and $d_K = d$.

Proof Let w denote $(1 + \sqrt{d})/2$ or $\sqrt{d}$ according as $d \equiv 1 \pmod 4$ or not. Clearly $\{1, w\}$ is linearly independent over $\mathbb{Q}$. Let $\alpha = a + b\sqrt{d}$ be an algebraic integer where a, b belong to $\mathbb{Q}$. It is to be shown that α can be written as a linear combination of $1, w$ with coefficients from $\mathbb{Z}$. Clearly this holds when $b = 0$. So assume that $b \neq 0$. In view of Theorem 1.4, the minimal polynomial $f_\alpha(X) = X^2 - 2aX + (a^2 - b^2 d)$ of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$, i.e.,

$$2a \in \mathbb{Z} \text{ and } a^2 - b^2 d \in \mathbb{Z}. \tag{2.4}$$

Set $2a = m$. So (2.4) implies that

$$m^2 - 4b^2 d \in 4\mathbb{Z}. \tag{2.5}$$

Since d is a squarefree integer, (2.5) shows that the rational number b in its reduced form has denominator either ± 1 or ± 2. So we can write b as $\dfrac{n}{2}$ with $n \in \mathbb{Z}$. Now (2.5) can be rewritten as

$$m^2 - n^2 d \equiv 0 \pmod 4. \tag{2.6}$$

The proof is split into two cases.
Case I. $d \equiv 2$ or $3 \pmod 4$. In this case, (2.6) is possible only when m and n are both even, which implies that $\alpha = \frac{m}{2} + \frac{n}{2}\sqrt{d}$ belongs to $\mathbb{Z}[\sqrt{d}]$. So $\{1, \sqrt{d}\}$ is an integral basis of K in this case. By definition

$$d_K = \begin{vmatrix} 1 & 1 \\ \sqrt{d} & -\sqrt{d} \end{vmatrix}^2 = 4d.$$

Case II. $d \equiv 1 \pmod 4$. In this case, (2.6) becomes $m^2 \equiv n^2 \pmod 4$. Therefore $m \equiv n \pmod 2$. So we can write

$$\alpha = \frac{m + n\sqrt{d}}{2} = \frac{m - n}{2} + n\Big(\frac{1 + \sqrt{d}}{2}\Big).$$

Hence $\{1, (1 + \sqrt{d})/2\}$ is an integral basis of K. It can be easily seen that $d_K = d$ in this case. □

2.2 Properties of Discriminant

Recall that if $A = (a_{ij})_{i,j}$ is an $n \times n$ matrix, then

$$\det A = \sum_{(j_1, j_2, \ldots, j_n)} a_{1j_1} a_{2j_2} \cdots a_{nj_n} - \sum_{(k_1, k_2, \ldots, k_n)} a_{1k_1} a_{2k_2} \cdots a_{nk_n},$$

where $(j_1, j_2, \ldots, j_n)$ runs over all even permutations of $\{1, 2, \ldots, n\}$ and $(k_1, k_2, \ldots, k_n)$ runs over all odd permutations of $\{1, 2, \ldots, n\}$.

The following theorem by Ludwig Stickelberger was first announced in the International Congress of Mathematicians held in Zurich in 1897. The present proof of this theorem was given by Schur in 1929.

Theorem 2.10 (Stickelberger's Theorem) *For any algebraic number field K, its discriminant d_K is congruent to* 0 *or* 1 *modulo* 4.

Proof Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of K. By definition, $d_K = \big(\det P\big)^2$, where $P = \big(w_i^{(j)}\big)_{i,j}$. Write $\det P = \alpha - \beta$ with

$$\alpha = \sum_{(j_1, j_2 \ldots, j_n)} w_1^{(j_1)} w_2^{(j_2)} \cdots w_n^{(j_n)}, \quad \beta = \sum_{(k_1, k_2 \ldots, k_n)} w_1^{(k_1)} w_2^{(k_2)} \cdots w_n^{(k_n)},$$

where $(j_1, j_2 \ldots, j_n)$, $(k_1, k_2 \ldots, k_n)$ run respectively over even permutations and odd permutations of $\{1, 2, \ldots, n\}$. So $d_K = \big(\alpha + \beta\big)^2 - 4\alpha\beta$. Therefore the theorem is proved once we show that $\alpha + \beta$ and $\alpha\beta$ belong to $\mathbb{Z}$.

Let θ be an element of $\mathcal{O}_K$ such that $K = \mathbb{Q}(\theta)$. Then $\theta^{(1)}, \ldots, \theta^{(n)}$ are all the distinct roots of the minimal polynomial of θ over $\mathbb{Q}$. Since each w_i can be written as a linear combination of $1, \theta, \ldots, \theta^{n-1}$ with rational coefficients, it follows that $\alpha + \beta$, $\alpha\beta$ are symmetric polynomials in $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ with rational coefficients. Hence $\alpha + \beta$, $\alpha\beta$ belong to $\mathbb{Q}$ in view of Lemma 1.16. As $\alpha + \beta$, $\alpha\beta$ are algebraic integers, these must be in $\mathbb{Z}$. □

Definition An isomorphism σ of an algebraic number field K into $\mathbb{C}$ will be called real if $\sigma(K) \subseteq \mathbb{R}$, otherwise it will be called non-real. Note that non-real isomorphisms of K occur in conjugate pairs.

The following theorem which determines the sign of the discriminant of an algebraic number field was first proved by Alexander von Brill in the year 1877.

Theorem 2.11 (Brill's Theorem) *Let K be an algebraic number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real isomorphisms of K and $2r_2$ is the number of non-real isomorphisms of K, then $(-1)^{r_2} d_K > 0$.*

Proof Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of K. Let $\sigma_1, \ldots, \sigma_n$ be the isomorphisms of K into $\mathbb{C}$ arranged so that $\sigma_1, \ldots, \sigma_{r_1}$ are real, $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ are non-real and $\overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j}$ for $1 \le j \le r_2$. Let $d_1 + \iota d_2$ denote the determinant of the matrix $P = \big(w_i^{(j)}\big)_{i,j}$, with d_1, d_2 real numbers and $\iota = \sqrt{-1}$. Since change of ι to $-\iota$ in the matrix P is equivalent to interchanging the $(r_1 + j)$th column with $(r_1 + r_2 + j)$th column for each $j = 1, ..., r_2$, it follows that

$$d_1 - \iota d_2 = (-1)^{r_2}(d_1 + \iota d_2). \tag{2.7}$$

We discuss two cases.
Case I. r_2 is even. In this case, (2.7) becomes $d_1 - \iota d_2 = d_1 + \iota d_2$, which implies $d_2 = 0$ and hence $d_K = d_1^2 > 0$ as asserted.
Case II. r_2 is odd. In this case, (2.7) implies that $d_1 = 0$ and hence $d_K = -d_2^2 < 0$, which completes the proof of the theorem. □

The next two lemmas besides being of independent interest will be used for finding the discriminant of algebraic number fields.

Lemma 2.12 *Let M be a free abelian group with basis $\{w_1, \ldots, w_m\}$ having rank $m \ge 1$. Let N be a non-zero subgroup of M. Then after a suitable reordering of $w_1, \ldots, w_m$, there exists a basis $\{\eta_1, \ldots, \eta_k\}$ of N of the form*

$$\begin{aligned}
\eta_1 &= c_{11}w_1 + c_{12}w_2 + \cdots + c_{1m}w_m \\
\eta_2 &= \quad\; c_{22}w_2 + \cdots + c_{2m}w_m \\
&\vdots \qquad\quad \ddots \qquad\quad \vdots \\
\eta_k &= \qquad\quad c_{kk}w_k + \cdots + c_{km}w_m
\end{aligned}$$

with $c_{ij} \in \mathbb{Z}$, $c_{ii} > 0$ *for* $1 \leq i \leq k \leq m$.

Proof The lemma will be proved by induction on the rank m of M. We first prove the lemma when $m = 1$, i.e., $M = \mathbb{Z}w_1$. Let s be the smallest positive integer such that sw_1 belongs to the non-zero subgroup N. Then $N = \mathbb{Z}sw_1$, because for any element cw_1 of N, on writing c by division algorithm as $c = sq + r$, $0 \leq r < s$, we see that $rw_1 \in N$ and hence $r = 0$ by minimality of s.

We now prove the lemma when $m \geq 2$ assuming that it holds for free abelian groups of rank $m - 1$. Let β be a non-zero element of N. We can write $\beta = b_1w_1 + \cdots + b_mw_m$, where the coefficients b_i belong to $\mathbb{Z}$ with at least one of them non-zero. By renaming $w_1, \ldots, w_m$ (if necessary), we can assume that $b_1 \neq 0$. If $b_1 < 0$, then the coefficient of w_1 in $-\beta$ will be positive. Among all the elements of the subgroup N, choose that element $\eta_1 = c_{11}w_1 + c_{12}w_2 + \cdots + c_{1m}w_m$ in which the coefficient c_{11} of w_1 is the smallest positive. Claim is that for any $\alpha \in N$, if we write $\alpha = \sum_{i=1}^{m} c_iw_i$, then c_{11} must divide c_1. To prove the claim, write by division algorithm $c_1 = c_{11}q + c'$ with $0 \leq c' < c_{11}$ and q, c' in $\mathbb{Z}$. Hence

$$\alpha - q\eta_1 = c'w_1 + c'_2w_2 + \cdots + c'_mw_m$$

for some $c'_2, \ldots, c'_m$ belonging to $\mathbb{Z}$. Since $\alpha - q\eta_1 \in N$ and $0 \leq c' < c_{11}$, it is clear from the choice of c_{11} that $c' = 0$. Therefore the claim is proved.

Consider the subgroup M_0 of M with basis $\{w_2, \ldots, w_m\}$. Since $N \cap M_0$ is a subgroup of the free abelian group M_0, on applying induction hypothesis, we see that after suitably renaming $w_2, \ldots, w_m$, the group $N \cap M_0$ has a basis $\{\eta_2, \ldots, \eta_k\}$ of the type

$$\begin{array}{lccccc}
\eta_2 = & c_{22}w_2 + & c_{23}w_3 + & \cdots & + & c_{2m}w_m \\
\eta_3 = & & c_{33}w_3 + & \cdots & + & c_{3m}w_m \\
\vdots & & & \ddots & & \vdots \\
\eta_k = & & & c_{kk}w_k + & \cdots + & c_{km}w_m
\end{array}$$

with $c_{ij} \in \mathbb{Z}$, $c_{ii} > 0$ for $2 \leq i \leq k \leq m$. The lemma is proved once we show that $\{\eta_1, \eta_2, \ldots, \eta_k\}$ is a basis of N. We first verify that $\{\eta_1, \eta_2, \ldots, \eta_k\}$ is linearly independent over $\mathbb{Z}$. Suppose that $r_1\eta_1 + r_2\eta_2 + \cdots + r_k\eta_k = 0$ for some $r_i \in \mathbb{Z}$. Then on substituting for η_i's, we see that

$$(r_1c_{11})w_1 + (r_1c_{12} + r_2c_{22})w_2 + \cdots + (r_1c_{1k} + \cdots + r_kc_{kk})w_k + \cdots = 0.$$

Since $\{w_1, w_2, \ldots, w_m\}$ is a basis of M and each c_{ii} is positive, it is immediate from the above equation that $r_i = 0$ for $1 \leq i \leq k$. Now we verify that $\{\eta_1, \eta_2, \ldots, \eta_k\}$ generates N. Let $\alpha = \sum_{i=1}^{m} c_iw_i$ be any element of N. By virtue of the claim proved in the above paragraph, $c_1 = c_{11}q_1$ for some $q_1 \in \mathbb{Z}$. So $\alpha - q_1\eta_1 = c'_2w_2 + \cdots + c'_mw_m$, for some $c'_i \in \mathbb{Z}$. Note that $\alpha - q_1\eta_1 \in N \bigcap M_0$. Therefore by induction hypothesis,

$\alpha - q_1\eta_1$ can be written as $\sum_{i=2}^{k} q_i\eta_i$ with q_i's in $\mathbb{Z}$. Consequently $\alpha = \sum_{i=1}^{k} q_i\eta_i$. Hence the lemma is proved. □

Remark 2.13 If M and N are as in the above lemma and have the same rank, then the proof shows that without reordering $w_1, w_2, \ldots, w_m$, one can construct a basis of N of the type $\eta_1, \eta_2, \ldots, \eta_m$.

Lemma 2.14 *If M is a free abelian group of finite rank and N is a subgroup of M such that rank(N) = rank(M), then the index $[M : N]$ is finite and equals the absolute value of the determinant of the transition matrix from any basis of M to any basis of N.*

Proof Let $\{w_1, w_2, \ldots, w_m\}$ be a basis of M. By Lemma 2.12 and the above remark, there exists a basis $\{\eta_1, \eta_2, \ldots, \eta_m\}$ of N such that

$$\begin{array}{lccccc} \eta_1 = & c_{11}w_1 & + & c_{12}w_2 & + \cdots + & c_{1m}w_m \\ \eta_2 = & & & c_{22}w_2 & + \cdots + & c_{2m}w_m \\ \vdots & & & & \ddots & \vdots \\ \eta_m = & & & & & c_{mm}w_m \end{array}$$

with $c_{ij} \in \mathbb{Z}$, $c_{ii} > 0$. If C denotes the transition matrix from $\{w_1, w_2, \ldots, w_m\}$ to $\{\eta_1, \eta_2, \ldots, \eta_m\}$, then $\det C = \prod_{i=1}^{m} c_{ii} = r$ (say). We have to prove that

$$[M : N] = r. \tag{2.8}$$

We prove (2.8) by showing that the r elements of the set

$$S = \left\{x_1w_1 + x_2w_2 + \cdots + x_mw_m \mid 0 \le x_i < c_{ii},\ 1 \le i \le m\right\}$$

form a complete system of coset representatives of the quotient group M/N.

Let $\alpha = \sum_{i=1}^{m} a_iw_i$ be any element of M. By division algorithm, write $a_1 = c_{11}q_1 + x_1$, with $q_1 \in \mathbb{Z}$ and $0 \le x_1 < c_{11}$. So

$$\alpha - q_1\eta_1 - x_1w_1 = a_2'w_2 + \cdots a_m'w_m$$

for some $a_i' \in \mathbb{Z}$. Similarly we may write $a_2' = c_{22}q_2 + x_2$, $0 \le x_2 < c_{22}$. Then

$$\alpha - q_1\eta_1 - q_2\eta_2 - x_1w_1 - x_2w_2 = a_3''w_3 + \cdots + a_m''w_m$$

with coefficients a_i'' in $\mathbb{Z}$. Continuing this process, we see that

$$\alpha - \sum_{i=1}^{m} q_i \eta_i - \sum_{i=1}^{m} x_i w_i = 0.$$

So $\alpha = x + y$ where $x = \sum_{i=1}^{m} x_i w_i$ belongs to S and $y = \sum_{i=1}^{m} q_i \eta_i$ belongs to N. Thus every coset of M/N is represented by an element of S.

It only remains to verify that different elements of S represent different cosets modulo N. Suppose to the contrary that $N + x = N + x'$ where $x = \sum_{i=1}^{m} x_i w_i$ and $x' = \sum_{i=1}^{m} x_i' w_i$ are different elements of S. Let t denote the smallest index such that $x_t \neq x_t'$. Since $x - x' = \sum_{i=t}^{m} (x_i - x_i') w_i$ belongs to N, there exist integers $b_1, \ldots, b_m$ such that

$$\sum_{i=t}^{m} (x_i - x_i') w_i = \sum_{i=1}^{m} b_i \eta_i.$$

Comparing the coefficients of $w_1, \ldots, w_{t-1}$ in the above equation, we see that $b_i = 0$ for $1 \leq i \leq t-1$. Therefore

$$\sum_{i=t}^{m} (x_i - x_i') w_i = \sum_{i=t}^{m} b_i \eta_i.$$

Equating the coefficients of w_t in the above equation, we have $x_t - x_t' = b_t c_{tt}$, which is impossible since $0 < |x_t - x_t'| < c_{tt}$. This proves the lemma. □

For an algebraic number field K, the following theorem gives the index of a subgroup of $\mathcal{O}_K$ generated by a basis $\mathcal{B}$ of $K/\mathbb{Q}$ consisting of algebraic integers in terms of discriminant of $\mathcal{B}$ and d_K. Its result is a refined version of Lemma 2.8.

Theorem 2.15 *Let $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be a basis of an algebraic number field K as a vector space over $\mathbb{Q}$ consisting of algebraic integers. Let N denote the free abelian group generated by $\beta_1, \beta_2, \ldots, \beta_n$. Then*

$$[\mathcal{O}_K : N]^2 = D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n)/d_K.$$

Proof Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of K. Let A denote the transition matrix from $\{w_1, w_2, \ldots, w_n\}$ to $\{\beta_1, \beta_2, \ldots, \beta_n\}$. In view of Lemma 2.14, we see that

$$[\mathcal{O}_K : N] = |\det A|. \tag{2.9}$$

By Lemma 2.3, we have

$$D_{K/\mathbb{Q}}(\beta_1, \beta_2, \ldots, \beta_n) = \big(\det A\big)^2 d_K. \tag{2.10}$$

The desired equality follows immediately from (2.9) and (2.10). □

The following corollary is an immediate consequence of Theorem 2.15.

Corollary 2.16 *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Then the index of the subgroup $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ is given by*

$$[\mathcal{O}_K : \mathbb{Z}[\theta]]^2 = D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1})/d_K.$$

In the set up of the above corollary, by Lemma 2.4, $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = discr(f)$, where $f(X)$ is the minimal polynomial of θ over $\mathbb{Q}$. So the above equation may be rewritten as

$$discr(f) = [\mathcal{O}_K : \mathbb{Z}[\theta]]^2 d_K.$$

Notation. Let $K = \mathbb{Q}(\theta)$ be as in the above corollary. The index of the subgroup $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$ is called the index of θ and will be denoted by $\operatorname{ind}\theta$.

Definition An algebraic number field K of degree n is said to be monogenic if there exists an element $\theta \in \mathcal{O}_K$ such that $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis of K; an integral basis of the type $\{1, \theta, \ldots, \theta^{n-1}\}$ is called a power basis of K.

In view of Theorem 2.9, every quadratic field is monogenic. It will be shown in Theorem 2.22 that a cubic field of the type $\mathbb{Q}(\sqrt[3]{m})$ is also monogenic when m is a squarefree integer which is not congruent to ± 1 modulo 9. Also in view of Theorem 2.31, every cyclotomic field is monogenic. In 1878, Dedekind showed that not every algebraic number field is monogenic by giving the following example of an algebraic number field K in which the index of each element of $\mathcal{O}_K$ generating the extension $K/\mathbb{Q}$ is even.

Example 2.17 Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - X^2 - 2X - 8$. It will be first shown that $f(X)$ is irreducible over $\mathbb{Q}$. If $f(X)$ is reducible over $\mathbb{Q}$, then $f(X)$ has a rational root, say α. Since each root of $f(X)$ is an algebraic integer, $\alpha \in \mathbb{Z}$. As $\alpha^3 - \alpha^2 - 2\alpha = 8$, we see that α divides 8 in $\mathbb{Z}$. Hence $\alpha \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$. By direct verification, none of these integers is a root of $f(X)$. So $f(X)$ is irreducible over $\mathbb{Q}$. By Lemma 2.6 and Corollary 2.16, we have

$$D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(f'(\theta)) = (-4)503 = d_K(\operatorname{ind}\theta)^2.$$

Since 503 is a prime number, $\operatorname{ind}\theta$ is 1 or 2. It can be easily seen that the characteristic polynomial of $(\theta + \theta^2)/2$ with respect to $K/\mathbb{Q}$ is $X^3 - 3X^2 - 10X - 8$. So $(\theta + \theta^2)/2 \in \mathcal{O}_K$. In view of Lemma 2.3,

$$D_{K/\mathbb{Q}}\left(1, \theta, \frac{\theta + \theta^2}{2}\right) = \frac{1}{4} D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -503.$$

So $\{1, \theta, (\theta + \theta^2)/2\}$ is an integral basis of K by virtue of Lemma 2.8. We denote $(\theta + \theta^2)/2$ by η. Let α be any element of $\mathcal{O}_K \setminus \mathbb{Z}$. We show that the index $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is even. By Lemma 2.14, $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$ is the absolute value of the determinant of the transition matrix P from the basis $\{1, \theta, \eta\}$ of $\mathcal{O}_K$ to $\{1, \alpha, \alpha^2\}$. It is enough to compute the entries of P modulo 2. Write $\alpha = a + b\theta + c\eta$, where $a, b, c \in \mathbb{Z}$. Keeping in mind that $\theta^2 = 2\eta - \theta$, $\theta\eta = 2\eta + 4$ and $\eta^2 = 6 + 2\theta + 3\eta$, a simple calculation shows that $\alpha^2 = (a^2 + 6c^2 + 8bc) + (2c^2 - b^2 + 2ab)\theta + (2b^2 + 3c^2 + 2ac + 4bc)\eta$. So

$$P \equiv \begin{bmatrix} 1 & 0 & 0 \\ a & b & c \\ a^2 & -b^2 & 3c^2 \end{bmatrix} \pmod 2.$$

Hence $\det P \equiv bc(b + c) \equiv 0 \pmod 2$ as asserted.

The next result is sometimes useful for computing the discriminant and integral basis.

Theorem 2.18 *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ an algebraic integer. If the minimal polynomial of θ over $\mathbb{Q}$ is an Eisenstein polynomial*[3] *with respect to a prime p, then p does not divide* $\operatorname{ind}\theta$.

Proof Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be the minimal polynomial of θ over $\mathbb{Q}$. Observe that θ^n/p belongs to $\mathcal{O}_K$ because

$$\frac{\theta^n}{p} = -\sum_{i=0}^{n-1} \frac{a_i}{p}\theta^i$$

and p divides a_i for $0 \le i \le n - 1$.

Suppose to the contrary p divides $\operatorname{ind}\theta$, then by Cauchy's theorem for finite groups, $\mathcal{O}_K/\mathbb{Z}[\theta]$ has an element of order p. So there exists $\alpha \in \mathcal{O}_K$ such that $\alpha \notin \mathbb{Z}[\theta]$ but $p\alpha \in \mathbb{Z}[\theta]$. Hence we may write

$$p\alpha = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1},$$

where at least one of the integers b_i is not divisible by p. Let j be the smallest index such that p does not divide b_j. Define an element β of $\mathcal{O}_K$ by

$$\beta = \alpha - \frac{b_0 + b_1\theta + \cdots + b_{j-1}\theta^{j-1}}{p} = \frac{b_j\theta^j + \cdots + b_{n-1}\theta^{n-1}}{p}.$$

So

[3] A polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ with coefficients from $\mathbb{Z}$ is said to be an Eisenstein polynomial with respect to a prime p if $p \nmid a_n$, $p|a_i$ for $0 \le i \le n - 1$ and $p^2 \nmid a_0$. Such a polynomial is irreducible over $\mathbb{Q}$.

$$\frac{b_j\theta^j}{p} = \beta - \frac{b_{j+1}\theta^{j+1} + \cdots + b_{n-1}\theta^{n-1}}{p}.$$

On multiplying the above equation by θ^{n-1-j}, we obtain

$$\frac{b_j\theta^{n-1}}{p} = \beta\theta^{n-1-j} - \frac{b_{j+1}\theta^n + \cdots + b_{n-1}\theta^{2n-2-j}}{p}. \tag{2.11}$$

Recall that $\theta^n/p \in \mathcal{O}_K$ by what has been shown in the first paragraph. Since β also belongs to $\mathcal{O}_K$, it now follows that the right hand side of (2.11) belongs to $\mathcal{O}_K$. So its left hand side namely $b_j\theta^{n-1}/p \in \mathcal{O}_K$. Consequently $N_{K/\mathbb{Q}}\big(\frac{b_j\theta^{n-1}}{p}\big) = \dfrac{b_j^n a_0^{n-1}}{p^n}$ is in $\mathbb{Z}$, which is impossible, because p does not divide b_j and p^2 does not divide a_0. This contradiction proves that p does not divide $\operatorname{ind}\theta$. □

The following examples illustrate the results proved in this section.

Example 2.19 We compute the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - X + 1$. Arguing as in Example 2.17, it can be easily seen that $f(X)$ is irreducible over $\mathbb{Q}$. Applying Lemma 2.6, we have

$$D_{K/\mathbb{Q}}(1, \theta, \theta^2) = (-1)^{\frac{3(3-1)}{2}} N_{K/\mathbb{Q}}(f'(\theta)) = -N_{K/\mathbb{Q}}(3\theta^2 - 1) = -23.$$

Therefore by Lemma 2.8, $d_K = -23$ and $\{1, \theta, \theta^2\}$ is an integral basis of K.

As pointed out at the end of Sect. 8.4, the field K in the above example is the cubic field whose discriminant has smallest absolute value among all cubic fields.

Example 2.20 Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - 2X^2 + 2$ which is an Eisenstein polynomial with respect to the prime 2 and hence is irreducible over $\mathbb{Q}$. We compute the discriminant and construct an integral basis of $K = \mathbb{Q}(\theta)$. By Corollary 2.16 and Lemma 2.6, we have

$$d_K(\operatorname{ind}\theta)^2 = D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(3\theta^2 - 4\theta) = -44,$$

which shows that $\operatorname{ind}\theta$ divides 2. In view of Theorem 2.18, $\operatorname{ind}\theta$ is coprime to 2. We conclude that $\operatorname{ind}\theta$ equals 1, $d_K = -44$ and $\{1, \theta, \theta^2\}$ is an integral basis of K.

Example 2.21 Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $f(X) = X^3 - 9X - 6$. Note that $f(X)$ is an Eisenstein polynomial with respect to the prime 3 and hence is irreducible over $\mathbb{Q}$. Using Corollary 2.16 and Lemma 2.6, we see that

$$d_K(\operatorname{ind}\theta)^2 = D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(3\theta^2 - 9) = 2^3 \cdot 3^5,$$

It follows from the above equation and from Theorem 2.18 that $\operatorname{ind}\theta$ is 1 or 2. If $\operatorname{ind}\theta$ is 2, then $d_K = 2 \cdot 3^5$ which is impossible because $d_K \equiv 0$ or 1 (mod 4) by Stickelberger's theorem. So $\operatorname{ind}\theta$ is 1 and $d_K = 2^3 \cdot 3^5$.

2.3 Integral Basis and Discriminant of $\mathbb{Q}(\sqrt[3]{m})$

The problem of computation of discriminant and construction of integral basis of pure number fields has been considered by several mathematicians. By a pure number field of degree n, we mean an algebraic number field $K = \mathbb{Q}(\theta)$, where θ is a root of an irreducible polynomial $X^n - a$ belonging to $\mathbb{Z}[X]$. In 1900, Dedekind was the first to describe an integral basis of pure cubic fields. An explicit construction of integral basis of pure prime degree number fields was given by Westlund in 1910 (cf. [Wes, Ja-Sa]). This problem has been solved for pure quartic fields by Funakura [Fun] in 1984 and for pure sextic fields by Jakhar in 2021 (cf. [Jak2]).

In this section, we now prove the following theorem which gives the discriminant and an integral basis of pure cubic fields.

Theorem 2.22 *Let $K = \mathbb{Q}(\theta)$ be a cubic field with $\theta^3 = m = ab^2$, where a, b are relatively prime squarefree integers. The following hold:*

(i) If $m \not\equiv 1$ or 8 (mod 9), then $\{1, \theta, \theta^2/b\}$ is an integral basis of K and $d_K = -27a^2b^2$.

(ii) If $m \equiv 1$ (mod 9), then $\{\theta, \theta^2/b, (1 + \theta + \theta^2)/3\}$ is an integral basis of K and $d_K = -3a^2b^2$.

(iii) If $m \equiv 8$ (mod 9), then $\{\theta, \theta^2/b, (1 - \theta + \theta^2)/3\}$ is an integral basis of K and $d_K = -3a^2b^2$.

The following lemma will be used in the proof of the above theorem.

Lemma 2.23 *Let $K = \mathbb{Q}(\theta)$ be a cubic field with $\theta^3 = m = ab^2$, where a, b are relatively prime squarefree integers. Then $d_K = -27a^2b^2$ if 3 divides ab and $d_K = -3^r a^2b^2$ with $r = 1$ or 3 when 3 does not divide ab.*

Proof In view of Lemma 2.6, we have

$$D_{K/\mathbb{Q}}\big(1, \theta, \theta^2\big) = -N_{K/\mathbb{Q}}(3\theta^2) = -27m^2 = -27a^2b^4. \tag{2.12}$$

The minimal polynomial $X^3 - m$ of θ is an Eisenstein polynomial with respect to each prime p dividing a. Therefore by Theorem 2.18, such a p does not divide $\operatorname{ind}\theta$. But by Corollary 2.16 and Eq. (2.12),

$$(\operatorname{ind}\theta)^2 = \frac{D_{K/\mathbb{Q}}(1, \theta, \theta^2)}{d_K} = -\frac{27m^2}{d_K}.$$

Therefore if p divides a, then p^2 divides d_K and if 3 divides a, then 3^5 divides d_K. Thus we conclude that

$$a^2 \mid d_K \text{ if } 3 \nmid a \text{ and } 27a^2 \mid d_K \text{ if } 3|a. \tag{2.13}$$

Note that θ^2/b is a root of the polynomial $X^3 - a^2b$ and $K = \mathbb{Q}(\theta^2/b)$. On interchanging the roles of a and b and arguing as for the proof of (2.13), it can be easily seen that

$$b^2 \mid d_K \text{ if } 3 \nmid b \text{ and } 27b^2 \mid d_K \text{ if } 3|b. \tag{2.14}$$

By virtue of Lemmas 2.6 and 2.8, we have

$$D_{K/\mathbb{Q}}\left(1, \theta, \theta^2/b\right) = \frac{1}{b^2} D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -27a^2b^2 = c^2 d_K \tag{2.15}$$

for some integer c. In particular, the above equation shows that

$$d_K \mid 27a^2b^2. \tag{2.16}$$

The lemma follows immediately from (2.13), (2.14) and (2.16) keeping in mind that $D_{K/\mathbb{Q}}(1, \theta, \theta^2)/d_K$ is a perfect square. □

Proof of Theorem 2.22 When $m \equiv 0 \pmod 3$, then by virtue of Eq. (2.15) and Lemma 2.23, we see that

$$D_{K/\mathbb{Q}}(1, \theta, \theta^2/b) = -27a^2b^2 = d_K$$

and hence $\{1, \theta, \theta^2/b\}$ is an integral basis of K in this case by Lemma 2.8. So it remains to prove the theorem when $m \not\equiv 0 \pmod 3$. We distinguish three cases.

Case I. $m \not\equiv \pm 1 \pmod 9$, and $3 \nmid m$.

It can be easily checked that in this case $m^3 \not\equiv m \pmod 9$. So the polynomial $(X + m)^3 - m = X^3 + 3mX^2 + 3m^2X + m^3 - m$ is an Eisenstein polynomial with respect to the prime 3. Therefore by Theorem 2.18, the prime 3 does not divide index of $(\theta - m)$ which is same as index of θ. So we conclude from (2.12) and the previous lemma that $d_K = -27a^2b^2$ in this case. Thus we have $D_{K/\mathbb{Q}}(1, \theta, \theta^2/b) = -27a^2b^2 = d_K$ and hence $\{1, \theta, \theta^2/b\}$ is an integral basis of K by Lemma 2.8.

Case II. $m \equiv 1 \pmod 9$.

A simple computation shows that the characteristic polynomial of $(1 + \theta + \theta^2)/3$ relative to $K/\mathbb{Q}$ is $X^3 - X^2 + \frac{(1-m)}{3}X - \frac{(1-m)^2}{27}$ and hence $(1 + \theta + \theta^2)/3$ is an algebraic integer in this case. If A denotes the transition matrix from $\{1, \theta, \theta^2\}$ to $\{\theta, \theta^2/b, (1 + \theta + \theta^2)/3\}$, then $\det A = 1/3b$. Consequently by Lemmas 2.3 and 2.8, we have

$$D_{K/\mathbb{Q}}\Big(\theta, \frac{\theta^2}{b}, \frac{1+\theta+\theta^2}{3}\Big) = \frac{1}{9b^2} D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -3a^2b^2 = c^2 d_K$$

for some integer c. It follows immediately from the above equation and Lemma 2.23 that $d_K = -3a^2b^2$ and hence $\{\theta, \theta^2/b, (1+\theta+\theta^2)/3\}$ is an integral basis of K.

Case III. $m \equiv -1 \pmod 9$.

Since $(-\theta)^3 = -m = -ab^2 \equiv 1 \pmod 9$, by virtue of Case II, we see that $d_K = -3a^2b^2$ and $\{-\theta, \theta^2/b, (1-\theta+\theta^2)/3\}$ is an integral basis of K. As the transition matrix from this integral basis to $\{\theta, \theta^2/b, (1-\theta+\theta^2)/3\}$ is unimodular, it follows that the latter set is also an integral basis of K.

Remark 2.24 A formula for the discriminant together with a method to compute integral basis of each cubic field has been given by Alaca in [Ala]; the same problem has been solved for all those quartic and quintic fields which are generated over $\mathbb{Q}$ by a root of an irreducible trinomial of the type $X^n + aX + b$ belonging to $\mathbb{Z}[X]$ when $n = 4, 5$ (cf. [Al-Wi1, Al-Al]). In 2020, it has been solved for those sextic fields which are generated over $\mathbb{Q}$ by a root of an irreducible trinomial of the above type when $n = 6$ (cf. [Ka-Kh]). For general n, the problem is solved with some conditions on a, b and n (cf. [Kom]).

2.4 Integral Basis and Discriminant of Cyclotomic Fields

We first find the discriminant and an integral basis of cyclotomic fields generated by pth root of unity for a prime p. Recall that if ζ is a primitive nth root of unity, then the degree of the nth cyclotomic field $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$ is $\phi(n)$ (cf. Theorem A.40).

Theorem 2.25 *Let ζ be a primitive pth root of unity, p an odd prime. Then $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is an integral basis of $K = \mathbb{Q}(\zeta)$ and $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$.*

Proof Let $\Phi(X)$ denote the minimal polynomial of ζ over $\mathbb{Q}$ of degree $p-1$. Using Lemma 2.6 and Corollary 2.16, we have

$$D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{p-2}) = (-1)^{\frac{p-1}{2}} N_{K/\mathbb{Q}}(\Phi'(\zeta)) = (\operatorname{ind} \zeta)^2 d_K.$$

So the theorem is proved in view of above equation once it is shown that $N_{K/\mathbb{Q}}(\Phi'(\zeta))$ equals p^{p-2} and p does not divide $\operatorname{ind} \zeta$. The polynomial $\Phi(X)$ satisfies the relation

$$\Phi(X)(X-1) = X^p - 1.$$

On differentiating both sides of above equation with respect to X and then substituting $X = \zeta$, we see that

$$\Phi'(\zeta) = \frac{p}{(\zeta-1)\zeta}.$$

Taking norm on both sides, we obtain

$$N_{K/\mathbb{Q}}(\Phi'(\zeta)) = \frac{p^{[K:\mathbb{Q}]}}{N_{K/\mathbb{Q}}(\zeta - 1)N_{K/\mathbb{Q}}(\zeta)}. \tag{2.17}$$

Since the minimal polynomial of ζ over $\mathbb{Q}$ is $\Phi(X) = X^{p-1} + X^{p-2} + \cdots + 1$, $N_{K/\mathbb{Q}}(\zeta) = (-1)^{p-1}$ in view of Theorem 1.18. On writing $\Phi(X)$ as $\prod_{i=1}^{p-1}(X - \zeta^{(i)})$ and keeping in mind Theorem 1.19, we see that

$$p = \Phi(1) = \prod_{i=1}^{p-1}(1 - \zeta^{(i)}) = N_{K/\mathbb{Q}}(1 - \zeta) = N_{K/\mathbb{Q}}(\zeta - 1). \tag{2.18}$$

It now follows from (2.17) that $N_{K/\mathbb{Q}}(\Phi'(\zeta)) = p^{p-2}$ as desired.

It only remains to verify that $p \nmid \operatorname{ind} \zeta$. Since $\mathbb{Z}[\zeta] = \mathbb{Z}[\zeta - 1]$, we verify that p does not divide $\operatorname{ind}(\zeta - 1)$. The minimal polynomial of $\zeta - 1$ over $\mathbb{Q}$ is

$$\Phi(X + 1) = \frac{(X + 1)^p - 1}{(X + 1) - 1} = X^{p-1} + \binom{p}{1}X^{p-2} + \cdots + \binom{p}{p-1},$$

which is an Eisenstein polynomial with respect to the prime p. Therefore by Theorem 2.18, p does not divide $\operatorname{ind}(\zeta - 1)$. □

The argument used in the proof of the above theorem has been extended to prove the following more general theorem.

Theorem 2.26 *Let ζ be a primitive (p^r)th root of unity, p any prime (odd or even), $p^r \geq 3$. Then $\{1, \zeta, \ldots, \zeta^{\phi(p^r)-1}\}$ is an integral basis of $K = \mathbb{Q}(\zeta)$ and $d_K = (-1)^{\frac{\phi(p^r)}{2}} p^{r\phi(p^r)-p^{r-1}}$.*

Proof Let $\Phi(X) = (X^{p^r} - 1)/(X^{p^{r-1}} - 1)$ denote the minimal polynomial of ζ over $\mathbb{Q}$ of degree $\phi(p^r)$. Since $p^r \geq 3$, $\phi(p^r)$ is even. Then by Lemma 2.6 and Corollary 2.16, we have

$$D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\phi(p^r)-1}) = (-1)^{\frac{\phi(p^r)}{2}} N_{K/\mathbb{Q}}(\Phi'(\zeta)) = (\operatorname{ind} \zeta)^2 d_K.$$

As proved in the following lemma, $\Phi(X + 1)$ is an Eisenstein polynomial with respect to p. So $p \nmid \operatorname{ind}(\zeta - 1)$, i.e., $p \nmid \operatorname{ind} \zeta$. Thus the theorem is proved once it is shown that

$$N_{K/\mathbb{Q}}(\Phi'(\zeta)) = p^{r\phi(p^r)-p^{r-1}}. \tag{2.19}$$

Differentiating both sides of the equation

$$\Phi(X)(X^{p^{r-1}} - 1) = X^{p^r} - 1$$

with respect to X and then substituting $X = \zeta$, we obtain

$$\Phi'(\zeta) = \frac{p^r}{\zeta(\zeta^{p^{r-1}} - 1)}. \tag{2.20}$$

Keeping in mind that $\zeta^{p^{r-1}} = \eta$ (say) is a primitive pth root of unity and using the fact that $N_{\mathbb{Q}(\eta)/\mathbb{Q}}(\eta - 1) = p$ derived in Eq. (2.18), it follows that

$$N_{K/\mathbb{Q}}(\zeta^{p^{r-1}} - 1) = N_{K/\mathbb{Q}}(\eta - 1) = [N_{\mathbb{Q}(\eta)/\mathbb{Q}}(\eta - 1)]^{[K:\mathbb{Q}(\eta)]} = p^{p^{r-1}}.$$

Note that $N_{K/\mathbb{Q}}(\zeta) = (-1)^{\phi(p^r)} = 1$ in view of Theorem 1.18. On taking norm on both sides of (2.20), the equality (2.19) is now proved. □

Lemma 2.27 *Let ζ be as in Theorem 2.26 and $\Phi(X)$ be the minimal polynomial of ζ over $\mathbb{Q}$. Then $\Phi(X + 1)$ is an Eisenstein polynomial with respect to the prime p.*

Proof Since $\Phi(X) = X^{(p-1)p^{r-1}} + X^{(p-2)p^{r-1}} + \cdots + X^{p^{r-1}} + 1$, we have

$$\Phi(X + 1) = \sum_{j=0}^{p-1} (X + 1)^{jp^{r-1}}. \tag{2.21}$$

Using the Binomial theorem, we can write

$$(X + 1)^{p^{r-1}} = (X^{p^{r-1}} + 1) + pW_1(X),$$

where $W_1(X) \in \mathbb{Z}[X]$ is a polynomial of degree less than p^{r-1} having constant term zero. Raising the above equation to any power $j \geq 1$, we see that

$$(X + 1)^{jp^{r-1}} = (X^{p^{r-1}} + 1)^j + pW_j(X), \tag{2.22}$$

where $W_j(X) \in \mathbb{Z}[X]$ is a polynomial of degree less than jp^{r-1} having constant term zero. In view of (2.21) and (2.22), we have

$$\Phi(X + 1) = \sum_{j=0}^{p-1} (X + 1)^{jp^{r-1}} = \sum_{j=0}^{p-1} (X^{p^{r-1}} + 1)^j + pV(X),$$

with $V(X) \in \mathbb{Z}[X]$, $\deg(V(X)) < (p - 1)p^{r-1}$ and $V(X)$ has constant term zero. It is clear from the last equation that

$$\begin{aligned}\Phi(X + 1) &= \frac{(X^{p^{r-1}} + 1)^p - 1}{(X^{p^{r-1}} + 1) - 1} + pV(X) \\ &= X^{(p-1)p^{r-1}} + \binom{p}{1} X^{(p-2)p^{r-1}} + \cdots + \binom{p}{p-1} + pV(X).\end{aligned}$$

Keeping in mind that $\deg(V(X)) < (p-1)p^{r-1}$ and $V(X)$ has constant term zero, it is immediate from the above equality that $\Phi(X+1)$ is an Eisenstein polynomial with respect to p. □

The following two propositions, which are of independent interest, will be used to compute the discriminant of a general cyclotomic field.

Notation. If S and T are subrings of a ring R, then ST will stands for the composite ring, i.e., the smallest subring of R containing $S \cup T$. Similar notation will be used for the composite of two subfields of a field.

Proposition 2.28 *Let K and L be algebraic number fields of degree m and n respectively. Let $d = \gcd(d_K, d_L)$. If $[KL : \mathbb{Q}] = mn$, then $\mathcal{O}_{KL} \subseteq \frac{1}{d}(\mathcal{O}_K\mathcal{O}_L)$. In particular when $d = 1$, then $\mathcal{O}_K\mathcal{O}_L = \mathcal{O}_{KL}$.*

Proof Let $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ be an integral basis of K and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ be an integral basis of L. Since $[KL : \mathbb{Q}] = mn$, the family $\{\alpha_j\beta_k \mid 1 \le j \le m, 1 \le k \le n\}$ is a $\mathbb{Q}$-vector space basis of KL. Let ξ be any element of $\mathcal{O}_{KL}$. We can write

$$\xi = \sum_{j,k} \frac{r_{jk}}{r}\alpha_j\beta_k, \quad r_{jk}, r \in \mathbb{Z}. \tag{2.23}$$

Since $[KL : \mathbb{Q}] = mn$, every embedding σ of K into $\mathbb{C}$ can be extended to KL acting trivially on L and hence

$$\sigma(\xi) = \sum_{j,k} \frac{r_{jk}}{r}\sigma(\alpha_j)\beta_k. \tag{2.24}$$

Set $x_j = \sum_{k=1}^{n} \frac{r_{jk}}{r}\beta_k$. On applying to (2.23) the L-isomorphisms $\sigma_1, \sigma_2, \ldots, \sigma_m$ of KL into $\mathbb{C}$ and keeping in mind (2.24), we obtain m equations

$$\sum_{j=1}^{m} \sigma_i(\alpha_j)x_j = \sigma_i(\xi),\ 1 \le i \le m.$$

On solving for x_j by Cramer's rule, we see that $x_j = \frac{\gamma_j}{\delta}$ with $\delta = \det(A)$, where A is the $m \times m$ matrix having (i, j)th entry $\sigma_i(\alpha_j)$ and γ_j is the determinant of the matrix obtained on replacing the entries of the jth column of A by $\sigma_1(\xi), \ldots, \sigma_m(\xi)$ respectively. So δ, γ_j and $\delta\gamma_j$ are algebraic integers for $1 \le j \le m$. Keeping in mind that $\delta^2 = d_K$, it now follows that $\delta\gamma_j = \delta^2 x_j = \sum_{k=1}^{n} \frac{\delta^2 r_{jk}}{r}\beta_k$ belongs to $\mathcal{O}_L$. Since $\{\beta_1, \ldots, \beta_n\}$ is an integral basis of L, we conclude that $\delta^2\frac{r_{jk}}{r} \in \mathbb{Z}$ for each pair j, k. Therefore

$$d_K\xi = \sum_j \sum_k \frac{\delta^2 r_{jk}}{r}\alpha_j\beta_k \in \mathcal{O}_K\mathcal{O}_L.$$

As ξ is an arbitrary element of $\mathcal{O}_{KL}$, we conclude that $d_K\mathcal{O}_{KL} \subseteq \mathcal{O}_K\mathcal{O}_L$. Interchanging the roles of K and L, we see that $d_L\mathcal{O}_{KL} \subseteq \mathcal{O}_K\mathcal{O}_L$; consequently $d\mathcal{O}_{KL} \subseteq \mathcal{O}_K\mathcal{O}_L$. This proves the proposition. □

Proposition 2.29 *Let K and L be algebraic number fields of degree m and n respectively such that $[KL : \mathbb{Q}] = mn$. If $\{\alpha_1, \alpha_2, \ldots, \alpha_m\}$ and $\{\beta_1, \beta_2, \ldots, \beta_n\}$ are bases of $K/\mathbb{Q}$ and $L/\mathbb{Q}$ respectively, then the discriminant of the basis $\{\alpha_i\beta_j \mid 1 \le i \le m, 1 \le j \le n\}$ of $KL/\mathbb{Q}$ is given by*

$$D_{KL/\mathbb{Q}}(\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_m\beta_{n-1}, \alpha_m\beta_n) = \Big(D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_m)\Big)^n \Big(D_{L/\mathbb{Q}}(\beta_1, \ldots, \beta_n)\Big)^m.$$

Proof Let $\sigma_1, \ldots, \sigma_m$ be all the isomorphisms of K into $\mathbb{C}$ and $\tau_1, \ldots, \tau_n$ be all the isomorphisms of L into $\mathbb{C}$. Let σ_{ij}, $1 \le i \le m$, $1 \le j \le n$ be the isomorphisms of KL into $\mathbb{C}$ such that $\sigma_{ij}|_K = \sigma_i$ and $\sigma_{ij}|_L = \tau_j$. We denote $\sigma_{ij}(\alpha_k\beta_l)$ by $\alpha_k^{(i)}\beta_l^{(j)}$. Let $A = (a_{ij})_{m\times m}$ with $a_{ij} = \alpha_j^{(i)}$ and $B = (b_{ij})_{n\times n}$ with $b_{ij} = \beta_j^{(i)}$. By definition

$$D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_m) = (\det A)^2,$$

$$D_{L/\mathbb{Q}}(\beta_1, \ldots, \beta_n) = (\det B)^2.$$

We arrange the elements $\alpha_i\beta_j$ of the $\mathbb{Q}$-basis of KL as well as the isomorphisms σ_{ij}, $1 \le i \le m, 1 \le j \le n$ of KL in lexicographic order. Then it can be easily seen that

$$D_{KL/\mathbb{Q}}(\alpha_1\beta_1, \ldots, \alpha_1\beta_n; \ldots; \alpha_m\beta_1, \ldots, \alpha_m\beta_n) = D \text{ (say)}$$

is the square of the determinant of the $mn \times mn$ matrix

$$\begin{bmatrix}
\alpha_1^{(1)}\beta_1^{(1)} & \cdots & \alpha_1^{(1)}\beta_n^{(1)} & \cdots\cdots & \alpha_m^{(1)}\beta_1^{(1)} & \cdots & \alpha_m^{(1)}\beta_n^{(1)} \\
\alpha_1^{(1)}\beta_1^{(2)} & \cdots & \alpha_1^{(1)}\beta_n^{(2)} & \cdots\cdots & \alpha_m^{(1)}\beta_1^{(2)} & \cdots & \alpha_m^{(1)}\beta_n^{(2)} \\
\cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots & \cdots\cdots & \cdots & \cdots & \cdots \\
\alpha_1^{(m)}\beta_1^{(n)} & \cdots & \alpha_1^{(m)}\beta_n^{(n)} & \cdots\cdots & \alpha_m^{(m)}\beta_1^{(n)} & \cdots & \alpha_m^{(m)}\beta_n^{(n)}
\end{bmatrix}$$

which can be expressed as a block matrix

$$\begin{bmatrix}
\alpha_1^{(1)}B & \cdots & \alpha_m^{(1)}B \\
\cdots & \cdots & \cdots \\
\cdots & \cdots & \cdots \\
\alpha_1^{(m)}B & \cdots & \alpha_m^{(m)}B
\end{bmatrix}.$$

Using the well known result regarding the determinant of Kronecker product of two square matrices, we see that

$$D = (\det A)^{2n}(\det B)^{2m} = (D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_m))^n (D_{L/\mathbb{Q}}(\beta_1, \ldots, \beta_n))^m$$

as desired. □

We quickly deduce the following corollary from the above two propositions.

Corollary 2.30 *Let $\mathbb{Q}(\sqrt{u}), \mathbb{Q}(\sqrt{v})$ be two distinct quadratic fields having discriminants u, v respectively which are coprime. Then the discriminant of the composite field $\mathbb{Q}(\sqrt{u}, \sqrt{v})$ is u^2v^2.*

Proof Let K, L denote the fields $\mathbb{Q}(\sqrt{u}), \mathbb{Q}(\sqrt{v})$ respectively. Let $\{u_1, u_2\}$ and $\{v_1, v_2\}$ be integral basis of K and L respectively. Since the discriminants of K and L are coprime, $\mathcal{O}_{KL} = \mathcal{O}_K\mathcal{O}_L$ in view of Proposition 2.28. So $\{u_1v_1, u_1v_2, u_2v_1, u_2v_2\}$ is an integral basis of KL. It now follows from Proposition 2.29 that $d_{KL} = d_K^2 d_L^2 = u^2v^2$. □

We now determine the discriminant and an integral basis of the mth cyclotomic field $\mathbb{Q}(\zeta_m)$ for general m, where ζ_m stands for a primitive mth root of unity. Note that if $m \equiv 2 \pmod 4$, then $-\zeta_m$ is a primitive $(m/2)$th root of unity and $\mathbb{Q}(\zeta_m) = \mathbb{Q}(-\zeta_m)$. So to compute the discriminant, we consider cyclotomic fields $\mathbb{Q}(\zeta_m)$ when $m \not\equiv 2 \pmod 4$. It is easy to see that for coprime numbers m and n, the composite ring $\mathbb{Z}[\zeta_m]\mathbb{Z}[\zeta_n]$ is given by

$$\mathbb{Z}[\zeta_m]\mathbb{Z}[\zeta_n] = \mathbb{Z}[\zeta_{mn}], \tag{2.25}$$

because there exist integers a, b such that $am + bn = 1$ and hence $\zeta_{mn} = (\zeta_{mn}^m)^a(\zeta_{mn}^n)^b$ is a product of powers of ζ_m and ζ_n. Using this observation, together with some of the results proved in this section, we derive the following important theorem.

Theorem 2.31 *Let m be any integer ≥ 3 such that $m \not\equiv 2 \pmod 4$. Let ζ a primitive mth root of unity. Then $\{1, \zeta, \ldots, \zeta^{\phi(m)-1}\}$ is an integral basis of $K = \mathbb{Q}(\zeta)$ and*

$$d_K = \frac{(-1)^{\frac{\phi(m)}{2}} m^{\phi(m)}}{\prod\limits_{p|m} p^{\phi(m)/(p-1)}},$$

where p runs over all primes dividing m.

Proof Let s denote the number of distinct primes dividing m. We shall prove the theorem by induction on s. When $s = 1$, i.e., m is a prime power, then the result follows from Theorem 2.26. We now prove the theorem when $s \geq 2$ assuming that it holds for those nth cyclotomic fields where n has at most $s - 1$ distinct prime divisors. Let q be a prime dividing m and write $m = q^r m'$ where q does not divide m'. Let ξ be a primitive (q^r)th root of unity and let ζ' be a primitive m'th root of unity. Denote the fields $\mathbb{Q}(\zeta')$ and $\mathbb{Q}(\xi)$ by K' and L respectively. In view of induction hypothesis, $\mathcal{O}_{K'} = \mathbb{Z}[\zeta']$ and $\mathcal{O}_L = \mathbb{Z}[\xi]$; moreover,

$$d_{K'} = \frac{(-1)^{\frac{\phi(m')}{2}} (m')^{\phi(m')}}{\prod\limits_{p|m'} p^{\phi(m')/(p-1)}} \quad \text{and} \quad d_L = \frac{(-1)^{\frac{\phi(q^r)}{2}} q^{r\phi(q^r)}}{q^{\phi(q^r)/(q-1)}}. \tag{2.26}$$

Note that $[K:\mathbb{Q}] = \phi(m) = \phi(m')\phi(q^r) = [K':\mathbb{Q}][L:\mathbb{Q}]$ and by virtue of Eq. (2.25), $K = K'L$. It is clear from (2.26) that $d_{K'}$ and d_L are coprime. Hence it follows from Proposition 2.28 and Eq. (2.25) that

$$\mathcal{O}_K = \mathcal{O}_{K'}\mathcal{O}_L = \mathbb{Z}[\zeta']\mathbb{Z}[\xi] = \mathbb{Z}[\zeta].$$

The above equality shows that $\{1, \zeta, \ldots, \zeta^{\phi(m)-1}\}$ is an integral basis of K. Keeping in mind that $\mathcal{O}_K = \mathcal{O}_{K'}\mathcal{O}_L$ and applying Proposition 2.29, we see that $d_K = (d_{K'})^{\phi(q^r)}(d_L)^{\phi(m')}$. On substituting for $d_{K'}$ and d_L in the last equality, we obtain

$$d_K = \frac{(-1)^{\phi(m)} m^{\phi(m)}}{\prod\limits_{p|m} p^{\phi(m)/(p-1)}}.$$

This proves the desired formula for d_K because $\phi(m)$ is a multiple of 4 when $s \geq 2$ in view of the hypothesis that $m \not\equiv 2 \pmod 4$. □

Corollary 2.32 *Let ζ be a primitive mth root of unity, $m \geq 3$. Then the ring of algebraic integers of $\mathbb{Q}(\zeta + \zeta^{-1})$ is $\mathbb{Z}[\zeta + \zeta^{-1}]$.*

Proof Since $\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})$ is extension of degree 2, it follows that the extension $\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}$ has degree $\phi(m)/2$. Suppose to the contrary there exists an algebraic integer α in $\mathbb{Q}(\zeta + \zeta^{-1})$ which does not belong to $\mathbb{Z}[\zeta + \zeta^{-1}]$. Write

$$\alpha = a_0 + a_1(\zeta + \zeta^{-1}) + \cdots + a_s(\zeta + \zeta^{-1})^s$$

where $s \leq (\phi(m)/2) - 1$ and a_i's belong to $\mathbb{Q}$. By subtracting those terms for which a_i's belong to $\mathbb{Z}$, we may assume that $a_s \notin \mathbb{Z}$. Multiplying the above equation by ζ^s on both sides and then on expanding the right hand side as a polynomial in ζ, we see that $\zeta^s\alpha = a_s + a_{s-1}\zeta + \cdots + a_s\zeta^{2s}$ is an algebraic integer in $\mathbb{Q}(\zeta)$. In view of Theorem 2.31, $\zeta^s\alpha \in \mathbb{Z}[\zeta]$, which is impossible because $2s \leq \phi(m) - 2$ and $a_s \notin \mathbb{Z}$. This contradiction proves the corollary. □

Remark 2.33 It may be pointed out that when $K = \mathbb{Q}(a^{1/n})$ is a pure field of degree n such that the integer a is either squarefree or coprime with n, then a formula for the discriminant of K and an explicit construction of an integral basis of K is known (see [J-K-S4, J-K-S5, Gas]). However the problem is still unsolved for extensions $K = \mathbb{Q}(a^{1/n})$ of degree n without any restriction on a or n. It is also an open problem to construct an integral basis of pure fields of squarefree degree n although the formula for the discriminant of such fields involving the prime powers dividing a and n was found in 2017 (see [J-K-S3]).

2.5 An Algorithm for Computing Integral Basis

We now prove a theorem which gives an algorithm for computing integral bases of algebraic number fields.

Theorem 2.34 *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Then K has an integral basis of the form $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$, where*

$$\xi_0 = 1 \text{ and } \xi_i = \frac{c_{i0} + c_{i1}\theta + \cdots + c_{i(i-1)}\theta^{i-1} + \theta^i}{d_i}$$

with c_{ij}, d_i belonging to $\mathbb{Z}$ and $d_i > 0$ dividing d_{i+1} for $1 \leq i \leq n-1$. The numbers d_i are uniquely determined by θ. In particular, $[\mathcal{O}_K : \mathbb{Z}[\theta]] = \prod_{i=1}^{n-1} d_i$.

Proof Let r denote the index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$. Then by Lagrange's theorem for finite groups $r\mathcal{O}_K \subset Z[\theta]$. So $\mathcal{O}_K$ is a subgroup of the free abelian group $\frac{1}{r}\mathbb{Z}[\theta]$ which has basis $\left\{\frac{1}{r}, \frac{\theta}{r}, \ldots, \frac{\theta^{n-1}}{r}\right\}$. By Lemma 2.12 and Remark 2.13, there exists a $\mathbb{Z}$- basis of $\mathcal{O}_K$ of the type $\{\xi_0, \xi_1, \ldots, \xi_{n-1}\}$, where for $0 \leq i \leq n-1$

$$\xi_i = \frac{a_{i0} + a_{i1}\theta + \cdots + a_{ii}\theta^i}{r},$$

with a_{ij} belonging to $\mathbb{Z}$ and $a_{ii} > 0$ for each i. Observe that the positive rational number $\xi_0 = \frac{a_{00}}{r}$ being an element of a $\mathbb{Z}$-basis of $\mathcal{O}_K$ must be 1.

We claim that a_{ii} divides r as well as a_{ij} when $0 \leq j < i$, $1 \leq i \leq n-1$ and that d_i divides d_{i+1} for $1 \leq i \leq n-1$ where $d_i = \frac{r}{a_{ii}}$. The claim together with the fact that $\xi_0 = 1$ immediately shows that $\{\xi_0, \ldots, \xi_{n-1}\}$ is an integral basis of K of the desired form once we set $c_{ij} = \frac{a_{ij}}{a_{ii}}$ and $d_i = \frac{r}{a_{ii}}$, $0 \leq j < i$, $1 \leq i \leq n-1$.

The claim will be proved by induction on i. Keeping in mind that $\{1, \xi_1, \ldots, \xi_{n-1}\}$ is an integral basis of K and each a_{ii} is positive, it can be easily seen that an element $\sum_{i=0}^{k} a_i\theta^i$ of $\mathbb{Q}[\theta]$ with $k \leq n-1$ belongs to $\mathcal{O}_K$ if and only if it is a $\mathbb{Z}$-linear combination of $1, \xi_1, \ldots, \xi_k$. So there exist integers b_0, b_1 such that

$$\theta = b_0 + b_1\xi_1 = b_0 + b_1\left(\frac{a_{10} + a_{11}\theta}{r}\right).$$

Comparing the coefficients of θ and constant term on both sides of the above equation, we see that

$$b_1\frac{a_{11}}{r} = 1, \; b_0 + b_1\frac{a_{10}}{r} = 0. \tag{2.27}$$

The first equality of (2.27) shows that $r = b_1a_{11}$. On substituting for r in the second equality of (2.27), we see that a_{11} divides a_{10} and hence the claim is proved for $i = 1$.

Suppose as induction hypothesis that the claim is true for all $i \leq k$; we prove it for $k+1 \leq n-1$. For simplicity of notation, we write $k+1$ as l. Note that the element $\theta\xi_k$ of $\mathcal{O}_K$ can be written as a linear combination of $\xi_0, ..., \xi_l$ with coefficients from $\mathbb{Z}$. So there exist $x_0, ..., x_l$ in $\mathbb{Z}$ such that

$$\theta\xi_k = x_0 + x_1\xi_1 + ... + x_l\xi_l. \tag{2.28}$$

On substituting

$$\xi_i = \frac{c_{i0} + c_{i1}\theta + \cdots + c_{i(i-1)}\theta^{i-1} + \theta^i}{d_i}$$

for $i \leq k$ in view of induction hypothesis and

$$\xi_l = \frac{a_{l0} + a_{l1}\theta + \cdots + a_{lk}\theta^k + a_{ll}\theta^l}{r}$$

in Eq. (2.28) and then comparing the coefficients of θ^l on both sides of this equation, we see that $\frac{1}{d_k} = x_l \frac{a_{ll}}{r}$, i.e.,

$$r = d_k x_l a_{ll}. \tag{2.29}$$

Recall that $l = k+1$ and $d_l = \frac{r}{a_{ll}}$. In view of the Eq. (2.29), d_k divides d_l. Next we show that a_{ll} divides a_{lj} for $0 \leq j \leq k$. Fix one such index j. Again equating first the coefficients of θ^j on both sides of (2.28) and then substituting for r from (2.29), we see that

$$\frac{c_{k(j-1)}}{d_k} = \frac{x_j}{d_j} + \sum_{t=j+1}^{k} \frac{x_t c_{tj}}{d_t} + \frac{x_l a_{lj}}{r} = \frac{x_j}{d_j} + \sum_{t=j+1}^{k} \frac{x_t c_{tj}}{d_t} + \frac{a_{lj}}{d_k a_{ll}}.$$

Since by induction hypothesis d_j divides d_k for $j \leq k$, it is immediate from the above equation that a_{ll} divides a_{lj} and hence the claim is proved.

It can be easily seen that for $j \leq n-1$, $\frac{1}{d_j}$ is the smallest positive element of the set S_j defined by

$$S_j = \left\{ a_j \in \mathbb{Q} \;\middle|\; \sum_{i=0}^{j} a_i\theta^i \in \mathcal{O}_K \text{ for some } a_0, a_1, ..., a_{j-1} \text{ in } \mathbb{Q} \right\},$$

because an element $\sum_{i=0}^{j} a_i\theta^i$ of $\mathbb{Q}[\theta]$ belongs to $\mathcal{O}_K$ if and only if it is a $\mathbb{Z}$-linear combination of $1, \xi_1, \ldots, \xi_j$. This completes the proof of the theorem. □

Remark 2.35 If $K = \mathbb{Q}(\theta)$ and $\{\xi_0, ..., \xi_{n-1}\}$ are as in above theorem, then using this basis together with the division algorithm, one can easily construct an integral basis $\{\beta_0, ..., \beta_{n-1}\}$ of K, where

$$\beta_0 = 1, \quad \beta_i = \frac{b_{i0} + b_{i1}\theta + \cdots + b_{i(i-1)}\theta^{i-1} + \theta^i}{d_i}$$

with b_{ij}, d_i belonging to $\mathbb{Z}$, $d_i > 0$ dividing d_{i+1}, $d_0 = 1$ and $0 \leq b_{ij} < \frac{d_i}{d_j}$ for $0 \leq j < i \leq n-1$. In fact, β_i can be obtained from ξ_i by subtracting a suitable $\mathbb{Z}$-linear combination of $\xi_0, \ldots, \xi_{i-1}$.

The following examples are given to illustrate the above theorem.

Example 2.36 We compute an integral basis and discriminant of the field $K = \mathbb{Q}(\theta)$, where θ is a root of the polynomial $f(X) = X^3 - X - 4$. It will be first shown that $f(X)$ is irreducible over $\mathbb{Q}$. If $f(X)$ is reducible over $\mathbb{Q}$, then $f(X)$ has a root in $\mathbb{Z}$, say α. Since $\alpha^3 - \alpha = 4$, we see that α divides 4 in $\mathbb{Z}$ and hence α belongs to $\{\pm 1, \pm 2, \pm 4\}$. We can check by direct verification that none of these integers is a root of $f(X)$. Thus $f(X)$ is irreducible over $\mathbb{Q}$. Using Corollary 2.16 and Lemma 2.6, we see that

$$d_K(\operatorname{ind}\theta)^2 = D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(3\theta^2 - 1) = -428 = -2^2 \cdot 107.$$

The above equation shows that $\operatorname{ind}\theta$ is either 1 or 2. If $\operatorname{ind}\theta$ is equal to 2, then in view of Theorem 2.34, $\{1, \theta, \eta\}$ will be an integral basis of K where $\eta = \frac{a+b\theta+\theta^2}{2}$ for some $a, b \in \mathbb{Z}$ with $0 \leq a, b \leq 1$. Keeping in mind that $Tr_{K/\mathbb{Q}}(\theta) = 0$ and $Tr_{K/\mathbb{Q}}(\theta^2) = 2$, we see that $Tr_{K/\mathbb{Q}}(\eta) = \frac{3a}{2} + 1$ which is an integer only when a is even. So we may assume that $a = 0$ and $\eta = \frac{b\theta+\theta^2}{2}$. Note that $b = 0$ is impossible because the characteristic polynomial of $\frac{\theta^2}{2}$ relative to $K/\mathbb{Q}$ is $X^3 - X^2 + \frac{X}{4} - 2$. Thus we see that if $\operatorname{ind}\theta$ is 2, then b must be 1. We are going to show that $\frac{\theta+\theta^2}{2}$ is an algebraic integer. A simple calculation shows that the characteristic polynomial of $\frac{\theta+\theta^2}{2}$ relative to $K/\mathbb{Q}$ is $X^3 - X^2 - 3X - 2$ which implies that $\frac{\theta+\theta^2}{2}$ belongs to $\mathcal{O}_K$. This proves that index of θ is 2, $d_K = -107$ and $\left\{1, \theta, (\theta + \theta^2)/2\right\}$ is an integral basis of K.

Example 2.37 We compute an integral basis and the discriminant of the field $K = \mathbb{Q}(\theta)$, where θ is a root of the polynomial $f(X) = X^3 + 11X + 4$. Arguing as in above example, one can check that $f(X)$ is irreducible over $\mathbb{Q}$ and

$$D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(3\theta^2 + 11) = -5756 = -2^2 \cdot 1439.$$

Since 1439 is a prime, $\operatorname{ind}\theta$ is 1 or 2. If $\operatorname{ind}\theta$ is 2, then $\{1, \theta, \eta\}$ will be an integral basis of K where $\eta = \frac{a+b\theta+\theta^2}{2}$ for some $a, b \in \mathbb{Z}$ with $0 \leq a, b \leq 1$. Keeping in mind that $Tr_{K/\mathbb{Q}}(\theta) = 0$ and $Tr_{K/\mathbb{Q}}(\theta^2) = -22$, we see that $Tr_{K/\mathbb{Q}}(\eta) = \frac{3a}{2} - 11$ which is an integer only when a is even. So we may assume $a = 0$ and $\eta = \frac{b\theta+\theta^2}{2}$. Note that $\frac{\theta^2}{2}$ does not belong to $\mathcal{O}_K$ because $\frac{\theta^3}{2} = -2 - \frac{11\theta}{2}$ is not in $\mathcal{O}_K$ since $\frac{\theta}{2}$ is not in $\mathcal{O}_K$. As regards $\frac{\theta+\theta^2}{2}$, it can be shown that its characteristic polynomial relative

to $K/\mathbb{Q}$ is $X^3 + 11X^2 + 36X + 4$ and hence it is an algebraic integer. Therefore ind θ is 2. Hence $\{1, \theta, (\theta + \theta^2)/2\}$ is an integral basis of K and $d_K = -1439$.

Example 2.38 We compute an integral basis and the discriminant of the field $K = \mathbb{Q}(\theta)$, where θ is a root of the polynomial $f(X) = X^4 + 9X + 9$. We first show that $f(X)$ is irreducible over $\mathbb{Q}$. Arguing as in Example 2.36, it can be easily seen that $f(X)$ does not have a linear factor over $\mathbb{Q}$, because none of the elements $\pm 1, \pm 3, \pm 9$ is a root of $f(X)$. Suppose to the contrary that $f(X)$ factors as a product of two quadratic monic irreducible polynomials $g(X), h(X)$ over $\mathbb{Q}$. Then $g(X), h(X) \in \mathbb{Z}[X]$ because their roots are algebraic integers. Write $g(X) = X^2 + aX + b$ and $h(X) = X^2 + a'X + b'$. On comparing coefficients of the like terms in $f(X)$ and $g(X)h(X)$, we see that $a + a' = 0$, $ab' + a'b = 9$ and $bb' = 9$. The first two equalities imply that $a(b' - b) = 9$ which is impossible because b, b' are odd in view of third equality. This contradiction proves that $f(X)$ is irreducible over $\mathbb{Q}$.

Applying Lemma 2.6, we see that $D_{K/\mathbb{Q}}(1, \theta, \theta^2, \theta^3) = 3^6 \cdot 13$. So ind θ divides 3^3. Therefore by Theorem 2.34, K has an integral basis of the form $\{1, \xi_1, \xi_2, \xi_3\}$, where

$$\xi_1 = \frac{a_0 + \theta}{3^{k_1}}, \xi_2 = \frac{b_0 + b_1\theta + \theta^2}{3^{k_2}}, \xi_3 = \frac{c_0 + c_1\theta + c_2\theta^2 + \theta^3}{3^{k_3}}$$

with $0 \le k_1 \le k_2 \le k_3 \le 3$ and $k_1 + k_2 + k_3 \le 3$. If $k_1 = 1$, then $\frac{a_0+\theta}{3}$ would belong to $\mathcal{O}_K$ for some $a_0 \in \mathbb{Z}$ with $0 \le a_0 \le 2$. Since $Tr_{K/\mathbb{Q}}(\frac{a_0+\theta}{3}) = \frac{4a_0}{3}$, we see that a_0 must be 0. Note that $\frac{\theta}{3}$ does not belong to $\mathcal{O}_K$ as the minimal polynomial of $\frac{\theta}{3}$ over $\mathbb{Q}$ is $X^4 + \frac{X}{3} + \frac{1}{9}$. So $k_1 = 0$. Recall that $0 \le k_2 \le 1$. One can check that $\frac{\theta^2}{3}$ belongs to $\mathcal{O}_K$ as its characteristic polynomial with respect to $K/\mathbb{Q}$ is $X^4 + 2X^2 - 3X + 1$. This proves that $k_2 = 1$. Now we explore the possibility whether k_3 can be 2 or not. Suppose that k_3 is 2, then $\frac{c_0+c_1\theta+c_2\theta^2+\theta^3}{3^2} \in \mathcal{O}_K$ for some $c_i \in \mathbb{Z}$, with $0 \le c_i < 9$ for $i = 0, 1$ and $0 \le c_2 < 3$ in view of Remark 2.35. Keeping in mind that $Tr_{K/\mathbb{Q}}(\theta) = Tr_{K/\mathbb{Q}}(\theta^2) = 0$ and $Tr_{K/\mathbb{Q}}(\theta^3) = 27$, we see that $c_0 = 0$. Taking $c_2 = 0, 1, 2$ respectively, we compute the characteristic polynomials relative to $K/\mathbb{Q}$ of $\frac{\theta^3+c_1\theta}{9}$, $\frac{\theta^3+\theta^2+c_1\theta}{9}$, $\frac{\theta^3+2\theta^2+c_1\theta}{9}$. These polynomials respectively are

- $X^4 + 3X^3 + (3 + \frac{4c_1}{9})X^2 + (\frac{c_1^3}{81} + \frac{5c_1}{9} + 1)X + \frac{c_1^4}{729} + \frac{2c_1^2}{81} + \frac{c_1}{9} + \frac{1}{9}$,
- $X^4 + 3X^3 + (\frac{29+7c_1}{9})X^2 + (\frac{c_1^3}{81} + \frac{4c_1^2}{81} + \frac{8c_1}{9} + \frac{1}{3})X + \frac{c_1^4}{729} + \frac{5c_1^2}{81} + \frac{4c_1}{81} + \frac{1}{81}$,
- $X^4 + 3X^3 + (\frac{35+10c_1}{9})X^2 + (\frac{c_1^3}{81} + \frac{8c_1^2}{81} + \frac{11c_1}{9} - \frac{11}{9})X + \frac{c_1^4}{729} + \frac{8c_1^2}{81} - \frac{5c_1}{27} + \frac{7}{81}$

Clearly the coefficient of X^2 in the first polynomial does not belong to $\mathbb{Z}$. In the second polynomial if the coefficient of X^2 is in $\mathbb{Z}$, then $c_1 = 1$, because $0 \le c_1 < 9$; in this situation the constant term of the second polynomial will not belong to $\mathbb{Z}$. By a similar argument, we see that the third polynomial also does not belong to $\mathbb{Z}[X]$. So $k_3 = 1$. Therefore $\{1, \theta, \frac{\theta^2}{3}, \frac{\theta^3}{3}\}$ is an integral basis of K and $d_K = 3^2 \cdot 13 = 117$.

Exercises

1. If the minimal polynomial of a complex number α over $\mathbb{Q}$ is $X^n + aX + b$, show that for $K = \mathbb{Q}(\alpha)$, $D_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}}\big(n^n b^{n-1} + a^n(1-n)^{n-1}\big)$.
2. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n and let $m \in \mathbb{Z}$. Show that $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = D_{K/\mathbb{Q}}\big(1, (\theta+m), \ldots, (\theta+m)^{n-1}\big)$.
3. If $\theta^3 + 4\theta + 7 = 0$, then prove that $\{1, \theta, \theta^2\}$ form an integral basis of $\mathbb{Q}(\theta)$.
4. Find the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$, where $\theta^3 + \theta + 1 = 0$.
5. Let $K = \mathbb{Q}(\theta)$, where θ satisfies $\theta^3 - 4\theta + 2 = 0$. Prove that $d_K = 148$.
6. Find an integral basis of each of the three cubic fields.
   (a) $K_1 = \mathbb{Q}(\theta)$, $\theta^3 - 18\theta - 6 = 0$.
   (b) $K_2 = \mathbb{Q}(\theta)$, $\theta^3 - 36\theta - 78 = 0$.
   (c) $K_3 = \mathbb{Q}(\theta)$, $\theta^3 - 54\theta - 150 = 0$.
   Verify all the three fields have the same discriminant.
7. Find an integral basis and the discriminant of $K = \mathbb{Q}(\theta)$, where $\theta^4 - 2\theta - 2 = 0$.
8. Find the discriminant and an integral basis of the field $K = \mathbb{Q}(\theta)$, where θ is a root of the polynomial $X^4 - 2$.
9. Let $K = \mathbb{Q}(\theta)$ where θ satisfies $\theta^3 - \theta - 2 = 0$. Prove that $1, \theta, \theta^2$ form an integral basis of $\mathbb{Q}(\theta)$ and $d_K = -104$.
10. Consider $K = \mathbb{Q}(\theta)$ where θ satisfies $\theta^3 - 6\theta + 36 = 0$. Prove that $\{1, \theta, \theta^2/6\}$ is an integral basis of K and $d_K = -2^2 \cdot 3 \cdot 79$.
11. Let $K = \mathbb{Q}(\theta)$, where $\theta^3 = 175$. Prove that K is not monogenic.
12. Let K be the field[4] $\mathbb{Q}(\theta)$, where θ is a root of the polynomial $f(X) = X^3 + X^2 - 2X - 1$. Prove that $d_K = 49$. Also find an integral basis of K.
13. Prove that conjugate algebraic number fields have the same discriminant.
14. For an algebraic number field K, prove that $\sqrt{d_K}$ belongs to the smallest normal extension of K containing $\mathbb{Q}$.
15. Let $\zeta = e^{2\pi\iota/p}$, p an odd prime. Show that the field $K = \mathbb{Q}(\zeta)$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$ and it contains $\sqrt{-p}$ if $p \equiv -1 \pmod 4$.
16. Prove that $\mathbb{Q}(\sqrt{2})$ is contained in $\mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi\iota/8}$.
17. Let D be the discriminant of a quadratic field $\mathbb{Q}(\sqrt{D})$. Then show that D can be written as the product[5] $d_1 \cdots d_t$ where $|d_1|, \ldots, |d_t|$ are powers of distinct primes and d_i is the discriminant of $\mathbb{Q}(\sqrt{d_i})$ for each i.
18. Show that a quadratic field with discriminant D is a subfield of $\mathbb{Q}(\zeta)$ where ζ is a primitive mth root of unity, m being the absolute value of D.
19. Find the discriminant and an integral basis of $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$.
20. Let D be the discriminant of a quadratic field $\mathbb{Q}(\sqrt{D})$ and $d_1, \ldots, d_t$ be as in Exercise 17. A divisor u of D of the type $\prod_{i=1}^{t}(d_i)^{a_i}$, where $a_i \in \{0, 1\}$ is called

[4] It is known that K is the field having smallest discriminant among all totally real cubic fields. An algebraic number field is said to be totally real if all its isomorphisms in $\mathbb{C}$ are real.

[5] For example, $-40 = 5(-8)$ and $28 = (-4)(-7)$.

a discriminantal divisor of D. Let u be a discriminantal divisor of D different from 1 and D. Then prove that the discriminant of the field $\mathbb{Q}(\sqrt{u}, \sqrt{D})$ is D^2.

21. Let $u_1, ..., u_s$ be pairwise coprime integers such that u_i is the discriminant of the quadratic field $\mathbb{Q}(\sqrt{u_i})$ for $1 \leq i \leq s$. Prove that the degree of the composite field $K = \mathbb{Q}(\sqrt{u_1}, ..., \sqrt{u_s})$ is 2^s. Find the discriminant of K.

Chapter 3
Properties of the Ring of Algebraic Integers

3.1 Factorisation into Irreducible Elements

We begin with a review of some basic notions of ring theory.

Definition Let R be an integral domain. An element α of R is said to be a *unit* of R if there exists $\beta \in R$ such that $\alpha\beta = 1$. Two elements α, β are said to be *associates* if there exists a unit ϵ of R such that $\beta = \alpha\epsilon$. A non-zero non-unit element α of R is said to be an *irreducible* element of R if whenever $\alpha = \beta\gamma$ with $\beta, \gamma \in R$, then either β or γ is a unit. A non-zero non-unit element α of R is said to be a *prime* element of R if whenever $\alpha \mid \beta\gamma$ with $\beta, \gamma \in R$, then either $\alpha \mid \beta$ or $\alpha \mid \gamma$.

Every prime element is irreducible in an integral domain but the converse is not true in general (see Example 3.36).

Definition An integral domain R is said to be a *factorization domain* if every non-zero non-unit element of R can be expressed as a product of finitely many irreducible elements of R. A factorization domain R is called a *unique factorization domain(UFD)* if whenever $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$ with every p_i, q_j irreducible in R, then $r = s$ and there is a permutation σ of $\{1, 2, \ldots, r\}$ such that p_i and $q_{\sigma(i)}$ are associates for all $i = 1, 2, \ldots, r$. An integral domain R is said to be a *principal ideal domain* if every ideal of R is a principal ideal.

Every principal ideal domain is a unique factorization domain but the converse is not true in general. However we shall prove in this chapter that the converse is true for the ring of algebraic integers $\mathcal{O}_K$ of an algebraic number field K. We shall also prove that each $\mathcal{O}_K$ is a factorization domain.

The following proposition characterizes the units of $\mathcal{O}_K$ in terms of their norms.

Proposition 3.1 *Let K be an algebraic number field. An element α of $\mathcal{O}_K$ is a unit if and only if $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.*

Proof Suppose first that α is a unit of $\mathcal{O}_K$. Then there exists $\beta \in \mathcal{O}_K$ such that $\alpha\beta = 1$. So $N_{K/\mathbb{Q}}(\alpha)N_{K/\mathbb{Q}}(\beta) = 1$. As norm of an algebraic integer with respect to the extension $K/\mathbb{Q}$ belongs to $\mathbb{Z}$ in view of Corollary 1.22, we see that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_3

Conversely suppose that $N_{K/\mathbb{Q}}(\alpha) = \pm 1$ for some $\alpha \in \mathcal{O}_K$. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be all the roots (counting multiplicities, if any) of the characteristic polynomial of α relative to $K/\mathbb{Q}$. By Theorem 1.18, $N_{K/\mathbb{Q}}(\alpha) = \alpha_1\alpha_2 \cdots \alpha_n = \pm 1$. Write $\beta = \prod_{i=2}^{n} \alpha_i$. Then β is an algebraic integer; also $\beta = \dfrac{\pm 1}{\alpha} \in \mathbb{Q}(\alpha) \subseteq K$. So $\beta \in \mathcal{O}_K$ and $\alpha\beta = \pm 1$. Thus α is a unit of $\mathcal{O}_K$. □

Recall that for an element $\alpha \in \mathcal{O}_K$ by virtue of Theorem 1.20, $N_{K/\mathbb{Q}}(\alpha) = (N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha))^{[K:\mathbb{Q}(\alpha)]}$. So Proposition 3.1 implies that α is a unit of $\mathcal{O}_K$ if and only if $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \pm 1$.

Corollary 3.2 *Let K be an algebraic number field and α be an element of $\mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\alpha)|$ is a prime number, then α is an irreducible element of $\mathcal{O}_K$.*

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

If α is as in the above corollary, then it will be proved in Corollary 3.35 that α is indeed a prime element of $\mathcal{O}_K$.

Lemma 3.3 *If α is a non-zero algebraic integer belonging to an algebraic number field K, then the element $N_{K/\mathbb{Q}}(\alpha)/\alpha$ is an algebraic integer in K.*

Proof Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_n$ be all the roots (counting multiplicities, if any) of the characteristic polynomial of α with respect to $K/\mathbb{Q}$. Then by Theorem 1.18, $N_{K/\mathbb{Q}}(\alpha) = \prod_{i=1}^{n} \alpha_i$, which shows that $N_{K/\mathbb{Q}}(\alpha)/\alpha = \prod_{i=2}^{n} \alpha_i$ is an algebraic integer belonging to $\mathbb{Q}(\alpha)$. □

We next prove that $\mathcal{O}_K$ is a factorization domain.

Theorem 3.4 *Let K be an algebraic number field. Then any non-zero non-unit element α of $\mathcal{O}_K$ can be written as a product of finitely many irreducible elements of $\mathcal{O}_K$.*

Proof We prove the theorem by induction on $|N_{K/\mathbb{Q}}(\alpha)|$. When $|N_{K/\mathbb{Q}}(\alpha)| = 1$, then α is a unit by Proposition 3.1. When $|N_{K/\mathbb{Q}}(\alpha)| = 2$, then α is irreducible by Corollary 3.2. Suppose the theorem holds for all $\alpha \in \mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(\alpha)| < m$. Let α be an element of $\mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(\alpha)| = m$. If α is irreducible, then we are done, otherwise we can write $\alpha = \beta\gamma$ where β, γ are non-units of $\mathcal{O}_K$. So $|N_{K/\mathbb{Q}}(\beta)| > 1, |N_{K/\mathbb{Q}}(\gamma)| > 1$ by Proposition 3.1. Therefore $|N_{K/\mathbb{Q}}(\beta)| < m, |N_{K/\mathbb{Q}}(\gamma)| < m$. By induction hypothesis β, γ can be written as a product of finitely many irreducible elements of $\mathcal{O}_K$ and hence $\alpha = \beta\gamma$ can be so written. □

It may be pointed out that the ring $\mathcal{A}$ consisting of all algebraic integers in $\mathbb{C}$ does not have an irreducible element, because for any $\alpha \in \mathcal{A}$, $\sqrt{\alpha} \in \mathcal{A}$. In particular $\mathcal{A}$ is not a factorization domain.

Corollary 3.5 *For an algebraic number field $K, \mathcal{O}_K$ has infinitely many non-associate irreducible elements.*

Proof For any rational prime p, there exists an irreducible element π_p (say) of $\mathcal{O}_K$ dividing p in view of the above theorem. If $p \neq q$ are prime numbers, then π_p, π_q cannot be associates, for otherwise $|N_{K/\mathbb{Q}}(\pi_p)| = |N_{K/\mathbb{Q}}(\pi_q)|$, which is impossible because $N_{K/\mathbb{Q}}(\pi_p)$ divides $N_{K/\mathbb{Q}}(p) = p^n$ and $N_{K/\mathbb{Q}}(\pi_q)$ divides q^n, where n is the degree of $K/\mathbb{Q}$. □

Remark 3.6 For an imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$ with d a negative square free integer, Gauss[1] proved that $\mathcal{O}_K$ is a UFD for $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. He also conjectured that these are the only nine imaginary quadratic fields K for which $\mathcal{O}_K$ is a UFD. This conjecture remained open until 1966 when it was proved independently by Baker [Bak] and Stark [Sta]. We will come back to this conjecture in Chap. 8 (see Remark 8.26). Gauss also conjectured that there are infinitely many real quadratic fields whose ring of algebraic integers are unique factorization domains. The second conjecture is still open.

3.2 $\mathcal{O}_K$ as a Dedekind Domain

In this section, we study properties of ideals of $\mathcal{O}_K$. We first recall some definitions.

