V. Three Theorems in Algebraic Number Theory, 262-312

DOI: 10.3792/euclid/9781429799928-5

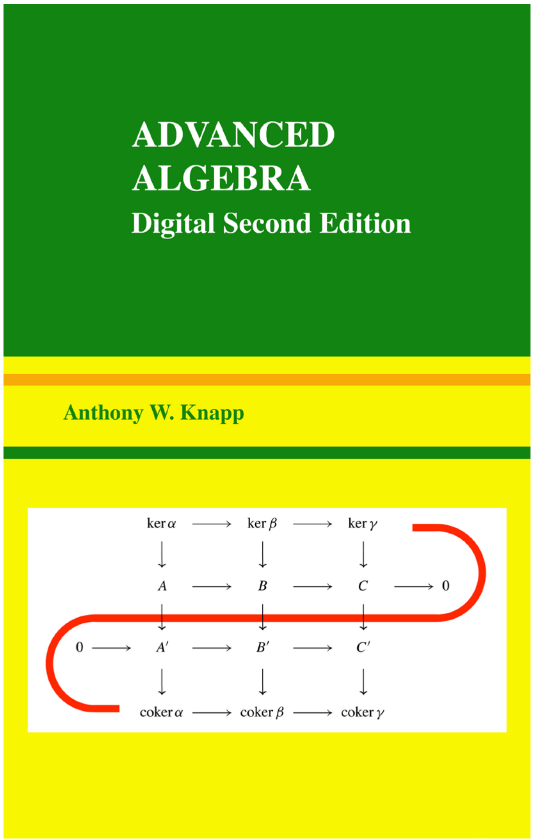
Advanced Algebra

Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799928

ISBN: 978-1-4297-9992-8



ADVANCED
ALGEBRA
Digital Second Edition

Anthony W. Knapp

$$\begin{tikzcd}
 & \ker\alpha \arrow[r] \arrow[d] & \ker\beta \arrow[r] \arrow[d] & \ker\gamma \arrow[d] \arrow[dddll, red, rounded corners] & \\
 & A \arrow[r] \arrow[d] & B \arrow[r] \arrow[d] & C \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A' \arrow[r] \arrow[d] & B' \arrow[r] \arrow[d] & C' \arrow[d] & \\
 & \operatorname{coker}\alpha \arrow[r] & \operatorname{coker}\beta \arrow[r] & \operatorname{coker}\gamma &
\end{tikzcd}$$

Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/∼aknapp

Title: Advanced Algebra
Cover: Content of the Snake Lemma; see page 185.

Mathematics Subject Classification (2010): 11–01, 13–01, 14–01, 16–01, 18G99, 55U99, 11R04, 11S15, 12F99, 14A05, 14H05, 12Y05, 14A10, 14Q99.

First Edition, ISBN-13 978-0-8176-4522-9
©2007 Anthony W. Knapp
Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN
©2016 Anthony W. Knapp
Published by the Author

CHAPTER V

Three Theorems in Algebraic Number Theory

Abstract. This chapter establishes some essential foundational results in the subject of algebraic number theory beyond what was already in *Basic Algebra*.

Section 1 puts matters in perspective by examining what was proved in Chapter I for quadratic number fields and picking out questions that need to be addressed before one can hope to develop a comparable theory for number fields of degree greater than 2.

Sections 2–4 concern the field discriminant of a number field. Section 2 contains the definition of discriminant, as well as some formulas and examples. The main result of Section 3 is the Dedekind Discriminant Theorem. This concerns how prime ideals (p) in $\mathbb{Z}$ split when extended to the ideal $(p)R$ in the ring of integers R of a number field. The theorem says that ramification, i.e, the occurrence of some prime ideal factor in R to a power greater than 1, occurs if and only if p divides the field discriminant. The theorem is proved only in a very useful special case, the general case being deferred to Chapter VI. The useful special case is obtained as a consequence of Kummer's criterion, which relates the factorization modulo p of irreducible monic polynomials in $\mathbb{Z}[X]$ to the question of the splitting of the ideal $(p)R$. Section 4 gives a number of examples of the theory for number fields of degree 3.

Section 5 establishes the Dirichlet Unit Theorem, which describes the group of units in the ring of algebraic integers in a number field. The torsion subgroup is the subgroup of roots of unity, and it is finite. The quotient of the group of units by the torsion subgroup is a free abelian group of a certain finite rank. The proof is an application of the Minkowski Lattice-Point Theorem.

Section 6 concerns class numbers of algebraic number fields. Two nonzero ideals I and J in the ring of algebraic integers of a number field are equivalent if there are nonzero principal ideals (a) and (b) with $(a)I = (b)J$. It is relatively easy to prove that the set of equivalence classes has a group structure and that the order of this group, which is called the class number, is finite. The class number is 1 if and only if the ring is a principal ideal domain. One wants to be able to compute class numbers, and this easy proof of finiteness of class numbers is not helpful toward this end. Instead, one applies the Minkowski Lattice-Point Theorem a second time, obtaining a second proof of finiteness, one that has a sharp estimate for a finite set of ideals that need to be tested for equivalence. Some examples are provided. A by-product of the sharp estimate is Minkowski's theorem that the field discriminant of any number field other than $\mathbb{Q}$ is greater than 1. In combination with the Dedekind Discriminant Theorem, this result shows that there always exist ramified primes over $\mathbb{Q}$.

1. Setting

It is worth stepping back from the results of Chapter I to put matters into perspective. Chapter I studied three problems, all of which could be stated in terms of elementary number theory. These were the questions of solvability of quadratic congruences, of representability of integers or rational numbers by primitive binary quadratic forms, and of the infinitude of primes in arithmetic progressions.

We had started from the more general problem of studying Diophantine equations, beginning with the observation that solvability in integers implies solvability modulo each prime.[1] Linear congruences being no problem, we began with quadratic congruences and were led to quadratic reciprocity. Then we sought to apply quadratic reciprocity to address representability of integers or rational numbers by binary quadratic forms. The reasons for studying the infinitude of primes in arithmetic progressions were more subtle; what we saw was that at various stages in dealing with binary quadratic forms, this question of infinitude kept arising, along with techniques that might be helpful in addressing it.

Work on at least the first two of the problems was helped to some extent by the use of algebraic integers, and we shall see momentarily that algebraic integers illuminate work on the third problem as well. In any event, it is apparent where to look for a natural generalization. We are to study higher-degree congruences, perhaps in more than one variable, and we are to use algebraic extensions of the rationals of degree greater than 2 to help in the study.

The situation studied in Section IX.17 of *Basic Algebra* will be general enough for now. Thus let $F(X)$ be a monic irreducible polynomial in $\mathbb{Z}[X]$. Section IX.17 began to look at the question of how $F(X)$ reduces modulo each prime p. We begin by reviewing the case of degree 2, the main results in this case having been obtained in Chapter I in the present volume. For the polynomial $F(X) = X^2 - m$ with $m \in \mathbb{Z}$, the assumed irreducibility means that m is not the square of an integer. For fixed m and most primes p, either $F(X)$ remains irreducible modulo p or $F(X)$ splits as the product of two distinct linear factors. The exceptional primes have the property that $F(X)$ modulo p is the square of a linear factor; these are the prime divisors of m and sometimes the prime 2. In short, they occur among the prime divisors of the discriminant $4m$ of $F(X)$. In terms of quadratic residues, the irreducibility of $F(X)$ modulo p means that m is not a quadratic residue modulo p, and the splitting into two distinct linear factors means that it is. The odd primes for which $F(X)$ modulo p is the square of a linear factor are the odd primes that divide m. Modulo 2, every integer is a square, and reduction modulo 2 was not helpful.

The number theory of quadratic number fields sheds additional light on this factorization. The relevant field is of course $\mathbb{Q}(\sqrt{m}\,)$; this is a nontrivial extension of $\mathbb{Q}$, since m is not square. In working with this field in Chapter I, we imposed the additional condition that m be square free. Promising a general definition for

[1] Solvability modulo each prime power is also of interest but played a role in Chapter I only for powers of 2.

later, we defined the **field discriminant** of $\mathbb{Q}(\sqrt{m}\,)$ in that chapter to be

$$D = \begin{cases} 4m & \text{if } m \equiv 2 \bmod 4 \text{ or } m \equiv 3 \bmod 4, \\ m & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

Problems 20–24 in Chapter I implicitly related the splitting of $F(X)$ modulo p to the factorization of ideals. Let R be the ring of algebraic integers in $\mathbb{Q}(\sqrt{m}\,)$. If p is an odd prime, those problems observed that $(p)R$ is a prime ideal in R if D is a nonsquare modulo p, is the product of two distinct prime ideals if D is a square modulo p but is not divisible by p, and is the square of a prime ideal if D is divisible by p. The factorization of $(2)R$ was more subtle and was addressed in Problem 21.

In any event, the pattern of reducibility modulo p of $X^2 - m$, at least when the prime p is odd, mirrors the pattern of factorization of the ideal generated by p in the ring of algebraic integers in the number field $\mathbb{Q}(\sqrt{m}\,)$. The role of quadratic reciprocity was to explain this pattern. Problem 1 at the end of Chapter I showed that one qualitative consequence of quadratic reciprocity is that the odd primes p for which $X^2 - m$ remains irreducible are the ones in certain arithmetic progressions, and similarly for the odd primes not dividing p for which a factorization into two linear factors occurs.

One objective of a generalization is to produce a corresponding theory for an arbitrary monic irreducible polynomial $F(X)$ in $\mathbb{Z}[X]$, say of degree n. Let $\mathbb{K}$ be the extension of $\mathbb{Q}$ generated by a root of $F(X)$, and let R be the ring of algebraic integers in $\mathbb{K}$. Theorem 9.60 of *Basic Algebra* shows for each prime number p that the decomposition of the ideal $(p)R$ in R as a product of powers of distinct prime ideals takes the form $(p)R = \prod_{i=1}^{g} P_i^{e_i}$ with $f_i = [R/P_i : \mathbb{Z}/(p)]$ and $\sum_{i=1}^{g} e_i f_i = n$. Meanwhile, $F(X)$ factors modulo p as a product of powers of irreducible polynomials modulo p. Sections 2–3 will describe a theory begun by Kummer and Dedekind for how the factorization of the ideal $(p)R$ and the factorization of the polynomial $F(X)$ modulo p are related. One introduces a field discriminant for $\mathbb{K}$ that is closely related to the discriminant of the polynomial $F(X)$, and a key result, the Dedekind Discriminant Theorem, says that some e_i is > 1 if and only if p divides the field discriminant. The primes p for which some e_i is greater than 1 are said to **ramify** in the extension field $\mathbb{K}$. These primes are not as well behaved as the others, and one's first inclination might be to try to ignore them. However, Problems 25–40 at the end of Chapter I show that the ramified primes encode a great deal of information; in particular, they explain the theory of genera and the relationship between exact representability of rational numbers and representability of integers modulo the field discriminant.

Generalizations of quadratic reciprocity lie much deeper and are central results of the subject of class field theory, a subject that is beyond the scope of the present book. Suffice it to say that class field theory in its established form seeks to parametrize all finite Galois extensions of any number field having abelian Galois group; the parametrization is to refer only to data within the given number field. The reciprocity theorem in this setting goes under the name "Artin reciprocity," which includes quadratic reciprocity as a very special case. Class field theory for nonabelian finite Galois extensions is at present largely conjectural, and the conjectural reciprocity statement goes under the name "Langlands reciprocity."

Beginning in Section I.6, we translated some of the theory of binary quadratic forms into facts about quadratic number fields. One tool we needed was a description of the units in the ring of algebraic integers within the quadratic number field. It is to be expected that a similar description for an arbitrary number field will play a foundational role in number theory beyond the quadratic case. The description in question is captured in the Dirichlet Unit Theorem, which appears as Theorem 5.13 in Section 5.

The translation of the notion of proper equivalence class of binary quadratic forms into the language of quadratic field extensions led to a notion of strict equivalence of ideals, as well as a notion of ordinary equivalence. Because there are only finitely many proper equivalence classes of forms, there could be only finitely many strict equivalence classes of ideals, and this set of classes of ideals acquired the structure of a finite abelian group. Dirichlet studied the order of this group, which figures into formulas for the value of certain Dirichlet L functions $L(s, \chi)$ at $s = 1$. The ideal class group for ordinary equivalence is a quotient of this group by a subgroup of order at most 2.

Although we shall not be concerned with representability of integers by forms of degree greater than 2, the ideal class group and its order (the "class number" of the field) are of interest for general number fields when defined in terms of ordinary equivalence, not strict equivalence. Section 6 is devoted to proving that the class number is finite for any number field and to developing some tools for computing class numbers. Class number 1 is equivalent to having the ring of algebraic integers in question be a principal ideal domain. Apart from the appearance of class numbers in various limit formulas, here is one other indicator of the importance of the ideal class group: It is possible to extend the above theory of ramification in such a way that it applies to any extension $\mathbb{K}/\mathbb{F}$ of number fields, not just to finite extensions of $\mathbb{Q}$. Hilbert proved that for any $\mathbb{F}$, there is a finite Galois extension $\mathbb{K}/\mathbb{F}$ with abelian Galois group that is small enough for the extension to be unramified at every prime ideal of $\mathbb{F}$ and that is large enough for any unramified abelian extension of $\mathbb{F}$ to lie in $\mathbb{K}$. Artin reciprocity can be used to show that $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is isomorphic to the ideal class group[2] of $\mathbb{F}$ and thus gives some control over the nature of $\mathbb{K}$. In particular, $\mathbb{K} = \mathbb{F}$ if and only if every ideal in the ring of integers of $\mathbb{F}$ is principal. When $\mathbb{F}$ is quadratic over $\mathbb{Q}$, the

[2] The field $\mathbb{K}$ is called the **Hilbert class field** of $\mathbb{F}$. The name "class field" is meant to be a reminder of this isomorphism.

field $\mathbb{K}$ can be used to give more definitive results than in Chapter I concerning representability of integers by binary quadratic forms.

2. Discriminant

Let us recall some material about Dedekind domains from Chapters VIII and IX of *Basic Algebra*. A Dedekind domain is a Noetherian integral domain that is integrally closed and has the property that every nonzero prime ideal is maximal. Any principal ideal domain is an example. Any Dedekind domain has unique factorization for its ideals. Theorem 8.54 of the book gave a construction for extending certain Dedekind domains to larger Dedekind domains: if D is a Dedekind domain with field of fractions $\mathbb{F}$ and if $\mathbb{K}$ is a finite separable extension of $\mathbb{F}$, then the integral closure of D in $\mathbb{K}$ is a Dedekind domain R. The hard step in the proof, which was not carried out until Section IX.15, was to deduce from the separability that R is finitely generated over D. The role of separability was to force the bilinear form $(a, b) \mapsto \mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(ab)$ to be nondegenerate, and this nondegeneracy in turn implied the desired result about finite generation.

In this section we introduce a tool that captures this last implication in quantitative fashion—that nondegeneracy of the trace form implies that the extended domain is finitely generated over the given domain. In a full-fledged treatment of algebraic number theory, one might well want to work in this full generality,[3] but we need less for our purposes: Throughout this section we assume that the given Dedekind domain is the ring $\mathbb{Z}$ of integers, that $\mathbb{K}$ is a number field, and that R is the integral closure of $\mathbb{Z}$ in $\mathbb{K}$, i.e., R is the ring of algebraic integers within $\mathbb{K}$. Let $n = [\mathbb{K} : \mathbb{Q}]$ be the degree of the field extension. Since $\mathbb{C}$ is algebraically closed, we can regard $\mathbb{K}$ as a subfield of $\mathbb{C}$.

The separability of $\mathbb{K}/\mathbb{Q}$ in combination with the fact that $\mathbb{C}$ is algebraically closed implies that there exist exactly n distinct field maps $\sigma_1, \dots, \sigma_n$ of $\mathbb{K}$ into $\mathbb{C}$; one of them is the identity. Recall how $\sigma_1, \dots, \sigma_n$ can be constructed: if ξ is a primitive element for $\mathbb{K}/\mathbb{Q}$, if $F(X)$ is the minimal polynomial of ξ over $\mathbb{Q}$, and if $\xi_1 = \xi,\ \xi_2, \dots, \xi_n$ are the n distinct roots of $F(X)$ in $\mathbb{C}$, then σ_j can be defined by $\sigma_j\big(\sum_{i=0}^{n-1} c_i\xi^i\big) = \sum_{i=0}^{n-1} c_i\xi_j^i$ on any $\mathbb{Q}$ linear combination of powers of ξ. For any $\eta = \sum_{i=0}^{n-1} c_i\xi^i$ in $\mathbb{K}$, primitive or not, the n elements $\sigma_i(\eta)$ of $\mathbb{C}$ are called the **conjugates** of η relative to $\mathbb{K}$. They are the roots of the field polynomial of η over $\mathbb{K}$, and each occurs with multiplicity $[\mathbb{K} : \mathbb{Q}(\eta)]$.[4]

[3] For example this full level of generality would be appropriate if one planned ultimately to study class field theory.

[4] The field polynomial of an element of $\mathbb{K}$ is the characteristic polynomial of left multiplication on $\mathbb{K}$ by the element. This notion is discussed in Section IX.15 of *Basic Algebra*.

Let $\Gamma = (v_1, \dots, v_n)$ be an ordered basis of $\mathbb{K}$ over $\mathbb{Q}$. The symmetric bilinear form $(u, v) \mapsto \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(uv)$ determines an n-by-n symmetric matrix $B_{ij} = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(v_i v_j)$, and we can recover the form from the matrix B by the formula $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(uv) = a^t Bb$ if $a = \left(\begin{smallmatrix} u \\ \Gamma \end{smallmatrix}\right)$ and $b = \left(\begin{smallmatrix} v \\ \Gamma \end{smallmatrix}\right)$ are the column vectors of u and v in the ordered basis Γ, i.e., if $u = \sum_{i=1}^n a_i v_i$ and $v = \sum_{j=1}^n b_j v_j$. From Section VI.1 of *Basic Algebra*, we know that the bilinear form determines a canonical $\mathbb{Q}$ linear map L from $\mathbb{K}$ to its vector space dual by the formula $L(u)(v) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(uv)$ and that the nondegeneracy of the form[5] implies that this linear map is one-one onto. Moreover, the matrix of L with respect to Γ and the dual basis of Γ is B. Thus the nondegeneracy implies that the matrix B is nonsingular. The **discriminant** $D(\Gamma)$ of the ordered basis Γ is given by

$$D(\Gamma) = \det B, \quad \text{where } B \text{ is the matrix of } (u, v) \mapsto \mathrm{Tr}_{L/K}(uv) \text{ in the basis } \Gamma.$$

Because of the nonsingularity of B, this is a nonzero member of $\mathbb{Q}$.