Definition Let R be an integral domain with quotient field F. A subset I of F is called a fractional ideal of R if the following three conditions are satisfied:

(i) I is an additive subgroup of F.
(ii) For every $a \in I$ and $r \in R$, $ar \in I$.
(iii) There exists $\alpha \neq 0$ in R such that $\alpha I \subseteq R$.

Note that every ideal of R is a fractional ideal of R, but the converse is not true. To be more specific, an ideal of R will sometimes be called an **integral ideal** of R.

Notation. If I, J are fractional ideals of R, then IJ is defined to be the set consisting of all finite sums of the type $\sum_i a_i b_i$ where a_i's belong to I and b_i's belong to J. Note that IJ is a fractional ideal of R and is called the product of I with J.

[1] At the age of 21, the German mathematician Carl Friedrich Gauss wrote a book (*cf.* [Gau]) in Latin entitled "Disquisitiones Arithmeticae" meaning "Arithmetical Investigations" . This book had a revolutionary impact on number theory and is considered to be the most important and wide-ranging since Euclid's series 'Elements' consisting of thirteen volumes.

Definition A non-zero fractional ideal I of R is called invertible if there exists a fractional ideal J of R such that $IJ = R$. Such an ideal J is called (the) inverse of I. One can check that if inverse of I exists, then it is unique. We shall denote the inverse of an ideal I by I^{-1}.

Note that if a fractional ideal I of an integral domain R with quotient field F is invertible, then

$$I^{-1} = \{\alpha \in F \mid \alpha I \subseteq R\}; \tag{3.1}$$

this holds because if I' denotes the ideal on the right hand side of (3.1) and J denotes the inverse of I, then clearly $J \subseteq I'$ and $I' = I'(IJ) = (I'I)J \subseteq RJ = J$.

Definition A fractional ideal I of R is said to be finitely generated if there exist $a_1, \ldots, a_n$ in I such that $I = Ra_1 + \cdots + Ra_n$, i.e., every $\alpha \in I$ can be written as $\alpha = r_1a_1 + \cdots + r_na_n$ for some $r_1, \ldots, r_n$ in R; in this situation $a_1, \ldots, a_n$ is called a system of generators of I and we sometimes express it by writing $I = \langle a_1, \ldots, a_n \rangle$. If a fractional ideal is generated by a single element, it is called a principal fractional ideal.

We are soon going to prove that every ideal of the ring of algebraic integers in an algebraic number field is finitely generated. Indeed we prove the following slightly more general result.

Theorem 3.7 *Let K be an algebraic number field of degree n. Any non-zero ideal I of $\mathcal{O}_K$ is a free abelian group of rank n.*

Proof Let I be a non-zero ideal of $\mathcal{O}_K$. Then by Theorem 2.7, $\mathcal{O}_K$ is a free abelian group of rank n and by Lemma 2.12, I is a free abelian group of rank $m \leq n$. We have to prove that $m = n$. So it only remains to be shown that I contains a set of n linearly independent elements over $\mathbb{Q}$. To verify the last statement, let $\{w_1, \ldots, w_n\}$ be an integral basis of K and let α be a non-zero element of I, then $\alpha w_i \in I$ for $1 \leq i \leq n$ and $\{\alpha w_1, \alpha w_2, \ldots, \alpha w_n\}$ is linearly independent over $\mathbb{Q}$. □

The following corollary is an immediate consequence of the above theorem.

Corollary 3.8 *Let K be an algebraic number field. Then every ideal of $\mathcal{O}_K$ is finitely generated.*

The class of commutative rings with identity in which every ideal is finitely generated is of fundamental importance in ring theory. Such rings are called *Noetherian rings* and are named after a great algebraist Emmy Noether[2] who introduced this

[2] Emmy Noether (1882–1935) obtained the fundamental results for Noetherian rings generalizing many of the earlier results for polynomial rings by Hilbert, Lasker and Macaulay. In the words of Professor Peter Roquette [Roq2, Sect. 5.5], "It is quite remarkable that the importance of Emmy Noether had been clearly recognised in the USA at that time already - at least among the leading mathematicians". He quotes Professor N. Wiener of MIT whose testimonial written for Emmy Noether says "Miss Noether is a great personality; the greatest woman mathematician who has ever lived and a greatest woman scientist of any sort now living. Leaving all questions of sex aside, she is one of the ten or twelve leading mathematicians of the entire world...".

concept. We now prove a basic proposition which gives two more equivalent conditions for a ring to be Noetherian.

Proposition 3.9 *For a commutative ring R with identity, the following conditions are equivalent.*

(i) Every ideal of R is finitely generated.
(ii) Every ascending chain of ideals of R is stationary i.e., if $I_1 \subseteq I_2 \subseteq \ldots$ are ideals of R, then there exists m such that $I_n = I_m$ for every $n \geq m$.
(iii) Every non-empty family S of ideals of R has a maximal element with respect to the inclusion relation, i.e., there exists $J \in S$ such that J is not properly contained in any member of S.

Proof (i) $\Longrightarrow$ (ii). Let $I_1 \subseteq I_2 \subseteq \ldots$ be a chain of ideals of R and let $I = \bigcup_{n=1}^{\infty} I_n$. Then I is an ideal of R. So I is finitely generated, say $I = \langle a_1, a_2, \ldots, a_r \rangle$. Clearly there exists a positive integer m such that $a_1, a_2, \ldots, a_r$ belong to I_m. Then $I = I_m$ and hence $I_n = I_m$ for every $n \geq m$.
(ii) $\Longrightarrow$ (iii). Let S be a non-empty set of ideals of R. Suppose to the contrary S does not have a maximal element. Choose I_1 belonging to S. Since I_1 is not maximal, there exists $I_2 \in S$ such that $I_1 \subsetneqq I_2$. Inductively, having found I_n we can choose $I_{n+1} \in S$ such that $I_n \subsetneqq I_{n+1}$. So we have an infinite chain $I_1 \subsetneqq I_2 \subsetneqq \ldots$ of ideals of R which is not stationary. This contradiction proves that (ii) implies (iii).
(iii) $\Longrightarrow$ (i). Let I be an ideal of R and let S be the set of all finitely generated ideals of R contained in I. Then S is non-empty as $\{0\} \in S$. So S has a maximal element, say J. If $a \in I \setminus J$, then $J + aR \subseteq I$ is a finitely generated ideal of R properly containing J, which is impossible. Hence $J = I$ and I is finitely generated. □

Recall that an ideal $\mathfrak{p} \neq R$ of a ring R is called a *prime ideal* if whenever $\alpha\beta \in \mathfrak{p}$ for $\alpha, \beta \in R$, then either $\alpha \in \mathfrak{p}$ or $\beta \in \mathfrak{p}$. An ideal $\mathfrak{m}$ of R is called *maximal* if $\mathfrak{m} \neq R$ and $\mathfrak{m}$ is not properly contained in any ideal of R except R.

It can easily be seen that every maximal ideal of a commutative ring with identity is a prime ideal but the converse is not true. For example, consider $R = \mathbb{Z}[X]$, then $\langle 2 \rangle$ is a prime ideal of R but it is not maximal as $\langle 2 \rangle \subsetneqq \langle 2, X \rangle \subsetneqq \mathbb{Z}[X]$. However the following theorem shows that the converse holds for the ring of algebraic integers of an algebraic number field.

Theorem 3.10 *Let K be an algebraic number field. Then every non-zero prime ideal of $\mathcal{O}_K$ is maximal.*

Proof Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. Let $\mathfrak{m}$ be an ideal of $\mathcal{O}_K$ such that $\mathfrak{p}$ is properly contained in $\mathfrak{m}$. We shall prove that $\mathfrak{m} = \mathcal{O}_K$. Fix a positive integer a belonging to $\mathfrak{p}$; such a positive integer exists, because if β is a non-zero element of $\mathfrak{p}$, then $N_{K/\mathbb{Q}}(\beta)$ belongs to $\mathfrak{p} \cap \mathbb{Z}$ in view of Lemma 3.3 and Corollary 1.22.

Let $\{w_1, \ldots, w_n\}$ be an integral basis of K and α be an element of $\mathcal{O}_K$. Then there exist $a_1, \ldots, a_n \in \mathbb{Z}$ such that $\alpha = \sum_{i=1}^{n} a_i w_i$. By division algorithm, write

$$a_i = aq_i + r_i, \quad q_i \in \mathbb{Z}, \quad 0 \leq r_i < a.$$

So α can be written as

$$\alpha = a \sum_{i=1}^{n} q_i w_i + \sum_{i=1}^{n} r_i w_i. \tag{3.2}$$

Define

$$S = \left\{ \sum_{i=1}^{n} b_i w_i \mid b_i \in \mathbb{Z}, 0 \leq b_i < a, 1 \leq i \leq n \right\}. \tag{3.3}$$

Then S is a finite set having a^n elements. Fix an element $\delta \in \mathfrak{m}$ such that $\delta \notin \mathfrak{p}$. Keeping in mind (3.2), for any positive integer j, we write

$$\delta^j = a\beta_j + \gamma_j; \quad \beta_j \in \mathcal{O}_K, \ \gamma_j \in S.$$

Since S is a finite set, there exist natural numbers j, k with $j > k$ such that $\gamma_j = \gamma_k$, i.e.,

$$\delta^j = a\beta_j + \gamma_j, \quad \delta^k = a\beta_k + \gamma_k = a\beta_k + \gamma_j.$$

It follows from the above equations that

$$\delta^k(\delta^{(j-k)} - 1) = a(\beta_k - \beta_j).$$

Keeping in mind that $a \in \mathfrak{p}$, we see that the right hand side of the above equation belongs to $\mathfrak{p}$. Since $\delta^k \notin \mathfrak{p}$, it follows that $\delta^{(j-k)} - 1 \in \mathfrak{p} \subseteq \mathfrak{m}$. But $\delta \in \mathfrak{m}$ and hence $1 \in \mathfrak{m}$. Therefore $\mathfrak{m} = \mathcal{O}_K$. □

Combining Corollaries 1.10, 3.8 and Theorem 3.10, we see that $\mathcal{O}_K$ is an integrally closed domain which is Noetherian and in which every non-zero prime ideal is maximal. This leads to the following definition.

Definition An integral domain R is called a *Dedekind* [3] *domain* if R is integrally closed Noetherian domain in which every non-zero prime ideal is maximal.

As pointed out above, $\mathcal{O}_K$ is a Dedekind domain for each algebraic number field K. It can be easily seen that every principal ideal domain is a Dedekind domain.

[3] Dedekind domains are named after a German mathematician Richard Dedekind (1831–1916) who made a number of highly significant contributions to ring theory, algebraic number theory and the foundations of real numbers. Several notions in mathematics are named after Richard Dedekind. For example Dedekind cut, Dedekind domain, Dedekind zeta-functions. Ideals were first proposed by him in the 3rd edition of the book-" Vorlesungen über Zahlentheorie" edited by Dedekind which is based on Dirichlet's lectures. In the words of H M Edwards [Edw], "Dedekind's legacy consisted not only of important theorems, examples and concepts, but a whole style of mathematics that has been an inspiration to each succeeding generation".

The theory of Dedekind domains was created as a generalization of results concerning rings of algebraic integers in algebraic number fields, obtained mainly by Dedekind in 1871. It was observed already by Dedekind and Weber that many of these results apply also to several other categories of integrally closed domains. However the general theory had to wait for the introduction of abstract methods and concepts in Algebra. In fact the definition of an abstract ring in the form used today appears for the first time in Fraenkel's paper of 1916. There are several equivalent definitions of a Dedekind domain (see [Lu-Pa1, Chap. 4], [Za-Sa, Chap. V]).

We now prove a few results regarding the factorization of ideals in a Dedekind domain which will be needed in the sequel.

Theorem 3.11 *Every non-zero fractional ideal of a Dedekind domain is invertible.*

Theorem 3.12 *Let R be a Dedekind domain. Then every non-zero proper ideal of R can be written as a product of prime ideals of R in one and only one way except for the order of factors.*[4]

It may be pointed out that the converse of the above two theorems is true. If every non-zero fractional ideal of an integral domain R is invertible, then R is a Dedekind domain (cf. [Lu-Pa1, Chap. 14]). It is also known that in an integral domain R, if every non-zero proper ideal R can be written as a product of prime ideals of R, then R is a Dedekind domain; the uniqueness of factorization follows from existence. An easy proof of this was given by Cohen (see [Za-Sa, Chap. V]). We shall not prove the above mentioned results as these are not needed in the sequel.

We first prove a couple of lemmas which are used in the proof of Theorems 3.11, 3.12.

Lemma 3.13 *If R is a Noetherian domain and I is a non-zero ideal of R different from R, then there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of R such that $\mathfrak{p}_1 \cdots \mathfrak{p}_r \subseteq I \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_r$.*

Proof Suppose that the lemma is false. Let S denote the set of all proper ideals of R which do not satisfy the property of the lemma. Let J be a maximal element of S. Such a maximal element exists because R is Noetherian. Then J cannot be a prime ideal of R. Hence there exist a, b in R such that $ab \in J$ but $a \notin J, b \notin J$. Consider $A = J + aR$, $B = J + bR$. Note that

$$AB \subseteq J \subseteq A \cap B. \tag{3.4}$$

We verify that $A \neq R$. Suppose if possible that $A = R$, then (3.4) implies that $RB \subseteq J \subseteq R \cap B = B$. So $B \subseteq J \subseteq B$ and therefore $J = B$. But $b \notin J$. This contradiction proves that $A \neq R$. Similarly it can be verified that $B \neq R$. By maximality

[4] For the ring of algebraic integers of an algebraic number field, this result is sometimes called the fundamental theorem of ideal theory.

of J, the lemma holds for both A and B, i.e., there exist prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ such that $\mathfrak{p}_1 \cdots \mathfrak{p}_s \subseteq A \subseteq \mathfrak{p}_1 \cap \ldots \cap \mathfrak{p}_s$ and $\mathfrak{q}_1 \cdots \mathfrak{q}_t \subseteq B \subseteq \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_t$. Therefore keeping in mind (3.4), we have

$$\prod_{i=1}^{s} \mathfrak{p}_i \prod_{j=1}^{t} \mathfrak{q}_j \subseteq AB \subseteq J \subseteq A \cap B \subseteq \bigcap_{i=1}^{s} \mathfrak{p}_i \bigcap_{j=1}^{t} \mathfrak{q}_j.$$

This shows that J satisfies the property of the lemma which is not so. □

Lemma 3.14 *If R is a Dedekind domain, then every non-zero prime ideal $\mathfrak{p}$ of R is invertible.*

Proof Let F denote the quotient field of R and $\mathfrak{p}'$ denote the fractional ideal of R defined by $\mathfrak{p}' = \{\alpha \in F \mid \alpha\mathfrak{p} \subseteq R\}$.

We first show that $\mathfrak{p}'$ contains R properly. Clearly R is contained in $\mathfrak{p}'$. Fix a non-zero element $a \in \mathfrak{p}$, then the principal ideal $aR \subseteq \mathfrak{p}$. Also aR contains a product of non-zero prime ideals of R by the previous lemma. Let k be the least number such that a product of k prime ideals of R is contained in aR, say $\mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq aR \subseteq \mathfrak{p}$ where each $\mathfrak{p}_i$ is a prime ideal of R. Therefore there exists at least one $\mathfrak{p}_i$, say $\mathfrak{p}_1$ which is contained in $\mathfrak{p}$. Since R is a Dedekind domain, $\mathfrak{p}_1$ is a maximal ideal and hence $\mathfrak{p}_1 = \mathfrak{p}$. By minimality of k, $\mathfrak{p}_2 \cdots \mathfrak{p}_k \nsubseteq aR$. So there exists an element $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_k$, $b \notin aR$. Since $b\mathfrak{p} \subseteq \mathfrak{p}_1 \cdots \mathfrak{p}_k \subseteq aR$, we see that $ba^{-1}\mathfrak{p} \subseteq R$. So $ba^{-1} \in \mathfrak{p}'$ and $ba^{-1} \notin R$. This proves that $\mathfrak{p}' \supsetneqq R$.

We now show that $\mathfrak{p}'\mathfrak{p} = R$. Since $\mathfrak{p} = R\mathfrak{p} \subseteq \mathfrak{p}'\mathfrak{p} \subseteq R$ and $\mathfrak{p}$ is a maximal ideal of R, so either $\mathfrak{p}'\mathfrak{p} = R$ or $\mathfrak{p}'\mathfrak{p} = \mathfrak{p}$. If $\mathfrak{p}'\mathfrak{p} = R$, then we are done. Suppose if possible that $\mathfrak{p}'\mathfrak{p} = \mathfrak{p}$. Then $\mathfrak{p}\mathfrak{p}'^2 = \mathfrak{p}\mathfrak{p}'\mathfrak{p}' = \mathfrak{p}'\mathfrak{p} = \mathfrak{p}$. Continuing like this, we see that

$$\mathfrak{p}\mathfrak{p}'^n = \mathfrak{p} \ \ \forall\, n \geq 1. \tag{3.5}$$

In view of the fact that $\mathfrak{p}' \supsetneqq R$ proved in the above paragraph, there exists $y \in \mathfrak{p}' \setminus R$; fix such an element y and a non-zero element x of $\mathfrak{p}$. Then (3.5) shows that $xy^n \in \mathfrak{p} \subseteq R$ for every $n \geq 1$. This implies that $xR[y] \subseteq \mathfrak{p} \subseteq R$. Since R is Noetherian, every ideal of R is finitely generated. In particular the ideal $xR[y]$ of R is finitely generated, say by $a_1, \ldots, a_n$. So $R[y]$ will be generated by $\frac{a_1}{x}, \ldots, \frac{a_n}{x}$ as R-module. It now follows from Theorem 1.8(iii) that y is integral over R, which is impossible as R is integrally closed and $y \notin R$. This contradiction proves that $\mathfrak{p}'\mathfrak{p} = R$. □

Lemma 3.15 *If R is a Dedekind domain, then every non-zero ideal of R except R is a product of prime ideals of R.*

Proof Let I be a non-zero proper ideal of R. By Lemma 3.13, I contains a finite product, say $\prod_{i=1}^{k} \mathfrak{p}_i$ of non-zero prime ideals $\mathfrak{p}_i$ of R. We prove the lemma by induction

on the number k of prime ideals. If $k = 1$, then $I \supseteq \mathfrak{p}_1$. Since $\mathfrak{p}_1$ is a maximal ideal, $I = \mathfrak{p}_1$.

Assume as induction hypothesis that a proper ideal of R which contains a product of $k-1$ non-zero prime ideals of R can be written as a product of prime ideals of R. Let I be an ideal of R which contains a product $\prod_{i=1}^{k} \mathfrak{p}_i$ of k non-zero prime ideals, $k \geq 2$. Let $\mathfrak{p}$ be a maximal ideal such that $\prod_{i=1}^{k} \mathfrak{p}_i \subseteq I \subseteq \mathfrak{p}$. So $\mathfrak{p}_i$ is contained in $\mathfrak{p}$ for some i, say $\mathfrak{p}_1 \subseteq \mathfrak{p}$ and hence $\mathfrak{p}_1 = \mathfrak{p}$. Also by Lemma 3.14, $\mathfrak{p}^{-1}$ exists. Multiplying by $\mathfrak{p}^{-1}$, we see that $\prod_{i=2}^{k} \mathfrak{p}_i \subseteq \mathfrak{p}^{-1} I \subseteq R$. Therefore $\mathfrak{p}^{-1} I$ is an ideal of R which contains a product of $k-1$ prime ideals. By induction on k, $\mathfrak{p}^{-1} I$ can be written as $\mathfrak{q}_1 \cdots \mathfrak{q}_s$, where $\mathfrak{q}_i$'s are prime ideals of R. Thus $I = \mathfrak{p}\mathfrak{q}_1 \cdots \mathfrak{q}_s$ is a product of prime ideals. □

Proof of Theorem 3.11. Let I be a non-zero fractional ideal of R. Let α be a non-zero element of R such that $\alpha I \subseteq R$. Applying Lemma 3.15, we write $\alpha I = \mathfrak{p}_1 \cdots \mathfrak{p}_s$ as a product of prime ideals $\mathfrak{p}_i$, $1 \leq i \leq s$. Therefore $I = (\alpha^{-1} R)\mathfrak{p}_1 \cdots \mathfrak{p}_s$. By Lemma 3.14, each $\mathfrak{p}_i$ is invertible, also every principal ideal is invertible and product of invertible ideals is invertible. So I is invertible. □

Proof of Theorem 3.12. By virtue of Lemma 3.15, it only remains to prove uniqueness. Let I be a proper ideal of a Dedekind domain R. Suppose I can be written as

$$I = \mathfrak{p}_1 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_s, \tag{3.6}$$

where $\mathfrak{p}_1, \ldots, \mathfrak{p}_r, \mathfrak{q}_1, \ldots, \mathfrak{q}_s$ are prime ideals of R. It is to be proved that $r = s$ and that $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ is a permutation of $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$. Since $\mathfrak{q}_1 \cdots \mathfrak{q}_s \subseteq \mathfrak{p}_1$, one of $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ is contained in $\mathfrak{p}_1$, say $\mathfrak{q}_i \subseteq \mathfrak{p}_1$. As every non-zero prime ideal is maximal, $\mathfrak{q}_i = \mathfrak{p}_1$. Multiplying both sides of (3.6) by ${\mathfrak{p}_1}^{-1}$, we have

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r = \mathfrak{q}_1 \cdots \mathfrak{q}_{i-1}\mathfrak{q}_{i+1} \cdots \mathfrak{q}_s.$$

If $r < s$, then repeating the process r times we shall see that R is a product of $s - r$ prime ideals which is impossible. So $r \geq s$. By symmetry $s \geq r$. Hence $r = s$ and $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ is a permutation of $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$. □

Now we give some corollaries of Theorems 3.11 and 3.12.

Corollary 3.16 *The set of all non-zero fractional ideals of a Dedekind domain R is a group under multiplication of ideals. This group is free abelian generated by all non-zero prime ideals of R.*

Proof First assertion is immediate from Theorem 3.11. Let I be a non-zero fractional ideal of R, then there exists a non-zero element α belonging to R such that $\alpha I \subseteq R$.

Denote αI by J, then J is an ideal of R and $I = J\alpha^{-1}R$. By Lemma 3.15, we can write $J = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, and $\alpha R = \mathfrak{p}_1^{b_1} \cdots \mathfrak{p}_r^{b_r}$ with $a_i, b_i \geq 0$ and $\mathfrak{p}_i$'s are distinct prime ideals . So $I = \mathfrak{p}_1^{a_1 - b_1} \cdots \mathfrak{p}_r^{a_r - b_r}$.

For proving uniqueness, let I be a non-zero fractional ideal of R and α be a non-zero element of R such that αI is contained in R. Suppose that $I = \mathfrak{p}_1^{c_1} \cdots \mathfrak{p}_r^{c_r} = \mathfrak{p}_1^{d_1} \cdots \mathfrak{p}_r^{d_r}$ and $\alpha R = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ with c_i, d_i, e_i in $\mathbb{Z}$ and $e_i \geq 0$. Then

$$\alpha I = \prod_i \mathfrak{p}_i^{c_i + e_i} = \prod_i \mathfrak{p}_i^{d_i + e_i},$$

which implies that $c_i + e_i = d_i + e_i$ for every i in view of Theorem 3.12. Thus $c_i = d_i$ for every i and so the uniqueness is proved. □

Corollary 3.17 *A Dedekind domain which is a unique factorization domain is a principal ideal domain.*

Proof Suppose that a Dedekind domain R is a unique factorization domain; in order to prove that R is a principal ideal domain, it is enough to prove that every prime ideal of R is a principal ideal because by Theorem 3.12 every non-zero ideal of R can be written as a product of prime ideals. Let $\mathfrak{p}$ be a non-zero prime ideal of R and let α be a non-zero element of $\mathfrak{p}$. Since R is a unique factorization domain, we can write $\alpha = \prod_{i=1}^{r} \pi_i$, where π_i's are irreducible elements of R . Now at least one of $\pi_1, \ldots, \pi_r$ belongs to $\mathfrak{p}$, say $\pi_1 \in \mathfrak{p}$. This implies that $\pi_1 R \subseteq \mathfrak{p}$. Note that $\pi_1 R$ is a prime ideal of R. Hence $\pi_1 R$ is a maximal ideal as R is a Dedekind domain. Thus $\mathfrak{p} = \pi_1 R$ is a principal ideal. □

Theorem 3.12 leads to the notion of the greatest common divisor (gcd) of ideals in Dedekind domains. We first recall the notion of divisibility of ideals.

Definition Let A and B be two ideals of an integral domain R. We say that A divides B and write $A|B$ if there is an (integral) ideal C of R such that $B = AC$. Note that if A divides B, then $B \subseteq A$. We shall show in Theorem 3.19 that the converse is true in a Dedekind domain R. But the converse is false for a general integral domain R as the following example shows.

Example 3.18 Consider $R = \mathbb{Z}[X]$, the ring of polynomials in indeterminate X with coefficients from $\mathbb{Z}$. Let $A = \langle 2, X \rangle$ and $B = \langle 2 \rangle$ be ideals of R. We show that $A \nmid B$. If $B = AC$ for some ideal C of R, then $Xg(X)$ has even coefficients for each $g(X) \in C$ which implies that $g(X)$ has all even coefficients. Hence $C \subseteq 2\mathbb{Z}[X]$. Also $C \supseteq B$. So $B = C = 2\mathbb{Z}[X]$. Multiplying the equation $B = AC$ on both sides by $\langle 2 \rangle^{-1}$,we see that $R = A = \langle 2, X \rangle$ which is not so.

Definition Let A and B be two non-zero ideals in an integral domain R. We say that an ideal D is the greatest common divisor (gcd) of A and B if $D|A$, $D|B$ and whenever an ideal $C|A$ and $C|B$, then $C|D$. Similarly one can define the least common multiple (lcm) of ideals. Two ideals are said to be relatively prime or coprime if their gcd is R.

It may be pointed out that gcd and lcm of two non-zero ideals always exist in a Dedekind domain in view of Theorem 3.12. However gcd or lcm of two non-zero elements may not exist in a Dedekind domain. Consider $R = \mathbb{Z}[\sqrt{-5}]$. It can be easily seen that $6, 3(1 + \sqrt{-5})$ do not have a gcd and $2, 1 + \sqrt{-5}$ have no lcm.

Theorem 3.19 *Let R be a Dedekind domain. The following hold:*

(i) For fractional ideals A, B of R, $A \subseteq B$ if and only if $A = BC$ for some integral ideal C of R.
(ii) If A and B are relatively prime ideals in R, then $AB = A \cap B$.
(iii) If A and B are ideals in R, then $\gcd(A, B) = A + B$.
(iv) If A and B are ideals in R, then $lcm(A, B) = A \cap B$.

Proof (i) If $A = BC$ for some integral ideal C, then $A \subseteq B$ as $BC \subseteq B$. Conversely if $A \subseteq B$ and if $A = 0$, then take $C = 0$. Suppose $A \neq 0$, then $B \neq 0$ and so B^{-1} exists. Hence $AB^{-1} \subseteq BB^{-1} = R$. Take C to be the ideal AB^{-1}, so that $BC = A$.

(ii) $A \cap B \subseteq A$ and $A \cap B \subseteq B$. By (i) $A|A \cap B$ and $B|A \cap B$. As A and B are coprime so $AB|A \cap B$. The inclusion $AB \subseteq A \cap B$ is always true. Hence $AB = A \cap B$

(iii) $A + B \supseteq A$ and $A + B \supseteq B$. By (i) $A + B|A$, $A + B|B$. If $C|A$ and $C|B$, then $C \supseteq A$ and $C \supseteq B$. This implies that $C \supseteq A + B$ and hence $C|A + B$. Thus the $\gcd(A, B) = A + B$.

(iv) Arguing as above, this assertion can be easily proved. □

Definition Let I be a non-zero ideal of R and a, b be elements of R. We say that a is congruent to b modulo I and write $a \equiv b \pmod{I}$ if $I|(a - b)R$, *i.e.*, if $a - b \in I$.

Proposition 3.20 *Let R be a Dedekind domain and I be a non-zero ideal of R. Let $a, b \in R$ with $a \neq 0$. Then the congruence $aX \equiv b \pmod{I}$ is solvable in R if and only if $\gcd(aR, I)|bR$, which is so if and only if $b \in aR + I$.*

Proof In view of Theorem 3.19, $\gcd(aR, I)|bR$ if and only if $aR + I \supseteq bR$, which is so if and only if $b \in aR + I$. So it is enough to prove the equivalence of the first and the last assertions of the proposition, which can be easily verified. □

Corollary 3.21 *Let $\mathfrak{p}$ be a non-zero prime ideal in a Dedekind domain R. Let $a \in R \setminus \mathfrak{p}$, then for every natural number n, the congruence $aX \equiv b \pmod{\mathfrak{p}^n}$ is solvable for each b belonging to R.*

Proof In view of the above proposition, it is enough to verify that $\gcd(aR, \mathfrak{p}^n) = R$. Clearly $\gcd(aR, \mathfrak{p}^n) = \mathfrak{p}^j$ for some j, $0 \leq j \leq n$. If $j > 0$, then $\mathfrak{p}^j | aR$. So $\mathfrak{p}^j \supseteq aR$. This implies that $a \in \mathfrak{p}^j \subseteq \mathfrak{p}$, a contradiction. So $j = 0$ and $\gcd(aR, \mathfrak{p}^n) = R$. □

We shall use the following theorem which is named after a classical theorem of elementary number theory.

Chinese Remainder Theorem. Let $I_1, \ldots, I_m$ be ideals of a commutative ring R with identity such that $I_i + I_j = R$ for $i \neq j$, $1 \leq i, j \leq m$. Then given $x_1, \ldots, x_m$ in R, there exists $x \in R$ such that $x \equiv x_j \pmod{I_j}$ for $1 \leq j \leq m$.

Proof Observe that given two ideals A and B of R with $A + B = R$, there exists y belonging to R such that $y \equiv 1 \pmod{A}$ and $y \equiv 0 \pmod{B}$, because on writing 1 as $a + b$ with $a \in A$ and $b \in B$, it is clear that $y = b$ works. We shall use this observation in the proof of the theorem below.

Fix any j, $1 \leq j \leq m$ and set $I_j^* = \prod_{i=1, i\neq j}^{m} I_i$. By hypothesis, $I_i + I_j = R$ if $i \neq j$. This shows that $\prod_{i=1, i\neq j}^{m} (I_i + I_j) = R$. So the ideal $I_j^* + I_j$ which contains $\prod_{i=1, i\neq j}^{m} (I_i + I_j)$ equals R. In view of what has been said in the above paragraph, there exists $y_j \in R$ such that $y_j \equiv 1 \pmod{I_j}$, $y_j \equiv 0 \pmod{I_j^*}$, $1 \leq j \leq m$. Take $x = x_1 y_1 + \ldots + x_m y_m$. Then $x \equiv x_j \pmod{I_j}$ for $1 \leq j \leq m$. □

We wish to point out that in Dedekind domains, generalized Chinese remainder theorem holds which is as follows: Let $I_1, \ldots, I_m$ be ideals of a Dedekind domain R, then for given $x_1, \ldots, x_m$ belonging to R, there exists $x \in R$ such that $x \equiv x_i \pmod{I_i}$ for $1 \leq i \leq m$ if and only if $x_i - x_j \in I_i + I_j$ for each pair i, j, $1 \leq i, j \leq m$ (cf. [Za-Sa, Chap. V]).

The following corollary describes an important property of ideals of a Dedekind domain. It is stronger than saying that every non-zero ideal is invertible.

Corollary 3.22 *If I and J are non-zero ideals of a Dedekind domain R, then there exists an ideal A of R such that $\gcd(A, IJ) = R$ and AI is principal.*

Proof Write $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ and $J = \prod_{i=1}^{r} \mathfrak{p}_i^{b_i}$, where $a_i \geq 0, b_i \geq 0$ and $\mathfrak{p}_i$'s are distinct prime ideals. For every i, choose x_i such that $x_i \in \mathfrak{p}_i^{a_i}$ but $x_i \notin \mathfrak{p}_i^{a_i+1}$. Then by Chinese remainder theorem, there exists $x \in R$ such that $x \equiv x_i \pmod{\mathfrak{p}_i^{a_i+1}}$ for $1 \leq i \leq r$. This is possible since $\mathfrak{p}_i^m + \mathfrak{p}_j^n = R$ for any non-negative integers m and n with $i \neq j$. Now clearly $x - x_i \in \mathfrak{p}_i^{a_i+1} \subseteq \mathfrak{p}_i^{a_i}$, but $x_i \in \mathfrak{p}_i^{a_i}$ for every i. So x belongs to $\bigcap_{i=1}^{r} \mathfrak{p}_i^{a_i}$,

which equals I in view of Theorem 3.19(ii). As $xR \subseteq I$, so I divides xR. Thus there exists an ideal A such that $xR = AI$. So AI is a principal ideal. We have to make sure that $\gcd(A, IJ) = R$, i.e., $\mathfrak{p}_i \nmid A$ for any i, $1 \leq i \leq r$. Suppose to the contrary that $\mathfrak{p}_i$ divides A for some i. Recall that $\mathfrak{p}_i^{a_i} | I$. So $xR = AI$ is divisible by $\mathfrak{p}_i^{a_i+1}$ i.e., $x \in \mathfrak{p}_i^{a_i+1}$. But by choice $x - x_i \in \mathfrak{p}_i^{a_i+1}$ which implies that $x_i \in \mathfrak{p}_i^{a_i+1}$ leading to a contradiction. Thus $\gcd(A, IJ) = R$. □

The following corollary sharpens the fact that every Dedekind domain is Noetherian.

Corollary 3.23 *Let I be an ideal of a Dedekind domain R. Given any non-zero $x \in I$, there exists $y \in I$ such that I is the ideal generated by x and y.*

Proof As $xR \subseteq I$, so in view of Theorem 3.19(i) I divides xR, say $xR = IJ$ for some ideal J of R. By the previous corollary, there exists an ideal A such that $\gcd(A, IJ) = R$ and AI is a principal ideal generated by y (say). This implies that $\gcd(AI, IJ) = I \gcd(A, J) = IR = I$; consequently in view of Theorem 3.19(iii), we see that $I = IA + IJ = yR + xR$. □

Corollary 3.24 *A Dedekind domain having only finitely many prime ideals is a principal ideal domain.*

Proof Let R be a Dedekind domain having r non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Since every proper ideal of R is a product of non-zero prime ideals, it is enough to show that each $\mathfrak{p}_i$ is principal. Fix an index i, $1 \leq i \leq r$ and choose α belonging to $\mathfrak{p}_i \setminus \mathfrak{p}_i^2$. By Chinese remainder theorem, there exists $x \in R$ such that $x \equiv \alpha \pmod{\mathfrak{p}_i^2}$ and $x \equiv 1 \pmod{\mathfrak{p}_j}$ for $j \neq i$, $1 \leq j \leq r$. Since xR is divisible by $\mathfrak{p}_i$ and neither by $\mathfrak{p}_i^2$ nor by $\mathfrak{p}_j$, it follows that $xR = \mathfrak{p}_i$ and hence $\mathfrak{p}_i$ is principal. □

The class of Dedekind domains having only one non-zero prime ideal is of great importance in algebraic number theory. These are known as discrete valuation rings. There are several equivalent definitions of a discrete valuation ring(cf. [Lu-Pa1, Chap. 14], [Nar, Chap. 1]). A principal ideal domain is called a discrete valuation ring if it has only one non-zero prime ideal. If R is a Dedekind domain with quotient field F and $\mathfrak{p}$ is a non-zero prime ideal of R, then the subset $R_{\mathfrak{p}}$ of F defined by

$$R_{\mathfrak{p}} = \left\{ \frac{r}{s} \;\middle|\; r \in R,\ s \in R \setminus \mathfrak{p} \right\}$$

is a subring of F called the localization of R at $\mathfrak{p}$. It can be easily seen that $R_{\mathfrak{p}}$ is a Dedekind domain with unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$. Therefore in view of Corollary 3.24, it is a principal ideal domain and hence it is a discrete valuation ring. We shall come back to discrete valuation rings in Sect. A.6 of Appendix A.

3.3 Norm of an Ideal

We now introduce the notion of norm of non-zero ideals in a Dedekind domain.

Definition Let R be a Dedekind domain and I be a non-zero ideal in R. The number of elements of R/I is called the norm of I and is denoted by $N(I)$. A Dedekind domain R is said to have finite norm property if R/I is a finite ring for every non-zero ideal I of R.

Example 3.25 If K is an algebraic number field, then $\mathcal{O}_K$ has finite norm property in view of Theorem 3.7 and Lemma 2.14.

Example 3.26 For any infinite field F, the ring $F[X]$ of polynomials in an indeterminate X (which is a PID and hence a Dedekind domain) does not have finite norm property.

Lemma 3.27 *Let R be a Dedekind domain and I be a non-zero ideal in R. Write $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ as a product of powers of distinct prime ideals, then the factor ring R/I is isomorphic to $R/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus R/\mathfrak{p}_r^{a_r}$.*

Proof Define a mapping

$$f : R \to R/\mathfrak{p}_1^{a_1} \oplus \cdots \oplus R/\mathfrak{p}_r^{a_r}$$

by $\alpha \longmapsto (\mathfrak{p}_1^{a_1} + \alpha, \ldots, \mathfrak{p}_r^{a_r} + \alpha)$. Then f is a homomorphism of rings and by Chinese remainder theorem, it is onto. Since $\bigcap_{i=1}^{r} \mathfrak{p}_i^{a_i} = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ in view of Theorem 3.19(ii), the lemma now follows from the first isomorphism theorem of rings. □

We are going to prove that norm is multiplicative.

Lemma 3.28 *If $\mathfrak{p}$ is a non-zero prime ideal in a Dedekind domain R, then $R/\mathfrak{p}$ is isomorphic to $\mathfrak{p}^m/\mathfrak{p}^{m+1}$ as an additive group for $m \geq 1$.*

Proof Fix an element $a \in \mathfrak{p}^m \setminus \mathfrak{p}^{m+1}$. Consider the mapping $f : R \to \mathfrak{p}^m/\mathfrak{p}^{m+1}$ defined by $f(x) = \mathfrak{p}^{m+1} + ax$. The mapping f is a homomorphism of additive groups and $\ker(f) = \{x \in R \mid ax \in \mathfrak{p}^{m+1}\} = \mathfrak{p}$.

In order to show that the map f is onto, we are required to show that given $y \in \mathfrak{p}^m$, there exists $x \in R$ such that $ax \equiv y \pmod{\mathfrak{p}^{m+1}}$. In view of Proposition 3.20, such an element exists if and only if $\gcd(aR, \mathfrak{p}^{m+1}) | yR$, which is so if and only if $\mathfrak{p}^m | yR$, i.e., $y \in \mathfrak{p}^m$. Thus the map f is onto. This proves the lemma in view of the first isomorphism theorem of groups. □

Theorem 3.29 *For a Dedekind domain R with finite norm property, the following hold:*

(i) If I, J are non-zero ideals of R, then $N(IJ) = N(I)N(J)$.
(ii) For a given positive integer t, the number of ideals I of R satisfying $N(I) \leq t$ is finite.

Proof Write $I = \prod_{i=1}^{s} \mathfrak{p}_i^{a_i}$, $a_i \geq 0$ and $J = \prod_{j=1}^{s} \mathfrak{p}_j^{b_j}$, $b_j \geq 0$, $\mathfrak{p}_i$'s are distinct prime ideals of R. Then by Lemma 3.27,

$$R/IJ = R/\prod_{i=1}^{s} \mathfrak{p}_i^{a_i+b_i} \cong R/\mathfrak{p}_1^{a_1+b_1} \oplus \cdots \oplus R/\mathfrak{p}_s^{a_s+b_s}.$$

So

$$N(IJ) = \prod_{i=1}^{s} N(\mathfrak{p}_i^{a_i+b_i}). \tag{3.7}$$

Similarly

$$N(I) = \prod_{i=1}^{s} N(\mathfrak{p}_i^{a_i}), \ N(J) = \prod_{i=1}^{s} N(\mathfrak{p}_i^{b_i}). \tag{3.8}$$

By virtue of (3.7), (3.8), the equality $N(IJ) = N(I)N(J)$ is proved once it is shown that for a non-zero prime ideal $\mathfrak{p}$ of R,

$$N(\mathfrak{p}^m) = (N(\mathfrak{p}))^m \tag{3.9}$$

for each $m \geq 1$. We verify (3.9) by induction on m. If $m = 1$, then there is nothing to prove. Assume it to be true for m. We prove it for $m + 1$. By the second isomorphism theorem of groups

$$(R/\mathfrak{p}^{m+1})/(\mathfrak{p}^m/\mathfrak{p}^{m+1}) \cong R/\mathfrak{p}^m$$

which implies that

$$\left|R/\mathfrak{p}^{m+1}\right| = \left|\mathfrak{p}^m/\mathfrak{p}^{m+1}\right|\left|R/\mathfrak{p}^m\right|. \tag{3.10}$$

By Lemma 3.28,

$$R/\mathfrak{p} \cong \mathfrak{p}^m/\mathfrak{p}^{m+1}. \tag{3.11}$$

Therefore (3.10) and (3.11) imply that $N\left(\mathfrak{p}^{m+1}\right) = N(\mathfrak{p})N\left(\mathfrak{p}^m\right)$. By induction hypothesis $N\left(\mathfrak{p}^m\right) = \left(N(\mathfrak{p})\right)^m$. Therefore (3.9) is proved for $m + 1$. Hence assertion (i) is proved.

For proving (ii), fix a set $\{a_1, a_2, \ldots, a_m\}$ of distinct elements of R having more than $t + 1$ elements. For every ideal I satisfying $N(I) \leq t$, i.e., $\left|R/I\right| \leq t$, there exist $i, j, i \neq j$ such that $I + a_i = I + a_j$, therefore $a_i - a_j \in I$ and hence $I|(a_i - a_j)R$. Since the set of differences $a_i - a_j$, $1 \leq i < j \leq m$ is finite and in view of Theorem

3.12, the number of ideals dividing a non-zero ideal of R is finite, it follows that I has only finitely many choices. This proves assertion (ii). □

Definition Let R be Dedekind domain with finite norm property and I be a non-zero fractional ideal of R. Suppose that $I = AB^{-1}$, where A, B are (integral) ideals, we define $N(I) = N(A)/N(B)$. This is well defined, because if $I = AB^{-1} = A_1B_1^{-1}$, then $AB_1 = A_1B$ and hence $N(A)N(B_1) = N(A_1)N(B)$.

3.4 Generalized Fermat's Theorem and Euler's Theorem

Using the notion of norm of ideals, we now prove the analogues of Fermat's little theorem and Euler's theorem for Dedekind domains with finite norm property.

Theorem 3.30 ***Generalized Fermat's Theorem.*** *Let R be a Dedekind domain with finite norm property. If $\mathfrak{p}$ is a non-zero prime ideal in R, then $x^{N(\mathfrak{p})} \equiv x \pmod{\mathfrak{p}}$ for every x belonging to R. Moreover $N(\mathfrak{p})$ is the smallest positive integer amongst integers $n \geq 2$ such that $x^n \equiv x \pmod{\mathfrak{p}}$ for every $x \in R$.*

Proof If $x \in \mathfrak{p}$, then $x^{N(\mathfrak{p})} \equiv x \equiv 0 \pmod{\mathfrak{p}}$. Suppose that $x \in R \setminus \mathfrak{p}$. As $R/\mathfrak{p}$ is a finite field having $N(\mathfrak{p})$ elements, its multiplicative group is a cyclic group of order $N(\mathfrak{p}) - 1$. So $x^{N(\mathfrak{p})-1} \equiv 1 \pmod{\mathfrak{p}}$ and hence $x^{N(\mathfrak{p})} \equiv x \pmod{\mathfrak{p}}$. This proves the first assertion. In order to prove the second, choose $y \in R$ such that $\mathfrak{p} + y$ is a generator of the multiplicative group $\left(R/\mathfrak{p}\right)^{\times}$. Therefore $\mathfrak{p} + 1, \mathfrak{p} + y, \ldots, \mathfrak{p} + y^{N(\mathfrak{p})-2}$ are distinct, i.e., y^m is not congruent to 1 (mod $\mathfrak{p}$) when $1 \leq m \leq N(\mathfrak{p}) - 2$ and hence y^n is not congruent to y (mod $\mathfrak{p}$) when $2 \leq n \leq N(\mathfrak{p}) - 1$. □

Theorem 3.31 ***Generalized Euler's Theorem.*** *Let R be a Dedekind domain with finite norm property. For any non-zero ideal I of R, let $\phi(I)$ denote the number of invertible elements of the ring R/I. Then $\phi(I) = N(I)\prod_{\mathfrak{p}|I}\left(1 - \frac{1}{N(\mathfrak{p})}\right)$, where the product extends over all prime ideals dividing I.*

Proof Write $I = \prod_{i=1}^{s} \mathfrak{p}_i^{a_i}$, where $\mathfrak{p}_i$'s are distinct primes and $a_i > 0$. By Lemma 3.27, we have

$$R/I \cong \bigoplus_{i=1}^{s} R/\mathfrak{p}_i^{a_i}.$$

Note that $(u_1, \ldots, u_s)$ belonging to the right hand side of the above expression is a unit if and only if each u_i is a unit of $R/\mathfrak{p}_i^{a_i}$ and therefore

$$\phi(I) = \prod_{i=1}^{s} \phi(\mathfrak{p}_i^{a_i}).$$

So it is enough to prove this theorem when I is a power of a prime ideal, say $I = \mathfrak{p}^n$. Since every non-zero element of $R/\mathfrak{p}$ is invertible, it follows that $\phi(\mathfrak{p}) = N(\mathfrak{p}) - 1$ and hence the result is proved when I is a prime ideal. For $n \geq 2$, observe that an element $\mathfrak{p}^n + a$ of $R/\mathfrak{p}^n$ is not invertible if and only if there does not exist any x' in R such that $(\mathfrak{p}^n + a)(\mathfrak{p}^n + x') = \mathfrak{p}^n + 1$, i.e., there does not exist any x' in R such that $ax' \equiv 1 \pmod{\mathfrak{p}^n}$; in view of Proposition 3.20, this holds if and only if $a \in \mathfrak{p}$. Hence $\phi(\mathfrak{p}^n) = |R/\mathfrak{p}^n| - |\mathfrak{p}/\mathfrak{p}^n|$. By virtue of the following lemma and Theorem 3.29(i), we see that $|\mathfrak{p}/\mathfrak{p}^n| = |R/\mathfrak{p}^{n-1}| = N(\mathfrak{p})^{n-1}$. This proves that $\phi(\mathfrak{p}^n) = N(\mathfrak{p}^n)(1 - \frac{1}{N(\mathfrak{p})})$. □

Lemma 3.32 *Let $\mathfrak{p}$ be a non-zero prime ideal of a Dedekind domain R, then $R/\mathfrak{p}^{n-1}$ and $\mathfrak{p}/\mathfrak{p}^n$ are isomorphic as additive groups for $n \geq 2$.*

Proof Fix an element $a \in \mathfrak{p} \setminus \mathfrak{p}^2$. Consider the mapping $f : R \to \mathfrak{p}/\mathfrak{p}^n$ defined by $x \longmapsto \mathfrak{p}^n + ax$. The mapping f is clearly homomorphism of additive groups. It is onto in view of Proposition 3.20. Since $\ker(f) = \{ x \in R \mid ax \in \mathfrak{p}^n\} = \mathfrak{p}^{n-1}$, the result follows from the first isomorphism theorem of groups. □

Corollary 3.33 *If I and J are coprime ideals of a Dedekind domain R, then $\phi(IJ) = \phi(I)\phi(J)$.*

Proof Write $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ and $J = \prod_{j=1}^{s} \mathfrak{q}_j^{b_j}$ as product of powers of distinct prime ideals. Then by Theorem 3.31, we have

$$\phi(IJ) = N(IJ) \prod_{i=1}^{r} \Big(1 - \frac{1}{N(\mathfrak{p}_i)}\Big) \prod_{j=1}^{s} \Big(1 - \frac{1}{N(\mathfrak{q}_j)}\Big),$$

$$\phi(I) = N(I) \prod_{i=1}^{r} \Big(1 - \frac{1}{N(\mathfrak{p}_i)}\Big),$$

$$\phi(J) = N(J) \prod_{j=1}^{s} \Big(1 - \frac{1}{N(\mathfrak{q}_j)}\Big).$$

The corollary now follows as norm is multiplicative. □

The following proposition describes the norm of principal ideals of $\mathcal{O}_K$.

Proposition 3.34 *Let K be an algebraic number field. For any non-zero element α of K, $N(\alpha\mathcal{O}_K) = |N_{K/\mathbb{Q}}(\alpha)|$.*

Proof It is clearly enough to prove the proposition when $\alpha \in \mathcal{O}_K$. Then by definition of norm of an integral ideal,

$$N(\alpha\mathcal{O}_K) = [\mathcal{O}_K : \alpha\mathcal{O}_K]. \tag{3.12}$$

Let $\{w_1, w_2, \ldots, w_n\}$ be an integral basis of K. In view of Theorem 2.15, we have

$$[\mathcal{O}_K : \alpha\mathcal{O}_K] = \sqrt{\frac{D_{K/\mathbb{Q}}(\alpha w_1, \ldots, \alpha w_n)}{d_K}}. \tag{3.13}$$

Keeping in mind that

$$D_{K/\mathbb{Q}}(\alpha w_1, \ldots, \alpha w_n) = (\det(\alpha^{(i)} w_j^{(i)})_{i,j})^2 = (N_{K/\mathbb{Q}}(\alpha))^2 (\det(w_j^{(i)})_{i,j})^2 = (N_{K/\mathbb{Q}}(\alpha))^2 d_K,$$

the desired equality follows from Eqs. (3.12) and (3.13). □

By virtue of the fact that if norm of an ideal I is a prime number, then I is a prime ideal, the following corollary is an immediate consequence of the above proposition.

Corollary 3.35 *Let α be an algebraic integer belonging to an algebraic number field K such that $|N_{K/\mathbb{Q}}(\alpha)|$ is a prime number, then α is a prime element of $\mathcal{O}_K$.*

In view of the above corollary, it can be easily seen that $1 - \omega$ and $1 + 2\omega$ are prime elements in the ring $\mathbb{Z}[\omega]$, where $\omega = (-1 + \sqrt{-3})/2$.

Example 3.36 Let $K = \mathbb{Q}(\sqrt{-5})$. Then the element $\alpha := 1 + \sqrt{-5}$ can not be a prime element of $\mathcal{O}_K$, for otherwise $\alpha\mathcal{O}_K$ would be a prime ideal and hence its norm will be a prime power which is not so, because in view of Proposition 3.34, $N(\alpha\mathcal{O}_K) = 6$. However α is an irreducible element of $\mathcal{O}_K$. If $\alpha = \beta\gamma$ with β, γ non-units of $\mathcal{O}_K$, then either β or γ has norm 2. So there exist $a, b \in \mathbb{Z}$ such that $a^2 + 5b^2 = 2$ which is impossible.

Example 3.37 We show that the ideal $I = \langle 1 + \sqrt{-5}, 1 - \sqrt{-5}\rangle$ is a maximal ideal of the Dedekind domain $\mathbb{Z}[\sqrt{-5}]$ and is not principal. As $(1 + \sqrt{-5}) \in I$, so I divides $\langle 1 + \sqrt{-5}\rangle$ and hence by virtue of Proposition 3.34, $N(I)$ divides $N_{K/\mathbb{Q}}(1 + \sqrt{-5}) = 6$, where $K = \mathbb{Q}(\sqrt{-5})$. Similarly keeping in view that $2 \in I$, we see that $N(I)$ divides 4. Hence $N(I)$ divides 2. We will show that $I \neq \mathbb{Z}[\sqrt{-5}]$. This will prove that $N(I) = 2$ and consequently I will be a prime and hence maximal ideal of $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. If $I = \mathcal{O}_K$, then there exist a, b, c, d in $\mathbb{Z}$ such that

$$1 = (1 + \sqrt{-5})(a + b\sqrt{-5}) + (1 - \sqrt{-5})(c + d\sqrt{-5}).$$

Separating the real and imaginary parts, the above equation gives $1 = a - 5b + c + 5d$, $0 = a + b - c + d$. On adding these equalities, we obtain $1 = 2a - 4b + 6d$, which leads to a contradiction. Hence $I \neq \mathcal{O}_K$. If I is a principal ideal generated by an element $\alpha = a + b\sqrt{-5}$ of $\mathbb{Z}[\sqrt{-5}]$, then by Proposition 3.34, $2 = N(I) = N_{K/\mathbb{Q}}(\alpha) = a^2 + 5b^2$, which is not possible.

Example 3.38 Let $I = \langle 3, 1 + 2\sqrt{-5} \rangle$ be the ideal of $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-5})$. As in the above example, it can be shown that I is a maximal ideal of $\mathcal{O}_K$ and $N(I) = 3$. We compute the inverse of the ideal I. In view of (3.1),

$$I^{-1} = \{\alpha \in K \mid \alpha I \subseteq \mathcal{O}_K\} = \{\alpha \in K \mid 3\alpha \in \mathcal{O}_K, (1 + 2\sqrt{-5})\alpha \in \mathcal{O}_K\}.$$

Let $a + b\sqrt{-5}$ be an element of K with $a, b \in \mathbb{Q}$. It can be easily seen that $3(a + b\sqrt{-5}) \in \mathcal{O}_K$ if and only if $3a, 3b \in \mathbb{Z}$. Further $(1 + 2\sqrt{-5})(a + b\sqrt{-5}) \in \mathcal{O}_K$ if and only if $a - 10b, 2a + b$ are in $\mathbb{Z}$. On writing $a = a'/3$ and $b = b'/3$ with $a', b' \in \mathbb{Z}$, we see that $a - 10b$ and $2a + b$ are in $\mathbb{Z}$ if and only if $a' \equiv b' \pmod 3$. So $I^{-1} = \{(a' + b'\sqrt{-5})/3 \mid a', b' \in \mathbb{Z}, a' \equiv b' \pmod 3\}$.

3.5 Characterisation of Imaginary Quadratic Euclidean Fields

We end up this chapter by classifying those imaginary quadratic fields K for which $\mathcal{O}_K$ is a Euclidean domain with respect to some Euclidean function. Recall that an integral domain R is called a Euclidean domain if there exists a mapping g from the set of non-zero elements of R into non-negative integers satisfying the following two properties for all elements α, β of R:

(i) If α divides β with α, β non-zero, then $g(\alpha) \leq g(\beta)$.
(ii) For every pair of elements $\alpha, \beta \in R, \beta \neq 0$, there exist elements $\gamma, \delta \in R$ such that $\alpha = \beta\gamma + \delta$ with $\delta = 0$ or $g(\delta) < g(\beta)$.

Such a map g is called a Euclidean function on R.

Theorem 3.39 *For an imaginary quadratic field K, $\mathcal{O}_K$ is a Euclidean domain if and only if $d_K = -3, -4, -7, -8, -11$.*[5]

Proof Write $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree negative integer. Suppose first that $\mathcal{O}_K$ is a Euclidean domain. We show that there exists $\beta \in \mathcal{O}_K$, β not belonging to $\{0, 1, -1\}$ such that

$$|N_{K/\mathbb{Q}}(\beta)| \leq 3. \tag{3.14}$$

Let g be a Euclidean function on $\mathcal{O}_K$. Consider the set

$$S = \{g(\alpha) \mid \alpha \in \mathcal{O}_K, \alpha \neq 0, \pm 1\}.$$

[5] It will be proved in Chap. 8 that besides the ring of algebraic integers of these five imaginary quadratic fields, there are four more imaginary quadratic fields K for which $\mathcal{O}_K$ is a unique factorization domain. These are when $d_K = -19, -43, -67, -163$. These rings provide us examples of unique factorization domains which are not Euclidean domains.

Then S being a subset of non-negative integers has a smallest element, say $g(\beta)$, $\beta \in \mathcal{O}_K$, $\beta \notin \{0, \pm 1\}$. We show that $[\mathcal{O}_K : \beta\mathcal{O}_K] \leq 3$. In view of Proposition 3.34, this will prove (3.14). Let α be any element of $\mathcal{O}_K$. By the definition of Euclidean function, there exist γ, δ in $\mathcal{O}_K$ such that $\alpha = \beta\gamma + \delta$, where either $\delta = 0$ or $g(\delta) < g(\beta)$. Since $g(\beta)$ is the minimum element of S, it follows that $\delta = 0$ or ± 1. This proves that $[\mathcal{O}_K : \beta\mathcal{O}_K] \leq 3$ and hence (3.14) holds.

Using (3.14), we next show that $d \in \{-1, -2, -3, -7, -11\}$. Two cases are distinguished.

Case 1. $d \not\equiv 1 \pmod 4$. In this case $\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$. Write $\beta = a + b\sqrt{d}, a, b \in \mathbb{Z}$. In view of (3.14), $0 \leq a^2 - b^2 d \leq 3$. This inequality implies that $b \neq 0$, for otherwise $\beta = a = \pm 1$, which is not so. Therefore the inequality can be satisfied only when $d = -1$ or -2.

Case 2. $d \equiv 1 \pmod 4$. In this case $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$. Write $\beta = a + \frac{b(1+\sqrt{d})}{2}, a, b \in \mathbb{Z}$. In view of (3.14), we have

$$(2a + b)^2 - b^2 d \leq 12. \tag{3.15}$$

Keeping in mind that $\beta \notin \{0, 1, -1\}$, it can be easily seen that (3.15) implies that $b \neq 0$ and hence it can hold only when $d \geq -12$. As $d \equiv 1 \pmod 4$, it follows that $d \in \{-3, -7, -11\}$ in this case.

Conversely suppose that $d \in \{-1, -2, -3, -7, -11\}$. We prove that $\mathcal{O}_K$ is a Euclidean domain with respect to the norm function. For this it is enough to verify that given $\alpha, \beta \in \mathcal{O}_K$, $\beta \neq 0$, there exists $\gamma, \delta \in \mathcal{O}_K$ such that $\alpha = \beta\gamma + \delta$ and $N_{K/\mathbb{Q}}(\delta) < N_{K/\mathbb{Q}}(\beta)$. Write $\frac{\alpha}{\beta} = x + y\sqrt{d}, x, y \in \mathbb{Q}$. Indeed we have to choose γ in $\mathcal{O}_K$ satisfying

$$N_{K/\mathbb{Q}}(x + y\sqrt{d} - \gamma) < 1. \tag{3.16}$$

The proof is split into two cases.

Case 1. $d = -1$ or -2.

Choose integers m, n nearest to x, y respectively so that $|x - m| \leq \frac{1}{2}$, $|y - n| \leq \frac{1}{2}$. Take $\gamma = m + n\sqrt{d}$, then

$$N_{K/\mathbb{Q}}(x + y\sqrt{d} - \gamma) = (x - m)^2 - d(y - n)^2 \leq \frac{1}{4} + \frac{2}{4} < 1$$

which shows that (3.16) holds.

Case 2. $d \in \{-3, -7, -11\}$.

We have to choose integers m, n so that (3.16) holds for $\gamma = m + \frac{n(1+\sqrt{d})}{2}$, i.e., the inequality

$$\left(x - m - \frac{n}{2}\right)^2 - d\left(y - \frac{n}{2}\right)^2 < 1$$

holds. Choose integer n nearest to $2y$, so that $|2y - n| \leq \frac{1}{2}$. Then take m as the nearest integer to $x - \frac{n}{2}$; consequently

$$\left(x - m - \frac{n}{2}\right)^2 - d\left(y - \frac{n}{2}\right)^2 \leq \frac{1}{4} - \frac{d}{16} \leq \frac{1}{4} + \frac{11}{16} < 1$$

as desired. □

In the proof of the above theorem, we have shown that for an imaginary quadratic field K, if $\mathcal{O}_K$ is a Euclidean domain, then it is a Euclidean domain with respect to the absolute value of the norm function. In general an algebraic number field K is called norm-Euclidean if the mapping $\alpha \longmapsto |N_{K/\mathbb{Q}}(\alpha)|$ is a Euclidean function on $\mathcal{O}_K$. It may be pointed out that unlike imaginary quadratic fields, the ring of algebraic integers of an algebraic number field K may be Euclidean but it may not be norm-Euclidean. In 1994, Clark [Cla] proved that $\mathbb{Z}[\sqrt{69}]$ is Euclidean but not norm-Euclidean and in 1996, he constructed two such examples of cubic fields. In fact determining all real quadratic norm-Euclidean fields has turned out to be much more difficult. In 1938 Hans Heilbronn [Hei] proved that their number is finite. Later after the efforts of several mathematicians, it was finally proved by Chatland and Davenport [Ch-Da] in 1950 that there are exactly 16 real quadratic norm-Euclidean fields and they are with discriminants 5, 8, 12, 13, 17, 21, 24, 28, 29, 33, 37, 41, 44, 57, 73 and 76.

Exercises

1. Give an example of an element α belonging to $K = \mathbb{Q}(\iota)$ such that $N_{K/\mathbb{Q}}(\alpha) = 1$ but α is not an algebraic integer.
2. Find the inverse of the ideal $I = \left\langle 2, \sqrt{6} \right\rangle$ in $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{6})$.
3. Determine the inverse of ideal $I = \left\langle 1 + \sqrt{-5}, 1 - \sqrt{-5} \right\rangle$ of $\mathcal{O}_K$, where $K = \mathbb{Q}(\sqrt{-5})$.
4. Prove that an invertible ideal in an integral domain is finitely generated.[6]
5. If I, J are non-zero fractional ideals of a Dedekind domain R with quotient field F, then show that $I^{-1}J = \{\alpha \in F \mid \alpha I \subseteq J\}$.
6. If I is a non-zero ideal of $\mathcal{O}_K$ with $N(I)$ a prime number, then I is a prime ideal. Give an example to show that the converse is not true.
7. Let I be a non-zero ideal of $\mathcal{O}_K$. Prove that I contains $N(I)$ and if m is the least positive integer in I, then m divides $N(I)$.
8. Prove that $3 + \omega$ and $5 + 2\omega$ are prime elements in the ring $\mathbb{Z}[\omega]$, where $\omega = (-1 + \sqrt{-3})/2$.
9. Let p be a prime such that $p \equiv 2 \pmod 3$. Prove that p is not expressible as $a^2 - ab + b^2$ with $a, b \in \mathbb{Z}$ and deduce that it is irreducible in $\mathbb{Z}[\omega]$, where $\omega = (-1 + \sqrt{-3})/2$. Factorize the rational primes 7, 13 and 19 into irreducible elements in $\mathbb{Z}[\omega]$.

[6] This result was first proved by Wolfgang Krull in 1935.

10. Prove that $1 + 2\sqrt{-5}$ and $4 + \sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$, but neither of them is a prime.
11. Prove that the ideal $\langle 1 + \sqrt{-5}, 3\rangle$ is a prime ideal of $\mathbb{Z}[\sqrt{-5}]$. Also prove that it is not a principal ideal.
12. Let $K = \mathbb{Q}(\sqrt{-23})$ and $w = (1 + \sqrt{-23})/2$. Determine the norms of the ideals $\langle 2, w\rangle$, $\langle 13, 4 + w\rangle$ of $\mathcal{O}_K$ and deduce that these are prime ideals. Further prove that neither of them is a principal ideal.
13. Let $K = \mathbb{Q}(\theta)$, where $\theta^3 - \theta - 1 = 0$. Prove that the ideal $\langle 23, 3 - \theta\rangle$ is a prime ideal in $\mathcal{O}_K$.
14. (Generalized Wilson Theorem) Let K be an algebraic number field. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ and $\{\xi_1, \ldots, \xi_s\}$ be a system of representatives of all non-zero distinct elements of $\mathcal{O}_K/\mathfrak{p}$. Prove that $\prod_{i=1}^{s} \xi_i \equiv -1 \pmod{\mathfrak{p}}$.
15. If $I \subsetneq J$ are ideals of $\mathcal{O}_K$, then prove that $N(I) > N(J)$.
16. Let I be an ideal of the ring $\mathcal{O}_K$ of algebraic integers of an algebraic number field K. Show that if there exist $\alpha \in I$ such that $N(I) = |N_{K/\mathbb{Q}}(\alpha)|$, then $I = \mathcal{O}_K\alpha$.
17. Let $K = \mathbb{Q}(\zeta)$ be an algebraic number field, where ζ is a primitive pth root of unity, p prime. Prove that $p\mathcal{O}_K = (1 - \zeta)^{p-1}\mathcal{O}_K$ and that $(1 - \zeta)\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.
18. Prove that in the ring $\mathbb{Z}[\sqrt{-5}]$, the elements $6, 3(1 + \sqrt{-5})$ do not have gcd. Also prove that $2, 1 + \sqrt{-5}$ do not have lcm but have gcd 1.
19. Prove that every unique factorization domain is integrally closed.
20. Prove that $\mathbb{Z}[\sqrt[3]{6}]$, $\mathbb{Z}[2\cos\frac{2\pi}{9}]$ are Dedekind domains.
21. Prove that the equation $x^2 - 10y^2 = \pm 2$ has no solution in integers x, y. Deduce that $\mathbb{Z}[\sqrt{10}]$ is not a unique factorization domain.
22. Let R be a Dedekind domain and let I be a non-zero ideal of R. Show that the ring R/I satisfies the descending chain condition for ideals, i.e., every descending chain of ideals of R/I is stationary.
23. Let R be a Dedekind Domain and $A = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$, $B = \prod_{i=1}^{r} \mathfrak{p}_i^{b_i}$ be non-zero ideals of R where $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ are distinct prime ideals and a_i, b_i are non-negative integers. Prove that $A + B = \prod_{i=1}^{r} \mathfrak{p}_i^{c_i}$ where $c_i = \min\{a_i, b_i\}$ and $A \cap B = \prod_{i=1}^{r} \mathfrak{p}_i^{d_i}$ where $d_i = \max\{a_i, b_i\}$. Also prove that if A, B, C are ideals of R, then $A \cap (B + C) = (A \cap B) + (A \cap C)$ and $A + (B \cap C) = (A + B) \cap (A + C)$. Give an example to show that the last two formulas may not hold if R is not a Dedekind Domain.
24. Let R be a Dedekind Domain and let I be a non-zero integral ideal of R. Show that every ideal of the ring R/I is principal.
25. Prove that the real quadratic fields with discriminants $d = 5, 8, 12, 13, 17, 21, 24, 28, 29$ are norm-Euclidean. (See [Nar, Theorem 3.31].)
26. Let I be a non-zero ideal of the ring $\mathcal{O}_K$ of algebraic integers of an algebraic number field K. Show that there exist $\alpha, \beta \in I$ such that $N(I) = \gcd(N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(\beta))$.

Chapter 4
Splitting of Rational Primes and Dedekind's Theorem

4.1 Ramification Index and Residual Degree

Let K be an algebraic number field. In this chapter, for a given rational prime p, our main aim is to factorize $p\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$. We first introduce the notions of ramification index and residual degree. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, $\mathcal{O}_K/\mathfrak{p}$ is a finite field in view of Example 3.25. So $\mathfrak{p}$ contains a unique rational prime p which is the characteristic of the finite field $\mathcal{O}_K/\mathfrak{p}$; in this situation $\mathfrak{p}$ contains $p\mathcal{O}_K$ and hence $\mathfrak{p}$ divides $p\mathcal{O}_K$.

Definition Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ containing a prime p. If $\mathfrak{p}^e | p\mathcal{O}_K$ and $\mathfrak{p}^{e+1} \nmid p\mathcal{O}_K$, then e is called the index of ramification of $\mathfrak{p}$ over p or the absolute index of ramification of $\mathfrak{p}$.

Definition Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$, then $\mathcal{O}_K/\mathfrak{p}$ being a finite field has order a power p^f of a prime p. The number f is called the residual degree of $\mathfrak{p}/p$ or the absolute residual degree of $\mathfrak{p}$.

Definition Let S be a ring having a subring R. Let A, B be ideals of R and S respectively such that $A \subseteq B$. We say that B lies above A or A lies below B if $B \cap R = A$.

When a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lies above $p\mathbb{Z}$, then by abuse of language we say that $\mathfrak{p}$ lies over p or that $\mathfrak{p}$ lies above p.

The following theorem gives us information about the prime ideals of $\mathcal{O}_K$ lying over a rational prime p when $K/\mathbb{Q}$ is a Galois extension[1].

Theorem 4.1 *Let $K/\mathbb{Q}$ be a finite Galois extension and p be a rational prime. Let $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be the factorization of $p\mathcal{O}_K$ with $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ distinct prime ideals of*

[1] Galois extensions are defined and discussed in Sect. A.5 of Appendix A.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_4

$\mathcal{O}_K$ and $e_1, \ldots, e_r$ positive integers. Then for any given pair $\mathfrak{p}_i, \mathfrak{p}_j$, there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_i) = \mathfrak{p}_j$.

We shall prove the following more general theorem.

Theorem 4.2 *Let R be an integrally closed domain with quotient field L and L' be a finite Galois extension of L. Let R' be the integral closure of R in L'. Let $\mathfrak{p}', \mathfrak{q}'$ be maximal ideals of R' lying over a maximal ideal $\mathfrak{p}$ of R. Then there exists $\sigma \in \mathrm{Gal}(L'/L)$ such that $\sigma(\mathfrak{p}') = \mathfrak{q}'$.*

Proof Suppose to the contrary that $\mathfrak{q}' \neq \sigma(\mathfrak{p}')$ for any $\sigma \in \mathrm{Gal}(L'/L) = G$(say). Then $\sigma(\mathfrak{p}') \neq \tau(\mathfrak{q}')$ for any $\sigma, \tau \in G$. Since $\mathfrak{p}', \mathfrak{q}'$ are maximal ideals of R', so are $\sigma(\mathfrak{p}'), \tau(\mathfrak{q}')$. Therefore they are pairwise comaximal, i.e., $\sigma(\mathfrak{p}') + \tau(\mathfrak{q}') = R'$. By Chinese remainder theorem, there exists $x \in R'$ such that for all σ, τ in G, we have

$$x \equiv 0 \pmod{\sigma(\mathfrak{p}')} \text{ and } x \equiv 1 \pmod{\tau(\mathfrak{q}')}.$$

In view of Theorem 1.19, $N_{L'/L}(x) = \prod_{\sigma \in G} \sigma(x)$ and it belongs to $R' \cap L$. Since R is an integrally closed domain, $R' \cap L = R$. So $N_{L'/L}(x) \in R$. By choice $x \in \mathfrak{p}'$ and hence $N_{L'/L}(x)$ belongs to $\mathfrak{p}' \cap R = \mathfrak{p} = \mathfrak{q}' \cap R$. Thus $\sigma(x) \in \mathfrak{q}'$ for some $\sigma \in G$, i.e., $x \in \sigma^{-1}(\mathfrak{q}')$, which is impossible because $x - 1 \in \sigma^{-1}(\mathfrak{q}')$ by virtue of choice of x. This contradiction proves the theorem. □

Using the above theorem, we prove

Theorem 4.3 *Let $K/\mathbb{Q}$ and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be as in Theorem 4.1. Let f_i denote the residual degree of $\mathfrak{p}_i/p$. Then $e_i = e_1$ and $f_i = f_1$ for $2 \leq i \leq r$.*

Proof Fix any $i \geq 2$. By Theorem 4.1, there exists $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ such that $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$. Consider the map $\psi : \mathcal{O}_K/\mathfrak{p}_1 \to \mathcal{O}_K/\mathfrak{p}_i$ defined by $\psi(\mathfrak{p}_1 + x) = \mathfrak{p}_i + \sigma(x)$. Clearly ψ is an isomorphism of fields which implies that $f_i = f_1$. On applying σ to the equality $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, we see that $p\mathcal{O}_K = \sigma(p\mathcal{O}_K) = \sigma(\mathfrak{p}_1)^{e_1} \cdots \sigma(\mathfrak{p}_r)^{e_r}$. Keeping in mind $\sigma(\mathfrak{p}_1) = \mathfrak{p}_i$ and the fact that factorization into prime ideals is unique, we conclude that $e_i = e_1$. □

We establish an equality which relates the indices of ramification and the residual degrees of various prime ideals of $\mathcal{O}_K$ lying over p with the degree of $K/\mathbb{Q}$.

Proposition 4.4 (Fundamental Equality). *Let $K/\mathbb{Q}$ be an extension of degree n and p be a rational prime. Let $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ be the factorisation of $p\mathcal{O}_K$ as a product of powers of distinct prime ideals of $\mathcal{O}_K$ and f_i denote the residual degree of $\mathfrak{p}_i/p$. Then*

$$\sum_{i=1}^{r} e_i f_i = n = [K : \mathbb{Q}].$$

Proof Taking norm on both sides of the equality $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$ and using Proposition 3.34, we see that

$$p^n = N(p\mathcal{O}_K) = N(\mathfrak{p}_1)^{e_1} \cdots N(\mathfrak{p}_r)^{e_r} = p^{e_1 f_1 + \cdots + e_r f_r}$$

and hence $n = \sum_{i=1}^{r} e_i f_i$. □

4.2 Dedekind's Theorem on Splitting of Primes

The following simple result is sometimes useful for computing index of ramification and residual degree.

Theorem 4.5 *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n, where θ is an algebraic integer. If the minimal polynomial of θ over $\mathbb{Q}$ is an Eisenstein polynomial with respect to a rational prime p, then there exists exactly one prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ which lies over p and $p\mathcal{O}_K = \mathfrak{p}^n$.*

Proof Let $F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ belonging to $\mathbb{Z}[X]$ be the minimal polynomial of θ over $\mathbb{Q}$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ which divides $p\mathcal{O}_K$. Let e be the positive integer such that $\mathfrak{p}^e | p\mathcal{O}_K$ but $\mathfrak{p}^{e+1} \nmid p\mathcal{O}_K$. In view of the fundamental equality, it is enough to prove that $e \geq n$. Suppose to the contrary that $e \leq n-1$. Since $\theta^n = -(a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0)$ and $a_i \in p\mathbb{Z}$ for $0 \leq i \leq n-1$, it follows that $\theta^n \in \mathfrak{p}$ which implies that $\theta \in \mathfrak{p}$; consequently in view of the assumption $e+1 \leq n$, we see that $a_0 = -\sum_{i=1}^{n-1} a_i\theta^i - \theta^n$ belongs to $\mathfrak{p}^{e+1}$. Hence

$$\mathfrak{p}^{e+1} | a_0\mathcal{O}_K. \tag{4.1}$$

By hypothesis $p^2 \nmid a_0$, so we can write $a_0 = pb_0$ with p, b_0 coprime and hence $a_0\mathcal{O}_K = (p\mathcal{O}_K)(b_0\mathcal{O}_K)$ with $b_0\mathcal{O}_K$ coprime to $p\mathcal{O}_K$; this equality together with (4.1) implies that $\mathfrak{p}^{e+1} | p\mathcal{O}_K$ leading to a contradiction. Hence the theorem is proved. □

The next two lemmas will be used in the proof of Theorem 4.8 which is due to Dedekind. In 1878, Dedekind proved that if $K = \mathbb{Q}(\theta)$ with θ an algebraic integer having minimal polynomial $F(X)$ over $\mathbb{Q}$ and if $p \nmid [\mathcal{O}_K : \mathbb{Z}[\theta]]$, then the factorization of $p\mathcal{O}_K$ into prime ideals is related to the factorization of the polynomial $F(X)$ modulo p.

Lemma 4.6 *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. If a rational prime p does not divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$, then the classes of $1, \theta, \ldots, \theta^{n-1}$ form a basis of $\mathcal{O}_K/p\mathcal{O}_K$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$.*

Proof Since $\mathcal{O}_K/p\mathcal{O}_K$ has exactly $N(p\mathcal{O}_K) = p^n$ elements, the dimension of $\mathcal{O}_K/p\mathcal{O}_K$ over $\mathbb{Z}/p\mathbb{Z}$ is n. So the lemma is proved once we show that the classes of $1, \theta, \ldots, \theta^{n-1}$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. Let $x_0, x_1, \ldots, x_{n-1}$ be integers such that

$$x_0 + x_1\theta + \cdots + x_{n-1}\theta^{n-1} \equiv 0 \pmod{p\mathcal{O}_K}. \tag{4.2}$$

We have to show that each $x_i \equiv 0 \pmod{p}$. Let $\{w_1, \ldots, w_n\}$ be an integral basis of K. Then there exists an $n \times n$ matrix $A = (a_{ij})_{i,j}$ with entries from $\mathbb{Z}$ such that

$$\begin{bmatrix} 1 \\ \theta \\ \vdots \\ \theta^{n-1} \end{bmatrix} = A \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix}.$$

Premultiplying the above equation by the row vector $[x_0, x_1, \ldots, x_{n-1}]$ and using (4.2), we see that

$$\begin{bmatrix} x_0 & \ldots & x_{n-1} \end{bmatrix} A \begin{bmatrix} w_1 \\ w_2 \\ \vdots \\ w_n \end{bmatrix} \equiv 0 \pmod{p\mathcal{O}_K}.$$

Since $\{w_1, \ldots, w_n\}$ is an integral basis of K, the above congruence implies that the following system of congruences holds:

$$\begin{aligned} a_{11}x_0 + a_{21}x_1 + \cdots + a_{n1}x_{n-1} &\equiv 0 \pmod{p} \\ \vdots \qquad\qquad & \ddots \ \vdots \\ a_{1n}x_0 + a_{2n}x_1 + \cdots + a_{nn}x_{n-1} &\equiv 0 \pmod{p}. \end{aligned}$$

In view of Lemma 2.14, $[\mathcal{O}_K : \mathbb{Z}[\theta]] = |\det A|$, which is not divisible by p by hypothesis. It now follows from the theory of linear equations that each $x_i \equiv 0 \pmod{p}$. □

It may be pointed out that the converse of the above lemma is also true which can be proved by retracing the steps of the proof.

Notation
Let p be a prime. For $f(X) \in \mathbb{Z}[X]$, $\overline{f}(X)$ will denote the polynomial obtained by replacing each coefficient of $f(X)$ by its image under the canonical homomorphism from $\mathbb{Z}$ onto $\mathbb{Z}/p\mathbb{Z}$. $\overline{f}(X)$ will be called the reduction of $f(X)$ modulo p.

Lemma 4.7 *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Let p be a rational prime not dividing $[\mathcal{O}_K : \mathbb{Z}[\theta]]$. Let $G(X) \in$*

$\mathbb{Z}[X]$ be a polynomial whose reduction modulo p is irreducible over $\mathbb{Z}/p\mathbb{Z}$. Then the ideal generated by $G(\theta)$ and p in $\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ or it equals $\mathcal{O}_K$.

Proof Let $\mathfrak{p}$ denote the ideal generated by $G(\theta)$ and p in $\mathcal{O}_K$. Let $\alpha, \beta \in \mathcal{O}_K$ be such that $\alpha\beta \in \mathfrak{p}$ and suppose that $\alpha \notin \mathfrak{p}$. We have to prove that $\beta \in \mathfrak{p}$. By the previous lemma, the classes of $1, \theta, \ldots, \theta^{n-1}$ generate $\mathcal{O}_K/p\mathcal{O}_K$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$. So there exists a polynomial $H(X) \in \mathbb{Z}[X]$ such that $\alpha \equiv H(\theta) \pmod{p\mathcal{O}_K}$. Since $\alpha \notin \mathfrak{p}$, it follows that

$$H(\theta) \notin \mathfrak{p}. \tag{4.3}$$

Claim is that the polynomials $\overline{G}(X), \overline{H}(X)$ are coprime, for otherwise $\overline{G}(X)$ being irreducible over $\mathbb{Z}/p\mathbb{Z}$, will divide $\overline{H}(X)$ and hence we could write

$$H(X) = G(X)U(X) + pV(X)$$

for some $U(X), V(X)$ belonging to $\mathbb{Z}[X]$; consequently $H(\theta) = G(\theta)U(\theta) + pV(\theta)$ would belong to $\mathfrak{p}$ contradicting (4.3). Thus the claim is proved. So there exist polynomials $W(X), q(X), T(X) \in \mathbb{Z}[X]$ such that

$$G(X)W(X) + H(X)q(X) = 1 + pT(X).$$

Substituting $X = \theta$ in the above equation and on multiplying both sides by β, we see that $\beta - H(\theta)q(\theta)\beta$ belongs to $\mathfrak{p}$. Keeping in mind the choice of $H(\theta)$ and the fact that $\alpha\beta \in \mathfrak{p}$, it follows that $\beta \in \mathfrak{p}$. □

Theorem 4.8 (Dedekind's Theorem on splitting of primes) *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Let $F(X)$ be the minimal polynomial of θ over $\mathbb{Q}$ and p be a rational prime not dividing the index of $\mathbb{Z}[\theta]$ in $\mathcal{O}_K$. Let $\overline{F}(X) = \overline{F}_1(X)^{e_1} \cdots \overline{F}_r(X)^{e_r}$ be the factorization of $\overline{F}(X)$ into powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, where each $F_i(X) \in \mathbb{Z}[X]$ is monic. Then $\mathfrak{p}_i = \langle F_i(\theta), p\rangle$ for $1 \le i \le r$ are distinct prime ideals of $\mathcal{O}_K$ and $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$; moreover the residual degree of $\mathfrak{p}_i/p$ is $\deg F_i(X)$ for $1 \le i \le r$.*

Proof In view of Lemma 4.7, $\mathfrak{p}_i = \langle F_i(\theta), p\rangle$ is a prime ideal of $\mathcal{O}_K$ once it is shown that $\mathfrak{p}_i \neq \mathcal{O}_K$. For simplicity of notation, we show that $\mathfrak{p}_1 \neq \mathcal{O}_K$. Suppose to the contrary $\mathfrak{p}_1 = \mathcal{O}_K$, i.e., $p\mathcal{O}_K$ and $F_1(\theta)\mathcal{O}_K$ are coprime. By hypothesis

$$0 = F(\theta) \equiv F_1(\theta)^{e_1} \cdots F_r(\theta)^{e_r} \pmod{p\mathcal{O}_K}.$$

In view of our supposition, the above congruence implies that

$$0 \equiv F_2(\theta)^{e_2} \cdots F_r(\theta)^{e_r} \pmod{p\mathcal{O}_K}, \tag{4.4}$$

which is impossible by virtue of Lemma 4.6, because $F_2(X)^{e_2} \cdots F_r(X)^{e_r}$ is a monic polynomial of degree less than n. This contradiction proves that $\mathfrak{p}_1 \neq \mathcal{O}_K$. We next

verify that $\langle F_i(\theta), p\rangle \neq \langle F_j(\theta), p\rangle$ when $i \neq j$. Since $\overline{F}_i(X), \overline{F}_j(X)$ are distinct monic irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, they are coprime. So there exist polynomials $U(X)$, $V(X)$ and $W(X)$ in $\mathbb{Z}[X]$ such that

$$F_i(X)U(X) + F_j(X)V(X) = 1 + pW(X);$$

consequently

$$F_i(\theta)U(\theta) + F_j(\theta)V(\theta) = 1 + pW(\theta).$$

If $\mathfrak{p}_i = \mathfrak{p}_j$, then the above equation implies that $1 \in \mathfrak{p}_i$, which is not so.

Now we prove that $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. Since $\mathfrak{p}_i$ contains $\langle F_i(\theta)\rangle$, $\mathfrak{p}_i$ divides $\langle F_i(\theta)\rangle$. We can write $\langle F_i(\theta)\rangle = \mathfrak{p}_i A_i$ with A_i an ideal of $\mathcal{O}_K$. Similarly there exists an ideal B_i such that $\langle p\rangle = \mathfrak{p}_i B_i$. Since the greatest common divisor of $\langle F_i(\theta)\rangle$ and $\langle p\rangle$ is $\mathfrak{p}_i$, it follows that the gcd of A_i, B_i is $\mathcal{O}_K$. Rewrite the congruence

$$0 = F(\theta) \equiv (F_1(\theta))^{e_1} \cdots (F_r(\theta))^{e_r} \pmod{p\mathcal{O}_K}$$

as

$$0 \equiv \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} A_1^{e_1} \cdots A_r^{e_r} \pmod{\mathfrak{p}_1 B_1}.$$

Keeping in mind that A_1, B_1 are coprime, the above congruence implies that $p\mathcal{O}_K = \mathfrak{p}_1 B_1$ divides $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} A_2^{e_2} \cdots A_r^{e_r}$. Similarly using the fact that A_2, B_2 are coprime and $p\mathcal{O}_K = \mathfrak{p}_2 B_2$, we see that the congruence

$$\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} A_2^{e_2} \cdots A_r^{e_r} \equiv 0 \pmod{\mathfrak{p}_2 B_2}$$

implies that $p\mathcal{O}_K$ divides $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r} A_3^{e_3} \cdots A_r^{e_r}$. Repeating the above process r times, we see that $p\mathcal{O}_K$ divides $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$. So $p\mathcal{O}_K = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, $0 \leq a_i \leq e_i$.

We next prove that $a_i = e_i$ for every i. Since $F_i(\theta) \in \mathfrak{p}_i$, it follows that $\prod_{i=1}^{r} F_i(\theta)^{a_i}$ belongs to $\prod_{i=1}^{r} \mathfrak{p}_i^{a_i} = p\mathcal{O}_K$, i.e.,

$$\prod_{i=1}^{r} F_i(\theta)^{a_i} \equiv 0 \pmod{p\mathcal{O}_K}. \tag{4.5}$$

Recall that by virtue of Lemma 4.6, the classes of $1, \theta, \ldots, \theta^{n-1}$ in $\mathcal{O}_K/p\mathcal{O}_K$ are linearly independent over $\mathbb{Z}/p\mathbb{Z}$. So (4.5) is possible only when

$$\sum_{i=1}^{r} a_i \deg F_i(x) \geq n. \tag{4.6}$$

But $\sum_{i=1}^{r} e_i \deg F_i(X) = \deg F(X) = n$. Since $a_i \leq e_i$ for every i, it now follows from (4.6) that $a_i = e_i$ for $1 \leq i \leq r$.

It only remains to show that the residual degree of $\mathfrak{p}_i/p$ to be denoted by f_i is $\deg F_i(X)$ for $1 \leq i \leq r$. Since $\mathfrak{p}_i + \theta$ satisfies the polynomial $\overline{F}_i(X)$ which is irreducible over $\mathbb{Z}/p\mathbb{Z}$, it follows that

$$f_i \geq \deg \overline{F}_i(X) = n_i \text{ (say)} . \tag{4.7}$$

By the fundamental equality, $n = \sum_{i=1}^{r} e_i f_i$. Since $n = \deg F(X) = \sum_{i=1}^{r} e_i n_i$ and $f_i \geq n_i$ by (4.7), it follows that $f_i = n_i$ for every i. The proof of the theorem is now complete. □

We wish to point out that the converse of Theorem 4.8 is also true. This was proved in 2008 (cf. [Kh-Ku2]). It can be stated as follows:

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer having minimal polynomial $F(X)$ over $\mathbb{Q}$. For a given prime p, let $\overline{F}(X) = \overline{F}_1(X)^{e_1} \cdots \overline{F}_r(X)^{e_r}$ be the factorization of the reduction of $F(X)$ modulo p into a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with each $F_i(X) \in \mathbb{Z}[X]$ monic. If $p\mathcal{O}_K$ has the analogous factorization into a product of powers of distinct prime ideals as $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}$, where $\mathfrak{p}_i = \langle F_i(\theta), p\rangle$ is prime ideal of $\mathcal{O}_K$ having $N(\mathfrak{p}_i) = p^{\deg F_i}$ for $1 \leq i \leq r$, then p does not divide the index of θ.

The examples given below illustrate Theorem 4.8.

Example 4.9 Let $K = \mathbb{Q}(\theta)$ with θ a root of $f(X) = X^3 - X - 4$. We compute the factorisation of the ideals $3\mathcal{O}_K, 5\mathcal{O}_K, 7\mathcal{O}_K$. As shown in Example 2.36, $f(X)$ is irreducible over $\mathbb{Q}$. Also by Lemma 2.6 and Corollary 2.16, we have $D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -N_{K/\mathbb{Q}}(3\theta^2 - 1) = -428 = -2^2 \cdot 107 = (\text{ind}\,\theta)^2 d_K$. So none of the primes 3, 5, 7 divide $\text{ind}\,\theta$. Therefore Dedekind's Theorem on splitting of primes is applicable. Since $f(X) = X^3 - X - 4$ has no root modulo 3, it is irreducible mod 3. We see that $3\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ with $N(3\mathcal{O}_K) = 3^3$. Since $f(3) = 20 \equiv 0 \pmod 5$, $f(X)$ has a factor $X - 3$ modulo 5. Now dividing $f(X)$ by $X - 3$, we see that $f(X) \equiv (X - 3)(X^2 - 2X + 3) \pmod 5$. Since $X^2 - 2X + 3$ has no root modulo 5, it is irreducible modulo 5. By Theorem 4.8, $5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5'$ where $\mathfrak{p}_5 = \langle 5, \theta - 3\rangle$, $\mathfrak{p}_5' = \langle 5, \theta^2 - 2\theta + 3\rangle$ are prime ideals of $\mathcal{O}_K$ with $N(\mathfrak{p}_5) = 5$ and $N(\mathfrak{p}_5') = 5^2$. It can be easily seen that $7\mathcal{O}_K = \mathfrak{p}_7\mathfrak{p}_7'$ where $\mathfrak{p}_7 = \langle 7, \theta - 4\rangle$, $\mathfrak{p}_7' = \langle 7, \theta^2 - 3\theta + 1\rangle$ are prime ideals of $\mathcal{O}_K$ with $N(\mathfrak{p}_7) = 7$ and $N(\mathfrak{p}_7') = 7^2$.

Example 4.10 Let $K = \mathbb{Q}(\theta)$ with θ a root of the polynomial $f(X) = X^4 + 8X + 8$. Note that the polynomial $f(X)$ is irreducible over $\mathbb{Q}$ in view of Eisenstein-Dumas Irreducibility Criterion which is proved in Sect. A.7 of Appendix. Using the formula given in Exercise 1 of Chap. 2, one can easily see that $D_{K/\mathbb{Q}}(1, \theta, \theta^2, \theta^3) = 2^{12} \cdot 5$, so

5 does not divide the index of θ. Here $f(X)$ factors as a product $(X-2)^2(X^2+4X+2)$ of powers of irreducible polynomials modulo 5. So by Theorem 4.8, $5\mathcal{O}_K = \mathfrak{p}_5^2\mathfrak{p}_5'$ where $\mathfrak{p}_5 = \langle 5, \theta - 2\rangle$, $\mathfrak{p}_5' = \langle 5, \theta^2 + 4\theta + 2\rangle$ are prime ideals of $\mathcal{O}_K$ with $N(\mathfrak{p}_5) = 5$ and $N(\mathfrak{p}_5') = 5^2$.

With the notations as in Theorem 4.8, Dedekind [Ded1] gave the following simple criterion in 1878 to verify whether a given prime p divides $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ or not.

Dedekind Criterion. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ in the ring $\mathcal{O}_K$ of algebraic integers of K. Let $F(X)$ be the minimal polynomial of θ over $\mathbb{Q}$. For a prime p, let $\overline{F}(X) = \overline{F}_1(X)^{e_1} \cdots \overline{F}_r(X)^{e_r}$ be the factorization of $\overline{F}(X)$ into powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, with each $F_i(X) \in \mathbb{Z}[X]$ monic. Then p does not divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ if and only if the polynomial $\prod_{i=1}^{r} \overline{F}_i(X)^{e_i - 1}$ is coprime with $\overline{M}(X)$, where $M(X) = \frac{1}{p}[F(X) - F_1(X)^{e_1} \cdots F_r(X)^{e_r}]$.

It may be pointed out that several equivalent versions and generalizations of Dedekind criterion are known (cf. [Coh, Theorem 6.1.4], [Kh-Ku1, Ja-Kh2]). Using the above criterion, in 2017 a set of necessary and sufficient conditions was given for a prime p to divide $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ when $K = \mathbb{Q}(\theta)$ with θ satisfying an irreducible trinomial $F(X) = X^n + aX^m + b$ belonging to $\mathbb{Z}[X]$; these conditions involve only the prime powers dividing a, b, m, n (see [J-K-S1, J-K-S2]). However it is still an open problem to find the exact power of a given prime p dividing $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ though some results are known in this direction (cf. [L-N-V1, L-N-V2]). For an arbitrary algebraic number field $K = \mathbb{Q}(\theta)$ with θ satisfying a monic irreducible polynomial $g(X)$ belonging to $\mathbb{Z}[X]$, an effective lower bound for the highest power of a given prime p dividing the index of θ was given in 2020 (cf. [Ja-Kh1]). This lower bound involves the degrees of the monic irreducible factors of $g(X)$ modulo p.

4.3 Splitting of Primes in Quadratic and Cyclotomic Fields

Coming back to Theorem 4.8, we shall apply it to describe splitting of primes in quadratic and cyclotomic fields. For this the following notation is needed.

Notation Let p be an odd prime. For any integer a, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined by

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

For $a \equiv 0$ or $1 \pmod 4$, the Kronecker symbol is given by

$$\left(\frac{a}{2}\right) = \begin{cases} 0 & \text{if } 4|a, \\ 1 & \text{if } a \equiv 1 \pmod 8, \\ -1 & \text{if } a \equiv 5 \pmod 8. \end{cases}$$

With the above notations, using Dedekind's theorem, we prove

Theorem 4.11 *Let K be a quadratic field having discriminant D. Let p be any prime odd or even. Then the following hold:*

(i) If $p|D$, then $p\mathcal{O}_K = \mathfrak{p}^2$, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $N(\mathfrak{p}) = p$.

(ii) If $\left(\frac{D}{p}\right) = 1$, then $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}_1$, $\mathfrak{p} \neq \mathfrak{p}_1$ are prime ideals of $\mathcal{O}_K$ and $N(\mathfrak{p}) = N(\mathfrak{p}_1) = p$.

(iii) If $\left(\frac{D}{p}\right) = -1$, then $p\mathcal{O}_K = \mathfrak{p}$, $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ and $N(\mathfrak{p}) = p^2$.

Proof Write $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer. In view of Theorem 2.9, $D = d$ or $4d$. The proof is split into two cases.

Case I. p an odd prime. In this case, $\left(\frac{D}{p}\right) = \left(\frac{d}{p}\right)$. Consider $\theta = \sqrt{d}$, $F(X) = X^2 - d$. Then $[\mathcal{O}_K : \mathbb{Z}[\theta]] = 1$ or 2. So Theorem 4.8 is applicable. If $p|d$, then $F(X) \equiv X^2 \pmod p$ and by this theorem, $p\mathcal{O}_K = \mathfrak{p}^2$ with $N(\mathfrak{p}) = p$. If $p \nmid d$, then $F(X)$ factors into two linear factors modulo p or is irreducible modulo p according as $\left(\frac{d}{p}\right) = +1$ or -1. Hence $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}_1$ if $\left(\frac{d}{p}\right) = 1$ and $p\mathcal{O}_K = \mathfrak{p}$ if $\left(\frac{d}{p}\right) = -1$.

Case II. $p = 2$. We divide this case into two subcases.

Consider first the subcase when D is even. So $D = 4d$ and $\{1, \sqrt{d}\}$ is an integral basis of K. Take $\theta = \sqrt{d}$. Then $\mathcal{O}_K = \mathbb{Z}[\theta]$ and $F(X) = X^2 - d \equiv (X - d)^2 \pmod 2$. So by Theorem 4.8, $2\mathcal{O}_K = \mathfrak{p}^2$, $N(\mathfrak{p}) = 2$.

Consider now the subcase when D is odd, i.e., $D = d \equiv 1 \pmod 4$. In this subcase, $\{1, (1 + \sqrt{d})/2\}$ is an integral basis of K. Take $\theta = (1 + \sqrt{d})/2$, $F(X) = X^2 - X + \dfrac{1 - d}{4}$. When $d \equiv 1 \pmod 8$, then $F(X) \equiv X^2 - X \pmod 2$. So $2\mathcal{O}_K = \mathfrak{p}\mathfrak{p}_1$, $N(\mathfrak{p}) = N(\mathfrak{p}_1) = 2$. When $d \equiv 5 \pmod 8$, then $F(X) \equiv X^2 - X - 1 \pmod 2$. In this situation, $F(X)$ is irreducible modulo 2. Therefore $2\mathcal{O}_K = \mathfrak{p}$ and $N(\mathfrak{p}) = 2^2$. □

Definition Let K be an algebraic number field. For a rational prime p, if there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ such that $\mathfrak{p}^2$ divides $p\mathcal{O}_K$, then p is said to be ramified in K otherwise, it is called unramified in K. So p is unramified in K if $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_m$, where $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$.

Definition Let K be an algebraic number field of degree n. A prime p is said to be totally ramified in K if $p\mathcal{O}_K = \mathfrak{p}^n$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. A prime p is said to split completely in K if $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_n$, where $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$.

It may be pointed out that a rational prime p is totally ramified in a quadratic field K with discriminant D if and only if p divides D by virtue of Theorem 4.11. Similarly p splits completely in K if and only if $\left(\frac{D}{p}\right) = 1$ and p is unramified in K if and only if p does not divide D.

We shall now discuss the splitting of a rational prime in a cyclotomic field for which the following lemma is needed.

Lemma 4.12 *Let $m \geq 2$ be an integer, ζ a primitive mth root of unity and $K = \mathbb{Q}(\zeta)$. Let p be a rational prime not dividing m. Then p does not divide $D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\phi(m)-1})$.*

Proof Let $\Phi_m(X)$ denote the minimal polynomial of ζ over $\mathbb{Q}$ and $\overline{\Phi}_m(X)$ denote its reduction modulo p. Since $\Phi_m(X)$ divides $X^m - 1$, $\overline{\Phi}_m(X)$ divides $X^m - \overline{1}$. By hypothesis $p \nmid m$, so $X^m - \overline{1}$ has no repeated root in the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$; consequently the same is true of $\overline{\Phi}_m(X)$. Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ dividing $p\mathcal{O}_K$ and $\zeta_1, \ldots, \zeta_{\phi(m)}$ be roots of $\Phi_m(X)$ in $\mathcal{O}_K$. For $1 \leq i \leq \phi(m)$, let $\bar{\zeta}_i$ denote the image of ζ_i in $\mathcal{O}_K/\mathfrak{p}$ under the canonical homomorphism. Then $\bar{\zeta}_i \neq \bar{\zeta}_j$ in $\mathcal{O}_K/\mathfrak{p}$ if $i \neq j$ by what has been shown above. Hence $\prod_{1 \leq i < j \leq \phi(m)} (\bar{\zeta}_i - \bar{\zeta}_j)^2 \neq \overline{0}$ in $\mathcal{O}_K/\mathfrak{p}$. Since

$$D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\phi(m)-1}) = \prod_{1 \leq i < j \leq \phi(m)} (\zeta_i - \zeta_j)^2$$

belongs to $\mathbb{Z}$, it follows that p does not divide $D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\phi(m)-1})$. □

Definition Let p be a prime and $m \geq 1$ be a number not divisible by p. If h is the smallest positive integer such that $p^h \equiv 1 \pmod{m}$, then h is called the order of p modulo m. In fact h is the order of $m\mathbb{Z} + p$ in the multiplicative group $(\mathbb{Z}/m\mathbb{Z})^\times$ of reduced residue classes modulo m.

We first discuss the splitting of a prime p in the mth cyclotomic field when $p \nmid m$.

Theorem 4.13 *Let $m \geq 2$ be an integer, ζ a primitive mth root of unity and $K = \mathbb{Q}(\zeta)$. Let p be a rational prime not dividing m and having order h modulo m. Then $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, where $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ are distinct prime ideals of $\mathcal{O}_K$, $g = \frac{\phi(m)}{h}$ and each $\mathfrak{p}_i$ has residual degree h.*

Proof Let $\Phi_m(X)$ denote the minimal polynomial of ζ over $\mathbb{Q}$ and $\overline{\Phi}_m(X)$ denote its reduction modulo p. As shown in the proof of Lemma 4.12, $\overline{\Phi}_m(X)$ has no repeated roots and hence it factors as a product of distinct monic irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$. Recall that by Corollary 2.16,

$$D_{K/\mathbb{Q}}(1, \zeta, \ldots, \zeta^{\phi(m)-1}) = (\operatorname{ind} \zeta)^2 d_K.$$

So in view of Lemma 4.12 that p does not divide ind ζ. It now follows from Theorem 4.8, p is unramified in K. So $p\mathcal{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$, where $\mathfrak{p}_i$'s are distinct prime ideals of $\mathcal{O}_K$. By Theorem 4.3, the residual degree of each $\mathfrak{p}_i$ is the same, say f. In view of the fundamental equality, $\phi(m) = fg$. We have to prove that $f = h$. As

$$\prod_{i=1}^{m-1}(X - \zeta^i) = \frac{X^m - 1}{X - 1} = X^{m-1} + X^{m-2} + \cdots + 1,$$

we have $\prod_{i=1}^{m-1}(1 - \zeta^i) = m$. Since p, m are coprime, it follows that $p\mathcal{O}_K$ and $(1 - \zeta^i)\mathcal{O}_K$ are also coprime; consequently $\mathfrak{p}_1 + (1 - \zeta^i)\mathcal{O}_K = \mathcal{O}_K$ for $1 \leq i \leq m - 1$. In particular, $1 - \zeta^i$ is not congruent to 0 modulo $\mathfrak{p}_1$ when $1 \leq i \leq m - 1$, i.e., ζ^i is not congruent to 1 modulo $\mathfrak{p}_1$. So the order of $\mathfrak{p}_1 + \zeta$ in the group $(\mathcal{O}_K/\mathfrak{p}_1)^\times$ is m. But the order of $(\mathcal{O}_K/\mathfrak{p}_1)^\times$ is $p^f - 1$. Therefore in view of Lagrange's theorem for finite groups, $m|(p^f - 1)$. Consequently $f \geq h$.

To prove that $f \leq h$, in view of Theorem 3.30, it is enough to show that

$$\alpha^{p^h} \equiv \alpha \pmod{\mathfrak{p}_1} \tag{4.8}$$

for each $\alpha \in \mathcal{O}_K$. To verify (4.8), let α be an element of $\mathcal{O}_K$. Since p does not divide ind ζ, the classes of $1, \zeta, \ldots, \zeta^{\phi(m)-1}$ form a basis of $\mathcal{O}_K/p\mathcal{O}_K$ as a vector space over $\mathbb{Z}/p\mathbb{Z}$ by Lemma 4.6. Thus

$$\alpha \equiv a_0 + a_1\zeta + \cdots + a_{\phi(m)-1}\zeta^{\phi(m)-1} \pmod{p\mathcal{O}_K}$$

for some integers a_i. Therefore in view of Fermat's little theorem

$$\alpha^{p^h} \equiv a_0 + a_1\zeta^{p^h} + \cdots + a_{\phi(m)-1}(\zeta^{\phi(m)-1})^{p^h} \pmod{p\mathcal{O}_K}. \tag{4.9}$$

Keeping in mind that $p^h \equiv 1 \pmod{m}$ and hence $\zeta^{p^h} = \zeta$, congruence (4.9) can be rewritten as

$$\alpha^{p^h} \equiv \alpha \pmod{p\mathcal{O}_K}$$

which implies that $\alpha^{p^h} \equiv \alpha \pmod{\mathfrak{p}_1}$ proving (4.8). Hence $f = h$. □

For obtaining the splitting of rational primes p dividing m in the mth cyclotomic field, we shall use the following lemma.

Lemma 4.14 *Let $\mathbb{Q} \subseteq K_1 \subseteq K$ be algebraic number fields. Let p be a prime number. Suppose that $p\mathcal{O}_{K_1} = \mathfrak{p}'_1 \cdots \mathfrak{p}'_g$, where $\mathfrak{p}'_1, \ldots, \mathfrak{p}'_g$ are distinct prime ideals of $\mathcal{O}_{K_1}$ with $N(\mathfrak{p}'_i) = p^{f'_i}$. If $\mathfrak{p}'_i\mathcal{O}_K = \mathfrak{p}_i^{e_i}$ for $1 \leq i \leq g$ with $\mathfrak{p}_i$ an ideal of $\mathcal{O}_K$ and if*

$\sum_{i=1}^{g} e_i f_i' = [K : \mathbb{Q}]$, *then each* $\mathfrak{p}_i$ *is a prime ideal of* $\mathcal{O}_K$ *and the residual degree of* $\mathfrak{p}_i/p$ *is* f_i' *for* $1 \le i \le g$.

Proof Write $\mathfrak{p}_i = \prod_{j=1}^{n_i} \mathfrak{p}_{ij}^{e_{ij}}$, $\mathfrak{p}_{ij}$ are prime ideals of $\mathcal{O}_K$, $e_{ij} > 0$. We have to prove that $n_i = 1$ for each i and $e_{ij} = 1$ for every i, j. In view of the hypothesis, we have

$$p\mathcal{O}_K = (\mathfrak{p}_1'\mathcal{O}_K)\cdots(\mathfrak{p}_g'\mathcal{O}_K) = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i} = \prod_{i=1}^{g}\prod_{j=1}^{n_i} \mathfrak{p}_{ij}^{e_i e_{ij}}.$$

Let f_{ij} denote the residual degree of $\mathfrak{p}_{ij}/p$. Observe that $f_{ij} \ge f_i'$, $1 \le i \le g$, $1 \le j \le n_i$. Also by the fundamental equality

$$\sum_{i=1}^{g}\sum_{j=1}^{n_i} e_i e_{ij} f_{ij} = [K : \mathbb{Q}].$$

By hypothesis

$$\sum_{i=1}^{g} e_i f_i' = [K : \mathbb{Q}].$$

Comparing the above two equations, we see that $n_i = 1$ and $e_{ij} = 1$, $f_{ij} = f_i'$ for $1 \le i \le g$. □

Recall that two elements α, β of $\mathcal{O}_K$ are said to be associates if there exists a unit ϵ of $\mathcal{O}_K$ such that $\beta = \alpha\epsilon$. If ζ_0 is a primitive (p^r)th root of unity, p prime, then for any positive integer k not divisible by p, $1 - \zeta_0^k$ and $1 - \zeta_0$ are associates because each divides the other in the ring $\mathbb{Z}[\zeta_0]$ as $1 - \zeta_0$ can also be written as $1 - \zeta_0^{kl}$, where $kl \equiv 1 \pmod{p^r}$.

Theorem 4.15 *Let* $m = p^r m'$ *be an integer, where* p *a prime number,* $r \ge 1$ *and* $p \nmid m'$. *Let* ζ *be a primitive* m*th root of unity. Then in the field* $K = \mathbb{Q}(\zeta)$, $p\mathcal{O}_K = (\mathfrak{p}_1 \cdots \mathfrak{p}_g)^{\phi(p^r)}$, *where* $\mathfrak{p}_1, \ldots, \mathfrak{p}_g$ *are distinct prime ideals of* $\mathcal{O}_K$, h *is the order of* p *modulo* m' *and* $g = \dfrac{\phi(m')}{h}$. *The residual degree of each* $\mathfrak{p}_i$ *is* h.

Proof Let ζ' be a primitive (m')th root of unity and let $K_1 = \mathbb{Q}(\zeta') \subseteq K$. In view of Theorem 4.13, we have

$$p\mathcal{O}_{K_1} = \mathfrak{p}_1' \cdots \mathfrak{p}_g', \tag{4.10}$$

where $g = \dfrac{\phi(m')}{h}$, h is the order of p modulo m' and $\mathfrak{p}_1', \ldots, \mathfrak{p}_g'$ are distinct prime ideals of $\mathcal{O}_{K_1}$ with residual degree h. Observe that for any positive integer n

$$\gcd(\mathfrak{p}_i'^{m}\mathcal{O}_K,\ p\mathcal{O}_K) = \mathfrak{p}_i'\mathcal{O}_K. \tag{4.11}$$

Let ζ_0 be a primitive (p^r)th root of unity. Then the minimal polynomial $\psi(X)$ of ζ_0 over $\mathbb{Q}$ is given by

$$\psi(X) = X^{p^{r-1}(p-1)} + X^{p^{r-1}(p-2)} + \cdots + X^{p^{r-1}} + 1 = \prod_{\substack{k=1\\(k,p^r)=1}}^{p^r} (X - \zeta_0^k).$$

Thus

$$\psi(1) = p = \prod_{\substack{k=1\\(k,p^r)=1}}^{p^r} (1 - \zeta_0^k). \tag{4.12}$$

In view of the fact that the element $(1 - \zeta_0^k)$ where k is a positive integer coprime with p^r, is an associate of $(1 - \zeta_0)$, it follows from (4.12) that

$$p\mathcal{O}_K = (1 - \zeta_0)^{\phi(p^r)}\mathcal{O}_K. \tag{4.13}$$

For each i, $1 \le i \le g$, we infer from (4.13) and (4.11) that

$$(\mathfrak{p}_i'\mathcal{O}_K, (1-\zeta_0)\mathcal{O}_K)^{\phi(p^r)} = (\mathfrak{p}_i'^{\phi(p^r)}\mathcal{O}_K, (1-\zeta_0)^{\phi(p^r)}\mathcal{O}_K) = (\mathfrak{p}_i'^{\phi(p^r)}\mathcal{O}_K, p\mathcal{O}_K) = \mathfrak{p}_i'\mathcal{O}_K.$$

It follows from the above equation that

$$\mathfrak{p}_i'\mathcal{O}_K = \mathfrak{p}_i^{\phi(p^r)} \tag{4.14}$$

for some ideal $\mathfrak{p}_i$ of $\mathcal{O}_K$. Since $\phi(p^r)hg = \phi(p^r)\phi(m') = \phi(m)$, keeping in mind Eqs. (4.10) and (4.14) we infer from Lemma 4.14 that $\mathfrak{p}_i$ is a prime ideal of $\mathcal{O}_K$ and h is the residual degree of $\mathfrak{p}_i/p$ for $1 \le i \le g$. □

4.4 Finiteness of Ramified Primes

In this section, we shall prove the following theorem whose converse is also true. The result of the theorem as well as its converse will be proved in a more general set up in Chap. 7.

Theorem 4.16 *If a rational prime p is ramified in an algebraic number field K, then p divides d_K.*

Proof Let p be a rational prime ramified in K and let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ such that $\mathfrak{p}^2$ divides $p\mathcal{O}_K$. Write $p\mathcal{O}_K = \mathfrak{p}^e A$ with $\mathfrak{p}$ not dividing the ideal A of $\mathcal{O}_K$. Let $\{w_1, \ldots, w_n\}$ be an integral basis of K. Choose $\alpha \in \mathfrak{p}^{e-1}A \setminus \mathfrak{p}^e A$. We can write $\alpha = a_1 w_1 + \cdots + a_n w_n, a_i \in \mathbb{Z}$; note that at least one coefficient a_i is not divisible by p because $\alpha \notin p\mathcal{O}_K$. Since $e > 1, \alpha^p \in \mathfrak{p}^{(e-1)p} A^p \subseteq \mathfrak{p}^e A = p\mathcal{O}_K$. So using Fermat's little theorem, we have

$$0 \equiv \alpha^p \equiv (a_1 w_1 + \cdots + a_n w_n)^p \equiv a_1 w_1^p + \cdots + a_n w_n^p \pmod{p\mathcal{O}_K}. \tag{4.15}$$

Let $K' \subseteq \mathbb{C}$ denote the smallest normal extension of $\mathbb{Q}$ containing K and $\sigma_1, \ldots, \sigma_n$ be the $\mathbb{Q}$-isomorphisms of K into K'. Let $\mathfrak{p}'$ denote a prime ideal of $\mathcal{O}_{K'}$ dividing $p\mathcal{O}_{K'}$. For $\beta \in \mathcal{O}_{K'}$, $\overline{\beta}$ will stand for the image of β under the canonical homomorphism from $\mathcal{O}_{K'}$ onto $\mathcal{O}_{K'}/\mathfrak{p}'$. Applying $\sigma_1, \ldots, \sigma_n$ to (4.15), we see that

$$\begin{aligned} a_1\sigma_1(w_1^p) + \cdots + a_n\sigma_1(w_n^p) &\equiv 0 \pmod{p\mathcal{O}_{K'}} \\ \vdots \qquad\qquad \ddots \qquad\qquad &\vdots \\ a_1\sigma_n(w_1^p) + \cdots + a_n\sigma_n(w_n^p) &\equiv 0 \pmod{p\mathcal{O}_{K'}}. \end{aligned}$$

Since $\mathfrak{p}'$ divides $p\mathcal{O}_{K'}$, the above congruences hold modulo $\mathfrak{p}'$ as well. So the system of n linear equations

$$\sum_{j=1}^{n} \overline{\sigma_i(w_j^p)} x_j = 0, \quad 1 \le i \le n$$

has a solution $(\overline{a_1}, \ldots, \overline{a_n})$ over the field $\mathcal{O}_{K'}/\mathfrak{p}'$. This solution is non-zero, because $p \nmid a_i$ for at least one i. Therefore by the theory of linear equations, $\det\left(\overline{\sigma_i(w_j^p)}\right)_{i,j} = \overline{0}$, i.e., $\det(\sigma_i(w_j^p))_{i,j} \equiv 0 \pmod{\mathfrak{p}'}$. So

$$\det \begin{pmatrix} \sigma_1(w_1^p) & \cdots & \sigma_1(w_n^p) \\ \vdots & \ddots & \vdots \\ \sigma_n(w_1^p) & \cdots & \sigma_n(w_n^p) \end{pmatrix}^2 \equiv 0 \pmod{\mathfrak{p}'}. \tag{4.16}$$

Let M denote the $n \times n$ matrix $\left(\sigma_i(w_j^p)\right)_{i,j}$. Keeping in mind that for $w \in K$, $Tr_{K/\mathbb{Q}}(w) = \sigma_1(w) + \cdots + \sigma_n(w)$, it can be easily seen that $M^t M = (Tr_{K/\mathbb{Q}}(w_i^p w_j^p))_{i,j}$, where M^t is a transpose of M. Thus (4.16) implies that

$$\det\left(Tr_{K/\mathbb{Q}}(w_i^p w_j^p)\right)_{i,j} \equiv 0 \pmod{\mathfrak{p}'}.$$

Since $Tr_{K/\mathbb{Q}}(w_i^p w_j^p) \in \mathbb{Z}$ in view of Corollary 1.22, the above congruence shows that

$$\det\left(Tr_{K/\mathbb{Q}}(w_i^p w_j^p)\right)_{i,j} \equiv 0 \pmod{p}. \tag{4.17}$$

Keeping in mind that for any w belonging to $\mathcal{O}_K$,

$$Tr_{K/\mathbb{Q}}(w^p) \equiv (Tr_{K/\mathbb{Q}}(w))^p \equiv Tr_{K/\mathbb{Q}}(w) \pmod{p},$$

it follows from (4.17) that $d_K = \det\left(Tr_{K/\mathbb{Q}}(w_i w_j)\right)_{i,j} \equiv 0 \pmod{p}$ as desired. □

Exercises

1. Find how the primes 3, 5 split in $\mathbb{Q}(\theta)$ where θ is a root of $X^3 + 4X + 7$.
2. Find which primes are ramified in $K = \mathbb{Q}(\theta)$ where θ satisfies $\theta^3 - \theta - 2 = 0$. Also find their prime ideal factorizations in $\mathcal{O}_K$.
3. Find all rational primes p that ramify in K together with their prime ideal factorizations in $\mathcal{O}_K$, when K is one of the following fields:

   (a) $\mathbb{Q}(\sqrt[3]{18})$;
   (b) $\mathbb{Q}(\sqrt[3]{20})$;
   (c) $\mathbb{Q}(e^{\frac{2\pi i}{27}})$.

4. Let $K = \mathbb{Q}(\sqrt{-23})$ and $w = (1 + \sqrt{-23})/2$. Show that $2, 2 - w$ are irreducible elements of $\mathcal{O}_K$ but not prime elements of $\mathcal{O}_K$.
5. Prove that 2 is not a prime element of $\mathbb{Z}[\zeta]$, where ζ is a primitive 23rd root of unity.
6. Let K_1, K_2, K_3 be three cubic fields as in Exercise 6 of Chap. 2. Describe how the primes 5 and 11 split in each of these fields. Deduce that these fields are different though they have the same discriminant.
7. Find how the primes 2, 3 and 5 split in $K = \mathbb{Q}(\zeta)$ where ζ is a primitive 28th root of unity.
8. Let $K = \mathbb{Q}(\zeta_0)$ be an algebraic number field, where ζ_0 is a primitive p^rth root of unity, p prime. Prove that $p\mathcal{O}_K = (1 - \zeta_0)^{\phi(p^r)}\mathcal{O}_K$ and that $(1 - \zeta_0)\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.
9. Let K_1 and K_2 be algebraic number fields. Suppose that a prime p is totally ramified in K_1 and unramified in K_2. Prove that $K_1 \cap K_2 = \mathbb{Q}$.
10. Let ζ be a primitive mth root of unity, $m \geq 3$. Show that an odd prime p splits completely in $\mathbb{Q}(\zeta)$ if and only if $p \equiv 1 \pmod{m}$. Also show that a prime p is totally ramified in $\mathbb{Q}(\zeta)$ if and only if m is a power of p.
11. Determine all primes $p < 50$ which split completely in $K/\mathbb{Q}$ when $K = \mathbb{Q}(\sqrt{5})$.
12. Determine all prime $p < 20$ which generate a prime ideal in $\mathcal{O}_K$ when $K = \mathbb{Q}(\sqrt{-2})$.
13. Find the number of ideals in $\mathbb{Z}[\sqrt{-2}]$ with absolute norm 18. Also write their factorisation into prime ideals of $\mathbb{Z}[\sqrt{-2}]$.
14. Find the number of ideals in $\mathbb{Z}[\sqrt{-5}]$ which contain the element 15.
15. Let ζ be a primitive 9th root of unity. Find the number of ideals of $\mathbb{Z}[\zeta]$ which contain 6.
16. Determine the prime ideal factorization of 7, 29 in the field $\mathbb{Q}(\sqrt[3]{2})$.

17. Let $K = \mathbb{Q}(\theta)$ where θ satisfies the polynomial $X^4 + 9X + 9$, which is irreducible over $\mathbb{Q}$ in view of Example 2.38. Write the factorization of ideal $2\mathcal{O}_K$ as a product of prime ideals of $\mathcal{O}_K$.
18. Determine how the primes $3, 5$ split in the field $K = \mathbb{Q}(\theta)$ where θ satisfies the polynomial $f(X) = X^4 + 8X - 8$. (Note that $f(X)$ is irreducible over $\mathbb{Q}$ in view of Eisenstein-Dumas Irreducibility Criterion proved in Sect. A.7.)
19. [2] Let p be an odd prime and $K = \mathbb{Q}(\theta)$ where θ is a root of an irreducible polynomial $X^p - a$ over $\mathbb{Z}$ with the integer a squarefree which is not divisible by p. Show that $\mathcal{O}_K = \mathbb{Z}[\theta]$ if and only if $a^p \not\equiv a \pmod{p^2}$.

[2] It may be pointed out that a more general result related to this exercise is proved in [Jh-Kh]. It asserts that if $K = \mathbb{Q}(\theta)$ with θ satisfying an irreducible polynomial $X^n - b$ over $\mathbb{Z}$, then $\mathcal{O}_K = \mathbb{Z}[\theta]$ if and only if b is a squarefree integer and whenever $k \geq 1$ is highest power of a prime p dividing n, p not dividing b, then p^2 does not divide $b^{p^k} - b$.

Chapter 5
Dirichlet's Unit Theorem

In this chapter, we shall prove a theorem which describes the structure of the group of units of $\mathcal{O}_K$ for an algebraic number field K. It was proved by Dirichlet[1] in 1846.

Dirichlet's Unit Theorem. *Let K be an algebraic number field of degree $n = r_1 + 2r_2$ where r_1 is the number of real isomorphisms of K and $2r_2$ is the number of non-real isomorphisms of K. Let $\mathcal{O}_K$ denote the ring of algebraic integers of K. Then there exist units $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ of $\mathcal{O}_K$ with $r = r_1 + r_2 - 1$ such that every unit ε of $\mathcal{O}_K$ can be uniquely written as $\varepsilon = \zeta \varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$ where $a_1, \ldots, a_r$ are in $\mathbb{Z}$ and ζ belongs to the finite cyclic group consisting of all roots of unity in K.*

With the above notations, Dirichlet's unit theorem says that the group $\mathcal{O}_K^\times$ of units of $\mathcal{O}_K$ is the direct product of a finite cyclic group with a free abelian group of rank $r_1 + r_2 - 1$. In particular, $\mathcal{O}_K^\times$ is a finitely generated abelian group. Note that in view of the above theorem, $\mathcal{O}_K^\times$ is finite if and only if $r_1 + r_2 - 1 = 0$, i.e., when either $K = \mathbb{Q}$ or K is an imaginary quadratic field.

To prove this theorem we need some definitions and preliminary results.

5.1 Preliminary Results

Definition Let R be a commutative ring with identity. Let c be a non-zero element of R; for $\alpha, \beta \in R$ we say α is congruent to β modulo c and write $\alpha \equiv \beta \pmod{c}$ if there exists $\gamma \in R$ such that $\alpha - \beta = c\gamma$. This is an equivalence relation on R and partitions R into a union of equivalence classes called congruence classes modulo c.

[1] Peter Gustav Lejeune Dirichlet (1805–1859) was a German mathematician who made deep contributions to Algebraic Number Theory, Analytic Number Theory and to other topics in mathematical analysis; he is credited with being one of the first mathematicians to give the modern formal definition of a function.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_5

The following lemma gives information about the congruence classes in $\mathcal{O}_K$ modulo a positive integer c.

Lemma 5.1 *Let K be an algebraic number field of degree n over $\mathbb{Q}$. Let c be a positive integer. Then there are at most c^n congruence classes modulo c in $\mathcal{O}_K$.*

Proof Let $\{w_1, \ldots, w_n\}$ be an integral basis of K. Let α be an element of $\mathcal{O}_K$. There exist $a_1, \ldots, a_n$ in $\mathbb{Z}$ such that

$$\alpha = a_1 w_1 + \cdots + a_n w_n.$$

By division algorithm, write $a_i = cq_i + r_i,\ 0 \le r_i < c,\ q_i \in \mathbb{Z}$. So

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

and hence

$$\alpha \equiv \sum_{i=1}^{n} r_i w_i \pmod{c}.$$

Therefore every $\alpha \in \mathcal{O}_K$ is congruent modulo c to a member of the set

$$S = \left\{ \sum_{i=1}^{n} b_i w_i \;\middle|\; 0 \le b_i < c,\ b_i \in \mathbb{Z} \right\}.$$

Since $|S| = c^n$, the lemma is proved. □

Theorem 5.2 *Let K be an algebraic number field. Then for every positive integer c, there are only finitely many non-associate elements $\alpha \in \mathcal{O}_K$ such that $|N_{K/\mathbb{Q}}(\alpha)| = c$.*

Proof In view of Lemma 5.1, the theorem is proved once we show that whenever α, β belonging to $\mathcal{O}_K$ are in the same congruence class modulo c and $|N_{K/\mathbb{Q}}(\alpha)| = c = |N_{K/\mathbb{Q}}(\beta)|$, then α and β must be associates. Let α and β be in the same congruence class modulo c, then there exists $\gamma \in \mathcal{O}_K$ such that $\alpha - \beta = c\gamma$. By Lemma 3.3, $\dfrac{N_{K/\mathbb{Q}}(\beta)}{\beta} \in \mathcal{O}_K$. Therefore $\dfrac{\alpha}{\beta} = 1 + \dfrac{c\gamma}{\beta} = 1 \pm \dfrac{N_{K/\mathbb{Q}}(\beta)\gamma}{\beta}$ belongs to $\mathcal{O}_K$. Similarly $\dfrac{\beta}{\alpha} \in \mathcal{O}_K$. So $\dfrac{\alpha}{\beta}$ is a unit of $\mathcal{O}_K$. This proves that α and β are associates as desired. As the total number of congruence classes modulo c is finite by Lemma 5.1, so there are only finitely many non-associate elements of $\mathcal{O}_K$ having norm $\pm c$. □

Proposition 5.3 *Let K be an algebraic number field of degree n and $\sigma_1, \ldots, \sigma_n$ be all the isomorphisms of K into $\mathbb{C}$. Then for any constant $C > 0$, there are only finitely many $\alpha \in \mathcal{O}_K$ such that $|\sigma_i(\alpha)| \le C$ for $1 \le i \le n$.*

Proof Let $\{w_1, \ldots, w_n\}$ be an integral basis of K and α be an element of $\mathcal{O}_K$. Write $\alpha = x_1 w_1 + \cdots + x_n w_n$ with $x_i \in \mathbb{Z}$. Taking the image under σ_i, we have

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

The above n equations in the matrix form can be rewritten as $PM = N$, where

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

Since $\det(P)^2 = d_K \neq 0$ in view of Lemma 2.5, P is invertible. Therefore

$$M = P^{-1}N. \tag{5.1}$$

Let q_{ij} denote the (i, j)th entry of P^{-1} and C_1 denote the maximum of the set $\{|q_{ij}| : 1 \le i, j \le n\}$. If $|\sigma_i(\alpha)| \le C$ for every i, then using (5.1), we see that $|x_j| \le nCC_1$ for each j and so the integers x_j will have only finitely many choices. Consequently, there are only finitely many elements $\alpha \in \mathcal{O}_K$ with $|\sigma_i(\alpha)| \le C$ for all i. □

Corollary 5.4 *An element α of an algebraic number field K is a root of unity if and only if $|\sigma(\alpha)| = 1$ for every isomorphism σ from K into $\mathbb{C}$.*

Proof If α is a root of unity in K, then $\sigma(\alpha)$ is also a root of unity for every isomorphism σ from K into $\mathbb{C}$ and hence $|\sigma(\alpha)| = 1$. Conversely let α be an element of K such that $|\sigma(\alpha)| = 1$ for every isomorphism σ from K into $\mathbb{C}$; then $|\sigma(\alpha^m)| = 1$ for every integer $m \ge 1$. Therefore in view of the above proposition, the set consisting of all positive powers of α is finite. So there exist integers i, j, $1 \le i < j$ such that $\alpha^i = \alpha^j$, which shows that α is a root of unity in K. □

We wish to point out that if an algebraic number field K has a real isomorphism, say σ, then ± 1 are the only roots of unity in K because if $\varepsilon \in K$ is a root of unity, then $\sigma(\varepsilon)$ is a root of unity which is real and hence $\sigma(\varepsilon) = \pm 1$; consequently $\varepsilon = \pm 1$.

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

The following proposition describes an important property of discrete subgroups of $\mathbb{R}^n$.

Proposition 5.5 *A discrete subgroup Γ of $\mathbb{R}^n$ is a free abelian group of rank not exceeding n. Moreover, any $\mathbb{Z}$-basis of Γ is linearly independent over $\mathbb{R}$.*

Proof Let V be the smallest subspace of $\mathbb{R}^n$ containing Γ and s denote its dimension over $\mathbb{R}$. We can choose s vectors in Γ, say $v_1, v_2, \ldots, v_s$ such that $v_1, v_2, \ldots, v_s$ form an $\mathbb{R}$-basis of the vector space V. Let Γ_0 denote the subgroup of Γ defined by

$\Gamma_0 = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_s$. We first show that $[\Gamma : \Gamma_0]$ is finite. Let $v = \sum_{i=1}^{s} a_i v_i$ be any element of Γ with $a_i \in \mathbb{R}$. Write $a_i = \lfloor a_i \rfloor + \delta_i$, where $\lfloor a_i \rfloor$ stands for the largest integer not exceeding a_i and $0 \leq \delta_i < 1$. Denote $\sum_{i=1}^{s} \lfloor a_i \rfloor v_i$ by w, $\sum_{i=1}^{s} \delta_i v_i$ by z and the length of the vector v_i in $\mathbb{R}^n$ by $||v_i||$. Therefore

$$v = \sum_{i=1}^{s} \lfloor a_i \rfloor v_i + \sum_{i=1}^{s} \delta_i v_i = w + z \tag{5.2}$$

with w in Γ_0 and z in $\Gamma \cap Y$, where Y is the subset of $\mathbb{R}^n$ defined by

$$Y = \left\{ y = (y_1, \ldots, y_n) \in \mathbb{R}^n \;\middle|\; ||y|| \leq \sum_{i=1}^{s} ||v_i|| \right\}.$$

It follows from (5.2) that $[\Gamma : \Gamma_0] \leq |\Gamma \cap Y|$. Since Y is a bounded set and Γ is discrete, $\Gamma \cap Y$ is a finite set. This proves that $[\Gamma : \Gamma_0]$ is finite, say $[\Gamma : \Gamma_0] = j$. By Lagrange's theorem of finite groups, $j\Gamma \subseteq \Gamma_0$ which implies that $\Gamma \subseteq \frac{1}{j}\Gamma_0$. As $\frac{1}{j}\Gamma_0$ is a free abelian group of rank s, so is Γ in view of Lemma 2.12 and the fact that its subgroup Γ_0 has rank s.

We now prove the second assertion. Recall that the absolute value of the determinant of the transition matrix from a $\mathbb{Z}$-basis of Γ to a $\mathbb{Z}$-basis of Γ_0 equals $[\Gamma : \Gamma_0]$ in view of Lemma 2.14 and hence is non-zero. Since Γ_0 has a $\mathbb{Z}$-basis which is linearly independent over $\mathbb{R}$, it now follows that any $\mathbb{Z}$-basis of Γ is linearly independent over $\mathbb{R}$. □

5.2 Modification and Application of Minkowski's Lemma on Real Linear Forms

We[2] shall use a modified form of Minkowski's lemma on real linear forms to prove Dirichlet's unit theorem. First we prove this lemma.

Minkowski's Lemma on real linear forms. Let $L_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} a_{ij} x_j$ be real linear forms for $1 \leq i \leq n$ with determinant of the coefficient matrix $A = (a_{ij})_{i,j}$ non-zero. Let $c_1, \ldots, c_n$ be positive real numbers such that $\prod_{i=1}^{n} c_i > |\det A|$, then

[2] This lemma was established by Hermann Minkowski in 1896. Minkowski's lemma on real linear forms is a corollary of a more general theorem of Minkowski on convex bodies proved in Chap. 8. The lemma on real linear forms goes back to Dirichlet. (see (Hec, Chap. 5, Sect. 32)).

there exist rational integers $u_1, \ldots, u_n$ not all zero such that $|L_i(u_1, u_2, \ldots, u_n)| < c_i$ for $1 \leq i \leq n$.

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

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

Note that if $g \neq g'$ are in $\mathbb{Z}^n$, then $\pi_{(g_1,\ldots,g_n)} \cap \pi_{(g'_1,\ldots,g'_n)} = \emptyset$, because if x belongs to this intersection, then $|L_i(g - g')| \leq |L_i(g - x)| + |L_i(x - g')| < c_i$ for $1 \leq i \leq n$ which shows that the vector $g - g' = (u_1, \ldots, u_n)$ (say), satisfies the inequality $|L_i(u_1, u_2, \ldots, u_n)| < c_i$ for $1 \leq i \leq n$, contrary to our assumption.

Let J denote the volume of any parallelotope $\pi_{(g_1,\ldots,g_n)}$ and d be a real number such that the co-ordinates of all points of $\pi_{(0,\ldots,0)}$ are less than d in absolute value. Let m be a positive integer. Consider the family $\mathbb{T}$ of all those $\pi_{(g_1,\ldots,g_n)}$ for which $g_i \in \mathbb{Z}$ and $|g_i| \leq m$ for each i. Clearly $\mathbb{T}$ consists of $(2m + 1)^n$ parallelotopes $\pi_{(g_1,\ldots,g_n)}$. If x belongs to a member $\pi_{(g_1,\ldots,g_n)}$ of $\mathbb{T}$, then $|x_i| \leq |x_i - g_i| + |g_i| \leq d + |g_i| \leq d + m$. Since the members of $\mathbb{T}$ are pairwise disjoint, we see that $(2m + 1)^n J \leq (2d + 2m)^n$. On dividing by $(2m)^n$ and taking limit as $m \longrightarrow \infty$, we see that $J \leq 1$.

On the other hand, using change of variables in multiple integration, we have

$$\begin{aligned} J &= \int\limits_{|L_i(x)| < c_i/2 \ \forall i} \cdots \int dx_1 \cdots dx_n \\ &= \frac{1}{|\det A|} \int\limits_{-c_1/2}^{c_1/2} \cdots \int\limits_{-c_n/2}^{c_n/2} dy_1 \cdots dy_n = \frac{\prod\limits_{i=1}^{n} c_i}{|\det A|}. \end{aligned}$$

The above equality together with $J \leq 1$ implies that $\prod\limits_{i=1}^{n} c_i \leq |\det A|$ contrary to the hypothesis. This contradiction proves the lemma. □

Modified Minkowski's Lemma on real linear forms. Let $L_i(x_1, \ldots, x_n) = \sum\limits_{j=1}^{n} a_{ij} x_j$ be real linear forms for $1 \leq i \leq n$ with determinant of the coefficient matrix $A = (a_{ij})_{i,j}$ non-zero . Let $c_1, \ldots, c_n$ be positive constants such that $|\det A| = \prod\limits_{i=1}^{n} c_i$. Then there exist rational integers $u_1, \ldots, u_n$ not all zero such that $|L_i(u_1, \ldots, u_n)| < c_i$ for $1 \leq i \leq n - 1$ and $|L_n(u_1, \ldots, u_n)| \leq c_n$.

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

$$K_\epsilon = \left\{ x \;:\; |L_i(x)| < c_i, 1 \leq i \leq n - 1, |L_n(x)| < c_n(1 + \epsilon) \right\}.$$

By hypothesis, $(1+\epsilon)\prod_{i=1}^{n} c_i = (1+\epsilon)|\det A| > |\det A|$. So by Minkowski's lemma on real linear forms, $K_\epsilon \cap \mathbb{Z}^n$ contains a non-zero vector. Let $\underline{0}$ stand for the zero vector in $\mathbb{Z}^n$. Since K_ϵ is a bounded set for each $\epsilon > 0$, $K_\epsilon \cap \mathbb{Z}^n$ must be finite. In particular on taking $\epsilon = 1$, we write

$$(K_1 \cap \mathbb{Z}^n) \setminus \{\underline{0}\} = \{A_1, A_2, \ldots, A_r\}$$

where $r \geq 1$.

Suppose to the contrary, the lemma is false. Keeping in mind the supposition and the definition of the set K_1, we see that if $(u_1, u_2, \ldots, u_n)$ belonging to $K_1 \cap \mathbb{Z}^n$ is a non-zero vector, then $|L_n(u_1, u_2, \ldots, u_n)| > c_n$. This implies that there exists ϵ_0 with $0 < \epsilon_0 < 1$ such that $|L_n(A_i)| \geq c_n(1+\epsilon_0)$ for $1 \leq i \leq r$. Consider the set K_{ϵ_0}. Then $K_{\epsilon_0} \subseteq K_1$. Since no A_i belongs to K_{ϵ_0}, we conclude that $K_{\epsilon_0} \cap \mathbb{Z}^n$ consists of only the zero vector, which contradicts the fact that $K_\epsilon \cap \mathbb{Z}^n$ contains a non-zero vector for each $\epsilon > 0$. This contradiction proves the lemma. □

Modified Minkowski's Lemma on complex linear forms. Let $L_i(x) = \sum_{j=1}^{n} a_{ij}x_j$ be linear forms for $1 \leq i \leq n$ with determinant of the matrix $A = (a_{ij})_{i,j}$ non-zero such that $L_1, \ldots, L_{r_1}$ are real linear forms and $L_{r_1+1}, \ldots, L_{r_1+2r_2}$ are complex linear forms satisfying $\overline{L}_{r_1+j} = L_{r_1+r_2+j}$ for $1 \leq j \leq r_2$. Let $c_1, \ldots, c_n$ be positive constants such that $\prod_{i=1}^{n} c_i = |\det A|$ and $c_{r_1+j} = c_{r_1+r_2+j}$ for $1 \leq j \leq r_2$. Then there exist rational integers $z_1, z_2, \ldots, z_n$ not all zero such that $|L_i(z_1, z_2, \ldots, z_n)| < c_i$ for $1 \leq i \leq n-1$ and $|L_n(z_1, z_2, \ldots, z_n)| \leq c_n$.

Proof We define n real linear forms $L'_1, \ldots, L'_n$ by setting $L'_j = L_j$ for $1 \leq j \leq r_1$ and

$$L'_{r_1+j} = \frac{1}{2}(L_{r_1+j} + L_{r_1+r_2+j}),\ L'_{r_1+r_2+j} = \frac{1}{2\iota}(L_{r_1+j} - L_{r_1+r_2+j}),\ 1 \leq j \leq r_2.$$

Let $B = (b_{ij})_{i,j}$ denote the coefficient matrix of these linear forms, i.e., $L'_i(x) = \sum_{j=1}^{n} b_{ij}x_j$ for $1 \leq i \leq n$ and D' denote the determinant of the matrix B. We first show that

$$D' = (-2\iota)^{-r_2} \det A.$$

For proving the above equality, to the (r_1+1)th row of B add ι times (r_1+r_2+1)th row, then in the new matrix multiply the (r_1+r_2+1)th row by -2ι and to it add the (r_1+1)th row. Repeating this process r_2 times with corresponding pairs of rows, we see that $D' = (-2\iota)^{-r_2} \det A$.

We now apply modified Minkowski's lemma of real linear forms to $L'_1, L'_2, \ldots, L'_n$ with constants $c'_1, c'_2, \ldots, c'_n$, where $c'_i = c_i$ for $1 \leq i \leq r_1$ and $c'_i = \frac{c_i}{\sqrt{2}}$ for $r_1+1 \leq i \leq r_1+2r_2 = n$. Then

$$\prod_{i=1}^{n} c_i' = (\prod_{i=1}^{n} c_i)/2^{r_2} = \frac{|\det A|}{2^{r_2}} = |D'|.$$

Hence by modified Minkowski's lemma on real linear forms, there exist integers $z_1, z_2, \ldots z_n$ not all zero such that

$$|L_i'(z_1, z_2, \ldots, z_n)| < c_i' \text{ for } 1 \leq i \leq n-1$$

and

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

Thus $|L_i(z_1, z_2, \ldots, z_n)| < c_i$ for $1 \leq i \leq r_1$ and for $r_1 + 1 \leq i \leq r_1 + r_2 - 1$, we have

$$\begin{aligned} |L_i(z_1, z_2, \ldots, z_n)| &= |L_{i+r_2}(z_1, \ldots, z_n)| \\ &= \sqrt{L_i'(z_1, \ldots, z_n)^2 + L_{i+r_2}'(z_1, \ldots, z_n)^2} \\ &< \sqrt{c_i'^2 + c_i'^2} = \sqrt{2}c_i' = c_i. \end{aligned}$$

Also

$$\begin{aligned} |L_n(z_1, z_2, \ldots, z_n)| &= |L_{r_1+r_2}'(z_1, z_2, \ldots, z_n) + \iota L_{r_1+2r_2}'(z_1, z_2, \ldots, z_n)| \\ &\leq \sqrt{c_{r_1+r_2}'^2 + c_{r_1+2r_2}'^2} = \sqrt{\frac{c_{r_1+r_2}^2}{2} + \frac{c_{r_1+2r_2}^2}{2}} = c_n. \end{aligned}$$

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

Notation. In this chapter, for an algebraic number field K of degree $n = r_1 + 2r_2$, the isomorphisms $\sigma_1, \ldots, \sigma_n$ of K into $\mathbb{C}$ are arranged so that $\sigma_1, \ldots, \sigma_{r_1}$ are real, $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ are non-real and $\sigma_{r_1+r_2+j} = \overline{\sigma}_{r_1+j}$ for $1 \leq j \leq r_2$. As in the previous chapters, we denote $\sigma_i(\alpha)$ by $\alpha^{(i)}$.

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

Lemma 5.6 *Let K be an algebraic number field of degree $n = r_1 + 2r_2$. Then for any given k, $1 \leq k \leq r_1 + r_2$, there exists a unit η of $\mathcal{O}_K$ such that $|\eta^{(k)}| > 1$ and $|\eta^{(j)}| < 1$ for $j \neq k$, $1 \leq j \leq r_1 + r_2$.*

Proof Let d_K denote the discriminant of K and $\{w_1, \ldots, w_n\}$ be an integral basis of K. Let $b_1, \ldots, b_n$ be positive real numbers satisfying $b_{r_1+j} = b_{r_1+r_2+j}$, for $1 \leq j \leq r_2$ and $\prod_{i=1}^{n} b_i = \sqrt{|d_K|}$. On applying modified Minkowski's lemma of complex linear

forms to the forms $L_1, \ldots, L_n$ given by $L_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} w_j^{(i)} x_j$ with constants $b_1, \ldots, b_n$, we obtain rational integers $z_1, \ldots, z_n$ not all zero such that

$$|L_i(z_1, \ldots, z_n)| \leq b_i, \quad 1 \leq i \leq n. \tag{5.3}$$

Set $\gamma = \sum_{j=1}^{n} z_j w_j$, then γ is a non-zero element of $\mathcal{O}_K$ and the above inequality (5.3) shows that $|\gamma^{(i)}| \leq b_i$ for $1 \leq i \leq n$. In particular

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

Take a fixed k, $1 \leq k \leq r_1 + r_2$. Using the above argument, we construct a sequence $\gamma_0, \gamma_1, \gamma_2, \ldots$ of elements in $\mathcal{O}_K$ such that for each $i \geq 0$, $|N_{K/\mathbb{Q}}(\gamma_i)| \leq \sqrt{|d_K|}$ and the inequality $|\gamma_i^{(j)}| > |\gamma_{i+1}^{(j)}|$ holds when $1 \leq j \leq r_1 + r_2$, $j \neq k$. To choose γ_0, take $b_j < 1$ when $1 \leq j \leq r_1 + r_2$, $j \neq k$ and $b_{r_1+r_2+j} = b_{r_1+j}$ for $1 \leq j \leq r_2$; determine b_k such that $\prod_{i=1}^{n} b_i = \sqrt{|d_K|}$. Arguing as above, we see that there exists a non-zero element $\gamma_0 \in \mathcal{O}_K$ such that $|\gamma_0^{(j)}| \leq b_j < 1$ for $j \neq k$, $1 \leq j \leq r_1 + r_2$ and $|N_{K/\mathbb{Q}}(\gamma_0)| \leq \sqrt{|d_K|}$. Set

$$m_0 = \min\{\, |\gamma_0^{(j)}| \;:\; 1 \leq j \leq r_1 + r_2 \,\}.$$

To construct γ_1, take a new set of b_j's such that $b_j < m_0$ when $1 \leq j \leq r_1 + r_2$, $j \neq k$ and $b_{r_1+r_2+j} = b_{r_1+j}$ for $1 \leq j \leq r_2$; choose b_k such that $\prod_{i=1}^{n} b_i = \sqrt{|d_K|}$. Again by the same argument, there exists a non-zero element γ_1 of $\mathcal{O}_K$ with $|N_{K/\mathbb{Q}}(\gamma_1)| \leq \sqrt{|d_K|}$ such that $|\gamma_1^{(j)}| < m_0$ for $1 \leq j \leq r_1 + r_2$, $j \neq k$. In particular, $|\gamma_1^{(j)}| < |\gamma_0^{(j)}|$, $1 \leq j \leq r_1 + r_2$, $j \neq k$. We may continue this process indefinitely to obtain a sequence $\gamma_0, \gamma_1, \gamma_2, \ldots$ of elements in $\mathcal{O}_K$ with desired properties. In view of Theorem 5.2, only finitely many γ_i's can be non-associates. So there exist natural numbers u and v with $v > u$ such that γ_u and γ_v are associates. Therefore there exists a unit η of $\mathcal{O}_K$ such that $\gamma_v = \eta\gamma_u$. Keeping in mind the choice of the sequence $\{\gamma_i\}$, we see that $|\gamma_v^{(j)}| < |\gamma_u^{(j)}|$ for $1 \leq j \leq r_1 + r_2$, $j \neq k$ and hence $|\eta^{(j)}| < 1$. Since $|N_{K/\mathbb{Q}}(\eta)| = 1$, we have $|\eta^{(k)}| > 1$. □

5.3 Proof of Dirichlet's Unit Theorem

Let $\mathcal{O}_K^\times$ denote the group of units of $\mathcal{O}_K$ and W_K the group of roots of unity contained in K. Set $r = r_1 + r_2 - 1$. We define a mapping

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

by

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

Clearly λ is a homomorphism of groups. The proof of the theorem is divided into four steps.

Step I. In this step, it will be proved that $W_K = \ker(\lambda)$ and it is a finite cyclic group. If ε is a root of unity in K, then $\varepsilon^{(j)}$ is also a root of unity. So $|\varepsilon^{(j)}| = 1$ for $1 \leq j \leq r$ which shows that $W_K \subseteq \ker(\lambda)$.

Conversely suppose that $\varepsilon \in \ker(\lambda)$. So $|\varepsilon^{(j)}| = |\varepsilon^{(j+r_2)}| = 1$ for $1 \leq j \leq r_1 + r_2 - 1$. As $|N_{K/\mathbb{Q}}(\varepsilon)| = 1$ by Proposition 3.1, we have

$$1 = \prod_{i=1}^{n} |\varepsilon^{(i)}| = |\varepsilon^{(r_1+r_2)}|^l,$$

where $l = 1$ or 2 according as $r_2 = 0$ or not; consequently $|\varepsilon^{(r_1+r_2)}| = 1$. Applying Proposition 5.3, we see that ε has only finitely many choices. So $\ker(\lambda)$ is a finite group. Hence each element of $\ker(\lambda)$ is a root of unity and consequently $W_K = \ker(\lambda)$ is finite. Since every finite subgroup of the multiplicative group of a field is cyclic, it follows that W_K is a cyclic group.

Step II. In this step, we show that the proof of the theorem is complete once it is proved that the image of λ is a free abelian group of rank r. In this situation if $\lambda(\mathcal{O}_K^{\times})$ has a $\mathbb{Z}$-basis $\{\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)\}$, then $\{\varepsilon_1, \ldots, \varepsilon_r\}$ will be a desired set of units. To see this, suppose ε is a unit of $\mathcal{O}_K$. Then $\lambda(\varepsilon) = a_1\lambda(\varepsilon_1) + \cdots + a_r\lambda(\varepsilon_r)$ for unique $a_1, \ldots, a_r$ in $\mathbb{Z}$ which implies that $\varepsilon\varepsilon_1^{-a_1} \cdots \varepsilon_r^{-a_r} \in \ker(\lambda)$. By Step I, we have $\varepsilon\varepsilon_1^{-a_1} \cdots \varepsilon_r^{-a_r} = \zeta$ with $\zeta \in W_K$ which shows that ε can be uniquely written as $\zeta\varepsilon_1^{a_1} \cdots \varepsilon_r^{a_r}$.

Step III. In this step, it will be shown that $\lambda(\mathcal{O}_K^{\times})$ is a free abelian group of rank not exceeding r. For this, it is enough to show that $\lambda(\mathcal{O}_K^{\times})$ is a discrete subgroup of $\mathbb{R}^r$ in view of Proposition 5.5. To check discreteness, let c be any positive real number. We will show that there are only finitely many ε in $\mathcal{O}_K^{\times}$ such that $-c \leq \log|\varepsilon^{(j)}| \leq c$ for $1 \leq j \leq r$, i.e.,

$$e^{-c} \leq |\varepsilon^{(j)}| \leq e^c \text{ for } 1 \leq j \leq r. \tag{5.4}$$

Let ε be any unit in $\mathcal{O}_K$ satisfying (5.4). Then

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

where $l = 1$ or 2 according as $r_2 = 0$ or not. The above inequality implies that $|\varepsilon^{(n)}| \leq e^{\frac{(n-l)c}{l}} \leq e^{nc}$. So all the conjugates of ε are bounded in absolute value by e^{nc}. In view of Proposition 5.3, ε has finitely many choices. Hence $\lambda(\mathcal{O}_K^{\times})$ is a discrete subgroup of $\mathbb{R}^r$.

Step IV. We will prove that the rank of the free abelian group $\lambda(\mathcal{O}_K^\times)$ is r by showing that $\lambda(\mathcal{O}_K^\times)$ contains r vectors which are linearly independent over $\mathbb{R}$. This will also imply that every $\mathbb{Z}$-basis of $\lambda(\mathcal{O}_K^\times)$ is linearly independent over $\mathbb{R}$. We introduce a new notation. For $\alpha \in K^\times$, define

$$l^{(j)}(\alpha) = \begin{cases} \log|\alpha^{(j)}| & \text{for } 1 \le j \le r_1 \\ 2\log|\alpha^{(j)}| & \text{for } r_1+1 \le j \le r_1+r_2. \end{cases}$$

Note that

$$\log|N_{K/\mathbb{Q}}(\alpha)| = \log(\prod_{j=1}^{r_1}|\alpha^{(j)}| \prod_{j=r_1+1}^{r_1+r_2}|\alpha^{(j)}|^2) = \sum_{j=1}^{r_1+r_2} l^{(j)}(\alpha). \tag{5.5}$$

By virtue of Lemma 5.6 applied r times, there exist units $\eta_1, \ldots, \eta_r$ of $\mathcal{O}_K$ such that $|\eta_i^{(i)}| > 1$, $|\eta_i^{(j)}| < 1$ if $i \ne j$, $1 \le i \le r$, $1 \le j \le r+1$. We shall prove that the vectors $\lambda(\eta_1), \ldots, \lambda(\eta_r)$ are linearly independent over $\mathbb{R}$ by showing that the $r \times r$ matrix formed by taking these vectors as row vectors has determinant non-zero. For this, it is enough to prove that the matrix $A = (a_{ij})_{r\times r} = (l^{(j)}(\eta_i))_{r\times r}$ is non-singular. The matrix A clearly satisfies the first two conditions of the following Lemma 5.7. Also by using equation (5.5), we have

$$\sum_{j=1}^{r_1+r_2} l^{(j)}(\eta_i) = \log|N_{K/\mathbb{Q}}(\eta_i)| = 0$$

and hence

$$\sum_{j=1}^{r} l^{(j)}(\eta_i) = -l^{(r_1+r_2)}(\eta_i)\ ;$$

the right hand side of the above equation is positive in view of the choice of η_i and the fact that $i \ne r_1+r_2$ as $1 \le i \le r$. So the third condition of Lemma 5.7 is also satisfied and hence $\det A \ne 0$. This completes the proof of Dirichlet's unit theorem.

Lemma 5.7 *Suppose that $A = (a_{ij})_{r\times r}$ is a matrix with real entries satisfying the following three properties:*

(i) $a_{ii} > 0\ \forall i$,
(ii) $a_{ij} \le 0$ *if* $i \ne j$,
(iii) $\sum_{j=1}^{r} a_{ij} > 0\ \forall i,\ 1 \le i \le r$.

Then $\det A \ne 0$.

Proof Suppose to the contrary $\det A = 0$. Then there exists a non-zero column vector $T = (t_1, \ldots, t_r)^t$ such that AT is a null matrix. Let s be an index such that $|t_s| = \max_{1 \le i \le r} |t_i|$. Then $AT = \mathbf{0}$ implies that

$$a_{ss} = -\sum_{j=1, j\neq s}^{r} \frac{a_{sj}t_j}{t_s} \text{ and hence } |a_{ss}| = \left| \sum_{j=1, j\neq s}^{r} \frac{a_{sj}t_j}{t_s} \right|.$$

Keeping in mind the conditions (i) and (ii) of the lemma, we have

$$a_{ss} = |a_{ss}| \le \sum_{j=1, j\neq s}^{r} |a_{sj}| \left| \frac{t_j}{t_s} \right| \le \sum_{j\neq s} |a_{sj}| = -\sum_{j\neq s} a_{sj},$$

which shows that $\sum_{j=1}^{r} a_{sj} \le 0$ contrary to condition (iii). This contradiction proves the lemma. □

5.4 Fundamental System of Units and Regulator

If $\varepsilon_1, \ldots, \varepsilon_r$ are as in the statement of Dirichlet's unit theorem, then $\{\varepsilon_1, \ldots, \varepsilon_r\}$ is called a fundamental system of units of $\mathcal{O}_K$ or of K. As shown in Step II of the proof of this theorem, $\{\varepsilon_1, \ldots, \varepsilon_r\}$ is a fundamental system of units of $\mathcal{O}_K$ if and only if $\{\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)\}$ is a $\mathbb{Z}$-basis of the free abelian group $\lambda(\mathcal{O}_K^\times)$. Another system of units $\{\eta_1, \ldots, \eta_r\}$ is a fundamental system of units of $\mathcal{O}_K$ if and only if the transition matrix from the basis $\{\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)\}$ to $\{\lambda(\eta_1), \ldots, \lambda(\eta_r)\}$ is unimodular. So if C denotes the $r \times r$ matrix whose row vectors are $\lambda(\eta_1), \ldots, \lambda(\eta_r)$ and B denotes the $r \times r$ matrix whose row vectors are $\lambda(\varepsilon_1), \ldots, \lambda(\varepsilon_r)$ and if each of $\{\varepsilon_1, \ldots, \varepsilon_r\}$, $\{\eta_1, \ldots, \eta_r\}$ is a fundamental system of units of $\mathcal{O}_K$, then $B = AC$ where A is a unimodular matrix. Therefore $|\det B| = |\det C|$. So $|\det B|$ does not depend on the choice of fundamental system of units. The regulator of K is defined to be $|\det B|$ or $2^{r_2-1}|\det B|$ according as $r_2 = 0$ or $r_2 > 0$. Note that the regulator of an algebraic number field is never zero because any $\mathbb{Z}$-basis of $\lambda(\mathcal{O}_K^\times)$ is linearly independent over $\mathbb{R}$ in view of Step IV in proof of Dirichlet's unit theorem.

5.5 Computation of Units in Quadratic Fields

The following proposition describes $\mathcal{O}_K^\times$ when K is an imaginary quadratic field.

Proposition 5.8 *Let $K = \mathbb{Q}(\sqrt{d})$, where d is a squarefree negative integer. Then $\mathcal{O}_K^\times = \{+1, -1\}$ except in the following two cases:*

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

Proof Suppose first that d is not congruent to 1 modulo 4. Let $x + y\sqrt{d}$ be a unit of $\mathcal{O}_K$ with $x, y \in \mathbb{Z}$. So

$$N_{K/\mathbb{Q}}(x + y\sqrt{d}) = x^2 - dy^2 = 1.$$

When $d < -1$, then $x^2 - dy^2 = 1$ is possible only if $x = \pm 1$, $y = 0$. When $d = -1$ then the equation $x^2 + y^2 = 1$ has only four solutions namely $x = \pm 1$, $y = 0$ and $x = 0$, $y = \pm 1$. In this case $\mathcal{O}_K^\times$ has four units $\pm 1, \pm\iota$.

Suppose now that $d \equiv 1 \pmod 4$. Let $(x + y\sqrt{d})/2$ be any unit of $\mathcal{O}_K$ with $x, y \in \mathbb{Z}$. On taking norm, we see that $x^2 - dy^2 = 4$. If $d < -3$, then $d \leq -7$; in this situation $x^2 - dy^2 = 4$ has only two solutions $x = \pm 2$, $y = 0$. So when $d < -3$, then ± 1 are the only units. If $d = -3$, we have the equation $x^2 + 3y^2 = 4$ which has six solutions viz., $x = \pm 1$, $y = \pm 1$ and $x = \pm 2$, $y = 0$. In this case $\mathcal{O}_K^\times$ has six units as asserted. □

When $K = \mathbb{Q}(\sqrt{d})$ is a real quadratic field, then by Dirichlet's unit theorem, there exists a unit ε of $\mathcal{O}_K$ such that every unit of $\mathcal{O}_K$ can be uniquely written as $\pm\varepsilon^n$ for some $n \in \mathbb{Z}$; such a unit is called a fundamental unit of $\mathcal{O}_K$ or of K. Note that if ε is a fundamental unit of a real quadratic field K, then so are $-\varepsilon, \varepsilon^{-1}, -\varepsilon^{-1}$. Since exactly one of these is greater than one, there exists a unique fundamental unit $\varepsilon > 1$ of $\mathcal{O}_K$. We shall prove that if $x + yw > 1$ is the fundamental unit of $\mathbb{Q}(\sqrt{d})$, $d \neq 5$, where $w = (1 + \sqrt{d})/2$ or $w = \sqrt{d}$ according as $d \equiv 1 \pmod 4$ or not, then x and y are the smallest positive integers for which $N_{K/\mathbb{Q}}(x + yw) = \pm 1$. This paves the way for an interesting relation between units of real quadratic fields and solutions of Pell's equation.[3]

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

Notation. In this section, for an element $\alpha = a + b\sqrt{d}$ with a, b in $\mathbb{Q}$, belonging to a real quadratic field $\mathbb{Q}(\sqrt{d})$, we shall denote by α' its conjugate defined by $\alpha' = a - b\sqrt{d}$.

Lemma 5.9 *Let* $K = \mathbb{Q}(\sqrt{d})$ *be a real quadratic field with* d *a squarefree integer. Let* w *stand for* $(1 + \sqrt{d})/2$ *or* $\sqrt{d}$ *according as* $d \equiv 1 \pmod 4$ *or not. If* $\eta = x + yw > 1$ *is any unit of* $\mathcal{O}_K$, *then* $x \geq 1$, $y \geq 1$ *except when* $d = 5$ *in which case* $x \geq 0$, $y \geq 1$ *and if* $x = 0$, *then* $y = 1$.

[3] An equation of the type $x^2 - my^2 = 1$ where m is a given positive non-square integer is called Pell's Equation. The Swiss mathematician Leonhard Euler(1701–1783) attributed to the English mathematician John Pell (1611–1685) a method of finding two integers x, y such that $x^2 - my^2 = 1$. That is why the equation came to be known as Pell's equation. However such a method had been already described by another English mathematician, William Brouncker in a series of letters written during 1657–1658 to Pierre de Fermat. Lagrange (1736–1813) was the first mathematician to prove that the equation $x^2 - my^2 = 1$ has infinitely many solutions in integers x, y.

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

$$|x + yw'| = |\eta'| = \left|\frac{1}{\eta}\right| < 1 \tag{5.6}$$

and $w' < -1$ except when $d = 5$. So $yw' < -1$ when $d \neq 5$; in this situation (5.6) implies that $x \geq 1$. When $d = 5$, then $w' = \dfrac{1 - \sqrt{5}}{2}$. As $y \geq 1$, in this case (5.6) implies that $x \geq 0$. Further if $x = 0$, (5.6) becomes $\left|\dfrac{y(1 - \sqrt{5})}{2}\right| < 1$ which is possible only when $y = 1$. □

Lemma 5.10 *Let $K = \mathbb{Q}(\sqrt{d})$ and w be as in Lemma 5.9. Let $\varepsilon = x + yw > 1$ be a unit of $\mathcal{O}_K$ with $x \neq 0$. For any $n \geq 1$, if ε^n is written as $x_n + y_n w$, $x_n, y_n \in \mathbb{Z}$, then $x_{n+1} > x_n$, $y_{n+1} > y_n$ for all $n \geq 1$.*

Proof The lemma is proved by induction on n. In view of Lemma 5.9, we have $x \geq 1$, $y \geq 1$. Keeping in mind $w^2 = d$ or $w^2 = \dfrac{d-1}{4} + w$, a simple calculation shows that

$$\varepsilon^2 = (x + yw)^2 = \begin{cases} x^2 + y^2 d + 2xy\sqrt{d} & \text{if } w = \sqrt{d}, \\ x^2 + y^2\dfrac{d-1}{4} + w(y^2 + 2xy) & \text{if } w = \dfrac{1+\sqrt{d}}{2}. \end{cases}$$

So $x_2 > x$, $y_2 > y$. Suppose that the result is true for n, we verify it for $n + 1$. Write ε^{n+1} as $(x + yw)(x_n + y_n w)$. Then

$$\varepsilon^{n+1} = \begin{cases} xx_n + yy_n d + \sqrt{d}(xy_n + yx_n) & \text{if } w = \sqrt{d}, \\ xx_n + yy_n\dfrac{d-1}{4} + w(xy_n + yx_n + yy_n) & \text{if } w = \dfrac{1+\sqrt{d}}{2}. \end{cases}$$

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

It may be pointed out that Lemma 5.10 does not hold when $x = 0$. For example, consider $d = 5$, $\varepsilon = \dfrac{1 + \sqrt{5}}{2} = w$, then $\varepsilon^2 = 1 + w$, $\varepsilon^3 = 1 + 2w$.

The following corollary is an immediate consequence of Lemmas 5.9 and 5.10.

Corollary 5.11 *Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with $d \neq 5$ a squarefree integer and w be as in Lemma 5.9. Then the fundamental unit > 1 of K is $x + yw$, where x and y are smallest positive integers such that $N_{K/\mathbb{Q}}(x + yw) = \pm 1$.*

Example 5.12 We determine all positive solutions of the equation $X^2 - 6Y^2 = 1$. Let K denote the field $\mathbb{Q}(\sqrt{6})$. By direct verification, $x = 5$, $y = 2$ are the smallest positive integers for which $N_{K/\mathbb{Q}}(x + y\sqrt{6}) = \pm 1$. So $5 + 2\sqrt{6}$ is the fundamental unit greater than 1 and it has norm 1. So every unit of $\mathcal{O}_K$ has norm 1. By Lemma 5.10, all positive solutions of $X^2 - 6Y^2 = 1$ are (x_n, y_n), $n \geq 1$, where x_n, y_n are given by $x_n + y_n\sqrt{6} = (5 + 2\sqrt{6})^n$.

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

Definition A multiple decked expression of the type

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

with $a_i > 0$ for $i \geq 1$ is called a finite continued fraction. When a_i's belong to $\mathbb{Z}$, then it is called a simple continued fraction. In symbols, it will be expressed as $[a_0; a_1, \ldots, a_n]$. For example,

$$\frac{24}{19} = 1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}} = [1; 3, 1, 4], \quad \frac{67}{24} = 2 + \cfrac{1}{1 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4}}}} = [2; 1, 3, 1, 4].$$

It may be recalled that every rational number can be written as a finite simple continued fraction. Each irrational number can be written as an infinite simple continued fraction in a unique way (see (Niv, Chap. 7)). In this section we shall deal with continued fraction expansion of those real numbers which satisfy an irreducible polynomial of degree 2 over $\mathbb{Q}$, i.e., real numbers of the type $\frac{P \pm \sqrt{D}}{Q}$ where P, Q are integers and D is a positive integer which is not a perfect square. Such real numbers are called quadratic irrationals. These irrational numbers are characterized by the property that their continued fraction expansion is periodic in the sense defined below (cf. (Niv, Chap. 7)).

Definition An infinite simple continued fraction $[a_0; a_1, a_2, \ldots]$ is called periodic if there exist a non-negative integer m and a positive integer s such that $a_n = a_{n+s}$ for all $n \geq m$; in this situation s is called the period of the continued fraction and we denote such a continued fraction by $[a_0; \ldots, a_{m-1}, \overline{a_m, a_{m+1}, \ldots, a_{m+s-1}}]$.

Example We compute the value of the periodic continued fraction $[1; \overline{1, 2}]$. We first compute $[\overline{1; 2}]$. On writing θ as $[\overline{1; 2}]$, we have

$$\theta = 1 + \frac{1}{2 + \frac{1}{\theta}}.$$

So θ satisfies the quadratic equation $2\theta^2 - 2\theta - 1 = 0$. We discard the negative value to get $\theta = (1 + \sqrt{3})/2$. On denoting $[1; \overline{1, 2}]$ by ξ, we see that $\xi = 1 + \frac{1}{\theta}$. Substituting for θ, we obtain $\xi = \sqrt{3}$.

Definition For a finite or infinite simple continued fraction $[a_0; a_1, a_2, \ldots]$, the continued fraction upto the kth stage $[a_0; a_1, \ldots, a_k]$ is called its kth convergent and will be denoted by $\dfrac{p_k}{q_k}$.

With notations as in the above definition, $a_0 = \dfrac{p_0}{q_0}$, $a_0 + \dfrac{1}{a_1} = \dfrac{a_0a_1 + 1}{a_1} = \dfrac{p_1}{q_1}$, $a_0 + \dfrac{1}{a_1 + \dfrac{1}{a_2}} = \dfrac{a_2(a_0a_1 + 1) + a_0}{a_2a_1 + 1} = \dfrac{a_2p_1 + p_0}{a_2q_1 + q_0} = \dfrac{p_2}{q_2}$.

One can prove by induction that $p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2}$ for $k \geq 2$. Note that $q_i > 0$ for every i. We shall consider continued fractions of positive real numbers. So $a_0 \geq 0$ and $p_{i+1} > p_i, q_{i+1} > q_i$ for every $i \geq 1$. The name convergent is appropriate because the infinite sequence $\left\{\dfrac{p_n}{q_n}\right\}$ of convergents of the continued fraction expansion of an irrational number ξ converges to ξ (see (Niv, Chap. 7)). We shall use the following theorem about continued fractions proved in (Niv, Chap. 7).

Theorem 5.13 *Let ξ be an irrational number. If there is a rational number $\dfrac{a}{b}$ with $b \geq 1$ such that $\left|\xi - \dfrac{a}{b}\right| < \dfrac{1}{2b^2}$, then $\dfrac{a}{b}$ equals one of the convergents of the simple continued fraction expansion of ξ.*

Lemma 5.14 *Let $K = \mathbb{Q}(\sqrt{d})$ and w be as in Lemma 5.9. Assume that $d \neq 5$. Let $x + yw > 1$ be a unit of $\mathcal{O}_K$ with $x, y \in \mathbb{Z}$. Then $\dfrac{x}{y}$ is a convergent to the continued fraction expansion of $-w'$, where w' is the conjugate of w.*

Proof In view of Lemma 5.9, x and y are positive. Since $N_{K/\mathbb{Q}}(x + yw) = (x + yw)(x + yw') = \pm 1$, we have

$$\left|\frac{x}{y} + w'\right| = \frac{1}{y(x + yw)}. \tag{5.7}$$

The proof is split into two cases.

Case I. $d \equiv 2$ or $3 \pmod 4$. In this case, we have $x^2 = dy^2 \pm 1 \geq dy^2 - 1 \geq y^2(d - 1)$ and hence $\dfrac{x}{y} \geq \sqrt{d - 1}$. It now follows from (5.7) that

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

So $\frac{x}{y}$ is a convergent to the continued fraction expansion of $-w' = \sqrt{d}$ by Theorem 5.13.

Case II. $d \equiv 1 \pmod 4$. Recall that $d \neq 5$, so $d \geq 13$ and $\frac{\sqrt{d}+1}{2} > 2$; consequently by virtue of (5.7), we see that

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

So again by the previous theorem, $\frac{x}{y}$ is a convergent to the continued fraction expansion of $-w'$. □

The following corollary is an immediate consequence of the above lemma and Corollary 5.11.

Corollary 5.15 *Let $K = \mathbb{Q}(\sqrt{d})$ and w be as in Corollary 5.11. The fundamental unit greater than one of K is $p_n + q_n w$, where n is the smallest non-negative integer for which $N_{K/\mathbb{Q}}(p_n + q_n w) = \pm 1$, $\frac{p_n}{q_n}$ being the nth convergent to the continued fraction expansion of $-w'$ where w' is the conjugate of w.*

Example 5.16 We compute a fundamental unit of $K = \mathbb{Q}(\sqrt{33})$. By Theorem 2.9, $\{1, (1+\sqrt{33})/2\}$ is an integral basis of K. In view of Corollary 5.15, the fundamental unit of $\mathbb{Q}(\sqrt{33})$ is $p_n + q_n(\frac{1+\sqrt{33}}{2})$, where n is the smallest non-negative integer for which $N_{K/\mathbb{Q}}(p_n + q_n(\frac{1+\sqrt{33}}{2})) = \pm 1$ and $\frac{p_n}{q_n}$ is the nth convergent to the continued fraction expansion of $\frac{-1+\sqrt{33}}{2}$. Note that $N_{K/\mathbb{Q}}(p_n + q_n(\frac{1+\sqrt{33}}{2})) = p_n^2 + p_n q_n - 8q_n^2$. Denote the continued fraction expansion of $\frac{-1+\sqrt{33}}{2}$ by $[a_0; a_1, a_2, a_3, \ldots]$. Then we have the following table:

k	0	1	2	3
a_k	2	2	1	2
p_k	2	5	7	19
q_k	1	2	3	8
$p_k^2 + p_k q_k - 8q_k^2$	-2	3	-2	1

So fundamental unit greater than one of $\mathbb{Q}(\sqrt{33})$ is $19 + 8\,(\frac{1+\sqrt{33}}{2})$.

Example 5.17 We find a fundamental unit of $K = \mathbb{Q}(\sqrt{22})$. Here $\{1, \sqrt{22}\}$ is an integral basis of K. By Corollary 5.15, the fundamental unit of $\mathbb{Q}(\sqrt{22})$ is $p_n + q_n(\sqrt{22})$, where n is the smallest non-negative integer for which $N_{K/\mathbb{Q}}(p_n + q_n(\sqrt{22})) = \pm 1$ and $\frac{p_n}{q_n}$ is the nth convergent to the continued fraction expansion of

$\sqrt{22}$. One can easily check that the continued fraction expansion of $\sqrt{22}$ is given by $[4; \overline{1, 2, 4, 2, 1, 8}]$.