Proposition 6.1 of *Basic Algebra* shows the effect on the matrix B of changing the basis. Specifically let $\Delta = (w_1, \dots, w_n)$ be a second ordered basis, and let C be the matrix of the form in this basis, namely $C_{ij} = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(w_i w_j)$. Let the two bases be related by $w_j = \sum_{i=1}^n a_{ij} v_i$, i.e., let $[a_{ij}] = \left(\begin{smallmatrix} I \\ \Gamma\Delta \end{smallmatrix}\right)$. Then the proposition gives

$$C = \left(\begin{smallmatrix} I \\ \Gamma\Delta \end{smallmatrix}\right)^t B \left(\begin{smallmatrix} I \\ \Gamma\Delta \end{smallmatrix}\right).$$

Taking determinants and using the fact that a matrix and its transpose have the same determinant, we obtain

$$D(\Delta) = D(\Gamma) \left(\det \left(\begin{smallmatrix} I \\ \Gamma\Delta \end{smallmatrix}\right)\right)^2.$$

One consequence of this formula is that the sign of $D(\Gamma)$ is independent of Γ. Another is that the value of $D(\Gamma)$ does not depend on the ordering of the n members of Γ; it depends only on Γ as an unordered set.

Now suppose that the members of the ordered basis Γ are in the subring R of algebraic integers within $\mathbb{K}$. Bases of $\mathbb{K}$ over $\mathbb{Q}$ consisting of members of R always exist, since we can always multiply the members of a basis of $\mathbb{K}$ over $\mathbb{Q}$ by a suitable integer to get them to be in R. In this case the entries $B_{ij} = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(v_i v_j)$ of the matrix of the bilinear form are in $\mathbb{Z}$, and $D(\Gamma)$ is therefore a nonzero member of $\mathbb{Z}$.

The **field discriminant**, or **absolute discriminant**, of $\mathbb{K}$, denoted by $D_{\mathbb{K}}$, is the value of $D(\Gamma)$ that minimizes $|D(\Gamma)|$ for all bases of $\mathbb{K}$ consisting of members

[5] The nondegeneracy of the trace form for a number field is a transparent result, not requiring anything deep from Section IX.15 of *Basic Algebra*, since any $u \neq 0$ in $\mathbb{K}$ has $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(uu^{-1}) = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(1) = n \neq 0$.

of R. This is a nonzero integer. The sign of $D_{\mathbb{K}}$ is well defined, since all values of $D(\Gamma)$ have the same sign.[6]

Fix an ordered basis $\Gamma = (v_1, \dots, v_n)$ of $\mathbb{K}$, and consider the abelian group consisting of the $\mathbb{Z}$ span $\mathbb{Z}(\Gamma)$ of the members of Γ. This is evidently a free abelian group of rank n. If an ordered basis $\Delta = (w_1, \dots, w_n)$ has the property that $\mathbb{Z}(\Delta) \subseteq \mathbb{Z}(\Gamma)$, then the theory in Section IV.9 of *Basic Algebra* that leads to the Fundamental Theorem of Finitely Generated Abelian Groups shows that if we write formally

$$\begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix} = C \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

then there exist n-by-n integer matrices M_1 and M_2 of determinant ± 1 such that $D = M_1 C M_2$ is diagonal, and moreover the order of $\mathbb{Z}(\Gamma)/\mathbb{Z}(\Delta)$ is $|\det D| = |\det C|$. Examining the definition of C, we see that $C = \begin{pmatrix} I \\ \Gamma\Delta \end{pmatrix}^t$. Consequently we obtain

$$|\mathbb{Z}(\Gamma)/\mathbb{Z}(\Delta)| = \Big|\det \begin{pmatrix} I \\ \Gamma\Delta \end{pmatrix}\Big|,$$

a formula we shall use repeatedly in this chapter without specific reference.

Proposition 5.1. If Γ is a basis of $\mathbb{K}$ over $\mathbb{Q}$ whose members all lie in R, then $|R\big/\mathbb{Z}(\Gamma)|^2 = D(\Gamma)/D_{\mathbb{K}}$. In particular, Γ is a $\mathbb{Z}$ basis of R if and only if $D(\Gamma) = D_{\mathbb{K}}$.

REMARKS. We already know from *Basic Algebra* that R is a free abelian group of rank n. The second conclusion of this proposition, in combination with the transparent observation that the trace form is nonsingular for a number field, gives a more direct proof of this fact. Introductory treatments of algebraic number theory sometimes give this more direct proof, whose details are spelled out in the second paragraph below.

PROOF. Let Δ and Ω be two bases of $\mathbb{K}$ over $\mathbb{Q}$ whose members all lie in R, and suppose that $\mathbb{Z}(\Delta) \subseteq \mathbb{Z}(\Omega)$. Then the above discussion shows that

$$|D(\Delta)| = |D(\Omega)| \Big(\det \begin{pmatrix} I \\ \Omega\Delta \end{pmatrix}\Big)^2$$

and that

$$\big|\mathbb{Z}(\Omega)/\mathbb{Z}(\Delta)\big|^2 = \Big(\det \begin{pmatrix} I \\ \Omega\Delta \end{pmatrix}\Big)^2.$$

Since $D(\Delta)$ and $D(\Omega)$ are nonzero and have the same sign, we obtain

$$D(\Delta)/D(\Omega) = \big|\mathbb{Z}(\Omega)/\mathbb{Z}(\Delta)\big|^2. \qquad (*)$$

[6] As was observed above, any $D(\Delta)$ is the product of $D(\Gamma)$ and the square of a rational number. Hence $D(\Delta)$ and $D(\Gamma)$ have the same sign.

To prove the proposition, we prove the "if" part of the second conclusion first—without using the known fact that R is free abelian. Choose Δ such that $D(\Delta) = D_{\mathbb{K}}$ and such that Δ has all its members in R. Arguing by contradiction, suppose that Δ fails to be a $\mathbb{Z}$ basis of R. Let r be an element of R not in $\mathbb{Z}(\Delta)$. Then the $\mathbb{Z}$ span of $\mathbb{Z}(\Delta) \cup \{r\}$ is a finitely generated additive subgroup of $\mathbb{K}$ and must be free abelian of rank $\geq n$. Being a subgroup of the additive group of $\mathbb{K}$, it cannot have rank greater than n and hence has rank exactly n. Let Ω be an ordered $\mathbb{Z}$ basis of this subgroup. Since $\mathbb{Z}(\Delta) \subsetneqq \mathbb{Z}(\Omega)$, the right side of $(*)$ is > 1, and thus $D_{\mathbb{K}} > D(\Omega)$. But this is a contradiction because the members of Ω lie in R, and hence Δ is a $\mathbb{Z}$ basis of R. In particular, a $\mathbb{Z}$ basis of R exists.

To prove the rest of the proposition, take Ω in $(*)$ to be a $\mathbb{Z}$ basis of R, and let $\Delta = \Gamma$ be any given basis of $\mathbb{K}$ over $\mathbb{Q}$ that lies in R. Then $(*)$ gives $|R/\mathbb{Z}(\Gamma)|^2 = D(\Gamma)/D(\Omega)$. Since $|R/\mathbb{Z}(\Gamma)|$ cannot be less than 1, $|D(\Gamma)|$ cannot be less than $|D(\Omega)|$. Thus $D_{\mathbb{K}} = D(\Omega)$, and $|R/\mathbb{Z}(\Gamma)|^2 = D(\Gamma)/D_{\mathbb{K}}$. This proves the first conclusion of the proposition, and the "only if" part of the second conclusion is immediate. □

EXAMPLE. Field discriminant of a quadratic number field. Let $\mathbb{K} = \mathbb{Q}(\sqrt{m}\,)$, where m is a square-free integer other than 1. From Section I.6 a $\mathbb{Z}$ ordered basis Γ of R is given by

$$\Gamma = \begin{cases} \{1,\ \sqrt{m}\,\} & \text{if } m \equiv 2 \text{ or } 3 \bmod 4, \\ \{1,\ \tfrac{1}{2}(\sqrt{m} - 1)\} & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

Proposition 5.1 allows us to compute $D_{\mathbb{K}}$ from this information. The matrix whose determinant is $D_{\mathbb{K}}$ in the two cases is $\begin{pmatrix} 2 & 0 \\ 0 & 2m \end{pmatrix}$ and $\begin{pmatrix} 2 & -1 \\ -1 & \frac{1}{2}(m+1) \end{pmatrix}$, respectively, and thus

$$D_{\mathbb{K}} = \begin{cases} 4m & \text{if } m \equiv 2 \text{ or } 3 \bmod 4, \\ m & \text{if } m \equiv 1 \bmod 4. \end{cases}$$

This is the formula that we took as a definition of field discriminant in Section I.6.

For a general number field $\mathbb{K}$ of degree n over $\mathbb{Q}$, there is no easy way to obtain a $\mathbb{Z}$ basis of R. Instead, one tries to compute $D_{\mathbb{K}}$ and find such a basis at the same time by successive refinements.

The first step is to use the special kind of $\mathbb{Q}$ basis of $\mathbb{K}$ whose existence is guaranteed by the Theorem of the Primitive Element. Specifically one can write $\mathbb{K} = \mathbb{Q}(\xi)$ for some ξ in $\mathbb{K}$, since $\mathbb{K}/\mathbb{Q}$ is a separable extension. Possibly after multiplying ξ by a suitably large integer, we may assume that ξ is in R. Then $\Gamma(\xi) = \{1, \xi, \xi^2, \ldots, \xi^{n-1}\}$ is a $\mathbb{Q}$ basis of $\mathbb{K}$ lying in R. We normally write $D(\xi)$ instead of $D(\Gamma(\xi))$ for the discriminant of $\Gamma(\xi)$. Write $\xi_i = \sigma_i(\xi)$ for the

i^{th} conjugate of ξ. Let $B = [B_{ij}]$ be the matrix whose determinant is $D(\xi)$. Since the trace of an element is the sum of its conjugates, B_{ij} is given by

$$B_{ij} = \operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\xi^{i-1}\xi^{j-1}) = \sum_{k=1}^{n} \sigma_k(\xi^{i-1}\xi^{j-1}) = \sum_{k=1}^{n} \xi_k^{i-1}\xi_k^{j-1},$$

and this is of the form $\sum_{k=1}^{n} V_{ik}V_{jk}^t$, where $V_{ik} = \xi_k^{i-1}$ is an entry of a Vandermonde matrix. Therefore

$$D(\xi) = \det B = (\det V)^2 = \Big(\prod_{i<j}(\xi_j - \xi_i)\Big)^2 = \prod_{i<j}(\xi_j - \xi_i)^2,$$

which coincides with the discriminant of the field polynomial of ξ over $\mathbb{Q}$.

EXAMPLES OF $D(\xi)$.

(1) $\mathbb{K} = \mathbb{Q}(\xi)$, where $\xi^5 - \xi - 1 = 0$. This field was studied in Example 1 of Section IX.17 of *Basic Algebra*. The discriminant of the polynomial $X^5 - X - 1$ is $2869 = 19 \cdot 151$, and thus $D(\xi) = 2869$. Proposition 5.1 shows that $D(\xi) = D_{\mathbb{K}}k^2$ for some nonzero integer k. Since 2869 is square free, we conclude that $D_{\mathbb{K}} = 2869$.

(2) $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$. The minimal polynomial of $\xi = \sqrt[3]{2}$ is $X^3 - 2$, and its roots are ξ, $\xi\omega$, and $\xi\omega^2$, where $\omega = e^{2\pi i/3}$. Then

$$D(\xi) = (\xi - \xi\omega)^2(\xi - \xi\omega^2)^2(\xi\omega - \xi\omega^2)^2 = \xi^6(1-\omega)^2(1-\omega^2)^2(\omega-\omega^2)^2,$$

and this simplifies to $D(\xi) = -2^2 3^3$. This quantity is the product of $D_{\mathbb{K}}$ by the square of an integer. Thus $D_{\mathbb{K}}$ is one of -3, -12, -27, and -108.

What happens with Example 2 is typical: a second step is needed to decide among finitely many possibilities for $D_{\mathbb{K}}$. In the general case an induction is involved, and Proposition 5.2 below says what is to be done at each step. At the end of this section, we shall return to Example 2 and use the proposition to see that $D_{\mathbb{K}} = -108$ is the correct choice.

Before stating Proposition 5.2, let us interpolate a generalization of the computation of $D(\xi)$ that preceded the above examples. Suppose that $\Gamma = (\alpha_1, \dots, \alpha_n)$ is any ordered $\mathbb{Q}$ basis of $\mathbb{K}$ lying in R. Let $B = [B_{ij}]$ be the matrix whose determinant is the discriminant of Γ. Then we have

$$B_{ij} = \operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} A_{ik}(A^t)_{kj},$$

where $A = [A_{ij}]$ is the matrix with $A_{ij} = \sigma_j(\alpha_i)$, and it follows that

$$D(\Gamma) = \big(\det[\sigma_j(\alpha_i)]\big)^2.$$

This formula can be useful for computing $D(\Gamma)$ when the conjugates of the α_i are readily available.

Proposition 5.2. Let $\Gamma = (v_1, \dots, v_n)$ be an ordered $\mathbb{Q}$ basis of $\mathbb{K}$ lying in R. If the $\mathbb{Z}$ span $\mathbb{Z}(\Gamma)$ of Γ is a proper subgroup of R, then there exists a prime number p such that p^2 divides $D(\Gamma)$ and such that some member

$$v'_k = p^{-1}(c_1v_1 + c_2v_2 + \cdots + c_{k-1}v_{k-1} + v_k)$$

of $\mathbb{K}$ lies in R with $1 \le k \le n$ and $0 \le c_j \le p-1$ for $j \le k-1$. If such an element v'_k is found, then $\Delta = (v_1, \dots, v_{k-1}, v'_k, v_{k+1}, \dots, v_n)$ has $\mathbb{Z}(\Delta)$ properly containing $\mathbb{Z}(\Gamma)$ with $D(\Delta) = p^{-2}D(\Gamma)$.

REMARKS. A finite computation is involved in finding p and k. On the one hand, for given p, at most $1+p+p^2+\cdots+p^{n-1}$ elements have to be checked for integrality. On the other hand, we in principle have to find the field polynomial of a certain element of $\mathbb{K}$ in each case and decide whether the coefficients are integers, and this computation may be lengthy. See Problem 2 at the end of the chapter for an easy example, Problem 16 for a harder example, and Problem 4b for a related computation.

PROOF. Let $\mathbb{Z}(\Gamma)$ be a proper subgroup of R, and put $m = |R/\mathbb{Z}(\Gamma)|$. Choose a $\mathbb{Z}$ basis $(w_1, \dots, w_n)$ of R, and write $v_i = \sum_{j=1}^n c_{ij}w_j$ with all $c_{ij} \in \mathbb{Z}$. We know that $|\det[c_{ij}]| = m$, and we let p be any prime divisor of m. Reducing the c_{ij} modulo p, we see that the matrix $[c_{ij}]$ is singular modulo p, and thus there exist integers $a_1, \dots, a_n$ not all divisible by p such that

$$\sum_{i=1}^n a_ic_{ij} \equiv 0 \bmod p \qquad \text{for } 1 \le j \le n.$$

Find k with $1 \le k \le n$ for which p divides all of $a_{k+1}, \dots, a_n$ but not a_k, and write $\sum_{i=1}^n a_ic_{ij} = pl_j$ for integers l_j. Then

$$\sum_{i=1}^k a_iv_i = \sum_{j=1}^n\sum_{i=1}^k a_ic_{ij}w_j = \sum_{j=1}^n \big(pl_j - \sum_{i=k+1}^n a_ic_{ij}\big)w_j,$$

and the integer in parentheses on the right side is a multiple of p. Therefore $r = \sum_{i=1}^k a_iv_i$ is exhibited as ps for some $s \in R$. Choose a' and d_k in $\mathbb{Z}$ with $a'a_k - d_kp = 1$, and choose c_i and d_i in $\mathbb{Z}$ for each i with $i \le k-1$ such that $0 \le c_i \le p-1$ and $a'a_i - pd_i = c_i$. Then the computation

$$pa's = a'r = \sum_{i=1}^k a'a_iv_i = \sum_{i=1}^{k-1}(c_i+pd_i)v_i + (1+pd_k)v_k = \sum_{i=1}^{k-1} c_iv_i + v_k + p\sum_{i=1}^k d_iv_i$$

shows that $p^{-1}\big(\sum_{i=1}^{k-1} c_iv_i + v_k\big) = a's - \sum_{i=1}^k d_iv_i$ lies in R. □

Proposition 5.1 shows that any primitive element ξ of $\mathbb{K}$ that lies in R has the property that $D(\xi)/D_{\mathbb{K}}$ is the square of a nonzero integer, and we write this quotient as $J(\xi)^2$ with $J(\xi) > 0$. One might hope that although some particular choice of ξ fails to have $J(\xi) = 1$, some other choice may be found for which equality holds. We shall see in Section 4 that for a class of integers m, $\mathbb{Q}(\sqrt[3]{m})$ has such an element ξ if and only if a certain nontrivial Diophantine equation in two variables has a solution. Both cases arise: for $m = 2$, such a ξ exists, while for $m = 175$, no such ξ exists.

But matters can be worse than this for a general $\mathbb{K}$. The quotient $J(\xi)^2 = D(\xi)/D_{\mathbb{K}}$ for a primitive element ξ of $\mathbb{K}$ lying in R is sometimes called the **index** of ξ. One might hope at least that each prime not dividing $D_{\mathbb{K}}$ fails to divide the index $J(\xi)^2$ for some ξ. However, Dedekind showed that there exist number fields $\mathbb{K}$ and primes p that are **common index divisors**[7] in the sense that p divides $J(\xi)$ for every primitive element ξ of $\mathbb{K}$ lying in R. Specifically he showed that $p = 2$ is such a prime when $\mathbb{K}$ is obtained by adjoining to $\mathbb{Q}$ a root of $X^3 + X^2 - 2X + 8$; here $D_{\mathbb{K}} = -503$. We shall study this example further in Section 4.

Let us now specialize our considerations from general additive subgroups of the form $\mathbb{Z}(\Gamma)$ to those that are ideals in R.

Proposition 5.3. If I is a nonzero ideal in R, then

(a) I contains a positive k in $\mathbb{Z}$ and
(b) I additively is of the form $I = \mathbb{Z}(\Gamma)$ for some $\mathbb{Q}$ basis Γ of $\mathbb{K}$ whose members lie in R.