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

Thus we see that the fundamental unit greater than one is $197 + 42\sqrt{22}$ corresponding to the convergent p_5/q_5.

Note that the continued fraction expansion of $\sqrt{22}$ is periodic with period 6 and the fundamental unit greater than one of $\mathbb{Q}(\sqrt{22})$ is $p_5 + q_5\sqrt{22}$. This is not by chance and in fact the following result is known (cf. (Nar, Theorem 3.19)).

Theorem. *Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with d a positive squarefree integer. Let s denote the period of simple continued fraction expansion of $\sqrt{d}$ and P/Q be its $(s-1)$th convergent. If $d \not\equiv 5 \pmod 8$, then the fundamental unit $\eta > 1$ of K is $P + Q\sqrt{d}$ and if $d \equiv 5 \pmod 8$, then either η or η^3 equals $P + Q\sqrt{d}$. Further $N_{K/\mathbb{Q}}(\eta)$ is positive if and only if the period s is even.*

Exercises

1. Show that an algebraic number field of odd degree contains only two roots of unity.
2. Let K be an algebraic number field which contains a root of unity different from ± 1. Prove that for each non-zero α in K, $N_{K/\mathbb{Q}}(\alpha) > 0$.
3. Let ζ be a primitive mth root of unity, $m \geq 2$. Find the number of roots of unity in $\mathbb{Q}(\zeta)$ when m is odd and when m is even.
4. Find the fundamental unit greater than 1 of each of the following fields:

   (a) $\mathbb{Q}(\sqrt{13})$;
   (b) $\mathbb{Q}(\sqrt{38})$;
   (c) $\mathbb{Q}(\sqrt{23})$;
   (d) $\mathbb{Q}(\sqrt{34})$.

5. If $m^2 - 1 > 1$ is a squarefree integer, then prove that a fundamental unit of real quadratic field $\mathbb{Q}(\sqrt{m^2 - 1})$ is $m + \sqrt{m^2 - 1}$.
6. Let d be a positive squarefree integer. Show that if there exist integers x, y such that $x^2 - dy^2 = -1$, then every odd prime factor of d is congruent to 1 modulo 4. Verify that the converse is not true for $d = 34$.
7. Find all the solutions of the equation $x^2 - 10y^2 = -1$ in positive integers x and y.
8. Find all the solutions of the equation $x^2 - 10y^2 = 10$ in positive integers x and y.

9. If an element α of an algebraic number field K satisfies a monic polynomial $g(X) \in \mathbb{Z}[X]$ and $g(r) = \pm 1$ for some $r \in \mathbb{Z}$, then prove that $\alpha - r$ is a unit of $\mathcal{O}_K$.
10. Determine a unit different from ± 1 in the ring of integers of $K = \mathbb{Q}(\theta)$, where $\theta^3 + 6\theta + 8 = 0$.
11. Show that if a positive squarefree integer d is congruent to 1 modulo 8, then the fundamental unit of $\mathbb{Q}(\sqrt{d})$ belongs to $\mathbb{Z}[\sqrt{d}]$.
12. Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field with d a squarefree integer. If the fundamental unit of K has norm -1, then prove that the equation $X^2 - dY^2 = -1$ is solvable over $\mathbb{Z}$.
13. Let $K = \mathbb{Q}(\theta)$ with θ satisfying an irreducible polynomial $X^3 - d$ over $\mathbb{Z}$, then prove that $N_{K/\mathbb{Q}}(x + y\theta + z\theta^2) = x^3 + dy^3 + d^2z^3 - 3dxyz$ for $x, y, z \in \mathbb{Z}$.
14. Find a unit different from ± 1 of $\mathcal{O}_K$, when K is the following field:

    (i) $\mathbb{Q}(\sqrt[3]{2})$;
    (ii) $\mathbb{Q}(\sqrt[3]{3})$;
    (iii) $\mathbb{Q}(\sqrt[3]{7})$.

15. Let K be an algebraic number field which is different from $\mathbb{Q}$ and not an imaginary quadratic field. Prove that for every real number $c > 0$, there exists an algebraic integer $\alpha \in K$ such that $0 < |\alpha| < c$.

Chapter 6
Prime Ideal Decomposition in Relative Extensions

6.1 Relative Ramification Index and Residual Degree

Let K'/K be an extension of algebraic number fields. Such an extension is traditionally called a relative extension. In this chapter, our aim is to introduce the notion of norm of ideals of $\mathcal{O}_{K'}$ with respect to K'/K and study factorisation of prime ideals of $\mathcal{O}_K$ in $\mathcal{O}_{K'}$.

Notation. We shall denote by $G(K)$ the group of non-zero fractional ideals of $\mathcal{O}_K$ and by $I(K)$ the semigroup of non-zero (integral)ideals of $\mathcal{O}_K$. Sometimes we shall write $\mathcal{O}'$ for $\mathcal{O}_{K'}$ and $\mathcal{O}$ for $\mathcal{O}_K$. By abuse of language a fractional ideal of $\mathcal{O}$ or $\mathcal{O}'$ will be referred to as a fractional ideal of K or K'.

The following proposition gives a natural embedding of $G(K)$ into $G(K')$.

Proposition 6.1 *Let K'/K be an extension of algebraic number fields, then the function $i_{K'/K} : G(K) \longrightarrow G(K')$ mapping A to $A\mathcal{O}_{K'}$ is a monomorphism of groups which maps $I(K)$ into $I(K')$.*

Proof One can easily see that the map $i_{K'/K}$ is a homomorphism which maps $I(K)$ into $I(K')$. Thus for proving the proposition, one needs to verify that the map is 1-1. Let $A \in G(K)$ be such that $A\mathcal{O}_{K'} = \mathcal{O}_{K'}$. Then

$$\mathcal{O}_K = \mathcal{O}_{K'} \cap K = A\mathcal{O}_{K'} \cap K \supseteq A. \tag{6.1}$$

Repeating the above process with A^{-1}, one can see that $A^{-1} \subseteq \mathcal{O}_K$. So we have

$$A = (A^{-1})^{-1} \supseteq \mathcal{O}_K{}^{-1} = \mathcal{O}_K. \tag{6.2}$$

In view of (6.1) and (6.2), $A = \mathcal{O}_K$. □

Definition Let $K \subset K'$ be as in the above proposition. If $A \in G(K)$, then $A\mathcal{O}_{K'}$ is known as the extension of the fractional ideal A to K' and if $A' \in G(K')$, then $A' \cap K$

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_6

is called the contraction of A' to K. The following lemma proves that $A' \cap K \in G(K)$.

Lemma 6.2 *If K'/K is an extension of algebraic number fields and A' is a non-zero fractional ideal of $\mathcal{O}'$, then $A' \cap K$ is a non-zero fractional ideal of $\mathcal{O}$.*

Proof There exists a non-zero element $\alpha \in \mathcal{O}'$ such that $\alpha A' \subseteq \mathcal{O}'$. Fix a non-zero element $a' \in A'$ and denote $\alpha a'$ by β. Then $\beta \in \mathcal{O}' \cap A'$ and $\beta A' \subseteq A'$. By Lemma 3.3, $\frac{N_{K'/\mathbb{Q}}(\beta)}{\beta}$ belongs to $\mathcal{O}'$. Therefore it follows that $N_{K'/\mathbb{Q}}(\beta) \in A'$ and $N_{K'/\mathbb{Q}}(\beta)A' \subseteq A'$; consequently $A' \cap K$ is non-zero and $N_{K'/\mathbb{Q}}(\beta)(A' \cap K) \subseteq A' \cap K$, which proves that $A' \cap K$ is a non-zero fractional ideal of $\mathcal{O}$. □

Let $K \subset K'$ be as above and A, A' belong to $G(K), G(K')$ respectively. The following natural questions arise: (i) Is $A\mathcal{O}' \cap K = A$? (ii) Is $(A' \cap K)\mathcal{O}' = A'$? The next lemma and the remark answer these questions.

Lemma 6.3 *If K'/K is an extension of algebraic number fields and A is a non-zero fractional ideal of K, then $A\mathcal{O}' \cap K = A$.*

Proof Suppose to the contrary that $A \subsetneqq A\mathcal{O}' \cap K$. Multiplying by A^{-1} on both sides, we have $AA^{-1} \subsetneqq (A\mathcal{O}' \cap K)A^{-1} \subseteq \mathcal{O}' \cap K = \mathcal{O}$. So $AA^{-1} \subsetneqq \mathcal{O}$, i.e., $\mathcal{O} \subsetneqq \mathcal{O}$, which is a contradiction. Hence $A = A\mathcal{O}' \cap K$. □

Remark 6.4 Let K'/K be an extension of algebraic number fields and A' be a fractional ideal of K'. Then $(A' \cap K)\mathcal{O}'$ need not be equal to A'. For example, consider $K = \mathbb{Q}$, $K' = \mathbb{Q}(\iota)$ with $\iota = \sqrt{-1}$ and the ideal $A' = (1 + \iota)\mathbb{Z}[\iota]$ of $\mathcal{O}' = \mathbb{Z}[\iota]$. Note that $A' \cap \mathbb{Q} = A' \cap \mathbb{Z} = 2\mathbb{Z}$ and $(2\mathbb{Z})\mathbb{Z}[\iota] \neq (1 + \iota)\mathbb{Z}[\iota]$.

Let $K \subseteq K'$ be an extension of algebraic number fields and $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. Note that if a prime ideal $\mathfrak{P}$ of $\mathcal{O}'$ lies above $\mathfrak{p}$, then $\mathfrak{P}$ contains $\mathfrak{p}\mathcal{O}'$ and hence $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}'$. The converse is also true because if $\mathfrak{P}$ divides $\mathfrak{p}\mathcal{O}'$, then $\mathfrak{P} \cap \mathcal{O} \supseteq \mathfrak{p}$. Since $\mathfrak{p}$ is maximal, $\mathfrak{P} \cap \mathcal{O} = \mathfrak{p}$.

For a relative extension K'/K, we now study the notions of (relative) index of ramification and (relative) residual degree of a non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K'}$ which lies over a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Note that $\mathfrak{p}$ is non-zero in view of Lemma 6.2, because $\mathfrak{P} \cap \mathcal{O}_K = \mathfrak{P} \cap K$.

Definition Let $K \subseteq K'$ be algebraic number fields. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}_{K'}$ and $\mathfrak{p}$ be the (non-zero) prime ideal of $\mathcal{O}_K$ lying below $\mathfrak{P}$. Then there is a natural embedding from $\mathcal{O}_K/\mathfrak{p}$ into $\mathcal{O}_{K'}/\mathfrak{P}$ which maps $\mathfrak{p} + \alpha$ to $\mathfrak{P} + \alpha$, $\alpha \in \mathcal{O}_K$. This is a monomorphism of fields. So $\mathcal{O}_K/\mathfrak{p}$ may be regarded as a subfield of $\mathcal{O}_{K'}/\mathfrak{P}$. The degree of the extension $\mathcal{O}_{K'}/\mathfrak{P}$ over $\mathcal{O}_K/\mathfrak{p}$ is called the (relative) residual degree of $\mathfrak{P}/\mathfrak{p}$ and will be denoted by $f_{K'/K}(\mathfrak{P})$ or by $f(\mathfrak{P}/\mathfrak{p})$.

Definition Let $K \subseteq K'$, $\mathfrak{P}$ and $\mathfrak{p}$ be as in the above definition. If $\mathfrak{P}^e | \mathfrak{p}\mathcal{O}_{K'}$ and $\mathfrak{P}^{e+1} \nmid \mathfrak{p}\mathcal{O}_{K'}$ then the number e is called the (relative) index of ramification of $\mathfrak{P}/\mathfrak{p}$ or of $\mathfrak{P}$ over K and will be denoted by $e_{K'/K}(\mathfrak{P})$ or by $e(\mathfrak{P}/\mathfrak{p})$.

Definition let K'/K be an extension of algebraic number fields. A non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K'}$ is said to be ramified in the extension K' over K if $e_{K'/K}(\mathfrak{P}) > 1$ and is called unramified otherwise. Similarly a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is said to be ramified in the extension K'/K if $e_{K'/K}(\mathfrak{P}) > 1$ for some prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$ and is called unramified otherwise, i.e., $\mathfrak{p}$ is said to be unramified in K', if $\mathfrak{p}\mathcal{O}_{K'} = \mathfrak{P}_1 \cdots \mathfrak{P}_r$, where $\mathfrak{P}_i$'s are distinct prime ideals of $\mathcal{O}_{K'}$.

Definition An extension K'/K of algebraic number fields is said to be unramified if every non-zero prime ideal of $\mathcal{O}_K$ is unramified in K'.

We shall prove in Chap. 8 that the only unramfied extension of $\mathbb{Q}$ is $\mathbb{Q}$ itself (See Corollary 8.4). All quadratic unramified extensions of a quadratic field are described in Example 7.29 .

The next proposition gives a basic property of index of ramification and residual degree.

Proposition 6.5 *Let $K \subseteq K' \subseteq K''$ be algebraic number fields. Let $\mathfrak{P}$ be a non-zero prime ideal of the ring of algebraic integers $\mathcal{O}''$ of K'' and $\mathfrak{p}$ be the non-zero prime ideal of $\mathcal{O}'$ lying below $\mathfrak{P}$. Then the following hold.*

(i) $e_{K''/K}(\mathfrak{P}) = e_{K''/K'}(\mathfrak{P})e_{K'/K}(\mathfrak{p})$.
(ii) $f_{K''/K}(\mathfrak{P}) = f_{K''/K'}(\mathfrak{P})f_{K'/K}(\mathfrak{p})$.

Proof Let e and e' denote the second and first factor on the right hand side of (i). By definition, we can write

$$\mathfrak{p}\mathcal{O}' = \mathfrak{p}^e A' \tag{6.3}$$

and

$$\mathfrak{p}\mathcal{O}'' = \mathfrak{P}^{e'} A'', \tag{6.4}$$

where A' is an (integral) ideal of $\mathcal{O}'$ coprime with $\mathfrak{p}$ and A'' is an ideal of $\mathcal{O}''$ coprime with $\mathfrak{P}$. Multiplying both sides of (6.3) by $\mathcal{O}''$, we have

$$\mathfrak{p}\mathcal{O}'' = (\mathfrak{p}\mathcal{O}'')^e A'\mathcal{O}''.$$

Substituting for $\mathfrak{p}\mathcal{O}''$ from (6.4), we obtain

$$\mathfrak{p}\mathcal{O}'' = (\mathfrak{P}^{e'})^e (A'')^e A'\mathcal{O}''. \tag{6.5}$$

Since $\mathfrak{p} + A' = \mathcal{O}'$, we have $\mathfrak{p}\mathcal{O}'' + A'\mathcal{O}'' = \mathcal{O}''$. So $\mathfrak{p}\mathcal{O}''$ and $A'\mathcal{O}''$ are coprime. This implies that $\mathfrak{P}$ which is a divisor of $\mathfrak{p}\mathcal{O}''$ must be coprime with $A'\mathcal{O}''$. It now follows from (6.5) that $\mathfrak{p}\mathcal{O}'' = (\mathfrak{P})^{ee'} B''$, where $\mathfrak{P}$ does not divide the ideal B'' of $\mathcal{O}''$. This proves that $e_{K''/K}(\mathfrak{P}) = ee'$ and hence assertion (i).

Let $\mathfrak{p}$ denote the prime ideal of $\mathcal{O}$ lying below $\mathfrak{P}$. Then $\mathcal{O}/\mathfrak{p} \subseteq \mathcal{O}'/\mathfrak{P} \subseteq \mathcal{O}''/\mathfrak{P}$. Therefore by Tower theorem of field extensions, we have

$$[\mathcal{O}''/\mathfrak{P} : \mathcal{O}/\mathfrak{p}] = [\mathcal{O}''/\mathfrak{P} : \mathcal{O}'/\mathfrak{P}][\mathcal{O}'/\mathfrak{P} : \mathcal{O}/\mathfrak{p}]$$

which proves assertion (ii). □

6.2 Splitting of Prime Ideals in Galois Extensions

The following theorem extends Theorems 4.1 and 4.3 to relative extensions.

Theorem 6.6 *Let K'/K be a Galois extension of algebraic number fields. Let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$ and $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ be the factorisation of $\mathfrak{p}\mathcal{O}'$ as a product of powers of distict prime ideals of $\mathcal{O}'$. Then given any i, j, $1 \leq i, j \leq r$, there exists $\sigma \in \mathrm{Gal}(K'/K)$ such that $\sigma(\mathfrak{P}_i) = \mathfrak{P}_j$. Moreover $e_{K'/K}(\mathfrak{P}_i) = e_{K'/K}(\mathfrak{P}_j)$ and $f_{K'/K}(\mathfrak{P}_i) = f_{K'/K}(\mathfrak{P}_j)$ for all i, j.*

Proof Keeping in mind the fact that $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ are maximal ideals of $\mathcal{O}'$ which lie over the maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, the first assertion follows immediately from Theorem 4.2. To prove the second assertion, fix any i, $1 \leq i \leq r$. By the first assertion, there exists $\sigma \in \mathrm{Gal}(K'/K)$ such that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_i$. Consider the mapping $\psi : \mathcal{O}'/\mathfrak{P}_1 \longrightarrow \mathcal{O}'/\mathfrak{P}_i$ defined by $\alpha + \mathfrak{P}_1 \longrightarrow \sigma(\alpha) + \mathfrak{P}_i$. Note that ψ is homomorphism of rings and is 1-1, onto. Also ψ is identity on $\mathcal{O}/\mathfrak{p}$. So $[\mathcal{O}'/\mathfrak{P}_1 : \mathcal{O}/\mathfrak{p}] = [\mathcal{O}'/\mathfrak{P}_i : \mathcal{O}/\mathfrak{p}]$, i.e., $f_{K'/K}(\mathfrak{P}_1) = f_{K'/K}(\mathfrak{P}_i)$.

Applying σ to the equality

$$\mathfrak{p}\mathcal{O}' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}, \tag{6.6}$$

we get

$$\mathfrak{p}\mathcal{O}' = \sigma(\mathfrak{P}_1)^{e_1} \cdots \sigma(\mathfrak{P}_r)^{e_r}. \tag{6.7}$$

Recall that $\sigma(\mathfrak{P}_1) = \mathfrak{P}_i$. So (6.6) and (6.7) together with the uniqueness of factorization imply that $e_{K'/K}(\mathfrak{P}_1) = e_{K'/K}(\mathfrak{P}_i)$. The proof of the theorem is now complete as i is arbitrary. □

6.3 Norm of an Ideal in Relative Extensions

The next lemma will be used in the sequel.

Lemma 6.7 *Let R be a commutative ring with identity and $\mathfrak{p}$ be a prime ideal of R. Let $X_1, \ldots, X_m$ be indeterminates and $\mathfrak{p}[X_1, \ldots, X_m]$ be the set of all polynomials in $X_1, \ldots, X_m$ whose coefficients belong to $\mathfrak{p}$. Then $\mathfrak{p}[X_1, \ldots, X_m]$ is a prime ideal of $R[X_1, \ldots, X_m]$.*

Proof We define a mapping $\psi : R[X_1, \ldots, X_m] \longrightarrow (R/\mathfrak{p})[X_1, \ldots, X_m]$. Since $R/\mathfrak{p}$ is an integral domain, so is $(R/\mathfrak{p})[X_1, \ldots, X_m]$. Define $\psi(f) = \bar{f}$ for any polynomial f, where $\bar{f}$ denotes the polynomial obtained by replacing each coefficient c of f by $\mathfrak{p} + c$ belonging to $\mathbb{R}/\mathfrak{p}$. Clearly ψ is an onto homomorphism of rings and so its kernel $\mathfrak{p}[X_1, \ldots, X_m]$ is a prime ideal of $R[X_1, \ldots, X_m]$. □

Definition If $h(X_1, \ldots, X_m)$ belongs to the polynomial ring $R[X_1, \ldots, X_m]$, we define the content of h to be the ideal of R generated by the coefficients of h. We shall denote it by $C_R(h)$ or by $C(h)$.

It may be pointed out that this definition of the content agrees with the usual definition of content of a polynomial h belonging to $\mathbb{Z}[X_1, \ldots, X_m]$ in the sense that the ideal of $\mathbb{Z}$ generated by the coefficients of h is the one generated by the gcd of these coefficients.

We now prove a proposition which extends the usual Gauss' lemma for polynomials with integral coefficients (cf. [Niv, Theorem 9.6],) to polynomials over Dedekind domains. This proposition is used to define the norm of an ideal in relative extensions.

Proposition 6.8 *Let R be a Dedekind domain. Let $h(X_1, \ldots, X_m)$ and $k(X_1, \ldots, X_m)$ belong to $R[X_1, \ldots, X_m]$, then $C(hk) = C(h)C(k)$.*

Proof Clearly $C(hk) \subseteq C(h)C(k)$. We only need to prove that $C(hk)$ divides $C(h)C(k)$. Let $\mathfrak{p}$ be any non-zero prime ideal of R. Let $\mathfrak{p}^r$ be the exact power of $\mathfrak{p}$ dividing $C(h)$ and $\mathfrak{p}^s$ be the exact power of $\mathfrak{p}$ dividing $C(k)$. To show $C(h)C(k) \subseteq C(hk)$, it is enough to verify that

$$\mathfrak{p}^{r+s+1} \nmid C(hk). \tag{6.8}$$

Write $C(h) = \mathfrak{p}^r I$ where $\mathfrak{p}$ does not divide the ideal I of R. Fix an element a belonging to $\mathfrak{p}^r \setminus \mathfrak{p}^{r+1}$, then we can write $Ra = \mathfrak{p}^r J$ where $\mathfrak{p}$ does not divides the ideal J of R. Choose an element $a' \in J$ such that $a' \notin \mathfrak{p}$, then $J \mid Ra'$ and we have $Ra' = JJ'$ for some ideal J' of R. It follows that $Ra \mid Ra'C(h)$ but $\mathfrak{p}$ does not divide $Ra^{-1}Ra'C(h) = J'I$. So if we consider the polynomial $\frac{a'h}{a}$, then $\frac{a'h}{a}$ belongs to $R[X_1, \ldots, X_m] \backslash \mathfrak{p}[X_1, \ldots, X_m]$ because $C(\frac{a'h}{a}) = \frac{a'}{a}C(h)$ is an integral ideal not divisible by $\mathfrak{p}$. Similarly one can show that there exist b', $b \in R$ with $\mathfrak{p}^{s+1}$ not dividing bR such that $\frac{b'}{b}k$ belongs to $R[X_1, \ldots, X_m] \backslash \mathfrak{p}[X_1, \ldots, X_m]$. By Lemma 6.7, $\mathfrak{p}[X_1, \ldots, X_m]$ is a prime ideal of $R[X_1, \ldots, X_m]$. So $\frac{a'b'}{ab}hk$ does not belong to $\mathfrak{p}[X_1, \ldots, X_m]$. Set $g = \frac{a'b'}{ab}hk$. Let g_i be a coefficient of a monomial occurring in the polynomial g such that $g_i \notin \mathfrak{p}$, then $\frac{g_i ab}{a'b'}$ is the coefficient of a monomial occurring in hk. We claim that $\frac{g_i ab}{a'b'}$ does not belong to $\mathfrak{p}^{r+s+1}$. This will prove that $C(hk) \nsubseteq \mathfrak{p}^{r+s+1}$, i.e., $\mathfrak{p}^{r+s+1} \nmid C(hk)$ as desired in (6.8). Suppose if possible $\frac{g_i ab}{a'b'} \in \mathfrak{p}^{r+s+1}$, which implies that $g_i ab \in \mathfrak{p}^{r+s+1}$, i.e., $\mathfrak{p}^{r+s+1} \mid g_i abR$. But $\mathfrak{p}$, $g_i R$ are coprime and the highest power of $\mathfrak{p}$ which divides aR is $\mathfrak{p}^r$. Thus the supposition

implies that $\mathfrak{p}^{s+1} \mid bR$, which is not so. This contradiction proves the claim and hence the theorem. □

The theorem proved below introduces the notion of norm of ideals in relative extensions.

Theorem 6.9 *Let K'/K be an extension of algebraic number fields of degree n. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the K-isomorphisms of K' into $\mathbb{C}$. Let $\widehat{K}$ be the smallest normal extension of K containing K' and $\hat{\mathcal{O}}$ be the ring of algebraic integers of $\widehat{K}$. If J' is a non-zero fractional ideal of K', then there exists a unique fractional ideal I of K such that $\prod_{i=1}^{n} \sigma_i(J')\widehat{\mathcal{O}} = I\widehat{\mathcal{O}}$. If J' is an integral ideal then so is I. The fractional ideal I is called the relative norm of J' and will be denoted by $N_{K'/K}(J')$.*

Proof We first consider the case when J' is an integral ideal of O'. Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the K-isomorphisms of K' into $\mathbb{C}$. Let $t_1, t_2, \ldots, t_m$ denote a system of generators of J' as an ideal of $\mathcal{O}'$. Define a polynomial $g(X_1, \ldots, X_m)$ belonging to $\mathcal{O}'[X_1, \ldots, X_m]$ by

$$g(X_1, \ldots, X_m) = t_1X_1 + \cdots + t_mX_m.$$

Then

$$C_{\mathcal{O}'}(g) = t_1\mathcal{O}' + \cdots + t_m\mathcal{O}' = J'.$$

For any i, $1 \leq i \leq n$, define the polynomial

$$g_i(X_1, \ldots, X_m) = \sigma_i(t_1)X_1 + \cdots + \sigma_i(t_m)X_m$$

belonging to $\sigma_i(\mathcal{O}')[X_1, \ldots, X_m] \subseteq \widehat{\mathcal{O}}[X_1, \ldots, X_m]$. Then

$$C_{\widehat{\mathcal{O}}}(g_i) = \sigma_i(t_1)\widehat{\mathcal{O}} + \cdots + \sigma_i(t_m)\widehat{\mathcal{O}} = \sigma_i(J')\widehat{\mathcal{O}}.$$

On taking product, we have $\prod_{i=1}^{n} \sigma_i(J')\widehat{\mathcal{O}} = \prod_{i=1}^{n} C_{\widehat{\mathcal{O}}}(g_i)$. Therefore in view of Proposition 6.8, we obtain

$$C_{\widehat{\mathcal{O}}}(\prod_{i=1}^{n} g_i) = \prod_{i=1}^{n} C_{\widehat{\mathcal{O}}}(g_i) = \prod_{i=1}^{n} \sigma_i(J')\widehat{\mathcal{O}}. \tag{6.9}$$

But the polynomial $\prod_{i=1}^{n} g_i(X_1, \ldots, X_m)$ is invariant under all automorphisms of $\widehat{K}/K$, because for any automorphism σ of $\widehat{K}/K$, the isomorphisms $\sigma \circ \sigma_1, \ldots, \sigma \circ \sigma_n$ form a permutation of $\sigma_1, \ldots, \sigma_n$. Hence by the fundamental theorem of Galois theory

(cf. Theorem A.44), $\prod_{i=1}^{n} g_i(X_1, \ldots, X_m)$ has coefficients in $K \cap \widehat{\mathcal{O}} = \mathcal{O}$. Denote $\prod_{i=1}^{n} g_i(X_1, \ldots, X_m)$ by $h(X_1, \ldots, X_m)$. It now follows from (6.9) that

$$\prod_{i=1}^{n} \sigma_i(J')\widehat{O} = C_{\widehat{O}}(h) = C_{\mathcal{O}}(h)\widehat{\mathcal{O}}$$

which proves the theorem in this case with $I = C_{\mathcal{O}}(h)$.

Next consider the case when J' is a non-zero fractional ideal of K'. There exists a non-zero element α in $\mathcal{O}'$ such that $\alpha J'$ is an integral ideal. Therefore by the first case $\prod_{i=1}^{n} \sigma_i(\alpha J')\widehat{\mathcal{O}} = I_1\widehat{\mathcal{O}}$ for some ideal I_1 of $\mathcal{O}$, which implies that

$$\prod_{i=1}^{n} \sigma_i(J')\widehat{\mathcal{O}} = (I_1 N_{K'/K}(\alpha^{-1}))\widehat{\mathcal{O}}.$$

So $I = I_1 N_{K'/K}(\alpha^{-1})$ works in this case. Uniqueness of I follows from Proposition 6.1, because the mapping $A \mapsto A\widehat{\mathcal{O}}$ from $G(K)$ into $G(\widehat{K})$ is a monomorphism. □

We next study some properties of relative norm.

Proposition 6.10 *Let K'/K be an extension of algebraic number fields of degree n. Let J_1', J_2' be two non-zero fractional ideals of K'. Then*

(i) $N_{K'/K}(J_1'J_2') = N_{K'/K}(J_1')N_{K'/K}(J_2')$,
(ii) *If* $\alpha \in K'$, *then* $N_{K'/K}(\alpha J_1') = N_{K'/K}(\alpha)N_{K'/K}(J_1')$,
(iii) *If I is a non-zero fractional ideal of K, then* $N_{K'/K}(I\mathcal{O}') = I^n$.

Proof (i). Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the K-isomorphisms of K' into $\mathbb{C}$. Let $\widehat{\mathcal{O}}$ be as in Theorem 6.9. By definition of norm, we have

$$\prod_{i=1}^{n} \sigma_i(J_1')\widehat{\mathcal{O}} = N_{K'/K}(J_1')\widehat{\mathcal{O}}, \tag{6.10}$$

$$\prod_{i=1}^{n} \sigma_i(J_2')\widehat{\mathcal{O}} = N_{K'/K}(J_2')\widehat{\mathcal{O}}. \tag{6.11}$$

Multiplying (6.10) and (6.11), we obtain

$$\prod_{i=1}^{n} \sigma_i(J_1'J_2')\widehat{\mathcal{O}} = N_{K'/K}(J_1')N_{K'/K}(J_2')\widehat{\mathcal{O}},$$

which implies that $N_{K'/K}(J_1'J_2') = N_{K'/K}(J_1')N_{K'/K}(J_2')$.

(ii). In view of assertion (i), it is enough to prove that if $\alpha \in K'$, then

$$N_{K'/K}(\alpha\mathcal{O}') = N_{K'/K}(\alpha)\mathcal{O}. \tag{6.12}$$

Observe that

$$\begin{aligned} N_{K'/K}(\alpha\mathcal{O}')\widehat{\mathcal{O}} &= \prod_{i=1}^{n}(\sigma_i(\alpha\mathcal{O}')\widehat{\mathcal{O}}) = \prod_{i=1}^{n}(\sigma_i(\alpha)\widehat{\mathcal{O}}) \\ &= (\prod_{i=1}^{n}\sigma_i(\alpha))\widehat{\mathcal{O}} = (N_{K'/K}(\alpha)\mathcal{O})\widehat{\mathcal{O}} \end{aligned}$$

and hence (6.12) is proved.
(iii). If I is a non-zero fractional ideal of K, then

$$N_{K'/K}(I\mathcal{O}')\widehat{\mathcal{O}} = \prod_{i=1}^{n}(\sigma_i(I)\widehat{\mathcal{O}}) = \underbrace{I\widehat{\mathcal{O}}\cdots I\widehat{\mathcal{O}}}_{n\text{-times}} = I^n\widehat{\mathcal{O}}\,;$$

this proves the desired result. □

Recall that for a non-zero ideal I of $\mathcal{O}_K$, the norm of I is defined to be the index of the subgroup I of $\mathcal{O}_K$. To distinguish it from relative norm, we shall sometimes refer to it as the **absolute norm** of I and retain the notation $N(I)$ already introduced in Sect. 3.3. For a non-zero fractional ideal $I = AB^{-1}$ of $\mathcal{O}_K$ with A, B integral ideals of $\mathcal{O}_K$, the absolute norm $N(I)$ of I is defined by $N(I) = N(A)/N(B)$.

Definition Let $G(K)$ be the group of all non-zero fractional ideals of an algebraic number field K and $P(K)$ denote its subgroup consisting of all non-zero principal fractional ideals. Then $G(K)/P(K)$ is called the class group of K and $|G(K)/P(K)|$ is called the class number of K.

We shall prove in Chap. 8 that the class number of an algebraic number field is finite. This fact will be used in the proof of the following proposition, which says that the notions of absolute norm $N(I)$ of a non-zero ideal I of $\mathcal{O}_K$ and that of relative norm $N_{K/\mathbb{Q}}(I)$ are essentially the same.

Proposition 6.11 *Let K be an algebraic number field. Let J be a non-zero fractional ideal of K. Then $N_{K/\mathbb{Q}}(J) = \mathbb{Z}N(J)$ where $N(J)$ stands for the absolute norm of J.*

Proof Let h denote the class number of K and $P(K)$ the group consisting of all non-zero principal fractional ideals. Since h is finite, then by Lagrange's Theorem for finite groups, we have $(P(K)J)^h = P(K)$, which implies that $J^h \in P(K)$, i.e., J^h is a principal ideal. Let $\alpha \in K$ be such that $J^h = \alpha\mathcal{O}$. Now $N_{K/\mathbb{Q}}(J^h) = (N_{K/\mathbb{Q}}(J))^h$ by Proposition 6.10(i). Also $N_{K/\mathbb{Q}}(J^h) = N_{K/\mathbb{Q}}(\alpha\mathcal{O}) = N_{K/\mathbb{Q}}(\alpha)\mathbb{Z}$ by Proposition 6.10(ii). Therefore

$$(N_{K/\mathbb{Q}}(J))^h = N_{K/\mathbb{Q}}(\alpha)\mathbb{Z}.$$

Keeping in mind the multiplicative property of absolute norm and Proposition 3.34, we have

$$N(J)^h = N(J^h) = N(\alpha\mathcal{O}) = |N_{K/\mathbb{Q}}(\alpha)|.$$

Comparing the above two equations, it follows that

$$(N_{K/\mathbb{Q}}(J))^h = (N(J)\mathbb{Z})^h$$

which shows that $N_{K/\mathbb{Q}}(J) = N(J)\mathbb{Z}$. □

Proposition 6.12 *Let $K \subset K' \subset K''$ be algebraic number fields. Let $\mathfrak{J}$ be a non-zero fractional ideal of K''. Then $N_{K'/K}(N_{K''/K'}(\mathfrak{J})) = N_{K''/K}(\mathfrak{J})$.*

Proof Case I. $\mathfrak{J}$ is a principal fractional ideal, say $\mathfrak{J} = \beta\mathcal{O}''$.
Using Proposition 6.10(ii) and Theorem 1.23, we see that

$$\begin{aligned} N_{K''/K}(\beta\mathcal{O}'') &= N_{K''/K}(\beta)\mathcal{O} = N_{K'/K}(N_{K''/K'}(\beta))\mathcal{O} \\ &= N_{K'/K}(N_{K''/K'}(\beta)\mathcal{O}') = N_{K'/K}(N_{K''/K'}(\beta\mathcal{O}'')). \end{aligned}$$

Case II. $\mathfrak{J}$ is any non-zero fractional ideal of K''.
Let h denote the class number of K'', then $\mathfrak{J}^h = \beta\mathcal{O}''$ for some $\beta \in K''$. Now by virtue of Case I, we have

$$\begin{aligned} (N_{K''/K}(\mathfrak{J}))^h &= N_{K''/K}(\mathfrak{J}^h) = N_{K''/K}(\beta\mathcal{O}'') \\ &= N_{K'/K}(N_{K''/K'}(\beta\mathcal{O}'')) = N_{K'/K}(N_{K''/K'}(\mathfrak{J}^h)) \\ &= N_{K'/K}(N_{K''/K}(\mathfrak{J}))^h = (N_{K'/K}(N_{K''/K'}(\mathfrak{J})))^h. \end{aligned}$$

Comparing the first and the last terms, we obtain $N_{K''/K}(\mathfrak{J}) = N_{K'/K}(N_{K''/K'}(\mathfrak{J}))$. □

6.4 The Fundamental Equality in Relative Extensions

The following proposition gives another definition of norm of ideals in relative extensions. This definition quickly yields an analogue of the fundamental equality proved in Proposition 4.4.

Proposition 6.13 *Let K'/K be an extension of algebraic number fields of degree n. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}'$ and $\mathfrak{p}$ be the prime ideal of $\mathcal{O}$ lying below $\mathfrak{P}$, then $N_{K'/K}(\mathfrak{P}) = \mathfrak{p}^f$, where f is the residual degree of $\mathfrak{P}$ over $\mathfrak{p}$.*

Proof Since $\mathfrak{P} \supseteq \mathfrak{p}\mathcal{O}'$, i.e., $\mathfrak{P} \mid \mathfrak{p}\mathcal{O}'$, we see that $N_{K'/K}(\mathfrak{P})$ divides $N_{K'/K}(\mathfrak{p}\mathcal{O}')$. As $N_{K'/K}(\mathfrak{p}\mathcal{O}') = \mathfrak{p}^n$, it follows that there exists s, $1 \le s \le n$ such that

$$N_{K'/K}(\mathfrak{P}) = \mathfrak{p}^s. \tag{6.13}$$

For proving the proposition, we have to prove that $s = f$. Let f_0, f' denote the respective degrees of $\mathcal{O}/\mathfrak{p}$, $\mathcal{O}'/\mathfrak{P}$ over $\mathbb{Z}/p\mathbb{Z}$. In view of Propositions 6.11, 6.12 and Eq. (6.13), we have

$$p^{f'}\mathbb{Z} = N_{K'/\mathbb{Q}}(\mathfrak{P}) = N_{K/\mathbb{Q}}(N_{K'/K}(\mathfrak{P})) = N_{K/\mathbb{Q}}(\mathfrak{p}^s) = p^{f_0 s}\mathbb{Z}.$$

So $f' = f_0 s$, i.e., $s = \frac{f'}{f_0}$ which is degree of $\mathcal{O}'/\mathfrak{P}$ over $\mathcal{O}/\mathfrak{p}$. This proves the proposition. □

Theorem 6.14 (General Fundamental Equality) *Let K'/K be a an extension of algebraic number fields of degree n. Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. Let $\mathfrak{p}\mathcal{O}' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ be the factorization of $\mathfrak{p}\mathcal{O}'$ into a product of powers of distinct prime ideals of $\mathcal{O}'$ and f_i denote the residual degree of $\mathfrak{P}_i/\mathfrak{p}$. Then $\sum_{i=1}^{r} e_i f_i = n$.*

Proof Taking norm on both sides of $\mathfrak{p}\mathcal{O}' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ and using Proposition 6.13, we have

$$\mathfrak{p}^n = (\mathfrak{p}^{f_1})^{e_1} \cdots (\mathfrak{p}^{f_r})^{e_r}$$

and hence $n = \sum_{i=1}^{r} e_i f_i$. □

The following corollaries are immediate consequences of the above theorem.

Corollary 6.15 *Let $K \subseteq K'$ and $\mathfrak{p}$ be as in the above theorem. If $\mathfrak{P}$ is a prime ideal of $\mathcal{O}'$ lying over $\mathfrak{p}$, then $e_{K'/K}(\mathfrak{P})$ and $f_{K'/K}(\mathfrak{P})$ do not exceed degree $[K' : K]$.*

Corollary 6.16 *There are at most $[K' : K]$ prime ideals of $\mathcal{O}'$ which lie over a given prime ideal $\mathfrak{p}$ of $\mathcal{O}$.*

Example 6.17 Let $K = \mathbb{Q}(\sqrt{2})$, $K' = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. By Theorem 4.11, there is only one prime ideal of $\mathcal{O}_K$ lying over 5, say $\mathfrak{p}$. We find the relative index of ramification and the residual degree of each prime ideal of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$. Note that $L := \mathbb{Q}(\sqrt{6}) \subset K'$ and there are exactly two prime ideals of $\mathcal{O}_L$ lying over 5 by Theorem 4.11. So there are at least two prime ideals of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$. Since $[K' : K] = 2$, it follows from Theorem 6.14 that there are exactly two prime ideals $\mathfrak{P}_1$, $\mathfrak{P}_2$, (say) of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$ and $e_{K'/K}(\mathfrak{P}_i) = f_{K'/K}(\mathfrak{P}_i) = 1$ for $i = 1, 2$.

Example 6.18 Let $K = \mathbb{Q}(\zeta)$ and $K' = \mathbb{Q}(\zeta, \eta)$, where ζ, η are respectively the primitive 7th and 12th roots of unity. We compute the relative index of ramification and relative residual degree of each prime ideal of $\mathcal{O}_{K'}$ lying over 2 with respect to the extension K'/K. Note that $K' = \mathbb{Q}(\zeta')$, where ζ' is a primitive 84th root of unity. Then by Theorem 4.15, $2\mathcal{O}_{K'} = \mathfrak{P}_1^2\mathfrak{P}_2^2$ where $\mathfrak{P}_1$, $\mathfrak{P}_2$ are distinct prime ideals of $\mathcal{O}_{K'}$ with $f_{K'/\mathbb{Q}}(\mathfrak{P}_i) = 6$ for $i = 1, 2$. Now applying Theorem 4.13, we see that $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are distinct prime ideals of $\mathcal{O}_K$ and $f_{K/\mathbb{Q}}(\mathfrak{p}_i) = 3$ for $i = 1, 2$. Therefore using Proposition 6.5, we see that the relative index of ramification and the relative residual degree of the prime ideals $\mathfrak{P}_1$, $\mathfrak{P}_2$ of $\mathcal{O}_{K'}$ lying over 2 are given by $e_{K'/K}(\mathfrak{P}_i) = 2$, $f_{K'/K}(\mathfrak{P}_i) = 2$ for $i = 1, 2$.

We now prove a result which is sometimes useful for factorization of prime ideals. We first give a definition extending the notion of Eisenstein polynomial. Let K be an algebraic number field and $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. A polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ with coefficients from $\mathcal{O}_K$ is called Eisenstein with respect to $\mathfrak{p}$ if each $a_i \in \mathfrak{p}$ and $a_0 \notin \mathfrak{p}^2$. As in the classical case it can be easily seen that such a polynomial is irreducible over K (cf. [Mar], Appendix 1]).

Proposition 6.19 *Let $K' = K(\theta)$ be an extension of an algebraic number field K where θ is a root of a polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ which is an Eisenstein polynomial with respect to a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$. Then $\mathfrak{p}\mathcal{O}_{K'} = \mathfrak{P}^n$ for a prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K'}$ i.e., $\mathfrak{p}$ is totally ramified in K'.*

Proof Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$ and let $\mathfrak{P}^e$ be its highest power dividing $\mathfrak{p}\mathcal{O}_{K'}$. Then by Corollary 6.15, $e \leq n$. In view of Theorem 6.14, it is enough to prove that $e = n$. Suppose to the contrary that $e < n$. Since $\theta^n = -\sum_{i=0}^{n-1} a_i\theta^i$ belongs to $\mathfrak{p}\mathcal{O}_{K'} \subseteq \mathfrak{P}$, it follows that $\theta \in \mathfrak{P}$. Keeping in mind that $e < n$, we see that $a_0 = -\sum_{i=1}^{n-1} a_i\theta^i - \theta^n$ belongs to $\mathfrak{P}^{e+1}$ which is impossible because $a_0 \notin \mathfrak{p}^2$. □

We conclude this chapter with an example of an extension K'/K of algebraic number fields for which $\mathcal{O}_{K'}$ is not a free $\mathcal{O}_K$-module.

Example 6.20 Let $K = \mathbb{Q}(\sqrt{-6})$, $K' = \mathbb{Q}(\sqrt{-6}, \sqrt{-3})$. Let $\mathcal{O}, \mathcal{O}'$ denote respectively their rings of algebraic integers. We show that $\mathcal{O}'$ is not a free $\mathcal{O}$-module. Suppose to the contrary that $\mathcal{O}'$ is a free $\mathcal{O}$-module with basis $\{w_1, w_2\}$. Then there exist a_1, a_2, a_3, a_4 in $\mathbb{Z}$ such that

$$a_1w_1 + a_2w_2 = 1 \quad \text{and} \quad a_3w_1 + a_4w_2 = \frac{1+\sqrt{-3}}{2}. \tag{6.14}$$

Let σ denote the automorphism of K'/K defined by $\sigma(\sqrt{-3}) = -\sqrt{-3}$. Applying σ to (6.14), we have

$$a_1\sigma(w_1) + a_2\sigma(w_2) = 1, \quad \text{and} \quad a_3\sigma(w_1) + a_4\sigma(w_2) = \frac{1-\sqrt{-3}}{2}. \tag{6.15}$$

Equations (6.14) and (6.15) can be rewritten in the matrix form as

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} w_1 & \sigma(w_1) \\ w_2 & \sigma(w_2) \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ \frac{1+\sqrt{-3}}{2} & \frac{1-\sqrt{-3}}{2} \end{bmatrix}.$$

Taking determinant on both sides, we obtain $aw = -\sqrt{-3}$, where $a = a_1a_4 - a_2a_3$ and $w = w_1\sigma(w_2) - \sigma(w_1)w_2$. Note that $\sigma(w) = -w$. So $\sigma(w^2) = w^2$. Hence $w^2 \in K$ by the fundamental theorem of Galois theory. Since w^2 is an algebraic integer, $w^2 \in \mathcal{O}$. The equality $a^2w^2 = -3$ together with Theorem 4.11 implies that

$$(a\mathcal{O})^2(w^2\mathcal{O}) = 3\mathcal{O} = \mathfrak{p}^2, \tag{6.16}$$

where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$ with $N(\mathfrak{p}) = 3$. Note that $\mathfrak{p}$ is not a principal ideal of $\mathcal{O}$ as no element of $\mathcal{O}$ has norm 3. Therefore it is clear from (6.16) that $a\mathcal{O} \neq \mathfrak{p}$ and so $a\mathcal{O} = \mathcal{O}$, which shows that a is a unit of $\mathcal{O}$. Since

$$\begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} = \begin{bmatrix} 1 \\ \frac{1+\sqrt{-3}}{2} \end{bmatrix},$$

it now follows that $\{1, (1+\sqrt{-3})/2\}$ is also an $\mathcal{O}$-basis of $\mathcal{O}'$. So we can write the element $\sqrt{2} = \sqrt{-6}/\sqrt{-3}$ of $\mathcal{O}'$ as

$$\sqrt{2} = a_0 + b_0\left(\frac{1+\sqrt{-3}}{2}\right)$$

for some a_0, b_0 in $\mathcal{O}$. Applying σ to the above equation, we obtain

$$-\sqrt{2} = a_0 + b_0\left(\frac{1-\sqrt{-3}}{2}\right).$$

On subtracting, the above equations show that $2\sqrt{2} = b_0\sqrt{-3}$, i.e., $b_0^2 = -8/3$ which is impossible, because b_0 is an algebraic integer. This contradiction proves that $\mathcal{O}'$ is not a free $\mathcal{O}$-module.

Exercises

1. Let $K = \mathbb{Q}(\sqrt{5})$ and $\mathfrak{p}$ be the prime ideal of $\mathcal{O}_K$ lying over 5. Find the relative index of ramification and the residual degree of each prime ideal of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$ when K' is one of the following fields:

   (i) $\mathbb{Q}(\sqrt{5}, \sqrt{-5})$;
   (ii) $\mathbb{Q}(\sqrt{2}, \sqrt{5})$.

2. Find the relative norm of the ideals $I_1' = \sqrt{2}\mathcal{O}_{K'}$, $I_2' = (\sqrt{2}+\sqrt{5})\mathcal{O}_{K'}$, where K'/K is as in part (ii) of the above exercise.
3. Let $K = \mathbb{Q}(\zeta)$, $K' = \mathbb{Q}(\zeta, \eta)$, where ζ, η are respectively primitive 5th and 12th roots of unity. Find the relative index of ramification and residual degree of all prime ideals of $\mathcal{O}_{K'}$ lying over the prime 3 with respect to K'/K.
4. Let $K = \mathbb{Q}(\sqrt{-23})$, $K' = \mathbb{Q}(\zeta)$ where ζ is a primitive 23rd root of unity. By Exercise 15 of Chap. 2, $K \subset K'$. Let $\mathfrak{p}_2$ be a prime ideal of $\mathcal{O}_K$ containing 2. Find the relative residual degree of each prime ideal of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}_2$.
5. Let K'/K be an extension of algebraic number fields. Given an ideal I of $\mathcal{O}_K$, prove that there exists an ideal of $\mathcal{O}_{K'}$ which lies over I.

6. Let K'/K be an extension of algebraic number fields. Prove that every non-zero fractional ideal of $\mathcal{O}_{K'}$ contains a vector space basis of K'/K consisting of algebraic integers.
7. Let K'/K be an extension of algebraic number fields. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}_{K'}$ and $\mathfrak{p}$ be the prime ideal of $\mathcal{O}_K$ lying below $\mathfrak{P}$. Let $d_{\mathfrak{P}}, d_{\mathfrak{p}}$ denote respectively the order of the classes $\mathfrak{P}P(K')$, $\mathfrak{p}P(K)$ in $G(K')/P(K')$, $G(K)/P(K)$. Prove that $d_{\mathfrak{p}} \mid d_{\mathfrak{P}} f(\mathfrak{P}/\mathfrak{p})$.
8. Let K'/K be an extension of algebraic number fields. Show that there is a homomorphism from $G(K')/P(K')$ into $G(K)/P(K)$ defined by taking any class $I'P(K')$ into $N_{K'/K}(I')P(K)$. Justify that the map is well defined. Give an example to show that the map is not necessarily onto. (See Remark 8.24)
9. Let K'/K be an extension of algebraic number fields of degree n and $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$. $\mathfrak{p}$ is said to be totally ramified in K' if $\mathfrak{p}\mathcal{O}_K = \mathfrak{P}^n$ for some prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K'}$. The prime ideal $\mathfrak{p}$ is said to split completely in K' if $\mathfrak{p}\mathcal{O}_K$ is a product of n distinct prime ideals of $\mathcal{O}_{K'}$. Prove that if a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is totally ramified (or splits completely) in K', then it does so in each intermediate field L lying between K and K'.

Chapter 7
Relative Discriminant and Dedekind's Theorem on Ramified Primes

7.1 Notions of Relative Different and Relative Discriminant

Let K'/K be an extension of algebraic number fields. In this chapter, our main aim is to prove a theorem of Dedekind characterizing those prime ideals of $\mathcal{O}_K$ which are ramified in K'/K. For this, we will introduce the notion of relative discriminant of K'/K. This can not be done in a way similar to that of introducing the absolute discriminant for an algebraic number field K in Chap. 2, because there we use the fact that $\mathcal{O}_K$ is a free abelian group of finite rank. In contrast to this, $\mathcal{O}_{K'}$ may not be a free $\mathcal{O}_K$-module for a relative extension K'/K in view of Example 6.20. Unlike the absolute discriminant, the relative discriminant of K'/K will not be an element of $\mathcal{O}_K$, but it will be an ideal of $\mathcal{O}_K$. However when $K = \mathbb{Q}$, it will coincide with the ideal of $\mathbb{Z}$ generated by $d_{K'}$. The relative discriminant will be defined using another important notion of relative different, which in turn, is defined using the concept of a dual of a module that is introduced in this section.

The ring of algebraic integers $\mathcal{O}_K, \mathcal{O}_{K'}$ will sometimes be denoted by $\mathcal{O}, \mathcal{O}'$ respectively. For $S' \subseteq K'$, $Tr_{K'/K}(S')$ will stand for the set $\{Tr_{K'/K}(\lambda) \mid \lambda \in S'\}$. As in the classical case, we define below the discriminant of a basis of K'/K.

Definition Let K'/K be a separable extension of degree n and $\sigma_1, \ldots, \sigma_n$ be the K-isomorphisms of K' into an algebraic closure of K. For a K-vector space basis $\{w_1, \ldots, w_n\}$ of K', $D_{K'/K}(w_1, \ldots, w_n)$ will stand for the square of determinant of the $n \times n$ matrix whose (i, j)th entry is $\sigma_i(w_j)$ and is called the discriminant of $\{w_1, \ldots, w_n\}$ relative to K'/K.

The result of the following lemma in classical case is already proved in Sect. 2.1.

Lemma 7.1 *Let K'/K, $\{w_1, \ldots, w_n\}$ be as in the above definition. Then the discriminant $D_{K'/K}(w_1, \ldots, w_n)$ equals determinant of the $n \times n$ matrix whose (i, j)th entry is $Tr_{K'/K}(w_i w_j)$ and is non-zero. In particular, the map $Tr_{K'/K}$ is not identically zero on K'.*

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_7

Proof Let $\sigma_1, \ldots, \sigma_n$ be the K-isomorphisms of K' into an algebraic closure of K. If A denotes the $n \times n$ matrix having (i, j)th entry $\sigma_i(w_j)$, then it can be easily verified that $A^t A$ is the matrix with (i, j)th entry $Tr_{K'/K}(w_i w_j)$. So $D_{K'/K}(w_1, \ldots, w_n)$ equals the determinant of the $n \times n$ matrix whose (i, j)th entry is $Tr_{K'/K}(w_i w_j)$. Since K'/K is a separable extension, it is simple in view of primitive element theorem (cf. Theorem A.28). Write $K' = K(\theta)$ and let C denote the transition matrix from $\{w_1, \ldots, w_n\}$ to $\{1, \theta, \ldots, \theta^{n-1}\}$. Arguing as for the proof of Lemma 2.3, it can be easily seen that

$$D_{K'/K}(1, \theta, \ldots, \theta^{n-1}) = (\det C)^2 D_{K'/K}(w_1, \ldots, w_n).$$

Since $D_{K'/K}(1, \theta, \ldots, \theta^{n-1})$ being the square of determinant of the Vandermonde matrix $(\sigma_i(\theta^{j-1}))_{i,j}$, equals the product $\prod_{1 \le i < j \le n} (\sigma_i(\theta) - \sigma_j(\theta))^2$ which is non-zero, it follows that $D_{K'/K}(w_1, \ldots, w_n)$ is non -zero. □

Definition. Let K'/K be an extension of algebraic number fields. For a subset M' of K', we define M'^* by

$$M'^* = \{\lambda \in K' \mid Tr_{K'/K}(\lambda M') \subseteq \mathcal{O}_K\}.$$

Observe that if M' is an $\mathcal{O}'$-module, then so is M'^*. M'^* is called the dual module of M'.

Proposition 7.2 *Let K'/K be an extension of algebraic number fields. The following hold:*

(I) *If $S \subseteq T \subseteq K'$, then $S^* \supseteq T^*$.*
(II) *$\mathcal{O}'^* \supseteq \mathcal{O}'$.*
(III) *If A' is a non-zero fractional ideal of $\mathcal{O}'$, then so is A'^* and $A'A'^* = \mathcal{O}'^*$.*

Proof The first assertion can be easily verified. The second follows from the fact that for $\alpha \in \mathcal{O}'$, $Tr_{K'/K}(\alpha)$ belongs to $\mathcal{O}$ in view of Corollary 1.21. For proving (III), let A' be a non-zero fractional ideal of K'. Since A'^* is an $\mathcal{O}'$-module, to prove it is a fractional ideal, it is enough to show that there exists $\alpha \neq 0$ in $\mathcal{O}'$ such that $\alpha A'^* \subset \mathcal{O}'$. Let $w_1, \ldots, w_n$ be algebraic integers in A' which form a basis of K' as a K-vector space. Let d denote the determinant of the $n \times n$ matrix P with (i, j)th entry $Tr_{K'/K}(w_i w_j)$. Note that $d \neq 0$ in view of Lemma 7.1. We show that

$$dA'^* \subseteq \mathcal{O}'. \tag{7.1}$$

Let $\beta \in A'^*$ .Write

$$\beta = a_1 w_1 + \cdots + a_n w_n, \quad a_i \in K. \tag{7.2}$$

Then for $1 \le j \le n$,

$$Tr_{K'/K}(\beta w_j) = \sum_{i=1}^{n} a_i Tr_{K'/K}(w_i w_j) = b_j \text{ (say)}$$

is in $\mathcal{O}$ in view of the definition of A'^* and the fact that $w_j \in A'$. We can write the above equations in the matrix form as

$$\begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix} = P \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}.$$

On applying Cramer's rule, we see that $a_i = \frac{\det P_i}{\det P}$, where P_i is the matrix obtained from P by replacing the entries of the ith column by $b_1, \ldots, b_n$ respectively. Keeping in mind that all entries of P_i are in $\mathcal{O}$, we conclude that $da_i \in \mathcal{O}$ and hence it follows from (7.2) that $d\beta \in \mathcal{O}'$. This proves (7.1).

It remains to prove that $A'A'^* = \mathcal{O}'^*$. We first show that $\mathcal{O}'^* A'^{-1} \subseteq A'^*$. Let $\lambda \in \mathcal{O}'^* A'^{-1}$ and a' be an element of A'. Write $\lambda = \sum \alpha_i b_i$, $\alpha_i \in \mathcal{O}'^*$, $b_i \in A'^{-1}$. As $b_i a'$ belongs to $\mathcal{O}'$, it follows that $Tr_{K'/K}(\lambda a') = \sum Tr_{K'/K}(\alpha_i b_i a')$ is in $\mathcal{O}$. This proves that $\lambda \in A'^*$. Thus $\mathcal{O}'^* A'^{-1} \subseteq A'^*$. It only remains to be shown that $A'A'^* \subseteq \mathcal{O}'^*$. To verify this, let $a \in A'$, $a^* \in A'^*$, we have to show that aa^* is in $\mathcal{O}'^*$. This holds because for any α in $\mathcal{O}'$, $Tr_{K'/K}(aa^*\alpha)$ is in $\mathcal{O}$ in view of the fact that $a\alpha$ is in A'. So $A'A'^* = \mathcal{O}'^*$. □

The following corollary is an immediate consequence of assertion (III) of the above proposition and the fact that the set of non-zero fractional ideals of $\mathcal{O}'$ form a group under multiplication.

Corollary 7.3 *If A' is a non-zero fractional ideal of $\mathcal{O}'$, then $(A'^*)^* = A'$.*

Definition. The integral ideal $(\mathcal{O}'^*)^{-1}$ is called the relative different of the extension K'/K and will be denoted by $\Delta_{K'/K}$. The integral ideal $d_{K'/K}$ defined by $d_{K'/K} = N_{K'/K}(\Delta_{K'/K})$ is called the relative discriminant of the extension K'/K.

7.2 Relative Discriminant as an Extension of Discriminant

In this section, it will be proved that for an algebraic number field K, the relative discriminant of $K/\mathbb{Q}$ is the ideal of $\mathbb{Z}$ generated by d_K. The following result of field theory will be used in the sequel.

Theorem 7.4 *Let L/K be a finite separable extension of fields. If $\{w_1, \ldots, w_n\}$ is a basis of the vector space L/K, then there exists a unique basis $\{w_1^*, \ldots, w_n^*\}$ of L/K such that $Tr_{L/K}(w_i w_j^*) = \delta_{ij}$, where δ_{ij} is 1 or 0 according as $i = j$ or not. The basis $\{w_1^*, \ldots, w_n^*\}$ of L/K is called dual to the basis $\{w_1, \ldots, w_n\}$.*

Proof Let $\mathrm{Hom}(L, K)$ denote the set of K-linear functionals on L. Define a mapping $T : L \to \mathrm{Hom}(L, K)$ by $\alpha \mapsto T_\alpha$, where $T_\alpha : L \to K$ is the linear functional given by $T_\alpha(\beta) = Tr_{L/K}(\alpha\beta)$ for $\beta \in L$. It can be easily seen that T is a linear transformation. Since L/K is separable, the trace map is not identically zero on L in view of Lemma 7.1. Consequently for $\alpha \neq 0$ in L, T_α is non-zero. Therefore T is one-to-one. Since the vector spaces L and $\mathrm{Hom}(L, K)$ have the same dimension over K, we conclude that T is onto. Let $f_1, \ldots, f_n$ be elements of $\mathrm{Hom}(L, K)$ defined by $f_i(w_j) = \delta_{ij}$. It can be easily checked that $\{f_1, \ldots, f_n\}$ is linearly independent over K and hence is a basis of $\mathrm{Hom}(L, K)$. Keeping in mind that T is an isomorphism, it follows that there exists a basis $\{w_1^*, \ldots, w_n^*\}$ of L/K such that $T(w_i^*) = f_i \ \forall i$. So $T_{w_i^*}(w_j) = f_i(w_j)$ for $1 \leq i, j \leq n$, i.e., $Tr_{L/K}(w_i^* w_j) = \delta_{ij}$ for all i, j as desired. □

Proposition 7.5 *Let K'/K be an extension of algebraic number fields of degree n. Let $M \subseteq K'$ be a free $\mathcal{O}$-module with basis $\{w_1, \ldots, w_n\}$. Then M^* is a free $\mathcal{O}$-module with basis $\{w_1^*, \ldots, w_n^*\}$ which is dual to the basis $\{w_1, \ldots, w_n\}$.*

Proof Note that w_j^* belongs to M^* for each j, because for any element $\alpha = \sum a_i w_i$ of M with a_i in $\mathcal{O}$, we have

$$Tr_{K'/K}(w_j^* \alpha) = \sum_i a_i Tr_{K'/K}(w_j^* w_i) = a_j.$$

Since M is an $\mathcal{O}$-module so is M^*. Therefore

$$\mathcal{O}w_1^* + \cdots + \mathcal{O}w_n^* \subseteq M^*.$$

To prove the equality, let β be an element of M^*. Since $\{w_1^*, \ldots, w_n^*\}$ is a vector space basis of K'/K, there exist b_i's belonging to K such that $\beta = \sum_i b_i w_i^*$. Keeping in mind that $Tr_{K'/K}(\beta w_j) = \sum_i b_i Tr_{K'/K}(w_i^* w_j) = b_j$ is in $\mathcal{O}$ for each j, we see that β belongs to $\mathcal{O}w_1^* + \cdots + \mathcal{O}w_n^*$. This completes the proof of the proposition. □

Corollary 7.6 *If $\mathcal{O}'$ is a free $\mathcal{O}$-module with $\mathcal{O}$-basis $\{w_1, \ldots, w_n\}$, then $\mathcal{O}'^* = \mathcal{O}w_1^* + \cdots + \mathcal{O}w_n^*$.*

The following lemma is used in the proof of the next theorem which relates $d_{K/\mathbb{Q}}$ with d_K.

Lemma 7.7 *Let K be an algebraic number field with ring of algebraic integers $\mathcal{O}$ and A containing $\mathcal{O}$ be a fractional ideal of K. Then $N(A) = \frac{1}{[A:\mathcal{O}]}$.*

Proof Let t be a positive integer such that $tA \subseteq \mathcal{O}$; such an integer exists because if α is a non-zero element of $\mathcal{O}$ with $\alpha A \subseteq \mathcal{O}$, then we may take $t = \pm N_{K/\mathbb{Q}}(\alpha)$ as $N_{K/\mathbb{Q}}(\alpha)/\alpha$ belongs to $\mathcal{O}$ in view of Lemma 3.3. Let $\{u_1, \ldots, u_n\}$, $\{w_1, \ldots, w_n\}$ be $\mathbb{Z}$-bases of $\mathcal{O}$ and A respectively. As tA is an ideal of $\mathcal{O}$, we have $N(tA) = [\mathcal{O} : tA]$ which gives

$$t^n N(A) = [\mathcal{O} : tA]. \tag{7.3}$$

Let d, d' denote the absolute values of the determinants of the transition matrices from $\{u_1, \ldots, u_n\}$ to $\{tw_1, \ldots, tw_n\}$ and from $\{w_1, \ldots, w_n\}$ to $\{u_1, \ldots, u_n\}$ respectively. Then clearly $d = t^n/d'$. On applying Lemma 2.14, we see that $d = [\mathcal{O} : tA]$. and $d' = [A : \mathcal{O}]$. The lemma now follows immediately from (7.3). □

Theorem 7.8 *The ideal $d_{K/\mathbb{Q}}$ is generated by d_K for an algebraic number field K.*

Proof Let $\{u_1, \ldots, u_n\}$ be an integral basis of K. Then in view of Proposition 7.5, its dual basis $\{u_1^*, \ldots, u_n^*\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}^* = (\Delta_{K/\mathbb{Q}})^{-1}$. So on applying Lemma 7.7 to $\mathcal{O}^*$, we have

$$N(\Delta_{K/\mathbb{Q}}) = 1/N(\mathcal{O}^*) = [\mathcal{O}^* : \mathcal{O}]. \tag{7.4}$$

By Lemma 2.14, $[\mathcal{O}^* : \mathcal{O}]$ equals the absolute value d (say) of the determinant of the transition matrix from $\{u_1^*, \ldots, u_n^*\}$ to $\{u_1, \ldots, u_n\}$. Recall that in view of Proposition 6.11 and the definition of relative discriminant, $d_{K/\mathbb{Q}}$ is the ideal of $\mathbb{Z}$ generated by $N(\Delta_{K/\mathbb{Q}})$. So the theorem will follow from (7.4) once we prove that $d = |d_K|$. To prove the last equality, write

$$u_i = \sum_k a_{ik} u_k^*, \quad a_{ik} \in \mathbb{Z}.$$

Then $Tr_{K/\mathbb{Q}}(u_i u_j) = a_{ij}$. So by definition of discriminant, $\det(a_{ij})_{i,j} = d_K$ and hence the desired equality $d = |d_K|$ is now proved. □

7.3 Properties of Relative Different and Relative Discriminant

The following proposition and its corollary give an important property of relative different and relative discriminant.

Proposition 7.9 *Let $K \subseteq K' \subseteq K''$ be a tower of algebraic number fields. Then $\Delta_{K''/K} = \Delta_{K'/K} \Delta_{K''/K'}$.*

Proof We shall prove that

$$(\Delta_{K''/K})^{-1} = (\Delta_{K'/K})^{-1} (\Delta_{K''/K'})^{-1}.$$

Let $\mathcal{O}$, $\mathcal{O}'$, $\mathcal{O}''$ denote the ring of algebraic integers of K, K' and K'' respectively. By definition, an element α of K'' belongs to $(\Delta_{K''/K})^{-1}$ if and only if $Tr_{K''/K}(\alpha \mathcal{O}'') \subseteq \mathcal{O}$. Using Theorem 1.23 together with Eq. (3.1), we see that for α in K''

$$\begin{aligned} Tr_{K''/K}(\alpha\mathcal{O}'') \subseteq \mathcal{O} &\iff Tr_{K'/K}(Tr_{K''/K'}(\alpha\mathcal{O}'')) \subseteq \mathcal{O} \\ &\iff Tr_{K'/K}(Tr_{K''/K'}(\alpha\mathcal{O}'')\mathcal{O}') \subseteq \mathcal{O} \\ &\iff Tr_{K''/K'}(\alpha\mathcal{O}'') \subseteq (\Delta_{K'/K})^{-1} \\ &\iff \Delta_{K'/K} Tr_{K''/K'}(\alpha\mathcal{O}'') \subseteq \mathcal{O}' \\ &\iff Tr_{K''/K'}(\alpha\Delta_{K'/K}\mathcal{O}'') \subseteq \mathcal{O}' \\ &\iff \alpha\Delta_{K'/K} \subseteq (\Delta_{K''/K'})^{-1} \\ &\iff \alpha \in (\Delta_{K'/K})^{-1}(\Delta_{K''/K'})^{-1}. \end{aligned}$$

This proves the desired equality. □

Corollary 7.10 *If $K \subseteq K' \subseteq K''$ is a tower of algebraic number fields, then*

$$d_{K''/K} = (d_{K'/K})^{[K'':K']} N_{K'/K}(d_{K''/K'}).$$

Proof On taking norm of the equality proved in the above proposition and using Proposition 6.12, we have

$$\begin{aligned} d_{K''/K} &= (d_{K'/K})^{[K'':K']} N_{K''/K}(\Delta_{K''/K'}) \\ &= (d_{K'/K})^{[K'':K']} N_{K'/K}(N_{K''/K'}(\Delta_{K''/K'})) \\ &= (d_{K'/K})^{[K'':K']} N_{K'/K}(d_{K''/K'}). \end{aligned}$$

□

The following corollary is an immediate consequence of Theorem 7.8 and Corollary 7.10.

Corollary 7.11 *If $K \subseteq L$ are algebraic number fields, then d_L is divisible by $d_K^{[L:K]}$.*

Notation. Let $K \subseteq K'$ be algebraic number fields. Let $\sigma_1, \ldots, \sigma_n$ be all the K - isomorphisms of K' into $\mathbb{C}$ with σ_1 as identity. Let θ be an element of K'. We shall denote $\prod_{i=2}^{n}(\theta - \sigma_i(\theta))$ by $\delta_{K'/K}(\theta)$. Observe that $\delta_{K'/K}(\theta) \neq 0$ if and only if the minimal polynomial $F(X)$ of θ over K has degree n in which case $\delta_{K'/K}(\theta) = F'(\theta)$, because on writing $F(X) = \prod_{i=1}^{n}(X - \sigma_i(\theta))$, we see that $F'(X) = \sum_{j=1}^{n} \frac{F(X)}{X-\sigma_j(\theta)}$.

The following theorem which describes a set of generators of $\Delta_{K'/K}$ will be used in the proof of the main result of this chapter.

Theorem 7.12 *Let K'/K be an extension of algebraic number fields. The relative different $\Delta_{K'/K}$ is the ideal of $\mathcal{O}'$ generated by $\delta_{K'/K}(\theta)$, where θ runs over elements of $\mathcal{O}'$.*

Before proving the above theorem, we shall prove a few preliminary results some of which are of independent interest as well. Lemmas 7.13, 7.14, 7.15 are needed for the proof of Proposition 7.16 which together with Lemmas 7.20 and 7.21 are used in the proof of Theorem 7.12.

Lemma 7.13 *Suppose $K(\theta)/K$ is an extension of algebraic number fields with θ an algebraic integer having minimal polynomial $F(X) = X^n + a_1X^{n-1} + \cdots + a_n$ over K. If $F(X) = (X - \theta)(\beta_0X^{n-1} + \cdots + \beta_{n-1})$, then*

$$\sum_{i=0}^{n-1} \mathcal{O}\theta^i = \sum_{i=0}^{n-1} \mathcal{O}\beta_i. \tag{7.5}$$

Proof Since $\mathcal{O}$ is an integrally closed domain, $F(X) \in \mathcal{O}[X]$ in view of Lemma 1.11. Hence all $\beta_i \in \mathcal{O}[\theta]$. Therefore the right hand side of (7.5) is contained in its left hand side. To prove equality, it is enough to show that the transition matrix from $\{1, \theta, \ldots, \theta^{n-1}\}$ to $\{\beta_0, \ldots, \beta_{n-1}\}$ is a triangular matrix with each diagonal entry 1. First observe that $\beta_0 = 1$, $a_1 = \beta_1 - \theta\beta_0$. In fact $a_i = \beta_i - \theta\beta_{i-1}$ for all $i \geq 1$. Therefore

$\beta_0 = 1$
$\beta_1 = a_1 + \theta\beta_0 = a_1 + \theta$
$\beta_2 = a_2 + \theta\beta_1 = a_2 + \theta(a_1 + \theta) = a_2 + a_1\theta + \theta^2$
$\vdots\ \vdots\ \vdots\ \vdots\ \vdots$
$\beta_{n-1} = a_{n-1} + a_{n-2}\theta + \cdots + \theta^{n-1}$.

Note that the transition matrix from $\{1, \theta, \ldots, \theta^{n-1}\}$ to $\{\beta_0, \beta_1, \ldots, \beta_{n-1}\}$ is

$$\begin{bmatrix} 1 & 0 & 0 & \cdots 0 \\ a_1 & 1 & 0 & \cdots 0 \\ a_2 & a_1 & 1 & \cdots 0 \\ \cdot & \cdot & \cdot & \cdots \cdot \\ \cdot & \cdot & \cdot & \cdots \cdot \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots 1 \end{bmatrix}$$

and hence the lemma is proved. □

Notation. Let K'/K be a finite separable extension of fields. For a polynomial $g(X) = \sum_{i=0}^{m} b_iX^i \in K'[X]$, $Tr_{K'/K}(g(X))$ will stand for the polynomial $\sum_{i=0}^{m} Tr_{K'/K}(b_i)X^i$.

With the above notation we prove

Lemma 7.14 *Let K be an arbitrary field and $K' = K(\theta)$ be a separable extension of K of degree n. Let $F(X)$ be the minimal polynomial of θ over K. Then $Tr_{K'/K}\left(\frac{F(X)}{X-\theta}\frac{\theta^i}{F'(\theta)}\right) = X^i$ for $0 \leq i \leq n-1$.*

Proof Since K'/K is a separable extension of degree n, $F(X)$ has n distinct roots say, $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$. Let $\sigma_1, \ldots, \sigma_n$ be all the distinct K-isomorphisms of K' into an algebraic closure of K defined by $\sigma_i(\theta) = \theta^{(i)}$. Fix any i, $0 \leq i \leq n-1$. In view of Theorem 1.19, we have

$$Tr_{K'/K}\left(\frac{F(X)}{X-\theta}\frac{\theta^i}{F'(\theta)}\right)=\sum_{j=1}^{n}\frac{F(X)\theta^{(j)^i}}{(X-\theta^{(j)})F'(\theta^{(j)})}.$$

The polynomial on the right hand side of the above equation is of degree less than or equal to $n-1$. So it suffices to show that n distinct elements namely $\theta^{(1)}, \theta^{(2)}, \ldots, \theta^{(n)}$ satisfy the polynomial

$$Tr_{K'/K}\left(\frac{F(X)}{X-\theta}\frac{\theta^i}{F'(\theta)}\right)-X^i$$

having degree less that or equal to $n-1$. For this it is enough to verify that the polynomial $Tr_{K'/K}\left(\frac{F(X)}{X-\theta}\frac{\theta^i}{F'(\theta)}\right)$ attains the value $(\theta^{(k)})^i$ at $X=\theta^{(k)}$ for $1\le k\le n$, which can be seen immediately because

$$\left[\frac{F(X)}{(X-\theta^{(j)})}\right]_{X=\theta^{(k)}}=\begin{cases}0 & \text{if } k\neq j,\\ F'(\theta^{(k)}) & \text{if } k=j.\end{cases}$$

□

Lemma 7.15 *Let K be an arbitrary field and $K'=K(\theta)$ be a separable extension of degree n. Let $F(X)$ be the minimal polynomial of θ over K. If $F(X)=(X-\theta)(b_{n-1}X^{n-1}+b_{n-2}X^{n-2}+\cdots+b_0)$, then the dual basis of $\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ is $\left\{\frac{b_0}{F'(\theta)},\frac{b_1}{F'(\theta)},\ldots,\frac{b_{n-1}}{F'(\theta)}\right\}$.*

Proof By Lemma 7.14, we have

$$Tr_{K'/K}\left(\frac{F(X)}{X-\theta}\frac{\theta^i}{F'(\theta)}\right)=X^i,\ 0\le i\le n-1.$$

Therefore

$$\sum_{j=0}^{n-1}Tr_{K'/K}\left(b_j\frac{\theta^i}{F'(\theta)}\right)X^j=X^i,\ 0\le i\le n-1.$$

Hence

$$Tr_{K'/K}\left(b_j\frac{\theta^i}{F'(\theta)}\right)=\delta_{ij}=\begin{cases}1 & \text{if } i=j,\\ 0 & \text{otherwise.}\end{cases}$$

So dual basis of $\{1,\theta,\theta^2,\ldots,\theta^{n-1}\}$ is $\left\{\frac{b_0}{F'(\theta)},\frac{b_1}{F'(\theta)},\ldots,\frac{b_{n-1}}{F'(\theta)}\right\}$. □

Using the above lemma, we first prove

Proposition 7.16 *Let $K'=K(\theta)$ be an algebraic number field with θ an algebraic integer having minimal polynomial $F(X)$ over K. If $M=\mathcal{O}[\theta]$, then $M^*=\frac{M}{F'(\theta)}$.*

Proof Let n denote the degree of K'/K. Then M is a free $\mathcal{O}$-module with basis $\{1, \theta, \ldots, \theta^{n-1}\}$. By Proposition 7.5, $M^* = \mathcal{O}w_1^* + \cdots + \mathcal{O}w_n^*$, where $\{w_1^*, \ldots, w_n^*\}$ is the basis dual to $\{1, \theta, \ldots, \theta^{n-1}\}$. Write

$$F(X) = (X - \theta)(\sum_{i=0}^{n-1} b_i X^i).$$

By Lemma 7.15, $\left\{ \frac{b_0}{F'(\theta)}, \frac{b_1}{F'(\theta)}, \ldots, \frac{b_{n-1}}{F'(\theta)} \right\}$ is dual basis to $\{1, \theta, \ldots, \theta^{n-1}\}$. So $M^* = \frac{1}{F'(\theta)} \sum_{i=0}^{n-1} \mathcal{O}b_i$. In view of Lemma 7.13, $\sum_{i=0}^{n-1} \mathcal{O}b_i = \sum_{i=0}^{n-1} \mathcal{O}\theta^i$. Therefore

$$M^* = \frac{1}{F'(\theta)} \sum_{i=0}^{n-1} \mathcal{O}\theta^i = \frac{M}{F'(\theta)}.$$

□

Example 7.17 We compute $\Delta_{K/\mathbb{Q}}$ when $K = \mathbb{Q}(\sqrt{-3})$ and calculate its norm. Note that $\mathcal{O}_K = \mathbb{Z}[\theta]$, where $\theta = \frac{1+\sqrt{-3}}{2}$. By Proposition 7.16, $\mathcal{O}_K{}^* = \frac{1}{F'(\theta)}\mathcal{O}_K$ where $F(X) = X^2 - X + 1$ is the minimal polynomial of θ over $\mathbb{Q}$. A simple calculation shows that $\mathcal{O}_K{}^* = \frac{1}{\sqrt{-3}}\mathcal{O}_K$. Therefore $\Delta_{K/\mathbb{Q}} = \sqrt{-3}\mathcal{O}_K$ and $N_{K/\mathbb{Q}}(\Delta_{K/\mathbb{Q}}) = 3\mathbb{Z}$.

Example 7.18 We compute $\Delta_{K/\mathbb{Q}}$ when $K = \mathbb{Q}(\theta)$ where θ satisfies the polynomial $F(X) = X^3 - X + 1$. In view of Example 2.19, $\mathcal{O}_K = \mathbb{Z}[\theta]$ and $d_K = -23$. By Proposition 7.16, we have $\mathcal{O}_K{}^* = \frac{1}{F'(\theta)}\mathcal{O}_K = \frac{1}{3\theta^2-1}(\mathbb{Z}[\theta])$. So $\Delta_{K/\mathbb{Q}} = (3\theta^2 - 1)(\mathbb{Z}[\theta])$.

The following simple lemma will be used in the proof of Lemma 7.21.

Lemma 7.19 *Let K'/K be an extension of algebraic number fields of degree n. If $\{w_1, \ldots, w_n\}$ is a vector space basis of K'/K consisting of algebraic integers and d is the determinant of the $n \times n$ matrix $\left(Tr_{K'/K}(w_i w_j)\right)_{i,j}$, then $\mathcal{O}' \subseteq \frac{1}{d} \sum_{i=1}^{n} \mathcal{O}w_i$.*

Proof Let α be any element of $\mathcal{O}'$. We can write $\alpha = \sum_{i=1}^{n} a_i w_i$, $a_i \in K$ which gives

$$\alpha w_j = \sum_{i=1}^{n} a_i w_i w_j, \quad a_i \in K.$$

Taking trace on both sides of the above equation, we have

$$Tr_{K'/K}(\alpha w_j) = \sum_{i=1}^{n} a_i Tr_{K'/K}(w_i w_j) = b_j \text{ (say)}.$$

Since α, w_j belong to $\mathcal{O}'$, we have $b_j = Tr_{K'/K}(\alpha w_j) \in \mathcal{O}$. Therefore we can write the above equations in the matrix form as

$$\begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} = P \begin{bmatrix} a_1 \\ \vdots \\ a_n \end{bmatrix}$$

where P is the matrix with (i, j)th entry $Tr_{K'/K}(w_i w_j)$. Recall that $\det P$ is non-zero in view of Lemma 7.1. By Cramer's rule, $a_i = \frac{\det P_i}{\det P}$ where P_i is the matrix obtained from P by replacing the entries of the ith column by $b_1, b_2, \ldots, b_n$ respectively. Since all entries of P_i are in $\mathcal{O}$, it follows that $\det P_i \in \mathcal{O}$, which proves that $\alpha = \sum_i a_i w_i$ belongs to $\frac{1}{d} \sum_i \mathcal{O} w_i$ as desired. □

The next lemma is a crucial step towards the proof of Theorem 7.12.

Lemma 7.20 *Let K'/K be an extension of algebraic number fields of degree n. Given a non-zero prime ideal $\wp$ of $\mathcal{O}'$, there exists an element $\theta \in \mathcal{O}'$ such that the following properties are satisfied:*

(i) *the element $\wp + \theta$ generates the multiplicative group of non-zero elements of $\mathcal{O}'/\wp$.*
(ii) $\theta^{N(\wp)} - \theta \not\equiv 0 \pmod{\wp^2}$.
(iii) *If $\mathfrak{p} = \wp \cap \mathcal{O}$ and $\mathfrak{p}\mathcal{O}' = \wp^e A'$ with $\wp$ not dividing the ideal A' of $\mathcal{O}'$, then* $\theta \equiv 0 \pmod{A'}$.
(iv) $K' = K(\theta)$.
(v) $\wp^s + \mathcal{O}[\theta] = \mathcal{O}' \ \forall\, s \geq 0$.

Proof If θ satisfies (i), then on replacing it if necessary by $\theta + \pi$, $\pi \in \wp \backslash \wp^2$, we can assume that θ satisfies (i) and (ii), because

$$(\theta+\pi)^{N(\wp)} - (\theta+\pi) = (\theta^{N(\wp)} - \theta) + \binom{N(\wp)}{1}\theta^{N(\wp)-1}\pi + \binom{N(\wp)}{2}\theta^{N(\wp)-2}\pi^2 + \cdots + \pi^{N(\wp)} - \pi$$

and every term on the right hand side of the above equation except the last term would be divisible by $\wp^2$ in case θ does not satisfy (ii). By Chinese remainder theorem, there exists $\xi \in \mathcal{O}'$ such that $\xi \equiv \theta \pmod{\wp^2}$ and $\xi \equiv 0 \pmod{A'}$. Since θ satisfies (i), (ii), clearly ξ satisfies (i), (ii) and (iii).

There exists an algebraic integer $\eta \in K'$ such that $K' = K(\xi, \eta)$. Let l and m denote respectively the degrees $[K(\xi) : K]$ and $[K' : K(\xi)]$. Let $\xi^{(1)} = \xi, \ldots, \xi^{(l)}$ denote K-conjugates of ξ and $\eta^{(1)} = \eta, \ldots, \eta^{(m)}$ denote $K(\xi)$-conjugates of η. Let $p \in \wp$ be the rational prime. By Lemma 6.2, $A' \cap \mathbb{Z}$ is non-zero and hence infinite. So we can choose $a \in A' \cap \mathbb{Z}$ such that all elements ξ_{ij} defined by $\xi_{ij} = \xi^{(i)} + ap^2\eta^{(j)}$ are distinct. Thus the element $\xi_{11} = \xi + ap^2\eta$ has lm different K-conjugates namely ξ_{ij}, $1 \leq i \leq l$, $1 \leq j \leq m$. Therefore $K' = K(\xi_{11})$. Since ξ satisfies (i), (ii), (iii), so ξ_{11} satisfies (i), (ii), (iii) and (iv). From now on, we denote ξ_{11} by θ and we show that θ satisfies (v).