Consequently R/I is a finite ring and satisfies $|R/I|^2 = D(\Gamma)/D_{\mathbb{K}}$.

PROOF. Let r be a nonzero member of I, and let $P(X)$ be the field polynomial of r. Then $P(X)$ is of the form $P(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X + (-1)^n N_{\mathbb{K}/\mathbb{Q}}(r)$, has integers for coefficients, and has r as one of its roots. Consequently the formula

$$(-1)^{n+1}N_{\mathbb{K}/\mathbb{Q}}(r) = r(r^{n-1} + a_{n-1}r^{n-2} + \cdots + a_1)$$

shows that the nonzero integer $N_{\mathbb{K}/\mathbb{Q}}(r)$ is the product of r by a member of R and hence lies in I. This proves (a) with $k = |N_{\mathbb{K}/\mathbb{Q}}(r)|$.

The ideal I additively is a subgroup of R and is thus free abelian of rank at most n. By (a), the integer $k = |N_{\mathbb{K}/\mathbb{Q}}(r)|$ has the property that $kR \subseteq I \subseteq R$. Since R/kR has k^n elements, R/I is finite. Therefore I has rank n as an additive group and must be of the asserted form $\mathbb{Z}(\Gamma)$. This proves (b). The formula $|R/I|^2 = D(\Gamma)/D_{\mathbb{K}}$ is immediate from Proposition 5.1. □

[7] Terminology varies for this notion. Such primes p are more usually called **common inessential discriminant divisors** or **essential discriminant divisors**. The very fact that these two more usual names appear to contradict each other is sufficient reason to avoid using either name.

The **absolute norm** $N(I)$ of a nonzero ideal I of R is defined to be $N(I) = |R/I|$. This is necessarily a positive integer by Proposition 5.3. To be able to work with this notion, we shall make use of the unique factorization of ideals of R as given in Theorem 8.55 of *Basic Algebra*. That theorem says that such an ideal I has a factorization of the form $\prod_{j=1}^{l} P_j^{e_j}$, where the P_j are distinct prime ideals of R, and that this factorization is unique except for the order of the factors.

Proposition 5.4. The absolute norms of nonzero ideals of R have the following properties:

(a) $N(R) = 1$.

(b) If $I \subseteq J$ are nonzero ideals in R, then $N(J)$ divides $N(I)$, and $I = J$ if and only if $N(J) = N(I)$.

(c) If I and J are nonzero ideals in R, then $N(IJ) = N(I)N(J)$.

(d) If (α) is a nonzero principal ideal in R, then $N((\alpha)) = |N_{\mathbb{K}/\mathbb{Q}}(\alpha)|$.

PROOF. Conclusion (a) is immediate, and so is most of (b). If $I \subseteq J$ and $N(J) = N(I)$, then the First Isomorphism Theorem for abelian groups yields $(R/I)\big/(J/I) \cong R/J$, and it follows that $N(I)\big/|J/I| = N(J)$. Since $N(I)$ and $N(J)$ are finite, $N(I) = N(J)$ if and only if $|J/I| = 1$, i.e., if and only if $I = J$.

For (c), we begin with the special case that I and J are powers of a nonzero prime ideal P. Inductively it is enough to show that $N(P^k) = N(P)N(P^{k-1})$ for $k \geq 1$. Since $(R/P^k)\big/(P^{k-1}/P^k) \cong R/P^{k-1}$ as abelian groups, it is enough to show that

$$|P^{k-1}/P^k| = |R/P|. \tag{$*$}$$

The ring R operates on the ideal P^{k-1}, carrying P^k into itself, and P carries P^{k-1} into P^k. Thus P^{k-1}/P^k is a unital module for the ring R/P, which is a field because P is maximal. Hence P^{k-1}/P^k is a vector space over R/P. Corollary 8.60 of *Basic Algebra* shows that this vector space is 1-dimensional, and then $(*)$ is immediate.

For the general case in (c), Corollary 8.63 of *Basic Algebra* shows that if $I = \prod_{j=1}^{l} P_j^{e_j}$ is the unique factorization of the nonzero ideal I as the product of positive powers of distinct prime ideals P_j, then $R/I \cong \prod_{j=1}^{l} R/P_j^{e_j}$. Hence $N(I) = \prod_{j=1}^{l} N(P_j^{e_j})$. Because of the special case that is already proved, $N(I) = \prod_{j=1}^{l} N(P_j)^{e_j}$. Then (c) follows in the general case.

For (d), if $\Gamma = (u_1, \dots, u_n)$ is an ordered $\mathbb{Z}$ basis of R, then the tuple $\alpha\Gamma = (\alpha u_1, \dots, \alpha u_n)$ is an ordered $\mathbb{Z}$ basis of (α), and we know that $N((\alpha)) = |R/(\alpha)| = |\mathbb{Z}(\Gamma)/\mathbb{Z}(\alpha\Gamma)| = \left|\det\begin{pmatrix} I \\ \Gamma,\alpha\Gamma \end{pmatrix}\right|$. But $\begin{pmatrix} I \\ \Gamma,\alpha\Gamma \end{pmatrix}$ is just the matrix of the $\mathbb{Q}$ linear map left-by-α in the $\mathbb{Q}$ basis Γ, and the determinant of this linear map is $N_{\mathbb{K}/\mathbb{Q}}(\alpha)$ by definition of the norm of an element. □

EXAMPLE 2 OF $D(\xi)$, CONTINUED. For $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$, we have seen that the discriminant of the $\mathbb{K}$ basis $\Gamma(\sqrt[3]{2})$ is $D(\sqrt[3]{2}) = -3^3 2^2$. We are going to show that $(1, \sqrt[3]{2}, \sqrt[3]{4})$ is a $\mathbb{Z}$ basis of R, and then it follows that the field discriminant of $\mathbb{K}$ is $D_{\mathbb{K}} = -3^3 2^2$. We apply Proposition 5.2. The only primes that need testing in that proposition are the ones dividing $D(\sqrt[3]{2})$, and thus we consider $p = 2$ and $p = 3$. We want to see that no expression $p^{-1}(1)$ or $p^{-1}(c_1 + \sqrt[3]{2})$ or $p^{-1}(c_1 + c_2\sqrt[3]{2} + \sqrt[3]{4})$ is an algebraic integer for some coefficients c_0 and c_1 between 0 and $p - 1$. We can discard $p^{-1}(1)$ because the only rational numbers that are algebraic integers are the members of $\mathbb{Z}$. If the field polynomial over $\mathbb{Q}$ of some ξ in $\mathbb{K}$ is $X^3 + a_2X^2 + a_1X + a_0$, then the field polynomial of $p^{-1}\xi$ is $X^3 + p^{-1}a_2X^2 + p^{-2}a_1X + p^{-3}a_0$. So the question of integrality is one of divisibility of the coefficients of the field polynomials of certain algebraic integers ξ by suitable powers of p. These coefficients, up to sign, are the values of the elementary symmetric polynomials on the three conjugates of ξ.

In the case at hand, only the coefficient a_0 is needed. That is, it is enough to see that the norm of ξ is never divisible by 8 or 27 for ξ equal to $c_1 + \sqrt[3]{2}$ or $c_1 + c_2\sqrt[3]{2} + \sqrt[3]{4}$ as above. Let us write $\xi = c_1 + c_2\theta + c_3\theta^2$ with $\theta = \sqrt[3]{2}$ and with c_1, c_2, c_3 in $\mathbb{Z}$. Then $a_0 = -N_{\mathbb{K}/\mathbb{Q}}(\xi)$, and the norm is the product of the three conjugates of ξ. If $\omega = e^{2\pi i/3}$, we compute that

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}(\xi) &= (c_1 + c_2\theta + c_3\theta^2)(c_1 + c_2\theta\omega + c_3\theta^2\omega^2)(c_1 + c_2\theta\omega^2 + c_3\theta^2\omega) \\ &= (c_1^3 + 2c_2^3 + 4c_3^3) + 2c_1c_2c_3(2\omega + 3\omega^2 + \omega^4) \\ &= (c_1^3 + 2c_2^3 + 4c_3^3) - 6c_1c_2c_3. \end{aligned}$$

For $p = 2$, we consider this expression when c_1, c_2, c_3 are chosen from $\{0, 1\}$. To get divisibility by 8, we check this expression modulo 8. Each c_i^3 is c_i for $c_i \in \{0, 1\}$. Looking at the expression modulo 2, we see that c_1 must be even, i.e., $c_1 = 0$. Then 8 must divide $2c_2^3 + 4c_3^3$, and we obtain $c_2 = c_3 = 0$, in contradiction to the formulas for the ξ's under consideration.

For $p = 3$, it is enough to consider this expression when c_1, c_2, c_3 are chosen from $\{-1, 0, +1\}$. Since each c_i has $|c_i| \leq 1$, we see that $|N_{\mathbb{K}/\mathbb{Q}}(\xi)| \leq 13$, and divisibility by 27 can occur only if $N_{\mathbb{K}/\mathbb{Q}}(\xi) = 0$, which we know entails $\xi = 0$. Thus no ξ meets the test of Proposition 5.2, and the conclusion is that $(1, \sqrt[2]{3}, \sqrt[3]{4})$ is a $\mathbb{Z}$ basis of R in $\mathbb{Q}(\sqrt[3]{2})$.

3. Dedekind Discriminant Theorem

The field discriminant plays a role in determining how a prime ideal (p) in $\mathbb{Z}$, p being a prime number, splits when one extends (p) to an ideal $(p)R$ in the ring R of algebraic integers in a number field $\mathbb{K}$ of degree n over $\mathbb{Q}$. In this situation, recall from Theorem 9.60 of *Basic Algebra* that the prime factorization of the ideal $(p)R$ in R is of the form $(p)R = \prod_{i=1}^{g} P_i^{e_i}$ with $\sum_{i=1}^{g} e_i f_i = n$; here $n = [\mathbb{K} : \mathbb{Q}]$, the P_i are distinct, and $f_i = \dim_{\mathbb{F}_p}(R/P_i)$. The integers e_i are called **ramification indices**, and the integers f_i are called **residue class degrees**. The extension $\mathbb{K}/\mathbb{Q}$ is said to be **ramified at** p, and the prime p of $\mathbb{Z}$ is said to **ramify in** $\mathbb{K}$, if some e_i is > 1 in this decomposition.[8]

Theorem 5.5 (Dedekind Discriminant Theorem). The prime p of $\mathbb{Z}$ ramifies in a number field $\mathbb{K}$ if and only if p divides the field discriminant $D_{\mathbb{K}}$ of $\mathbb{K}$.

In this chapter we shall prove this theorem only in a useful special case, namely in the case that p is not a common index divisor. Only finitely many primes can divide the index $J(\xi) = (D(\xi)/D_{\mathbb{K}})^{1/2}$ for a single primitive element ξ of $\mathbb{K}$ lying in R, and thus there are only finitely many common index divisors.[9] Consequently the special case that we are proving implies that only finitely many primes of $\mathbb{Z}$ ramify in $\mathbb{K}$.

The difficulty in proving Theorem 5.5 in full generality is that we lack sufficient tools for addressing questions by localization. At the end of this section, we shall make some comments about how one can proceed with further tools.

As we shall see later in this section, Theorem 5.5 for primes that are not common index divisors is an easy consequence of the following theorem.

Theorem 5.6 (Kummer's criterion). Let $\mathbb{K}$ be a number field, and let R be its ring of algebraic integers. Suppose that $F(X)$ is a monic irreducible polynomial in $\mathbb{Z}[X]$, that ξ is a root of $F(X)$ in $\mathbb{C}$, and that p is a prime number that does not divide the integer $J(\xi)$ such that $J(\xi)^2 = D(\xi)/D_{\mathbb{K}}$. Write $\overline{F}(X)$ for the reduction of $F(X)$ modulo p, let

$$\overline{F}(X) = \overline{F}_1(X)^{e_1} \cdots \overline{F}_g(X)^{e_g}$$

be the unique factorization of $\overline{F}(X)$ in $\mathbb{F}_p[X]$ into a product of powers of distinct irreducible monic polynomials, and let $f_i = \deg(\overline{F}_i)$. For each i with $1 \leq i \leq g$, select a monic polynomial $F_i(X)$ in $\mathbb{Z}[X]$ whose reduction modulo p is $\overline{F}_i(X)$, and let P_i be the ideal in R defined by

$$P_i = pR + F_i(\xi)R.$$

Then the P_i's are distinct prime ideals of R with $\dim_{\mathbb{F}_p}(R/P_i) = f_i$, and the unique factorization of $(p)R$ into prime ideals is

$$(p)R = P_1^{e_1} \cdots P_g^{e_g}.$$

[8] More generally "relative discriminants," which we have not defined, play a role in the splitting of prime ideals in passing from a general number field to a finite extension. The cited Theorem 9.60 applies in this more general situation as well. This more general topic will be discussed further in Problems 5–9 at the end of this chapter and very briefly in Chapter VI.

[9] In fact, it can be shown that every common index divisor is less than $[\mathbb{K} : \mathbb{Q}]$.

REMARKS. The additive group $\mathbb{Z}(\Gamma(\xi))$ generated by the powers of ξ through ξ^{n-1} is a ring, since ξ^n is an integral combination of the lower powers of ξ, and this ring has index $J(\xi)$ as a subring of R. We divide the proof into two parts. The first part will give a complete proof in the special case that the subring $\mathbb{Z}(\Gamma(\xi))$ is all of R, but we shall retain notation that distinguishes the subring from the whole ring in order to see how much of the proof works for the general case. After the first part we pause for a lemma that will be used to tie results for the subring to results for all of R, and then we return to apply the lemma and complete the proof of Theorem 5.6.

FIRST PART OF PROOF. Let P_i' be the ideal $p\mathbb{Z}[X] + F_i(X)\mathbb{Z}[X]$ in $\mathbb{Z}[X]$. The passage from $\mathbb{Z}[X]$ to the quotient $\mathbb{Z}[X]/P_i'$ can be achieved in two steps, first using the substitution homomorphism carrying $\mathbb{Z}$ to $\mathbb{F}_p$ and X to itself and then taking the quotient by the principal ideal $(\overline{F}_i(X))$. Since $\overline{F}_i(X)$ is irreducible in $\mathbb{F}_p[X]$, the quotient is a field and P_i' has to be prime. The number of elements in $\mathbb{Z}[X]/P_i'$ is p^{f_i} because $\deg(\overline{F}_i(X)) = f_i$. The ideals P_i' are distinct because the polynomials $\overline{F}_i(X)$ are distinct.

Meanwhile, the substitution homomorphism of $\mathbb{Z}[X]$ leaving $\mathbb{Z}$ fixed and carrying X to ξ is a ring homomorphism of $\mathbb{Z}[X]$ onto $\mathbb{Z}(\Gamma(\xi))$. Let P_i'' be the image of P_i' under this homomorphism, i.e., let $P_i'' = p\mathbb{Z}(\Gamma(\xi)) + F_i(\xi)\mathbb{Z}(\Gamma(\xi))$. This is an ideal. The composite ring homomorphism of $\mathbb{Z}[X]$ onto $\mathbb{Z}(\Gamma(\xi))/P_i''$ factors through to a ring homomorphism of $\mathbb{Z}[X]/P_i'$ onto $\mathbb{Z}(\Gamma(\xi))/P_i''$. Since the domain is a field and the identity maps to the identity, the homomorphism is one-one and the image is a field. Thus P_i'' is a prime ideal, the order of $\mathbb{Z}(\Gamma(\xi))/P_i''$ is p^{f_i}, and and P_i' is the complete inverse image of P_i''. Since the ideals P_i' can be recovered from the P_i'' and since the P_i' are distinct, the P_i'' are distinct.

The next step is to compare the ideals $\prod_{i=1}^g P_i^{e_i}$ and $(p)R$. We shall use the fact that the polynomial $\prod_{i=1}^g F_i(X)^{e_i} - F(X)$ in $\mathbb{Z}[X]$ has coefficients divisible by p and therefore lies in $p\mathbb{Z}[X]$. The computation

$$\begin{aligned}
\prod_{i=1}^g P_i^{e_i} &= \prod_{i=1}^g (pR + F_i(\xi)R)^{e_i} \\
&\subseteq pR + \prod_{i=1}^g F_i(\xi)^{e_i} R \\
&\subseteq pR + \Big(\prod_{i=1}^g F_i^{e_i} - F\Big)(\xi) \qquad \text{since } F(\xi) = 0 \\
&\subseteq pR + p\mathbb{Z}(\Gamma(\xi)) \qquad\qquad \text{since } \textstyle\prod_{i=1}^g F_i(X)^{e_i} - F(X) \text{ lies in } p\mathbb{Z}[X] \\
&= pR
\end{aligned}$$

shows that $\prod_{i=1}^g P_i^{e_i} \subseteq (p)R$. If we can show that $N\big(\prod_{i=1}^g P_i^{e_i}\big) = N((p)R)$, then Proposition 5.4b will allow us to conclude that $\prod_{i=1}^g P_i^{e_i} = (p)R$.

At this point let us specialize to the case that $\mathbb{Z}(\Gamma(\xi)) = R$ and see how to complete the proof. Under this assumption the definitions of P_i and P_i'' exactly match. What we have shown about the P_i'' thus says that the P_i are distinct prime ideals in R with $|R/P_i| = p^{f_i}$, hence with $\dim_{\mathbb{F}_p}(R/P_i) = f_i$. Use of Proposition 5.4 and the fact that $|\mathbb{Z}(\Gamma(\xi))/P_i''| = p^{f_i}$ gives $N\big(\prod_{i=1}^g P_i^{e_i}\big) = \prod_{i=1}^g N(P_i)^{e_i} = \prod_{i=1}^g p^{e_i f_i} = p^{\sum_{i=1}^g e_i f_i} = p^n$, the last equality holding because $\deg \overline{F}(X) = \sum_{i=1}^g e_i \deg \overline{F}_i(X)$. Since p^n equals $N((p)R)$, the desired equality of norms has been proved. This completes the proof of the theorem when $\mathbb{Z}(\Gamma(\xi)) = R$. □

We interrupt the general proof for the promised lemma. When we apply the lemma to finish the proof of Theorem 5.6, we shall take $A = \mathbb{Z}(\Gamma(\xi))$, $J = J(\xi)$, and $m = p$. The hypotheses of Theorem 5.6 show that the condition $\mathrm{GCD}(p, J(\xi)) = 1$ is satisfied.

Lemma 5.7. Suppose that A is an additive subgroup of finite index J in R and that $m \geq 1$ is an integer relatively prime to J. Then for each $r \in R$, there exists $a \in A$ with $r - a$ in mR.

PROOF. Let $\{u_1, \dots, u_n\}$ be a $\mathbb{Z}$ basis of R, and let $\{v_1, \dots, v_n\}$ be a $\mathbb{Z}$ basis of A. We can write $v_j = \sum_{i=1}^n c_{ij} u_i$ for an integer matrix $[c_{ij}]$ with $|\det[c_{ij}]| = J$. Let $r = \sum_{i=1}^n b_i u_i$ be given, and let the unknown $a \in A$ be expanded as $a = \sum_{i=1}^n a_j v_j$. Then $a = \sum_{i,j} a_j c_{ij} u_i$, and we are to arrange that the element

$$r - a = \sum_{i=1}^n \big(b_i - \sum_{j=1}^n c_{ij} a_j\big) u_i$$

is in mR. Thus we are to arrange that each coefficient of a u_i is divisible by m. Since $|\det[c_{ij}]| = J$ is relatively prime to m, the system of linear equations

$$\sum_{j=1}^n c_{ij} a_j \equiv b_i \bmod m$$

with unknowns $a_1, \dots, a_n$ has a nonsingular coefficient matrix modulo m and therefore has a solution. □

SECOND PART OF PROOF OF THEOREM 5.6. The ring homomorphism of $\mathbb{Z}(\Gamma(\xi))$ into $R/(pR + F_i(\xi)R)$ given by the composition of the inclusion followed by the quotient map descends to a ring homomorphism

$$\mathbb{Z}(\Gamma(\xi))\big/(p\mathbb{Z}(\Gamma(\xi)) + F_i(\xi)\mathbb{Z}(\Gamma(\xi))) \longrightarrow R/(pR + F_i(\xi)R). \qquad (*)$$

To see that $(*)$ is onto, let $r \in R$ be given. Take $A = pR$ in Lemma 5.7. Choose $z \in \mathbb{Z}(\Gamma(\xi))$ by the lemma in such a way that $z - r$ is in pR. Under the mapping

$(*)$, the coset of z goes to $r+(z-r)+pR+F_i(\xi)R = r+pR+F_i(\xi)R$, which is the coset of r. Hence $(*)$ is onto.

To see that $(*)$ is one-one, suppose that z maps to the 0 coset in the image. Then $z = pr_1 + F_i(\xi)r_2$ with r_1 and r_2 in R. Lemma 5.7 produces z_2 in $\mathbb{Z}(\Gamma(\xi))$ with $r_2 - z_2$ in pR. Hence the decomposition $z = pr_1 + F_i(\xi)(r_2 - z_2) + F_i(\xi)z_2$ exhibits z as in $pR + F_i(\xi)\mathbb{Z}(\Gamma(\xi))$. The product $F_i(\xi)\mathbb{Z}(\Gamma(\xi))$ is in $\mathbb{Z}(\Gamma(\xi))$, since $\mathbb{Z}(\Gamma(\xi))$ is a ring, and $(*)$ will be one-one if we show that $pR \cap \mathbb{Z}(\Gamma(\xi)) \subseteq p\mathbb{Z}(\Gamma(\xi))$. Let $\{u_i\}$ be a $\mathbb{Z}$ basis of R, let $\{v_j\}$ be a $\mathbb{Z}$ basis of $\mathbb{Z}(\Gamma(\xi))$, and write $v_j = \sum_i c_{ij}u_i$ for integers c_{ij}. If z' is in $pR \cap \mathbb{Z}(\Gamma(\xi))$, let us write $z' = \sum_j a_j v_j$. Substitution gives $z' = \sum_i \big(\sum_j a_j c_{ij}\big)u_i$. Since z' is in pR, we see that $\sum_j c_{ij}a_j \equiv 0 \bmod p$ for all i. The determinant of $[c_{ij}]$ is the index $J(\xi)$, up to sign, and this by assumption is not divisible by p. Therefore $a_j \equiv 0 \bmod p$ for all j, and it follows that z' is in $p\mathbb{Z}(\Gamma(\xi))$. Hence $(*)$ is one-one.

We have thus proved that $(*)$ is a ring isomorphism, i.e., that $\mathbb{Z}(\Gamma(\xi))/P_i'' \cong R/P_i$ for all i. The left side is a field, and hence P_i is a prime ideal. From the isomorphism we obtain $N(P_i) = |\mathbb{Z}(\Gamma(\xi))/P_i''| = p^{f_i}$. The computation $N\big(\prod_{i=1}^g P_i^{e_i}\big) = \prod_{i=1}^g N(P_i)^{e_i} = \prod_{i=1}^g p^{e_i f_i} = p^{\sum_{i=1}^g e_i f_i} = p^n$ in the last paragraph of the first part of the proof is now fully justified, and we can therefore conclude as in the special case that $\prod_{i=1}^g P_i^{e_i} = (p)R$.

Finally we have to prove that the ideals P_i are distinct. If indices $i \neq j$ are given, we know that $P_i'' \neq P_j''$. Choose z in P_i'' but not P_j''. Then z is in P_i because $P_i'' \subseteq P_i$, and z is not in P_j because the proof above that $(*)$ is one-one showed that $\mathbb{Z}(\Gamma(\xi)) \cap P_j \subseteq P_j''$. This completes the proof of Theorem 5.6. □

PROOF OF THEOREM 5.5 WHEN p IS NOT A COMMON INDEX DIVISOR. If p is not a common index divisor, we can choose a primitive ξ for $\mathbb{K}/\mathbb{Q}$ such that ξ is in R and p does not divide $J(\xi) = |R/\mathbb{Z}(\Gamma(\xi))|$. Let $F(X)$ be the field polynomial of ξ over $\mathbb{Q}$. Since $D(\xi) = J(\xi)^2 D_{\mathbb{K}}$, p divides $D_{\mathbb{K}}$ if and only if p divides $D(\xi)$. Thus p divides $D_{\mathbb{K}}$ if and only if p divides the discriminant of $F(X)$. This happens if and only if the discriminant of $\overline{F}(X)$ is $\equiv 0 \bmod p$, if and only if $\overline{F}(X)$ has a root of multiplicity > 1 in an algebraic closure of $\mathbb{F}_p$, if and only if the factorization over $\mathbb{F}_p$ of $\overline{F}(X)$ as a product of powers of distinct irreducible monic polynomials has some factor with exponent > 1. Applying Theorem 5.6, we see that this last condition is satisfied if and only if the unique factorization of the ideal $(p)R$ in R as $\prod_{i=1}^g P_i^{e_i}$ has some $e_i > 1$. □

As was mentioned earlier in this section, the difficulty in proving Theorem 5.5 in complete generality is that we lack sufficient tools for addressing questions by localization. The different prime numbers are interacting in some fashion, and the above proofs were unable to separate them. The usual technique of localization in our situation[10] suggests enlarging one or the other of the rings $\mathbb{Z}$ and R by adjoining inverses for all elements not in some prime ideal of interest. Then we piece together the results. If the localizing is done with respect to a prime ideal (p) of $\mathbb{Z}$, then $\mathbb{Z}$ gets replaced by the subring $S^{-1}\mathbb{Z}$ of all members of $\mathbb{Q}$ with no factors of p in the denominators, and R gets replaced by $S^{-1}R$. One advantage of this procedure is that $S^{-1}R$ is a principal ideal domain, whereas R is typically not such a domain.

Localization in that formulation does not by itself reveal a clear path to a proof of Theorem 5.5. Two additional ideas enter the argument to make a path seem natural; Dedekind succeeded without the second of them, and historically it is only with hindsight that one sees the benefit of the second idea. The first idea is to use a more fundamental object than the discriminant of $\mathbb{K}$, called the "relative different" of $\mathbb{K}/\mathbb{Q}$; this makes it possible to aim for a more precise description of the ramification indices when they are not equal to 1. The second idea is due to K. Hensel and involves forming a kind of completion of the localized rings; the ring $\mathbb{Z}$ gets replaced by the ring $\mathbb{Z}_p$ of "p-adic integers," and the field $\mathbb{Q}$ gets replaced by the field $\mathbb{Q}_p$ of "p-adic numbers." We return to these ideas in Chapter VI.

4. Cubic Number Fields as Examples

In treating examples of cubic fields, it will be convenient to have one further tool available for computing discriminants. Let $\mathbb{K}$ be a number field, let ξ be a primitive element of $\mathbb{K}/\mathbb{Q}$, and let $F(X)$ be its field polynomial over $\mathbb{Q}$. Let $\xi_i = \sigma_i(\xi)$ be the conjugates of ξ, and assume that $\xi_1 = \xi$. The conjugates are the roots of $F(X)$ in $\mathbb{C}$, and hence

$$F(X) = \prod_{i=1}^{n} (X - \xi_i).$$

The derivative is $F'(X) = \sum_{i=1}^{n} \prod_{j \neq i} (X - \xi_j)$, and therefore

$$F'(\xi) = \prod_{j=2}^{n} (\xi - \xi_j).$$

Observe that the form of the left side shows that this element lies in $\mathbb{K}$, and it lies in R if ξ lies in R. The **different** $\mathcal{D}(\xi)$ of the element ξ is defined to be this element of $\mathbb{K}$, namely[11]

[10] Localization was introduced in Section VIII.10 of *Basic Algebra*.

[11] The different of an element is related to the notion of relative different mentioned at the end of Section 3, but the nature of that relationship will not concern us at this time.

$$\mathcal{D}(\xi) = F'(\xi) = \prod_{j=2}^{n} (\xi - \xi_j).$$

Since $F'(X)$ has coefficients in $\mathbb{Q}$, the conjugates $\sigma_i(F'(\xi))$ of $F'(\xi)$ are the elements $F'(\sigma_i(\xi)) = F'(\xi_i)$ for $1 \leq i \leq n$. The formula for $F'(X)$ shows that $F'(\xi_i) = \prod_{j \neq i} (\xi_i - \xi_j)$. Therefore the norm of $\mathcal{D}(\xi)$ is

$$\begin{aligned} N_{\mathbb{K}/\mathbb{Q}}(\mathcal{D}(\xi)) = N_{\mathbb{K}/\mathbb{Q}}(F'(\xi)) &= \prod_{i=1}^{n} F'(\xi_i) = \prod_{i=1}^{n} \prod_{j \neq i} (\xi_i - \xi_j) \\ &= (-1)^{n(n-1)/2} \prod_{i<j} (\xi_i - \xi_j)^2 = (-1)^{n(n-1)/2} D(\xi). \end{aligned}$$

In other words, the norm of the different of ξ is, up to sign, equal to the discriminant of $\Gamma(\xi)$, which in turn equals the discriminant of the field polynomial of the primitive element ξ. The definitions of $\mathcal{D}(\xi)$ and $D(\xi)$ and the formula connecting them make sense if ξ is allowed to be any element of $\mathbb{K}$, primitive or not. Both $\mathcal{D}(\xi)$ and $D(\xi)$ have the property of being nonzero if and only if ξ is primitive.

EXAMPLE. For the field $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$, the different of $\xi = \sqrt[3]{2}$ is $3X^2\big|_{X=\sqrt[3]{2}} = 3\sqrt[3]{4}$, and the discriminant of $X^3 - 2$, up to the sign $(-1)^{3\cdot 2/2}$, is the norm of this, i.e.,

$$\begin{aligned} D(\sqrt[3]{2}) &= -(3\sqrt[3]{4})(3\sqrt[3]{4}\,\omega)(3\sqrt[3]{4}\,\omega^2), \qquad \text{where } \omega = e^{2\pi i/3}, \\ &= -3^3 2^2. \end{aligned}$$

Alternatively, the norm can be computed from a field polynomial. Specifically the norm of $3\sqrt[3]{4}$ is the determinant of left multiplication by this element when considered as a $\mathbb{Q}$ linear mapping of $\mathbb{K}$ into itself.

We saw already in Example 2 of Section 2 that $D(\sqrt[3]{2}) = -3^3 2^2$, but the earlier method of computation was longer. At the end of Section 2, we saw in addition that $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ is a $\mathbb{Z}$ basis of the ring of algebraic integers in the field $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2})$. The use of differents does not simplify the proof of this latter fact.

In this section we consider further examples of cubic extensions of $\mathbb{Q}$. The first such fields that we study are the **pure cubic** extensions $\mathbb{K} = \mathbb{Q}(\sqrt[3]{m})$, where m is any cube-free positive integer > 1. Already with these fields $\mathbb{K}$, we shall see that $D_{\mathbb{K}}$ is not necessarily equal to $\mathcal{D}(\xi)$ for some algebraic integer ξ. However, all these fields have no common index divisors. Then we examine Dedekind's example of a cubic number field for which 2 is a common index divisor.

The correspondence of cube-free integers $m > 1$ to fields $\mathbb{Q}(\sqrt[3]{m}\,)$ is many-to-one: if m is given and p is a prime dividing m, let $m' = m/p$ if p^2 divides m and $m' = mp$ if p^2 does not divide m; then $\mathbb{Q}(\sqrt[3]{m}\,) = \mathbb{Q}(\sqrt[3]{m'}\,)$. In analyzing $\mathbb{Q}(\sqrt[3]{m}\,)$, it will be convenient to normalize matters so as to resolve this ambiguity. We can write m uniquely as a product $m = ab^2$ for positive square-free integers a and b; these have $\mathrm{GCD}(a, b) = 1$, b^2 is the largest square dividing m, and a is given by $a = m/b^2$. Then m and $m' = a^2b$ lead to the same field.

Proposition 5.8. For a cube-free integer $m > 1$, let $\mathbb{K} = \mathbb{Q}(\sqrt[3]{m}\,)$, and let R be the ring of algebraic integers in $\mathbb{K}$. Write $m = ab^2$ for positive square-free integers a and b with $\mathrm{GCD}(a, b) = 1$, and define two members of R to be the real cube roots $\theta_1 = \sqrt[3]{ab^2}$ and $\theta_2 = \sqrt[3]{a^2b}$. Then a $\mathbb{Z}$ basis of R consists of

(a) $\{1, \theta_1, \theta_2\}$ if $a \not\equiv \pm b \bmod 9$, i.e., if m is of **Type I,**

(b) $\{\frac{1}{3}(1 \pm \theta_1 \pm \theta_2),\ \theta_1, \theta_2\}$ for exactly one choice of the pair of signs if $a \equiv \pm b \bmod 9$, i.e., if m is of **Type II**.

In the respective cases the field discriminant is given by

$$D_{\mathbb{K}} = \begin{cases} -27a^2b^2 & \text{if } m \text{ is of Type I,} \\ -3a^2b^2 & \text{if } m \text{ is of Type II.} \end{cases}$$

REMARKS. More precisely in Type II, the congruence $a \equiv \pm b \bmod 9$ implies that a and b are prime to 3. Choose signs $s = \pm 1$ and $t = \pm 1$ such that $sa \equiv 1 \bmod 3$ and $tb \equiv 1 \bmod 3$. Then the first member of the $\mathbb{Z}$ basis is to be $\frac{1}{3}(1 + s\theta_1 + t\theta_2)$. The smallest m leading to Type I is $m = 2$, and this case was examined in Example 2 in Section 2. The smallest m leading to Type II is $m = 10$, and then the first member of the asserted $\mathbb{Z}$ basis of R is $\frac{1}{3}(1 + \sqrt[3]{10} + \sqrt[3]{100}\,)$.

PROOF. Let $\omega = e^{2\pi i/3}$. The conjugates of θ_1 can be taken to be $\sigma_1(\theta_1) = \theta_1$, $\sigma_2(\theta_1) = \omega\theta_1$, and $\sigma_3(\theta_1) = \omega^2\theta_1$. Since $\theta_1^2 = b\theta_2$, we have $\sigma_i(\theta_2) = b^{-1}\sigma_i(\theta_1)^2$, and therefore $\sigma_1(\theta_2) = \theta_2$, $\sigma_2(\theta_2) = \omega^2\theta_2$, and $\sigma_3(\theta_2) = \omega\theta_2$. In view of the formula before Proposition 5.2, $D((1, \theta_1, \theta_2))$ is the square of

$$\det\begin{pmatrix} 1 & 1 & 1 \\ \theta_1 & \omega\theta_1 & \omega^2\theta_1 \\ \theta_2 & \omega^2\theta_2 & \omega\theta_2 \end{pmatrix},$$

and we calculate that $D((1, \theta_1, \theta_2)) = -27a^2b^2$.

Let us apply Proposition 5.2 to the triple $\{1, \theta_1, \theta_2\}$ of members of R. For each prime p dividing $27a^2b^2$, we are to check whether certain elements are integral. First suppose that p divides a but $p \neq 3$. It is enough to check the elements $p^{-1}(a_0 + \theta_1)$ or $p^{-1}(a_0 + a_1\theta_1 + \theta_2)$ for integrality when a_0 and a_1 are integers from 0 to $p - 1$. Form the extension $\mathbb{L} = \mathbb{K}(\sqrt[3]{p}\,) = \mathbb{Q}(\sqrt[3]{m},\ \sqrt[3]{p}\,)$ of $\mathbb{K}$, and let T be its ring of algebraic integers. The degree $[\mathbb{L}:\mathbb{Q}]$ equals 9 if $\mathbb{L}\neq\mathbb{K}$ and equals 3 if $\mathbb{L}=\mathbb{K}$. If $p^{-1}(a_0+\theta_1)$ is integral, then $a_0+p^{1/3}((a/p)b^2)^{1/3}=pr$ with $r\in R$, and hence $a_0=p^{1/3}c$ with $c\in T$. Applying $N_{\mathbb{L}/\mathbb{Q}}$ to both sides, we obtain $a_0^9=p^3N_{\mathbb{L}/\mathbb{Q}}(c)$ if $\mathbb{L}\neq\mathbb{K}$, and we obtain $a_0^3=pN_{\mathbb{K}/\mathbb{Q}}(c)$ if $\mathbb{L}=\mathbb{K}$. In either case, p divides a_0, and $a_0=0$. So $p^{-1}\theta_1$ is integral, in contradiction to the facts that the field polynomial for $\mathbb{K}$ of $p^{-1}\theta_1$ is $X^3-p^{-3}ab^2$ and that ab^2 contains p as a factor only once. We conclude that $p^{-1}(a_0+\theta_1)$ is not integral.