Assertion (v) will be proved by induction on s. We first prove it for $s = 1$. Let α be any element of $\mathcal{O}'$ with $\alpha \notin \wp$. Since $(\mathcal{O}'/\wp)^\times$ is generated by $\wp + \theta$, there exists an integer $r \geq 0$ such that $\wp + \theta^r = \wp + \alpha$, which implies $\alpha = \theta^r + \beta$ where $\beta \in \wp$. So we have shown that

$$\mathcal{O}' = \mathcal{O}[\theta] + \wp.$$

Therefore (v) is proved for $s = 1$. Suppose by induction $\mathcal{O}' = \mathcal{O}[\theta] + \wp^s$. We prove the result for $s + 1$. Denote $\theta^{N(\wp)} - \theta$ by $H(\theta)$. Recall that $H(\theta)$ is not divisible by $\wp^2$. So

$$\wp^s = \gcd(H(\theta)^s, \wp^{s+1}) = H(\theta)^s\mathcal{O}' + \wp^{s+1}.$$

Using the above equation together with the induction hypothesis, we have

$$\mathcal{O}' = \mathcal{O}[\theta] + \wp^s = \mathcal{O}[\theta] + H(\theta)^s\mathcal{O}' + \wp^{s+1}.$$

Replacing $\mathcal{O}'$ by $\mathcal{O}[\theta] + \wp$ in the right hand side of the above equation, we see that $\mathcal{O}' = \mathcal{O}[\theta] + \wp^{s+1}$ which proves assertion (v) of the lemma. □

Lemma 7.21 *Let K'/K be an extension of algebraic number fields of degree n and $\wp$ be a non-zero prime ideal of $\mathcal{O}'$ with $\mathfrak{p}$ the prime ideal of $\mathcal{O}$ lying below $\wp$. Let θ be an algebraic integer such that the properties* (i) - (v) *of Lemma 7.20 are satisfied. If $\langle D_{K'/K}(1, \theta, \ldots, \theta^{n-1})\rangle = \mathfrak{p}^l B$ with $\mathfrak{p}$ not dividing the ideal B of $\mathcal{O}$ and $l \geq 0$, then there exists $\beta \in \mathcal{O}\backslash\mathfrak{p}$ such that $\beta\theta^l\mathcal{O}' \subseteq \mathcal{O}[\theta]$.*

Proof We denote $D_{K'/K}(1, \theta, \ldots, \theta^{n-1})$ by $D_{K'/K}(\theta)$. Claim is that any element $\beta \in B \setminus \mathfrak{p}$ works, i.e., $\beta\theta^l\mathcal{O}' \subseteq \mathcal{O}[\theta]$.

Let w be an element of $\mathcal{O}'$. Since θ satisfies property (v) for $s = le$ with e as in Lemma 7.20, there exists $h(\theta) \in \mathcal{O}[\theta]$ such that $w - h(\theta) \equiv 0 \pmod{\wp^{le}}$. Denote $w - h(\theta)$ by w^*. Note that $w^*\theta^l$ is divisible by $\wp^{le}A'^l$ where A' is as in Lemma 7.20. But $\wp^{le}A'^l = \mathfrak{p}^l\mathcal{O}'$. Therefore $\beta w^*\theta^l$ is divisible by $\mathfrak{p}^l B\mathcal{O}' = D_{K'/K}(\theta)\mathcal{O}'$. So $\dfrac{\beta w^*\theta^l}{D_{K'/K}(\theta)}$ is an algebraic integer. In view of Lemma 7.19 applied to the basis $\{1, \theta, \ldots, \theta^{n-1}\}$, we see that $\dfrac{\beta w^*\theta^l}{D_{K'/K}(\theta)}$ belongs to $\dfrac{1}{D_{K'/K}(\theta)}\mathcal{O}[\theta]$. Hence $\beta w^*\theta^l = g(\theta)$ (say) belongs to $\mathcal{O}[\theta]$. So it follows that $\beta[w - h(\theta)]\theta^l = g(\theta)$. Consequently $\beta w\theta^l \in \mathcal{O}[\theta]$. This proves the claim and hence the lemma. □

Proof of Theorem 7.12. Let $\theta \in \mathcal{O}'$. If $K(\theta) \neq K'$, then $\delta_{K'/K}(\theta) = 0$ and we have $\delta_{K'/K}(\theta) \in \Delta_{K'/K}$. Assume that $K' = K(\theta)$, then $\delta_{K'/K}(\theta) = F'(\theta)$ where $F(X)$ is minimal polynomial of θ over K. Keeping in mind that $F'(\theta)\mathcal{O}[\theta]^* = \mathcal{O}[\theta]$ by virtue of Proposition 7.16, we see that

$$F'(\theta)(\Delta_{K'/K})^{-1} = F'(\theta)\mathcal{O}'^* \subseteq F'(\theta)\mathcal{O}[\theta]^* = \mathcal{O}[\theta] \subseteq \mathcal{O}';$$

consequently $F'(\theta) \subseteq \Delta_{K'/K}$. Thus if I' denotes the ideal generated by the set $\{\, \delta_{K'/K}(\theta) \mid \theta \in \mathcal{O}' \,\}$, then we have shown that

$$I' \subseteq \Delta_{K'/K}. \tag{7.6}$$

Claim is that for any non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}'$, there exists $\theta \in \mathcal{O}'$ such that $\mathfrak{P} \nmid \delta_{K'/K}(\theta)\Delta_{K'/K}^{-1}$; consequently $\mathfrak{P}$ will not divide the bigger integral ideal $I'\Delta_{K'/K}^{-1}$. Since this holds for all prime ideals $\mathfrak{P}$, we shall conclude that $I'\Delta_{K'/K}^{-1}$ is the unit ideal, i.e., equality holds in (7.6) as desired.

To prove the claim, let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}'$ and $\mathfrak{p}$ be the prime ideal of $\mathcal{O}$ lying below $\mathfrak{P}$. Then there exists $\theta \in \mathcal{O}'$ such that the properties (i) - (v) of Lemma 7.20 are satisfied. As in the above lemma we denote $D_{K'/K}(1, \theta, \ldots, \theta^{n-1})$ by $D_{K'/K}(\theta)$. Write

$$D_{K'/K}(\theta)\mathcal{O} = \mathfrak{p}^l B, \ \mathfrak{p} \nmid B, \quad l \geq 0.$$

By Lemma 7.21, there exists $\beta \in \mathcal{O}\backslash\mathfrak{p}$ such that $\beta\theta^l\mathcal{O}' \subseteq \mathcal{O}[\theta]$. Denote $\beta\theta^l\mathcal{O}'$ by B'. Now $B' \subseteq \mathcal{O}[\theta]$, which implies that $B'^* \supseteq \mathcal{O}[\theta]^*$. Recall that $\mathcal{O}[\theta]^* = \frac{1}{F'(\theta)}\mathcal{O}[\theta]$ in view of Proposition 7.16. So $B'^* \supseteq \frac{1}{F'(\theta)}\mathcal{O}[\theta]$. But by Proposition 7.2, B'^* is an $\mathcal{O}'$-module. Hence $B'^* \supseteq \frac{\mathcal{O}'}{F'(\theta)}$. Therefore for all $b' \in B'$, we have $Tr_{K'/K}(\frac{b'\mathcal{O}'}{F'(\theta)}) \subseteq \mathcal{O}$ which implies that $\frac{B'}{F'(\theta)} \subseteq \mathcal{O}'^*$, i.e., $B' \subseteq F'(\theta)\Delta_{K'/K}^{-1}$. Recall that β does not belong to $\mathfrak{p}$ and hence $\mathfrak{P}$ is coprime with $\beta\mathcal{O}'$. Also $\mathfrak{P} \nmid \theta$. So $\mathfrak{P} \nmid B'$ and consequently $\mathfrak{P} \nmid F'(\theta)(\Delta_{K'/K}^{-1})$ in view of the fact that $B' \subseteq F'(\theta)\Delta_{K'/K}^{-1}$. This proves the claim and hence the theorem. □

7.4 Dedekind's Theorem on Ramified Primes

Using the results of the previous section, we shall prove a well known theorem by Dedekind in this section.

Theorem 7.22 *Let K'/K be an extension of algebraic number fields. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}'$ and $\mathfrak{p}$ be the prime ideal of $\mathcal{O}$ lying below $\mathfrak{P}$. If $\mathfrak{p}\mathcal{O}' = \mathfrak{P}^e A'$, $\mathfrak{P} \nmid A'$ and if $e \not\equiv 0 \pmod{\mathfrak{P}}$, then $\mathfrak{P}^e$ does not divide $\Delta_{K'/K}$.*

Proof Choose an element $a \in \mathfrak{p} \setminus \mathfrak{p}^2$. There exists an ideal A such that $A\mathfrak{p} = \langle a \rangle$ and $\mathfrak{p} \nmid A$. Choose $g \in A \setminus \mathfrak{p}$, then $\langle g \rangle = AB_1$ for some ideal B_1 of $\mathcal{O}$ not divisible by $\mathfrak{p}$. For the given prime ideal $\mathfrak{P}$ of $\mathcal{O}'$, there exists an algebraic integer θ such that the properties (i) - (v) of Lemma 7.20 are satisfied. Let $F(X)$ be the minimal polynomial of θ over K. Then $F(X) \in \mathcal{O}[X]$ in view of Lemma 1.11. Write

$$D_{K'/K}(1, \theta, \theta^2, \ldots, \theta^{n-1})\mathcal{O} = \mathfrak{p}^l B, \ \mathfrak{p} \nmid B, \ l \geq 0.$$

Consider $w = \dfrac{(\theta^{N(\mathfrak{P})} - \theta)^e}{a} g$. Note that $w \in \mathcal{O}'$, because keeping in mind that $\theta \equiv 0 \pmod{A'}$ and $\theta^{N(\mathfrak{P})} - \theta \equiv 0 \pmod{\mathfrak{P}}$, we see that

$$w\mathcal{O}' = (\theta^{N(\mathfrak{P})} - \theta)^e a^{-1} g\mathcal{O}' = (\theta^{N(\mathfrak{P})} - \theta)^e \mathfrak{P}^{-e} A'^{-1} B_1 \mathcal{O}' \subseteq \mathcal{O}'.$$

By Lemma 7.21, there exists $\beta \in \mathcal{O} \setminus \mathfrak{p}$ such that $\beta\theta^l w \in \mathcal{O}[\theta]$, say $\beta\theta^l w = h(\theta)$. So we have

$$\beta g\theta^l(\theta^{N(\mathfrak{P})} - \theta)^e - ah(\theta) = 0.$$

But $F(X)$ is minimal polynomial of θ over K. So there exists $G(X) \in \mathcal{O}[X]$ such that

$$\beta g X^l (X^{N(\mathfrak{P})} - X)^e - ah(X) = F(X)G(X).$$

Differentiating both sides of the last equation with respect to X and then substituting $X = \theta$, we obtain

$$\beta gl\theta^{l-1}(\theta^{N(\mathfrak{P})} - \theta)^e + \beta g\theta^l e(\theta^{N(\mathfrak{P})} - \theta)^{e-1}(N(\mathfrak{P})\theta^{N(\mathfrak{P})-1} - 1) - ah'(\theta) = F'(\theta)G(\theta).$$

Hence

$$F'(\theta)G(\theta) \equiv \beta g\theta^l e(\theta^{N(\mathfrak{P})} - \theta)^{e-1}(N(\mathfrak{P})\theta^{N(\mathfrak{P})-1} - 1) \pmod{\mathfrak{P}^e}.$$

Since none of g, β, θ, e is divisible by $\mathfrak{P}$ and $< N(\mathfrak{P})\theta^{N(\mathfrak{P})-1} - 1 >$ is also coprime to $\mathfrak{P}$, we see that $F'(\theta)G(\theta) \not\equiv 0 \pmod{\mathfrak{P}^e}$ which implies that $F'(\theta) \not\equiv 0 \pmod{\mathfrak{P}^e}$. Since $F'(\theta) \in \Delta_{K'/K}$ in view of Eq. (7.6), so we conclude that $\Delta_{K'/K} \not\equiv 0 \pmod{\mathfrak{P}^e}$. This completes the proof of the theorem. □

It may be pointed out that the converse of Theorem 7.22 also holds, i.e., if K, K', $\mathfrak{p}$, $\mathfrak{P}$ and $\mathcal{O}$ are as in the theorem and if $e \equiv 0 \pmod{\mathfrak{P}}$, then $\mathfrak{P}^e$ divides $\Delta_{K'/K}$ (for proof see [Nar, Corollary 2 to Proposition 6.2]). Note that Theorem 7.22 immediately yields the following corollary.

Corollary 7.23 *Let K'/K be an extension of algebraic number fields and $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}'$. If $\mathfrak{P}$ is unramified in K'/K, then $\mathfrak{P}$ does not divide $\Delta_{K'/K}$.*

The corollary stated below will be quickly deduced from Corollary 7.23.

Corollary 7.24 *Let K'/K be as above and $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}$. If $\mathfrak{p}$ is unramified in K', then $\mathfrak{p}$ does not divide $d_{K'/K}$.*

Proof Since $\mathfrak{p}$ is unramified in K'/K. So $\mathfrak{p}\mathcal{O}' = \mathfrak{P}_1 \ldots \mathfrak{P}_g$, where $\mathfrak{P}_i$ are distinct prime ideals. In view of Proposition 6.13, $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$ are only prime ideals of $\mathcal{O}'$ whose relative norm is divisible by $\mathfrak{p}$. By the above corollary, $\mathfrak{P}_i$ does not divide $\Delta_{K'/K}$ for any i. So $\mathfrak{p}$ does not divide $N_{K'/K}(\Delta_{K'/K}) = d_{K'/K}$. □

The converse of each of Corollaries 7.23, 7.24 is true which can be easily deduced from Theorem 7.25 to be proved soon.

Theorem 7.25 *Let K'/K be an extension of algebraic number fields. Let $\mathfrak{P}$ be a non-zero prime ideal of $\mathcal{O}'$ and $\mathfrak{p}$ be the prime ideal of $\mathcal{O}$ lying below $\mathfrak{P}$. If e is the index of ramification of $\mathfrak{P}/\mathfrak{p}$, then $\mathfrak{P}^{e-1}$ divides $\Delta_{K'/K}$.*

It may be pointed out that Theorems 7.22, 7.25 were first proved by Dedekind in 1882. The following results which are immediate consequences of these two theorems are known as "Different Theorem" and "Discriminant Theorem".

Theorem 7.26 (Dedekind.) *Let K'/K be an extension of algebraic number fields. The following hold :*

(i) Different theorem. *A non-zero prime ideal $\mathfrak{P}$ of $\mathcal{O}'$ is ramified in K'/K if and only if $\mathfrak{P}$ divides $\Delta_{K'/K}$.*

(ii) Discriminant theorem. *A non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}$ is ramified in K'/K if and only if $\mathfrak{p}$ divides $d_{K'/K}$.*

Proof (Proof of Theorem 7.25.) Write $\mathfrak{p}\mathcal{O}' = \mathfrak{P}^e A'$ where $\mathfrak{P}$ does not divide the ideal A' of $\mathcal{O}'$. It is obvious that

$$\begin{aligned}
\mathfrak{P}^{e-1} \supseteq \Delta_{K'/K} &\iff \mathfrak{P}^{-e+1} \subseteq \Delta_{K'/K}^{-1} = \mathcal{O}'^{*} \\
&\iff \mathfrak{p}^{-1}\mathcal{O}'A'\mathfrak{P} \subseteq \mathcal{O}'^{*} \\
&\iff Tr_{K'/K}(\mathfrak{p}^{-1}\mathcal{O}'A'\mathfrak{P}) \subseteq \mathcal{O} \\
&\iff Tr_{K'/K}(A'\mathfrak{P}) \subseteq \mathfrak{p}.
\end{aligned}$$

So it is enough to prove that if $\alpha \in A'\mathfrak{P}$, then $Tr_{K'/K}(\alpha) \in \mathfrak{p}$. Let $\sigma_1, \ldots, \sigma_n$ be all the K-isomorphism of K' into a finite Galois extension K'' of K containing K' and $\mathcal{O}''$ denote the ring of algebraic integers of K''. Let α be an element of $A'\mathfrak{P}$ which implies that $\alpha^e \in \mathfrak{P}^e A'^e = \mathfrak{p}\mathcal{O}'A'^{e-1} \subseteq \mathfrak{p}\mathcal{O}'$. So $\sigma_i(\alpha)^e \in \mathfrak{p}\mathcal{O}''$ for $1 \leq i \leq n$. Therefore we conclude that

$$[Tr_{K'/K}(\alpha)]^{ne} = [\sigma_1(\alpha) + \cdots + \sigma_n(\alpha)]^{ne}$$

belongs to $\mathfrak{p}\mathcal{O}'' \cap K = \mathfrak{p}$, because $[\sigma_1(\alpha) + \cdots + \sigma_n(\alpha)]^{ne} = \sum \sigma_1(\alpha)^{j_1} \cdots \sigma_n(\alpha)^{j_n}$ where the summation runs over tuples $(j_1, \ldots, j_n)$ of non-negative integers with $j_1 + \cdots + j_n = ne$ and hence at least one index j_i is greater than or equal to e. Since $\mathfrak{p}$ is a prime ideal of $\mathcal{O}$, it follows that $Tr_{K'/K}(\alpha) \in \mathfrak{p}$ as desired. □

Example 7.27 Let $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive (p^r)th root of unity, p an odd prime. We compute the discriminant of the extension $K_0/\mathbb{Q}$. By Theorems 4.13 and 4.15, p is the only prime which is ramified in $K = \mathbb{Q}(\zeta)$, moreover it is totally ramified in K. Let $\mathfrak{p}$, $\mathfrak{P}$ denote respectively the prime ideals of $\mathcal{O}_{K_0}$, $\mathcal{O}_K$ lying over p. Then $e_{K_0/\mathbb{Q}}(\mathfrak{p}) = \phi(p^r)/2$ and $e_{K/K_0}(\mathfrak{P}) = 2$. Keeping in mind p is an odd prime, it follows from Theorems 7.22, 7.25 that $\Delta_{K/K_0} = \mathfrak{P}$ and hence

$d_{K/K_0} = \mathfrak{p}$; consequently $N_{K_0/\mathbb{Q}}(d_{K/K_0}) = p\mathbb{Z}$. Recall that by Theorem 2.26, $|d_K| = p^{r\phi(p^r)-p^{r-1}}$. Therefore in view of Theorem 7.8, $d_{K/\mathbb{Q}}$ is the ideal of $\mathbb{Z}$ generated by $p^{r\phi(p^r)-p^{r-1}}$. Applying Corollary 7.10, we now conclude that $d_{K_0/\mathbb{Q}}$ is the ideal of $\mathbb{Z}$ generated by p^d, where $d = (r\phi(p^r) - p^{r-1} - 1)/2$. Since all isomorphisms of K_0 are real, it follows from Stickelberger's theorem that $d_{K_0} = p^d$, where $d = (r\phi(p^r) - p^{r-1} - 1)/2$.

Example 7.28 Let p, q be distinct primes both congruent to 1 modulo 4 and $K = \mathbb{Q}(\sqrt{pq})$. We show that $K' = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ is an unramified extension of K. Since K' is the composite of two quadratic fields with coprime discriminants, it follows from Corollary 2.30 that $d_{K'} = p^2q^2$. Keeping in mind Theorem 7.8 and Corollary 7.10, we see that $d_{K'/K}$ is the unit ideal. Hence by Theorem 7.26 (Discriminant Theorem), K' is an unramified extension of K.

It is shown below that the above example can be extended to all quadratic fields.

Example 7.29 Let D be the discriminant of a quadratic field $K = \mathbb{Q}(\sqrt{D})$. Let u be a discriminantal divisor of D (as defined in Exercise 20 of Chap. 2) such that $u \neq 1, D$. We show that $K' = \mathbb{Q}(\sqrt{u}, \sqrt{D})$ is an unramified extension of K. Since K' is the composite of two quadratic fields $\mathbb{Q}(\sqrt{u})$, $\mathbb{Q}(\sqrt{D/u})$ with coprime discriminants, it follows from Corollary 2.30 that $d_{K'} = u^2(D/u)^2 = D^2$. Applying Theorem 7.8 and Corollary 7.10, we see that $d_{K'/K}$ is the unit ideal and hence by Theorem 7.26, K'/K is an unramified extension. It may be pointed out that the converse of the above result is also true, i.e., every quadratic unramified extension of a quadratic field $\mathbb{Q}(\sqrt{D})$ with discriminant D is of the type $\mathbb{Q}(\sqrt{u}, \sqrt{D})$, where u is a discriminantal divisor of D. For proof see [Go-Lu].

Exercises

1. Calculate the different of the extension $K/\mathbb{Q}$, where

   (i) $K = \mathbb{Q}(\sqrt{13})$;
   (ii) $K = \mathbb{Q}(\sqrt[3]{2})$;
   (iii) $K = \mathbb{Q}(e^{\frac{2\pi i}{5}})$.

   Check that $N(\Delta_{K/\mathbb{Q}}) = |d_K|$ in each case.
2. Let K'/K be an extension of algebraic number fields. Prove that $d_{K'}$ is divisible by $d_K{}^{[K':K]}$. Give a necessary and sufficient condition when these two integers are equal in absolute value.
3. Let K be an algebraic number field with squarefree discriminant. Then prove that there is no intermediate field between $\mathbb{Q}$ and K.
4. Let K'/K be an extension of algebraic number fields of degree n. Let $\{\beta_1, \ldots, \beta_n\}$ be a vector space basis of K'/K consisting of algebraic integers. Let $\{\beta_1^*, \ldots, \beta_n^*\}$ be dual basis of $\{\beta_1, \ldots, \beta_n\}$. Prove that $D_{K'/K}(\beta_1, \ldots, \beta_n) D_{K'/K}(\beta_1^*, \ldots, \beta_n^*) = 1$.

5. Let K be an algebraic number field. Prove that the cardinality of $(\mathcal{O}_K)^*/\mathcal{O}_K$ is equal to the absolute value of the discriminant of K.
6. If $\{1, \theta, \ldots, \theta^{n-1}\}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_{K'}$ and $F(X)$ is the minimal polynomial of θ over K, then what is the relative different and the relative discriminant of the extension K'/K ? Give a brief justification of your answer.
7. Let $K = \mathbb{Q}(\zeta)$ where ζ be a primitive pth root of unity, p an odd prime. Prove that $\Delta_{K/\mathbb{Q}} = \langle (1-\zeta) \rangle^{p-2}$.
8. Let $K = \mathbb{Q}(\zeta)$ where ζ be a primitive (p^r)th root of unity, p any prime (odd or even), $p^r \geq 3$. Compute $\Delta_{K/\mathbb{Q}}$.
9. Prove that $K = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ is an unramified extension of $\mathbb{Q}(\sqrt{-6})$.
10. Suppose that an algebraic number field K contains a primitive mth root of unity. Prove that m divides $2d_K$.
11. Let K'/K be an extension of algebraic number fields and let σ be a K-isomorphism from K' into $\mathbb{C}$. Prove that $d_{K'/K} = d_{\sigma(K')/K}$.
12. Let K_1/K, K_2/K be extensions of algebraic number fields and L be the compositum of K_1, K_2. Prove that the sets of prime ideals dividing $d_{L/K}$ and $d_{K_1/K} d_{K_2/K}$ coincide.
13. Let K_1/K, K_2/K be extensions of algebraic number fields and L be the compositum of K_1, K_2. Prove that a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L/K if and only if it is unramified in K_1/K and in K_2/K.
14. Let K'/K be an extension of algebraic number fields. If a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in K', then prove that $\mathfrak{p}$ is unramified in the smallest normal extension of K containing K'.

Chapter 8
Class Group and Class Number

The fundamental notion of class group of an algebraic number field K has been defined in Sect. 6.3. The order of this group is called the class number of K. One of its basic property is that the class number of K is 1 if and only if $\mathcal{O}_K$ is a unique factorisation domain. In some sense, the class number of K is a measure of how far $\mathcal{O}_K$ is from being a unique factorisation domain. The larger the class group of K, the more $\mathcal{O}_K$ fails to be a unique factorisation domain.

In this chapter, we shall prove that the class number of an algebraic number field is finite.[1] We shall also prove Minkowski's convex body theorem and use it to describe a method to compute the class number of algebraic number fields having small discriminants. This will also be applied to prove Hermite's theorem which asserts that only finitely many algebraic number fields can have the same discriminant. In the last section, we prove the first case of Fermat's Last Theorem for regular primes.

8.1 Finiteness of Class Number

Definition. Let K be an algebraic number field. Let $G(K)$ denote the group of all non-zero fractional ideals of K and $P(K)$ the subgroup of all non-zero principal fractional ideals of K. The group $G(K)/P(K)$ is called the class group or the ideal class group of K and its order is called the class number of K. It will be shown that $G(K)/P(K)$ is a finite group. A member of $G(K)/P(K)$ is called an ideal class of K.

In this section, we prove.

[1] The finiteness of class number for all algebraic number fields was first proved by Dedekind in 1871 in his account of ideal theory.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_8

Theorem 8.1 *The group of ideal classes of an algebraic number field is finite.*

We shall first prove the following theorem from which the above theorem will be deduced.

Theorem 8.2 *Let K be an algebraic number field different from $\mathbb{Q}$. Then in every ideal class of K, there exists an integral ideal B of $\mathcal{O}_K$ such that $N(B) < \sqrt{|d_K|}$.*

Proof Let $\mathcal{C}$ be any ideal class of K and C be a fixed ideal belonging to $\mathcal{C}$. Since C^{-1} is a fractional ideal, there exists a non-zero element β of $\mathcal{O}_K$ such that $\beta C^{-1} \subseteq \mathcal{O}_K$. Then $A = \beta C^{-1}$ is an integral ideal of $\mathcal{O}_K$ such that AC is a principal ideal. Fix a $\mathbb{Z}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of A. Let $\sigma_1, \ldots, \sigma_{r_1}$ be all the real isomorphisms of K and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be the non-real isomorphisms of K which are arranged such that $\overline{\sigma}_{r_1+j} = \sigma_{r_1+r_2+j}$ for $1 \leq j \leq r_2$.

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

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

The absolute value of the determinant of these linear forms is

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

which in view of Theorem 2.15 equals $[\mathcal{O}_K : A]\sqrt{|d_K|}$. Define constants c_i by

$$c_i = \left([\mathcal{O}_K : A]\sqrt{|d_K|}\right)^{\frac{1}{n}} \quad \text{for } 1 \leq i \leq n. \tag{8.1}$$

Applying modified Minkowski's lemma on complex linear forms (proved in Sect. 5.2) to these linear forms $L_1, L_2, \ldots, L_n$ with constants $c_1, c_2, \ldots, c_n$, we see that there exist rational integers $u_1, u_2, \ldots, u_n$ not all zero such that

$$|L_i(u_1, u_2, \ldots, u_n)| < c_i \quad \text{for } 1 \leq i \leq n-1 \tag{8.2}$$

and

$$|L_n(u_1, u_2, \ldots, u_n)| \leq c_n. \tag{8.3}$$

Consider the element $\alpha = u_1\alpha_1 + \cdots + u_n\alpha_n$ belonging to A, then $\alpha \neq 0$. It follows from (8.2), (8.3) that $|\sigma_i(\alpha)| < c_i$ for $1 \leq i \leq n-1$ and $|\sigma_n(\alpha)| \leq c_n$; consequently keeping in mind that $K \neq \mathbb{Q}$ and using (8.1), we have

$$|N_{K/\mathbb{Q}}(\alpha)| < \prod_{i=1}^{n} c_i = [\mathcal{O}_K : A]\sqrt{|d_K|} = N(A)\sqrt{|d_K|}. \tag{8.4}$$

Since $\alpha \in A$, there exists an integral ideal B such that $\alpha\mathcal{O}_K = AB$. On recalling that AC is a principal ideal, we conclude that B and C lie in the same ideal class $\mathcal{C}$.

In view of Proposition 3.34, $|N_{K/\mathbb{Q}}(\alpha)| = N(\alpha\mathcal{O}_K) = N(A)N(B)$. It now follows from (8.4) that $N(B) < \sqrt{|d_K|}$. □

Proof of Theorem 8.1. Observe that for any (integral) ideal A, $N(A) \in A$ because the order of the element $A + 1$ belonging to the finite group $\mathcal{O}_K/A$ divides the order of $\mathcal{O}_K/A$. By Theorem 8.2, in every ideal class of K, there exists an ideal B such that $N(B) < \sqrt{|d_K|}$. Thus $N(B)$ has only finitely many choices and B being a divisor of $N(B)\mathcal{O}_K$ in view of the above observation, has only finitely many choices by virtue of Theorem 3.12. So the number of ideals of $\mathcal{O}_K$ having norm not exceeding $\sqrt{|d_K|}$ is finite and hence the class number of K is finite. □

The following corollary is an immediate consequence of Theorem 8.2.

Corollary 8.3 *For an algebraic number field $K \neq \mathbb{Q}$, $|d_K| > 1$.*

Corollary 8.4 *If $K \neq \mathbb{Q}$ is an algebraic number field, then some rational prime is ramified in K, i.e., there is no unramified extension of degree > 1 of $\mathbb{Q}$.*

Proof By Corollary 8.3, $|d_K| > 1$. So there exists a prime p such that $p \mid d_K$. By the Discriminant Theorem proved in Chapter 7, p is ramified in K. □

It may be pointed out that there exist algebraic number fields that have proper unramified extensions; see Example 7.29.

The corollary stated below is proved using the finiteness of the class number.

Corollary 8.5 *Let K be an algebraic number field with class number h. Let I be a non-zero ideal of $\mathcal{O}_K$ and q be a number coprime with h. If I^q is a principal ideal of $\mathcal{O}_K$, then I is a principal ideal.*

Proof Let u, v be integers such that $uq + vh = 1$. In view of Lagrange's theorem for finite groups, $I^h P(K) = (I P(K))^h = P(K)$. So I^h is a principal ideal. Since I^q is a principal ideal, it follows that $I = (I)^{uq+vh} = (I^q)^u (I^h)^v$ is also principal ideal. □

Theorem 8.2 can be used to compute the class number of algebraic number fields having small degree and small discriminant as is done in following examples.

Example 8.6 We find the class number of $K = \mathbb{Q}(\sqrt{-7})$. Here $d_K = -7$. By Theorem 8.2, in every ideal class of K, there exists an integral ideal B such that $N(B) < \sqrt{7} < 3$. So $N(B) = 1$ or 2. If $N(B) = 1$, then $B = \mathcal{O}_K$ and the ideal class of B is $P(K)$. Now we consider the possibility when $N(B) = 2$. By Theorem 4.11, $2\mathcal{O}_K$ factors as product of two distinct prime ideals, say $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2'$ with $N(\mathfrak{p}_2) = N(\mathfrak{p}_2') = 2$. We first check whether $\mathfrak{p}_2, \mathfrak{p}_2'$ are principal or not. As $\mathfrak{p}_2\mathfrak{p}_2' = \langle 2 \rangle$ is a principal ideal, it follows that $\mathfrak{p}_2$ will be a principal ideal if and only if $\mathfrak{p}_2'$ is principal. Note that $\mathfrak{p}_2$ is principal if and only if there exist a, b in $\mathbb{Z}$ such that $2 = N(\mathfrak{p}_2) = N_{K/\mathbb{Q}}\left(a + \frac{b}{2}(1 + \sqrt{-7})\right)$, i.e., $8 = (2a + b)^2 + 7b^2$, which is possible when $a = 0, b = \pm 1$. We may take $\mathfrak{p}_2 = \frac{1+\sqrt{-7}}{2}\mathcal{O}_K$ and $\mathfrak{p}_2' = \frac{1-\sqrt{-7}}{2}\mathcal{O}_K$. So $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are principal ideals. Thus in every ideal class of K, there lies a principal ideal. Hence $|G(K)/P(K)| = 1$.

Example 8.7 We compute the class number of $K = \mathbb{Q}(\sqrt{-11})$. By Theorem 8.2, in every ideal class of K, there exists an integral ideal B such that $N(B) < \sqrt{11} < 4$. So $N(B) = 1$ or 2 or 3. In view of Theorem 4.11, $2\mathcal{O}_K$ is a prime ideal with $N(2\mathcal{O}_K) = 4$. So there is no integral ideal of norm 2. Now we consider the possibility when $N(B) = 3$. Since $\left(\frac{-11}{3}\right) = 1$, the ideal $3\mathcal{O}_K$ factors as $\mathfrak{p}_3\mathfrak{p}_3'$ with $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$. We now try to see whether $\mathfrak{p}_3$ is a principal ideal or not. Note that $\mathfrak{p}_3$ is principal if and only if there exist $a, b \in \mathbb{Z}$ such that $N_{K/\mathbb{Q}}\left(a + b(\frac{1+\sqrt{-11}}{2})\right) = 3$, i.e., $12 = (2a + b)^2 + 11b^2$. Clearly $a = 0$ and $b = \pm 1$ work. We may take $\mathfrak{p}_3 = \frac{1+\sqrt{-11}}{2}\mathcal{O}_K$ and $\mathfrak{p}_3' = \frac{1-\sqrt{-11}}{2}\mathcal{O}_K$. Thus in every ideal class of $\mathbb{Q}(\sqrt{-11})$, there exists a principal ideal. Hence the class number of K is 1.

Next our aim is to give an improvement of Theorem 8.2. It will be shown that given an algebraic number field K of degree $n = r_1 + 2r_2$, the constant $C_K = \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|d_K|}$ satisfies the property that in every ideal class of K, there exists an integral ideal B with $N(B) \leq C_K$. This bound will be used for computing the class number slightly more quickly. It will be obtained using Minkowski's convex body theorem which will be proved in the next section.

8.2 Minkowski's Convex Body Theorem

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

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

Example 8.8 Let $A = (a_{ij})_{n\times n}$ be a non-singular matrix with entries from $\mathbb{R}$ and $c_1, c_2, \ldots, c_n$ be fixed positive constants. We show that the set

$$P = \{x \in \mathbb{R}^n : |a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n| < c_1, \ldots, |a_{n1}x_1 + \cdots + a_{nn}x_n| < c_n\}$$

is a convex set. To verify this, define linear forms $L_1, L_2, \ldots, L_n$ in $X = (X_1, X_2, \ldots, X_n)$ by $L_i(X) = \sum_{j=1}^{n} a_{ij}X_j$, $1 \leq i \leq n$. Suppose $x, y \in P$ and $\lambda \in \mathbb{R}$ is such that $0 \leq \lambda \leq 1$. We have $|L_i(x)| < c_i$ and $|L_i(y)| < c_i$ for $1 \leq i \leq n$. Now

$$|L_i(\lambda x + (1 - \lambda)y)| = |\lambda L_i(x) + (1 - \lambda)L_i(y)| \leq \lambda|L_i(x)| + (1 - \lambda)|L_i(y)| < c_i$$

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

Definition. By an n-dimensional lattice in $\mathbb{R}^n$, we mean a subgroup of $\mathbb{R}^n$ which is generated as a group by n linearly independent vectors over $\mathbb{R}$. Such a set of

generators is called a basis of the lattice. If $\{A_1, A_2, \ldots, A_n\}$ and $\{B_1, B_2, \ldots, B_n\}$ are two bases of a lattice $\mathfrak{L}$, then there exists an $n \times n$ unimodular matrix U such that

$$\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_n \end{bmatrix} = U \begin{bmatrix} B_1 \\ B_2 \\ \vdots \\ B_n \end{bmatrix}.$$

So the absolute value of the determinant of the matrix with row vectors $A_1, A_2, \ldots, A_n$ is well defined. It is called the determinant of $\mathfrak{L}$. In what follows all lattices under consideration are n-dimensional.

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

Notation. In what follows $\mathrm{vol}(S)$ stands for the volume of subset of $\mathbb{R}^n$ whenever S has a volume.

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

Observe that fundamental parallelepiped T of a lattice $\mathfrak{L}$ is not uniquely determined by $\mathfrak{L}$. However the volume of a fundamental parallelepiped of $\mathfrak{L}$ depends only upon $\mathfrak{L}$ as it equals the determinant of the lattice $\mathfrak{L}$.

Theorem 8.9 (Minkowski's Convex Body Theorem). *Let $\mathfrak{L}$ be an n-dimensional lattice in $\mathbb{R}^n$ with the volume of a fundamental parallelepiped of $\mathfrak{L}$ denoted by Δ. Let S be a bounded, centrally symmetric, convex subset of $\mathbb{R}^n$ such that* $\mathrm{vol}(S) > 2^n\Delta$. *Then S contains at least one non-zero vector of $\mathfrak{L}$.*

For proving the above theorem, we first prove some lemmas.

Lemma 8.10 *Every bounded subset of $\mathbb{R}^n$ contains only finitely many points of a lattice $\mathfrak{L}$.*

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

Lemma 8.11 *If T is a fundamental parallelepiped of an n-dimensional lattice $\mathfrak{L}$, then the sets $T_z = T + z$, where z runs through all the points of $\mathfrak{L}$, are pairwise disjoint and fill the entire space $\mathbb{R}^n$.*

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

Lemma 8.12 *Let $T, \mathfrak{L}$ be as in the above lemma. Then for any given bounded set $S \subseteq \mathbb{R}^n$, there are only finitely many translates T_z, $z \in \mathfrak{L}$, whose intersection with S is non-empty.*

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

$$||u|| \leq \alpha_1||u_1|| + \cdots + \alpha_n||u_n|| < d. \tag{8.5}$$

Since S is bounded, there exists $r > 0$ such that $||x|| \leq r$ for all $x \in S$. Let $z \in \mathfrak{L}$ be such that $T_z \cap S \neq \emptyset$, say $x \in T_z \cap S$. We can write $x = z + u$ with $u \in T$. This implies that $||z|| \leq ||x|| + ||u|| \leq r + d$ by (8.5), which shows that z belongs to a sphere with centre at origin and radius $r + d$. So by Lemma 8.10, there are only finitely many choices for $z \in \mathfrak{L}$. □

Proof of Theorem 8.9. The proof is divided into two steps.

Step 1. In this step, we prove that when a bounded subset Y of $\mathbb{R}^n$ has the property that all of its translates $Y + z$ by vectors of $\mathfrak{L}$ are pairwise disjoint and if the volume of Y exists, then $\text{vol}(Y) \leq \Delta$. Let T be a fundamental parallelepiped of $\mathfrak{L}$. In view of Lemma 8.11, we see that

$$\text{vol}(Y) = \sum_{z \in \mathfrak{L}} \text{vol}(Y \cap T_{-z}); \tag{8.6}$$

the sum on right hand side of above equation contains only a finite number of non-zero terms by virtue of Lemma 8.12. We can rewrite (8.6) as

$$\text{vol}(Y) = \sum_{z \in \mathfrak{L}} \text{vol}((Y + z) \cap T). \tag{8.7}$$

By assumption of Step 1, the translates $Y + z$, $z \in \mathfrak{L}$ are pairwise disjoint. Therefore the sum on the right hand side of (8.7) does not exceed $\text{vol}(T) = \Delta$ and hence the assertion of Step 1 is proved.

Step 2. We now prove the theorem using the assertion of Step 1. Since the volume of S exists, so the volume of $\frac{1}{2}S$ exists and $\text{vol}(\frac{1}{2}S) = \frac{\text{vol}(S)}{2^n} > \Delta$. Therefore in view of Step 1, there exist at least two translations $\frac{1}{2}S + z$, $\frac{1}{2}S + z'$ with $z \neq z'$ in $\mathfrak{L}$ having non-empty intersection. Hence there exist x, x' in S such that $\frac{1}{2}x + z = \frac{1}{2}x' + z'$. So $\frac{1}{2}(x - x') = z' - z$ belongs to $\mathfrak{L}$. Since S is centrally symmetric, $-x' \in S$. Also S being convex, we see that $\frac{1}{2}(x - x')$ belongs to S. Consequently S contains a non-zero vector of $\mathfrak{L}$. □

Theorem 8.13 (Modified Minkowski's Convex Body Theorem). *Let $\mathfrak{L}$ be an n-dimensional lattice in $\mathbb{R}^n$ with determinant Δ. Let S be a bounded, centrally symmetric, convex subset of $\mathbb{R}^n$ with volume $2^n\Delta$. Then the closure[2] of S contains a non-zero vector of $\mathfrak{L}$.*

Proof Let S^c denote the closure of S with respect to the usual metric on $\mathbb{R}^n$. For $y \in \mathbb{R}^n$, let $d(y, S)$ denote the distance of y from S defined by

$$d(y, S) = inf\{||y - x|| \mid x \in S\}.$$

Suppose to the contrary S^c does not contain any non-zero vector of $\mathfrak{L}$. Let r be a positive real number such that $||x|| < r$ for all $x \in S$. Fix any $\epsilon > 0$. Consider the set $(1+\epsilon)S$. Since $\text{vol}((1+\epsilon)S) = (1+\epsilon)^n \text{ vol}(S) > 2^n\Delta$, it follows that $(1+\epsilon)S$ contains a non-zero vector of $\mathfrak{L}$ by Theorem 8.9; moreover $(1+\epsilon)S$ being bounded can contain only finitely many points of $\mathfrak{L}$ in view of Lemma 8.10. Denote the zero vector in $\mathbb{R}^n$ by $\underline{0}$ and write

$$(\mathfrak{L} \setminus \{\underline{0}\}) \cap (1+\epsilon)S = \{y_1, y_2, \ldots, y_k\}. \tag{8.8}$$

As $y_i \notin S^c$ in view of our assumption, it follows that the distance $d(y_i, S) > 0$. So there exist $\epsilon_0 > 0$ such that

$$d(y_i, S) > \epsilon_0 \text{ for } 1 \le i \le k. \tag{8.9}$$

Choose $\epsilon_1 > 0$ such that $\epsilon_1 < \epsilon$ and $\epsilon_1 < \frac{\epsilon_0}{r}$. Then $(1+\epsilon_1)S \subseteq (1+\epsilon)S$ in view of the fact that $\lambda S \subseteq S$ for $0 < \lambda < 1$, which can be verified keeping in mind that S is convex and $\underline{0} \in S$. In view of Theorem 8.9, $(\mathfrak{L} \setminus \{\underline{0}\}) \cap (1+\epsilon_1)S \neq \emptyset$ and it is a subset of $\{y_1, y_2, \ldots, y_k\}$ by (8.8). So there exists i such that $y_i = (1+\epsilon_1)x$ for some $x \in S$. Then $d(y_i, x) = d((1+\epsilon_1)x, x) = \epsilon_1||x|| \le \epsilon_1 r < \epsilon_0$ which contradicts (8.9). This contradiction proves the theorem.

□

It may be pointed out that Minkowski's lemma on real linear forms proved in Sect. 5.2 is a quick application of Minkowski's convex body theorem. In fact we take $\mathfrak{L}$ to be the integral lattice. With notations as in the lemma, if S is the subset of $\mathbb{R}^n$ defined by $S = \left\{ x \ : \ \left| \sum_{j=1}^{n} a_{ij}x_j \right| < c_i \ \textit{for} \ 1 \le i \le n \right\}$, then S is a bounded, centrally symmetric, convex set having volume $\frac{2^n c_1 \cdots c_n}{|\det A|} > 2^n$. Hence S contains a non-zero vector of $\mathbb{Z}^n$.

[2] The closure is with respect to the usual metric on $\mathbb{R}^n$ defined by $d(x, y) = ||x - y||$.

8.3 Minkowski's Bound

We now give an improvement of Theorem 8.2.

Theorem 8.14 *Let K be an algebraic number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real isomorphisms of K and $2r_2$ is the number of non-real isomorphisms of K. Then in every ideal class of K, there exists an integral ideal B such that*

$$N(B) \leq \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} \sqrt{|d_K|}.$$

It is immediate from the above theorem that $\sqrt{|d_K|} \geq \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}$. One can prove by induction on n that $\frac{n^n}{n!} \geq 2^{n-1}$ for $n \geq 2$. Since $r_2 \leq \frac{n}{2}$, it follows that when $K \neq \mathbb{Q}$, then $\sqrt{|d_K|} \geq \left(\frac{\pi}{4}\right)^{r_2} 2^{n-1} \geq \left(\frac{\pi}{4}\right)^{n/2} 2^{n-1} = \frac{1}{2}\pi^{\frac{n}{2}}$. Thus Theorem 8.14 yields the following corollary.

Corollary 8.15 $|d_K| \longrightarrow \infty$ *as* $[K : \mathbb{Q}]$ *approaches* ∞.

For proving Theorem 8.14, we need the following lemmas.

Lemma 8.16 *Let t be a fixed positive real number and r_1, r_2 be non-negative integers with $n = r_1 + 2r_2$. Let X_t be the subset of $\mathbb{R}^n$ consisting of all points $x = (x_1, \ldots, x_{r_1}, y_{r_1+1}, z_{r_1+1}, \ldots, y_{r_1+r_2}, z_{r_1+r_2})$ for which $\sum_{i=1}^{r_1} |x_i| + 2 \sum_{j=r_1+1}^{r_1+r_2} \sqrt{y_j^2 + z_j^2} < t$. Then X_t is a bounded, open, centrally symmetric, convex subset of $\mathbb{R}^n$.*

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

$$Z = \sum_{i=1}^{r_1} |\lambda x_i + (1-\lambda)x_i'| + 2 \sum_{j=r_1+1}^{r_1+r_2} \sqrt{(\lambda y_j + (1-\lambda)y_j')^2 + (\lambda z_j + (1-\lambda)z_j')^2}.$$

Clearly Z is less than or equal to

$$\sum_{i=1}^{r_1} (\lambda|x_i| + (1-\lambda)|x_i'|) + 2 \sum_{j=r_1+1}^{r_1+r_2} \sqrt{\lambda^2(y_j^2 + z_j^2) + (1-\lambda)^2(y_j'^2 + z_j'^2) + 2\lambda(1-\lambda)(y_j y_j' + z_j z_j')}.$$

By Cauchy-Schwarz inequality,

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

Hence

$$\begin{aligned} Z &\le \sum_{i=1}^{r_1} \left(\lambda|x_i| + (1-\lambda)|x_i'|\right) + 2\sum_j \left(\lambda\sqrt{y_j^2+z_j^2} + (1-\lambda)\sqrt{y_j'^2+z_j'^2}\right) \\ &= \lambda\left(\sum_{i=1}^{r_1}|x_i| + 2\sum_j \sqrt{y_j^2+z_j^2}\right) + (1-\lambda)\left(\sum_{i=1}^{r_1}|x_i'| + 2\sum_j \sqrt{y_j'^2+z_j'^2}\right) \\ &< \lambda t + (1-\lambda)t = t. \end{aligned}$$

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

Lemma 8.17 *If X_t is as in Lemma 8.16, then*

$$\mathrm{vol}(X_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!}.$$

This lemma will be proved after proving Theorem 8.14.

Proof of Theorem 8.14. Let $\mathcal{C}$ be any ideal class in K. Let C be a fixed ideal in class $\mathcal{C}$. As in the proof of Theorem 8.2, we can choose a non-zero integral ideal A of $\mathcal{O}_K$ such that AC is a principal ideal. Let $\sigma_1, \ldots, \sigma_{r_1}$ be all the real isomorphisms of K and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be non-real isomorphisms of K arranged so that $\overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j}$, $1 \le j \le r_2$. Consider the homomorphism

$$\Psi : \mathcal{O}_K \longrightarrow \mathbb{R}^n$$

defined by

$$\Psi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), Re(\sigma_{r_1+1}(\alpha)), Im(\sigma_{r_1+1}(\alpha)), \ldots, Im(\sigma_{r_1+r_2}(\alpha))).$$

Clearly Ψ is a homomorphism of additive groups and is 1–1. Then $\Psi(A)$ is a subgroup of $\mathbb{R}^n$. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a $\mathbb{Z}$-basis of A. So $\Psi(\alpha_1), \ldots, \Psi(\alpha_n)$ form a $\mathbb{Z}$-basis of $\Psi(A)$. Therefore $\Psi(A)$ will be a lattice in $\mathbb{R}^n$ once we show that $\Psi(\alpha_1), \ldots, \Psi(\alpha_n)$ form a linearly independent set over $\mathbb{R}$. This is verified if we show that the matrix with row vectors $\Psi(\alpha_1), \ldots, \Psi(\alpha_n)$ has determinant non-zero. The absolute value of the determinant of the matrix will be the determinant of the lattice $\Psi(A)$.

Let D_0 denote the determinant of the matrix P_0 with row vectors $\Psi(\alpha_1), \ldots, \Psi(\alpha_n)$. We write $\sigma_i(\alpha_j) = x_j^{(i)}$, $1 \le i \le r_1$ and $\sigma_{r_1+i}(\alpha_j) = y_j^{(r_1+i)} + \iota z_j^{(r_1+i)}$ for $1 \le i \le r_2$, where ι stands for $\sqrt{-1}$. So we have

$$P_0 = \begin{bmatrix} x_1^{(1)} & \cdots & x_1^{(r_1)} & y_1^{(r_1+1)} & z_1^{(r_1+1)} & \cdots & y_1^{(r_1+r_2)} & z_1^{(r_1+r_2)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n^{(1)} & \cdots & x_n^{(r_1)} & y_n^{(r_1+1)} & z_n^{(r_1+1)} & \cdots & y_n^{(r_1+r_2)} & z_n^{(r_1+r_2)} \end{bmatrix}.$$

To the (r_1+1)th column of P_0 add ι times (r_1+2)th column, then in the new matrix multiply the (r_1+2)th column by -2ι and to it add the (r_1+1)th column. Repeating this process r_2 times with successive pairs of last $2r_2$ columns, we obtain

$$(-2\iota)^{r_2} D_0 = \det \begin{bmatrix} \sigma_1(\alpha_1) & \cdots & \sigma_{r_1}(\alpha_1) & \sigma_{r_1+1}(\alpha_1) & \overline{\sigma_{r_1+1}(\alpha_1)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \sigma_1(\alpha_n) & \cdots & \sigma_{r_1}(\alpha_n) & \sigma_{r_1+1}(\alpha_n) & \overline{\sigma_{r_1+1}(\alpha_n)} & \cdots & \overline{\sigma_{r_1+r_2}(\alpha_n)} \end{bmatrix}.$$

Taking square on both sides of the above equation and using Theorem 2.15, we have

$$(-2\iota)^{2r_2} D_0^2 = D_{K/\mathbb{Q}}(\alpha_1, \ldots, \alpha_n) = d_K [\mathcal{O}_K : A]^2 = d_K N(A)^2.$$

Therefore

$$|D_0| = \frac{\sqrt{|d_K|} N(A)}{2^{r_2}} \neq 0. \tag{8.10}$$

This is the determinant of the lattice $\Psi(A)$. Now we shall choose a real number $t_0 > 0$ in such a way that

$$\mathrm{vol}(X_{t_0}) = 2^n |D_0| = \frac{2^n \sqrt{|d_K|} N(A)}{2^{r_2}}. \tag{8.11}$$

In view of Lemma 8.17, t_0 is chosen such that

$$\mathrm{vol}(X_{t_0}) = 2^{r_1} \left(\frac{\pi}{2}\right)^{r_2} \frac{t_0^n}{n!} = 2^n |D_0| = \frac{2^n \sqrt{|d_K|} N(A)}{2^{r_2}}.$$

Thus

$$t_0^n = \left(\frac{4}{\pi}\right)^{r_2} n! \sqrt{|d_K|} N(A). \tag{8.12}$$

So by Theorem 8.13, there exists a non-zero element $\alpha \in A$ such that the vector $\Psi(\alpha)$ in the lattice $\Psi(A)$ belongs to the closure of X_{t_0}. Hence keeping in mind the definition of X_{t_0}, we see that

$$\sum_{i=1}^{r_1} |\sigma_i(\alpha)| + 2 \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(\alpha)| \leq t_0.$$

In view of Arithmetic Mean-Geometric Mean inequality (proved below), the above inequality yields

$$\left(\prod_{i=1}^{r_1} |\sigma_i(\alpha)| \prod_{j=r_1+1}^{r_1+r_2} |\sigma_j(\alpha)|^2 \right)^{\frac{1}{n}} \leq \frac{\sum_{i=1}^{r_1} |\sigma_i(\alpha)| + 2 \sum_{j=r_1+1}^{r_1+r_2} |\sigma_j(\alpha)|}{n} \leq \frac{t_0}{n}.$$

The above inequality implies by virtue of equation (8.12) that

$$|N_{K/\mathbb{Q}}(\alpha)| \leq \frac{t_0^n}{n^n} = \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}N(A). \tag{8.13}$$

Recall that $\alpha \in A$. So there exists an integral ideal B such that $\alpha\mathcal{O}_K = AB$. Also AC is a principal ideal. Therefore B and C belong to the same ideal class $\mathcal{C}$. By virtue of (8.13),

$$N(A)N(B) = |N_{K/\mathbb{Q}}(\alpha)| \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}N(A).$$

So $N(B) \leq \frac{n!}{n^n}\left(\frac{4}{\pi}\right)^{r_2}\sqrt{|d_K|}$ as desired. □

Arithmetic Mean-Geometric Mean Inequality. If $a_1, \ldots, a_n$ are positive real numbers, then

$$\sqrt[n]{a_1 \cdots a_n} \leq \frac{a_1 + \cdots + a_n}{n}. \tag{8.14}$$

Proof We first prove (8.14) when n is a power of 2. For $n = 2$, the inequality (8.14) is clear because $(\sqrt{a_1} - \sqrt{a_2})^2 \geq 0$. Now we verify it for $n = 4$.

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

Suppose (8.14) is true for $n = 2^{k-1}$. To verify it for $n = 2^k$, we have by induction

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

To prove (8.14) for general n, clearly it is enough to prove that if $b_1, \ldots, b_n$ are positive real numbers such that $\prod_{i=1}^{n} b_i = 1$, then $b_1 + \cdots + b_n \geq n$. This has been proved in above paragraph when n is a power of 2. Let k be such that $n < 2^k$. Set

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

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

Proof of Lemma 8.17. We shall prove that

$$\mathrm{vol}(X_t) = 2^{r_1}\left(\frac{\pi}{2}\right)^{r_2}\frac{t^n}{n!} \tag{8.15}$$

by induction on $r_1 + r_2$. In the case of $r_1 = 1, r_2 = 0$ and $r_1 = 0, r_2 = 1$, the above equality can be easily verified. Assume now that (8.15) holds for $r_1 = a, r_2 = b$, a and b are non-negative integers. Then for $r_1 = a + 1, r_2 = b$, we have

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

Consider now the situation when $r_1 = a, r_2 = b + 1$. Then

$$\mathrm{vol}(X_t) = \frac{2^{a-b}\pi^b}{(a+2b)!}\int\int_{y^2+z^2 \le \frac{t^2}{4}} (t - 2\sqrt{(y^2+z^2)})^{a+2b} dydz.$$

Substituting $y = rcos\theta, z = rsin\theta$, we see that

$$\begin{aligned}\mathrm{vol}(X_t) &= \frac{2^{a-b}\pi^b}{(a+2b)!}\int_0^{2\pi}\int_0^{\frac{t}{2}} (t-2r)^{a+2b} r dr d\theta \\ &= (-1)^{a+2b}\frac{2^{a-b}\pi^b}{(a+2b)!}2\pi\int_0^{\frac{t}{2}} (2r-t)^{a+2b} r dr.\end{aligned}$$

On integrating by parts, we see that

$$\begin{aligned}\mathrm{vol}(X_t) &= (-1)^{a+2b}\frac{2^{a-b}\pi^b}{(a+2b)!}2\pi\left\{\frac{(2r-t)^{a+2b+1}}{2(a+2b+1)}r - \int\frac{(2r-t)^{a+2b+1}}{2(a+2b+1)}dr\right\}\Big|_0^{\frac{t}{2}} \\ &= (-1)^{a+2b}\frac{2^{a-b}\pi^b}{(a+2b)!}2\pi\frac{(-t)^{a+2b+2}}{4(a+2b+1)(a+2b+2)} \\ &= \frac{2^{a-b-1}\pi^{1+b}}{(a+2b+2)!}t^{a+2b+2}.\end{aligned}$$

This proves the formula when $r_1 = a, r_2 = b + 1$ and hence the lemma is proved. □

8.4 Computation of Class Number

In this section, some applications of Theorem 8.14 are given. First we define signature of an algebraic number field K.

Definition. Let K be an algebraic number field of degree $n = r_1 + 2r_2$ having r_1 real isomorphisms and $2r_2$ non-real isomorphisms, then $[r_1, r_2]$ is called the signature of K.

Example 8.18 We compute the class number of $K = \mathbb{Q}(\theta)$, where θ satisfies the polynomial $X^3 - X + 1$. In view of Example 2.19, $d_K = -23$. Since the discriminant is negative, all the isomorphisms of K into $\mathbb{C}$ can't be real. So signature of K is $[1, 1]$. By Theorem 8.14, in every ideal class of K, there exists an (integral)ideal B such that $N(B) \leq \left(\frac{4}{\pi}\right) \frac{3!}{3^3}\sqrt{23} < 2$. So $N(B) = 1$ and hence $B = \mathcal{O}_K$. Therefore there is only one ideal class namely $P(K)$ i.e., the class number of K is one.

Example 8.19 We compute the class number of $K = \mathbb{Q}(\sqrt{10})$. Here $d_K = 40$. By Theorem 8.14, in every ideal class of K, there exists an ideal B such that $N(B) \leq \frac{2!}{2^2}\sqrt{40} < 4$. We first look for ideals of $\mathcal{O}_K$ having norm 2. In view of Theorem 4.11, $2\mathcal{O}_K = \mathfrak{p}_2^2$ with $N(\mathfrak{p}_2) = 2$. We check whether $\mathfrak{p}_2$ is a principal ideal or not. Note that $\mathfrak{p}_2$ is principal if and only if there exist $a, b \in \mathbb{Z}$ such that $2 = N(\mathfrak{p}_2) = |N_{K/\mathbb{Q}}(a + b\sqrt{10})|$ i.e., $\mathfrak{p}_2$ is principal if and only if $a^2 - 10b^2 = \pm 2$ for some $a, b \in \mathbb{Z}$, which is impossible because the congruence $x^2 \equiv \pm 2 \pmod 5$ is not solvable. Next we look for ideals of norm 3. By Theorem 4.11, $3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$ where $\mathfrak{p}_3, \mathfrak{p}_3'$ are distinct prime ideals with $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$. If $\mathfrak{p}_3$ or $\mathfrak{p}_3'$ is principal ideal, then $a^2 - 10b^2 = \pm 3$ for some $a, b \in \mathbb{Z}$ which is again impossible as the congruence $x^2 \equiv \pm 3 \pmod 5$ is not solvable. So $\mathfrak{p}_3$ and $\mathfrak{p}_3'$ are not principal ideals. Keeping in mind that $N_{K/\mathbb{Q}}(2 + \sqrt{10}) = -6$, it follows that $\langle 2 + \sqrt{10}\rangle$ is the product of $\mathfrak{p}_2$ with an ideal of norm 3, say $\langle 2 + \sqrt{10}\rangle = \mathfrak{p}_2\mathfrak{p}_3$. Since $\langle 2 + \sqrt{10}\rangle \neq \langle 2 - \sqrt{10}\rangle$, we see that $\langle 2 - \sqrt{10}\rangle = \mathfrak{p}_2\mathfrak{p}_3'$. So $\mathfrak{p}_3, \mathfrak{p}_3'$ lie in the ideal class of ${\mathfrak{p}_2}^{-1}$ which is same as the ideal class of $\mathfrak{p}_2$. Hence there are only two ideal classes $P(K), \mathfrak{p}_2 P(K)$. Therefore the class number of K is 2.

Example 8.20 We find the class number of $K = \mathbb{Q}(\sqrt{-23})$. Note that $r_1 = 0, r_2 = 1$ and $d_K = -23$. By Theorem 8.14, in every ideal class of K, there exists an ideal B with $N(B) \leq \left(\frac{4}{\pi}\right) \frac{2!}{2^2}\sqrt{23} < 4$. We look for ideals of norm 2 and 3 in $\mathcal{O}_K$ and check which ones are principal ideals. By Theorem 4.11, $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2'$ with $N(\mathfrak{p}_2) = N(\mathfrak{p}_2') = 2$. Note that $\mathfrak{p}_2$ is principal if and only if there exist $a, b \in \mathbb{Z}$ such that $2 = N(\mathfrak{p}_2) = \left|N_{K/\mathbb{Q}}\left(a + b\left(\frac{1+\sqrt{-23}}{2}\right)\right)\right|$, i.e., $8 = (2a + b)^2 + 23b^2$ which is impossible. Therefore $\mathfrak{p}_2, \mathfrak{p}_2'$ are not principal.

Consider the splitting of the prime 3 in $\mathcal{O}_K$. By Theorem 4.11, $3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$ with $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$. If $\mathfrak{p}_3$ is principal, then $\mathfrak{p}_3 = \alpha\mathcal{O}_K$, where $\alpha = a + b\left(\frac{1+\sqrt{-23}}{2}\right)$, $a, b \in \mathbb{Z}$. Thus $3 = N(\mathfrak{p}_3) = |N_{K/\mathbb{Q}}(\alpha)|$ which implies that $12 = (2a + b)^2 + 23b^2$ leading to a contradiction. Therefore $\mathfrak{p}_3, \mathfrak{p}_3'$ are not principal.

Since $N_{K/\mathbb{Q}}(\frac{1+\sqrt{-23}}{2}) = 6$, it follows that $\langle \frac{1+\sqrt{-23}}{2} \rangle$ is the product of an ideal of norm 2 with an ideal of norm 3, say $\langle \frac{1+\sqrt{-23}}{2} \rangle = \mathfrak{p}_3\mathfrak{p}_2'$. So $\mathfrak{p}_2$ and $\mathfrak{p}_3$ lie in the same ideal class and hence $\mathfrak{p}_2'$ and $\mathfrak{p}_3'$ lie in the same ideal class. Now we show that $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ lie in the different ideal classes, for otherwise $\mathfrak{p}_2^2$ would be a principal ideal of norm 4, say $\mathfrak{p}_2^2 = \langle c + d(\frac{1+\sqrt{-23}}{2}) \rangle$, which on taking norm implies that $16 = (2c+d)^2 + 23d^2$. This is possible only when $c = \pm 1$ and $d = 0$, i.e., $\mathfrak{p}_2^2$ is an ideal generated by 2 which is not so, because $\langle 2 \rangle$ is a product of two distinct prime ideals in K. Therefore there are three ideal classes $P(K)$, $\mathfrak{p}_2 P(K)$, $\mathfrak{p}_2' P(K)$.

Example 8.21 We find the class number of $K = \mathbb{Q}(\theta)$ where θ is root of $f(X) = X^3 - 4X + 2$. In view of Exercise 5 of Chap. 2, $d_K = D_{K/\mathbb{Q}}(1, \theta, \theta^2) = 148$. Keeping in mind Brill's Theorem, we see that the signature of K is $[3, 0]$. By Theorem 8.14, in every ideal class of K there exists an ideal B such that $N(B) \leq \frac{3!}{3^3}\sqrt{148} < 3$. We now try to explore whether there exists an ideal of norm 2 and if it exists whether it is principal or not. Note that 2 does not divide $\operatorname{ind}\theta$. Therefore Theorem 4.8 is applicable. By this theorem, $2\mathcal{O}_K = \mathfrak{p}_2^3$ where $\mathfrak{p}_2$ is the prime ideal generated by 2, θ with norm 2. Since $\theta^3 - 4\theta = -2$, θ divides 2 and hence $\mathfrak{p}_2 = \langle \theta \rangle$ is principal. So in every ideal class of K there is a principal ideal. Hence the class number of K is 1.

Example 8.22 We compute the class number of the cubic field $K = \mathbb{Q}(\theta)$, where θ is root of the polynomial $f(X) = X^3 - 5$. In view of Theorem 2.22, $\{1, \theta, \theta^2\}$ is an integral basis of K and $d_K = -27 \cdot 5^2$. By Theorem 8.14, in every ideal class of K there exists an ideal B such that $N(B) \leq (\frac{4}{\pi})\frac{3!}{3^3}\sqrt{27 \cdot 5^2} < 8$. We look for ideals of norm 2, 3, 4, 5, 6 and 7 in $\mathcal{O}_K$ and check which ones are principal ideals. Since $\operatorname{ind}\theta = 1$, Theorem 4.8 is applicable. Note that $f(X)$ factors as a product $(X+1)(X^2+X+1)$ of irreducible factors modulo 2. So by Theorem 4.8, $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2, \mathfrak{p}_2'$ are distinct prime ideals of $\mathcal{O}_K$ with $N(\mathfrak{p}_2) = 2$ and $N(\mathfrak{p}_2') = 4$. Since $\{1, \theta, \theta^2\}$ is an integral basis of K, $\mathfrak{p}_2$ will be a principal ideal if and only if there exist a, b, c in $\mathbb{Z}$ such that $|N_{K/\mathbb{Q}}(a + b\theta + c\theta^2)| = 2$. For $x, y, z \in \mathbb{Q}$, keeping in mind the formula

$$N_{K/\mathbb{Q}}(x + y\theta + z\theta^2) = x^3 + 5y^3 + 25z^3 - 15xyz, \tag{8.16}$$

given in Exercise 13 of Chap. 5, we see that $N_{K/\mathbb{Q}}(3 - \theta^2) = 2$. So $\mathfrak{p}_2 = \langle 3 - \theta^2 \rangle$ is principal. Therefore $\mathfrak{p}_2'$ is also principal. Since $f(X) \equiv (X+1)^3 \pmod 3$, $3\mathcal{O}_K = \mathfrak{p}_3^3$ with $N(\mathfrak{p}_3) = 3$ by Theorem 4.8. In view of (8.16), $N_{K/\mathbb{Q}}(2 - \theta) = 3$. So $\mathfrak{p}_3 = \langle 2 - \theta \rangle$ is principal. Since $5\mathcal{O}_K = \langle \theta^3 \rangle$ with $N(\langle \theta \rangle) = |N_{K/\mathbb{Q}}(\theta)| = 5$, we see that $5\mathcal{O}_K = \mathfrak{p}_5^3$ where $\mathfrak{p}_5 = \langle \theta \rangle$ is a prime ideal of $\mathcal{O}_K$. Thus we have shown that every ideal of $\mathcal{O}_K$ with norm less than or equal to 6 is a principal ideal. It will follow that the class number of K is 1 once we show that $\mathcal{O}_K$ has no ideal of norm 7. Since the polynomial $f(X)$ has no root modulo 7, it is irreducible modulo 7. So by Theorem 4.8, $7\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ with norm 7^3. Thus there is no ideal of $\mathcal{O}_K$ of norm 7. Hence the class number of K is 1.

Example 8.23 Let $K' = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$ and $K = \mathbb{Q}(\sqrt{-6})$. We show that the class number of K' is 1 and the class number of its subfield K is 2. The field K' is

the compositum of two quadratic fields $K_1 = \mathbb{Q}(\sqrt{2})$, $K_2 = \mathbb{Q}(\sqrt{-3})$ with coprime discriminants 8 and -3 respectively. Hence $d_{K'} = (24)^2$ in view of Corollary 2.30. By Theorem 8.14, in every ideal class of K' there exists an ideal B such that $N(B) \leq (\frac{4}{\pi})^2 \frac{4!}{4^4} \cdot 24 < 4$. So to prove that the class number of K' is 1, it is enough to show that $\mathcal{O}_{K'}$ does not have any ideal of norm 2 or 3. Since the prime ideal of $\mathcal{O}_{K_2}$ lying over 2 has residual degree 2, it follows that the (absolute) residual degree of a prime ideal of $\mathcal{O}_{K'}$ lying over 2 is at least 2 in view of Proposition 6.5. Thus there is no ideal of $\mathcal{O}_{K'}$ with norm 2. Similarly the prime ideal of $\mathcal{O}_{K_1}$ lying over 3 has residual degree 2 and consequently $\mathcal{O}_{K'}$ has no ideal of norm 3. This proves that the class number of K' is 1.

For computing the class number of K on again applying Theorem 8.14, we see that in every ideal class of K there exists an ideal B of $\mathcal{O}_K$ such that $N(B) \leq (\frac{2}{\pi}) \cdot \sqrt{24} < 4$. Note that $2\mathcal{O}_K = \mathfrak{p}_2^2$ with $N(\mathfrak{p}_2) = 2$ and $3\mathcal{O}_K = \mathfrak{p}_3^2$ with $N(\mathfrak{p}_3) = 3$. Since there do not exist any integers a and b such that $|N_{K/\mathbb{Q}}(a + b\sqrt{-6})| = 2$ or 3, it follows that $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are not principal ideals. Keeping in mind that $N_{K/\mathbb{Q}}(\sqrt{-6}) = 6$, we see that $\langle\sqrt{-6}\rangle = \mathfrak{p}_2\mathfrak{p}_3$. So $\mathfrak{p}_3$ lies in the ideal class of $\mathfrak{p}_2^{-1}$ which is same as the ideal class of $\mathfrak{p}_2$. Hence class number of K is 2.

Remark 8.24 The above example shows that if K'/K is an extension of algebraic number fields, then the canonical homomorphism from $G(K')/P(K')$ into $G(K)/P(K)$ defined by taking any class $I'P(K')$ into $N_{K'/K}(I')P(K)$ is not necessarily onto.

Example 8.25 We compute the class number of $K = \mathbb{Q}(\zeta)$, where ζ is a primitive $7th$ root of unity. In view of Theorem 2.25, $d_K = -7^5$. Note that each isomorphism of K maps ζ to a primitive $7th$ root of unity. So signature of K is $[0, 3]$. By Theorem 8.14, in every ideal class of K there exists an ideal B such that $N(B) \leq (\frac{4}{\pi})^3 \frac{6!}{6^6} (\sqrt{7})^5 < 5$. Thus $N(B) = 1, 2, 3$ or 4. We now try to explore whether there exists an ideal of norm 2 or 3 or 4. Applying Theorem 4.13, we see that $2\mathcal{O}_K = \mathfrak{p}_2\mathfrak{p}_2'$ where $\mathfrak{p}_2$ and $\mathfrak{p}_2'$ are prime ideals of $\mathcal{O}_K$ each having norm 2^3. Hence there is no ideal of norm 2 or 4. Again applying Theorem 4.13, we see that $3\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ and $N(3\mathcal{O}_K) = 3^6$. So there is no ideal of norm 3. Thus every ideal class of K contains the unit ideal. Therefore the class number of K is 1.

Remark 8.26 Using Theorem 8.14 and arguing as in above examples, one can quickly prove that $\mathbb{Q}(\sqrt{d})$ has class number one when $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$. As pointed out in Remark 3.6, it is known that these are the only nine imaginary quadratic fields with class number one. On the other hand, there are numerous examples of real quadratic fields having class number one; however it is not known that their number is infinite. In fact, it is not known whether there are infinitely many algebraic number fields of arbitrary degree having class number one.

Regarding imaginary quadratic fields, Gauss made a more general conjecture known as Class Number Problem. It states that for any given number h, there are only finitely many imaginary quadratic fields having class number h. This conjecture was proved in 1934 by Hans Heilbronn and Edward Linfoot (cf. [He-Li]). In 1936, Carl Ludwig Siegel [Sie] proved a more general result which says that if K runs over

quadratic extensions of $\mathbb{Q}$ with class number h_K and regulator R_K, then $\frac{\log(h_K R_K)}{\log|d_K|}$ tends to $\frac{1}{2}$ as $|d_K| \longrightarrow \infty$. In 1950, Sarvadaman Chowla [Cho] gave a different proof of Siegel's result. This result was extended by Richard Brauer to all extensions of any fixed degree over $\mathbb{Q}$ and is known as Brauer-Siegel Theorem (see [Bra] or Chapter XVI of [Lan2]). A detailed survey of Class Number Problem was given in 1983 by Dorian Goldfeld [Gol] along with his own contribution.

8.5 Hermite's Theorem on Discriminant

In this section, we prove a well known theorem which was first proved by Hermite in 1857 using quadratic forms. About 30 years later, Minkowski gave a different proof of this theorem. The proof given here resembles with the one given by Minkowski and makes use of Minkowski's convex body theorem.

Theorem 8.27 (Hermite). *Only a finite number of algebraic number fields can have the same discriminant.*

Proof In view of Corollary 8.15, it suffices to show that there exist only finitely many algebraic number fields with a fixed degree $n = r_1 + 2r_2$ whose discriminant has a given value d_0. Let K be one such field. We shall show that K has finitely many choices. In the space $\mathbb{R}^n$ consisting of all points $(x_1, \ldots, x_{r_1}, y_1, z_1, \ldots, y_{r_2}, z_{r_2})$, consider the subset S defined in case $r_1 > 0$ by

$$|x_1| < \sqrt{|d_0|+1},\ |x_k| < 1,\ 2 \le k \le r_1,\ y_j^2 + z_j^2 < 1,\ 1 \le j \le r_2$$

and in case $r_1 = 0$, S is defined by

$$|y_1| < \frac{1}{2},\ |z_1| < \sqrt{|d_0|+1},\ y_j^2 + z_j^2 < 1,\ \ 2 \le j \le r_2.$$

Clearly S is bounded, centrally symmetric and open. Using Cauchy-Schwarz inequality as in the proof of Lemma 8.16, it can be easily seen that S is convex. Note that the volume of S is given by

$$\text{vol}(S) = 2^{r_1}\pi^{r_2}\sqrt{|d_0|+1} \ \text{ or } \ 2\pi^{r_2-1}\sqrt{|d_0|+1} \tag{8.17}$$

according as $r_1 > 0$ or $r_1 = 0$. Let $\sigma_1, \ldots, \sigma_{r_1}$ be all the real isomorphisms of K and $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be non-real isomorphisms of K arranged so that $\overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j}$, $1 \le j \le r_2$.

We define a map Ψ from $\mathcal{O}_K$ into $\mathbb{R}^n$ by

$$\Psi(\alpha) = (\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha), Re(\sigma_{r_1+1}(\alpha)), Im(\sigma_{r_1+1}(\alpha)), \ldots, Im(\sigma_{r_1+r_2}(\alpha))).$$

As shown in the proof of Theorem 8.14, $\Psi(\mathcal{O}_K)$ is a lattice in $\mathbb{R}^n$ with determinant

$$\frac{\sqrt{|d_K|}}{2^{r_2}} = \frac{\sqrt{|d_0|}}{2^{r_2}} = \Delta \ (say);$$

in fact the above equality follows from (8.10) on taking $A = \mathcal{O}_K$. In view of (8.17), $\mathrm{vol}(S) > 2^n\Delta$. So by Theorem 8.9, the lattice $\Psi(\mathcal{O}_K)$ contains a non-zero vector $\Psi(\theta)$ of S with $\theta \in \mathcal{O}_K$. Note that there is only one isomorphism σ of K into $\mathbb{C}$ such that $|\sigma(\theta)| \geq 1$. In particular $\sigma(\theta) \neq \tau(\theta)$ for any isomorphism τ of K into $\mathbb{C}$ when $\tau \neq \sigma$. Hence θ is a primitive element of the extension $K/\mathbb{Q}$. Since $\Psi(\theta) \in S$, the roots of the minimal polynomial of θ over $\mathbb{Q}$ and hence its coefficients are bounded by a constant depending only upon d_0 and n. Therefore θ and hence K has only finitely many choices. □

It may be pointed out that Hermite's theorem on discriminant is of fundamental importance in Number Theory. In fact, it has given rise to the problem of determining the list of number fields with given signature whose discriminants are bounded in absolute value by a given constant. In particular, it has led to the search for the smallest absolute value of discriminant of number fields with a given signature $[r_1, r_2]$; the absolute value of the discriminant of such a number field is traditionally denoted by $M(r_1, r_2)$. It is immediate from Theorem 2.9 that $M(2, 0) = 5$ and $M(0, 1) = 3$. For cubic fields, it is known that $M(1, 1) = 23$ realized by $K = \mathbb{Q}(\alpha)$ with α satisfying $\alpha^3 = 1 + \alpha$ and $M(3, 0) = 49$ realized by the field $\mathbb{Q}(\beta)$ with β satisfying $\beta^3 + \beta^2 = 2\beta + 1$. For more details of this problem, see [Kau1], [Kau2], [Poh].

8.6 A Special Case of Fermat's Last Theorem

In this section, we prove the first case of Fermat's Last Theorem for regular primes. Recall that an odd prime p is said to be regular if p does not divide the class number of the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ is a primitive pth root of unity. In 1850, Kummer proved Fermat's Last Theorem for regular primes and he thus laid the foundation for an eventual complete proof of Fermat's Last Theorem.[3] Using Kummer's idea of proof, we shall prove the following theorem.

Theorem 8.28 *Let p be a regular odd prime. Then the equation $X^p + Y^p = Z^p$ has no solution in integers x, y, z not divisible by p.*

We first prove some lemmas.

Lemma 8.29 *Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive pth root of unity with p an odd prime. Then $1 - \zeta$ is a prime element of the ring $\mathcal{O}_K$ with $N_{K/\mathbb{Q}}(1 - \zeta) = p$ and $p\mathcal{O}_K = \langle 1 - \zeta \rangle^{p-1}$.*

[3] For this great achievement of Kummer, the French Academy of Sciences awarded him its Grand Prize in 1857.

Proof Let $\Phi(X)$ denote the minimal polynomial of ζ over $\mathbb{Q}$. Then

$$\Phi(X) = X^{p-1} + X^{p-2} + \cdots + 1 = \prod_{i=1}^{p-1}(X - \zeta^i).$$

Substituting $X = 1$ in the above equation, we obtain

$$p = \prod_{i=1}^{p-1}(1 - \zeta^i). \tag{8.18}$$

The above equality in view of Theorem 1.19 shows that $N_{K/\mathbb{Q}}(1 - \zeta) = p$. Hence $1 - \zeta$ is a prime element of $\mathcal{O}_K$ by virtue of Corollary 3.35. For each i, $1 \leq i \leq p - 1$, clearly $1 - \zeta$ divides $1 - \zeta^i$ and $1 - \zeta^i$ divides $1 - \zeta$, because $1 - \zeta$ can be written as $1 - \zeta^{ij}$, where j is a positive integer such that $ij \equiv 1 \pmod{p}$. So $1 - \zeta$ and $1 - \zeta^i$ are associates. It now follows from (8.18) that $p\mathcal{O}_K = \langle 1 - \zeta \rangle^{p-1}$. □

Lemma 8.30 *Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive mth root of unity and $m \geq 1$. Then the number of roots of unity in K is either m or $2m$ according as m is even or odd.*

Proof Let s denote the order of the group W of roots of unity contained in K which is a cyclic subgroup of $K^\times$. Let η be a generator of W. Since $\mathbb{Q}(\eta) \subseteq K$, the degree $\phi(s)$ of the extension $\mathbb{Q}(\eta)/\mathbb{Q}$ divides the degree $\phi(m)$ of the extension $K/\mathbb{Q}$. Keeping in view that -1 and ζ belong to W, it follows from Lagrange's theorem for finite groups that s is even and m divides s. In particular, $\phi(m)$ divides $\phi(s)$. Hence $\phi(m)$=$\phi(s)$. The last equality together with the fact that m divides the even number s immediately implies that s is either m or $2m$ acoording as m is even or odd. □

Lemma 8.31 (Kummer's Lemma). *Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive pth root of unity, p an odd prime. Then each unit of $\mathcal{O}_K$ is the product of a power of ζ with a real unit of $\mathcal{O}_K$.*

Proof Let ε be a unit of $\mathcal{O}_K$. Then $\varepsilon = g(\zeta)$ for some $g(X) \in \mathbb{Z}[X]$ of the form $g(X) = a_0 + a_1X + \cdots + a_{p-2}X^{p-2}$, where $a_0, a_1, \cdots, a_{p-2} \in \mathbb{Z}$. The complex conjugate $\overline{\varepsilon} = g(\overline{\zeta}) = g(\zeta^{p-1})$ is also a unit of $\mathcal{O}_K$, because there exists $h(X) \in \mathbb{Z}[X]$ such that $g(\zeta)h(\zeta) = 1$ and hence $g(\overline{\zeta})h(\overline{\zeta}) = g(\zeta^{p-1})h(\zeta^{p-1}) = 1$. Consider the unit $\mu = \varepsilon/\overline{\varepsilon}$ of $\mathcal{O}_K$. Let $\sigma_1, \cdots, \sigma_{p-1}$ be all the isomorphisms of K into $\mathbb{C}$ defined by $\sigma_i(\zeta) = \zeta^i$, $1 \leq i \leq p - 1$. Since

$$\sigma_i(\mu) = \frac{g(\zeta^i)}{g(\zeta^{(p-1)i})} = \frac{g(\zeta^i)}{g(\overline{\zeta}^i)},$$

it follows that $|\sigma_i(\mu)| = 1$ for $1 \leq i \leq p - 1$. So μ is a root of unity in K by Corollary 5.4. In view of Lemma 8.30, the only roots of unity in K are $\{\pm\zeta^i \mid 0 \leq i \leq p - 1\}$. Therefore $\mu = \pm\zeta^k$ for some k, i.e.,

$$\varepsilon = \pm\zeta^k\overline{\varepsilon}. \tag{8.19}$$

We show that the plus sign occurs in (8.19). Suppose to the contrary

$$\varepsilon = -\zeta^k\overline{\varepsilon}. \tag{8.20}$$

We denote $1-\zeta$ by λ. Keeping in mind that $\zeta^i \equiv 1 \pmod{\lambda}$ for each i, we see that

$$\varepsilon \equiv M \pmod{\lambda}, \quad \text{where} \quad M = a_0 + a_1 + \cdots + a_{p-2}. \tag{8.21}$$

Similarly, $\overline{\varepsilon} = \sum_{i=0}^{p-2} a_i\zeta^{(p-1)i} \equiv M \pmod{\lambda}$. It now follows from (8.20) that $M \equiv -M \pmod{\lambda}$. So λ divides $2M$. Therefore $N_{K/\mathbb{Q}}(\lambda)$ divides $N_{K/\mathbb{Q}}(2M)$. By Lemma 8.29, $N_{K/\mathbb{Q}}(\lambda) = p$ and $\lambda \mid p$. So $p \mid 2M$ and hence $\lambda \mid M$. Thus (8.21) implies that $\varepsilon \equiv 0 \pmod{\lambda}$, which is impossible because ε is a unit of $\mathcal{O}_K$ and λ is a prime element of $\mathcal{O}_K$ with norm p. This contradiction proves that the plus sign occurs in (8.19), i.e., $\varepsilon = \zeta^k\overline{\varepsilon}$. Choose an integer s such that $2s \equiv k \pmod{p}$. Then $\varepsilon = \zeta^{2s}\overline{\varepsilon}$, i.e.,

$$\frac{\varepsilon}{\zeta^s} = \zeta^s\overline{\varepsilon} = \overline{\left(\frac{\varepsilon}{\zeta^s}\right)}.$$

This shows that ε/ζ^s is a real unit and hence the lemma is proved. □

Proof of Theorem 8.28. We shall deal with the equation

$$X^p + Y^p + Z^p = 0 \tag{8.22}$$

which is symmetric in $X,\ Y,\ Z$. For proving the theorem, it is clearly enough to show that (8.22) has no solution in integers $x,\ y,\ z$ such that $p \nmid xyz$. Suppose to the contrary there exists a solution of (8.22) in integers $x,\ y,\ z$ not divisible by p. If a number d divides two of $x,\ y,\ z$, then it divides the third one and can be removed after division. So it may be assumed that $x,\ y,\ z$ are relatively prime in pairs. Let ζ be a primitive pth root of unity. We shall denote $\mathbb{Q}(\zeta)$ by K and $1-\zeta$ by λ. The relation $x^p + y^p + z^p = 0$ can be written as

$$\prod_{i=0}^{p-1}(x + \zeta^i y) = -z^p.$$

On passing to ideals in $\mathbb{Z}[\zeta]$, we have

$$\prod_{i=0}^{p-1}\langle(x + \zeta^i y)\rangle = \langle z\rangle^p. \tag{8.23}$$

We first show that the ideals on the left hand side of (8.23) are pairwise coprime. Suppose there exists a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ which divides $\langle (x+\zeta^i y)\rangle$ and $\langle (x+\zeta^j y)\rangle$ for some pair $(i,\ j), 0 \le i < j \le p-1$. Then $\mathfrak{p}$ contains both $x+\zeta^i y,\ x+\zeta^j y$ and hence their difference $\zeta^i y(1-\zeta^{j-i})$. Since $1-\zeta^{j-i}$ is an associate of $1-\zeta = \lambda$, it follows that $\mathfrak{p}$ contains either y or λ. Note that in view of (8.23), $z^p \in \mathfrak{p}$ and hence $z \in \mathfrak{p}$. Therefore $y \notin \mathfrak{p}$ as $y,\ z$ are coprime. So $\lambda \in \mathfrak{p}$ i.e., $\langle\lambda\rangle \subseteq \mathfrak{p}$. By Lemma 8.29, $\langle\lambda\rangle$ is a prime ideal of $\mathcal{O}_K$ and hence it is a maximal ideal. So $\mathfrak{p} = \langle\lambda\rangle$. Recall that $z \in \mathfrak{p}$. Thus λ divides z; consequently $N_{K/\mathbb{Q}}(\lambda)$ divides $N_{K/\mathbb{Q}}(z)$. By Lemma 8.29, $N_{K/\mathbb{Q}}(\lambda) = p$. Therefore $p \mid z$, which contradicts the hypothesis. This proves that the ideals on the left hand side of (8.23) are pairwise coprime. So in view of the fundamental theorem of ideal theory (Theorem 3.12), each of these ideals is the pth power of an ideal of $\mathcal{O}_K$. In particular, $\langle x+\zeta y\rangle = I^p$ for some ideal I of $\mathcal{O}_K$. Since p does not divide the class number of K, it follows from Corollary 8.5 that I is a principal ideal of $\mathcal{O}_K$, say $I = \langle\alpha\rangle$. So there exists a unit ε of $\mathcal{O}_K$ such that

$$x + \zeta y = \varepsilon\alpha^p. \tag{8.24}$$

On writing α as

$$\alpha = a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2}$$

and using Fermat's little theorem, we see that

$$\alpha^p \equiv a_0^p + a_1^p\zeta^p + \cdots + a_{p-2}^p\zeta^{p(p-2)} \equiv a \pmod{p\mathcal{O}_K},$$

where $a = a_0 + a_1 + \cdots + a_{p-2}$. By Lemma 8.31, ε can be written in the form $\zeta^g u$, where u is a real unit of $\mathcal{O}_K$ and $g \in \mathbb{Z}$. Hence from (8.24), we obtain the congruence

$$x + \zeta y \equiv \zeta^g au \pmod{p\mathcal{O}_K}$$

with au real. Since ζ is a unit, we can rewrite the above congruence as

$$\zeta^{-g}(x+\zeta y) \equiv au \pmod{p\mathcal{O}_K}. \tag{8.25}$$

Keeping in mind that the complex conjugate $\overline{\beta}$ of an element β of $\mathcal{O}_K$ lies in $\mathcal{O}_K$, it can be easily seen that for β, γ in $\mathcal{O}_K$, if $\beta \equiv \gamma \pmod{p\mathcal{O}_K}$, then $\overline{\beta} \equiv \overline{\gamma} \pmod{p\mathcal{O}_K}$. Passing now from (8.25) to its complex conjugate, we have

$$\zeta^g(x+\zeta^{-1}y) \equiv au \pmod{p\mathcal{O}_K}.$$

It follows from (8.25) and the above congruence that

$$x\zeta^{-g} + y\zeta^{1-g} - x\zeta^g - y\zeta^{g-1} \equiv 0 \pmod{p\mathcal{O}_K}. \tag{8.26}$$

Observe that $g \not\equiv 0 \pmod{p}$, for otherwise $\zeta^g = 1$ and hence (8.26) becomes

$$y(\zeta - \zeta^{-1}) \equiv 0 \pmod{p\mathcal{O}_K}.$$

So p divides $y(\zeta - \zeta^{-1})$. Since $1 - \zeta$, $1 - \zeta^2$ are associates, $1 + \zeta$ is a unit of $\mathcal{O}_K$. Hence the above congruence shows that $p \mid y(1 - \zeta)$. By Lemma 8.29, $\langle p \rangle = \langle 1 - \zeta \rangle^{p-1}$. Since $p > 2$, it follows that $1 - \zeta$ divides y; consequently $p = N_{K/\mathbb{Q}}(1 - \zeta)$ divides $y^{p-1} = N_{K/\mathbb{Q}}(y)$, which contradicts the hypothesis that $p \nmid y$. This contradiction proves that $g \not\equiv 0 \pmod{p}$. Arguing similarly, it can be seen that $g \not\equiv 1 \pmod{p}$.