Similarly if the element $p^{-1}(a_0+a_1\theta_1+\theta_2)$ is integral, then we see that $a_0+a_1p^{1/3}((a/p)b^2)^{1/3}+p^{2/3}((a/p)^2b)^{1/3}=pr$ with $r\in R$. So $a_0=p^{1/3}c$ with $c\in T$, and the same argument as above shows that $a_0=0$. Hence $a_1((a/p)b^2)^{1/3}+p^{1/3}((a/p)^2b)^{1/3}=p^{2/3}r$, and $a_1((a/p)b^2)^{1/3}=p^{1/3}c'$ with $c'\in T$. Taking the norm gives $a_1^9((a/p)b^2)^3=p^3N_{\mathbb{L}/\mathbb{Q}}(c')$ if $\mathbb{L}\neq\mathbb{K}$ and $a_1^3(a/p)b^2=pN_{\mathbb{K}/\mathbb{Q}}(c')$ if $\mathbb{L}=\mathbb{K}$. Since a/p and b are prime to p, we conclude that p divides a_1 in both cases. Therefore $a_1=0$, and $p^{-1}\theta_2$ is integral. The field polynomial for $\mathbb{K}$ of $p^{-1}\theta_2$ is $X^3-p^{-3}a^2b$, and a^2b contains p as a factor only twice. We conclude that $p^{-1}(a_0+a_1\theta_1+\theta_2)$ is not integral.

This disposes of the prime divisors of a other than $p=3$, and we handle the prime divisors of b other than $p=3$ in the same way, except that we start from the ordered triple $(1,\theta_2,\theta_1)$ and therefore need check only $p^{-1}(a_0+\theta_2)$ and $p^{-1}(a_0+a_1\theta_2+\theta_1)$.

Now let us apply Proposition 5.2 to the ordered triple $(1,\theta_1,\theta_2)$ for the prime $p=3$, except that we allow coefficients 0 and ±1 instead of $0,1,2$. We check integrality for the elements $\frac{1}{3}(1\pm\theta_1)$, $\frac{1}{3}(1\pm\theta_2)$, $\frac{1}{3}(\theta_1\pm\theta_2)$, and $\frac{1}{3}(1\pm\theta_1\pm\theta_2)$ by checking whether the coefficients of their field polynomials are in $\mathbb{Z}$. For the first two, let φ be $\pm\theta_1$ or $\pm\theta_2$. The coefficient of the first-degree term in the field polynomial of $\frac{1}{3}(1+\varphi)$ is $\frac{1}{9}$ times

$$\begin{aligned}(1+\varphi)(1+\omega\varphi)&+(1+\varphi)(1+\omega^2\varphi)+(1+\omega\varphi)(1+\omega^2\varphi)\\&=(1+\varphi)(2+\omega\varphi+\omega^2\varphi)+(1+\omega\varphi)(1+\omega^2\varphi)\\&=(1+\varphi)(2-\varphi)+(1-\varphi+\varphi^2)=2+\varphi-\varphi^2+1-\varphi+\varphi^2=3,\end{aligned}$$

hence is $\frac{1}{3}$. This is not an integer, and thus $\frac{1}{3}(1+\varphi)$ is not in R. If $\varphi=\pm\theta_1$ and $\psi=\pm\theta_2$, then the corresponding computation for $\varphi+\psi$ is

$$\begin{aligned}(\varphi+\psi)(\omega\varphi+\omega^2\psi)&+(\varphi+\psi)(\omega^2\varphi+\omega\psi)+(\omega\varphi+\omega^2\psi)(\omega^2\varphi+\omega\psi)\\&=-(\varphi+\psi)(\varphi+\psi)+(\varphi^2-\varphi\psi+\psi^2)\\&=-3\varphi\psi=-3ab(\operatorname{sgn}\varphi)(\operatorname{sgn}\psi),\end{aligned}\qquad(*)$$

and $\frac{1}{9}$ of this is an integer only if 3 divides ab. In this case our hypotheses show that 9 does not divide ab. The constant term in the field polynomial of $\frac{1}{3}(\varphi+\psi)$ is $-\frac{1}{27}$ times

$$\begin{aligned}(\varphi+\psi)(\omega\varphi+\omega^2\psi)(\omega^2\varphi+\omega\psi) &= \varphi^3+\psi^3\\ &= (\operatorname{sgn}\varphi)ab^2+(\operatorname{sgn}\psi)a^2b\\ &= ab(b\operatorname{sgn}\varphi+a\operatorname{sgn}\psi). \qquad (**)\end{aligned}$$

When 3 divides ab exactly once, 3 divides $(**)$ exactly once, and hence $-\frac{1}{27}$ of $(**)$ is not an integer. Thus $\frac{1}{3}(\varphi+\psi)$ is not in R.

It remains to check $\frac{1}{3}(1+\varphi+\psi)$ with $\varphi=\pm\theta_1$ and $\psi=\pm\theta_2$. The coefficient of the second-degree term in the field polynomial of $\frac{1}{3}(1+\varphi+\psi)$ is equal to $-\frac{1}{3}\operatorname{Tr}(1+\varphi+\psi)=-1$ and is an integer; thus it imposes no restrictions. The first-degree term of the field polynomial is $\frac{1}{9}$ of

$$\begin{aligned}(1+\varphi+\psi)&(1+\omega\varphi+\omega^2\psi)+(1+\varphi+\psi)(1+\omega^2\varphi+\omega\psi)\\ &+(1+\omega\varphi+\omega^2\psi)(1+\omega^2\varphi+\omega\psi)\\ &=(1+\varphi+\psi)(2-\varphi-\psi)+(1-\varphi-\psi+\varphi^2-\varphi\psi+\psi^2)\\ &=3-3\varphi\psi=3(1-ab(\operatorname{sgn}\varphi)(\operatorname{sgn}\psi)), \qquad (\dagger)\end{aligned}$$

and $\frac{1}{9}$ of $(\dagger)$ is an integer if and only if $ab\equiv(\operatorname{sgn}\varphi)(\operatorname{sgn}\psi)$ mod 3. In particular, the proof is now complete unless $ab\equiv(\operatorname{sgn}\varphi)(\operatorname{sgn}\psi)$ mod 3. Thus we may assume from now on that neither a nor b is divisible by 3.

The constant term of the field polynomial of $\frac{1}{3}(1+\varphi+\psi)$ is $-\frac{1}{27}$ times

$$\begin{aligned}(1+\varphi+\psi)&(1+\omega\varphi+\omega^2\psi)(1+\omega^2\varphi+\omega\psi)\\ &=1+\operatorname{Tr}_{\mathbb{K}/\mathbb{Q}}(\varphi+\psi)+(*)+(**)\\ &=1+0-3ab(\operatorname{sgn}\varphi)(\operatorname{sgn}\psi)+ab(b\operatorname{sgn}\varphi+a\operatorname{sgn}\psi).\end{aligned}$$

Put $\alpha=a\operatorname{sgn}\varphi$ and $\beta=b\operatorname{sgn}\psi$, so that $1-3\alpha\beta+\alpha\beta(\alpha+\beta)$ is to be divisible by 27. Since neither β nor α is divisible by 3, we can define l mod 27 by the congruence $\beta=l\alpha$ mod 27. Substituting shows that $1-3l\alpha^2+l\alpha^2(\alpha+l\alpha)\equiv 0$ mod 27, hence that $l(l+1)\alpha^3\equiv 3l\alpha^2-1$ mod 27, which we can rewrite as

$$\alpha^3l^2+(\alpha^3-3\alpha^2)l+1\equiv 0 \bmod 27.$$

Completing the square in l allows us to write this congruence as

$$(l+\tfrac{1}{2}(1-3\alpha^{-1}))^2\equiv\tfrac{1}{4}(1-3\alpha^{-1})^2-\alpha^{-3} \bmod 27.$$

Factoring the right side, we obtain

$$(l+\tfrac{1}{2}(1-3\alpha^{-1}))^2\equiv\tfrac{1}{4}\alpha^{-4}[\alpha(\alpha-1)^2(\alpha-4)] \bmod 27. \qquad (\dagger\dagger)$$

If $\alpha \equiv 1 \bmod 3$, the expression in square brackets on the right side is $\equiv 0 \bmod 27$, and 0 is the square of 0 and ± 9. If $\alpha \equiv 2 \bmod 3$, then the expression in square brackets is a square if and only if $\alpha(\alpha - 4) \equiv c^2 \bmod 27$. Considering the congruence only modulo 3 gives $2(-2) \equiv c^2 \bmod 3$ and therefore $c^2 \equiv 2 \bmod 3$, which has no solutions. Thus $\alpha \equiv 2 \bmod 3$ leads to no solutions of (††). We can summarize by saying that the solutions of (††) are given by $\alpha \equiv 1 \bmod 3$ and

$$l + \tfrac{1}{2}(1 - 3\alpha^{-1}) \equiv 0 \bmod 9.$$

One checks that the values $\alpha \equiv 1, 4, 7 \bmod 9$ all lead to $l = 1$.

Let us summarize. Let s and t be signs $\pm$. Then $\frac{1}{3}(1 + s\theta_1 + t\theta_2)$ is integral if and only if both of the following conditions are satisfied:

(i) $sa \equiv tb \equiv 1 \bmod 3$,
(ii) $sa \equiv tb \bmod 9$.

When these conditions are satisfied, we are in Type II; otherwise we are in Type I. This completes the proof. □

In the setting of Type I in Proposition 5.8, let us form the discriminants of $\Gamma(\theta_1) = (1, \theta_1, \theta_1^2)$ and $\Gamma(\theta_2) = (1, \theta_2, \theta_2^2)$. Using the method of computation at the beginning of this section, we see that the differents in the two cases are $3\theta_1^2$ and $3\theta_2^2$. Therefore the discriminant of $\Gamma(\theta_1)$ is $D(\theta_1) = -N_{\mathbb{K}/\mathbb{Q}}(3\theta_1^2) = -3^3(\theta_1^2)^3 = -3^3(ab^2)^2 = -3^3a^2b^4$, and the discriminant of $\Gamma(\theta_2)$ similarly is $D(\theta_2) = -3^3a^4b^2$. The absolute value of the greatest common divisor of these two expressions is $3^3a^2b^2 = |D_{\mathbb{K}}|$, and therefore there are never any common index divisors in Type I.

On the other hand, there exist situations in Type I in which no primitive element ξ of $\mathbb{Q}(\sqrt[3]{m})$ lying in R has $\Gamma(\xi)$ as a $\mathbb{Z}$ basis. To prove this fact, we make use of the following proposition.

Proposition 5.9. For a pure cubic extension $\mathbb{K} = \mathbb{Q}(\sqrt[3]{ab^2})$ of Type I, an element $\xi = x + y\theta_1 + z\theta_2$ with $\mathbb{Z}$ coefficients has $D(\xi) = D_{\mathbb{K}}$ if and only if $y^3b - z^3a = \pm 1$.

PROOF. The matrix whose determinant is $D(\Gamma(\xi))$ is given by

$$M = \begin{pmatrix} 3 & \mathrm{Tr}(\xi) & \mathrm{Tr}(\xi^2) \\ \mathrm{Tr}(\xi) & \mathrm{Tr}(\xi^2) & \mathrm{Tr}(\xi^3) \\ \mathrm{Tr}(\xi^2) & \mathrm{Tr}(\xi^3) & \mathrm{Tr}(\xi^4) \end{pmatrix},$$

where Tr is short for $\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}$. The element $\theta_1^i\theta_2^j$ has conjugates $\theta_1^i\theta_2^j$, $\omega^{i+2j}\theta_1^i\theta_2^j$, and $\omega^{2i+j}\theta_1^i\theta_2^j$, where $\omega = e^{2\pi i/3}$. Thus

$$\mathrm{Tr}(\theta_1^i\theta_2^j) = (1 + \omega^{i+2j} + \omega^{2i+j})\theta_1^i\theta_2^j = (1 + \omega^{i+2j} + \omega^{2(i+2j)})\theta_1^i\theta_2^j.$$

This is 0 if $i + 2j$ is not divisible by 3 and is $3\theta_1^i\theta_2^j$ otherwise. We compute the trace of each power of ξ by applying the formula

$$\operatorname{Tr}(\xi^l) = \sum_{k=0}^{n} \tbinom{l}{k} x^{l-k} \operatorname{Tr}((y\theta_1 + z\theta_2)^k),$$

which comes from treating ξ as a binomial. The traces of the powers of $y\theta_1 + z\theta_2$ work out to be

$$\begin{aligned}
\tfrac{1}{3}\operatorname{Tr}(y\theta_1 + z\theta_2) &= 0,\\
\tfrac{1}{3}\operatorname{Tr}((y\theta_1 + z\theta_2)^2) &= 2yz\theta_1\theta_2 = ab(2yz),\\
\tfrac{1}{3}\operatorname{Tr}((y\theta_1 + z\theta_2)^3) &= ab(y^3b + z^3a),\\
\tfrac{1}{3}\operatorname{Tr}((y\theta_1 + z\theta_2)^4) &= (ab)^2 6y^2z^2.
\end{aligned}$$

Substituting, we find the following formulas for the trace of each power of ξ:

$$\begin{aligned}
\tfrac{1}{3}\operatorname{Tr}(\xi) &= x,\\
\tfrac{1}{3}\operatorname{Tr}(\xi^2) &= x^2 + 2(ab)yz,\\
\tfrac{1}{3}\operatorname{Tr}(\xi^3) &= x^3 + 3x(ab)2yz + (ab)(y^3b + z^3a),\\
\tfrac{1}{3}\operatorname{Tr}(\xi^4) &= x^4 + 6x^2(ab)2yz + 4x(ab)(y^3b + z^3a) + (ab)^2 6y^2z^2.
\end{aligned}$$

The matrix M is therefore of the form

$$\tfrac{1}{3}M = \begin{pmatrix} 1 & x & x^2 + A \\ x & x^2 + A & x^3 + B \\ x^2 + A & x^3 + B & x^4 + C \end{pmatrix},$$

where

$$\begin{aligned}
A &= 2(ab)yz,\\
B &= 3x(ab)2yz + (ab)(y^3b + z^3a),\\
C &= 6x^2(ab)2yz + 4x(ab)(y^3b + z^3a) + (ab)^2 6y^2z^2.
\end{aligned}$$

Expansion of $\det \tfrac{1}{3}M$ results in an expression that simplifies to

$$\det \tfrac{1}{3}M = AC + 2xAB - 3x^2A^2 - A^3 - B^2.$$

Thus we have only to substitute. The resulting expression simplifies greatly, and we obtain $\det \tfrac{1}{3}M = -(ab)^2(y^3b - z^3a)^2$. Consequently

$$D(\xi) = -3^3(ab)^2(y^3b - z^3a)^2.$$

Since Proposition 5.8 has shown that $D_{\mathbb{K}} = -3^3(ab)^2$, the result follows. □

Thus in order to give an example of an m for which no ξ has $D(\xi) = D_{\mathbb{K}}$, we have only to select a and b for which the Diophantine equation $y^3b - z^3a = 1$ in y, z has no solution. Choose $a = 7$ and $b = 5$, so that $m = ab^2 = 175$. To verify that the Diophantine equation has no solution, take the equation modulo 7 and then modulo 5, obtaining $5y^3 \equiv 1 \bmod 7$ and $-7z^3 \equiv 1 \bmod 5$. These congruences say that $y^3 \equiv 3 \bmod 7$ and $z^3 \equiv 2 \bmod 5$. The only cubes modulo 7 are ± 1, and thus the congruence for y has no solution.

We turn to the question of the splitting of prime ideals in pure cubic extensions $\mathbb{K} = \mathbb{Q}(\sqrt[3]{m}\,)$. In the notation of Proposition 5.8, we again write $m = ab^2$, and we shall assume that the extension is of Type I. We saw in Proposition 5.8 and the remarks afterward that $D_{\mathbb{K}}$ equals the greatest common divisor of $D(\sqrt[3]{ab^2}\,)$ and $D(\sqrt[3]{a^2b}\,)$. Therefore the splitting of every prime ideal (p) in $\mathbb{Z}$ is described by Theorem 5.6. We have only to sort out the details.

Proposition 5.10. Let $\mathbb{K} = \mathbb{Q}(\sqrt[3]{m}\,)$ be a pure cubic extension of Type I, and let R be its ring of algebraic integers. If p is a prime number, then the ideal $(p)R$ of R splits into prime ideals as follows:

(a) $(p)R = P_1P_2$ with $N(P_1) = p$ and $N(P_2) = p^2$ if $p \equiv -1 \bmod 3$ and p does not divide $D_{\mathbb{K}}$,

(b) $(p)R = P_1P_2P_3$ with P_1, P_2, P_3 distinct of norm p if $p \equiv 1 \bmod 3$, $x^3 \equiv m \bmod p$ is solvable in $\mathbb{F}_p$, and p does not divide $D_{\mathbb{K}}$,

(c) $(p)R$ is prime of norm p^3 if $p \equiv 1 \bmod 3$, $x^3 \equiv m \bmod p$ is not solvable in $\mathbb{F}_p$, and p does not divide $D_{\mathbb{K}}$,

(d) $(p)R = P^3$ with $N(P) = p$ if p divides $D_{\mathbb{K}}$.

PROOF. The prime divisors of $D_{\mathbb{K}}$ are 3 and the prime divisors of a and b. For all other primes Theorem 5.6 shows that all ramification indices are 1. Let p be a prime of the form $6k \pm 1$ not dividing $D_{\mathbb{K}}$. The multiplicative group $\mathbb{F}_p^\times$ of $\mathbb{F}_p$ is cyclic of order $p - 1$ and hence has order divisible by 3 if and only if $p = 6k + 1$. Thus there are three cube roots of 1 when $p = 6k + 1$ but only 1 when $p = 6k - 1$. In the latter case the cubing map is one-one onto from $\mathbb{F}_p^\times$ to itself. Thus $X^3 - m$ factors modulo p as the product of a first-degree factor and an irreducible second-degree factor if $p = 6k - 1$, and (a) follows for such primes from Theorem 5.6. If $p = 6k + 1$, then $X^3 - m$ either factors modulo p as the product of three first-degree factors or is irreducible, since 1 has three cube roots. Thus (b) and (c) follow for such primes from Theorem 5.6.

For $p = 2$ if m is odd, then $X^3 - m \equiv X^3 - 1 \equiv (X-1)(X^2 + X + 1) \bmod 2$, and we are in the situation of (a). This completes the discussion of primes that do not divide $D_{\mathbb{K}}$. If p divides m, then $X^3 - m \equiv X^3 \bmod p$ is the cube of a first-degree factor, and (d) follows in these cases. For $p = 3$ whether or not p divides m, we have $X^3 - m \equiv X^3 - m^3 \equiv (X - m)^3 \bmod 3$, and (d) follows in this case. □

We conclude this section by discussing Dedekind's example of a common index divisor. The field in question is again of degree 3 over $\mathbb{Q}$ but is not of the form $\mathbb{Q}(\sqrt[3]{m})$. Instead, the field is $\mathbb{K} = \mathbb{Q}(\xi)$, where ξ is a root of $F(X) = X^3 + X^2 - 2X + 8$. The polynomial $F(X)$ is irreducible over $\mathbb{Q}$ because Gauss's Lemma shows that its only possible linear factors are $X - k$ with k dividing 8 and because routine computation rules out each such linear factor. As usual, let R be the ring of algebraic integers in $\mathbb{K}$.

The different of ξ is $\mathcal{D}(\xi) = F'(\xi) = 3\xi^2+2\xi-2$, and the discriminant $D(\xi)$ therefore is given by $D(\xi) = -N_{\mathbb{K}/\mathbb{Q}}(3\xi^2+2\xi-2)$. We calculate this norm as the determinant of left multiplication by $3\xi^2 + 2\xi - 2$ on $\mathbb{K}$, using the ordered basis $(1, \xi, \xi^2)$. Since $\xi^3 = -\xi^2+2\xi-8$ and $\xi^4 = -\xi^3+2\xi^2-8\xi = 3\xi^2-10\xi+8$, we have

$$\begin{aligned}(3\xi^2 + 2\xi - 2)(1) &= -2 + 2\xi + 3\xi^2,\\ (3\xi^2 + 2\xi - 2)(\xi) &= -2\xi + 2\xi^2 + 3\xi^3 = -24 + 4\xi - \xi^2,\\ (3\xi^2 + 2\xi - 2)(\xi^2) &= -2\xi^2 + 2\xi^3 + 3\xi^4 = 8 - 26\xi + 5\xi^2.\end{aligned}$$

Thus

$$N_{\mathbb{K}/\mathbb{Q}}(3\xi^2 + 2\xi - 2) = \det\begin{pmatrix} -2 & -24 & 8\\ 2 & 4 & -26\\ 3 & -1 & 5\end{pmatrix} = 2^2 \cdot 503,$$

and $D(\xi) = -2^2 \cdot 503$. Thus either the index $J(\xi)$ of $\mathbb{Z}(\Gamma(\xi))$ in R is 1 with $D_{\mathbb{K}} = -2^2 \cdot 503$, or $J(\xi) = 2$ with $D_{\mathbb{K}} - 503$.

Problems 24–25 at the end of the chapter show that $\frac{1}{2}(\xi^2 + \xi)$ is in R and that consequently the correct choice is $J(\xi) = 2$ with $D_{\mathbb{K}} = -503$ and with $\{1, \xi, \frac{1}{2}(\xi^2 + \xi)\}$ as a $\mathbb{Z}$ basis of R. In fact, 2 divides $J(\eta)$ for every primitive element of $\mathbb{K}$ lying in R, and therefore 2 is a common index divisor in the sense of Section 2. One way to check this assertion would be to calculate $D(\eta)$ for every such η. The computation would be feasible because we can express η as a $\mathbb{Z}$ linear combination of the members of $\{1, \xi, \frac{1}{2}(\xi^2 + \xi)\}$ and calculate the field polynomial of η in the same way that $N_{\mathbb{K}/\mathbb{Q}}(\xi)$ was calculated above.

However, there is an easier way. Problem 28 at the end of the chapter shows that $(2)R$ splits as the product of three distinct prime ideals of R. If there were some η for which 2 did not divide $J(\eta)$, then Theorem 5.6 would show that the minimal polynomial of η when reduced modulo 2 splits as the product of three distinct first-degree factors. But $\mathbb{F}_2$ has only 2 elements, hence only two possible distinct linear factors to offer. Thus Theorem 5.6 must not be applicable to η and the prime 2, and we conclude that 2 divides $J(\eta)$. Going over this argument, we see that we have established the following more general result.

Proposition 5.11. Let $\mathbb{K}/\mathbb{Q}$ be a field extension of degree n, and let R be the ring of algebraic integers in $\mathbb{K}$. If p is a prime number with $2 \leq p \leq n-1$ such that $(p)R$ splits as the product of n distinct prime ideals of R, then p is a common index divisor for $\mathbb{K}$.

5. Dirichlet Unit Theorem

Let $\mathbb{K}$ be a number field of degree n over $\mathbb{Q}$, and let R be its ring of algebraic integers. We regard $\mathbb{K}$ as a subfield of $\mathbb{C}$. The **units** of $\mathbb{K}$ are understood to be the members of the group $R^\times$ of units of the ring R. As was observed in Section 2, there exist exactly n field mappings of $\mathbb{K}$ into $\mathbb{C}$, and we denote them by $\sigma_1, \dots, \sigma_n$; one of these is the inclusion of $\mathbb{K}$ into $\mathbb{C}$. If x is in $\mathbb{K}$, then the images $\sigma_1(x), \dots, \sigma_n(x)$ are called the **conjugates** of x.

In Section I.6 we studied the group of units in the quadratic case $n = 2$, and we found, particularly in the problems at the end of that chapter, that an understanding of this group was essential to working successfully on the number-theoretic problems studied in that chapter. When $n = 2$, we found that the qualitative nature of the group $R^\times$ depends on the sign of the field discriminant. The group turned out to be the finite subgroup of roots of unity in $\mathbb{K}$ if $D_{\mathbb{K}} < 0$, and it turned out to be isomorphic to the product of a copy of $\mathbb{Z}$ and a cyclic group of order 2 if $D_{\mathbb{K}} > 0$. The hard step in this analysis was constructing an element in the subgroup $\mathbb{Z}$ in the latter case.

Because of the importance of $R^\times$ in the quadratic case, we can expect that an understanding of $R^\times$ for our general number field $\mathbb{K}$ is important for higher-degree number-theoretic questions. In this section we shall obtain a structure theorem for $R^\times$ for general n analogous to the structure theorem for $n = 2$ mentioned in the previous paragraph. Such a theorem may not answer all important questions about $R^\times$, but it will be a good start.[12] The main theorem is Theorem 5.13 below, the Dirichlet Unit Theorem.

The units of R are the members ε of R with $N_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = \pm 1$. This simple fact is verified for general $\mathbb{K}$ in the same way that it was verified for quadratic $\mathbb{K}$ in Section I.6.

Any element ε of finite order in $R^\times$ is a complex number with $\varepsilon^k = 1$ for some k and hence lies on the unit circle of $\mathbb{C}$. Since such an element ε is a root of $X^k - 1$, all its conjugates $\sigma_j(\varepsilon)$ lie on the unit circle of $\mathbb{C}$. We shall prove the following proposition about these elements.

[12] For example, when $n = 2$, we defined the **fundamental unit** ε_1 for the case $D_{\mathbb{K}} > 0$ to be the least unit > 1, and the sign of $N_{\mathbb{K}/\mathbb{Q}}(\varepsilon_1)$ was a thorny question that we did not answer fully but that affected results in the problems at the end of the chapter.

Proposition 5.12. The subgroup of $R^\times$ of elements of finite order consists of all l^{th} roots of unity in $\mathbb{C}$, where l is an integer depending on $\mathbb{K}$ that is bounded when the degree $n = [\mathbb{K} : \mathbb{Q}]$ is bounded.

PROOF. We are to bound the integers k for which primitive k^{th} roots of unity occur in $\mathbb{K}$. Let k have prime decomposition $k = p_1^{m_1} \cdots p_r^{m_r}$. From Section IX.9 of *Basic Algebra*, we know that the cyclotomic polynomial $\Phi_k(X)$ is a monic irreducible member of $\mathbb{Z}[X]$ whose roots in $\mathbb{C}$ are exactly all primitive k^{th} roots of unity; moreover, the degree of $\Phi_k(X)$ is given by the Euler φ function:

$$\varphi(k) = k \prod_{p \text{ divides } k} \big(1 - \tfrac{1}{p}\big).$$

If primitive k^{th} roots of unity occur in $\mathbb{K}$, then $\varphi(k) \leq n$ because $\Phi_k(X)$ is irreducible over $\mathbb{Q}$, and hence $(p_1 - 1) \cdots (p_r - 1) \leq n$. Allowing $p_1 = 2$ possibly, we see that each factor $p_j - 1$ with $j > 1$ is at least 2, and thus $2^{r-1} \leq n$. So r is bounded as a function of n by $\log_2 2n$, and we obtain

$$\varphi(k) \geq k \prod_{\substack{\text{first } \log_2 2n \\ \text{primes}}} \big(1 - \tfrac{1}{2}\big) = 2^{-\log_2 2n} k = \tfrac{k}{2n}.$$

Consequently $k \leq 2n\varphi(k) \leq 2n^2$, as required. If $R^\times$ contains one primitive k^{th} root of unity in $\mathbb{C}$, then it contains them all, since the k^{th} roots of unity form a cyclic group and any primitive such root is a generator. The result follows. □

We shall use the field mappings $\sigma_j : \mathbb{K} \to \mathbb{C}$ for $1 \leq j \leq n$ to introduce useful "absolute values" on $\mathbb{K}$. The mappings σ_j are of two types:

(i) those carrying $\mathbb{K}$ into $\mathbb{R}$,

(ii) those carrying $\mathbb{K}$ into $\mathbb{C}$ but not into $\mathbb{R}$; these come in pairs σ and $\overline{\sigma}$, where $\overline{\sigma}$ denotes the composition of σ followed by complex conjugation.

Suppose that there are r_1 mappings σ_j of the first kind and that there are r_2 pairs of the second kind. Then $r_1 + 2r_2 = n$. Renumbering $\sigma_1, \ldots, \sigma_n$ if necessary, let us arrange that $\sigma_1, \ldots, \sigma_{r_1}$ are of the first kind, that $\sigma_{r_1+1}, \ldots, \sigma_n$ are of the second kind, and that $\sigma_{r_1+r_2+i} = \overline{\sigma}_{r_1+i}$ for $1 \leq i \leq r_2$. We introduce $r_1 + r_2$ **absolute values**[13] on $\mathbb{K}$ by the definition

$$\|x\|_s = |\sigma_s(x)| \qquad \text{for } 1 \leq s \leq r_1 + r_2,$$

where $|\cdot|$ denotes the usual absolute value function on $\mathbb{C}$. Then the function $\operatorname{Log} : \mathbb{K}^\times \to \mathbb{R}^{r_1+r_2}$ given by

$$\operatorname{Log}(\varepsilon) = (\log \|\varepsilon\|_1, \ldots, \log \|\varepsilon\|_{r_1+r_2})$$

[13] These are called **archimedean absolute values** of $\mathbb{K}$ in the general theory. Some authors refer to them as **archimedean valuations**.

is evidently a group homomorphism.

A **lattice** in a Euclidean space $\mathbb{R}^l$ is an additive subgroup $\mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_l$ such that $\{u_1, \dots, u_l\}$ is linearly independent over $\mathbb{R}$. Such a subgroup is discrete,[14] and the quotient is compact, by the Heine–Borel Theorem.

Theorem 5.13 (Dirichlet Unit Theorem). Let $\mathbb{K}$ be a number field of degree n with $r_1 + r_2$ absolute values, and let R be the ring of algebraic integers in $\mathbb{K}$. The kernel of the restriction to $R^\times$ of the function Log is the finite subgroup of roots of unity in $\mathbb{K}^\times$, and the image of this restriction of Log is a lattice in the vector subspace of elements $(x_1, \dots, x_{r_1+r_2})$ in $\mathbb{R}^{r_1+r_2}$ satisfying

$$x_1 + \cdots + x_{r_1} + 2x_{r_1+1} + \cdots + 2x_{r_1+r_2} = 0.$$

Consequently $R^\times$ is a finitely generated abelian group of rank $r_1 + r_2 - 1$.

EXAMPLES.

(1) The theorem reduces when $n = 2$ to results known from Chapter I. Specifically if $\mathbb{K} = \mathbb{Q}(\sqrt{m}\,)$, then $m > 0$ makes $r_1 = 2$ and $r_2 = 0$, while $m < 0$ makes $r_1 = 0$ and $r_2 = 1$.

(2) For $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$, let $\omega = e^{2\pi i/3}$. The field mappings of $\mathbb{K}$ into $\mathbb{C}$ carry $\mathbb{K}$ into $\mathbb{R}$ or $\mathbb{R}\omega$ or $\mathbb{R}\omega^2$. Thus $r_1 = 1$ and $r_2 = 1$.

(3) The polynomial $F(X) = X^5 - 5X + 1$ in $\mathbb{Q}[X]$ was studied as an example in connection with Galois theory in Section IX.11 of *Basic Algebra*. The polynomial was shown to be irreducible over $\mathbb{Q}$ and to have three real roots and one pair of complex conjugate roots. For $\mathbb{K} = \mathbb{Q}[X]/(X^5 - 5X + 1)$, we therefore have $r_1 = 3$ and $r_2 = 1$. The primitive element ξ of $\mathbb{K}$ with $\xi^5 - 5\xi + 1 = 0$ lies in R; it is a nontrivial example of a member of $R^\times$ because $\xi(\xi^4 - 5) = -1$.

The proof of Theorem 5.13 will occupy the remainder of this section. We begin by clarifying in Lemma 5.14 the relationship between discrete subgroups and lattices in Euclidean space and by proving in Proposition 5.15 a weak version of Theorem 5.13 that addresses everything except the existence questions.

Lemma 5.14. A discrete subgroup of $\mathbb{R}^l$ is a free abelian group of rank $\leq l$ and is necessarily of the form $\mathbb{Z}u_1 \oplus \cdots \oplus \mathbb{Z}u_m$ for some set $\{u_1, \dots, u_m\}$ that is linearly independent over $\mathbb{R}$. The discrete subgroup is a lattice if and only if the rank is l.

[14] A **discrete** subset of $\mathbb{R}^l$ is a subset S such that every one-point subset of S is open when S is given the relative topology. See Lemma 5.14 below for a converse assertion.

PROOF. We begin by proving that any discrete subgroup of $\mathbb{R}^l$ is topologically closed. Let G be the subgroup, and choose by discreteness an open ball $V = \{x \in \mathbb{R}^l \bigm| |x| < \epsilon\}$ V about 0 with $V \cap G = \{0\}$. The open ball $U = \{x \in \mathbb{R}^l \bigm| |x| < \epsilon/2\}$ has the property that $U + U \subseteq V$. If G is not closed, let x_0 be a limit point of G that is not in G. Then the open ball $x_0 - U$ about x_0 must contain a member g of G, and g cannot equal x_0. Write $x_0 - u = g$ with $u \in U$. Then $u = x_0 - g$ is a limit point of G that is not in G, and we can find $g' \neq 1$ in G such that g' is in $u + U$. But $u + U \subseteq U + U \subseteq V$, and so g' is in $G \cap V = \{0\}$, contradiction. We conclude that G contains all its limit points and is therefore closed.

From the fact that any discrete subgroup G of $\mathbb{R}^l$ is closed, let us see that any bounded subset of G is finite. It is enough to see that the intersection X of G with any (finite-radius) closed ball is finite. The set X is closed because G is closed, and it is therefore compact by the Heine–Borel Theorem. By discreteness, find for each $g \in G$ an open ball U_x centered at x that contains no member of G other than x. These open sets form an open cover of the compact set X, and a finite subcollection of them covers X. Each such open set contains only one member of X, and hence X is finite.

Returning to the statement of the lemma, we induct on the dimension of the $\mathbb{R}$ linear span of the discrete subgroup, the base case being that the $\mathbb{R}$ linear span is 0. Let G be the discrete subgroup, and let $\{v_1, \dots, v_m\}$ in G be a maximal set that is linearly independent over $\mathbb{R}$. Let $G_0 = G \cap \big(\sum_{j=0}^{m-1} \mathbb{R}v_j\big)$. By induction we may assume that every $u \in G_0$ is a $\mathbb{Z}$ linear combination of $v_1, \dots, v_{m-1}$. Let S be the set of $\mathbb{R}$ linear combinations of $\{v_1, \dots, v_m\}$ of the form

$$S = \left\{ v = c_1v_1 + \cdots + c_mv_m \in G \;\middle|\; \begin{array}{l} 0 \le c_i < 1 \text{ for } 1 \le i \le m-1, \\ 0 \le c_m \le 1 \end{array} \right\}.$$

The set S is bounded, and we saw in the previous paragraph that any bounded subset of G is finite. So S is finite. Let v' be a member of S with the smallest positive coefficient for v_m, say

$$v' = a_1v_1 + \cdots + a_mv_m.$$

If v is any member of S and its coefficient c_m is not a multiple of a_m, then $v - jv'$ for a suitable integer j has m^{th} coefficient positive but less than a_m; by subtracting from $v - jv'$ a suitable $\mathbb{Z}$ linear combination v'' of $v_1, \dots, v_{m-1}$, we can make $v - jv' - v''$ be in S, and then we have a contradiction to the minimality of a_m. We conclude that c_m is always a multiple of a_m. Then $v - jv'$ is in G_0 for some integer j, and it follows that the $\mathbb{Z}$ linear combinations of $v_1, \dots, v_{m-1}, v'$ span G. This completes the induction and the proof of the first conclusion of the lemma. The second conclusion is an immediate consequence of the first. □

For the remainder of the section, we adopt the notation in the statement of Theorem 5.13, and we shall not repeat it in the statement of every intermediate result.

Proposition 5.15 (weak form of Dirichlet Unit Theorem). The kernel of the restriction to $R^\times$ of Log is the finite subgroup of roots of unity in $\mathbb{K}^\times$, and the image of this restriction of Log is a discrete additive subgroup in the vector subspace of elements $(x_1, \dots, x_{r_1+r_2})$ in $\mathbb{R}^{r_1+r_2}$ satisfying

$$x_1 + \cdots + x_{r_1} + 2x_{r_1+1} + \cdots + 2x_{r_1+r_2} = 0.$$

Consequently $R^\times$ is a finitely generated abelian group of rank $\leq r_1 + r_2 - 1$.

PROOF. For α in $R^\times$, we calculate that

$$\begin{aligned}\log\|\alpha\|_1 + \cdots + \log\|\alpha\|_{r_1} + 2\log\|\alpha\|_{r_1+1} + \cdots + 2\log\|\alpha\|_{r_1+r_2}&\\ = \log\big(|\sigma_1(\alpha)|\cdots|\sigma_{r_1}(\alpha)||\sigma_{r_1+1}(\alpha)|^2\cdots|\sigma_{r_1+r_2}(\alpha)|^2\big)&\\ = \log\big|\prod_{j=1}^n \sigma_j(\alpha)\big|&\\ = \log|N_{\mathbb{K}/\mathbb{Q}}(\alpha)| = \log 1 = 0.&\end{aligned}$$

Hence the image lies in the vector subspace in the statement of the proposition.