By virtue of (8.26), there exists $\beta \in \mathcal{O}_K$ such that

$$p\beta = x\zeta^{-g} + y\zeta^{1-g} - x\zeta^g - y\zeta^{g-1}. \tag{8.27}$$

As shown in the above paragraph, none of the exponents of ζ occurring on the right hand side of (8.27) is divisible by p. Recall that $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$ is an integral basis of K and the elements $\zeta^{-g}, \zeta^{1-g}, \zeta^g, \zeta^{g-1}$ belong to this integral basis. So keeping in mind the hypothesis $p \nmid xy$ and the fact that the element

$$\beta = \frac{x}{p}\zeta^{-g} + \frac{y}{p}\zeta^{1-g} - \frac{x}{p}\zeta^g - \frac{y}{p}\zeta^{g-1}$$

belongs to $\mathcal{O}_K$, we infer that at least two of the exponents of ζ occurring in the right hand side of the above equation must be congruent to each other modulo p. Since $g \not\equiv 0, 1 \pmod{p}$, it follows that $2g \equiv 1 \pmod{p}$. Therefore (8.27) can be rewritten as

$$p\beta\zeta^g = x + y\zeta - x\zeta^{2g} - y\zeta^{2g-1} = (x - y)(1 - \zeta).$$

Taking norm on both sides of the above equation, we see that $p \mid (x - y)$, i.e., $x \equiv y \pmod{p}$.

Since the equation $x^p + y^p + z^p = 0$ is symmetric in x, y and z, on interchanging the roles of y, z, i.e., writing

$$\prod_{i=0}^{p-1}(x + \zeta^i z) = -y^p$$

and arguing in a similar way as before, we obtain $x \equiv z \pmod{p}$. Hence

$$0 = x^p + y^p + z^p \equiv 3x^p \pmod{p}.$$

Thus, $p \mid 3x^p$. But $p \nmid x$. So $p = 3$.

It remains to deal with the case when $p = 3$. In this case, we prove the theorem by showing that $x^3 + y^3 + z^3 \equiv 0 \pmod{9}$ has no solution in integers x, y, z not divisible by 3. It can be easily seen that the cube of an integer of the form $3k \pm 1$

is congruent to 1 or -1 modulo 9. So if $3 \nmid xyz$, then $x^3 + y^3 + z^3 \equiv \pm 1 \pm 1 \pm 1 \pmod 9$, which is not congruent to 0 modulo 9 for any choice of the $\pm$ signs. □

Remark 8.32 Let $K = \mathbb{Q}(\zeta)$, where ζ be a primitive pth root of unity with p an odd prime and let $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$ be the maximal real subfield of K. Let h_p, h_p^+ denote respectively the class numbers of K, K_0. It is known that h_p^+ divides h_p and if p does not divide h_p / h_p^+ then it does not divide h_p; moreover h_p / h_p^+ is a computable number(cf. [Nar, Proposition 8.11], [Bo-Sh, Chap. 5]). The factors h_p / h_p^+ and h_p^+ are traditionally called the first and the second factors of h_p. By very beautiful number theoretic and analytic arguments, analysing the first factor of h_p, Kummer obtained a fairly simple criterion which allows one to easily check whether a given prime is regular or not. In fact he proved that an odd prime p is regular if and only if it does not divide the numerators of the Bernoulli numbers[4] $B_2, B_4, \ldots, B_{p-3}$ (cf. [Bo-Sh, Chap. 5], [Rib, Chap. 19]). Using this criterion, Kummer showed that all odd primes <165, except 37, 59, 67, 101, 103, 131, 149, and 157 are regular. It is not known whether the number of regular primes is infinite.

Exercises

1. Prove that $\mathbb{Q}(\sqrt{d})$ has class number one when $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$.
2. Prove that the class number of the fields $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{17})$ is one.
3. Prove that the rings $\mathbb{Z}[\sqrt{6}]$, $\mathbb{Z}[\sqrt{7}]$, $\mathbb{Z}[\sqrt{14}]$ and $\mathbb{Z}[\sqrt{23}]$ are principal ideal domains.
4. Prove that $\mathcal{O}_K$ is a PID, where $K = \mathbb{Q}(\theta)$ with θ satisfying $\theta^3 + \theta + 1 = 0$.
5. Prove that $\mathbb{Z}[\sqrt{34}]$ is not a principal ideal domain.
6. Let $K = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - 2X^2 + 2$. Compute the class number of K.
7. Prove that the class number of $\mathbb{Q}(\sqrt[3]{2})$ and $\mathbb{Q}(\sqrt[3]{3})$ is one.
8. Prove that $\mathbb{Z}[\zeta]$ is a UFD when ζ is a primitive 5th root of unity.
9. If ζ is a primitive 7th root of unity, then prove that $\mathbb{Z}[\zeta + \zeta^{-1}]$ is a principal ideal domain.
10. Prove that $\mathbb{Q}(\sqrt{-10})$, $\mathbb{Q}(\sqrt{-13})$, $\mathbb{Q}(\sqrt{-15})$ have class number 2 each.
11. Prove that $\mathbb{Q}(\sqrt{15})$, $\mathbb{Q}(\sqrt{65})$ have class number 2 each.
12. Prove that the class number of $\mathbb{Q}(\sqrt{-14})$ is 4.
13. Prove that in any two distinct ideal classes of an algebraic number field, there exist relatively prime integral ideals.

[4] Recall that the kth Bernoulli number B_k is defined by the series expansion

$$\frac{t}{e^t - 1} = 1 + \sum_{k=1}^{\infty} \frac{B_k}{k!} t^k.$$

14. Let K_1 and K_2 be algebraic number fields whose discriminants are coprime. Prove that $[K_1K_2 : \mathbb{Q}] = [K_1 : \mathbb{Q}]\,[K_2 : \mathbb{Q}]$.
15. Let p be a prime number, $p \equiv 1 \pmod 4$. Prove that the class number of $\mathbb{Q}(\sqrt{-p})$ is even.
16. Let ζ be a primitive pth root of unity, p an odd prime. Let $K_0 = \mathbb{Q}(\zeta + \zeta^{-1})$ be the subfield of $K = \mathbb{Q}(\zeta)$. Prove that a fundamental system of units of K_0 is also a fundamental system of units of K. Deduce that the regulator R_0 of K_0 is related to the regulator R of K by $R = 2^{\frac{p-3}{2}} R_0$.
17. Let K be an algebraic number field and I be an ideal of $\mathcal{O}_K$ such that $I^m = \langle\alpha\rangle$ is a principal ideal. Show that in $K' = K(\alpha^{1/m})$, the ideal $I\mathcal{O}_{K'}$ is a principal ideal.
18. Let K be an algebraic number field. Show that there exists a finite extension L of K such that $I\mathcal{O}_L$ is a principal ideal for each ideal I of $\mathcal{O}_K$.

Chapter 9
Dirichlet's Class Number Formula and its Applications

9.1 Dirichlet's Class Number Formula and Ideal Theorem

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

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

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

Theorem 9.1 *(Dirichlet's Class Number Formula) Let K be an algebraic number field of degree $r_1 + 2r_2$ with class number h, where r_1 is the number of real isomorphisms of K and $2r_2$ is the number of non-real isomorphisms of K into $\mathbb{C}$. Let R stand for the regulator of K and d_K for the discriminant of K. The series $\sum_A \frac{1}{N(A)^s}$ converges uniformly on all compact subsets of $(1, \infty)$ and represents a continuous function of s in $(1, \infty)$, where A runs over all non-zero (integral) ideals of $\mathcal{O}_K$. If $\zeta_K(s)$ denotes its sum function,[1] then*

[1] This function is called Dedekind zeta-function. In 1917 Hecke proved that this function can be extended to a meromorphic function in the complex plane and found its functional equation. A version of Hecke's proof is given in (Neu).

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_9

$$\lim_{s\to 1^+}(s-1)\zeta_K(s) = h\frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{|d_K|}} \tag{9.1}$$

where m is the number of roots of unity in K. The constant $\frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{|d_K|}}$ is traditionally denoted by κ.

For proving the above theorem, we shall first prove the Ideal Theorem by Dedekind stated below.

Theorem 9.2 (Ideal Theorem) *Let K be an algebraic number field of degree n and r_1, r_2, R, d_K, m be as in the above theorem. Let $\mathcal{C}$ be an ideal class of K. For a positive real number T, let $\mathcal{Z}(T, \mathcal{C})$ be the number of integral ideals in $\mathcal{C}$ whose norm is less than or equal to T. Then*

$$\lim_{T\to\infty}\frac{\mathcal{Z}(T,\mathcal{C})}{T} = \frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{|d_K|}}.$$

We now prove a lemma, which will be used in the proof of the above theorem.

For any real number $t > 0$ and for a subset S of $\mathbb{R}^n$, we denote by $S(t)$ the set

$$\{(tx_1, \ldots, tx_n) \mid (x_1, \ldots, x_n) \in S\}.$$

Note that if the volume of S exists, then the change of variables formula of multivariable calculus shows that the volume of $S(t)$ exists and $\mathrm{Vol}(S(t)) = t^n\mathrm{Vol}(S)$.

Lemma 9.3 *Let S be a bounded subset of $\mathbb{R}^n$. For each positive real number t, let $N(t)$ denote the number of points in $S(t)$ with integral co-ordinates. If volume of S exists, say V, then $\lim_{t\to\infty}\frac{N(t)}{t^n} = V$.*

Proof Fix a positive real number t. Consider the family $\mathcal{F}_t$ consisting of all n-cubes in $\mathbb{R}^n$ of the type

$$\left\{(y_1, \ldots, y_n) : \frac{z_i}{t} \le y_i < \frac{z_i+1}{t}, 1 \le i \le n\right\},$$

where $(z_1, \ldots, z_n)$ runs over $\mathbb{Z}^n$. Then $\mathbb{R}^n$ is a disjoint union of members of $\mathcal{F}_t$. Let $\underline{n_t}$ denote the number of n-cubes in $\mathcal{F}_t$ contained inside S and let $\overline{n_t}$ denote the number of n-cubes in $\mathcal{F}_t$ whose intersection with S is non-empty. Note that each n-cube in $\mathcal{F}_t$ has volume $1/t^n$. Since the volume of S exists and equals V, we have

$$\lim_{t\to\infty}\frac{\underline{n_t}}{t^n} = \lim_{t\to\infty}\frac{\overline{n_t}}{t^n} = V.$$

We claim that $\underline{n_t} \le N(t) \le \overline{n_t}$. In view of the above equality, the claim would imply that $\lim_{t\to\infty}\frac{N(t)}{t^n} = V$, as desired.

To prove the claim, observe that given a cube C in the family $\mathcal{F}_t$, it has 2^n vertices out of which only one belongs to C. Therefore for a given point $(z_1, \ldots, z_n)$ with integral co-ordinates in $S(t)$, there exists a unique $C \in \mathcal{F}_t$ such that $C \cap S$ contains $(z_1/t, \ldots, z_n/t)$; in fact this point is a vertex of C.

Let $C_1, \ldots, C_{\underline{n_t}}$ be all the n-cubes from $\mathcal{F}_t$ inside S. Let v_i denote the unique vertex of C_i, which belongs to C_i. Then $v_1, \ldots, v_{\underline{n_t}}$ belong to S. Therefore $\underline{n_t} \leq N(t)$. To prove that $N(t) \leq \overline{n_t}$, let $P_1, \ldots, P_{N(t)}$ be all the points with integral co-ordinates inside $S(t)$. Let Q_i denote the point obtained from P_i by dividing its co-ordinates by t. Then in view of the above observation, $Q_1, \ldots, Q_{N(t)}$ are the vertices of pairwise disjoint n-cubes $C'_1, \ldots, C'_{N(t)}$ of $\mathcal{F}_t$ such that $Q_i \in C'_i \cap S$ for all $i = 1, \ldots, N(t)$. Consequently, $C'_i \cap S$ is non-empty for each $i = 1, \ldots, N(t)$. Therefore $N(t) \leq \overline{n_t}$. This proves the claim and hence the lemma. □

9.2 Proof of Ideal Theorem

Let $\sigma_1, \ldots, \sigma_{r_1}$ be all the real isomorphisms of K and let $\sigma_{r_1+1}, \ldots, \sigma_{r_1+2r_2}$ be the non-real isomorphisms of K arranged so that $\overline{\sigma_{r_1+j}} = \sigma_{r_1+r_2+j}$, $1 \leq j \leq r_2$. For $\alpha \in K$, we shall denote $\sigma_i(\alpha)$ by $\alpha^{(i)}$ and $|N_{K/\mathbb{Q}}(\alpha)|$ by $N(\alpha)$. Let $\{\epsilon_1, \ldots, \epsilon_r\}$ be a fundamental system of units of K, where $r = r_1 + r_2 - 1$, and let ζ be a primitive mth root of unity in K. Recall that the regulator R of the field K is the absolute value of the determinant of $r \times r$ matrix whose (i, j)th entry is $e_j \log |\epsilon_i^{(j)}|$, where e_j equals 1 or 2 according as $1 \leq j \leq r_1$ or $j > r_1$. Since $R \neq 0$, it follows that the determinant of the matrix $(\log |\epsilon_i^{(j)}|)_{i,j}$ is non-zero. We fix an (integral) ideal B in the class $\mathcal{C}^{-1}$.

The proof of the theorem is split into three steps.

Step I. If A is an integral ideal in the class $\mathcal{C}$, then AB is a principal ideal say $AB = w\mathcal{O}_K$. Also if B divides a principal ideal $w_1\mathcal{O}_K$, then $w_1\mathcal{O}_K = A_1 B$ for some integral ideal $A_1 \in \mathcal{C}$. Hence the integral ideals $A \in \mathcal{C}$ with $N(A) \leq T$ are in one-to-one correspondence with principal ideals $w\mathcal{O}_K \subseteq \mathcal{O}_K$ divisible by B such that $|N_{K/\mathbb{Q}}(w)| \leq TN(B)$. Also observe that two principal ideals $w\mathcal{O}_K$ and $w_1\mathcal{O}_K$ are equal if and only if $w_1 = \epsilon w$, where ϵ is unit of $\mathcal{O}_K$. In the following paragraph, we try to fix the choice of generator of such a principal ideal upto some extent.

Given a non-zero element w of $\mathcal{O}_K$, the vector $\left(\log \left|\frac{w^{(1)}}{\sqrt[n]{N(w)}}\right|, \ldots, \log \left|\frac{w^{(r)}}{\sqrt[n]{N(w)}}\right|\right)$ can be written as a linear combination of the row vectors of the non-singular matrix $(\log |\epsilon_i^{(j)}|)_{i,j}$ i.e., given a non-zero element w in $\mathcal{O}_K$, there exist real numbers $c_1, \ldots, c_r$ satisfying

$$\log \left|\frac{w^{(i)}}{\sqrt[n]{N(w)}}\right| = c_1 \log |\epsilon_1^{(i)}| + \cdots + c_r \log |\epsilon_r^{(i)}|, \quad 1 \leq i \leq r. \tag{9.2}$$

We now show that (9.2) holds for $i = r+1$ also (and hence for $1 \le i \le n$ in view of the arrangement of the isomorphisms $\sigma_1, \ldots, \sigma_n$). Since

$$\sum_{i=1}^{r+1} e_i \log \left| \frac{w^{(i)}}{\sqrt[n]{N(w)}} \right| = \log \left| \frac{N(w)}{N(w)} \right| = 0 \text{ and } \sum_{i=1}^{r+1} e_i \log |\epsilon_j^{(i)}| = \log |N(\epsilon_j)| = 0,$$

we see by virtue of (9.2) that

$$\begin{aligned} e_{r+1} \log \left| \frac{w^{(r+1)}}{\sqrt[n]{N(w)}} \right| &= -\sum_{i=1}^{r} e_i \log \left| \frac{w^{(i)}}{\sqrt[n]{N(w)}} \right| \\ &= -\sum_{i=1}^{r} e_i \sum_{j=1}^{r} c_j \log |\epsilon_j^{(i)}|. \end{aligned}$$

So

$$e_{r+1} \log \left| \frac{w^{(r+1)}}{\sqrt[n]{N(w)}} \right| = -\sum_{j=1}^{r} c_j \sum_{i=1}^{r} e_i \log |\epsilon_j^{(i)}| = -\sum_{j=1}^{r} c_j (-e_{r+1} \log |\epsilon_j^{(r+1)}|).$$

Cancelling e_{r+1} from both sides, we get

$$\log \left| \frac{w^{(r+1)}}{\sqrt[n]{N(w)}} \right| = \sum_{j=1}^{r} c_j \log |\epsilon_j^{(r+1)}|.$$

Combining the last equation with (9.2), we see that

$$\log \left| \frac{w^{(i)}}{\sqrt[n]{N(w)}} \right| = c_1 \log |\epsilon_1^{(i)}| + \cdots + c_r \log |\epsilon_r^{(i)}|, \quad 1 \le i \le r+1. \tag{9.3}$$

If w and w_1 are non-zero elements of $\mathcal{O}_K$ which are associates, then by Dirichlet's unit theorem, there exist unique integers $s_1, s_2, \ldots, s_r$ and a non-negative integer $k < m$ such that

$$w_1 = w\zeta^k \epsilon_1^{s_1} \cdots \epsilon_r^{s_r}.$$

Therefore

$$w_1^{(i)} = w^{(i)} (\zeta^{(i)})^k (\epsilon_1^{(i)})^{s_1} \cdots (\epsilon_r^{(i)})^{s_r}, \quad 1 \le i \le r+1.$$

Taking logarithm of the absolute value on both sides in the above equation, keeping in view the equality $N(w) = N(w_1)$, we see that

$$\log \left| \frac{w_1^{(i)}}{\sqrt[n]{N(w_1)}} \right| = \log \left| \frac{w^{(i)}}{\sqrt[n]{N(w)}} \right| + s_1 \log |\epsilon_1^{(i)}| + \cdots + s_r \log |\epsilon_r^{(i)}|, \quad 1 \le i \le r+1.$$

Using Eq. (9.3), the above equation gives

$$\log\left|\frac{w_1^{(i)}}{\sqrt[n]{N(w_1)}}\right| = (c_1+s_1)\log|\epsilon_1^{(i)}| + \cdots + (c_r+s_r)\log|\epsilon_r^{(i)}|, \quad 1 \le i \le r+1.$$

Hence the last equation shows that in every equivalence class of non-zero associate elements of $\mathcal{O}_K$, there are exactly m elements w for which, in Eq. (9.3), the coefficients c_j satisfy $0 \le c_j < 1$ for $j = 1, 2, \ldots, r$. In fact, if w is one such element then others are $w\zeta^k$ with $1 \le k < m$. This shows that $m\mathcal{Z}(T, \mathcal{C})$ is the number of those algebraic integers w lying in the ideal B for which the following two conditions are satisfied:

$$0 < |N(w)| \le TN(B) \tag{9.4}$$

and when we write for $1 \le i \le r$

$$\log\left|\frac{w^{(i)}}{\sqrt[n]{N(w)}}\right| = \sum_{j=1}^{r} c_j \log|\epsilon_j^{(i)}|, \quad \text{then } 0 \le c_j < 1 \text{ for } j = 1, \ldots, r. \tag{9.5}$$

In fact, (9.5) holds for $1 \le i \le n$ in view of (9.3) and the arrangement of isomorphisms.

Step II. Let $\{\beta_1, \ldots, \beta_n\}$ be a $\mathbb{Z}$-basis of the ideal B. If $w \in B$, then we can write $w = \sum_{j=1}^{n} \beta_j x_j$, $x_j \in \mathbb{Z}$. So we have $w^{(i)} = \sum_{j=1}^{n} \beta_j^{(i)} x_j$. Hence $m\mathcal{Z}(T, \mathcal{C})$ is the number of points with integral co-ordinates in the subset S' of $\mathbb{R}^n$ consisting of points $(x_1, \ldots, x_n)$ satisfying the following conditions:

If $y_i = \sum_{j=1}^{n} \beta_j^{(i)} x_j$, $1 \le i \le n$ and if y^* stands for $\left|\prod_{i=1}^{n} y_i\right|$, then

$$0 < \left|\prod_{i=1}^{n}\sum_{j=1}^{n} \beta_j^{(i)} x_j\right| = y^* \le N(B)T$$

and in the equations

$$\log\left|\frac{y_i}{\sqrt[n]{y^*}}\right| = \sum_{q=1}^{r} c_q \log|\epsilon_q^{(i)}| \quad \text{for } 1 \le i \le n,$$

the coefficients c_q satisfy $0 \le c_q < 1$ for $q = 1, \ldots, r$.

Note that if K is $\mathbb{Q}$ or an imaginary quadratic field, then $r = 0$. In this case, the condition on c_q in the definition of S' is vacuous.

We now verify that S' is a bounded subset of $\mathbb{R}^n$. We shall denote by S the subset of $\mathbb{R}^n$ defined so as $S' = S(T^{\frac{1}{n}})$. In fact ,the set $S(T^{1/n})$ results from the set S by

multiplying all co-ordinates by $T^{1/n}$. So S is a subset of $\mathbb{R}^n$ consisting of all those $(x_1, \ldots, x_n) \in \mathbb{R}^n$ such that if $y_i = \sum_{j=1}^{n} \beta_j^{(i)} x_j,\ 1 \le i \le n$, then

$$0 < \left| \prod_{i=1}^{n} y_i \right| \le N(B) \text{ and for } 1 \le i \le n,$$

$$\log \left| \frac{y_i}{\sqrt[n]{\prod y_j}} \right| = \sum_{q=1}^{r} c_q \log \left| \epsilon_q^{(i)} \right| \quad \text{with each } c_q \in [0, 1).$$

We shall prove that S is bounded and that its volume exists. Consequently by Lemma 9.3, we would have

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

So the theorem is proved once it is shown that S is bounded, its volume exists and is given by

$$\text{vol}(S) = \frac{2^{r_1 + r_2} \pi^{r_2} R}{\sqrt{|d_K|}}. \tag{9.6}$$

We first verify that S is a bounded set. Consider the mapping

$$\Lambda : \mathbb{C}^n \longrightarrow \mathbb{C}^n$$

defined by

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

which is a non-singular linear transformation, because the absolute value of its determinant is $\sqrt{|D_{K/\mathbb{Q}}(\beta_1, \ldots, \beta_n)|}$, which is non-zero. Therefore a subset V of $\mathbb{C}^n$ is bounded if and only if $\Lambda(V)$ is a bounded subset of $\mathbb{C}^n$. So it is enough to prove that the set $\Lambda(S)$ is bounded, where $\Lambda(S)$ is the subset of $\mathbb{C}^n$ consisting of all those vectors $(y_1, \ldots, y_n)$ for which the following two conditions are satisfied on taking $y^* = \left| \prod_{j=1}^{n} y_j \right|$:

$$0 < y^* \le N(B)$$

and in the equations

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

the inequalities $0 \le c_q < 1$ hold for $1 \le q \le r$.

Taking exponential in the above equality, we see that

$$|y_i| = \sqrt[n]{y^*}\prod_{q=1}^{r}|\epsilon_q^{(i)}|^{c_q} \le (N(B))^{\frac{1}{n}}\exp\left(\sum_{q=1}^{r} c_q \log|\epsilon_q^{(i)}|\right) \le (N(B))^{\frac{1}{n}}\exp(m_0 r),$$

where

$$m_0 = \max_{1\le q\le r,\ 1\le i\le n} |\log|\epsilon_q^{(i)}||.$$

Therefore $\Lambda(S)$ is a bounded set and hence so is S.

Step III. In this step, we shall show that the volume of S exists and compute its value. By making successive change of variables, we shall replace S by another set which is defined by a simpler set of conditions and for which the volume exists besides being easily computable. First consider the substitutions

$$z_i = \begin{cases} y_i, & \text{for } i = 1, \ldots, r_1, \\ \frac{y_i + y_{i+r_2}}{2} & \text{for } i = r_1 + 1, \ldots, r_1 + r_2, \\ \frac{y_{i-r_2} - y_i}{2\iota} & \text{for } i = r_1 + r_2 + 1, \ldots, r_1 + 2r_2. \end{cases}$$

Recall that $y_i = \sum_{j=1}^{n} \beta_j^{(i)} x_j$ where $(x_1, \ldots, x_n) \in \mathbb{R}^n$. In view of the arrangement of the isomorphisms, it is clear that $(x_1, \ldots, x_n) \mapsto (z_1, \ldots, z_n)$ is a transformation of $\mathbb{R}^n \to \mathbb{R}^n$, which is given by

$$z_i = \begin{cases} \sum_{j=1}^{n} \beta_j^{(i)} x_j & \text{for } i = 1, \ldots, r_1, \\ \sum_{j=1}^{n} \mathrm{Re}(\beta_j^{(i)}) x_j & \text{for } i = r_1 + 1, \ldots, r_1 + r_2, \end{cases}$$

$$z_{i+r_2} = \sum_{j=1}^{n} \mathrm{Im}(\beta_j^{(i)}) x_j \qquad \text{for } i = r_1 + 1, \ldots, r_1 + r_2.$$

Thus by an argument similar to that in the proof of Theorem 8.14, we see that the absolute value of Jacobian of $z_1, \ldots, z_n$ with respect to $x_1, \ldots, x_n$ is given by

$$\left|\frac{\partial(z_1, \ldots, z_n)}{\partial(x_1, \ldots, x_n)}\right| = 2^{-r_2}|\det(\beta_j^{(i)})_{i,j}|.$$

Also by Theorem 2.15, we have

$$|\det(\beta_j^{(i)})_{i,j}| = \sqrt{|D_{K/\mathbb{Q}}(\beta_1,\ldots,\beta_n)|} = [\mathcal{O}_K : B]\sqrt{|d_K|} = N(B)\sqrt{|d_K|}.$$

So $\left|\frac{\partial(z_1,\ldots,z_n)}{\partial(x_1,\ldots,x_n)}\right| = 2^{-r_2}N(B)\sqrt{|d_K|}$. Consequently with S as in Step II, volume of S exists once it is shown that volume of S^* exists, where S^* is the subset of $\mathbb{R}^n$ consisting of all points $(z_1,\ldots,z_n)$ such that the following two conditions are satisfied on taking $z^* = \prod_{j=1}^{r_1}|z_j| \prod_{j=r_1+1}^{r_1+r_2}(z_j^2 + z_{j+r_2}^2)$:

$$0 < z^* \le N(B),$$

and in the equations

$$\left.\begin{aligned} \log\left|\frac{z_i}{\sqrt[n]{z^*}}\right| &= \sum_{q=1}^{r} c_q \log|\epsilon_q^{(i)}|, \quad 1 \le i \le r_1, \\ \log\left|\frac{\sqrt{z_j^2 + z_{j+r_2}^2}}{\sqrt[n]{z^*}}\right| &= \sum_{q=1}^{r} c_q \log|\epsilon_q^{(j)}|, \quad r_1+1 \le j \le r_1+r_2, \end{aligned}\right\} \tag{9.7}$$

the coefficients c_q satisfy $0 \le c_q < 1$ for $1 \le q \le r$.

In view of the Jacobian computed above, the volumes of S and S^* (in case of existence) are related by

$$\mathrm{vol}(S) = \underbrace{\int\cdots\int}_{S} dx_1\cdots dx_n = \frac{2^{r_2}}{N(B)\sqrt{|d_K|}}\Big(\underbrace{\int\cdots\int}_{S^*} dz_1\cdots dz_n\Big).$$

On replacing each coordinate z_i by $z_i/N(B)^{1/n}$, clearly it is enough to prove that the volume of the set S^{**} exists where S^{**} is the subset of $\mathbb{R}^n$ consisting of all points $(z_1,\ldots,z_n)$ which satisfy the following conditions with z^* as above:

$$0 < z^* \le 1, \quad z_j > 0, \ 1 \le j \le r_1,$$

and in Eqs. (9.7), the coefficients c_q satisfy $0 \le c_q < 1$ for $1 \le q \le r$.
If volume of S^{**} exists, then volume of S will exist and will be given by

$$\mathrm{vol}(S) = \frac{2^{r_1+r_2}}{\sqrt{|d_K|}}\underbrace{\int\cdots\int}_{S^{**}} dz_1\cdots dz_n = \frac{2^{r_1+r_2}}{\sqrt{|d_K|}}\,\mathrm{vol}(S^{**}). \tag{9.8}$$

We now take new variables $\rho_1,\ldots,\rho_{r_1+r_2},\phi_{r_1+1},\ldots,\phi_{r_1+r_2}$ and make the following substitution into polar coordinates:

$$z_i = \begin{cases} \rho_i, & \text{if } 1 \le i \le r_1 \\ \rho_i \cos\phi_i, & \text{if } i = r_1+1, \ldots, r_1+r_2 \end{cases}$$
$$z_{i+r_2} = \rho_i \sin\phi_i, \qquad \text{if } i = r_1+1, \ldots, r_1+r_2$$

Then $dz_i dz_{i+r_2} = \rho_i d\rho_i d\phi_i$ for $i = r_1+1, \ldots, r_1+r_2$ and the Jacobian of this transformation is $(\prod_{i=r_1+1}^{r_1+r_2} \rho_i)$. On denoting $(\prod_{i=1}^{r_1+r_2} \rho_i^{e_i})$ by ρ, the set S^{**} in terms of the coordinates $\rho_1, \ldots, \rho_{r_1+r_2}, \phi_{r_1+1}, \ldots, \phi_{r_1+r_2}$ is given by the following conditions:

$$\left.\begin{array}{c} 0 < \rho \le 1, \ \rho_i > 0 \text{ for each } i = 1, \ldots, r_1+r_2 \text{ and in the equations} \\ \log\left(\dfrac{\rho_i}{\sqrt[n]{\rho}}\right) = \displaystyle\sum_{q=1}^{r} c_q \log|\epsilon_q^{(i)}|, \quad 1 \le i \le r_1+r_2, \\ \text{the coefficients } c_q \in [0,1) \text{ for } 1 \le q \le r. \end{array}\right\} \tag{9.9}$$

Since these conditions do not impose any restrictions on the coordinates $\phi_{r_1+1}, \ldots, \phi_{r_1+r_2}$, they independently take all values in $[0, 2\pi)$. We now replace $\rho_1, \ldots, \rho_{r_1+r_2}$ by new variables $\rho, c_1, \ldots, c_r$. The set S^{**} is determined by the conditions

$$0 < \rho \le 1, \quad 0 \le c_q < 1, \ \ q = 1, 2, \ldots, r.$$

It is now clear that volume of S^{**} exists. Therefore volume of S exists.

Next we compute the Jacobian of the last transformation. Rewriting the equations mentioned in (9.9), we see that

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

Differentiating the above equations with respect to ρ and c_q, we obtain

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

Therefore the Jacobian $\left|\frac{\partial(\rho_1,\ldots,\rho_{r+1})}{\partial(\rho,c_1,\ldots,c_r)}\right|$ equals the absolute value of the determinant of the matrix

$$\begin{bmatrix} \frac{\rho_1}{n\rho} & \frac{\rho_2}{n\rho} & \cdots & \frac{\rho_{r+1}}{n\rho} \\ \rho_1\log|\epsilon_1^{(1)}| & \rho_2\log|\epsilon_1^{(2)}| & \cdots & \rho_{r+1}\log|\epsilon_1^{(r+1)}| \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \rho_1\log|\epsilon_r^{(1)}| & \rho_2\log|\epsilon_r^{(2)}| & \cdots & \rho_{r+1}\log|\epsilon_r^{(r+1)}| \end{bmatrix} = P \ (say).$$

Keeping in mind that $\prod_{i=1}^{r+1} \rho_i^{e_i} = \rho$, it is clear that

$$\det P = \frac{1}{n \prod_{i=r_1+1}^{r_1+r_2} \rho_i} \det \begin{bmatrix} 1 & 1 & \cdots & 1 \\ \log|\epsilon_1^{(1)}| & \log|\epsilon_1^{(2)}| & \cdots & \log|\epsilon_1^{(r+1)}| \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \log|\epsilon_r^{(1)}| & \log|\epsilon_r^{(2)}| & \cdots & \log|\epsilon_r^{(r+1)}| \end{bmatrix}.$$

Note that if $r_2 = 0$, then $\prod_{i=r_1+1}^{r_1+r_2} \rho_i$ being an empty product equals to 1. Keeping in mind $\sum_{i=1}^{r+1} e_i = n$ and $\sum_{i=1}^{r+1} e_i \log|\epsilon_q^{(i)}| = \log|N_{K/\mathbb{Q}}(\epsilon_q)| = 0$, on multiplying the ith column of the above matrix by e_i for $1 \le i \le r+1$ and adding them to the last column, and then expanding the determinant by the last column, we see that

$$\left| \frac{\partial(\rho_1, \ldots, \rho_{r+1})}{\partial(\rho, c_1, \ldots, c_r)} \right| = \frac{R}{2^{r_2} \prod_{i=r_1+1}^{r_1+r_2} \rho_i}. \tag{9.10}$$

So the volume of S^{**} is given by

$$\begin{aligned} \mathrm{vol}(S^{**}) &= \underbrace{\int \cdots \int}_{S^{**}} dz_1 \cdots dz_n \\ &= (2\pi)^{r_2} \underbrace{\int \cdots \int}_{U} \rho_{r_1+1} \ldots \rho_{r_1+r_2} d\rho_1 \ldots d\rho_{r_1+r_2}, \end{aligned}$$

where U is the subset of $\mathbb{R}^{r_1+r_2}$ consisting of all vectors $(\rho_1, \ldots, \rho_{r_1+r_2})$ satisfying the conditions of (9.9). Keeping in mind (9.10), it follows that

$$\mathrm{vol}(S^{**}) = (\pi)^{r_2} R \int_0^1 \cdots \int_0^1 d\rho dc_1 \ldots dc_r = (\pi)^{r_2} R.$$

Therefore combining the above equation with (9.8), we see that

$$\mathrm{vol}(S) = \frac{2^{r_1+r_2} \pi^{r_2} R}{\sqrt{|d_K|}}.$$

This proves (9.6), which completes the proof of the theorem. □

Theorem 9.2 yields the following corollary.

Corollary 9.4 *Let K be an algebraic number field having class number h and let κ be as in Theorem 9.1. For a positive real number T, if $\mathcal{Z}(T)$ denotes the number of integral ideals of $\mathcal{O}_K$ whose norm does not exceed T. Then*

$$\lim_{T\to\infty} \frac{\mathcal{Z}(T)}{T} = h\kappa.$$

Proof Let $\mathcal{C}_1, \ldots, \mathcal{C}_h$ be the ideal classes of K. Let $\mathcal{Z}(T, \mathcal{C}_i)$ denote the number of integral ideals in $\mathcal{C}_i$ whose norm does not exceed T, then $\mathcal{Z}(T) = \sum_{i=1}^{h} \mathcal{Z}(T, \mathcal{C}_i)$. So by Theorem 9.2,

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

□

9.3 Derivation of Dirichlet's Class Number Formula

For deducing Dirichlet's Class Number Formula from Ideal Theorem, we define Dirichlet series[2] and study their properties.

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

Proposition 9.5 *The series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges for $s > 1$. Its sum function denoted by $\zeta(s)$ (Riemann zeta-function) for $s > 1$ is a continuous function of s in $(1, \infty)$ and $\lim_{s\to 1^+} (s-1)\zeta(s) = 1$.*

Proof When $s > 1$, then $\frac{1}{x^s}$ is a monotonically decreasing function of x in the interval $(0, \infty)$. Therefore for $s > 1$, we have

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

where the above inequality on the left hand side holds for $n \geq 1$ and on the right hand side it holds for $n \geq 2$. Hence for $N > 1$,

[2] The first application of Dirichlet series to number theory was given by Dirichlet in 1937. He used the function $L(s, \chi)$ defined in the next chapter.

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

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

$$\int_1^{\infty} \frac{dx}{x^s} \leq \zeta(s) \leq 1 + \int_1^{\infty} \frac{dx}{x^s}$$

and hence

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

Multiplying throughout by $(s-1)$ and then taking limit as $s \to 1^+$, it follows that $\lim_{s \to 1^+} (s-1)\zeta(s) = 1$.

We now verify that $\zeta(s)$ is a continuous function of s in the region $s > 1$. Fix a positive real number δ. For $s \geq 1 + \delta$, we have $\sum_{n=1}^{\infty} \frac{1}{n^s} \leq \sum_{n=1}^{\infty} \frac{1}{n^{1+\delta}}$. Since the latter series converges, the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges uniformly in $[1+\delta, \infty)$ by Weierstrass M-test. Each term of series is continuous function of s. So its sum function is a continuous function of s in interval $(1+\delta, \infty)$. As this is true for every $\delta > 0$, the proposition is proved. □

Proposition 9.6 *Let $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series. For $n \geq 1$, let P_n stand for $\sum_{j=1}^{n} a_j$. If there exists a non-negative real number σ_0 such that the sequence $\{|\frac{P_n}{n^{\sigma_0}}|\}$ is bounded, then the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges uniformly on each compact subset of (σ_0, ∞) and represents a continuous function of s in (σ_0, ∞).*

Proof Recall that a series is uniformly convergent in a set U if and only if the sequence of its partial sums is uniformly Cauchy in U. Let F_0 be a compact subset of the interval (σ_0, ∞). So F_0 is closed and bounded. Let f_0 denote the greatest lower bound of F_0, then $f_0 \in F_0$. Hence $f_0 > \sigma_0$. So there exists a real number $r > 0$ such that $f_0 \geq \sigma_0 + r$. We now show that the sequence of partial sums of the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is uniformly Cauchy in F_0.

Let b be an upper bound for the sequence $\{|\frac{P_n}{n^{\sigma_0}}|\}$ and u_0 be an upper bound for F_0. Let M, N be any natural numbers with $M > N$. Then for s belonging to F_0, we have

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

Substituting $s \int_n^{n+1} \frac{dx}{x^{s+1}}$ for $\left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right)$ in the above equation, it follows that for s belonging to F_0

$$\begin{aligned}
\left| \sum_{n=N}^{M} \frac{a_n}{n^s} \right| &\leq \frac{bM^{\sigma_0}}{M^s} + \frac{b(N-1)^{\sigma_0}}{N^s} + \sum_{n=N}^{M-1} bn^{\sigma_0} \left[\frac{1}{n^s} - \frac{1}{(n+1)^s} \right] \\
&= \frac{bM^{\sigma_0}}{M^s} + \frac{b(N-1)^{\sigma_0}}{N^s} + \sum_{n=N}^{M-1} sbn^{\sigma_0} \int_n^{n+1} \frac{dx}{x^{s+1}} \\
&\leq \frac{b}{M^{f_0-\sigma_0}} + \frac{b}{N^{f_0-\sigma_0}} + sb \sum_{n=N}^{M-1} \int_n^{n+1} \frac{x^{\sigma_0}}{x^{s+1}} dx \\
&\leq \frac{2b}{N^{f_0-\sigma_0}} + sb \int_N^{\infty} \frac{dx}{x^{s-\sigma_0+1}} = \frac{2b}{N^{f_0-\sigma_0}} + \frac{sb}{s-\sigma_0} \frac{1}{N^{s-\sigma_0}} \\
&\leq \frac{2b}{N^r} + \frac{u_0 b}{r} \frac{1}{N^r}.
\end{aligned}$$

Since $r > 0$, the last expression $\frac{2b}{N^r} + \frac{u_0 b}{r} \frac{1}{N^r}$ tends to 0 as N tends to ∞. We have shown that sequence of partial sum of the series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is uniformly Cauchy in any compact subset F_0 of the interval (σ_0, ∞). So $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is uniformly convergent in every compact subset of F_0. Since each term of the series is continuous in F_0, the sum $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ is continuous function in F_0. □

Theorem 9.7 *Let $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ be a Dirichlet series which converges for $s > 1$ with sum denoted by $f(s)$. For $n \geq 1$, let $P_n = \sum_{j=1}^{n} a_j$. If there is a constant c such that $\lim_{n\to\infty} \frac{P_n}{n} = c$, then $\lim_{s\to 1^+} (s-1) f(s) = c$.*

Proof By Proposition 9.5, $\lim_{s\to 1^+} (s-1)\zeta(s) = 1$. So it is enough to show that

$$\lim_{s\to 1^+} |(s-1) f(s) - c(s-1)\zeta(s)| = 0. \tag{9.11}$$

We first find an estimate for the sequence of partial sums of the series $\sum_{n=1}^{\infty} \frac{a_n - c}{n^s}$. Write $P_n = cn + n\epsilon_n$, then $\epsilon_n \to 0$ as $n \to \infty$. Let $M \geq 2$ be an integer. For $s > 1$, on substituting for P_n, we have

$$\left| \sum_{n=1}^{M} \frac{a_n}{n^s} - c \sum_{n=1}^{M} \frac{1}{n^s} \right| = \left| \sum_{n=1}^{M} \frac{[P_n - P_{n-1} - c]}{n^s} \right|$$
$$= \left| \sum_{n=1}^{M} \frac{[n\epsilon_n - (n-1)\epsilon_{n-1}]}{n^s} \right|.$$

It is now clear that

$$\left| \sum_{n=1}^{M} \frac{a_n}{n^s} - c \sum_{n=1}^{M} \frac{1}{n^s} \right| = \left| \sum_{n=1}^{M-1} n\epsilon_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) + \frac{M\epsilon_M}{M^s} \right|$$
$$\leq \left| \sum_{n=1}^{M-1} n\epsilon_n \left(\frac{1}{n^s} - \frac{1}{(n+1)^s} \right) \right| + \frac{M|\epsilon_M|}{M^s}$$
$$= \left| \sum_{n=1}^{M-1} sn\epsilon_n \int_n^{n+1} \frac{dx}{x^{s+1}} \right| + \frac{|\epsilon_M|}{M^{s-1}};$$

consequently for $s > 1$, we see that

$$\left| \sum_{n=1}^{M} \frac{a_n}{n^s} - c \sum_{n=1}^{M} \frac{1}{n^s} \right| \leq s \sum_{n=1}^{M-1} |\epsilon_n| \int_n^{n+1} \frac{dx}{x^s} + \frac{|\epsilon_M|}{M^{s-1}}. \tag{9.12}$$

Let $\epsilon > 0$ be any given real number. For proving (9.11), we shall show that there exists $\delta > 0$ depending upon ϵ such that for every $s \in (1, 1+\delta)$, we have

$$|(s-1)f(s) - c(s-1)\zeta(s)| < \epsilon. \tag{9.13}$$

Since the sequence $\{\epsilon_n\} \to 0$ as $n \to \infty$, so there exists a natural number N such that $|\epsilon_n| < \frac{\epsilon}{3}$, $\forall\, n \geq N$. Also every convergent sequence is bounded. So there exists k such that $|\epsilon_n| \leq k$ for all n. In view of (9.12), for $M > N$ and $s > 1$, we have

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

Since $\{\epsilon_n\}$ is a bounded sequence and the integral $\int_1^\infty \frac{dx}{x^s}$ is convergent for $s > 1$, upon letting $M \to \infty$, the above inequality yields

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

Therefore

$$\begin{aligned} |f(s) - c\zeta(s)| &\leq s \sum_{n=1}^{N-1} |\epsilon_n| \int_n^{n+1} \frac{dx}{x} + \frac{s\epsilon}{3} \int_N^{\infty} \frac{dx}{x^s} + \frac{\epsilon}{3} \\ &\leq sk \int_1^N \frac{dx}{x} + \frac{s\epsilon}{3} \int_N^{\infty} \frac{dx}{x^s} + \frac{\epsilon}{3} \\ &= sk \log(N) + \frac{s\epsilon}{3(s-1)} \frac{1}{(N)^{s-1}} + \frac{\epsilon}{3}. \end{aligned}$$

Thus we have shown that

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

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

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

Note that the right hand side of above inequality tends to $\frac{\epsilon}{3}$ as $s \to 1^+$. So there exists $\delta > 0$ depending upon ϵ such that for every $s \in (1, 1+\delta)$, we have

$$|(s-1)f(s) - c(s-1)\zeta(s)| < \epsilon.$$

This proves (9.13) and hence the theorem. □

Proof of Theorem 9.1. For any ideal class $\mathcal{C}$ of K, we denote the sum $\sum_{A \in \mathcal{C}} \frac{1}{N(A)^s}$ by $\zeta_K(s, \mathcal{C})$, where A runs over integral ideals of the class $\mathcal{C}$. We shall prove that the above series converges uniformly on all compact subsets of $(1, \infty)$ and

$$\lim_{s \to 1^+} (s-1)\zeta_K(s, \mathcal{C}) = \kappa, \tag{9.14}$$

where κ is as in the statement of the theorem. For any number j, let $f(j, \mathcal{C})$ denote the number of integral ideals in $\mathcal{C}$ having norm j. With this notation, the series $\sum_{A \in \mathcal{C}} \frac{1}{N(A)^s}$

can be rewritten as $\sum_{j=1}^{\infty} \frac{f(j,\mathcal{C})}{j^s}$. If $\mathcal{Z}(n,\mathcal{C})$ stands for the number of integral ideals in $\mathcal{C}$ whose norm does not exceed n, then $\sum_{j=1}^{n} f(j,\mathcal{C}) = \mathcal{Z}(n,\mathcal{C})$. By Theorem 9.2, we have

$$\lim_{n\to\infty} \frac{\mathcal{Z}(n,\mathcal{C})}{n} = \kappa. \tag{9.15}$$

So the sequence $\{\frac{\mathcal{Z}(n,\mathcal{C})}{n}\}$ is bounded and hence by Proposition 9.6, the series $\sum_{j=1}^{\infty} \frac{f(j,\mathcal{C})}{j^s} = \sum_{A\in\mathcal{C}} \frac{1}{N(A)^s}$ converges uniformly on all compact subsets of $(1,\infty)$. Since this is true for each ideal class $\mathcal{C}$ and the number of ideal classes is the finite number h, it follows that the series $\sum_{A} \frac{1}{N(A)^s}$ with A running over all non-zero ideals of $\mathcal{O}_K$, converges uniformly on compact subsets of $(1,\infty)$. Further using (9.15) and Theorem 9.7, we conclude that (9.14) holds. In view of the fact that $\zeta_K(s) = \sum_{\mathcal{C}} \zeta_K(s,\mathcal{C})$ for $s > 1$, formula (9.1) now follows immediately from (9.14). □

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

Proposition 9.8 *(Euler's Product Formula.) Let K be an algebraic number field. Then for $s > 1$*

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}, \tag{9.16}$$

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

Proof For every non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$,

$$\left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = 1 + \frac{1}{N(\mathfrak{p})^s} + \frac{1}{N(\mathfrak{p})^{2s}} + \dots,$$

where the series on the right hand side converges absolutely for $s > 0$. Let M be any natural number and $\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r$ be all the prime ideals of $\mathcal{O}_K$ with norm not exceeding M. So

$$\prod_{\substack{\mathfrak{p}\\ N(\mathfrak{p})\le M}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} = \sum_{k_1,\dots,k_r=0}^{\infty} \frac{1}{N(\mathfrak{p}_1^{k_1}\cdots\mathfrak{p}_r^{k_r})^s};$$

consequently

$$\left| \prod_{\substack{\mathfrak{p} \\ N(\mathfrak{p}) \le M}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1} - \sum_{\substack{A \\ N(A) \le M}} \frac{1}{N(A)^s} \right| \le \sum_{A^*} \frac{1}{N(A^*)^s}, \tag{9.17}$$

where A^* runs over those integral ideals of $\mathcal{O}_K$ whose norm is strictly greater than M but which can be divisible by only those prime ideals whose norm is less than or equal to M. The right hand side of (9.17) being dominated by the tail of a convergent series (namely the series for $\zeta_K(s)$) tends to 0 as $M \to \infty$ when $s > 1$. Hence the result is proved. □

The proof of Proposition 9.8 can be imitated to prove the following proposition which will be used in the next chapter.

Proposition 9.9 *Let $\{a_n\}$ be sequence of complex numbers such that $a_1 = 1$, $|a_m| < 1 \ \forall\ m > 1$ and $a_{mn} = a_m a_n$ for all natural numbers m, n. If $\sum_{m=1}^{\infty} |a_m| < \infty$, then $\sum_{m=1}^{\infty} a_m = \prod_p (1 - a_p)^{-1}$, where p runs over all rational primes.*

Proof Let N be any natural number. Using the hypothesis for the terms a_n, it can be easily seen that

$$\left| \prod_{p \le N} (1 - a_p)^{-1} - \sum_{m=1}^{N} a_m \right| \le \sum_{m^*} |a_{m^*}|,$$

where in the product, p runs over primes not exceeding N and on the right hand side, m^* runs over all those positive integers which are strictly greater than N but whose prime divisors do not exceed N. The series $\sum_{m^*} |a_{m^*}|$ is dominated by $\sum_{m=N+1}^{\infty} |a_m|$ which tends to zero as $N \to \infty$ because $\sum_{m=1}^{\infty} |a_m|$ converges by hypothesis. Therefore the proposition is proved. □

9.4 Applications of Dirichlet's Class Number Formula

The next two theorems are applications of Dirichlet's Class Number Formula.

Theorem 9.10 *An algebraic number field K has infinite number of prime ideals $\mathfrak{p}$ such that the absolute residual degree of $\mathfrak{p}$ is* 1.

Proof For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $f_{\mathfrak{p}}$ denote its absolute residual degree, then $N(\mathfrak{p}) = p^{f_{\mathfrak{p}}}$, where p is the rational prime lying below $\mathfrak{p}$. By Euler's product formula for $s > 1$

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

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

$$\log \zeta_K(s) = \sum_{\mathfrak{p}} \sum_{m=1}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}}. \tag{9.18}$$

The sum on the right hand side of the above equation will be split into two parts. For $s > 1$, define

$$P(s) = \sum_{\mathfrak{p}_1} \frac{1}{N(\mathfrak{p}_1)^s},$$

where $\mathfrak{p}_1$ runs over all those prime ideals of $\mathcal{O}_K$ whose absolute residual degree is 1 and denote the sum of the remaining terms of (9.18) by $G(s)$. Therefore for $s > 1$

$$G(s) = \sum_{\substack{\mathfrak{p} \\ f_{\mathfrak{p}} \geq 2}} \sum_{m=1}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}} + \sum_{\substack{\mathfrak{p} \\ f_{\mathfrak{p}} = 1}} \sum_{m=2}^{\infty} \frac{1}{mN(\mathfrak{p})^{ms}}.$$

So (9.18) is rewritten as

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

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ and p be the rational prime lying below it. If $f_{\mathfrak{p}} \geq 2$, then

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

and if $f_{\mathfrak{p}} = 1$, then

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

Consequently for $s > 1$, we have

$$G(s) \leq \sum_{\mathfrak{p} \mid p} \sum_{p} \frac{2}{p^{2s}},$$

where p runs over all rational primes and $\mathfrak{p}$ runs over prime ideals of $\mathcal{O}_K$.

In view of the fundamental equality proved in Chap. 4, for any rational prime p there exist at most n prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ which lie over p, where n is the degree of $K/\mathbb{Q}$. Thus for $s > 1$

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

By Proposition 9.5, $\zeta(s)$ is a continuous function of s in the interval $(1, \infty)$. Therefore in view of the above inequality, $G(s)$ is bounded when $s \to 1^+$. By Dirichlet's Class number formula, we know that $\lim_{s \to 1^+} (s-1)\zeta_K(s) = h\kappa \neq 0$, which implies $\zeta_K(s) \to \infty$ as $s \to 1^+$; consequently $\log \zeta_K(s) \to \infty$ as $s \to 1^+$. But $\log \zeta_K(s) = P(s) + G(s)$, and $G(s)$ remains bounded as $s \to 1^+$. So $P(s) \to \infty$ as $s \to 1^+$ and hence there are infinitely many terms in the sum for $P(s)$. Therefore there are infinitely many prime ideals with absolute residual degree 1. □

The following results are interesting applications of the above theorem.

Theorem 9.11 *Let $K \subseteq K'$ be algebraic number fields. Then there are infinitely many prime ideals of $\mathcal{O}_K$ which split completely in K'.*

Proof Let L be a finite normal extension of $\mathbb{Q}$ containing K'. Note that if a rational prime p splits completely in L, then each prime ideal of $\mathcal{O}_K$ lying over p splits completely in K'. So it is enough to prove that there are infinitely many rational primes which split completely in L. Since $L/\mathbb{Q}$ is a finite Galois extension, the absolute residual degree of all prime ideals of $\mathcal{O}_L$ which lie over a given rational prime p is the same in view of Theorem 4.3; let f_p denote this residual degree. Note that in view of the fundamental equality, a rational prime p splits completely in L if and only if $f_p = 1$ and p is unramified in L. Recall that all but finitely many rational primes are unramified in L in view of Theorem 4.16. By Theorem 9.10, there are infinitely many prime ideals of $\mathcal{O}_L$ which have absolute residual degree 1. Keeping in mind the fact that there are at most $[L : \mathbb{Q}]$ prime ideals of $\mathcal{O}_L$ lying over a given rational prime p, it now follows that there are infinitely many rational primes which split completely in L. □

Corollary 9.12 *Let $F(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial. Then there are infinitely many primes p for which the reduction of $F(X)$ modulo p factors into linear factors over $\mathbb{Z}/p\mathbb{Z}$.*

Proof Let $K = \mathbb{Q}(\theta)$, where θ is a root of $F(X)$. In view of Theorem 9.11, there are infinitely many rational primes p which split completely in K. The corollary now follows, because in view of Theorem 4.8, a prime p which does not divide the index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ splits completely in K if and only if the reduction of $F(X)$ modulo p factors into distinct monic linear factors over $\mathbb{Z}/p\mathbb{Z}$. □

The following result is a particular case of the above corollary.

Corollary 9.13 *Given any integer a which is not a perfect square, there exist infinitely many rational primes p such that $\left(\frac{a}{p}\right) = 1$.*

The above corollary gives rise to the following natural question: Given an integer a which is not a perfect square, are there infinitely many rational primes p such that $\left(\frac{a}{p}\right) = -1$? The answer is given by the following theorem which we prove using Dirichlet's class number formula.

Theorem 9.14 *Given any integer a which is not a perfect square, there exist infinitely many rational primes p such that $\left(\frac{a}{p}\right) = -1$.*

Proof Write $a = b^2 d$ where b, d are integers and d is squarefree. So we have to prove that there exist infinitely many rational primes p such that $\left(\frac{d}{p}\right) = -1$. Suppose the result is false. Let D denote the discriminant of the field $K = \mathbb{Q}(\sqrt{d})$ and $\left(\frac{D}{p}\right)$ stand for the Legendre or Kronecker symbol according as p is odd or even prime. Let $\mathcal{P}$ denote the set of primes p for which $\left(\frac{D}{p}\right) = -1$ and $\mathcal{P}_1$ denote the set of primes p for which $\left(\frac{D}{p}\right) = +1$. By Euler's product formula,

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

for $s > 1$, where $\mathfrak{p}$ runs over all non-zero prime ideals of $\mathcal{O}_K$. By Theorem 4.11, if $p \in \mathcal{P}_1$, then there are two prime ideals of $\mathcal{O}_K$ lying over p each having norm p and for $p \in \mathcal{P}$, there exists only one prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p having $N(\mathfrak{p}) = p^2$. When p divides D, then there is only one prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p and $N(\mathfrak{p}) = p$. So the above product formula shows that for $s > 1$,

$$\zeta_K(s) = \prod_{p \in \mathcal{P}_1} \left(1 - \frac{1}{p^s}\right)^{-2} \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^{2s}}\right)^{-1} \prod_{p \mid D} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{9.19}$$

Recall that $\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ for $s > 1$, where p runs over all rational primes. Keeping in mind the assumption that $\mathcal{P}$ is a finite set, Eq. (9.19) for $s > 1$ can be rewritten as

$$\zeta_K(s) = \zeta(s)^2 \prod_{p \in \mathcal{P}} \left(1 + \frac{1}{p^s}\right)^{-1} \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right) \prod_{p \mid D} \left(1 - \frac{1}{p^s}\right).$$

By Proposition 9.5, $\lim_{s\to 1^+}(s-1)\zeta(s)=1$. So the above equation shows that

$$\lim_{s\to 1^+}(s-1)^2\zeta_K(s)=\prod_{p\in\mathcal{P}}\left(1+\frac{1}{p}\right)^{-1}\prod_{p\in\mathcal{P}}\left(1-\frac{1}{p}\right)\prod_{p\mid D}\left(1-\frac{1}{p}\right);$$

the expression on the right hand side is non-zero being a finite product of non-zero terms. On the other hand, by Dirichlet's class number formula, $\lim_{s\to 1^+}(s-1)^2\zeta_K(s)=0$. This contradiction proves the theorem.

□

Exercises

1. Give a simplified version of the proof of Theorem 9.2 when K is an imaginary quadratic field.
2. Let K be a real quadratic field with discriminant d_K and let $\varepsilon>1$ be the fundamental unit of K. Let $\mathcal{C}$ be an ideal class of K. For a positive real number T, let $\mathcal{Z}(T,\mathcal{C})$ be the number of integral ideals in $\mathcal{C}$ whose norm is less than or equal to T. Prove that
$$\lim_{T\to\infty}\frac{\mathcal{Z}(T,\mathcal{C})}{T}=\frac{2\log\varepsilon}{\sqrt{|d_K|}}.$$
3. Prove that $\log\zeta(s)-\sum_p\frac{1}{p^s}$ remains bounded as $s\to 1^+$, where p runs over all prime numbers.
4. Let $F(X)\in\mathbb{Z}[X]$ be a monic irreducible polynomial. Prove that there are infinitely many primes p for which $F(X)\equiv 0 \pmod p$ has a solution in $\mathbb{Z}$.
5. Calculate $\lim_{s\to 1^+}(s-1)\zeta_K(s)$ when K is one of the following fields:
   (i) $\mathbb{Q}(\sqrt{-1})$;
   (ii) $\mathbb{Q}(\sqrt{3})$;
   (iii) $\mathbb{Q}(\sqrt{6})$.
6. For any algebraic number field K, prove that the sum $\sum_{\mathfrak{p}}\frac{1}{N(\mathfrak{p})^s}$ converges for $s>1$, where $\mathfrak{p}$ runs over all non-zero prime ideals of $\mathcal{O}_K$.
7. Prove that for $s>1$,
$1-\frac{1}{2^s}+\frac{1}{3^s}-\frac{1}{4^s}+\cdots=(1-2^{1-s})\zeta(s)$.
8. For an algebraic number field K, let $\nu(n)$ denote the number of integral ideals of $\mathcal{O}_K$ with norm n. Prove that if m,n are coprime numbers, then $\nu(mn)=\nu(m)\nu(n)$.

9. Compute the first ten terms ($1 \leq n \leq 10$) of the series $\sum_{n=1}^{\infty} \frac{\nu(n)}{n^s}$, when K is one of the following fields:

   (i) $\mathbb{Q}(\sqrt{-3})$;
   (ii) $\mathbb{Q}(\sqrt{11})$;
   (iii) $\mathbb{Q}(e^{\frac{2\pi i}{9}})$;
   (iv) $\mathbb{Q}(e^{\frac{2\pi i}{15}})$.

10. Let K be an algebraic number field. For any positive integer n, let $\nu(n)$ denote the number of integral ideals of $\mathcal{O}_K$ with norm n. Prove that for $s > 1$, $\zeta_K(s)/\zeta(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$ with $c_n = \sum_{d|n} \mu(d)\nu(\frac{n}{d})$, where μ is the Möbius function defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^r & \text{if } n \text{ is a product of } r \text{ distinct primes}, \\ 0 & \text{otherwise.} \end{cases}$$

Chapter 10
Simplified Class Number Formula for Cyclotomic, Quadratic Fields

10.1 Numerical Characters and L-functions

In this chapter, we give a simplified version of Dirichlet's Class Number Formula for cyclotomic and quadratic fields using special kind of Dirichlet's series called L-functions attached to numerical characters and derive Dirichlet's Theorem for primes in arithmetic progressions. We first define these notions and prove some basic results regarding characters of finite abelian groups.

Definition. Let G be a finite abelian group. By a character χ of G, we mean a homomorphism $\chi : G \longrightarrow \{z : |z| = 1, z \in \mathbb{C}\}$. If G has order n and e is the identity of G, then for $x \in G$, $x^n = e$ which implies that $\chi(x)^n = \chi(x^n) = \chi(e) = 1$. So $\chi(G)$ is contained in the group of nth root of unity.

Note that if G is a cyclic group of order m generated by a, then G has exactly m characters $\chi_0, \ldots, \chi_{m-1}$, defined by $\chi_i(a) = \epsilon^i$, where ϵ is a fixed primitive mth root of unity. In fact this is true for every finite abelian group as asserted by the following proposition.

Proposition 10.1 *The number of characters of a finite abelian group equals the order of the group.*

Proof We can write $G = \prod_{i=1}^{s} G_i$ as a direct product of cyclic groups. Suppose G_i is generated by a_i and G_i has order m_i. Any element $x \in G$ is of the form

$$x = a_1^{k_1} a_2^{k_2} \cdots a_s^{k_s}. \tag{10.1}$$

So a character of G is completely determined if we define $\chi(a_1), \ldots, \chi(a_s)$. Since $a_i^{m_i}$ is the identity of G, so $\chi(a_i)$ is an (m_i)th root of unity. Conversely let ϵ_i be an (m_i)th root of unity, then for any $x \in G$ given by (10.1), we can define

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8_10

$$\chi(x) = \epsilon_1^{k_1}\epsilon_2^{k_2}\cdots\epsilon_s^{k_s} \tag{10.2}$$

and this is well defined because the right hand side of (10.2) is independent of the choice of k_i (which are unique modulo m_i). Each root ϵ_i can be chosen in m_i ways. So there are $m_1 m_2 \cdots m_s$ characters of G. □

Observe that the set of all characters of a finite abelian group is a group under usual multiplication of mappings. This group is called the character group of a finite abelian group G.

Proposition 10.2 *If G is a finite abelian group and H is a subgroup, then any character of H can be extended to a character of G and the number of such extensions equals the index of H in G.*

Proof Let G be of order n and H be of order m. When we restrict a character χ of G to H, we obtain a character of H. It is clear that the map Λ sending χ to the restriction map $\chi|_H$ is a homomorphism from the character group $\widehat{G}$ of G into the character group $\widehat{H}$ of H. Note that $\chi \in \ker(\Lambda)$ if and only if $\chi(g) = 1$ for all $g \in H$. It can be easily verified that the group $\ker(\Lambda)$ is in one-to-one correspondence with the group of characters of G/H. Thus by the previous proposition $|\ker(\Lambda)| = |G/H| = \frac{n}{m}$. By the first isomorphism theorem of groups, $\widehat{G}/\ker(\Lambda) \cong \Lambda(\widehat{G})$. So order of $\Lambda(\widehat{G}) = m$. But $\widehat{H}$ has order m. Thus $\Lambda(\widehat{G}) = \widehat{H}$ which implies that Λ is onto. Therefore, given any character of H, it can be extended to a character of G and the number of such extensions equals $\frac{n}{m}$. □

Corollary 10.3 *Let G be a finite abelian group. If $g \neq e$, $g \in G$, then there exists a character χ of G such that $\chi(g) \neq 1$.*

Proof Let H be the subgroup of G generated by g, then $H \neq \{e\}$. Let ψ be a non-trivial character of H, so that $\psi(g) \neq 1$. By Proposition 10.2, we can extend the character ψ of H to a character χ of G. So $\chi(g) = \psi(g) \neq 1$. □

Proposition 10.4 *Let G be a finite abelian group of order n with identity e. Let $\widehat{G}$ be the character group of G with identity χ_0. Then the following hold.*

(i) *For $\chi \in \widehat{G}$, $\sum_{g\in G} \chi(g)$ equals n if $\chi = \chi_0$ and 0 otherwise.*

(ii) *For $g \in G$, $\sum_{\chi\in\widehat{G}} \chi(g)$ equals n if $g = e$ and 0 otherwise.*

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

(ii) If $g = e$, then clearly $\sum_{\chi\in\widehat{G}} \chi(g) = |\widehat{G}| = n$. If $g \neq e$, then by Corollary 10.3, there exists a character χ' of G such that $\chi'(g) \neq 1$. As χ runs over all the elements of

$\widehat{G}$, so does $\chi\chi'$. Thus $\sum_{\chi\in\widehat{G}} \chi(g) = \sum_{\chi\in\widehat{G}} \chi\chi'(g) = \chi'(g) \sum_{\chi\in\widehat{G}} \chi(g)$. Since $\chi'(g) \neq 1$, we have $\sum_{\chi\in\widehat{G}} \chi(g) = 0$. □

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

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

Such a function χ^* defined on $\mathbb{Z}$ is called a numerical character modulo m. So a function $\chi^* : \mathbb{Z} \longrightarrow \mathbb{C}$ is called a numerical character modulo m if it has the following properties:

(i) $\chi^*(ab) = \chi^*(a)\chi^*(b)$ for all $a, b \in \mathbb{Z}$,
(ii) $\chi^*(a) = 0$ if and only if $(a, m) > 1$,
(iii) $\chi^*(a) = \chi^*(a')$ if $a \equiv a' \pmod{m}$.

In view of Proposition 10.1, the number of numerical characters modulo m is $\phi(m)$. In future, we shall denote the numerical character χ^* corresponding to a character χ of G_m by χ again. Corresponding to the trivial character χ_0 of G_m, we shall denote again by χ_0, the numerical character modulo m which is defined by

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

It will be called the principal character modulo m.

Remark 10.5 If χ is a numerical character modulo m and $\chi \neq \chi_0$, then in view of the first assertion of Proposition 10.4, $\sum_g \chi(g) = 0$, where g runs over a reduced residue system or a complete residue system modulo m. Further for any positive integer n, $\left| \sum_{j=1}^{n} \chi(j) \right| \leq m - 1$. To verify this, for a fixed n write by division algorithm $n = mq + r, 0 \leq r < m$. For an integer i, let T_i denote the set $\{im + 1, im + 2, \ldots, (i + 1)m\}$ consisting of m consecutive integers. Then T_i represents a complete residue system modulo m. So $\sum_{x\in T_i} \chi(x) = 0$. Thus $\sum_{x=1}^{mq} \chi(x) = \sum_{i=0}^{q-1} \sum_{x\in T_i} \chi(x) = 0$. Therefore $\sum_{j=1}^{n} \chi(j) = \sum_{j=mq+1}^{mq+r} \chi(j)$. Hence $\left| \sum_{j=1}^{n} \chi(j) \right| \leq \sum_{j=mq+1}^{mq+r} |\chi(j)| \leq r \leq m - 1$.

Proposition 10.6 *Let $\chi \neq \chi_0$ be a numerical character modulo m, then the series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges uniformly on all the compact subsets of $(0, \infty)$ and represents a continuous function of s in $(0, \infty)$. The convergence of the series is absolute when $s \in (1, \infty)$.*

Proof Let P_n be a sequence defined by $P_n = \sum_{j=1}^{n} \chi(j)$. In view of the above remark, $|P_n| \leq m - 1$ for each $n \geq 1$. So P_n is a bounded sequence. It now follows from Proposition 9.6 that $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges uniformly on compact subsets of $(0, \infty)$ and represents a continuous function of s in $(0, \infty)$. Since the series $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converges for $s > 1$, we see that the series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ converges absolutely for $s > 1$. □

Definition. For a numerical character χ modulo m, we denote the sum of the series $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$ by $L(s, \chi)$ whenever it converges and its sum function is called L-function attached with character χ. Applying Proposition 9.9 (with $a_n = \frac{\chi(n)}{n^s}$), we see that for $s > 1$

$$\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}, \tag{10.3}$$

where the product in the above equation is taken over all rational primes p.

10.2 Simplification of Class Number Formula for Cyclotomic Fields

Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive mth root of unity, $m \geq 3$. We want to simplify Dirichlet's Class Number Formula for K. Keeping in mind that K has no real isomorphism and Dirichlet's Class Number formula given by (9.1), we have

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

where h is the class number of K, R is the regulator of K and w is the number of roots of unity contained in K. In view of Lemma 8.30, $w = m$ or $2m$ according as m is even or odd. By Euler's Product formula, $\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$ for s > 1, where $\mathfrak{p}$ runs over all non-zero prime ideals of $\mathcal{O}_K$. We shall first write the above product in a clear manner.

For $s > 0$, define $G(s) = \prod_{p|m} \prod_{\mathfrak{p}|p} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$. If $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ lying over a rational prime p not dividing m, then we denote the absolute residual degree of $\mathfrak{p}$ by f_p, it is independent of the choice of $\mathfrak{p}$ lying over p in view of Theorem 4.3. In fact f_p is the smallest positive integer such that $p^{f_p} \equiv 1 \pmod{m}$ by Theorem 4.13. Also the number of distinct prime ideals $\mathfrak{p}$ of $\mathcal{O}_K$ lying over p is $\frac{\phi(m)}{f_p}$. Thus for $s > 1$, we can write

$$\zeta_K(s) = G(s) \prod_{p \nmid m} \left(1 - \frac{1}{p^{sf_p}}\right)^{-\frac{\phi(m)}{f_p}}. \tag{10.4}$$

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

$$(1 - p^{-sf_p})^{\frac{\phi(m)}{f_p}} = \prod_{k=0}^{f_p-1} (1 - \epsilon^k p^{-s})^{\frac{\phi(m)}{f_p}}. \tag{10.5}$$

Clearly the number of factors on the right hand side of the above equation is $\phi(m)$, which is independent of p. Thus if we wish to combine terms corresponding to different rational primes p, then we have the same number of terms available to us.

Let χ be any character of the group G_m of reduced residue classes modulo m. Since the class $\bar{p}$ has order f_p in the group G_m, $\chi(\bar{p})$ is an (f_p)th root of unity and hence $\chi(\bar{p}) = \epsilon^k$ for some k, $0 \le k \le f_p - 1$, $\epsilon = e^{\frac{2\pi\iota}{f_p}}$. Conversely if ϵ^k is taken, then there exists exactly one character χ_1 of the cyclic group generated by $\bar{p}$ such that $\chi_1(\bar{p}) = \epsilon^k$. Extend χ_1 to a character of G_m and this can be done in exactly $\frac{\phi(m)}{f_p}$ ways by Proposition 10.2. Thus as χ runs through all characters of G_m, $\chi(\bar{p})$ takes each value ϵ^k, $0 \le k \le f_p - 1$, exactly $\frac{\phi(m)}{f_p}$ times. Therefore it follows from (10.4), (10.5) that for $s > 1$, we have

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

where χ runs over all the characters of G_m. Now let us denote the numerical character modulo m which corresponds to χ again by χ. Since $\chi(p) = 0$ if $p \mid m$ by the

definition of numerical character, we see that $\zeta_K(s) = G(s)\prod_p\prod_\chi\left(1-\frac{\chi(p)}{p^s}\right)^{-1}$ for $s>1$, where χ runs over all numerical characters modulo m and p runs over all primes. Therefore keeping in mind (10.3), it follows that for $s>1$,

$$\zeta_K(s) = G(s)\prod_\chi\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1} = G(s)\prod_\chi L(s,\chi), \tag{10.6}$$

where χ runs over all numerical characters modulo m. If $\chi=\chi_0$ is the principal character modulo m, then for $s>1$

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

because $\zeta(s) = \prod_p\left(1-\frac{1}{p^s}\right)^{-1}$ by Euler's product formula. Thus we have shown that for $s>1$

$$\zeta_K(s) = F(s)\zeta(s)\prod_{\chi\neq\chi_0} L(s,\chi), \tag{10.7}$$

where

$$F(s) = \prod_{p\mid m}\left(1-\frac{1}{p^s}\right)\prod_{p\mid m}\prod_{\mathfrak{p}\mid p}\left(1-\frac{1}{N(\mathfrak{p})^s}\right)^{-1}. \tag{10.8}$$

On multiplying both sides of (10.7) by $s-1$ and taking limit as $s\longmapsto 1^+$, it follows from Theorem 9.1 and Proposition 10.6 that the class number h of $K=\mathbb{Q}(\zeta)$ satisfies

$$h\kappa = F(1)\prod_{\chi\neq\chi_0} L(1,\chi), \quad \text{where} \quad \kappa = \frac{2^{\frac{\phi(m)}{2}}\pi^{\frac{\phi(m)}{2}}R}{w\sqrt{|d_K|}},$$

with R the regulator K, w the number of roots of unity in K and $L(1,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}$.

Keeping in mind that w is m or $2m$ according as m is even or odd in view of Lemma 8.30, we have proved the following theorem.

Theorem 10.7 *Let $K=\mathbb{Q}(\zeta)$ where ζ is a primitive mth root of unity, $m\geq 3$. Let R denote the regulator of K, then the class number h of K is given by*

$$h = \frac{w\sqrt{|d_K|}}{(2\pi)^{\frac{\phi(m)}{2}}R}F(1)\prod_{\chi\neq\chi_0} L(1,\chi)$$

where $|d_K|$ is explicitly given by Theorem 2.31, χ runs over all non- principal numerical characters modulo m, $w = m$ or $2m$ according as m is even or odd and $F(s)$ is defined by (10.8) for $s > 0$.

The following corollary is an immediate consequence of the above theorem.

Corollary 10.8 *If χ is a non-principal numerical character modulo m, then $L(1, \chi)$ is non-zero.*

The corollary stated below is a particular case of Theorem 10.7.

Corollary 10.9 *Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive pth root of unity, p an odd prime. Then the class number h_p of K is given by $h_p = \frac{2p^{(p/2)}}{(2\pi)^{\frac{p-1}{2}} R} \prod_{\chi \neq \chi_0} L(1, \chi)$, where R is the regulator of K and χ runs over all non-principal numerical characters modulo p.*

10.3 Dirichlet's Theorem for Primes in Arithmetic Progressions

Using Corollary 10.8, we now prove a celebrated theorem due to Dirichlet. The theorem in the form given below was first conjectured by Gauss and proved by Dirichlet in 1837 using L-functions.

Theorem 10.10 *(*Dirichlet's Theorem for primes in A.P). *Let $m \geq 2$ be an integer. For any integer a coprime with m, the arithmetic progression a, $a + m$, $a + 2m$, $a + 3m, \ldots$ contains infinitely many primes.*

Proof The theorem is obvious when $m = 2$. Thus we shall assume that $m \geq 3$. Fix an integer a' such that $a'a \equiv 1 \pmod{m}$ (which exists since a is relatively prime to m). Then $\overline{\chi(a)} = \frac{1}{\chi(a)} = \chi(a')$, where χ is a numerical character modulo m. So by Proposition 10.4, we obtain the following "orthogonality relation"

$$\sum_{\chi} \overline{\chi(a)}\chi(b) = \sum_{\chi} \chi(a'b) = \begin{cases} \phi(m) & \text{if } a'b \equiv 1 \pmod{m}, \text{ i.e., } a \equiv b \pmod{m}, \\ 0 & \text{otherwise,} \end{cases}$$

where χ in both the summations varies over all the numerical characters modulo m. Now let $s > 1$ and let χ be a numerical character modulo m. Then, in view of (10.3),

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

where the product is over all primes p. Taking log of both sides, we see that

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

Summing both sides of the above equality as χ varies over all the numerical characters modulo m, and using the above "orthogonality relation", we obtain

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

Splitting the last summation on positive integers n satisfying $p^n \equiv a \pmod m$ according as $n = 1$ or $n \geq 2$, we see that

$$\sum_{\chi} \overline{\chi(a)} \log L(s,\chi) = \phi(m) \sum_{\substack{p \\ p\equiv a \pmod m}} \frac{1}{p^s} + \phi(m) \sum_{p} \sum_{\substack{n\geq 2 \\ p^n \equiv a \pmod m}} \frac{1}{np^{ns}}. \quad (10.9)$$

We shall show that the second sum on the right hand side of (10.9) remains bounded for $s > 1$, whereas the sum on the left hand side tends to ∞ as $s \to 1^+$. This would imply that $\sum_{p\equiv a \pmod m} \frac{1}{p^s} \to \infty$ as $s \to 1^+$ and hence the theorem will be proved. The boundedness of the second sum on the right hand side of (10.9) for $s > 1$ follows since

$$\sum_{p} \sum_{\substack{n\geq 2 \\ p^n \equiv a \pmod m}} \frac{1}{np^{ns}} \leq \sum_{p}\sum_{n=2}^{\infty} \frac{1}{p^{ns}} \leq \sum_{p}\sum_{n=2}^{\infty} \frac{1}{p^n} = \sum_{p} \frac{1}{p(p-1)} \leq \zeta(2).$$

It only remains to prove that the sum on the left hand side of (10.9) tends to ∞ as $s \to 1^+$. Recall that by Proposition 10.6 for $\chi \neq \chi_0$, $L(s,\chi)$ is continuous in $(0,\infty)$ and $L(s,\chi)$ does not vanish in $(1,\infty)$ by virtue of infinite product formula (10.3). Also in view of Corollary 10.8, $L(1,\chi) \neq 0$ for a non-principal numerical character χ modulo m; consequently $\lim_{s\to 1^+} \log L(s,\chi) = \log L(1,\chi)$ is finite. On the other hand, in view of Euler's product formula, $L(s,\chi_0) = \zeta(s) \prod_{p|m} \left(1 - \frac{1}{p^s}\right)$ for $s > 1$, we see that

$$\log L(s,\chi_0) = \log \zeta(s) + \sum_{p|m} \log\left(1 - \frac{1}{p^s}\right).$$

Now by Proposition 9.5, $\log \zeta(s)$ tends to ∞ when $s \to 1^+$. Hence so does $\log L(s,\chi_0)$. This proves the desired assertion. □

10.4 Jacobi-Kronecker Symbol and Character Associated with a Quadratic Field

To simplify Dirichlet's Class Number Formula for quadratic fields, we shall use Legendre symbol, Kronecker symbol and Jacobi-Kronecker symbol (cf. [Niv, Chapter 3], [Es-Mu, Chapter 7]). The first two symbols have already been defined in Sect. 4.3. We first recall some properties of Legendre symbol and then we give definition of Jacobi symbol, Jacobi-Kronecker symbol along with their basic properties.

Legendre symbol satisfies the following properties for an odd prime p:

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

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

(iii) $\left(\frac{-1}{p}\right) = (-1)^{\frac{(p-1)}{2}}$

(iv) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

(v) **Gauss' Reciprocity Law.**[1] If p, q are distinct odd primes, then $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

The lemma stated below can be easily proved by using induction on k. Its proof is omitted.

Lemma 10.11 *Let $n_1, n_2, \ldots, n_k$ be odd integers, then the following hold.*

(i) $(\prod_{i=1}^{k} n_i) - 1 \equiv \sum_{i=1}^{k}(n_i - 1) \pmod 4$.

(ii) $(\prod_{i=1}^{k} n_i^2) - 1 \equiv \sum_{i=1}^{k}(n_i^2 - 1) \pmod{16}$.

Definition (Jacobi Symbol). Let m be a positive odd integer having prime factorization $\prod_{i=1}^{r} p_i$, where $p_1, p_2, \ldots, p_r$ are primes not necessarily distinct and n be an integer. The Jacobi symbol $\left(\frac{n}{m}\right)$ is defined to be $\prod_{i=1}^{r}\left(\frac{n}{p_i}\right)$.

Note that if the congruence $x^2 \equiv n \pmod m$ is solvable and $(n, m) = 1$, then the Jacobi symbol $\left(\frac{n}{m}\right) = 1$. The converse is false, e.g. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = 1$ but $x^2 \equiv 2 \pmod{15}$ is not solvable.

[1] This is also known as the Quadratic Reciprocity law for Legendre symbol. It was conjectured by Euler and Legendre and first proved by Gauss, who referred to it as the "fundamental theorem" in Disquisitiones Arithmeticae and in his papers. During his life time he published six proofs for it, and two more were found in his posthumous papers.

Using properties of Legendre symbol and Lemma 10.11, one can quickly verify the following properties of Jacobi symbol, m being a positive odd integer.

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

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

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

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

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

(vi) **Reciprocity law for Jacobi symbol.** If m and n are positive odd relatively prime integers, then $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{(m-1)(n-1)}{4}}$.

Definition (Generalized Jacobi symbol). If m is a negative odd integer, then for any integer a, the generalized Jacobi symbol $\left(\frac{a}{m}\right)$ is defined to be $\left(\frac{a}{|m|}\right)$.

Let m, n be odd integers which are coprime. Let $sgn(m)$ stand for $+1$ or -1 according as $m > 0$ or $m < 0$. The following properties can be quickly verified using the above properties of Jacobi symbol.

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

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

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

The last formula (III) is known as the reciprocity law for generalized Jacobi symbol. Note that reciprocity law for generalized Jacobi symbol remains the same as the one for Jacobi symbol when at least one of m or n is positive.

Definition.(Jacobi-Kronecker symbol) Let $a \equiv 0$ or $1 \pmod 4$ be an integer and let n be any non-zero integer. We write $n = n_1 2^c$, where $2 \nmid n_1$, the Jacobi-Kronecker symbol is defined by $\left(\frac{a}{n}\right) = \left(\frac{a}{n_1}\right)\left(\frac{a}{2}\right)^c$, where $\left(\frac{a}{n_1}\right)$ is generalized Jacobi symbol and $\left(\frac{a}{2}\right)$ is Kronecker symbol given by $\left(\frac{a}{2}\right) = 0$ or $(-1)^{\frac{a^2-1}{8}}$ according as $a \equiv 0$ or $1 \pmod 4$.

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

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

Then χ is called the character associated with the quadratic field $\mathbb{Q}(\sqrt{d})$.

We now prove that χ is a numerical character modulo $|D|$. For this it is to be shown that

(i) $\chi(xy) = \chi(x)\chi(y)$ for all $x, y \in \mathbb{Z}$.
(ii) If $x \equiv x' \pmod{|D|}$, then $\chi(x) = \chi(x')$.

Clearly (i) needs to be verified only when $(xy, D) = 1$. We distinguish three cases.