Fix a (large) positive number M, and consider the set E_M of all members α of $R^\times$ for which all coordinates of $\mathrm{Log}(\alpha)$ are $\leq M$ in absolute value. Then the field polynomials

$$\det\big(XI - (\text{left by }\alpha)\big) = \prod_{j=1}^n (X - \sigma_j(\alpha))$$

of such elements α have all coefficients bounded by some M' depending on M, since each $|\sigma_j(\alpha)|$ is of the form $\|\alpha\|_j$ and is $\leq e^M$. Such a field polynomial is equal to $g(X)^r$, where $g(X)$ is the minimal polynomial of α and r is given by $r\deg(g(X)) = n$. Since α is in R, the coefficients of $g(X)$ are integers, and hence so are the coefficients of the corresponding field polynomial. There are only finitely many members of $\mathbb{Z}[X]$ of degree n whose coefficients are in a given bounded set, and hence there are only finitely many α's in E_M.

It follows that the image subgroup is discrete. Taking $M = 0$, we see also that the kernel of the restriction of Log to $R^\times$ is finite. Hence every element of this kernel has finite order and is therefore a root of unity. □

We come to the proof of Theorem 5.13. For quadratic extensions of $\mathbb{Q}$, which were handled in Section I.6, the crucial question of existence was addressed by means of an approximation result (Lemma 1.15) for irrational numbers. That result did not immediately establish the existence of units of infinite order, but it was applied infinitely many times in the course of proving Proposition 1.16, and the total effect was to produce a unit of infinite order.

We do something similar in general. In place of the approximation result in Lemma 1.15, we shall use a result known as the Minkowski Lattice-Point Theorem, which asserts the existence of lattice points in certain compact convex sets in Euclidean space. This result appears as Theorem 5.16 below. As was true in the quadratic case, it is not just a single application of this theorem that produces the desired units, but an infinite sequence of applications of it. The details will be more complicated here than in the quadratic case. Before describing how the argument is to proceed, let us establish the Minkowski theorem.

Let $\{v_1, \dots, v_m\}$ be an $\mathbb{R}$ basis of $\mathbb{R}^m$, and let $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_m$ be the corresponding lattice. The **fundamental parallelotope** for L corresponding to this basis is the set

$$\big\{c_1 v_1 + \cdots + c_m v_m \,\big|\, 0 \leq c_j \leq 1 \text{ for } 1 \leq j \leq m\big\}.$$

The volume of this fundamental parallelotope is independent of the choice of the $\mathbb{Z}$ basis for L. In fact, any two such $\mathbb{Z}$ bases are carried from one to the other by an integer matrix of determinant ± 1, and any linear transformation from $\mathbb{R}^m$ to itself of determinant ± 1 is volume preserving. The one fundamental parallelotope is mapped to the other when the one basis is carried to the other, and hence the two fundamental parallelotopes have the same volume.

Theorem 5.16 (Minkowski Lattice-Point Theorem).[15] Let L be a lattice in $\mathbb{R}^m$, and let V_0 be the volume of a fundamental parallelotope. If E is any compact convex set in $\mathbb{R}^m$ containing 0, closed under negatives, and having volume$(E) \geq 2^m V_0$, then E contains a nonzero point of L.

REMARK. The constant 2^m in the statement is best possible, as is shown by taking L to be the standard lattice and E to be a cube oriented consistently with L, centered at 0, and having each side slightly less than 2. We need merely some constant, not the best possible one, in the application to Theorem 5.13, and the proof can be simplified a little for that purpose.[16] But the present theorem will be applied again in the next section, and this time the best possible constant yields the most useful information.

[15] The simple proof given here is due to H. Blichfeldt and is the standard one, so standard that Blichfeldt's name is sometimes attached to the theorem.

[16] In particular, the final paragraph of the proof can be omitted, and we can fix a value of M proportional to s in making the argument.

PROOF. Without loss of generality, L is the standard lattice of points with all coordinates in $\mathbb{Z}$, and V_0 is 1. Fix an arbitrarily small positive constant ϵ, and first assume that the given set E has $\text{volume}(E) \geq (2+\epsilon)^m V_0$. Arguing by contradiction, suppose that the only lattice point in E is 0. Since E is bounded, we can choose a number $s > 0$ in such a way that E is contained in the cube C_s centered at 0, oriented consistently with the lattice, and having side $2s$. Let us see that the sets $l + \frac{1}{2}E$ for $l \in L$ are disjoint. In fact, in obvious notation if $l_1 + \frac{1}{2}e_1 = l_2 + \frac{1}{2}e_2$ with $l_1 \neq l_2$, then $l_1 - l_2 = \frac{1}{2}(e_2 - e_1)$, and this is in E because e_2 and $-e_1$ are in E and E is convex. Thus the sets $l + \frac{1}{2}E$ are indeed disjoint.

Choose an integer M large enough to have $s/M < \epsilon$. Any lattice point l whose coordinates are all $\leq M$ in absolute value has $l + \frac{1}{2}E \subseteq C_{M+\frac{1}{2}s}$. Since the sets $l + \frac{1}{2}E$ for these l's are disjoint,

$$(2(M + \tfrac{1}{2}s))^m = \text{volume}(C_{M+\frac{1}{2}s}) \geq \sum_{\substack{\text{all } l \in L \text{ with} \\ \text{all coordinates } \leq M}} \text{volume}(l + \tfrac{1}{2}E)$$

$$\geq (2M)^m \text{volume}(\tfrac{1}{2}E) = M^m \text{volume}(E),$$

and therefore $\text{volume}(E) \leq (2+s/M)^m$, in contradiction to our extra assumption that $\text{volume}(E) \geq (2+\epsilon)^m$.

Now suppose that $\text{volume}(E) = 2^m$. For each $\epsilon > 0$, let E_ϵ be the dilate $(1 + \frac{1}{2}\epsilon)E$. The sets E_ϵ satisfy the extra assumption made in the previous part of the proof, and therefore E_ϵ contains a nonzero lattice point. Since E_1 is bounded, there are only finitely many possibilities for this nonzero lattice point for each $\epsilon \leq 1$. Thus we can find a sequence of ϵ's tending to 0 for which this lattice point is the same. The convexity of the sets E_ϵ, in combination with the fact that the sets contain 0, implies that the sets are nested, and therefore this lattice point lies in E_ϵ for all $\epsilon > 0$. Since E is compact, $E = \bigcap_{\epsilon > 0} E_\epsilon$, and therefore this lattice point lies in E. □

Let us describe the lattice to be used when the Minkowski Lattice-Point Theorem is applied to obtain the Dirichlet Unit Theorem. Let Ω be the real vector space $\Omega = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$, and let $|\omega|_s$ be the magnitude of the s^{th} component of $\omega \in \Omega$ for $1 \leq s \leq r_1 + r_2$. We introduce a homomorphism Φ of the additive group of $\mathbb{K}$ into the additive group of Ω given by

$$\Phi(x) = \big(\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)\big)$$

for $x \in \mathbb{K}$. We shall be mostly interested in the restriction of Φ to R, but the values on $\mathbb{K}$ will help a little with motivation when the Minkowski Lattice-Point Theorem is applied once again in the next section. Observe that our definitions make $\|x\|_s = |\sigma_s(x)| = |\Phi(x)|_s$ for $x \in \mathbb{K}$ and $1 \leq s \leq r_1 + r_2$.

Lemma 5.17. The image $\Phi(R)$ is a lattice in Ω.

PROOF. The homomorphism Φ is one-one on R because σ_1, being a field map, is one-one. Since R is a free abelian group of rank n and Φ is one-one, $\Phi(R)$ is free abelian of rank n. Lemma 5.14 therefore shows that it is sufficient to show that $\Phi(R)$ is discrete as an additive subgroup of Ω. It is enough to show that a bounded region of Ω contains only finitely many points of $\Phi(R)$.

The verification of this fact is similar to an argument in the proof of Proposition 5.15: A bound by some M on all $|\sigma_j(\alpha)|$ for certain elements $\alpha \in R$ implies that each field polynomial

$$\det\big(XI - (\text{left by } \alpha)\big) = \prod_{j=1}^{n} (X - \sigma_j(\alpha))$$

has all its coefficients bounded by some M' depending on M. These coefficients are integers when α is in R, and thus there are only finitely many such polynomials. Each polynomial has at most n distinct roots, and consequently only finitely many α's satisfy such a bound. □

We are now ready to prove Theorem 5.13, but we precede the proof by an outline. The proof has three steps to it:

(1) We apply the Minkowski Lattice-Point Theorem to the set $\Phi(R) \subseteq \Omega$, which we know is a lattice because of Lemma 5.17. For each s_0 with $1 \leq s_0 \leq r_1 + r_2$, let E_{s_0} be a set of ω's in Ω defined by the conditions that $|\omega|_s$ is to be small for $s \neq s_0$ and $|\omega|_{s_0}$ is allowed to be large—with the understanding that E_{s_0} is a bounded set and that E_{s_0} has volume $\geq 2^n V_0$, where V_0 is the volume of a fundamental parallelotope of $\Phi(R)$. Using a nonzero lattice point in $\Phi(R)$ obtained from applying Theorem 5.16 to E_{s_0} and squeezing E_{s_0} even more, we can obtain an infinite sequence of points α in R such that $|N_{\mathbb{K}/\mathbb{Q}}(\alpha)|$ remains bounded and such that the size of this norm is contributed to mostly by $\|\alpha\|_{s_0}$.

(2) Applying the same argument that was used for quadratic extensions of $\mathbb{Q}$ in the proof of Proposition 1.16, we obtain infinite sequences of units whose norm is contributed to mostly by $\|\cdot\|_{s_0}$. We can do this for $1 \leq s_0 \leq r_1 + r_2$.

(3) We pass to the Log map, proving and applying the following result from linear algebra: a real square matrix $[a_{ij}]$ with the property that $|a_{ii}| > \sum_{j\neq i} |a_{ij}|$ for all i is nonsingular. In the application of this result, we have $\log \|\varepsilon_{s_0}\|_{s_0} > 0$ for the $s_0{}^{\text{th}}$ constructed unit, $\log \|\varepsilon_{s_0}\|_s < 0$ for $s \neq s_0$, and an equality that we can write either as $\sum_{s=1}^{n} \log \|\varepsilon_{s_0}\|_s = 0$ or as $\sum_{s=1}^{r_1} \log \|\varepsilon_{s_0}\|_s + 2\sum_{s=r_1+1}^{r_1+r_2} \log \|\varepsilon_{s_0}\|_s = 0$. If we drop all terms corresponding to the $(r_1+r_2)^{\text{th}}$ unit, then we are in a situation for which the result from linear algebra immediately implies the theorem.

PROOF OF THEOREM 5.13. The proof is carried out in three steps.

Step 1. For fixed s_0 with $1 \le s_0 \le r_1 + r_2$, we construct an infinite sequence $\alpha_j^{(s_0)}$ in R with

(i) $|N_{\mathbb{K}/\mathbb{Q}}(\alpha_j^{(s_0)})| \le 2^n V_0$,

(ii) $\|\alpha_j^{(s_0)}\|_s$ tends to 0 for each $s \ne s_0$ as j tends to infinity,

(iii) $\|\alpha_j^{(s_0)}\|_{s_0}$ tends to infinity as j tends to infinity.

For the construction, form for each $j > 0$ the compact convex set in Ω closed under multiplication by -1 consisting of all ω such that

$$\begin{aligned} |\omega|_s &\le j^{-1} \qquad \text{for } s \ne s_0, \\ |\omega|_{s_0} &\le \begin{cases} 2^n j^{n-1} 2^{-r_1} \pi^{-r_2} V_0 & \text{if } 1 \le s_0 \le r_1, \\ (2^n j^{n-2} 2^{-r_1} \pi^{-r_2} V_0)^{1/2} & \text{if } r_1 + 1 \le s_0 \le r_1 + r_2. \end{cases} \end{aligned}$$

This set has volume

$$\begin{cases} (2j^{-1})^{r_1-1} \cdot 2(2^n j^{n-1} 2^{-r_1} \pi^{-r_2} V_0)(\pi j^{-2})^{r_2} = 2^n V_0 & \text{if } s_0 \le r_1, \\ (2j^{-1})^{r_1} (\pi j^{-2})^{r_2-1} \pi (2^n j^{n-2} 2^{-r_1} \pi^{-r_2} V_0) = 2^n V_0 & \text{if } s_0 > r_1. \end{cases}$$

Theorem 5.16 shows that the set contains a nonzero lattice point $\alpha_j^{(s_0)}$. Let us check that this point satisfies (i), (ii), and (iii). For (i), we have

$$\begin{aligned} |N_{\mathbb{K}/\mathbb{Q}}(\alpha_j^{(s_0)})| &= \Big(\prod_{j=1}^{r_1} \|\alpha_j^{(s_0)}\|_s\Big)\Big(\prod_{s=r_1+1}^{r_1+r_2} \|\alpha_j^{(s_0)}\|_s\Big)^2 \\ &\le \begin{cases} (j^{-1})^{r_1-1}(2^n j^{n-1} 2^{-r_1} \pi^{-r_2} V_0) j^{-2r_2} & \text{if } s_0 \le r_1 \\ (j^{-1})^{r_1} (j^{-2})^{r_2-1} (2^n j^{n-2} 2^{-r_1} \pi^{-r_2} V_0) & \text{if } s_0 > r_1 \end{cases} \\ &= 2^n V_0 2^{-r_1} \pi^{-r_2} \\ &\le 2^n V_0. \end{aligned}$$

Property (ii) is immediate from the inequality $\|\alpha_j^{(s_0)}\|_s \le j^{-1}$ for $s \ne s_0$. For (iii), we have

$$1 \le |N_{\mathbb{K}/\mathbb{Q}}(\alpha_j^{(s_0)})| = \Big(\prod_{j=1}^{r_1} \|\alpha_j^{(s_0)}\|_s\Big)\Big(\prod_{s=r_1+1}^{r_1+r_2} \|\alpha_j^{(s_0)}\|_s\Big)^2;$$

thus (ii) implies (iii).

Step 2. For fixed s_0 with $1 \le s_0 \le r_1 + r_2$, we construct an infinite sequence of units $\varepsilon_j^{(s_0)}$ such that

(ii′) $\|\varepsilon_j^{(s_0)}\|_s$ tends to 0 for each $s \ne s_0$ as j tends to infinity,

(iii′) $\|\varepsilon_j^{(s_0)}\|_{s_0}$ tends to infinity as j tends to infinity.

For the construction, we pass to a subsequence from Step 1, still denoting it by $\alpha_j^{(s_0)}$, such that $N_{\mathbb{K}/\mathbb{Q}}(\alpha_j^{(s_0)})$ is a constant integer, say M. Since $R/(M)$ is finite, we can pass to a further subsequence, still with no change in notation, such that all $\alpha_j^{(s_0)}$ lie in the same residue class[17] modulo the principal ideal (M) of R. Put

$$\varepsilon_j^{(s_0)} = \alpha_j^{(s_0)} \big/ \alpha_1^{(s_0)}.$$

Then $N_{\mathbb{K}/\mathbb{Q}}(\alpha_j^{(s_0)}) = N_{\mathbb{K}/\mathbb{Q}}(\alpha_1^{(s_0)})$, since $N_{\mathbb{K}/\mathbb{Q}}(\alpha_j^{(s_0)})$ is a constant integer, and $\frac{1}{M}(\alpha_j^{(s_0)} - \alpha_1^{(s_0)})$ is in R, since all $\alpha_j^{(s_0)}$ lie in the same residue class modulo (M). The computation

$$\varepsilon_j^{(s_0)} = 1 + \frac{\alpha_j^{(s_0)} - \alpha_1^{(s_0)}}{\alpha_1^{(s_0)}} = 1 + \frac{\alpha_j^{(s_0)} - \alpha_1^{(s_0)}}{M} \prod_{\sigma \neq 1} \sigma(\alpha_1^{(s_0)})$$

shows that $\varepsilon_j^{(s_0)}$ is an algebraic integer. Hence it is in R. We certainly have

$$N_{\mathbb{K}/\mathbb{Q}}(\varepsilon_j^{(s_0)}) = \frac{N_{\mathbb{K}/\mathbb{Q}}(\alpha_j^{(s_0)})}{N_{\mathbb{K}/\mathbb{Q}}(\alpha_1^{(s_0)})} = \frac{M}{M} = 1.$$

Therefore $\varepsilon_j^{(s_0)}$ is a unit. Also, the computation

$$\|\varepsilon_j^{(s_0)}\|_s = \frac{\|\alpha_j^{(s_0)}\|_s}{\|\alpha_1^{(s_0)}\|_s}$$

shows that (ii) and (iii) in Step 1 imply (ii′) and (iii′) here.

Step 3. For each s_0 with $1 \le s_0 \le r_1 + r_2$, choose j large enough for the unit $\varepsilon^{(s_0)} = \varepsilon_j^{(s_0)}$ in Step 2 to satisfy

(ii″) $\|\varepsilon^{(s_0)}\|_s < 1$ if $s \neq s_0$,

(iii″) $\|\varepsilon^{(s_0)}\|_{s_0} > 1$.

We assert that the vectors $\operatorname{Log}(\varepsilon^{(s_0)})$ for $1 \le s_0 \le r_1 + r_2 - 1$ are linearly independent over $\mathbb{R}$. Hence $\operatorname{Log}(R^\times)$ has rank $\ge r_1 + r_2 - 1$, and Proposition 5.15 therefore implies that $\operatorname{Log}(R^\times)$ has rank equal to $r_1 + r_2 - 1$.

To verify this assertion, form the square matrix $[a_{ij}]$ of size $r_1 + r_2$ given by

$$a_{ij} = \begin{cases} \log \|\varepsilon^{(i)}\|_j & \text{if } 1 \le j \le r_1, \\ 2 \log \|\varepsilon^{(i)}\|_j & \text{if } r_1 + 1 \le j \le r_1 + r_2. \end{cases}$$

[17] This conclusion uses a result known as the **Dirichlet pigeonhole principle** or the **Dirichlet box principle**.