Case 1. $d \equiv 1 \pmod 4$.
In this case,

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

Case 2. $d \equiv 3 \pmod 4$.
Then $\chi(xy) = (-1)^{\frac{xy-1}{2}} \left(\frac{xy}{|d|}\right)$. By Lemma 10.11, $\frac{xy-1}{2} \equiv \frac{x-1}{2} + \frac{y-1}{2} \pmod 2$. This implies that $(-1)^{\frac{xy-1}{2}} = (-1)^{\frac{x-1}{2}}(-1)^{\frac{y-1}{2}}$. Thus $\chi(xy) = (-1)^{\frac{x-1}{2}}(-1)^{\frac{y-1}{2}} \left(\frac{x}{|d|}\right) \left(\frac{y}{|d|}\right) = \chi(x)\chi(y)$.

Case 3. $d = 2d'$, d' odd.
In the present case,

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

By Lemma 10.11, $\frac{x^2y^2-1}{8} \equiv \frac{x^2-1}{8} + \frac{y^2-1}{8} \pmod 2$ and $\frac{xy-1}{2} \equiv \frac{x-1}{2} + \frac{y-1}{2} \pmod 2$. Therefore

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

To verify (ii), we again distinguish three cases and assume that $(x, D) = 1$.

Case 1. $d \equiv 1 \pmod 4$.
Then $D = d$ and

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

Case 2. $d \equiv 3 \pmod 4$.
In this case, $D = 4d$ and $\chi(x') = (-1)^{\frac{x'-1}{2}} \left(\frac{x'}{|d|}\right)$. Since $x \equiv x' \pmod{|D|}$ we have $x \equiv x' \pmod 4$ and $x \equiv x' \pmod{|d|}$. Thus $\chi(x') = (-1)^{\frac{x'-1}{2}} \left(\frac{x'}{|d|}\right) = (-1)^{\frac{x-1}{2}} \left(\frac{x}{|d|}\right) = \chi(x)$.

Case 3. $d = 2d'$, d' odd.
Here $D = 4d = 8d'$. Since $x \equiv x' \pmod{|D|}$, we have $x \equiv x' \pmod{|d'|}$. Therefore $\left(\frac{x}{|d'|}\right) = \left(\frac{x'}{|d'|}\right)$. Also $x \equiv x' \pmod 8$ which implies that $\frac{x-1}{2} \equiv \frac{x'-1}{2} \pmod 2$ and $\frac{x^2-1}{8} \equiv \frac{x'^2-1}{8} \pmod 2$. Thus $\chi(x) = \chi(x')$.

The following proposition describes χ on positive integers.

Proposition 10.12 *Let K be a quadratic field having discriminant D. Let χ be the character associated with K. Then $\chi(x) = \left(\frac{D}{x}\right)$ for every positive integer x, where $\left(\frac{D}{x}\right)$ is the Jacobi-Kronecker symbol.*

Proof The desired equality needs to be proved when $(x, D) = 1$. Write $K = \mathbb{Q}(\sqrt{d})$ with d a squarefree integer. The proof is divided into three cases.

Case 1. $d \equiv 1 \pmod 4$. This case is split into three subcases :

Subcase (1.1). x is odd.
By reciprocity law for generalized Jacobi symbol, we have

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

Subcase (1.2). $x = 2^r y$ with r even and y odd.
Using reciprocity law for generalised Jacobi symbol, we see that

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

By definition,

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

Hence $\chi(x) = \left(\dfrac{D}{x}\right)$.
Subcase (1.3). $x = 2^r y$, with r, y odd.
Using the fact that $\left(\dfrac{d}{2}\right) = \left(\dfrac{2}{d}\right) = (-1)^{\frac{d^2-1}{8}}$ together with the reciprocity law, we have

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

the last equality holds because r is odd. Thus we have shown that

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

Case 2. $d \equiv 3 \pmod 4$.
For x odd, we have

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

Case 3. $d = 2d'$, d' odd.
For x odd, we have

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

□

The above proposition yields the following corollary.

Corollary 10.13 *Let $\mathbb{Q}(\sqrt{D})$ be a quadratic field with discriminant D and let χ be the character associated with $\mathbb{Q}(\sqrt{D})$. Then $\chi(p) = \left(\dfrac{D}{p}\right)$ for all primes p.*

10.5 Simplified Class Number Formula for Quadratic Fields

Using Corollary 10.13, we now prove

Theorem 10.14 *Let K be a quadratic field with discriminant D and χ be the numerical character modulo $|D|$ associated with K. Then the class number h of K is given by*

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

where $\epsilon > 1$ is the fundamental unit of K in case $D > 0$ and m is the number of roots of unity in K.

Proof In view of Theorem 4.11 and Euler's product formula, we have for $s > 1$

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

The numerical character χ associated with $\mathbb{Q}(\sqrt{D})$ is non-principal by virtue of the following Lemma 10.16. By Corollary 10.13, for each prime p, we have $\chi(p) = \left(\dfrac{D}{p}\right)$. Thus for $s > 1$, we can write

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

In view of the fact that $\chi(p) = 0$ when $p|D$ and $L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$ *for* $s > 1$,we can rewrite the above equation as

$$\zeta_K(s) = L(s,\chi)\zeta(s). \tag{10.10}$$

Multiply both sides of (10.10) by $s - 1$ and take the limit as $s \to 1^+$. Then on applying Theorem 9.1 and Proposition 9.5 with notations as in Theorem 9.1, we conclude that $h\kappa = L(1,\chi)$, because $L(s,\chi)$ is a continuous function in $(0,\infty)$ by Proposition 10.6. Now since K is a quadratic field with discriminant D, we see that

$$\kappa = \frac{2^{r_1+r_2}\pi^{r_2}R}{m\sqrt{|d_K|}} = \begin{cases} \dfrac{2^2 \log \epsilon}{2\sqrt{D}} & \text{if } D > 0, \\ \dfrac{2\pi}{m\sqrt{|D|}} & \text{if } D < 0. \end{cases}$$

This yields the desired formula for $h = L(1, \chi)/\kappa$.

□

The following corollary is an immediate consequence of the above theorem.

Corollary 10.15 *Let χ be the character associated with a quadratic field having discriminant D. Then $L(1, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n} > 0$, i.e., $\sum_{n=1}^{\infty} \frac{1}{n}\left(\frac{D}{n}\right) > 0$.*

Lemma 10.16 *The character χ associated with a quadratic field is always non-principal.*

Proof Let D denote the discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$ with d a square-free integer. The proof is split into three cases.

Case 1. $d \equiv 1 \pmod 4$.
Choose a prime p such that $p \mid d$ and an integer s such that $\left(\frac{s}{p}\right) = -1$. By Chinese remainder theorem, there exists an integer x such that $x \equiv s \pmod p$ and $x \equiv 1 \pmod{\frac{d}{p}}$. Then

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

Case 2. $d \equiv 3 \pmod 4$, $D = 4d$.
Using Chinese remainder theorem, choose an integer x such that $x \equiv 1 \pmod d$, $x \equiv 3 \pmod 4$. Then $\chi(x) = (-1)^{\frac{x-1}{2}}\left(\frac{x}{|d|}\right) = -1$.

Case 3. $d = 2d'$, d' odd.
Again by Chinese remainder theorem, choose an integer x such that $x \equiv 5 \pmod 8$, $x \equiv 1 \pmod{|d'|}$, then

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

□

Exercises

1. Let χ be the character associated with a quadratic field K. Calculate $L(1, \chi)$ when K is one of the following fields :

   (i) $\mathbb{Q}(\sqrt{14})$;
   (ii) $\mathbb{Q}(\sqrt{10})$;
   (iii) $\mathbb{Q}(\sqrt{-6})$;
   (iv) $\mathbb{Q}(\sqrt{-11})$.

2. Let $K = \mathbb{Q}(\zeta)$, where ζ is a primitive qth root of unity, q an odd prime. Prove that for $s > 1$, $\zeta_K(s) = \left(1 - \frac{1}{q^s}\right)^{-1} \prod_{\chi} L(s, \chi)$, where χ runs over all the numerical characters modulo q.
3. Let D be the discriminant of a quadratic field $\mathbb{Q}(\sqrt{D})$. Prove that there exist infinitely many positive integers n such that $\left(\frac{D}{n}\right) = -1$.
4. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field with discriminant D. Let $\nu(n)$ denote the number of integral ideals of $\mathcal{O}_K$ with norm n. Prove that $\nu(n) = \sum_{k} \left(\frac{D}{k}\right)$, where k runs over positive divisors of n.
5. Let $K = \mathbb{Q}(\sqrt{D})$ be a quadratic field with discriminant D. Prove that for every integer $N > 0$, one has

$$\left| \sum_{n \leq N} \left(\frac{D}{n} \right) \right| \leq |D|.$$

Appendix A
Field Theory

A.1 Introduction

Fields have been used implicitly ever since the discovery of addition, subtraction, multiplication and division. Cardano's formula dating 16th century used $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Lagrange used the field of rational functions in n variables in his study of roots of polynomials in 1770. Number fields also appeared around this time. Euler used $\mathbb{Q}(\sqrt{-3})$ to show that the equation $x^3 + y^3 = z^3$ has no non-trivial solution in $\mathbb{Z}$. The first truly abstract notion of field is due to Dedekind. In 1877, he gave the following definition: "*I call a system A of numbers (not all zero) a field when the sum, difference, product and quotient of any two numbers in A also belong to A.*" This is not completely general as the numbers in this definition are all complex. In fact in 1893, his student Weber gave the first fully abstract definition of field which we use today.

Definition A *binary operation* denoted by '$*$' on a set A is given by a function from $A \times A$ into A mapping (a, b) to $a * b$. A non-empty set G with a binary operation '$*$' is said to be a *group*[1] with respect to '$*$' if the following three conditions are satisfied: (i) for all a, b, c belonging to G, $a * (b * c) = (a * b) * c$ (associativity), (ii) there exists an element $e \in G$, such that $a * e = a = e * a$ for all $a \in G$ (existence of identity), (iii) for every $a \in G$, there exists an element $a' \in G$ such that $a * a' = e = a' * a$ (existence of inverse). Further G is called commutative/abelian[2] if $a * b = b * a$ for all $a, b \in G$. A set R with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *ring* if (i) $(R, +)$ is a commutative group, (ii) Multiplication is

[1] The abstract form of the definition of a group, which we use today, was built up slowly over the course of 19th century, with suggested definitions by Cayley, Kronecker, Weber, Burnside, and Pierpont. The axioms of associativity, identity element and inverse were first stated in their present form by Pierpont.

[2] The term abelian is derived from the name of Norwegian Mathematician Niels Henrik Abel (1802-1829) who showed the importance of such groups in the theory of equations.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8

associative, i.e., $a.(b.c) = (a.b).c$ for every $a, b, c \in R$, (iii) Distributive laws hold: $a.(b + c) = a.b + a.c$ and $(b + c).a = b.a + c.a$ for every $a, b, c \in R$.

Definition A non-empty set F with two binary operations denoted by '$+$' and '$\cdot$' is said to be a *field* if the following axioms are satisfied:
(i) $(F, +)$ is a commutative group (with identity element to be denoted by 0).
(ii) $(F \setminus \{0\}, \cdot)$ is a commutative group (with identity element to be denoted by 1).
(iii) Distributive laws hold, i.e., $a.(b + c) = a.b + a.c$ and $(b + c).a = b.a + c.a$ for every $a, b, c \in F$.

Examples

(i). $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields with respect to ordinary addition and multiplication.
(ii). The set $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field with respect to the usual addition and multiplication.
(iii). Let n be a positive integer. For a, b belonging to $\mathbb{Z}$, we write $a \equiv b \pmod{n}$ and say a is congruent[3] to b modulo n if n divides $a - b$. This is an equivalence relation on $\mathbb{Z}$. The equivalence class of an integer m for this equivalence relation is denoted by $[m]$. The set $\mathbb{Z}/n\mathbb{Z} = \{[m] \mid m = 0, 1, \ldots, n - 1\}$ is a ring with respect to the operations $[i] + [j] = [i + j]$ and $[i] \cdot [j] = [ij]$. The ring $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is a prime.
(iv). In what follows, x will stand for an indeterminate and $F[x]$ will denote the set of all polynomials in x with coefficients from F. It is a ring with respect to the usual addition and multiplication of polynomials. Its quotient field to be denoted by $F(x)$ is the field of rational functions in x over F. Similarly one can define the field of rational functions $F(x_1, x_2, \ldots, x_n)$ in n indeterminates.

Definition A non-empty subset E of a field F is said to be a *subfield* of F if E is a field under the induced addition and multiplication operations on F. If a subfield E of F is not equal to F, we shall say that E is a *proper subfield* of F. If E is a subfield of F, then F is said to be an *overfield* of E.

Remark If $\{E_i\}_{i \in I}$ is a family of subfields of a field F, then so is $E = \bigcap_{i \in I} E_i$.

Definition Let F be a field. By the *prime subfield* of F we mean the smallest subfield of F. It is the intersection of all subfields of F.

Definition Let F be a field and K be a field containing F as a subfield. Then K is called an *extension* of F or K/F is called a field extension. K can be regarded as a vector space over F. A basis of this vector space is called a *basis of the extension* K/F and its dimension is called the *degree of the extension* K/F, which will be denoted by $[K : F]$. K is said to be *finite* or *infinite* extension of F according as the degree of K/F is *finite* or *infinite*.

[3] It was Gauss who first introduced congruence notation in Sect. VII of *Disquistiones Arithmeticae* published in 1801.

Example With operations of usual addition and multiplication, $\mathbb{C}$ is an extension of $\mathbb{R}$ of degree two and $\mathbb{R}$ is an infinite extension of $\mathbb{Q}$, because $\mathbb{R}$ is uncountable and $\mathbb{Q}$ is countable.

In 1894, Dedekind developed the theory of field extensions that included the concept of degree. He formulated the proof of Tower theorem stated below.

Theorem A.1 (Tower Theorem) *If K is a finite extension of F and L is a finite extension of K, then L is a finite extension of F and* $[L : F] = [L : K][K : F]$.

Proof Let $\{e_1, e_2, \ldots, e_m\}$ be a basis of K/F and $\{f_1, f_2, \ldots, f_n\}$ be a basis of L/K. We claim that $\{e_i f_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$ is a basis of L/F. Let α be any element of L. Write $\alpha = \sum_j b_j f_j$, $b_j \in K$ and $b_j = \sum_i \lambda_{ij} e_i$, $\lambda_{ij} \in F$. Then

$$\alpha = \sum_j \left(\sum_i \lambda_{ij} e_i \right) f_j = \sum_{i,j} \lambda_{ij} e_i f_j.$$

This shows that the set $\{e_i f_j \mid 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$ generates the vector space L over F. To prove its linear independence over F, suppose that $\sum_{i,j} \mu_{ij} e_i f_j = 0$ for some $\mu_{ij} \in F$. Then

$$\sum_j \left(\sum_i \mu_{ij} e_i \right) f_j = 0.$$

As $\{f_1, f_2, \ldots, f_n\}$ is linearly independent over K, it follows that

$$\sum_i \mu_{ij} e_i = 0 \ \text{ for all } \ j.$$

Since $\{e_1, e_2, \ldots, e_m\}$ is linearly independent over F, $\mu_{ij} = 0$ for all i, j. Thus $\{e_i f_j,\ 1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant n\}$ is a basis of the vector space L over F consisting of mn elements. □

Definition Let F and F' be fields. A mapping f from F to F' is called an *isomorphism* (of fields) if (i) f is 1-1, (ii) $f(a + b) = f(a) + f(b)$, $f(ab) = f(a) f(b)$ for all $a, b \in F$. Two fields F and F' are said to be isomorphic if there exists an isomorphism from one onto the other. An isomorphism from F onto itself is called an *automorphism* of F.

It can be easily checked that if F_0 is the prime subfield of a field F, then F_0 is isomorphic to either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p. A field with p elements will be denoted by F_p.

Definition The *characteristic* of a field F is defined to be 0 or p according as the prime subfield of F is isomorphic to $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$, where p is a prime.

Remark If F is a finite field[4] of characteristic p, then F can be regarded as an extension of $F_p = \mathbb{Z}/p\mathbb{Z}$ and if $\{w_1, \ldots, w_m\}$ is a basis of the extension F/F_p, then clearly F has exactly p^m elements, because each element of F can be uniquely written as $a_1w_1 + \cdots + a_mw_m$ with a_i's in F_p. We shall prove later that given a prime p and any number $m \geq 1$, there exists a finite field with p^m elements which is "unique" in some sense.

Definition Let K/F be an extension of fields and $S \subseteq K$. The smallest subfield of K containing $F \bigcup S$ is called the subfield generated by S over F and is denoted by $F(S)$. In fact $F(S)$ is the intersection of all the subfields of K containing $F \bigcup S$. If $S = \{\alpha_1, \ldots, \alpha_n\}$ is a finite set, then we say that $F(S)$ is finitely generated over F and write $F(S)$ as $F(\alpha_1, \ldots, \alpha_n)$.

Definition An extension K/F is called a *simple* extension if K/F is generated by a single element, i.e., $K = F(\alpha)$ for some $\alpha \in K$; such an element α is called a primitive element for the extension K/F.

Example Any extension of prime degree is a simple extension.

Definition Let K/F be an extension of fields and $\{\alpha_1, \ldots, \alpha_n\}$ be a subset of K. The smallest subring of K containing F and $\alpha_1, \ldots, \alpha_n$ will be denoted by $F[\alpha_1, \ldots, \alpha_n]$. It consists of all polynomial expressions in $\alpha_1, \ldots, \alpha_n$ with coefficients from F. Note that $F(\alpha_1, \ldots, \alpha_n)$ is quotient field of $F[\alpha_1, \ldots, \alpha_n]$.

Given a field extension K/F and elements $\alpha_1 = \alpha, \ldots, \alpha_n$ in K, it would be interesting to know when is $F(\alpha) = F[\alpha]$ or more generally when is $F(\alpha_1, \ldots, \alpha_n) = F[\alpha_1, \ldots, \alpha_n]$. These questions are related to algebraic extensions introduced in the next section.

A.2 Algebraic Extensions

Definition Let K/F be a field extension. An element $\alpha \in K$ is called *algebraic* over F if it satisfies a non-zero polynomial with coefficients from F. An element of K which is not algebraic over F is called *transcendental* over F. If every element of K is algebraic over F, then we say that K/F is an *algebraic extension*. An extension which is not algebraic is called a transcendental extension.

A complex number α is called an algebraic number if it is algebraic over $\mathbb{Q}$, otherwise it is called a transcendental number. It was in 1853 that the existence of transcendental numbers was proved by Joseph Liouville. Charles Hermite proved that e is a transcendental number in 1873 and Lindemann showed that π is a transcendental number in 1882. To this day, it is not known whether $e + \pi$ is transcendental or not. Although it is often difficult to prove that a given complex number is transcendental, it is fairly easy to show that the set of all transcendental numbers is uncountable.

[4] Finite fields were introduced by Galois in 1830 for solving congruences of the type $f(x) \equiv 0 \pmod{p}$, where p is a prime number and $f(x) \in \mathbb{Z}[x]$ is irreducible modulo p. That is why finite fields are also known as Galois fields.

This follows from Theorem 1.2 which asserts that the set of algebraic numbers is countable.

Definition Let K/F be an extension of fields. If α belonging to K is algebraic over F, then the monic polynomial $g(x)$ of smallest degree over F satisfied by α is called the *minimal polynomial* of α over F. It can be easily seen that $g(x)$ is irreducible over F.

Examples The minimal polynomial of $1+\sqrt{3}$ over $\mathbb{Q}$ is x^2-2x-2. The minimal polynomial of $20^{1/3}$ over $\mathbb{Q}$ is x^3-20 in view of Eisenstein irreducibility criterion stated in the last section of this appendix.

Proposition A.2 *Let K/F be an extension of fields. Suppose $\alpha \in K$ is algebraic over F with minimal polynomial $g(x)$ over F of degree n. Then $F(\alpha)$ is an extension of degree n of F. Indeed we have*

$$F(\alpha) = \{a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \mid a_i \in F \text{ for } 0 \le i \le n-1\} = F[\alpha].$$

Proof Since the minimal polynomial of α over F has degree n, the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is linearly independent over F. So all we need to verify is that for any $h(x) \in F[x]$ with $h(\alpha) \neq 0$, the elements $h(\alpha)$ and $1/h(\alpha)$ are linear combinations of $1, \alpha, \ldots, \alpha^{n-1}$ with coefficients from F. By division algorithm, we can write $h(x) = g(x)q(x) + r(x)$, with $q(x) \in F[x]$ and $\deg r(x) < n$. On substituting α in the above equation, we see that $h(\alpha) = r(\alpha)$ as desired. Since $h(\alpha) \neq 0$, $g(x)$ does not divide $h(x)$. So $g(x)$ being irreducible over F is coprime to $h(x)$. Therefore there exist $u(x),\ v(x)$ in $F[x]$ such that $u(x)g(x) + v(x)h(x) = 1$; on substituting $x = \alpha$, the last equality shows that $1/h(\alpha) = v(\alpha)$ and hence $1/h(\alpha)$ can be written as an F-linear combination of $1, \alpha, \ldots, \alpha^{n-1}$. □

It may be pointed out that Abel was the first to notice that $F(\alpha) = F[\alpha]$ when α is algebraic over F. The converse of this result is also true because if $F(\alpha) = F[\alpha]$, then $1/\alpha = g(\alpha)$ for some polynomial $g(x) \in F[x]$. So α satisfies the non-zero polynomial $xg(x) - 1$ and hence α is algebraic over F.

Corollary A.3 *If $F(\alpha_1, \alpha_2, \ldots, \alpha_r)$ is a finitely generated extension of F with each α_i algebraic over F, then $F(\alpha_1, \alpha_2, \ldots, \alpha_r)/F$ is a finite extension and $F(\alpha_1, \alpha_2, \ldots, \alpha_r) = F[\alpha_1, \alpha_2, \ldots, \alpha_r]$.*

Proof By Proposition A.2, each of the extensions $F(\alpha_1)/F$, $F(\alpha_1, \alpha_2)/F(\alpha_1)$, $\ldots$, $F(\alpha_1, \alpha_2, \ldots, \alpha_r)/F(\alpha_1, \alpha_2, \ldots, \alpha_{r-1})$ is finite. So by Tower theorem, the extension $F(\alpha_1, \alpha_2, \ldots, \alpha_r)/F$ is also finite. Keeping in mind the second assertion of Proposition A.2, we see that $F(\alpha_1, \alpha_2) = F(\alpha_1)[\alpha_2] = F[\alpha_1][\alpha_2] = F[\alpha_1, \alpha_2]$. Repeating this argument finitely many times, the last assertion of the corollary follows. □

Proposition A.4 *Every finite extension is algebraic.*

Proof Suppose that K/F is a finite extension of degree n. Let $\alpha \in K$. Then the $n+1$ elements $1, \alpha, \ldots, \alpha^n$ are linearly dependent over F as $[K : F] = n$. Hence

there exist $a_0, a_1, \ldots, a_n \in F$, not all zero such that $a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0$. This implies that α is algebraic over F. □

Remark Converse of Proposition A.4 is not true. Let $\mathbb{A}$ denote the set of all complex numbers which are algebraic over $\mathbb{Q}$. Then $\mathbb{A}$ is a subfield of $\mathbb{C}$ in view of Theorem A.6. Using Eisenstein irreducibility criterion, it can be easily seen that $\mathbb{A}/\mathbb{Q}$ is an infinite extension.

Theorem A.5 (Transitive property of algebraic extensions) *If K/F and L/K are algebraic extensions, then so is L/F.*

Proof Let α be an element of L. Since L/K is algebraic, α satisfies a relation $\alpha^n + a_1\alpha^{n-1} + \ldots + a_n = 0$ for some a_i's $\in K$. Then α is also algebraic over the field $F' = F(a_1, a_2, \ldots, a_n)$. Since $a_i \in K$, they are algebraic over F. Hence F'/F is a finite extension by Corollary A.3. As $F'(\alpha)/F'$ is also a finite extension, therefore $F'(\alpha)/F$ is finite. Consequently α is algebraic over F by Proposition A.4. □

Theorem A.6 *Let K/F be an extension of fields. The set E of all elements of K which are algebraic over F is a subfield of K containing F.*

Proof Clearly each element of F is algebraic over F. Thus $F \subseteq E$. Let α, β be elements of $\mathcal{A}$ with $\beta \neq 0$. Then $F(\alpha, \beta)/F$ is a finite extension by Corollary A.3. Hence it is an algebraic extension by Proposition A.4. In particular, $\alpha \pm \beta, \alpha\beta, \alpha/\beta$ are algebraic over F, i.e., these elements belong to E. This proves that E is a subfield of K. □

Theorem A.7 *Let K/F be a finite simple extension with $K = F(\alpha)$ and $g(x)$ be the minimal polynomial of α over F. Let $\langle g(x)\rangle$ denote the ideal generated by $g(x)$ in $F[x]$. Then $F[x]/\langle g(x)\rangle$ is isomorphic to $F(\alpha) = F[\alpha]$.*

Proof Consider the map $\psi : F[x] \to F[\alpha]$ defined by $\psi(h(x)) = h(\alpha)$, $h(x) \in F[x]$. Clearly ψ is an onto ring homomorphism with $\ker(\psi) = \langle g(x)\rangle$. The theorem now follows from the first isomorphism theorem of rings. □

Cauchy's observation in 1847 that $\mathbb{R}[x]/ < x^2 + 1 >$ is a field that contains a zero of $x^2 + 1$ paved the way for the following sweeping generalization proved by Kronecker in 1887.

Theorem A.8 (Kronecker) *If $g(x)$ is a polynomial of degree $n \geqslant 1$ with coefficients in field F and is irreducible over F, then there is an extension K of F with $[K : F] = n$ in which $g(x)$ has a root.*

Proof Since $g(x)$ is irreducible over F, the ideal $I =< g(x) >$ in the principal ideal domain $F[x]$ is a maximal ideal and hence $F[x]/I$ is a field. Denote $F[x]/I$ by K. The mapping from F into K defined by $a \mapsto I + a$ is an isomorphism of F onto its image F' contained in K. Identifying F with F', we can consider K as an extension of F. Note that the element $I + x$ belonging to K is a root of the polynomial $g(X)$, because $g(I + x) = I + g(x) = I$ as $g(x) \in I$. It can be easily checked that $I + 1, I + x, \ldots, I + x^{n-1}$ form a basis of K=$F[x]/I$ over F. So $[K : F] = n$. □

The corollary stated below follows quickly from Theorem A.8.

Corollary A.9 *If $h(x)$ is a polynomial with coefficients in a field F, then there is a finite extension K of F in which $h(x)$ has a root. Moreover $[K : F] \leqslant \deg h(x)$.*

Theorem A.10 *Let $h(x)$ be a polynomial of degree $n \geqslant 1$ with coefficients in a field F. Then there is an extension K of F of degree at most $n!$ in which $h(x)$ has n roots.*

Proof The theorem is proved by induction on the degree n of $h(x)$. If $\deg h(x) = 1$, then the result is obvious. Suppose it is true for polynomials of degree $n-1$ over an arbitrary field. Let $h(x)$ be a polynomial of degree n over F. By the above corollary, there is an extension F_1 of F with $[F_1 : F] \leqslant n$ in which $h(x)$ has a root, say α. Thus in $F_1[x]$, $h(x)$ factors as $h(x) = (x-\alpha)h_1(x)$, where $h_1(x) \in F_1[x]$ is of degree $n-1$. In view of induction hypothesis, there is an extension K of F_1 of degree at most $(n-1)!$ in which $h_1(x)$ has all its roots. Since any root of $h(x)$ is either α or a root of $h_1(x)$, we see that K contains all roots of $h(x)$. As $[K : F] = [K : F_1][F_1 : F] \leqslant (n-1)!n = n!$, the theorem is proved. □

Definition Let $h(x)$ belonging to $F[x]$ be a polynomial of degree n. An extension K/F is called a *splitting field* of $h(x)$ over F if K contains n roots $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $h(x)$ and $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

The following corollary is an immediate consequence of Theorem A.10.

Corollary A.11 *Let $h(x)$ be a polynomial of degree $n \geqslant 1$ with coefficients in a field F. Then $h(x)$ has a splitting field L and $[L : F] \leqslant n!$.*

Examples

(i) The splitting field contained in $\mathbb{C}$ of the polynomial $x^3 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/3}, \omega)$ where $\omega \neq 1$ is a cube root of unity.
(ii) The splitting field contained in $\mathbb{C}$ of $x^4 - 2$ over $\mathbb{Q}$ is $\mathbb{Q}(2^{1/4}, \sqrt{-1})$.
(iii) A splitting field of $x^2 + x + \bar{1}$ over $\mathbb{Z}/2\mathbb{Z}$ consists of $\bar{0}$, $\bar{1}$, α, $\bar{1} + \alpha$ where $\alpha^2 + \alpha + \bar{1} = 0$. It provides an example of a field having exactly four elements.
(iv) Let α be a root of the polynomial $x^2 + \bar{1}$ with coefficients in $F_3 = \mathbb{Z}/3\mathbb{Z}$ in an extension of $\mathbb{Z}/3\mathbb{Z}$. Then $K = F_3(\alpha)$ is a splitting field of $x^2 + \bar{1}$. By Proposition A.2, $K = \{a + b\alpha \mid a, b \in F_3\}$ is a field of nine elements.

Definition Let K and K' be extensions of a field F. A field isomorphism from K into K' which is identity on F is called an *F-isomorphism* of K into K'. An F-isomorphism of K onto itself is called an *F-automorphism* of K.

We shall now prove that if L_1 and L_2 are splitting fields of a polynomial $h(x)$ over F, then there is an F-isomorphism from L_1 onto L_2. Indeed we prove:

Theorem A.12 *Let $\sigma : F \to F'$ be an isomorphism of a field F onto a field F'. Let $h(x) = \sum a_i x^i$ be a polynomial belonging to $F[x]$ and $h^\sigma(x) = \sum \sigma(a_i)x^i$ be its image polynomial. Let K and K' be splitting fields of $h(x)$ and $h^\sigma(x)$ over F, F' respectively. Then there exists an isomorphism $\bar{\sigma}$ from K onto K' such that $\bar{\sigma}|_F = \sigma$.*

To prove the theorem, we need the following lemma.

Lemma A.13 *Let $\sigma : F \to F'$ be an isomorphism of a field F onto a field F'. Let $g(x) = \sum a_i x^i$ belonging to $F[x]$ be an irreducible polynomial. Let $g^\sigma(x) = \sum \sigma(a_i)x^i$ be the image polynomial in $F'[x]$. Let α, α' be respectively the roots of $g(x)$ and $g^\sigma(x)$. Then σ can be extended to an isomorphism $\bar{\sigma}$ from $F[\alpha]$ onto $F'[\alpha']$ such that $\bar{\sigma}(\alpha) = \alpha'$.*

Proof Since the polynomial $g(x)$ is irreducible over F, $g^\sigma(x)$ is irreducible over $\sigma(F) = F'$. For $h(\alpha) \in F[\alpha]$, define $\overline{\sigma}(h(\alpha)) = h^\sigma(\alpha')$. The mapping $\overline{\sigma}$ is well defined, because if $h(\alpha) = h_1(\alpha)$ with $h_1(x) \in F[x]$, then $g(x)$ divides $h(x) - h_1(x)$ and hence $g^\sigma(x)$ divides $h^\sigma(x) - h_1^\sigma(x)$; consequently $h^\sigma(\alpha') = h_1^\sigma(\alpha')$. The mapping $\overline{\sigma}$ is one-to-one, because if $\overline{\sigma}(h(\alpha)) = 0$, then the polynomial $g^\sigma(x)$ being the minimal polynomial of α' over F' divides $h^\sigma(x)$ and hence $g(x)$ divides $h(x)$ which gives $h(\alpha) = 0$. Clearly the mapping $\overline{\sigma}$ is onto and a homomorphism of rings. So the lemma is proved. □

Proof of Theorem A.12 The proof is by induction on the degree of $h(x)$. If $\deg h(x) = 1$, then $K = F$, $K' = F'$ and there is nothing to prove. Assume that the theorem holds for polynomials of degree not exceeding $n - 1$ over an arbitrary field and that $h(x) \in F[x]$ has degree n. Let $g_1(x)$ be an irreducible factor of $h(x)$ over F. Let α be a root of $g_1(x)$ and α' a root of the polynomial $g_1^\sigma(x)$. By Lemma A.13, σ can be extended to an isomorphism σ_1 from $F[\alpha]$ to $F'[\alpha']$ mapping α onto α'. Write $h(x) = (x - \alpha)h_1(x)$ where $h_1(x) \in F(\alpha)[x]$ so that $h^\sigma(x) = h^{\sigma_1}(x) = (x - \alpha')h_1^{\sigma_1}(x)$. Therefore K, K' are splitting fields of the polynomials $h_1(x)$, $h_1^{\sigma_1}(x)$ over $F(\alpha)$, $F'(\alpha')$ respectively. By induction, σ_1 can be extended to an isomorphism $\bar{\sigma}$ from K onto K'. □

The following corollary follows immediately from Theorem A.12.

Corollary A.14 *A splitting field of a polynomial over a field F is unique upto F-isomorphism.*

Corollary A.15 [5] *Any two finite fields having the same number of elements are isomorphic.*

Proof Let K be a finite field with $q = p^m$ elements. Since $K^\times$ is a group of order $q - 1$, for any element $\alpha \in K^\times$, $\alpha^{q-1} = 1$ by Lagrange's theorem for finite groups. So each element of K is a root of the polynomial $x^q - x$ which can have at most q roots. Thus K is a splitting field of $x^q - x$ over F_p. The result now follows from Corollary A.14. □

Definition A field F is called *algebraically closed* if it has no proper algebraic extension, i.e., if K is an algebraic extension of F, then $K = F$.

Remark In 1799, Gauss at the age of 22, proved that $\mathbb{C}$ is algebraically closed. This result was then considered so important that it was called "The Fundamental

[5] This result was first obtained in 1893 by American mathematician E. H. Moore.

Theorem of Algebra". Over a period of fifty years, Gauss gave four different proofs of this theorem.

Example Let $\mathbb{A}$ denote the set of all those complex numbers which are algebraic over $\mathbb{Q}$. In view of Theorem A.6, $\mathbb{A}$ is a subfield of $\mathbb{C}$ and is called the field of algebraic numbers. Assuming that $\mathbb{C}$ is algebraically closed we show that $\mathbb{A}$ is algebraically closed. Let ξ be an element of an overfield of $\mathbb{A}$ which is algebraic over $\mathbb{A}$, then ξ being algebraic over $\mathbb{C}$ belongs to $\mathbb{C}$. Since ξ satisfies a polynomial $x^n + a_1 x^{n-1} + \cdots + a_n$ for some a_i's belonging to $\mathbb{A}$, it follows that ξ is algebraic over the finite extension $\mathbb{Q}(a_1, a_2, \ldots, a_n)$ of $\mathbb{Q}$ and hence ξ is algebraic over $\mathbb{Q}$ in view of Theorem A.5. This proves that ξ belongs to $\mathbb{A}$.

Definition An extension $\hat{F}$ of a field F is called an algebraic closure of F if $\hat{F}/F$ is an algebraic extension and $\hat{F}$ is an algebraically closed field.

Example The field $\mathbb{A}$ of algebraic numbers is an algebraic closure of $\mathbb{Q}$.
Remark In 1910, Ernst Steinitz proved that every field F has an algebraic closure which is unique upto F-isomorphism, i.e., if $\hat{F}_1$ and $\hat{F}_2$ are two algebraic closures of F, then there exists an isomorphism from $\hat{F}_1$ onto $\hat{F}_2$ which is identity on F (for proof see [Za-Sa, Lu-Pa2]).

A.3 Separable Extensions

Definition Let $g(x)$ belonging to $F[x]$ be an irreducible polynomial. $g(x)$ is called a *separable polynomial* if all its roots in its splitting field are distinct, otherwise it is called inseparable.

Definition Let K/F be an extension of fields. An element $\alpha \in K$ is called *separable* over F if it is algebraic over F and its minimal polynomial over F is a separable polynomial, otherwise α is called *inseparable* over F. An extension K/F is called *separable* if it is algebraic and every $\alpha \in K$ is separable over F.

Examples

(i). $3^{1/5}$ is separable over $\mathbb{Q}$. In fact $a^{1/n}$ is separable over $\mathbb{Q}$ for any integer a.
(ii). Let $F = F_p(t)$ where t is an indeterminate. Then $\alpha = t^{1/p}$ is not separable over F.

Using Taylor's expansion of a polynomial, the following proposition can be easily proved.

Proposition A.16 *Let $h(x)$ belonging to $F[x]$ be a non-constant polynomial. A root α of $h(x)$ in some extension field is a repeated root of $h(x)$ if and only if $h'(\alpha) = 0$.*

Proposition A.17 *A monic irreducible polynomial $g(x)$ over a field F has a repeated root if and only if $g'(x)$ is the zero polynomial.*

Proof If $g(x)$ has a repeated root, say α in an extension of F, then by the above proposition $g'(\alpha) = 0$. But $g(x)$ being the minimal polynomial of α over F divides every other polynomial $h(x) \in F[x]$ with $h(\alpha) = 0$. So in particular $g(x)$ divides $g'(x)$. Since $\deg g'(x) < \deg g(x)$, we conclude that $g'(x)$ is identically zero. Conversely suppose that $g'(x)$ is the zero polynomial. Then by Proposition A.16, every root of $g(x)$ is a repeated root. □

Corollary A.18 *Each irreducible polynomial over a field of characteristic zero is separable.*

Corollary A.19 *An irreducible polynomial $g(x) \in F[x]$ is inseparable if and only if the field F is of characteristic $p > 0$ and $g(x)$ is a polynomial in x^p.*

Proof In view of Proposition A.17, a monic irreducible polynomial $g(x)$ belonging to $F[x]$ is inseparable if and only if $g'(x)$ is the zero polynomial. On writing $g(x)$ as $g(x) = \sum a_i x^i$, we see that $g'(x)$ is the zero polynomial if and only if characteristic of F is a prime p and $a_i = 0$ for each index i not divisible by p, i.e., $g(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \ldots$. □

Definition A field F is called *perfect* if all finite extensions of F are separable.

It is immediate from Corollary A.18 that every field of characteristic zero is a perfect field. Note that if F is a field of characteristic $p > 0$, then $F^p = \{a^p \mid a \in F\}$ is a subfield of F. The following theorem asserts that $F^p = F$ if and only if F is perfect.

Theorem A.20 *Let F be a field of characteristic $p > 0$. Then F is perfect if and only if every element of F has a pth root in F, i.e., for every $a \in F$, there exists $b \in F$ with $b^p = a$.*

Proof We first verify that if $a \in F$ has a pth root, it is unique, for if $b_1^p = a = b_2^p$, then $(b_1 - b_2)^p = b_1^p - b_2^p = 0$, i.e., $b_1 = b_2$. Assume that F is perfect. Suppose to the contrary that there exists an element $a \in F$ which has no pth root in F. The polynomial $f(x) = x^p - a \in F[x]$ is clearly inseparable. We verify that it is irreducible over F. Let α be a root of $f(x)$. Then $\alpha \notin F$ due to our supposition. Let $g(x)$ be the minimal polynomial of α over F. Since $g(x)$ is a divisor of $f(x)$, $g(x)$ is not a separable polynomial. So by Corollary A.19, $g(x)$ is a polynomial in x^p. Therefore $\deg g(x) = p = \deg f(x)$ and hence $f(x) = g(x)$ is irreducible over F. Adjoining a root of $f(x)$ gives an inseparable extension of F of degree p, a contradiction. Hence every element of F has a pth root in F.

Conversely, assume that every $a \in F$ has a pth root in F. Suppose α is an inseparable element over F. Then the minimal polynomial $g(x)$ of α over F is a polynomial in x^p by Corollary A.19. So $g(x) = a_0 + a_1 x^p + \ldots + a_n x^{pn}$ with a_i's belonging to F. If $b_i \in F$ is a pth root of a_i, i.e., $b_i^p = a_i$, then

$$g(x) = b_0^p + b_1^p x^p + \ldots + b_n^p x^{np} = (b_0 + b_1 x + \ldots + b_n x^n)^p$$

which is impossible as $g(x)$ is irreducible over F. □

Corollary A.21 *Any finite field is perfect.*

Proof Let F be a finite field of characteristic $p > 0$. The mapping $a \mapsto a^p$ defined from F into F is 1-1 and hence onto. Therefore the corollary follows from Theorem A.20. □

Definition Let K_1, K_2 be subfields of a field L. The smallest subfield of L containing K_1 and K_2 is called the *compositum*(composite) of K_1 and K_2 and will be denoted by K_1K_2.

If K_1, K_2 are algebraic extensions of field F which are subfields of a field L, then we show that the compositum K_1K_2 consists of all finite sums of the type $\sum \alpha_i\beta_i$ where α_i's $\in K_1$, β_i's $\in K_2$. This is so because the inverse of an element of the type $\sum_{i=1}^{k} \alpha_i\beta_i$ with α_i's $\in K_1$, β_i's $\in K_2$, belongs to the subfield $F(\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k)$ which equals the subring $F[\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k]$ in view of Corollary A.3. In particular if K is an algebraic extension of a field F of characteristic $p > 0$, then F, K^p are algebraic extensions of the field F^p and hence the compositum FK^p consists of all finite sums of the type $\sum b_i y_i^p$ with $b_i \in F$, $y_i \in K$.

The following theorem gives a necessary and sufficient condition for a finite extension to be separable.

Theorem A.22 *Suppose F is a field of characteristic $p > 0$. A finite extension K/F is separable if and only if $K = FK^p$.*

Proof Suppose first that K/F is separable. Clearly $FK^p \subseteq K$. To show that $K \subseteq FK^p$, let α be an element of K. We show that the hypothesis α separable over F implies that

$$F(\alpha) = F(\alpha^p). \tag{A.1}$$

Since α is separable over F, it is separable over $F(\alpha^p)$. Note that α satisfies the polynomial $x^p - \alpha^p$ over $F(\alpha^p)$. Let $g(x)$ be the minimal polynomial of α over $F(\alpha^p)$. Then $g(x)$ divides $x^p - \alpha^p$. Since $g(x)$ is separable, we see that the degree of $g(x)$ is 1. Therefore $\alpha \in F(\alpha^p)$ and hence $F(\alpha) = F(\alpha^p) = F[\alpha^p]$. Consequently α can be written as $c_0 + c_1\alpha^p + \ldots + c_r(\alpha^p)^r$ for some $c_i \in F$; thus $\alpha \in FK^p$, which proves that $K \subseteq FK^p$ as desired.

Conversely suppose that $FK^p = K$. It is to be shown that K/F is separable. Claim is that if $\{l_1, l_2, \ldots, l_n\}$ is a basis of K/F, then $\{l_1^p, l_2^p, \ldots, l_n^p\}$ is also a basis of K/F. Let α be any element of $K = FK^p$. Recall that FK^p consists of finite sums of the type $\sum b_i y_i^p$ with $b_i \in F$, $y_i \in K$. So we can write $\alpha = b_1 y_1^p + b_2 y_2^p + \ldots + b_r y_r^p$ for some $b_i \in F$, $y_i \in K$, $1 \leqslant i \leqslant r$. Write $y_i = \sum_{j=1}^{n} a_{ij} l_j$, $a_{ij} \in F$, then $y_i^p = \sum_{j=1}^{n} a_{ij}^p l_j^p$ which implies that

$$\alpha = \sum_{i=1}^{r} b_i y_i^p = \sum_{i=1}^{r} b_i \left(\sum_{j=1}^{n} a_{ij}^p l_j^p \right) = \sum_{j=1}^{n} \left(\sum_{i=1}^{r} b_i a_{ij}^p \right) l_j^p .$$

Hence α is an F-linear combination of $l_1^p, l_2^p, \ldots, l_n^p$. Thus $\{l_1^p, l_2^p, \ldots, l_n^p\}$ spans K/F and therefore it is a basis of K/F. In particular, using basis extension theorem, it follows from the claim that whenever a subset $\{\beta_1, \beta_2, \ldots, \beta_m\}$ of K is linearly independent over F, then so is $\{\beta_1^p, \beta_2^p, \ldots, \beta_m^p\}$.

Let α be any element of K and $g(x)$ be the minimal polynomial of α over F. It is to be shown that α is separable over F. Suppose to the contrary $g(x)$ is not separable. Then $g(x) \in F[x^p]$ by Corollary A.19. So there exists $f(x) \in F[x]$ such that $g(x) = f(x^p)$. Let d, d_1 denote respectively the degrees of $g(x)$ and $f(x)$. Then $d = pd_1$ which implies that $d_1 < d$. Since $[F(\alpha) : F] = d$, $\{1, \alpha, \ldots, \alpha^{d_1}\}$ is linearly independent over F. By what has been proved in the above paragraph, $\{1, \alpha^p, \ldots, \alpha^{d_1 p}\}$ is linearly independent over F. But $0 = g(\alpha) = f(\alpha^p)$ which implies that $\{1, \alpha^p, \ldots, \alpha^{d_1 p}\}$ is linearly dependent over F. This contradiction proves that α is separable over F. □

The following corollary is an immediate consequence of the above theorem.

Corollary A.23 *Let α be algebraic over a field F of characteristic $p > 0$. Then $F(\alpha)/F$ is separable if and only if $F(\alpha^p) = F(\alpha)$.*

Corollary A.24 *If α is separable over a field F, then $F(\alpha)/F$ is a separable extension.*

Proof Since every finite extension of a field of characteristic zero is separable, it is enough to prove the corollary when characteristic of F is $p > 0$. Arguing as for the proof of equation (A.1), we see that $F(\alpha) = F(\alpha^p)$. Hence by the above corollary, $F(\alpha)$ is a separable extension of F. □

Theorem A.25 (Transitive property of separable extensions) *If L/K and K/F are separable extensions, then so is the extension L/F.*

Proof The theorem needs to be proved when F is a field of characteristic $p > 0$. We first prove the result when L/K and K/F are finite. By Theorem A.22, $K = FK^p$ and $L = KL^p$. Now $L = KL^p = FK^pL^p \subseteq FL^p \subseteq L$. Hence $L = FL^p$. Again applying Theorem A.22, we see that L/F is a separable extension.

We now prove the result for general separable extensions. Let α be any element of L and $g(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ be the minimal polynomial of α over K. Consider the subfield $F_1 = F(a_1, a_2, \ldots, a_n)$ of K. Then $g(x)$ is a separable polynomial over F_1. So α is separable over F_1. Therefore by Corollary A.24, $F_1(\alpha)/F_1$ is a separable extension. Also F_1/F is a finite separable extension because each element of the subfield F_1 of K is separable over F. It follows from the transitive property of finite separable extensions that $F_1(\alpha)/F$ is a separable extension. Hence α is separable over F. □

Corollary A.26 *Let K/F be an extension of fields. The set F^S of all elements of K which are separable over F forms a subfield of K.*

Proof Let $\alpha, \beta \in K$ be separable over F. It is to be shown that $\alpha \pm \beta, \alpha\beta$ and α/β are separable over F. Now $F(\alpha)/F$ is separable by Corollary A.24 . Also $F(\alpha, \beta)/F(\alpha)$ is separable by the same corollary. Therefore by the transitive property of separable extensions, $F(\alpha, \beta)/F$ is separable. □

The following corollary is an immediate consequence of the above Corollary A.26.

Corollary A.27 *If elements $\alpha_1, \alpha_2, \ldots, \alpha_n$ of an extension of a field F are separable over F, then $F(\alpha_1, \alpha_2, \ldots, \alpha_n)/F$ is a separable extension.*

Definition The set F^S given in Corollary A.26 is called the *separable closure* of F in K and the degree $[F^S : F]$ is called the *separable degree* of the extension K/F. The degree of K/F^S is called the *inseparable degree* of K/F.

Finite separable extensions have a special property which is given by the following theorem.

Theorem A.28 (Primitive Element Theorem) *Every finite separable extension is simple. More generally if $K = F(\theta_1, \theta_2, \ldots, \theta_n)$ is a finite extension of a field F and if at least $n - 1$ of the elements $\theta_1, \ldots, \theta_n$ are separable over F, then K is a simple extension of F.*

Proof We prove the second assertion and its proof is split into two cases.
Case I. F is a finite field.
In this case, K is a finite field and the multiplicative group of non-zero elements of K is cyclic, say generated by δ in view of a basic result of group theory (cf. [Her, Chap. 2]). In this case, $K = F(\delta)$ is a simple extension.
Case II. F is infinite.
Let $K = F(\theta_1, \theta_2, \ldots, \theta_n)$ where at least $n - 1$ of $\theta_1, \theta_2, \ldots, \theta_n$ are separable over F. In this case, we prove the result by induction on n. It is trivial when $n = 1$. Next we prove the theorem when $n = 2$ and suppose $K = F(\alpha, \beta)$ with α separable over F. We need to show that K/F is a simple extension when α, β do not belong to F. Let $f(x), g(x) \in F[x]$ be the minimal polynomials of α, β respectively over F. Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_r$ be the roots of $f(x)$, $\beta_1 = \beta, \beta_2, \ldots, \beta_s$ be the roots of $g(x)$ in a splitting field of $f(x)g(x)$. As α is separable over F so the roots of $f(x)$ are distinct. Since F is infinite, there exists a non-zero element $c \in F$ such that c is different from $\frac{\beta-\beta_j}{\alpha_i-\alpha}$, for $2 \leqslant i \leqslant r$, $1 \leqslant j \leqslant s$. Set $\gamma = \beta + c\alpha$. We claim that $F(\gamma) = F(\alpha, \beta)$. Clearly $F(\gamma) \subseteq F(\alpha, \beta)$. Since $\beta = \gamma - c\alpha$, $g(\gamma - c\alpha) = 0$. Thus α is a common root of the polynomials $f(x)$ and $h(x) := g(\gamma - cx)$. Write

$$h(x) = \prod_{j=1}^{s}(\gamma - cx - \beta_j) = (-c)^s \prod_{j=1}^{s}[(x - \alpha) - c^{-1}(\beta - \beta_j)].$$

In view of the choice of c, the above equation shows that α is the only common root of $f(x)$ and $h(x)$. Since $f(x)$ is separable, $(x-\alpha)$ is the greatest common divisor of $f(x)$ and $h(x)$. As the coefficients of $f(x)$ and $h(x)$ lie in $F(\gamma)$, the coefficients of their greatest common divisor also lie in $F(\gamma)$. So $\alpha \in F(\gamma)$. Then $\beta = \gamma - c\alpha \in F(\gamma)$. Hence $F(\alpha, \beta) \subseteq F(\gamma)$ so that $F(\gamma) = F(\alpha, \beta)$ as claimed. This completes the proof when $n = 2$.

When $n > 2$, assume that $\theta_1, \ldots, \theta_{n-1}$ are separable over F, then by induction hypothesis, $F(\theta_2, \ldots, \theta_n)$ is a finite simple extension, say $F(\theta)$ of F. Therefore by the case $n = 2$, $F(\theta_1, \theta_2, \ldots, \theta_n) = F(\theta_1, \theta)$ is a simple extension of F. □

Definition Let K/F be an extension of fields of characteristic $p > 0$. An element α of K is said to be *purely inseparable* over F if the minimal polynomial of α over F has only one root. The extension K/F is said to be purely inseparable if every element of K is purely inseparable over F.

Note that an element α of K is both separable and inseparable over F if and only if $\alpha \in F$.

Theorem A.29 *Let K/F be an algebraic extension of fields of characteristic $p > 0$. Let F^S denote the separable closure of F in K. Then K/F^S is a purely inseparable extension. In particular every algebraic extension can be written as a separable extension followed by a purely inseparable extension.*

Proof Let α be any element of K. To prove the theorem, it is enough to show that there exists $e \geqslant 0$ such that $\alpha^{p^e} \in F^S$; this will prove that α is purely inseparable over F^S because it will satisfy the polynomial $x^{p^e} - \alpha^{p^e} = (x-\alpha)^{p^e}$ over F^S. Let $g(x)$ be the minimal polynomial of α over F. If α is separable over F, then $\alpha \in F^S$. If not, then by Corollary A.19, $g(x)$ is a polynomial in x^p, say $g(x) = g_1(x^p)$, $g_1(x) \in F[x]$. Note that $g_1(x)$ being irreducible over F is the minimal polynomial of α^p over F. If α^p is separable over F, then $\alpha^p \in F^S$. If not, then by Corollary A.19, $g_1(x) = g_2(x^p)$ for some $g_2(x) \in F[x]$. Note that $g_2(x)$ is the minimal polynomial of α^{p^2} over F and $\deg g_2(x) = \frac{\deg g_1(x)}{p} = \frac{\deg g(x)}{p^2}$. Repeating the above argument, we see that there exists e such that α^{p^e} must be separable over F. □

A.4 Normal Extensions

Definition An algebraic extension K/F is called a *normal extension* if whenever an irreducible polynomial $g(x) \in F[x]$ has one root in K, then it has all roots in K.

Examples

(i) Any extension K/F of degree two is normal because if an irreducible polynomial $g(x) = ax^2 + bx + c$ has one root β in K, then its other root namely $-\beta - b/a$ also belongs to K.

(ii) If K/F is a normal extension, then the separable closure F^S of F in K is also a normal extension of F.

(iii) Let θ be a root of the polynomial $x^4 - 2$, then $\mathbb{Q}(\theta)/\mathbb{Q}$ is not a normal extension.

Definition Two elements α and α' lying in an extension of a field F and both algebraic over F are said to be *conjugates* over F or F-*conjugates* if they have the same minimal polynomial over F.

Proposition A.30 *Let α and α' be algebraic over a field F. Then α and α' are conjugates over F if and only if there exists an F-isomorphism σ from $F(\alpha)$ onto $F(\alpha')$ with $\sigma(\alpha) = \alpha'$.*

Proof Suppose first that α and α' are the roots of the same monic irreducible polynomial $g(x)$ belonging to $F[x]$. By Proposition A.2, $F(\alpha) = F[\alpha]$ and $F(\alpha') = F[\alpha']$. Let $h(\alpha)$ be any element of $F(\alpha)$, $h(x) \in F[x]$. We define $\sigma(h(\alpha)) = h(\alpha')$. Then σ is well defined because if $h(\alpha) = h_1(\alpha)$ with $h_1(x) \in F[x]$, then $g(x)$ divides $h(x) - h_1(x)$ and hence $h(\alpha') = h_1(\alpha')$. It can be easily seen that σ is an F-isomorphism of $F(\alpha)$ onto $F(\alpha')$.

Conversely, assume that there exists an F-isomorphism σ from $F(\alpha)$ onto $F(\alpha')$ with $\sigma(\alpha) = \alpha'$. Let $g(x)$ denote the minimal polynomial of α over F. Now $g(\alpha) = 0$ implies that $\sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\alpha') = 0$. Therefore α and α' have the same minimal polynomial $g(x)$ over F. □

Remark A.31 If $g(x)$ is an irreducible polynomial over a field F having a root α and L is an extension of F containing a splitting field of $g(x)$ over F, then arguing as in the proof of above proposition, it can be easily seen that the number of F-isomorphisms of $F(\alpha)$ into L is the number of distinct roots of $g(x)$. In fact each of these F-isomorphisms is defined by mapping α onto a root of $g(x)$. In particular, if K/F is a finite separable extension of degree n, then by Theorem A.28, K/F is a simple extension and hence there are exactly n F-isomorphisms of K into a normal extension of F containing K.

The following two results will be used to give two more equivalent definitions of a finite normal extension.

Proposition A.32 *Let K be a splitting field of a polynomial $h(x) \in F[x]$ over a field F. If σ is an F-isomorphism from K into an extension of K, then $\sigma(K) = K$.*

Proof Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $h(x)$ in K so that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let σ be an F-isomorphism from K into an extension of K. Write $h(x) = \prod_{i=1}^{n}(x - \alpha_i)$. Applying σ, we obtain $h(x) = \prod_{i=1}^{n}(x - \sigma(\alpha_i))$. So $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$ is a permutation of $\alpha_1, \alpha_2, \ldots, \alpha_n$. Therefore

$$\begin{aligned}\sigma(K) = \sigma(F(\alpha_1, \alpha_2, \ldots, \alpha_n)) &= F(\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)) \\ &= F(\alpha_1, \alpha_2, \ldots, \alpha_n) = K.\end{aligned}$$

□

Theorem A.33 *Let K/F be a finite extension of fields. Then the extension K/F is normal if and only if K is a splitting field over F of some polynomial in $F[x]$.*

Proof Let K/F be a finite normal extension. Write $K = F(\beta_1, \beta_2, \ldots, \beta_m)$. Let $g_i(x) \in F[x]$ be the minimal polynomial of β_i over F and define $h(x) = \prod_{i=1}^{m} g_i(x)$. Then K contains all roots of $h(x)$ and hence it is a splitting field of $h(x)$ over F.

Conversely let K be a splitting field of a polynomial $h(x) \in F[x]$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be all the roots of $h(x)$ so that $K = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Let $\beta \in K$ be any root of a monic irreducible polynomial $g(x) \in F[x]$. Let β' be another root of $g(x)$ in an extension of K. We have to prove that $\beta' \in K$. Since β and β' are F-conjugates, there exists an F-isomorphism σ from $F(\beta)$ onto $F(\beta')$ with $\sigma(\beta) = \beta'$ by Proposition A.30. Note that splitting fields of $h(x)$ over $F(\beta)$ and $F(\beta')$ are respectively $K(\beta) = K$ and $K(\beta') = F(\beta', \alpha_1, \ldots, \alpha_n)$. Therefore by Theorem A.12, σ can be extended to an F-isomorphism σ_1 from K onto $K(\beta')$. By Proposition A.32, $\sigma_1(K) = K$, so $\beta' = \sigma_1(\beta)$ belongs to K. This proves that K/F is normal. □

Definition Let K/F be a finite extension. It can be easily seen that there exists a smallest normal extension L of F such that $K \subseteq L$. The field L is called a *normal closure* of K over F. In fact if $K = F(\beta_1, \beta_2, \ldots, \beta_m)$ and $g_i(x) \in F[x]$ is the minimal polynomial of β_i over F, then L is a splitting field of $h(x) = \prod_{i=1}^{m} g_i(x)$ over F. So L is unique upto F-isomorphism.

Proposition A.34 *Let K be a finite normal extension of a field F and E be a subfiled of K containing F. Then every F-isomorphism of E into K can be extended to an F-automorphism of K.*

Proof Let σ be an F-isomorphism of E into K. Since K/F is a finite normal extension, K is a splitting field of a polynomial say $h(x) \in F[x]$ over F by Theorem A.33. So K is also a splitting field of $h(x)$ over E. Therefore in view of Theorem A.12, σ can be extended to an F-automorphism of K. □

Using the above proposition, we prove the following theorem which gives two more equivalent definitions of a finite normal extension.

Theorem A.35 *The following statements are equivalent for a finite extension K of a field F:*

(i) *K/F is a normal extension.*
(ii) *K is a splitting field over F of a polynomial $h(x)$ belonging to $F[x]$.*
(iii) *Every F-isomorphism of K into any extension of K has image K.*

Proof (i) and (ii) are equivalent in view of Theorem A.33 and (ii) implies (iii) in view of Theorem A.32. We now prove that (iii) implies (i). Let L be a finite normal extension of F containing K. Let $\beta \in K$ be any root of a monic irreducible polynomial $g(x) \in F[x]$. Let β' be another root of $g(x)$ in the extension L of K. We have to prove that $\beta' \in K$. Since β and β' are F-conjugates, there exists an F-isomorphism τ from $F(\beta)$ onto $F(\beta')$ with $\tau(\beta) = \beta'$ in view of Proposition A.30. By Proposition A.34, τ can be extended to an F-automorphism $\bar{\tau}$ (say) of L. On restricting $\bar{\tau}$ to K and using assertion (iii), we see that $\bar{\tau}(K) = K$ and hence $\beta' = \bar{\tau}(\beta)$ belongs to K. This proves that K/F is normal. □

Keeping in mind the above theorem, the following corollary can be easily verified.

Corollary A.36 *If K_1, K_2 are finite normal extensions of a field F, then so are K_1K_2 and $K_1 \cap K_2$.*

We shall quickly deduce the following corollary from Proposition A.34 and Theorem A.35.

Corollary A.37 *Let K be a finite normal extension of field F and E be a subfiled of K containing F. Then E/F is a normal extension if and only if $\sigma(E) = E$ for every F-automorphism σ of K.*

Proof It is immediate from Theorem A.35 that if E/F is a normal extension, then $\sigma(E) = E$ for every F-automorphism σ of K. To prove the converse, assume that $\sigma(E) = E$ for every F-automorphism σ of K. Let $g(x) \in F[x]$ be an irreducible polynomial having a root $\beta \in E$ and β' be another root of $g(x)$. Since K/F is normal, $\beta' \in K$. Let τ be an F-isomorphism from $F(\beta)$ into K defined by $\tau(\beta) = \beta'$. By Proposition A.34, τ can be extended to an F-automorphism $\bar{\tau}$ (say) of K. Then by our assumption $\bar{\tau}(E) = E$ and therefore $\beta' = \bar{\tau}(\beta)$ belongs to E. This proves that E/F is a normal extension. □

Example A.38 Every finite extension K of a finite field F is normal, because if $|K| = q = p^m$, then as shown in the proof of Corollary A.15, K is a splitting field of $X^q - X$ over F_p and hence it is also splitting field of $X^q - X$ over F. Therefore K/F is normal by Theorem A.35. In fact every algebraic extension L of a finite field F is normal because whenever L contains a root α of an irreducible polynomial $g(x)$ belonging to $F[x]$, then all roots of $g(x)$ belong to the normal extension $F(\alpha)$ of F.

Remark Normality is not a transitive relation. For example; consider $K = \mathbb{Q}(\theta)$ where θ is a real root of $x^4 - 2$, then $\mathbb{Q}(\theta)/\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ are normal but $\mathbb{Q}(\theta)/\mathbb{Q}$ is not a normal extension.

A.5 Galois Extensions

> "Galois theory is a show piece of mathematical unification, bringing together several different branches of the subject and creating a powerful machine for the study of problems of considerable historical and mathematical importance."
>
> Ian Stewart—Galois Theory[6]

Definition An extension K/F is called a *Galois extension* if it is both normal and separable.

Examples

(i) An extension of degree 2 of a field of characteristic different from 2 is a Galois extension.

(ii) A generator of the cyclic group consisting of all nth roots of unity in $\mathbb{C}$ is called a primitive nth root of unity. If ζ is a primitive nth root of unity in $\mathbb{C}$, then $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a Galois extension being the splitting field of $X^n - 1$ over $\mathbb{Q}$. The field $\mathbb{Q}(\zeta)$ is called nth cyclotomic field. Such extensions of $\mathbb{Q}$ are called cyclotomic extensions.

(iii) An algebraic extension of a finite field is a Galois extension in view of Corollary A.21 and Example A.38.

(iv) If K/F is a Galois extension and E is a subfield of K containing F, then K/E is also a Galois extension because the minimal polynomial of any element $\beta \in K$ over E divides the minimal polynomial of β over F. On the other hand E/F may fail to be Galois extension. For example: $K = \mathbb{Q}(2^{1/3}, \sqrt{-3})$ being a splitting field of the polynomial $x^3 - 2$, is a Galois extension of $\mathbb{Q}$ but $E = \mathbb{Q}(2^{1/3})$ fails to be a Galois extension of $\mathbb{Q}$.

Galois extensions are named after the French mathematician Évariste Galois (1811–1832) and are of fundamental importance in field theory. Galois gave a complete solution to the problem partially solved by Gauss, Ruffini and Abel of solving a polynomial equation by radicals in 1830 when he submitted a memoir to the Paris Academy of Sciences on the theory of equations. In this memoir, he described what is now known as the Galois group of a polynomial and used this group to derive necessary and sufficient conditions for a polynomial to be solvable by radicals. For complete details along with the history of this problem, the reader is referred to the interesting book [Tig] by Jean-Pierre Tignol.

Definition Let K/F be a Galois extension. The set of all F-automorphisms of K is a group with respect to the composition of maps. This group is called the *Galois group*[7] of K/F and will be denoted by $\mathrm{Gal}(K/F)$.

---

[6] The book entitled Galois Theory by Ian Stewart is published by CRC Press, 2003.

[7] It may be pointed out that this definition of Galois group is very different from the one given by Galois in his memoir written by him at the age of 19. He only dealt with splitting fields of polynomials and for him, the Galois group consisted of certain permutations of the roots. The modern formulation of Galois theory is due to Emil Artin who published his own account of Galois theory in 1938 and 1942 (cf. [Art]).

Example Let d, d_1 be distinct squarefree integers. We show that $K = \mathbb{Q}(\sqrt{d}, \sqrt{d_1})$ is a Galois extension of $\mathbb{Q}$ having Galois group isomorphic to Klein's 4-group. Since K is the splitting field of the polynomial $(x^2 - d)(x^2 - d_1)$ over $\mathbb{Q}$, it is a normal extension of $\mathbb{Q}$ of degree 4. If $\sigma \in \text{Gal}(K/\mathbb{Q})$, then $\sigma(\sqrt{d}) = \epsilon\sqrt{d}$, with $\epsilon \in \{1, -1\}$ and so $\sigma^2(\sqrt{d}) = \sqrt{d}$. Similarly $\sigma^2(\sqrt{d_1}) = \sqrt{d_1}$ and hence σ^2 is identity. Therefore $\text{Gal}(K/\mathbb{Q})$ is isomorphic to Klein's 4-group.

We shall now compute the degree of the nth cyclotomic field over $\mathbb{Q}$ as well as its Galois group.

Definition Let n be a positive integer. The polynomial $\prod_{\eta}(x - \eta)$, where η runs over all primitive nth roots of unity in $\mathbb{C}$ is called the nth cyclotomic polynomial and will be denoted by $\Phi_n(x)$. The degree of $\Phi_n(x)$ is $\phi(n)$.

Note that $\Phi_1(x) = x - 1$, $\Phi_2(x) = x + 1$ belong to $\mathbb{Z}[x]$. The following lemma shows that this holds for every n.

Lemma A.39 *The nth cyclotomic polynomial $\Phi_n(x)$ is in $\mathbb{Z}[x]$ for every $n \geq 1$.*

Proof The lemma is proved by induction on n. We first show that $\forall n \geq 1$,

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \tag{A.2}$$

The above equality holds because every nth root of unity is a primitive dth root of unity for a unique divisor d of n and the polynomials on either side of (A.2) do not have any repeated root. By induction hypothesis, the polynomial

$$g(x) := \prod_{\substack{d|n \\ d \neq n}} \Phi_d(x)$$

belongs to $\mathbb{Z}[x]$. Since $g(x)$ is monic, it now follows from (A.2) that the polynomial $\Phi_n(x) = (x^n - 1)/g(x)$ belongs to $\mathbb{Z}[x]$. □

Theorem A.40 *If ζ is a primitive nth root of unity in $\mathbb{C}$, then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$. Equivalently, the cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.*

Proof Let $f(x) \in \mathbb{Q}[x]$ be the minimal polynomial of ζ over $\mathbb{Q}$. In view of Lemma A.39, $f(x)$ divides $\Phi_n(x)$. We shall prove that if $f(x)$ has a root η, then η^p is also a root of $f(x)$ for each prime p not dividing n. Since every primitive nth root of unity can be written as $\zeta^{p_1 \cdots p_r}$ for some primes p_i not dividing n, successive application of the above result will imply that every primitive nth root of unity is a root of $f(x)$ and hence the theorem will be proved.

Since $f(x)$ divides $x^n - 1$, there exists $h(x) \in \mathbb{Q}[x]$ such that $x^n - 1 = f(x)h(x)$. Using Gauss' lemma,[8] it can be easily seen that the monic polynomials $f(x), h(x)$

[8] Gauss' lemma states that product of two primitive polynomials over $\mathbb{Z}$ is primitive.

belong to $\mathbb{Z}[x]$. Suppose to the contrary, η^p is not a root of $f(x)$ for some prime p not dividing n and for some root η of $f(x)$. Then η^p is a root of $h(x)$, i.e., η is a root of $h(x^p)$. Since $f(x)$ is the minimal polynomial of η over $\mathbb{Q}$, we can write $h(x^p) = f(x)g(x)$ for some $g(x) \in \mathbb{Q}[x]$. As $f(x)$ is a monic polynomial with coefficients in $\mathbb{Z}$, so $g(x) \in \mathbb{Z}[x]$. Using Fermat's little theorem, we see that $h(x^p) \equiv (h(x))^p \pmod{p}$ and hence

$$(h(x))^p \equiv f(x)g(x) \pmod{p}.$$

If $\overline{f}(x), \overline{h}(x)$ denote the polynomials over $\mathbb{Z}/p\mathbb{Z}$ obtained by reducing the coefficients of $f(x), h(x)$ modulo p, then it follows from the above congruence that $\overline{f}(x)$ and $\overline{h}(x)$ have a common factor. But $x^n - \overline{1} = \overline{f}(x)\overline{h}(x)$ and hence $x^n - \overline{1}$ has a repeated root in an extension of $\mathbb{Z}/p\mathbb{Z}$. In view of Proposition A.16, this is impossible because p does not divide n and the theorem is proved. □

Corollary A.41 *Let $K = \mathbb{Q}(\zeta)$ where ζ is a primitive nth root of unity. Then the Galois group G of the extension $K/\mathbb{Q}$ consists of $\phi(n)$ automorphisms σ_r, $1 \leq r \leq n$, $(r, n) = 1$, defined by $\sigma_r(\zeta) = \zeta^r$ and G is isomorphic to the group $(\mathbb{Z}/n\mathbb{Z})^\times$ of reduced residue classes modulo n.*

Proof By Theorem A.40, $\Phi_n(x)$ is the minimal polynomial of ζ over $\mathbb{Q}$. So the $\mathbb{Q}$-conjugates of ζ are ζ^r, $1 \leq r \leq n$, $(r, n) = 1$. Consequently by Remark A.31, we have exactly $\phi(n)$ isomorphisms σ_r from K into K defined by $\sigma_r(\zeta) = \zeta^r$ with r as above; in fact each of these is an automorphism of K because $\sigma_r(K) = \mathbb{Q}(\zeta^r) = \mathbb{Q}(\zeta)$. So the first assertion of the corollary is proved. Since ζ^r and hence σ_r depends only upon the residue class $\overline{r}$ of r modulo n, therefore the mapping $\overline{r} \mapsto \sigma_r$ from $(\mathbb{Z}/n\mathbb{Z})^\times$ into G is well defined and bijective. It is a group homomorphism, because if $(rs, n) = 1$, then

$$\sigma_{rs}(\zeta) = \zeta^{rs} = \sigma_r(\zeta^s) = \sigma_r(\sigma_s(\zeta)) = \sigma_r \circ \sigma_s(\zeta).$$

This completes the proof of the corollary. □

Definition Let G be a subgroup of the group of all automorphisms of a field K. Then it can be easily seen that the set $\{\alpha \in K \mid \sigma(\alpha) = \alpha \ \forall\, \sigma \in G\}$ is a subfield of K. It is called the *fixed field* of G.

Theorem A.42 *Let K/F be a Galois extension of degree n. Then the Galois group of K/F is a group of order n and F is the fixed field of* $\mathrm{Gal}(K/F)$.

Proof Since K/F is a separable extension, we can write $K = F(\alpha)$ by virtue of Theorem A.28 of primitive elements. Let $g(x)$ denote the minimal polynomial of α over F. Since K/F is a normal extension, all the roots of $g(x)$, say $\alpha_1, \alpha_2, \ldots, \alpha_n$ are in K and these are distinct. If σ is any F-isomorphism of K into an extension of K, then by Theorem A.35, $\sigma(K) = K$. Therefore in view of Remark A.31, $\mathrm{Gal}(K/F)$ consists of F-automorphisms, $\sigma_1, \ldots, \sigma_n$ of K defined by $\sigma_i(\alpha) = \alpha_i$. This proves the first assertion of the theorem.

Let L denote the fixed field of $\mathrm{Gal}(K/F)$. Suppose to the contrary that $F \subsetneqq L$. Choose an element $\beta \in L \setminus F$. Let $h(x)$ denote the minimal polynomial of β over F. Then $\deg h(x) > 1$ and $h(x)$ is a separable polynomial. So there exists a root $\beta' \neq \beta$ of $h(x)$ in K. Let $\sigma : F(\beta) \to F(\beta')$ be an F-isomorphism such that $\sigma(\beta) = \beta'$. By Proposition A.34 applied to the intermediate field $F(\beta)$, we see that σ can be extended to an F-automorphism σ_1 of K. But $\sigma_1(\beta) = \sigma(\beta) = \beta' \neq \beta$, which contradicts the fact that β belongs to the fixed field of Galois group of K/F. This contradiction proves that $L = F$. □

Theorem A.43 (Artin's Theorem) *Let G be a finite group of automorphisms of a field K and F be the fixed field of G. Then K/F is a Galois extension with* $\mathrm{Gal}(K/F) = G$.

Proof Let $\sigma_1, \sigma_2, \ldots, \sigma_n$ be all the distinct elements of G. We first prove that K/F is a separable extension. Indeed we prove that every element α of K is separable over F and $[F(\alpha) : F] \leq n$. Let α be an element of K. Let $\beta_1, \ldots, \beta_m$ be all the distinct elements among $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$. Note that for any $\sigma \in G$, $\sigma(\beta_1), \sigma(\beta_2), \ldots, \sigma(\beta_m)$ are distinct and hence form a permutation of $\beta_1, \ldots, \beta_m$. Consider the polynomial $g(x) \in K[x]$ of degree $m \leqslant n$ defined by $g(x) = \prod_{i=1}^{m}(x - \beta_i)$. Then in view of what has been said above, for every σ belonging to G,

$$g^{\sigma}(x) = \prod_{i=1}^{m}(x - \sigma(\beta_i)) = \prod_{i=1}^{m}(x - \beta_i) = g(x).$$

Hence $g(x) \in F[x]$. Since $g(x)$ has distinct roots, the minimal polynomial of α over F being a factor of $g(x)$ has distinct roots. Therefore α is separable over F with $[F(\alpha) : F] \leq n$. Hence K/F is a separable extension.

We next prove that K/F is a finite extension of degree not exceeding n. Note that for any finite subextension N/F of K/F, N/F is a simple extension by Theorem A.28 and hence $[N : F] \leq n$ by what has been proved in the above paragraph. Among all finite subextensions N/F, choose the one for which $[N : F]$ is the maximum and denote this extension by M. We claim $M = K$. Suppose to the contrary that there exists $\beta \in K \setminus M$ and denote $M(\beta)$ by M_1. Then $[M_1 : F] = [M_1 : M][M : F] > [M : F]$ contrary to the choice of M. So $K = M$, which is a finite extension of F of degree not exceeding n.

Now it will be shown that K/F is a normal extension. By Theorem A.28, we can write $K = F(\delta)$. Then for $i \neq j$, $\sigma_i(\delta) \neq \sigma_j(\delta)$. Consider $h(x) = \prod_{i=1}^{n}(x - \sigma_i(\delta))$. Arguing as in the first paragraph of the proof, we see that $h(x) \in F[x]$. Since each $\sigma_i(\delta) \in K$, K is a splitting field of $h(x) \in F[x]$. Therefore K/F is a normal extension in view of Theorem A.35 .

Clearly $G \subseteq \mathrm{Gal}(K/F)$. By Theorem A.42, $\mathrm{Gal}(K/F)$ has order $[K : F]$. As shown above $[K : F] \leqslant n$. Therefore keeping in view the fact $|G| = n$, we see that $G = \mathrm{Gal}(K/F)$. □

Using above two results, we prove the main result of this chapter.

Theorem A.44 (Fundamental Theorem of Galois Theory) *Let K/F be a finite Galois extension. For any subfield T of K which contains F, let $G(K, T)$ denote the subgroup of $G(K, F) = \mathrm{Gal}(K/F)$ consisting of those automorphisms which are identity on T. For any subgroup H of $G(K, F)$, let K_H denote the fixed field of H. Then the mapping $T \mapsto G(K, T)$ sets up a one-to-one correspondence between the set of subfields of K which contain F onto the set of subgroups of $G(K, F)$ such that*

(i) $T = K_{G(K,T)}$,
(ii) $H = G(K, K_H)$,
(iii) $[K : T] =$ *order of* $G(K, T)$ *and* $[T : F] =$ *index of* $G(K, T)$ *in* $G(K, F)$,
(iv) T *is a normal extension of* F *if and only if* $G(K, T)$ *is a normal subgroup of* $G(K, F)$,
(v) *when* T *is a normal extension of* F, *then* $G(T, F)$ *is isomorphic to* $G(K, F)/G(K, T)$.

Proof Note that for any intermediate field T, K/T is a Galois extension, therefore by Theorem A.42, T is the fixed field of $G(K, T)$ which proves (i). Second assertion follows from Theorem A.43 applied to H. Also in view of Theorem A.42, we see that $|G(K, F)| = [K : F]$, $|G(K, T)| = [K : T]$. Therefore on dividing, assertion (iii) follows.

To prove (iv), suppose first that $G(K, T)$ is a normal subgroup of $G(K, F)$. For every $\sigma \in G(K, F)$, $\sigma G(K, T)\sigma^{-1} = G(K, T)$. In particular, their fixed fields are the same. Keeping in mind that the fixed field of $\sigma G(K, T)\sigma^{-1}$ is $\sigma(T)$, we see that $\sigma(T) = T \ \forall \ \sigma \in G(K, F)$. This proves that T/F is a normal extension in view of Corollary A.37. Conversely suppose that T is a normal extension of F. Note that for any $\sigma \in G(K, F)$, $\sigma(T) = T$ in view of Theorem A.35. Therefore the mapping $\Phi : G(K, F) \to G(T, F)$ given by $\Phi(\sigma) = \sigma|_T$ is clearly a group homomorphism with $\ker(\Phi) = G(K, T)$. By virtue of Proposition A.34, Φ is onto. So by first isomorphism theorem of groups, $G(K, F)/G(K, T)$ is isomorphic to $G(T, F)$. Therefore $G(K, T)$ is a normal subgroup of $G(K, F)$ and hence the theorem is proved. □

Definition A Galois extension K/F is called *cyclic* (respectively abelian) if its Galois group is cyclic (respectively abelian[9]).

In view of the fact that a subgroup of an abelian group is normal and a factor group of an abelian (respectively cyclic) group is abelian (respectively cyclic), the corollary stated below follows quickly from assertions (iv), (v) of Theorem A.44.

Corollary A.45 *Let K be a finite Galois extension of a field F which is abelian (respectively cyclic). If E is an intermediate field of the extension K/F, then E/F is a Galois extension and is abelian (respectively cyclic).*

[9] The terminology 'abelian extension' seems to have been initiated by Leopold Kronecker who stated and partially proved Kronecker-Weber Theorem which says that every finite abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension.

Keeping in mind that the number of subgroups of a cyclic group of order n is the number of divisors of n, the following corollary is an immediate consequence of Theorem A.44.

Corollary A.46 *Let K be a finite cyclic extension of a field F of degree n. Then the number of intermediate fields of K/F (including K, F) is the number of divisors of n.*

Remark An analogue of the fundamental theorem of Galois theory also holds for infinite Galois extensions. In fact Krull defined a topology on $\mathrm{Gal}(K/F)$ by taking as a fundamental system of open neighbourhoods of the identity the set of subgroups belonging to finite extensions of F contained in K. The closed subgroups are precisely those subgroups which are of the type $\mathrm{Gal}(K/L)$ where L runs over intermediate fields between K and F (cf. [Lan, Chap. VI], [Lu-Pa2, Chap. 2]).

Definition Let K be a finite extension of a finite field F consisting of q elements. The mapping σ defined on K by $\sigma(\alpha) = \alpha^q$, $\alpha \in K$ is clearly an F-automorphism of K. It is called the Frobenius automorphism of K/F.

With K/F as in the above definition, we shall prove below that its Frobenius automorphism generates the Galois group of K/F.

Proposition A.47 *Let K/F be an extension of finite fields. Then* $\mathrm{Gal}(K/F)$ *is a cyclic group generated by the Frobenius automorphism of K/F.*

Proof Let K/F be an extension of degree n with $|F| = q$. Then $|\mathrm{Gal}(K/F)| = n$ by the fundamental theorem of Galois theory. Consider the map $\sigma : K \longrightarrow K$ defined by $\sigma(\alpha) = \alpha^q$, $\alpha \in K$. It is easily checked that σ is an F-automorphism of K. Its powers $\sigma^0, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ are distinct, because otherwise σ^i is the identity map for some i, $0 < i < n$ and consequently $\alpha^{q^i} = \alpha$ for each α in K which is impossible as the polynomial $x^{q^i} - x$ can't have more roots than its degree. Thus $\mathrm{Gal}(K/F)$ is a cyclic group generated by σ. □

Definition Let $g(x)$ be a monic polynomial without repeated roots having coefficients in a field F. Let $\alpha_1, ..., \alpha_m$ be all the roots of $g(x)$ in its splitting field. In view of Corollary A.27 and Theorem A.33, $F(\alpha_1, ..., \alpha_m)$ is a Galois extension of F. Its Galois group is called the Galois group of $g(x)$ over F. This group is also called the Galois group of the equation $g(x) = 0$ over F.

Example Let m be an integer with $|m| > 1$ which is not divisible by the cube of any prime number. Then we show that the Galois group of the polynomial $g(x) = x^3 - m$ over $\mathbb{Q}$ is isomorphic to the symmetric group S_3 of degree 3. It can be easily seen that $g(x)$ is irreducible over $\mathbb{Q}$. Note that the splitting field K of $g(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(\theta, \omega)$, where θ is a root of $g(x)$ and $\omega \neq 1$ is a cube root of unity. Hence $[K : \mathbb{Q}] = 6$. So the Galois group of $g(x)$ over $\mathbb{Q}$ is either abelian or isomorphic to S_3. But this group can not be abelian in view of Corollary A.45, because the subextension $\mathbb{Q}(\theta)/\mathbb{Q}$ is not normal. Therefore $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to S_3.

A.6 Valued Fields

The development of Valuation Theory has a long history. It has its roots in the theory of p-adic numbers developed by Kurt Hensel in the first decade of 20th century. Motivated by the work of Hensel on p-adic numbers, it was the Hungarian mathematician Josef Kürschàk who gave the formal definition of valuation during the Cambridge International Congress of Mathematicians in 1912. His paper [Kür] which appeared one year later uses the term 'Bewertung' for a valuation. According to him, the notion of a valuation of a field K is a generalization of the notion of ordinary absolute value of the field $\mathbb{C}$ of complex numbers. In modern terminology, the valuations defined by Kürschàk are called 'absolute values'. An absolute value of a field K is a mapping ψ from K into real numbers satisfying the following axioms for all $a, b \in K$:

(I) $\psi(a) > 0$ for $a \neq 0$, $\psi(0) = 0$,
(II) $\psi(ab) = \psi(a)\psi(b)$,
(III) $\psi(a + b) \leq \psi(a) + \psi(b)$.

The development of valuation theory gained momentum by the discovery of the fact that much of Algebraic Number Theory can be better understood by using valuations. It is the famous number theorist Helmut Hasse who is often credited with this discovery.[10] Further significant contributions to Valuation Theory were made by Alexander Ostrowski. The terminology Archimedean and non-Archimedean for absolute values was introduced by Ostrowski in 1917. An absolute value ψ on a field K is called non-Archimedean if $\psi(a + b) \leq \max\{\psi(a), \psi(b)\}$ for all $a, b \in K$. It was Ostrowski who first used valuations in additive form in his 1918 paper [Ost]. An additive valuation v of a field K is a mapping $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ which satisfies the following properties for all $a, b \in K$:

(i) $v(a) = \infty$ if and only if $a = 0$,
(ii) $v(ab) = v(a) + v(b)$,
(iii) $v(a + b) \geq \min\{v(a), v(b)\}$.

The subgroup $v(K^\times)$ of $(\mathbb{R}, +)$ is called the value group of v and the pair (K, v) is called a valued field. It can be easily seen that additive valuations of K are in one-to-one correspondence with its non-Archimedean absolute values via the correspondence $v \longrightarrow \psi = e^{-v}$. Additive valuations are also known as classical valuations or real valuations. Hereafter by a valuation, we mean an additive valuation. To every valuation v of K is associated a subring R_v of K defined by $R_v = \{\alpha \in K \mid v(\alpha) \geq 0\}$ which is called the valuation ring of v. Two real valuations v, v' of K are said to be equivalent if there exists a real number $c > 0$ such that $v'(\alpha) = cv(\alpha)$ for every $\alpha \in K$. Note that equivalent valuations have the same valuation ring. The converse is also true (cf. [Iya, Chap. 2], [Nar, Chap. 1]); we shall omit the proof of the converse as it is not needed in the sequel.

[10] A detailed description of development of Valuation Theory and its applications in Algebraic Number Theory is given in Peter Roquette's masterly article [Roq1].

An additive valuation v is said to be discrete if its value group is a cyclic subgroup of $(\mathbb{R}, +)$ i.e., a valuation v is called discrete if it is equivalent to a valuation having value group $\mathbb{Z}$. One can easily verify that the valuation ring of a discrete valuation is indeed a discrete valuation ring as defined at the end of Sect. 3.2. Conversely if R is a discrete valuation ring with quotient field K, then one can define a discrete valuation v of K whose valuation ring is R as is done in the following example.
Note that if the field K is the quotient field of an integral domain R and v is a mapping on R satisfying properties (i), (ii), (iii) mentioned in the definition of an additive valuation, then v can be extended uniquely to a valuation of K in a natural way.

Example Let R be a unique factorization domain with quotient field K and π be a prime element of R. For any non-zero element α of R, let $v_\pi(\alpha)$ denote the highest power of π dividing α, i.e., $v_\pi(\alpha) = r$, where $\alpha = \pi^r\delta, \delta \in R, \pi \nmid \delta$. It is natural to set $v_\pi(0) = \infty$. Clearly the mapping v_π satisfies $v_\pi(\alpha\beta) = v_\pi(\alpha) + v_\pi(\beta)$ and $v_\pi(\alpha + \beta) \geq \min\{v_\pi(\alpha), v_\pi(\beta)\}$ for α, β in R. Hence v_π uniquely extends to a valuation of the quotient field of R. In particular when $K = \mathbb{Q}$ and π is a prime number p, then v_p is called the *p-adic* valuation of $\mathbb{Q}$. In 1916, Ostrowski proved that any non-trivial[11] valuation of $\mathbb{Q}$ is equivalent to v_p for some prime number p; a simple proof of this result is given in [Bo-Sh, Chap. 1, Sect. 4.2]).

Example Let $\mathfrak{p}$ be a maximal ideal of the ring of algebraic integers $\mathcal{O}_K$ of an algebraic number field K. For any non-zero element α of $\mathcal{O}_K$, let $v_\mathfrak{p}(\alpha)$ denote the highest power of $\mathfrak{p}$ dividing $\alpha\mathcal{O}_K$. If we set $v_\mathfrak{p}(0) = \infty$, then clearly $v_\mathfrak{p}$ satisfies $v_\mathfrak{p}(ab) = v_\mathfrak{p}(a) + v_\mathfrak{p}(b)$ and $v_\mathfrak{p}(a + b) \geq \min\{v_\mathfrak{p}(a), v_\mathfrak{p}(b)\}$ for a, b in $\mathcal{O}_K$ and hence it gives rise to a valuation of K which is denoted by $v_\mathfrak{p}$. It is also known that if v is a non-trivial valuation of an algebraic number field K , then v is equivalent to $v_\mathfrak{p}$ for some maximal ideal $\mathfrak{p}$ of $\mathcal{O}_K$ (cf.[Nar, Theorem 3.3]).

Strong Triangle Law. Let v be a valuation of a field K. If $\alpha, \beta \in K$ are such that $v(\alpha) \neq v(\beta)$, then $v(\alpha + \beta) = \min\{v(\alpha), v(\beta)\}$.

Proof. Assume that $v(\alpha) < v(\beta)$. By the definition of valuation

$$v(\alpha + \beta) \geq \min\{v(\alpha), v(\beta)\} = v(\alpha). \tag{A.3}$$

Again by a defining property of valuation,

$$v(\alpha) = v(\alpha + \beta - \beta) \geq \min\{v(\alpha + \beta), v(-\beta)\}.$$

Since $2v(-1) = v(1) = 0$, we have $v(-\beta) = v(\beta)$. So the above minimum has to be $v(\alpha + \beta)$ in view of the assumption $v(\alpha) < v(\beta)$. It now follows from (A.3) that $v(\alpha + \beta) = v(\alpha)$ as desired.

[11] A valuation is said to be non-trivial if its value group is not the singleton set $\{0\}$.

A.7 Eisenstein-Dumas Irreducibility Criterion

In 1850, Eisenstein proved a criterion which states that if $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is a polynomial with coefficients from $\mathbb{Z}$ and if there exists a prime p such that $p \nmid a_n$, $p|a_i$ for $0 \leq i \leq n-1$ and $p^2 \nmid a_0$, then the polynomial $f(x)$ is irreducible over $\mathbb{Q}$. This criterion has been widely generalised and extended to polynomials with coefficients in valued fields. In 1906, Dumas [Dum] generalised the criterion and proved the following result.

Eisenstein-Dumas Irreducibility Criterion. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients from $\mathbb{Z}$. Suppose that there exists a prime p such that $v_p(a_n) = 0$, $nv_p(a_i) \geq (n-i)v_p(a_0)$ for $1 \leq i \leq n-1$ and $v_p(a_0)$ is coprime to n, then $f(x)$ is irreducible over $\mathbb{Q}$.

Note that Eisenstein criterion is a special case of the above criterion with $v_p(a_0) = 1$. The following proposition will be used in the proof of this criterion.

Proposition A.48 *Let v be a valuation of a field K, μ be a real number and let $w : K[x] \longrightarrow \mathbb{R} \cup \{\infty\}$ be the mapping defined by*

$$w\Big(\sum_i c_i x^i\Big) = \min_i\{v(c_i) + i\mu\}, \quad c_i \in K.$$

Then w gives rise to a valuation on $K(x)$ whose restriction to K is v and whose value group is the subgroup of $\mathbb{R}$ generated by the value group of v and μ.

Proof Observe that $w(f(x)) = \infty$ if and only if $f(x)$=0. It will now be shown that if $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j$ are polynomials in $K[x]$, then

$$w(fg) = w(f) + w(g), \ w(f+g) \geq \min\{w(f), w(g)\}.$$

Write $fg = \sum_{k=0}^{m+n} c_k x^k$ where $c_k = \sum_{i+j=k} a_i b_j$. Let i_o, j_o be chosen so that

$$i_o = \min\{i \mid v(a_i) + i\mu = w(f)\}, \ j_o = \min\{j \mid v(b_j) + j\mu = w(g)\}.$$

Then

$$c_{i_o+j_o} = a_{i_o}b_{j_o} + \sum_{i+j=i_o+j_o, i\neq i_o} a_i b_j. \tag{A.4}$$

We show that

$$v(c_{i_o+j_o}) = v(a_{i_o}b_{j_o}).$$

Since $i \neq i_o, i+j = i_o+j_o$ imply that either $i < i_o$ or $j < j_o$, so either $v(a_{i_o}) + i_o\mu < v(a_i) + i\mu$ or $v(b_{j_o}) + j_o\mu < v(b_j) + j\mu$. Thus $v(a_{i_o}) + i_o\mu + v(b_{j_o}) +$

$j_o\mu < v(a_i) + i\mu + v(b_j) + j\mu$ *when* $i + j = i_o + j_o, i \neq i_o$. Consequently with $i + j = i_o + j_o, i \neq i_o$, we have $v(a_{i_o}b_{j_o}) < v(a_ib_j)$. Hence by (A.4) and strong triangle law, we have

$$v(c_{i_o+j_o}) = v(a_{i_o}b_{j_o}).$$

Therefore

$$v(c_{i_o+j_o}) + (i_o + j_o)\mu = v(a_{i_o}b_{j_o}) + (i_o + j_o)\mu = w(f) + w(g)$$

Thus we have shown that

$$w(fg) \leq v(c_{i_o+j_o}) + (i_o + j_o)\mu = w(f) + w(g). \tag{A.5}$$

On the other hand, for any $k, 0 \leq k \leq m + n$,

$$\begin{aligned} v(c_k) + k\mu &= v(\sum_{i+j=k} a_ib_j) + k\mu \geq \min_{i,j}\{v(a_i) + v(b_j) \mid i + j = k\} + k\mu \\ &= \min_{i,j}\{(v(a_i) + i\mu) + (v(b_j) + j\mu) \mid i + j = k\} \\ &\geq w(f) + w(g). \end{aligned}$$

So

$$w(fg) \geq w(f) + w(g). \tag{A.6}$$

By (A.5) and (A.6), we have $w(fg) = w(f) + w(g)$.

It remains to verify that $w(f + g) \geq \min\{w(f), w(g)\}$. Assume without loss of generality that $n = \max\{\deg f, \deg g\}$. Set $b_i = 0$ if $m + 1 \leq i \leq n$. Then for any i, $0 \leq i \leq n$, we have

$$\begin{aligned} v(a_i + b_i) + i\mu &\geq \min\{v(a_i), v(b_i)\} + i\mu \\ &= \min\{(v(a_i) + i\mu, v(b_i) + i\mu)\} \\ &\geq \min\{w(f), w(g)\}. \end{aligned}$$

Therefore

$$w(f + g) \geq \min\{w(f), w(g)\}.$$

□

We now prove the following theorem which has been proved in 2020 by Anuj Jakhar with slightly stronger hypothesis that the valuation of each coefficient except the leading coefficient of the polynomial is positive (cf. [Jak1]). This theorem immediately yields Eisenstein-Dumas Irreducibility Criterion. It has been shown that our version of the theorem quickly yields a well known irreducibility criterion by Angermüler.

Theorem A.49 *Let v be a valuation of a field K with value group G. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_0 \neq 0$ be a polynomial having coefficients in K with $v(a_n) = 0$ and $nv(a_i) \geq (n-i)v(a_0)$ for $0 \leq i \leq n-1$. Let d be the smallest positive integer such that $d\frac{v(a_0)}{n} \in G$. Then each irreducible factor of $f(x)$ over K has degree at least d.*

Proof Set $\mu = v(a_0)/n$. Let w denote the mapping on $K[x]$ defined by

$$w(\sum_i c_i x^i) = \min_i \{v(c_i) + i\mu\}, \quad c_i \in K.$$

By the above proposition, w gives a valuation on $K[x]$. In view of the hypothesis, we see that $\mu = \frac{v(a_0)}{n} = \min\limits_{0\leq i\leq n-1} \left\{\frac{v(a_i)}{n-i}\right\}$. Therefore

$$w(f(x)) = \min_{0\leq i\leq n} \{v(a_i) + i\mu\} = v(a_0) = n\mu. \tag{A.7}$$

Let $f(x) = f_1(x)f_2(x)\cdots f_t(x)$ be the factorization of $f(x)$ into irreducible factors over K where $f_i(x) = \sum\limits_{j=0}^{d_i} b_{ij}x^j$ has degree d_i and leading coefficient b_{id_i}. Since $v(a_n) = 0$, we may assume that $v(b_{id_i}) = 0$ for $1 \leq i \leq t$. Observe that

$$v(a_0) = v(\prod_{i=1}^{t} b_{i0}) = v(b_{10}) + \cdots + v(b_{t0})$$

and $n = d_1 + \cdots + d_t$. Therefore using (A.7), we see that

$$w(f(x)) = v(a_0) = v(b_{10}) + \cdots + v(b_{t0}) = n\mu = d_1\mu + \cdots + d_t\mu. \tag{A.8}$$

Also by definition of w, we have $w(f_i(x)) = \min\limits_{0\leq j\leq d_i} \{v(b_{ij}) + j\mu\}$; consequently

$$w(f_i(x)) \leq v(b_{i0}), \quad w(f_i(x)) \leq v(b_{id_i}) + d_i\mu = d_i\mu. \tag{A.9}$$

Now using (A.8), (A.9) and keeping in mind that

$$w(f(x)) = w(f_1(x)) + \cdots + w(f_t(x)),$$

it follows that

$$w(f_i(x)) = v(b_{i0}) = d_i\mu, \ 1 \leq i \leq t.$$

Consequently $d_i\mu \in G$ for $1 \leq i \leq t$. By hypothesis d is the smallest positive element such that $d\mu \in G$, hence $d_i \geq d$ for $1 \leq i \leq t$. This completes the proof of the theorem. □

The next corollary which extends Eisenstein-Dumas Irreducibility Criterion is an immediate consequence of the above theorem.

Corollary A.50 *Let v be a valuation of a field K having value group $\mathbb{Z}$. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, $a_0 \neq 0$ be a polynomial having coefficients in K with $v(a_n) = 0$ and $v(a_i)n \geq v(a_0)(n-i)$ for $1 \leq i \leq n-1$. The following hold:*

(i) *If n, $v(a_0)$ are coprime, then $f(x)$ is irreducible over K.*
(ii) *If $gcd(n, v(a_0)) = 2$, then either $f(x)$ is irreducible over K or it is a product of two irreducible polynomials of degree $\frac{n}{2}$ over K.*

Recall that if $f(x), g(y)$ are two polynomials in different indeterminates x, y, then $f(x) - g(y)$ is called a difference polynomial. As in [Ang], a polynomial $f(x, y)$ with coefficients in a field F in two indeterminates x, y is said to be a generalized difference polynomial (with respect to x) of the type (m, n) if $f(x, y) = cx^n + \sum_{i=1}^{n} P_i(y)x^{n-i}$, where $0 \neq c \in F$, $n \geq 1$, $m = \deg P_n(y) \geq 1$ and $\deg P_i(y) < \frac{mi}{n}$ for $1 \leq i \leq n-1$. Note that a difference polynomial is a generalized difference polynomial, because in this situation $\deg P_i(y) = 0$ for $1 \leq i \leq n-1$. It may be pointed out that contrary to appearances, the property of being a generalized difference polynomial is actually symmetric in x, y (see [Bh-Kh]).

The following corollary which gives a new and simpler proof of a well-known result by Angermüler (cf. [Ang, Bh-Kh]) regarding generalized difference polynomials is shown to be a quick application of assertion (i) of Corollary A.50.

Corollary A.51 *Let $P(x, y) = cx^n + \sum_{i=1}^{n} P_i(y)x^{n-i}$ be a generalized difference polynomial of the type (m, n) having coefficients in a field F with m, n coprime, then $P(x, y)$ is irreducible over F.*

Proof Consider the field $K = F(y)$, the field of rational functions in an indeterminate y with coefficients from F. Let v denote the valuation of K defined on its subring $F[y]$ by

$$v(h(y)) = -\deg(h(y)), \quad h(y) \in F[y].$$

Let $Q(x)$ denote the polynomial $P(x, y)$ when regarded as a polynomial in x with coefficients from K. In view of the definition of a generalized difference polynomial, $Q(x)$ satisfies the hypothesis of assertion (i) of Corollary A.50. Thus $Q(x)$ is irreducible over K and hence $P(x, y)$ is irreducible over F, because the gcd of the coefficients of $Q(x)$ in the unique factorisation domain $F[y]$ is a unit. □

The following corollary is an application of Theorem A.49. The irreducibility of the class of polynomials occurring in this corollary cannot be established by Eisenstein-Dumas Irreducibility Criterion.

Corollary A.52 *Let p be a prime number and a be an integer with $v_p(a)$ positive and even. Then the polynomial $f(x) = x^6 + ax + p^2$ is irreducible over $\mathbb{Q}$.*

Proof Suppose to the contrary that $f(x)$ is reducible over $\mathbb{Q}$. Then by assertion (ii) of Corollary A.50, $f(x)$ factors as a product of two monic irreducible polynomials, say $g(x)$, $g_1(x)$ of degree 3 over $\mathbb{Q}$. Since $f(x) \in \mathbb{Z}[x]$ is monic, using Gauss's lemma for primitive polynomials, it can be easily seen that $g(x)$, $g_1(x)$ are in $\mathbb{Z}[x]$. Write $g(x) = x^3 + bx^2 + cx + d$, $g_1(x) = x^3 + b_1x^2 + c_1x + d_1$. On comparing coefficients in the equation $f(x) = g(x)g_1(x)$, we see that

$$dd_1 = p^2, \tag{A.10}$$

$$cd_1 + c_1d = a, \tag{A.11}$$

$$bd_1 + b_1d + cc_1 = 0, \tag{A.12}$$

$$c + c_1 + bb_1 = 0, \tag{A.13}$$

$$b + b_1 = 0. \tag{A.14}$$

Since $f(x) \equiv x^6 \pmod{p}$, each of b, b_1, c, c_1, d, d_1 is divisible by p. So (A.10) implies that

$$d = d_1 = \pm p. \tag{A.15}$$

Hence (A.11) shows that $c + c_1 = \pm(a/p)$. It follows from (A.12), (A.14) and (A.15) that $cc_1 = 0$, say $c_1 = 0$. Using (A.13), (A.14), we have $\pm(a/p) = c = b^2$, which is impossible as $v_p(a/p)$ is odd. This contradiction proves that $f(x)$ is irreducible over $\mathbb{Q}$. □

Exercises

1. Let I denote the ideal generated by $x^2 + 1$ in the ring $\mathbb{R}[x]$ of polynomials in an indeterminate x with coefficients from the field $\mathbb{R}$ of real numbers. Prove that $\mathbb{R}[x]/I$ is isomorphic to $\mathbb{C}$.
2. Prove that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.
3. Show that $x^4 - 10x^2 + 1$ is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.
4. Prove that the polynomial[12] $\frac{x^3}{3!} + \frac{x^2}{2!} + x + 1$ is irreducible over $\mathbb{Q}$.
5. Prove or disprove that $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{-3})$ are isomorphic as fields.
6. Let F be a field of characteristic $p > 0$, $p \neq 3$. If α is a zero of the polynomial $f(x) = x^p - x + 3$ is an extension field of F, show that $f(x)$ has p distinct zeros in the field $F(\alpha)$.
7. For any root α of the polynomial[13] $x^4 - x - 1$, prove that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

[12] In 1930, Schur proved that the polynomial $f_n(x) = \frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \cdots + x + 1$ is irreducible over $\mathbb{Q}$ for each n and showed that the Galois group of $f_n(x)$ over $\mathbb{Q}$ is A_n, the alternating group of degree n, if 4 divides n and is S_n, the symmetric group of degree n, otherwise (cf. [Col]).

[13] In 1956, Selmer [Sel] proved that $x^n - x - 1$ is irreducible over $\mathbb{Q}$ for all n.

8. Let $F = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$. Prove that F is a field and each element in F has a unique representation as $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with $a, b, c \in \mathbb{Q}$. Also find the inverse of $1 - \sqrt[3]{2}$ in F.
9. Prove that any finite subgroup of the multiplicative group of a field is cyclic.
10. If the elements $\theta,\ \theta'$ of an extension K of F are roots of the same irreducible polynomial in $F[x]$ of degree n, show that $[F(\theta, \theta') : F] \leqslant n(n-1)$.
11. Let K/F be an extension, $\alpha, \beta \in K$ algebraic over F of degrees m and n respectively. Show that if $\gcd(m, n) = 1$, then $[F(\alpha, \beta) : F] = mn$.
12. Suppose that α and β are algebraic over F with minimal polynomials $f(x)$ and $g(x)$ respectively. Prove the reciprocity theorem: $f(x)$ is irreducible over $F(\beta)$ if and only if $g(x)$ is irreducible over $F(\alpha)$.
13. For θ a real number, let $F_\theta = \mathbb{Q}(\sin\theta)$ and $E_\theta = \mathbb{Q}(\sin\frac{\theta}{3})$. Show that E_θ is an extension field of F_θ and determine all possibilities of $[E_\theta : F_\theta]$.
14. Let $f(x) = x^5 - 8x^3 + 9x - 3$ and $g(x) = x^4 - 5x^2 - 6x + 3$. Prove that there is an integer d such that the polynomials $f(x)$ and $g(x)$ have a common root in the field $\mathbb{Q}(\sqrt{d})$. Write one such integer d?
15. Exhibit infinitely many pairwise non-isomorphic quadratic extensions of $\mathbb{Q}$.
16. Let F be a field of characteristic $p > 0$ and x, y be indeterminates. Show that $F(x, y)$ is not a simple extension of $F(x^p, y^p)$.
17. Let $\mathbb{A}$ denote the field of all algebraic numbers. Prove that $\mathbb{A}/\mathbb{Q}$ is an infinite extension.
18. Prove that a finite field cannot be algebraically closed.
19. Let F_{p^n} be the finite field with p^n elements. Prove that for each divisor m of n, F_{p^n} has a unique subfield of order p^m.
20. For every prime p and number $n \geqslant 1$, show that there exists a finite field with p^n elements.
21. Let E be the splitting field of $x^p - 2$ over $\mathbb{Q}$, where p is an odd prime. Find $[E : \mathbb{Q}]$.
22. Let F be a finite field with q elements. Let G be the group of invertible 2×2 matrices with entries from F. Prove that G has order $(q^2 - 1)(q^2 - q)$.
23. Let p be an odd prime and F_p the field of p elements. How many elements of F_p have square roots in F_p?
24. Let a be an element in a field F of characteristic $p > 0$. Assume a is not a pth power in F. Show that the polynomial $x^p - a$ is irreducible in $F[x]$.
25. If the minimal polynomial $g(x)$ of α over a field F is of the form $(x - \alpha)^m$, $m \geqslant 2$, then prove that there exists $e \geqslant 0$ such that $g(x) = x^{p^e} - \alpha^{p^e}$ where $p > 0$ is the characteristic of F.
26. Let K/F be a finite extension and Ω be an algebraically closed field containing K. Prove that any isomorphism σ of F into Ω can be extended to an isomorphism of K into Ω.
27. Find all conjugates of $\sqrt{2} + i$ and $\sqrt{1 + \sqrt{2}}$ over $\mathbb{Q}$.
28. Let $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $x^{10} - 2$. Prove that K has degree 10 over $\mathbb{Q}$, and that the group of automorphisms of K has order 2.

29. Let $f(x) = x^3 + bx + c$ be an irreducible polynomial over $\mathbb{Q}$. Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Show that $K = \mathbb{Q}(\sqrt{D}, \alpha)$ for any root α of $f(x)$, where $D = -4b^3 - 27c^2$. (See [Lu-Pa2, Chap. 2].)
30. If K_1, K_2 are finite Galois extensions of a field F, prove that so are K_1K_2 and $K_1 \cap K_2$.
31. Let H be a subgroup of the group G of automorphisms of a field K. Let σ be an element of G. If T is the fixed field of H, prove that the fixed field of $\sigma H \sigma^{-1}$ is $\sigma(T)$.
32. Prove that $\mathbb{Q}(\sqrt{2 + \sqrt{2}})$ is a cyclic extension of $\mathbb{Q}$ of degree 4.
33. Prove using the fundamental theorem of Galois theory that the field $\mathbb{C}$ of complex numbers is algebraically closed. (See [Lan, Chap. VI].)
34. Find the Galois group of each of the polynomials over the field $\mathbb{Q}$ of rational numbers.

    (a) $x^3 - 2$.
    (b) $x^4 + 1$.

35. Prove that the Galois group of the polynomial $x^4 - 4x^2 + 2$ over $\mathbb{Q}$ is cyclic.
36. Let n be a positive integer not divisible by the characteristic of a field F. Prove that the Galois groups of the polynomial $x^n - 1$ over F is isomorphic to a subgroup of $\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}$.
37. Let m, n be relatively prime positive integers. How are the Galois groups of the polynomials $x^{mn} - 1, x^m - 1, x^n - 1$ over $\mathbb{Q}$ related to each other?
38. Prove that $x^9 - 1$ and $x^7 - 1$ have isomorphic Galois groups over $\mathbb{Q}$.
39. Prove that the Galois groups of $x^{10} - 1$ and $x^8 - 1$ over $\mathbb{Q}$ are not isomorphic.
40. Let N be a finite abelian extension of a field K. Show that every subextension of N/K is an abelian extension.
41. Let E be the splitting field of $x^5 - 1$ over $\mathbb{Q}$. Show that there exists a unique field K with $\mathbb{Q} \subsetneq K \subsetneq E$.
42. Let $a \neq \pm 1$ be a squarefree integer, p an odd prime number. Determine the Galois group of the polynomial $x^p - a$ over $\mathbb{Q}$. Is it cyclic?
43. Let K and L be extensions of a field F having a common overfield. If K/F is a finite Galois extension and L/F is any extension, then show that $[KL : L]$ divides $[K : F]$. Give an example to show that the result need not be true if K/F is not a Galois extension.
44. If K is a cyclic extension of degree n of a field F, show that for every divisor d of n there exists a unique subextension of K of degree d over F.
45. Prove that the Galois group of the polynomial $x^n - 2$ over $\mathbb{Q}$ is not abelian when $n > 2$.
46. Let F be a field of characteristic $p > 0$ and a be an element of F such that the polynomial $g(x) = x^p - x - a$ is irreducible over F. Prove that the Galois group of $g(x)$ over F is cyclic of order p.
47. Prove that the Galois group of the polynomial $x^3 - 3x - 1$ over $\mathbb{Q}$ has order 3.
48. Prove that the Galois group of the polynomial $x^3 - 4x - 1$ over $\mathbb{Q}$ is S_3, the symmetric group of degree three.

49. Let $x^3 + bx + c$ be a separable polynomial irreducible over a field F of characteristic different from 2. Prove that the Galois group over F of the polynomial $x^3 + bx + c$ is cyclic of order 3 or is isomorphic to S_3 according as $D = -4b^3 - 27c^2$ is a square in F or not.
50. Let G be a finite abelian group. Prove that there exists a Galois extension K of $\mathbb{Q}$ contained in a cyclotomic extension of $\mathbb{Q}$ such that G is the Galois group[14] of $K/\mathbb{Q}$.
51. If R is the valuation ring of a discrete valuation, then prove that it is a principal ideal domain having only one non-zero prime ideal.

[14] The following problem was posed in early 19th century: Given a finite group G, whether there exists a Galois extension of $\mathbb{Q}$ whose Galois group is G? This is called the Inverse Problem of Galois Theory and is one of the most challenging problems in mathematics. Several classes of groups are known to occur as Galois groups of Galois extensions of $\mathbb{Q}$, for example the symmetric group S_n, the alternating group A_n for all $n \geq 1$, p-groups for odd primes p and finite solvable groups.

Hints and Answers to Selected Exercises

Chapter 1

2. If $f(X) \in \mathbb{Z}[X]$ is a monic polynomial of degree m and if $f(\alpha)$ satisfies an equation $f(\alpha)^n + c_1 f(\alpha)^{n-1} + \cdots + c_n = 0$ for some $c_1, \ldots, c_n$ belonging to $\mathbb{Z}$, then α satisfies a monic polynomial of degree mn over $\mathbb{Z}$.
4. Note that an algebraic number α is an algebraic integer if and only if α^2 is an algebraic integer. Since $\cos^2 \frac{\pi}{12} = \frac{1}{2}(1 + \cos \frac{\pi}{6}) = \frac{1}{4}(2 + \sqrt{3})$ is not an algebraic integer, it follows that $\cos \frac{\pi}{12}$ is not an algebraic integer.
5. Denote the polynomial $X^3 + X + 1$ by $f(X)$. If $f(X)$ is reducible over $\mathbb{Q}$, then $f(X)$ has a rational root, say α. Since each root of $f(X)$ is an algebraic integer, $\alpha \in \mathbb{Z}$. As $\alpha(\alpha^2 + 1) = -1$, we see that $\alpha = +1$ or -1. But by direct verification, neither 1 nor -1 is a root of $f(X)$. This contradiction proves that $f(X)$ is irreducible over $\mathbb{Q}$.
   Arguing similarly, it can be seen that the polynomials $X^3 - 4$ and $X^3 - 4X + 2$ are irreducible over $\mathbb{Q}$.
6. By Lemma A.39 and Theorem A.40, the minimal polynomial of ζ over $\mathbb{Q}$ is $X^4 + X^3 + X^2 + X + 1$.
7. The characteristic polynomial of $\sqrt{2} + \sqrt{3}$ with respect to $K/\mathbb{Q}$ is $f(X) = X^4 - 10X^2 + 1$. This is also the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ because $f(X)$ does not have a repeated root and characteristic polynomial is a power of minimal polynomial.
8. The characteristic polynomial of $\sqrt{-1} + \sqrt{2}$ with respect to $K/\mathbb{Q}$ is $X^4 - 2X^2 + 9$ and it is also the minimal polynomial of $\sqrt{-1} + \sqrt{2}$ over $\mathbb{Q}$.
9. (a) $N_{K/\mathbb{Q}}(\alpha) = 1$, $Tr_{K/\mathbb{Q}}(\alpha) = -1$.
   (b) $N_{K/\mathbb{Q}}(\alpha) = N_{K/\mathbb{Q}}(\zeta) N_{K/\mathbb{Q}}(1 + \zeta) = 1$,
   $Tr_{K/\mathbb{Q}}(\alpha) = Tr_{K/\mathbb{Q}}(\zeta) + Tr_{K/\mathbb{Q}}(\zeta^2) = -2$.
   (c) $N_{K/\mathbb{Q}}(\alpha) = 0$, $Tr_{K/\mathbb{Q}}(\alpha) = 0$.

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8

10. Denote $\zeta^{p^{r-1}}$ by η and the field $\mathbb{Q}(\eta)$ by K'. Then η is a primitive pth root of unity. So by Lemma A.39 and Theorem A.40, the minimal polynomial of η over $\mathbb{Q}$ is $1 + X + \cdots + X^{p-1}$. Deduce that $N_{K'/\mathbb{Q}}(1-\eta) = p$ and hence $N_{K/\mathbb{Q}}(1-\eta) = p^{p^{r-1}}$ by Theorem 1.23.
11. Use Lemma 1.14.
12. $Tr_{K/\mathbb{Q}}(\theta^2 + \theta) = 0$ and $N_{K/\mathbb{Q}}(\theta^2 - \theta) = 12$.
13. $Tr_{K/\mathbb{Q}}(\theta^2 + 2) = 4$ and $N_{K/\mathbb{Q}}(3\theta^2 + 1) = 31$.
14. Let $\{\theta_1, \theta_2\}$ and $\{w_1, w_2, w_3\}$ be bases of L/K and K/F respectively. Write down the matrix of the F-linear transformation T_γ from L to L defined by $T_\gamma(\xi) = \gamma\xi$ with respect to the basis $\{w_1\theta_1, w_2\theta_1, w_3\theta_1; w_1\theta_2, w_2\theta_2, w_3\theta_2\}$ of L/F and then compute the trace of the matrix.
15. It is enough to prove the desired equality when $L = K(\gamma)$. Let $\{w_1, w_2\}$ be a basis of K/F. Write down the matrix of the F-linear transformation $\xi \longmapsto \xi\gamma$ of $K(\gamma)$ with respect to the basis $\{w_1, w_2; \gamma w_1, \gamma w_2; \gamma^2 w_1, \gamma^2 w_2\}$ and compute its determinant.
16. Use Theorem 1.20 and the fact that the minimal polynomial of α over F is same as the minimal polynomial of $\sigma(\alpha)$ over F.
17. Let $A \otimes B$ denote the Kronecker product of two square matrices A and B as defined in the exercise. If A, C are $m \times m$ and B, D are $n \times n$ matrices with entries from $\mathbb{C}$, then using matrix multiplication one can easily verify that

$$(A \otimes B)(C \otimes D) = (AC) \otimes (BD).$$

By an elementary result of linear algebra, there exists an invertible matrix P with entries in $\mathbb{C}$ such that $P^{-1}AP$ is an upper triangular matrix, say

$$P^{-1}AP = \begin{bmatrix} u_{11} & u_{12} & \cdots & u_{1m} \\ 0 & u_{22} & \cdots & u_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & u_{mm} \end{bmatrix}.$$

Using the above formula, we see that

$$(P \otimes I)^{-1}(A \otimes B)(P \otimes I) = (P^{-1}AP) \otimes B,$$

which can be written as

$$\begin{bmatrix} u_{11}B & u_{12}B & \cdots & u_{1m}B \\ \mathbf{0} & u_{22}B & \cdots & u_{2m}B \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \cdots & u_{mm}B \end{bmatrix}.$$

Hence

$$\det(A \otimes B) = \det\left((P^{-1}AP) \otimes B\right) = \prod_{i=1}^{m} \det(u_{ii}B)$$
$$= \prod_{i=1}^{m} (u_{ii}^n \det B) = (\det A)^n (\det B)^m.$$

Chapter 2

1. In view of Lemma 2.6,

$$D_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(n\alpha^{n-1} + a).$$

   Show that the determinant of the $\mathbb{Q}$-linear transformation $\xi \mapsto \xi(n\alpha^{n-1} + a)$ of K is $n^n b^{n-1} + a^n(1-n)^{n-1}$, which equals $N_{K/\mathbb{Q}}(n\alpha^{n-1} + a)$ by definition.
2. Show that the determinant of the transition matrix from $\{1, \theta, \ldots, \theta^{n-1}\}$ to $\{1, (\theta + m), \ldots, (\theta + m)^{n-1}\}$ is 1.
3. Show that $D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -1579$ and note that 1579 is a prime number.
4. $d_K = -31$ and $\{1, \theta, \theta^2\}$ is an integral basis of K.
6. $d_{K_i} = 22356 = 23 \cdot 2^2 \cdot 3^5$ and $\{1, \theta, \theta^2\}$ is an integral basis of K_i for each i.
7. $d_K = -2480$ and $\{1, \theta, \theta^2, \theta^3\}$ is an integral basis of K.
8. $d_K = -2^{11}$ and $\{1, \theta, \theta^2, \theta^3\}$ is an integral basis of K.
9. Show that $D_{K/\mathbb{Q}}(1, \theta, \theta^2) = -104 = -2^2 \cdot 26$ and use Stickelberger's theorem.
10. Show that $\theta^2/6 \in \mathcal{O}_K$ and $D_{K/\mathbb{Q}}(1, \theta, \theta^2/6) = -2^2 \cdot 3 \cdot 79$. Use Lemma 2.8 and Stickelberger's theorem to justify that $d_K = -2^2 \cdot 3 \cdot 79$.
11. Consider the integral basis $\{1, \theta, \theta^2/5\}$ of K, then proceed as in Example 2.17 and use the fact that the congruence $5X^3 \equiv \pm 1 \pmod 7$ is not solvable in $\mathbb{Z}$ to deduce that K is not monogenic.
12. Show that the polynomial $f(X + 2)$ is an Eisenstein polynomial with respect to the prime 7 and $D_{K/\mathbb{Q}}(1, \theta, \theta^2) = 49$.
13. Use Exercise 16 of Chap. 1.
14. Recall that if $\{w_1, w_2, \ldots, w_n\}$ is an integral basis of K, then by definition d_K is the square of the determinant of the matrix $(w_i^{(j)})_{i,j}$.
15. In view of Theorem 2.25, $d_K = (-1)^{\frac{p-1}{2}} p^{p-2}$ which is a square in K by virtue of the previous exercise.
17. Let $p_1, p_2, \ldots, p_s$ be all the odd primes dividing D which are arranged such that $p_1, p_2, \ldots, p_r$ are congruent to 1 modulo 4 and $p_{r+1}, \ldots, p_s$ are congruent to 3 modulo 4. Set $d_i = p_i$ for $1 \le i \le r$ and $d_i = -p_i$ for $r + 1 \le i \le s$, then d_i is the discriminant of $\mathbb{Q}(\sqrt{d_i})$ for each i. Three cases are distinguished.
    Consider first the case when $D \equiv 1 \pmod 4$. Keeping in mind that $|D| = p_1 p_2 \cdots p_s = |d_1 d_2 \cdots d_s|$ and each $d_i \equiv 1 \pmod 4$, we see that $D = d_1 d_2 \cdots d_s$.
    Consider now the case when $D \equiv 4 \pmod 8$. Since D is the discriminant of the quadratic field $\mathbb{Q}(\sqrt{D})$, this case arises when $\frac{D}{-4} \equiv 1 \pmod 4$. So arguing as above, we can write $D = (-4)d_1 d_2 \cdots d_s$.

In the last case when $D \equiv 0 \pmod 8$, we can write $D = 8d_1d_2\cdots d_s$ or $(-8)d_1d_2\cdots d_s$ according as $\frac{D}{8} \equiv 1$ or $-1 \pmod 4$.

18. Use the previous three Exercises 15–17.
19. $d_K = 24^2$ and $\{1, \sqrt{2}, \sqrt{-3}, \sqrt{-6}\}$ is an integral basis of K.
21. $d_K = \left(\prod_{i=1}^{s} u_i\right)^{2^{s-1}}$.

Chapter 3

2. $I^{-1} = \{a + \frac{b}{2}\sqrt{6} \mid a, b \in \mathbb{Z}\}$
3. $I^{-1} = \{(a + b\sqrt{-5})/2 \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2\}$.
9. $7 = (3+\omega)(3+\omega^2)$, $13 = (4+\omega)(4+\omega^2)$, $19 = (5+3\omega)(5+3\omega^2)$ is factorization into irreducible elements in $\mathbb{Z}[\omega]$.
12. The norm of the ideal $\langle 2, w\rangle$ is 2 and of $\langle 13, 4+w\rangle$ is 13. Neither of them is a principal ideal, because no element of $\mathcal{O}_K$ has norm 2 or 13 with respect to $K/\mathbb{Q}$.
15. If $I \subsetneqq J$ are ideals of $\mathcal{O}_K$, then index of the subgroup I of $\mathcal{O}_K$ is strictly bigger than the index of J in $\mathcal{O}_K$.
18. We first show that $2, 1+\sqrt{-5}$ have gcd 1. Denote $\mathbb{Q}(\sqrt{-5})$ by K. Since $N_{K/\mathbb{Q}}(2) = 4$, $N_{K/\mathbb{Q}}(1+\sqrt{-5}) = 6$ and no element of $\mathcal{O}_K$ has norm 2 or 3, it follows that $2, 1+\sqrt{-5}$ are non-associate irreducible elements in $\mathcal{O}_K$. Hence $2, 1+\sqrt{-5}$ have gcd 1.
Next it will be shown that the elements $6, 3(1+\sqrt{-5})$ do not have a gcd. Suppose to the contrary these elements have a gcd in $\mathcal{O}_K$, say d. So gcd of $2, (1+\sqrt{-5})$ is $d/3$. But as shown above $2, 1+\sqrt{-5}$ have gcd 1. Therefore $d/3$ is a unit of $\mathcal{O}_K$, i.e., $d = \pm 3$. Since $1+\sqrt{-5}$ divides 6 as well as $3(1+\sqrt{-5})$, it follows that $(1+\sqrt{-5})$ divides their gcd 3. This is false, because $\dfrac{3}{1+\sqrt{-5}} = \dfrac{1-\sqrt{-5}}{2}$ does not belong to $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$. Hence $6, 3(1+\sqrt{-5})$ do not have a gcd.
Finally it remains to be shown that $2, 1+\sqrt{-5}$ have no lcm. Suppose these elements have lcm, say $\lambda = a + b\sqrt{-5}$. Then $N_{K/\mathbb{Q}}(\lambda)$ is divisible by $N_{K/\mathbb{Q}}(2)$ and $N_{K/\mathbb{Q}}(1+\sqrt{-5})$. So $N_{K/\mathbb{Q}}(\lambda)$ is divisible by 12. Since λ divides $2(1+\sqrt{-5})$, we see that $N_{K/\mathbb{Q}}(\lambda)$ divides $N_{K/\mathbb{Q}}(2(1+\sqrt{-5})) = 24$. Consequently $a^2 + 5b^2 = N_{K/\mathbb{Q}}(\lambda) = 12$ or 24. This is clearly impossible as $a, b \in \mathbb{Z}$. This contradiction proves that $2, 1+\sqrt{-5}$ have no lcm.
19. Show that if β, γ are elements of a unique factorization domain R with β/γ integral over R, then each prime element of R dividing γ divides β.
20. $\mathbb{Z}[2\cos\frac{2\pi}{9}]$ is a Dedekind domain because in view of Corollary 2.32, it is the ring of algebraic integers of $\mathbb{Q}(\zeta + \zeta^{-1})$ where ζ is a primitive 9th root of unity.
22. Recall that every non-zero ideal in a Dedekind domain R can be uniquely written as a product of prime ideals of R. So there are only finitely many ideals of R dividing the given non-zero ideal I of R. Since an ideal J of R contains I if and only if J divides I, it follows that there are only finitely many ideals of R containing the non-zero ideal I of R. This yields the desired assertion.

24. Let J/I be an ideal of R/I where J is an ideal of R containing I. Fix a non-zero element $\alpha \in I$. By Corollary 3.23, there is $\beta \in J$ such that $J = \langle \alpha, \beta \rangle$. Hence J/I is the ideal generated by $\beta + I$.

26. Write $I = \prod_{i=1}^{r} \mathfrak{p}_i^{a_i}$ where $\mathfrak{p}_i$'s are distinct prime ideals and a_i's are positive integers. For every i, choose x_i such that $x_i \in \mathfrak{p}_i^{a_i}$, but $x_i \notin \mathfrak{p}_i^{a_i+1}$. By Chinese remainder theorem, there exists $\alpha \in \mathcal{O}_K$ such that

$$\alpha \equiv x_i \pmod{\mathfrak{p}_i^{a_i+1}} \quad \text{for} \quad 1 \leq i \leq r,$$

and

$$\alpha \equiv 1 \pmod{\mathfrak{q}}$$

for every prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$ which divides $N(I)\mathcal{O}_K$ and is different from $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$. Note that the exact power of $\mathfrak{p}_i$ dividing $\alpha\mathcal{O}_K$ is a_i and $\alpha\mathcal{O}_K = IA$ where A is an ideal of $\mathcal{O}_K$ which is not divisible by any prime ideal of $\mathcal{O}_K$ dividing $N(I)\mathcal{O}_K$. So $N(I)$, $N(A)$ are coprime numbers. By classical Chinese Remainder Theorem, choose $b \in \mathbb{Z}$ such that $b \equiv 0 \pmod{N(I)}$ and $b \equiv 1 \pmod{N(A)}$. Then $b\mathcal{O}_K$ is divisible by $N(I)$ and hence by I. So we can write $b\mathcal{O}_K = IB$ for some ideal B of $\mathcal{O}_K$. Therefore $N(B)$ divides $N(b\mathcal{O}_K) = |b|^n$ where $n = [K : \mathbb{Q}]$. Since b is coprime with $N(A)$, it follows that $N(A)$, $N(B)$ are coprime. Consequently

$$\gcd(N_{K/\mathbb{Q}}(\alpha), N_{K/\mathbb{Q}}(b)) = \gcd(N(I)N(A), N(I)N(B)) = N(I).$$

Chapter 4

In what follows, $\mathfrak{p}_i, \mathfrak{p}_i'$ stand for distinct non-zero prime ideals of the ring of algebraic integers of the given algebraic number field for $i = 2, 3, 5$.

1. By Exercise 3 of Chap. 2, the index of θ is 1. So Theorem 4.8 is applicable. Using this theorem, we see that $3\mathcal{O}_K$ is a product of two distinct prime ideals $\mathfrak{p}_3, \mathfrak{p}_3'$ with $N(\mathfrak{p}_3) = 3$, $N(\mathfrak{p}_3') = 3^2$. Also $5\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.
2. By Exercise 9 of Chap. 2, index of θ is 1 and $d_K = -104 = -8 \cdot 13$. So by Theorem 4.16, only the primes 2, 13 can be ramified in K. Using Theorem 4.8, we see that $2\mathcal{O}_K = \mathfrak{p}_2^2\mathfrak{p}_2'$ with $N(\mathfrak{p}_2) = N(\mathfrak{p}_2') = 2$ and $13\mathcal{O}_K = \mathfrak{p}^2\mathfrak{p}'$ with $N(\mathfrak{p}) = N(\mathfrak{p}') = 13$, where $\mathfrak{p}_2 \neq \mathfrak{p}_2'$, $\mathfrak{p} \neq \mathfrak{p}'$ are prime ideals of $\mathcal{O}_K$.
3. (a) $K = \mathbb{Q}(\theta)$ where $\theta^3 = 18$. In view of Theorem 2.22, $d_K = -2^2 \cdot 3^5$. So by Theorem 4.16, only the primes 2, 3 can be ramified in K. Since the minimal polynomial of θ over $\mathbb{Q}$ is an Eisenstein polynomial with respect to the prime 2, it follows from Theorem 4.5 that $2\mathcal{O}_K = \mathfrak{p}_2^3$ with $N(\mathfrak{p}_2) = 2$. Note that $\theta^2/3$ satisfies the polynomial $X^3 - 12$ which is an Eisenstein polynomial with respect to the prime 3. Since $K = \mathbb{Q}(\theta^2/3)$, we have $3\mathcal{O}_K = \mathfrak{p}_3^3$.
   (b) $K = \mathbb{Q}(\theta)$ where $\theta^3 = 20$. Arguing as above it can be seen that only the primes 2, 3, 5 can be ramified in K; in fact $2\mathcal{O}_K = \mathfrak{p}_2^3$ and $5\mathcal{O}_K = \mathfrak{p}_5^3$. By Theorem 2.22, $\{1, \theta, \theta^2/2\}$ is an integral basis of K. Therefore 3 does not

divide $\operatorname{ind}\theta$. So Theorem 4.8 is applicable and by this theorem we have $3\mathcal{O}_K = \mathfrak{p}_3^3$.

(c) $K = \mathbb{Q}(e^{2\pi\iota/27})$. By Theorem 4.15, $3\mathcal{O}_K = \mathfrak{p}^{18}$ where $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ with $N(\mathfrak{p}) = 3$.

4. By Theorem 4.11, $2\mathcal{O}_K$ can be written as a product $\mathfrak{p}_2\mathfrak{p}_2'$ of distinct prime ideals of $\mathcal{O}_K$ with $N(\mathfrak{p}_2) = N(\mathfrak{p}_2') = 2$. So $2\mathcal{O}_K$ is not a prime ideal and hence 2 is not a prime element of $\mathcal{O}_K$. Since $N_{K/\mathbb{Q}}(2 - w) = 8$, it follows that the ideal generated by $2 - w$ is not a prime ideal. It can be seen that no element of $\mathcal{O}_K$ has norm 2 or 4. So 2 and $2 - w$ are irreducible elements of $\mathcal{O}_K$.
6. In view of Theorem 4.8, $5\mathcal{O}_{K_1}$ is a prime ideal of $\mathcal{O}_{K_1}$, $5\mathcal{O}_{K_2}$ is a prime ideal of $\mathcal{O}_{K_2}$ and $5\mathcal{O}_{K_3}$ is a product of three distinct prime ideals of $\mathcal{O}_{K_3}$ each of norm 5. This shows that $K_1 \neq K_3$ and $K_2 \neq K_3$. Further $11\mathcal{O}_{K_1}$ is a product of three distinct prime ideals of $\mathcal{O}_{K_1}$ each of norm 11 and $11\mathcal{O}_{K_i}$ is a prime ideal of $\mathcal{O}_{K_i}$ for $i = 2, 3$. This shows that $K_1 \neq K_2$.
7. $2\mathcal{O}_K = (\mathfrak{p}_2\mathfrak{p}_2')^2$ with $N(\mathfrak{p}_2) = N(\mathfrak{p}_2') = 2^3$,
$3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$ with $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3^6$,
$5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5'$ with $N(\mathfrak{p}_5) = N(\mathfrak{p}_5') = 5^6$.
8. Arguing exactly as for the proof of equation (4.13), it can be shown that

$$p\mathcal{O}_K = (1 - \zeta_0)^{\phi(p^r)}\mathcal{O}_K.$$

Taking absolute norm on both sides of the above equation, we see that the absolute norm of the ideal $(1 - \zeta_0)\mathcal{O}_K$ is p and hence it is a prime ideal of $\mathcal{O}_K$.

11. 11, 19, 29, 31 and 41 are the only primes less than 50 which split completely in K.
12. 5, 7 and 13 are the only primes less than 20 each of which generates a prime ideal in $\mathcal{O}_K$.
13. Denote $\mathbb{Q}(\sqrt{-2})$ by K. The primes 2 and 3 split in $\mathcal{O}_K$ as $2\mathcal{O}_K = \mathfrak{p}_2^2$ with $N(\mathfrak{p}_2) = 2$ and $3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$ with $N(\mathfrak{p}_3) = N(\mathfrak{p}_3') = 3$. So $\mathfrak{p}_2\mathfrak{p}_3^2$, $\mathfrak{p}_2(\mathfrak{p}_3')^2$, $\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_3'$ are the only three ideals of $\mathcal{O}_K$ with norm 18.
14. Denote $\mathbb{Q}(\sqrt{-5})$ by K. Note that $15\mathcal{O}_K$ factors as a product $\mathfrak{p}_5^2\mathfrak{p}_3\mathfrak{p}_3'$ of powers of distinct prime ideals of $\mathcal{O}_K$. So the number of ideals of $\mathcal{O}_K$ dividing $15\mathcal{O}_K$ is 12. Hence the number of ideals containing 15 is 12.
15. The desired number of ideals is 14.
16. $7\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$ and $29\mathcal{O}_K$ is a product $\mathfrak{p}\mathfrak{p}'$ of prime ideals of $\mathcal{O}_K$ with $N(\mathfrak{p}) = 29$, $N(\mathfrak{p}') = 29^2$.
17. In view of Example 2.38, $\operatorname{ind}\theta$ is not divisible by 2. So Theorem 4.8 is applicable. On applying this theorem, it can be seen that $2\mathcal{O}_K$ is a prime ideal of $\mathcal{O}_K$.
18. $f(X)$ is irreducible over $\mathbb{Q}$ in view of Eisenstein-Dumas Irreducibility Criterion proved in Sect. A.7. Using Exercise 1 of Chap. 2, we see that $D_{K/\mathbb{Q}}(1, \theta, \theta^2, \theta^3)$ is not divisible by 3. In particular $\operatorname{ind}\theta$ is not divisible by 3. So applying Theorem 4.8, $3\mathcal{O}_K = \mathfrak{p}_3\mathfrak{p}_3'$ with $N(\mathfrak{p}_3) = 3$, $N(\mathfrak{p}_3') = 3^3$.
19. Applying Lemma 2.6 and Corollary 2.16, we see that

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{p-1}) = (-1)^{p(p-1)/2}p^p a^{p-1} = (\operatorname{ind}\theta)^2 d_K.$$

Since $X^p - a$ is an Eisenstein polynomial with respect to every prime dividing the squarefree integer a, it follows that ind θ is coprime to a in view of Theorem 2.18. Therefore the only prime which can divide ind θ is p.
Suppose first that $a^p \not\equiv a \pmod{p^2}$, then the minimal polynomial $(X+a)^p - a$ of $\theta - a$ over $\mathbb{Q}$ is an Eisenstein polynomial with respect to p. Therefore p does not divide $\text{ind}(\theta - a) = \text{ind}\,\theta$ and hence $\mathcal{O}_K = \mathbb{Z}[\theta]$.
Conversely suppose that $\mathcal{O}_K = \mathbb{Z}[\theta]$. Since $X^p - a \equiv (X-a)^p \pmod{p}$, on applying Theorem 4.8, we see that

$$p\mathcal{O}_K = \mathfrak{p}^p$$

where $\mathfrak{p} = \langle p, \theta - a\rangle$. Note that $\theta - a \in \mathfrak{p}$ but $\theta - a \notin \mathfrak{p}^2$. So we can write $\langle \theta - a\rangle = \mathfrak{p}I$ where I is an ideal of $\mathcal{O}_K$ not divisible by $\mathfrak{p}$. On taking norm we see that

$$pN(I) = N(\langle \theta - a\rangle) = |N_{K/\mathbb{Q}}(\theta - a)| = |a^p - a|.$$

Hence $a^p \not\equiv a \pmod{p^2}$.

Chapter 5

3. The number of roots of unity in $\mathbb{Q}(\zeta)$ is m or $2m$ according as m is even or odd.
4. (a) $(3+\sqrt{13})/2$.
   (b) $37 + 6\sqrt{38}$.
   (c) $24 + 5\sqrt{23}$.
   (d) $35 + 6\sqrt{34}$.
7. Note that the fundamental unit $3 + \sqrt{10}$ of $\mathbb{Q}(\sqrt{10})$ has norm -1. So by Lemma 5.10, all positive solutions (x_n, y_n) of $x^2 - 10y^2 = -1$ are given by

$$x_n + y_n\sqrt{10} = (3+\sqrt{10})^{2n-1},$$

where n runs over natural numbers.
8. Let x, y be positive integers satisfying $x^2 - 10y^2 = 10$. Then 10 divides x^2 and hence 10 divide x. Write $x = 10z$. Thus $y^2 - 10z^2 = -1$. By the previous exercise, $y + z\sqrt{10} = (3+\sqrt{10})^{2n-1}$ for some $n \in \mathbb{N}$. Hence all positive solutions (x_n, y_n) of $x^2 - 10y^2 = 10$ are given by

$$x_n + y_n\sqrt{10} = \sqrt{10}(3+\sqrt{10})^{2n-1},$$

where n runs over natural numbers.
9. Write $g(X) = X^m + a_1X^{m-1} + \cdots + a_m$ with $a_i \in \mathbb{Z}$. Clearly $\alpha - r$ divides $g(\alpha) - g(r) = (\alpha^m - r^m) + a_1(\alpha^{m-1} - r^{m-1}) + \cdots + a_{m-1}(\alpha - r)$ over $\mathcal{O}_K$. By hypothesis $g(\alpha) - g(r) = \pm 1$. It follows that $\alpha - r$ is a unit in $\mathcal{O}_K$.
10. In view of the previous exercise, $\theta + 1$ is a unit in $\mathcal{O}_K$.
11. Let $x + y(1+\sqrt{d})/2$ be a fundamental unit of $\mathbb{Q}(\sqrt{d})$. On taking norm, we have $(2x+y)^2 - dy^2 = \pm 4$. Suppose to the contrary y is odd. Since $d \equiv 1 \pmod 8$, the above equality implies that $(2x+y)^2 \equiv 5 \pmod 8$ which is false.

12. If $d \equiv 1 \pmod 4$ and $\epsilon = x + y(1+\sqrt{d})/2$ is a fundamental unit of K with y odd, then show that $\epsilon^3 \in \mathbb{Z}[\sqrt{d}]$.
14. (i) $-1 + \sqrt[3]{2}$.
    (ii) $-2 + 3^{2/3}$.
    (iii) $2 - \sqrt[3]{7}$.
15. It is enough to prove that there exists $\gamma \in \mathcal{O}_K$ such that $|\gamma| < 1$. Let $\{w_1, \ldots, w_n\}$ be an integral basis of K. Apply modified Minkowski's lemma of complex linear forms to the forms $L_1, \ldots, L_n$ given by $L_i(x_1, \ldots, x_n) = \sum_{j=1}^{n} w_j^{(i)} x_j$ with suitable constants $b_1, \ldots, b_n$, as in the proof of Lemma 5.6 (taking $b_1 < 1$ and the isomorphism $\alpha \longmapsto \alpha^{(1)}$ to be the identity isomorphism) and obtain an element $\gamma \in \mathcal{O}_K$ with $|\gamma| < 1$.

Chapter 6

1. (i) There are two prime ideals $\mathfrak{P}, \mathfrak{P}'$ of $\mathcal{O}_{K'}$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and
$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p}) = f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p}) = 1.$$
   (ii) There is only one prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K'}$ lying over the prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ and
$$e(\mathfrak{P}/\mathfrak{p}) = 1, \quad f(\mathfrak{P}/\mathfrak{p}) = 2.$$
2. $N(I_1') = 2\mathcal{O}_K$, $N(I_2') = 3\mathcal{O}_K$.
3. There is only one prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ lying over 3 and there are two prime ideals $\mathfrak{P}, \mathfrak{P}'$ of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}$.
$$e(\mathfrak{P}/\mathfrak{p}) = e(\mathfrak{P}'/\mathfrak{p}) = 2, \quad f(\mathfrak{P}/\mathfrak{p}) = f(\mathfrak{P}'/\mathfrak{p}) = 1.$$
4. There is only one prime ideal $\mathfrak{P}$ of $\mathcal{O}_{K'}$ lying over $\mathfrak{p}_2$ and $f(\mathfrak{P}/\mathfrak{p}_2) = 11$.

Chapter 7

1. (i) $< \sqrt{13} >$.
   (ii) $< 3 \cdot 2^{2/3} >$.
   (iii) $< 4\theta^3 + 3\theta^2 + 2\theta + 1 >$ where $\theta = e^{2\pi\iota/5}$.
2. In view of Corollary 7.10 and the Discriminant theorem, $d_{K'}$ equals $d_K{}^{[K':K]}$ in absolute value, if and only if K'/K is an unramified extension.
4. Consider the matrix product $\left(\sigma_j(\beta_i)\right)_{i,j}\left(\sigma_i(\beta_j^*)\right)_{i,j}$.
5. See proof of Theorem 7.8.
6. $\Delta_{K'/K} =< F'(\theta) >$, $d_{K'/K} =< N_{K'/K}(F'(\theta)) >$.
8. Using equation (2.20), deduce that
$$\Delta_{K/\mathbb{Q}} = \left\langle p^r/(\zeta^{p^{r-1}} - 1) \right\rangle.$$

10. Write $m = \prod_{i=1}^{k} p_i^{r_i}$, where p_i's are distinct primes and r_i's are positive integers. Let η_i be a primitive $(p_i^{r_i})$th root of unity in $\mathbb{C}$. Then $\mathbb{Q}(\eta_i)$ is contained in K for $1 \leq i \leq k$. So in view of Corollary 7.11, d_K is divisible by the discriminant of $\mathbb{Q}(\eta_i)$, $1 \leq i \leq k$. But by Theorem 2.26, the discriminant of $\mathbb{Q}(\eta_i)$ is $\pm p_i^{s_i}$, where $s_i = r_i\phi(p_i^{r_i}) - p_i^{r_i-1}$. Note that $s_i \geq r_i$ when $p_i \neq 2$ and $s_i \geq r_i - 1$ when $p_i = 2$. Since $\prod_{i=1}^{k} p_i^{s_i}$ divides d_K, it now follows that m divides $2d_K$.
11. Let σ be a K-isomorphism from K' into $\mathbb{C}$. Keeping in mind that for any $\alpha \in K'$, $Tr_{K'/K}(\alpha) = Tr_{\sigma(K')/K}(\sigma(\alpha))$, it can be easily seen that $\sigma(\Delta_{K'/K}) = \Delta_{\sigma(K')/K}$. Therefore using the definition of relative norm as given in Theorem 6.9, it follows that $d_{K'/K} = d_{\sigma(K')/K}$.
12. In view of Corollary 7.11, every prime ideal of $\mathcal{O}_K$ dividing the product $d_{K_1/K}d_{K_2/K}$ also divides $d_{L/K}$. Assume now that $\mathfrak{p}$ is a prime ideal of $\mathcal{O}_K$ dividing $d_{L/K}$, but not dividing $d_{K_1/K}$. It needs to be shown that $\mathfrak{p}$ divides $d_{K_2/K}$. Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_L$ lying above $\mathfrak{p}$, and dividing $\Delta_{L/K}$. Our claim is that $\mathfrak{P}$ divides Δ_{L/K_1}. In view of the equality

$$\Delta_{L/K} = \Delta_{L/K_1}\Delta_{K_1/K}$$

(obtained in Proposition 7.9), the claim is proved once we show that $\mathfrak{P}$ does not divide $\Delta_{K_1/K}\mathcal{O}_L$. Suppose to the contrary $\mathfrak{P} \mid \Delta_{K_1/K}\mathcal{O}_L$, then with $f = f_{L/K}(\mathfrak{P})$, the supposition implies that $\mathfrak{p}^f = N_{L/K}(\mathfrak{P})$ divides

$$N_{L/K}(\Delta_{K_1/K}\mathcal{O}_L) = N_{K_1/K}(N_{L/K_1}(\Delta_{K_1/K}\mathcal{O}_L)) = N_{K_1/K}(\Delta_{K_1/K}^{[L:K_1]}) = d_{K_1/K}^{[L:K_1]},$$

which shows that $\mathfrak{p}$ divides $d_{K_1/K}$. This is contrary to the assumption and hence the claim is proved.
Let $\theta \in K_2$ be an algebraic integer with $K_2 = K(\theta)$, and denote by F, G its minimal polynomials over K and K_1 respectively. Then $L = K_1(\theta)$ and $F(X) = G(X)H(X)$ for some polynomial $H(X)$ having coefficients in $\mathcal{O}_{K_1}$. Thus $F'(\theta) = G'(\theta)H(\theta)$, and so $F'(\theta)$ lies in the ideal $G'(\theta)\mathcal{O}_L$. By Theorem 7.12, $G'(\theta) \in \Delta_{L/K_1}$ which is contained in $\mathfrak{P}$ by virtue of the claim proved above. Therefore $F'(\theta) \in \mathfrak{P}$. Since θ is an arbitrary algebraic integer generating the extension K_2/K, it now follows from Theorem 7.12 that $\Delta_{K_2/K} \subset \mathfrak{P}$. This proves that $\mathfrak{P}$ divides $\Delta_{K_2/K}\mathcal{O}_L$ and hence on taking norm, we see that $\mathfrak{p}$ divides $d_{K_2/K}$.
13. If a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in L/K, then clearly it is unramified in K_1/K and in K_2/K. The converse follows immediately from the Discriminant theorem and Exercise 12 above.
14. If a prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ is unramified in K', then by the Discriminant theorem $\mathfrak{p}$ does not divide $d_{K'/K}$. Therefore using Exercise 11, $\mathfrak{p}$ does not divide $d_{\sigma(K')/K}$ for any K-isomorphism σ of K' into $\mathbb{C}$. Hence in view of Exercise 12, $\mathfrak{p}$ does

not divide $d_{N/K}$ where N is the smallest normal extension of K containing K'. Thus $\mathfrak{p}$ is unramified in N.

Chapter 8

1. Proceed as in Example 8.20.
4. In view of Exercise 4 of Chap. 2, $d_K = -31$. Applying Theorem 8.14, we see that the class number of K is 1.
5. Let $K = \mathbb{Q}(\sqrt{34})$. Then $5\mathcal{O}_K = \mathfrak{p}_5\mathfrak{p}_5'$ with $N(\mathfrak{p}_5) = N(\mathfrak{p}_5') = 5$. We show that $\mathfrak{p}_5$ is not a principal ideal. Suppose to the contrary $\mathfrak{p}_5$ is principal, say generated by $a + b\sqrt{34}$ with $a, b \in \mathbb{Z}$. So $|N_{K/\mathbb{Q}}(a + b\sqrt{34})| = |a^2 - 34b^2| = 5$. Therefore $a^2 \equiv \pm 5 \pmod{17}$ which is not possible as the Legendre symbol $\left(\frac{\pm 5}{17}\right) = -1$.
6. In view of Example 2.20, $d_K = -44$. Hence the signature of K is $[1, 1]$. By Theorem 8.14, in every ideal class of K, there exists an ideal B with $N(B) \leq \left(\frac{4}{\pi}\right) \frac{3!}{3^3}\sqrt{44} < 2$. So $N(B) = 1$ and hence the class number of K is 1.
7. Proceed as in Example 8.22.
13. Let $\mathcal{C}, \mathcal{C}'$ be two distinct ideal classes of an algebraic number field K. Choose integral ideals I, J such that $I \in \mathcal{C}^{-1}$ and $J \in \mathcal{C}'$. By Corollary 3.22, there exists an integral ideal A of $\mathcal{O}_K$ such that $\gcd(A, IJ) = \mathcal{O}_K$ and AI is a principal ideal. Therefore $A \in \mathcal{C}$ and it is coprime with $J \in \mathcal{C}'$.
14. Let N denote the smallest normal extension of $\mathbb{Q}$ containing K_1. In view of Exercises 11, 12 of Chap. 7, the only primes dividing d_N are the primes dividing d_{K_1}. So d_N and d_{K_2} are coprime. Write $K_1 = \mathbb{Q}(\theta)$ and let $F(X), G(X)$ be the minimal polynomials of θ over $\mathbb{Q}$ and K_2 respectively. Clearly $G(X)$ divides $F(X)$ and we show that $F(X) = G(X)$. For this, it is enough to prove that $G(X) \in \mathbb{Q}[X]$. Note that $G(X) \in N[X]$ because each root of $F(X)$ and hence that of $G(X)$ belongs to N. So if $N \cap K_2$ is denoted by K, then $G(X) \in K[X]$. By Corollary 7.11, d_K divides both d_N and d_{K_2}. Since d_N and d_{K_2} are coprime, it follows that $d_K = \pm 1$. But in view of Corollary 8.3, this is possible only when $K = \mathbb{Q}$. Therefore $G(X) \in \mathbb{Q}[X]$ and hence $F = G$; consequently $[K_1K_2 : K_2] = \deg G = \deg F = [K_1 : \mathbb{Q}]$.
15. Denote $\mathbb{Q}(\sqrt{-p})$ by K. Then $2\mathcal{O}_K = \mathfrak{p}_2^2$ with $N(\mathfrak{p}_2) = 2$. Note that $\mathfrak{p}_2$ is not a principal ideal because if $\mathfrak{p}_2$ is generated by $a + b\sqrt{-p}$ with $a, b \in \mathbb{Z}$, then $2 = N(\mathfrak{p}_2) = a^2 + pb^2$, which is not possible for any integers a, b. So the ideal class of $\mathfrak{p}_2$ has order 2 in the class group of K and hence the class number of K is even.
16. Use Lemma 8.31 together with the fact that all the $(p-1)/2$ $\mathbb{Q}$-isomorphisms of K_0 into $\mathbb{C}$ are real.
18. Let $\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_h$ be all the distinct ideal classes of K. Fix an integral ideal $A_i \in \mathcal{C}_i$ for each i. By Corollary 8.5, A_i^h is a principal ideal of $\mathcal{O}_K$, say $A_i^h = \langle \alpha_i \rangle$. Let θ_i be a complex number which is a root of the polynomial $X^h - \alpha_i$ and denote the field $K(\theta_i)$ by K_i. Set $L = K(\theta_1, \theta_2, \ldots, \theta_h)$. In view of the previous exercise, $A_i\mathcal{O}_{K_i}$ is a principal ideal of $\mathcal{O}_{K_i}$ and hence $A_i\mathcal{O}_L$ is a principal ideal of $\mathcal{O}_L$. Since any non-zero ideal of $\mathcal{O}_K$ is a product of a principal fractional ideal of $\mathcal{O}_K$ with A_i for some i, it follows that $I\mathcal{O}_L$ is a principal ideal of $\mathcal{O}_L$ for each ideal I of $\mathcal{O}_K$.

Chapter 9

2. Following the steps of the proof of Theorem 9.2, show that the set S^{**} in Step III of this proof can be identified with the subset of $\mathbb{R}^2$ given by

$$\{(x, y) \in \mathbb{R}^2 \mid x, y > 0,\ 0 < xy \leq 1,\ \text{and } 1 \leq \frac{x}{y} < \varepsilon^2\}.$$

Show by an elementary argument that the area of the above set is $\log \varepsilon$.

5. (i) $\pi/4$.
   (ii) $\dfrac{\log(2+\sqrt{3})}{\sqrt{3}}$.
   (iii) $\dfrac{\log(5+2\sqrt{6})}{\sqrt{6}}$.
9. The numbers $\nu(i)$ for $1 \leq i \leq 10$ are respectively given by
   (i) 1, 0, 1, 1, 0, 0, 2, 0, 1, 0
   (ii) 1, 1, 0, 1, 2, 0, 2, 1, 1, 2
   (iii) 1, 0, 1, 0, 0, 0, 0, 0, 1, 0
   (iv) 1, 0, 0, 0, 0, 0, 0, 0, 0, 0
10. It is elementary and well known that $\sum_{d|n} \mu(d) = 1$, if $n = 1$ and 0, otherwise. This implies that for $s > 1$,

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

Since $\zeta_K(s) = \sum_{n=1}^{\infty} \frac{\nu(n)}{n^s}$ for $s > 1$, we have

$$\frac{\zeta_K(s)}{\zeta(s)} = \left(\sum_{m=1}^{\infty} \frac{\nu(m)}{m^s}\right)\left(\sum_{d=1}^{\infty} \frac{\mu(d)}{d^s}\right) = \sum_{n=1}^{\infty} \frac{c_n}{n^s},$$

where $c_n = \sum_{d|n} \mu(d)\nu\left(\frac{n}{d}\right)$ for each $n \in \mathbb{N}$.

Chapter 10

1. (i) $\dfrac{\log(15+4\sqrt{14})}{\sqrt{14}}$.
   (ii) $\dfrac{2\log(3+\sqrt{10})}{\sqrt{10}}$.
   (iii) $\dfrac{\pi}{\sqrt{6}}$.
   (iv) $\dfrac{\pi}{\sqrt{11}}$.

3. Let χ denote the character associated with the quadratic field $\mathbb{Q}(\sqrt{D})$. Then χ is a non-trivial numerical character modulo $|D|$ in view of Lemma 10.16. So there exists an integer s such that $\chi(s) = -1$. We can choose an infinite sequence $n_1 < n_2 < \cdots$ of positive integers such that $n_i \equiv s \pmod{|D|}$ for each i. So $\chi(n_i) = -1$ for all i. The desired assertion now follows from Proposition 10.12.
4. In view of equation (10.10), we have for $s > 1$,

$$\sum_{n=1}^{\infty} \frac{\nu(n)}{n^s} = \zeta_K(s) = L(s, \chi)\zeta(s) = \left(\sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}\right)\left(\sum_{m=1}^{\infty} \frac{1}{m^s}\right),$$

where χ is the character associated with the quadratic field $\mathbb{Q}(\sqrt{D})$. Using uniqueness theorem regarding Dirichlet's series [Apo, Theorem 11.3], we see that $\nu(n) = \sum_{k|n} \chi(k)$ for all $n \in \mathbb{N}$. Keeping in mind that $\chi(k) = \left(\frac{D}{k}\right)$ for each positive integer k by virtue of Proposition 10.12, the desired equality follows.
5. Let χ be the character associated with the quadratic field K with discriminant D. Then χ is a numerical character modulo $|D|$ and $\chi(k) = \left(\frac{D}{k}\right)$ for $k \in \mathbb{N}$. It now follows from Remark 10.5 that for each positive integer N, we have

$$\left|\sum_{j=1}^{N} \left(\frac{D}{j}\right)\right| = \left|\sum_{j=1}^{N} \chi(j)\right| < |D|.$$

Appendix A

5. $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{-3})$ are not isomorphic as fields because -3 is a square in $\mathbb{Q}(\sqrt{-3})$ but not in $\mathbb{Q}(\sqrt{3})$.
8. The inverse of $1 - \sqrt[3]{2}$ is $-(1 + 2^{1/3} + 2^{2/3})$.
13. $[E_\theta : F_\theta] \leq 3$.
14. $d = 5$ is one of the possibilities. In fact, $x^2 - 3x + 1$ is a common factor of $f(x)$ and $g(x)$.
21. $[E : \mathbb{Q}] = p(p-1)$.
26. Let M be a subfield of K of maximum degree over F for which there is an isomorphism σ_1 from M into Ω extending σ. It is to be shown that $M = K$. If $\alpha \in K \setminus M$, then using the hypothesis that Ω is algebraically closed, one can extend σ_1 to an isomorphism from $M(\alpha)$ into Ω in a natural way.
27. The $\mathbb{Q}$-conjugates of $\sqrt{2} + \iota$ are $\sqrt{2} + \iota$, $\sqrt{2} - \iota$, $-\sqrt{2} + \iota$, $-\sqrt{2} - \iota$.
The $\mathbb{Q}$-conjugates of $\sqrt{1 + \sqrt{2}}$ are $\sqrt{1 + \sqrt{2}}$, $\sqrt{1 - \sqrt{2}}$, $-\sqrt{1 + \sqrt{2}}$, $-\sqrt{1 - \sqrt{2}}$.
35. (a) The Galois group of $x^3 - 2$ over $\mathbb{Q}$ is a non-abelian group of order 6.
(b) The Galois group of $x^4 + 1$ over $\mathbb{Q}$ is isomorphic to Klein's four-group.
37. Let G, H and H_1 denote respectively the Galois groups of the polynomials $x^{mn} - 1$, $x^m - 1$ and $x^n - 1$ over $\mathbb{Q}$. Then G is isomorphic to the direct product of H and H_1.

39. Let G, H denote the Galois groups of the polynomials $x^{10} - 1$ and $x^8 - 1$ over $\mathbb{Q}$ respectively. Then G is a cyclic group of order 4 and H is isomorphic to Klein's four-group.
41. Note that E is a cyclic extension of $\mathbb{Q}$ of degree 4.
42. Let θ be a root of $x^p - a$ and ζ be a primitive pth root of unity. Then the Galois group of the polynomial $x^p - a$ over $\mathbb{Q}$ is isomorphic to the semi-direct product of a group of order p and a cyclic group of order $p - 1$. It consists of $p(p-1)$ automorphisms σ_{ij}, $1 \leq i \leq p-1$, $0 \leq j \leq p-1$ with σ_{ij} defined by

$$\zeta \longmapsto \zeta^i, \quad \theta \longmapsto \zeta^j \theta.$$

45. When $n > 2$, then $\mathbb{Q}(\theta)$ is not a normal extension of $\mathbb{Q}$ where θ is a root of $x^n - 2$.
50. Write $G = \prod_{i=1}^{k} H_i$ as a direct product of cyclic groups $H_1, \ldots, H_k$ with $|H_i| = m_i$, say. By Dirichlet's Theorem for primes in arithmetic progressions (cf. Theorem 10.10), there exist distinct primes $p_1, p_2, \ldots, p_k$ such that $p_i \equiv 1 \pmod{m_i}$. Let $n = \prod_{i=1}^{k} p_i$ and $\zeta = e^{2\pi\iota/n}$. Then in view of Corollary A.41, $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is isomorphic to the direct product $\prod_{i=1}^{k} C_i$, where each C_i is a cyclic group of order $p_i - 1$. Let D_i denote the subgroup of C_i of order $(p_i - 1)/m_i$ for $1 \leq i \leq k$. By the fundamental theorem of Galois theory, there is a subfield K of $\mathbb{Q}(\zeta)$ such that $\mathrm{Gal}(\mathbb{Q}(\zeta)/K)$ is isomorphic to $\prod_{i=1}^{k} D_i$. Deduce that $\mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $\prod_{i=1}^{k} H_i = G$.

References

[Ala] Ş Alaca, p -Integral basis of a cubic field. Proc. Amer. Math. Soc. **126**, 1949–1953 (1998)

[Al-Wi1] Ş Alaca, K.S. Williams, p -Integral basis of a quartic field defined by a trinomial $x^4 + ax + b$. Far East J. Math. Sci. **12**, 137–168 (2004)

[Al-Al] A. Alaca, Ş Alaca, An integral basis and the discriminant of a quintic field defined by a trinomial $x^5 + ax + b$, JP. J. Algebra, Number Theory Appl. **4**, 261–299 (2004)

[Al-Wi2] Ş Alaca, K.S. Williams, *Introductory Algebraic Number Theory* (Cambridge University Press, Cambridge, 2004)

[Ang] G. Angermüller, A generalisation of Ehrenfeucht's irreducibility criterion. J. Number Theory **36**, 80–84 (1990)

[Apo] T.M. Apostol, *Introduction to Analytic Number Theory* (Springer, New York, 1976)

[Art] E. Artin, *Galois Theory, University of Notre Dame Press, Notre Dame, 1942* (Reprint by Dover, New York, 1998)

[Bak] A. Baker, Linear forms in the logarithms of algebraic numbers. Mathematika **13**, 204–216 (1966)

[Bh-Kh] S. Bhatia, S.K. Khanduja, Difference polynomials and their generalisations. Mathematika **48**, 293–299 (2001)

[Bo-Sh] Z.I. Borevich, I.R. Shafarevich, *Number Theory* (Academic, New York, 1966)

[Bra] R. Brauer, On the zeta-functions of algebraic number fields. Amer. J. Math. **69** (1947), 243–250; II, **72**, 739–746 (1950)

[Ch-Da] H. Chatland, H. Davenport, Euclid's algorithm in real quadratic fields. Canad. J. Math. **2**, 289–296 (1950)

[Cla] D.A. Clark, A quadratic field which is Euclidean but not norm-Euclidean. Manuscr. Math. **83**, 327–330 (1994)

[Cho] S. Chowla, A new proof of a theorem of Siegel. Ann. Math. **51**, 120–122 (1950)

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, Berlin, 1993)

[Col] R.F. Coleman, On the Galois groups of the exponential Taylor polynomials. L'Enseignement Math. **33**, 183–189 (1987)

[Ded1] R. Dedekind, Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. Götttingen Abh. **23**, 1–23 (1878)

[Ded2] R. Dedekind, *Theory of Algebraic Integers* (Cambridge University Press, Cambridge, 1996)

[Dum] G. Dumas, Sur quelques cas d'irréductibilité des polynômes á coefficients rationnels. J. Math. Pures Appl. **6**, 191–258 (1906)

[Edw] H.M. Edwards, Dedekind's invention of ideals. Bull. Lond. Math. Soc. **15**(1), 8–17 (1983)

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8

[Es-Mu] J. Esmonde, M. Ram Murty, *Problems in Algebraic Number Theory*. Graduate Texts in Mathematics, vol. 190 (Springer, New York, 1999)
[Fun] T. Funakura, On integral bases of pure quartic fields. Math. J. Okayama Univ. **26**, 27–41 (1984)
[Gas] T.A. Gassert, A note on monogenity of power maps. Albanian J. Math. **11**, 3–12 (2017)
[Gau] C.F. Gauss, *Disquisitiones Arithmeticae (1801), English Translation* (Yale University Press, London, 1966)
[Go-Lu] S.K. Khanduja (nee Gogia), I.S.Luthar, Quadratic unramified extensions of $\mathbb{Q}(\sqrt{d})$. J. Reine Angew. Math. **298**, 108–111 (1978)
[Gol] D.M. Goldfeld, Gauss' class number problem for imaginary quadratic fields. Bull. Amer. Math. Soc. **13**, 23–37 (1985)
[Hec] E. Hecke, *Lectures on the Theory of Algebraic Numbers, Graduate Texts in Mathematics* vol. 77 (Springer, New York, 1981)
[Hei] H. Heilbronn, On Euclid's algorithm in real quadratic fiels. Proc. Cambridge Phil. Soc. **34**, 521–526 (1938)
[He-Li] H. Heilbronn, E.H. Linfoot, On the imaginary quadratic corpora of class number one. Quart. J. Math. (Oxford) **5**, 293–301 (1934)
[Her] I.N. Herstein, *Topics in Algebra*, 2nd edn. (Wiley, New York, 2006)
[Iya] S. Iyanaga, *The Theory of Numbers* (North-Holland, Oxford, 1975)
[Jak1] A. Jakhar, On the factors of a polynomial. Bull. London. Math. Soc. **52**, 158–160 (2020)
[Jak2] A. Jakhar, Explicit integral basis of pure sextic number fields. Rocky Mountain J. Math. **51**, 571–580 (2021)
[Ja-Kh1] A. Jakhar, S.K. Khanduja, On the index of an algebraic integer and beyond. J. Pure Appl. Algebra **224**, 106281 (10 pages) (2020)
[Ja-Kh2] A. Jakhar, S.K. Khanduja, A note on Dedekind criterion. J. Algebra Appl. **20**, 2150066 (7 pages) (2021)
[Ja-Sa] A. Jakhar, N. Sangwan, The integral basis of pure prime degree number fields. Indian J. Pure Appl. Math. **50**, 309–314 (2019)
[Jh-Kh] B. Jhorar, S.K. Khanduja, On power basis of a class of algebraic number fields. Int. J. Number theory **12**, 2317–2321 (2016)
[J-K-S1] A. Jakhar, S.K. Khanduja, N. Sangwan, On prime divisors of the index of an algebraic integer. J. Number Theory **166**, 47–61 (2016)
[J-K-S2] A. Jakhar, S.K. Khanduja, N. Sangwan, Characterization of primes dividing the index of a trinomial. Int. J. Number Theory **13**, 2205–2214 (2017)
[J-K-S3] A. Jakhar, S.K. Khanduja, N. Sangwan, Discriminant of pure squarefree degree number fields. Acta Arith **181**, 287–296 (2017)
[J-K-S4] A. Jakhar, S.K. Khanduja, N. Sangwan, On the discriminant of pure number fields. Colloq. Math. **167**, 149–157 (2021)
[J-K-S5] A. Jakhar, S.K. Khanduja, N. Sangwan, On integral basis of pure number fields. Mathematika **67**, 187–195 (2021)
[Ka-Kh] S. Kaur, S.K. Khanduja, Discriminant and integral bases of sextic fields defined by $x^6 + ax + b$, Comm. Algebra (to appear); https://doi.org/10.1080/00927872.2022.2025820
[Kau1] G. Kaur, The minimum discriminant of sixth degree totally real algebraic number fields and other results, Ph.D. Thesis (Panjab University, Chandigarh, 1964)
[Kau2] G. Kaur, The minimum discriminant of sixth degree totally real algebraic number fields. J. Indian Math. Soc. **34**, 123–134 (1970)
[Kh-Ku1] S.K. Khanduja, M. Kumar, A generalization of Dedekind criterion. Commun. Algebra **35**, 1479–1486 (2007)
[Kh-Ku2] S.K. Khanduja, M. Kumar, On a theorem of Dedekind. Int. J. Number Theory **4**, 1019–1025 (2008)
[Kom] K. Komatsu, Integral bases in algebraic number fields. J. Reine Angew. Math. **278**(279), 137–144 (1975)
[Kür] J. Kürschàk, Über Limesbildung und allgemeine Körpertheorie. J. Reine Angew. Math. **142**, 211–253 (1913)

[Lan] S. Lang, *Algebra, (Revised)*, 3rd edn. (Springer, New York, 2002)
[Lan2] S. Lang, *Algebraic Number Theory*, 2nd edn. (Springer, New York, 1994)
[L-N-V1] P. Llorente, E. Nart, N. Vila, Discriminants of number fields defined by trinomials. Acta Arith **43**, 367–373 (1984)
[L-N-V2] P. Llorente, E. Nart, N. Vila, Decomposition of primes in number fields defined by trinomials. Séminaire de Théorie des Nombres Bordeaux **3**, 27–41 (1991)
[Lu-Pa1] I.S. Luthar, I.B.S. Passi, *Algebra, volume 2, Rings* (Narosa Publishing House, New Delhi, 2002)
[Lu-Pa2] I.S. Luthar, I.B.S. Passi, *Algebra volume 4, , Field Theory* (Narosa Publishing House, New Delhi, 2004)
[Mar] D.A. Marcus, *Number Fields, Universitext* (Springer, New York, 1977)
[Nar] W. Narkiewicz, *Elementary and Analytical Theory of Algebraic Numbers* (Springer, Berlin, 2004)
[Neu] J. Neukirch, *Algebraic Number Theory* (Springer, Berlin, 1999)
[Ost] A. Ostrowski, Über einige Lösungen der Funktionalgleichung $\phi(x)\phi(y) = \phi(xy)$. Acta Math. **41**, 271–284 (1918)
[Poh] M. Pohst, On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields. J. Number Theory **14**, 99–117 (1982)
[Rib] P. Ribenboim, *Classical Theory of Algebraic Numbers* (Springer, New York, 2001)
[Roq1] P. Roquette, *History of Valuation Theory Part 1, Valuation Theory and Its Applications, vol. 1*. Fields Institute Communications, vol. 32 (American Mathematical Society, Providence, 2002), pp. 291–355
[Roq2] P. Roquette, *Contributions to the history of Number Theory in the 20th centuary* (Eur. Math, Soc, 2013)
[Sie] C.L. Siegel, Über die Classenzahl quadratischer Zahlkörper. Acta Arith **1**, 83–86 (1936)
[Sin] S. Singh, *Fermat's Last Theorem* (Fourth Estate Ltd., 1997)
[Niv] I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers* (Wiley, Canada, 1991)
[Sel] E.S. Selmer, On the irreducibility of certain trinomials. Math. Scand. **4**, 287–302 (1956)
[Sta] H.M. Stark, A complete determination of the complex quadratic fields of class-number one. Michigan Math. J. **14**, 1–27 (1967)
[St-Ta] I. Stewart, D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 4th edn. (CRC Press, 2015)
[Ta-Wi] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras. Ann. Math. **141**, 553–572 (1995)
[Tig] J.-P. Tignol, *Galois' Theory of Algebraic Equations* (World Scientific Publishing Company, 2001)
[Wes] J. Westlund, On the fundamental number of the algebraic number field $k(\sqrt[p]{m})$. Trans. Amer. Math. Soc. **11**, 388–392 (1910)
[Wil] A. Wiles, Modular elliptic curves and Fermat's last theorem. Ann. Math. **141**, 443–551 (1995)
[Za-Sa] O. Zariski, P. Samuel, *Commutative Algebra Volume I*. Graduate Texts in Mathematics, vol. 28, Ist edn. (Springer, 1975)

Index

S. K. Khanduja, *A Textbook of Algebraic Number Theory*, UNITEXT 135,
https://doi.org/10.1007/978-981-16-9150-8