Then $a_{ii} > 0$ for each i by (iii$''$), $a_{ij} < 0$ for $i \neq j$ by (ii$''$), and $\sum_j a_{ij} = 0$ for each i because $N_{\mathbb{K}/\mathbb{Q}}(\varepsilon^{(i)}) = 1$. Let $[b_{ij}]$ be the upper left block of $[a_{ij}]$ of size $r_1 + r_2 - 1$. For each i, we then have $b_{ii} > 0$ and $\sum_{j \text{ with } j \neq i} |b_{ij}| < b_{ii}$. Let us prove that the matrix $[b_{ij}]$ is nonsingular. Assuming the contrary, let $[c_j]$ be a nonzero column vector with

$$\sum_j b_{ij} c_j = 0 \qquad \text{for all } i. \tag{$*$}$$

If i_0 is an index such that $|c_{i_0}| \geq |c_j|$ for all j, then setting $i = i_0$ leads to the strict inequality

$$|c_{i_0} b_{i_0 i_0}| = |c_{i_0}| b_{i_0 i_0} > |c_{i_0}| \sum_{j \neq i_0} |b_{i_0 j}| \geq \sum_{j \neq i_0} |b_{i_0 j} c_j| \geq \Big| \sum_{j \neq i_0} b_{i_0 j} c_j \Big|,$$

which contradicts $(*)$. Thus $[b_{ij}]$ is nonsingular.

We conclude that $[b_{ij}]$ has rank $r_1 + r_2 - 1$. Thus its rows are linearly independent, and the first $r_1 + r_2 - 1$ rows of $[a_{ij}]$ must be linearly independent. Therefore the vectors

$$\big(\log \|\varepsilon^{(s_0)}\|_1, \dots, \log \|\varepsilon^{(s_0)}\|_{r_1}, 2\log \|\varepsilon^{(s_0)}\|_{r_1+1}, \dots, 2\log \|\varepsilon^{(s_0)}\|_{r_1+r_2}\big),$$

indexed by s_0 for $1 \leq s_0 \leq r_1 + r_2 - 1$, are linearly independent in $\mathbb{R}^{r_1+r_2}$. In other words, the vectors $\operatorname{Log}(\varepsilon^{(s_0)})$ are linearly independent for $1 \leq s_0 \leq r_1 + r_2 - 1$. □

6. Finiteness of the Class Number

As in Section 5, let $\mathbb{K}$ be a number field of degree n over $\mathbb{Q}$, and let R be its ring of algebraic integers. Let $\sigma_1, \dots, \sigma_n$ be the distinct field maps of $\mathbb{K}$ into $\mathbb{C}$, and assume that the first r_1 of them have image in $\mathbb{R}$ and the remaining ones come in conjugate pairs with $\sigma_{r_1+r_2+k} = \overline{\sigma}_{r_1+k}$ for $1 \leq k \leq r_2$.

As in Section I.7, where we treated the case of quadratic extensions, we define two nonzero ideals I and J of R to be **equivalent** if $(r)I = (s)J$ for suitable nonzero elements r and s of R. The same argument as given in that section shows that the result is an equivalence relation. The principal ideals form a single equivalence class.[18]

[18] Section I.7 worked also with a notion of strict equivalence of ideals, but we shall not attempt to extend strict equivalence to the present setting.

Proposition 5.18. Multiplication of nonzero ideals in R descends to a well-defined multiplication of equivalence classes of ideals, and the resulting multiplication makes the set of equivalence classes into an abelian group. The identity element of this group is the class of principal ideals.

REMARKS. The proofs of this result and of Theorem 5.19 below will use the following fact proved in Problems 48–53 of Chapter VIII of *Basic Algebra*: if I is any nonzero ideal in R and if I^{-1} is defined by $I^{-1} = \{x \in \mathbb{K} \mid xI \subseteq R\}$, then $I^{-1}I = R$ and there exists $r \in R$ with rI^{-1} equal to an ideal of R. This fact can be made to look more beautiful by introducing the notion of "fractional ideal," but we shall not carry out that step at this time.[19]

PROOF. If I is a nonzero ideal, let $[I]$ denote its equivalence class, and define $[I][J] = [IJ]$. Suppose that $(r)I = (s)I'$ exhibits an equivalence. Then the equality $(s)I'J = (r)IJ$ shows that $[I'J] = [IJ]$. A similar argument applies in the J variable, and therefore multiplication of classes is well defined. It is immediate that multiplication of classes is associative and commutative and also that the class of principal ideals is an identity. If a class $[I]$ is given, let I^{-1} be as in the remarks above, and choose a nonzero $r \in R$ such that $rI^{-1} = J$ is an ideal in R. Multiplying by J gives $(r) = r(I^{-1}I) = (rI^{-1})I = JI$, and thus $[J][I]$ is the class of the principal ideals. So $[I]$ has an inverse. □

The group of equivalence classes of nonzero ideals as in Proposition 5.18 is called the **ideal class group** of $\mathbb{K}$. Its order is called the **class number** of $\mathbb{K}$ and will be denoted by $h_{\mathbb{K}}$. The main theorem of this section is as follows.

Theorem 5.19. The class number $h_{\mathbb{K}}$ of any number field is finite.

As we shall see in a moment, it is not too difficult at this stage to prove this finiteness. However, $h_{\mathbb{K}}$ is an important invariant of a number field that determines whether R is a principal ideal domain, that occurs in various limit formulas in the subject, and that occurs also in dimension formulas connected with "Hilbert class fields." It is therefore of considerable interest to be able to compute $h_{\mathbb{K}}$ in specific examples. For quadratic fields this computation can be carried out by the techniques of Chapter I because of the close connection between ideal classes and proper equivalence classes of binary quadratic forms. But no comparable theory is available as an aid in computation for number fields of degree greater than 2. As we shall see, the relatively easy proof of Theorem 5.19 that we give in a moment does not offer any helpful clues about the value of $h_{\mathbb{K}}$. The main

[19] The result of the beautification is that the fractional ideals form a group generated by the ideals, and the group of equivalence classes is a homomorphic image of the group of fractional ideals.

task of this section will therefore be to provide a better proof of Theorem 5.19 that helps us find the value of $h_{\mathbb{K}}$ in specific examples.

The two proofs have the following lemma in common. The lemma eliminates the notion of equivalence of ideals from the investigation and shows that the problem is really that of finding elements in each ideal of relatively small norm.

Lemma 5.20. For a particular number field $\mathbb{K}$, if there exists a real constant C with the property that each nonzero ideal J of R contains an element $s \neq 0$ with

$$|N_{\mathbb{K}/\mathbb{Q}}(s)| \leq C\,N(J),$$

then each equivalence class of ideals contains a member L whose absolute norm satisfies $N(L) \leq C$. Consequently the class number $h_{\mathbb{K}}$ is at most the number of nonzero ideals I in R with $N(I) \leq C$. This is a finite number.

PROOF. Let a nonzero ideal I in R be given. By the remarks with Proposition 5.18, choose a nonzero element r in R and an ideal J such that $rI^{-1} = J$. Multiplication by I and use of the remarks shows that $(r) = JI$. By hypothesis for the lemma, choose a nonzero $s \in J$ with $|N_{\mathbb{K}/\mathbb{Q}}(s)| \leq C\,N(J)$. Since s is in J, (s) is contained in J, and therefore $(s) = JL$ for some ideal L. Multiplying both sides of $(r) = JI$ by L gives $(r)L = LJI = (s)I$, and L is therefore equivalent to I. Applying Proposition 5.4, we obtain $N(J)N(L) = N(JL) = N((s)) = |N_{\mathbb{K}/\mathbb{Q}}(s)| \leq C\,N(J)$. Therefore $N(L) \leq C$ as required.

Let us now count the ideals I with $N(I) \leq C$. In terms of the unique factorization $I = \prod_{i=1}^{l} P_i^{e_i}$ of I, we have $N(I) \geq \prod_{i=1}^{l} p_i^{e_i}$, where p_i is the prime number such that $P_i \cap \mathbb{Z} = (p_i)$. In each case, $N(P_i) \geq p_i$. There are only finitely many primes p with $p \leq C$, each is associated with only finitely many prime ideals P of R with $P \cap \mathbb{Z} = (p)$, and P^e contributes at least 2^e toward $N(I)$. The inequality $N(I) \leq C$ shows that these p's and their associated P's are the only possible contributors to I and that each exponent is bounded by $\log_2 N(I)$. Hence there are only finitely many possibilities for I. □

Here is the relatively easy proof of Theorem 5.19.

FIRST PROOF OF THEOREM 5.19. Let $x_1, \dots, x_n$ be a $\mathbb{Z}$ basis of R, and express members of R in terms of this basis as $r = \sum_{i=1}^{n} c_i x_i$ with all $c_i \in \mathbb{Z}$. The value of $N_{\mathbb{K}/\mathbb{Q}}(r)$ is the value of the determinant of left multiplication by r on $\mathbb{K}$, and this value, as a function of $c_1, \dots, c_n$, is a homogeneous polynomial of degree n. Consequently we can find a constant C such that $\big|N_{\mathbb{K}/\mathbb{Q}}\big(\sum_{i=1}^{n} c_i x_i\big)\big| \leq C \max_{1 \leq i \leq n} |c_i|^n$.

It is enough to show that the condition of Lemma 5.20 is satisfied for this C. Thus let an ideal J be given. As each c_i runs through the integers from 0 to

$N(J)^{1/n}$, we obtain more than $N(J)$ members $r = \sum_{i=1}^n c_i x_i$ of R. Since there are only $N(J)$ cosets modulo J, at least two of these members of r, say r_1 and r_2, must lie in the same coset.[20] Then $r_1 - r_2$ is a nonzero member of J, it has all coefficients between $-N(J)^{1/n}$ and $+N(J)^{1/n}$, and our construction of C forces $|N_{\mathbb{K}/\mathbb{Q}}(r_1 - r_2)| \le C\big(N(J)^{1/n}\big)^n = C\,N(J)$. □

The second proof of Theorem 5.19 is to combine Lemma 5.20 with the deeper and more quantitative estimate given in the following theorem.

Theorem 5.21 (Minkowski). For any number field $\mathbb{K}$ of degree n, each nonzero ideal J of R contains an element $s \ne 0$ with

$$|N_{\mathbb{K}/\mathbb{Q}}(s)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\,|D_{\mathbb{K}}|^{1/2} N(J).$$

Here r_2 is half the number of nonreal embeddings of $\mathbb{K}$ in $\mathbb{C}$, and $D_{\mathbb{K}}$ is the field discriminant. Therefore every equivalence class of ideals contains a member L whose absolute norm satisfies

$$N(L) \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\,|D_{\mathbb{K}}|^{1/2}.$$

We shall prove Theorem 5.21 shortly by applying Minkowski's Lattice-Point Theorem to the lattice $\Phi(J)$ in $\Omega = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, where Φ is the mapping described after the proof of Theorem 5.16. The particular compact convex set in the application takes some time to describe, and we return to that matter shortly.

Meanwhile, let us see a little of the utility of Theorem 5.21. The techniques of Chapter I are more useful for computing class numbers for $n = 2$ than Theorem 5.21 is, and we therefore consider only $n \ge 3$. For $n = 3$, we must have $r_2 \le 1$. Theorem 5.21 shows that every equivalence class of ideals in R has a representative L with

$$N(L) \le \frac{4}{\pi}\,\frac{3!}{3^3}\,|D_{\mathbb{K}}|^{1/2} = \frac{8}{9\pi}\,|D_{\mathbb{K}}|^{1/2} < (0.283)\,|D_{\mathbb{K}}|^{1/2}.$$

Problems 1–2 at the end of the chapter give examples of cubic extensions of $\mathbb{Q}$ whose discriminants are -23, -31, and -44. Since these have $(0.283)|D_{\mathbb{K}}|^{1/2} \le (0.283)7 < 2$, the representative ideal in each case must have norm 1 and must be R. Thus for all three of these cubic fields, R is a principal ideal domain.

[20] Again we are applying the Dirichlet pigeonhole principle.

For the cubic field $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$, we know from Section 2 that the discriminant is $D_{\mathbb{K}} = -108$. Consequently the estimate shows that every class of ideals has a representative with norm ≤ 2. If an ideal J has $N(J) = 2$, then 2 has to be a member, and J divides $(2)R$. Proposition 5.10d shows that the factorization of $(2)R$ is as P^3 for a certain unique prime ideal P. Thus R and P represent all equivalence classes, and $h_{\mathbb{K}}$ is 1 or 2. If there is some $r \in R$ with $N_{\mathbb{K}/\mathbb{Q}}(r) = 2$, then $P = (r)$, and the class number is 1; otherwise it is 2. The element $\sqrt[3]{2}$ has $|N_{\mathbb{K}/\mathbb{Q}}(\sqrt[3]{2}\,)| = 2$, and thus $P = (\sqrt[3]{2})$. Therefore R is a principal ideal domain when $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}\,)$.

For Dedekind's example, namely the cubic number field $\mathbb{K}$ built from $X^3 + X^2 - 2X + 8$, we saw in Section 4 that the discriminant is $D_{\mathbb{K}} = -503$. Then the constant in the estimate is $< (0.283)\sqrt{503} < 6.35$. So the interest is in ideals of norm ≤ 6. In ruling out ideals that are principal, we need consider only prime ideals with norm ≤ 6. Problems 24–32 at the end of the chapter identify all the prime ideals of this form and show that they are all principal ideals! We conclude that $h_{\mathbb{K}} = 1$, i.e., that the R in Dedekind's example is a principal ideal domain. Not every cubic number field has class number 1, however; Problem 4 gives an example.

Before turning to the proof of Theorem 5.21, let us observe the following striking consequence.

Corollary 5.22 (Minkowski). For any number field $\mathbb{K}$ of degree n,

$$|D_{\mathbb{K}}|^{1/2} \ge \left(\frac{\pi}{4}\right)^{r_2} \frac{n^n}{n!}.$$

Therefore $D_{\mathbb{K}} > 1$ if $n \ge 2$, and there exists at least one prime number that ramifies in $\mathbb{K}$.

REMARKS. With a more general number field $\mathbb{F}$ than $\mathbb{Q}$ as base field, it can happen that no prime ideal ramifies in a certain nontrivial extension field $\mathbb{K}/\mathbb{F}$. See Problems 5–9 at the end of the chapter.

PROOF. Set $J = R$ in Theorem 5.21, so that $N(J) = 1$. The nonzero element s must have $|N_{\mathbb{K}/\mathbb{Q}}(s)| \ge 1$. The theorem says that $(4/\pi)^{r_2}(n!/n^n)|D_{\mathbb{K}}|^{1/2} \ge 1$, and this is the displayed inequality of the corollary. Since $r_2 \le \frac{1}{2}n$, $(\pi/4)^{r_2} \ge (\pi/4)^{n/2}$, and thus $|D_{\mathbb{K}}|^{1/2} \ge 2^{-n}\pi^{n/2}n^n/n!$. Denote the right side of this inequality by a_n. For $n = 2$, we have $a_2 = \pi/2 > 1$. Also, $a_{n+1}/a_n = \frac{1}{2}\pi^{1/2}(1 + \frac{1}{n})^n \ge \pi^{1/2}$, since $(1 + \frac{1}{n})^n$ is monotone increasing[21] with n and is ≥ 2 for $n = 2$. Hence $a_n > 1$ for all $n \ge 2$. By Theorem 5.5 some prime number ramifies in $\mathbb{K}$. □

[21] To see this monotonicity, expand $a_{n+1} = (1 + \frac{1}{n+1})^{n+1}$ and $a_n = (1 + \frac{1}{n})^n$ by the Binomial Theorem, and observe that the asserted inequality holds term by term.

We turn to the proof of Theorem 5.21. We again make use of the map $\Phi : \mathbb{K} \to \Omega = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^n$ of the previous section. Lemma 5.17 shows that $\Phi(R)$ is a lattice in Ω, and our interest will be in the sublattice $\Phi(J)$, J being the nonzero ideal under study. The idea is to consider the set of $\omega \in \Omega$ for which the function

$$N(\omega) = \Big(\prod_{i=1}^{r_1} |\omega|_i\Big)\Big(\prod_{i=r_1+1}^{r_1+r_2} |\omega|_i^2\Big)$$

has $N(\omega) \le c$, c being a positive number. Since $N(\Phi(x)) = |N_{\mathbb{K}/\mathbb{Q}}(x)|$ for $x \in \mathbb{K}$, the question of finding a member s of J with $|N_{\mathbb{K}/\mathbb{Q}}(s)| \le c$ is the same as the question of finding a nonzero lattice point in the set for which $N(\omega) \le c$. Once we sort out how large c has to be for the answer to be affirmative, then the inequality of the theorem will result. The tool will again be the Minkowski Lattice-Point Theorem (Theorem 5.16), but the difficulty is that the set for which $N(\omega) \le c$ is not necessarily convex.

The nature of the set for which $N(\omega) \le c$ becomes clearer by considering the case of $\mathbb{K} = \mathbb{Q}(\sqrt{m}\,)$ with $m > 0$. The map Φ carries $x + y\sqrt{m}$ for x and y in $\mathbb{Q}$ to the pair $(x + y\sqrt{m}, x - y\sqrt{m})$ in $\mathbb{R}^2$, and if we parametrize ω by the pair (x, y), then the set for which $N(\omega) \le c$ is the part of the (x, y) plane containing the origin and bounded by the two hyperbolas $x^2 - my^2 = c$ and $x^2 - my^2 = -c$. This set is not convex, and it is not even bounded.

Briefly, an individual coordinate of our $\Omega = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, whether a factor of type $\mathbb{R}$ or a factor of type $\mathbb{C}$, contributes something compact convex to the set for which $N(\omega) \le c$ as long as the other coordinates are fixed, but as soon as we allow more than one coordinate to vary, then the product formula defining $N(\omega)$ produces sets that are neither convex nor bounded. To use Theorem 5.16, we want to inscribe a compact convex set within the set for which $N(\omega) \le c$, making the inscribed set contain the origin, be closed under negatives, and have volume as large as possible.

If we were trying to inscribe such a compact convex set in a region cut out by two hyperbolas as above, then the best possible set to use would be a rectangle with sides parallel to the axes. However, the description above in terms of those two hyperbolas used a noncanonical parametrization of elements of $\mathbb{Q}(\sqrt{m}\,)$ as all rational combinations $x + y\sqrt{m}$.

Let us proceed for the general case by using only the structure that is given to us, without using any noncanonical parametrization. The things that are canonical are the factors $\mathbb{R}$ and $\mathbb{C}$, the functions $\|\cdot\|_i$ defined on them, and functions of these. For the example above, the function $N(\omega)$ is given by $N(\omega) = |\omega|_1|\omega|_2$. The geometric set in $\mathbb{R}^2 = \{(\omega_1, \omega_2)\}$ to consider is changed from above; it is still the set toward the origin from two hyperbolas, but the hyperbolas are changed to be $\omega_1\omega_2 = \pm c$, having the axes as asymptotes. The inscribed convex set becomes the set with $|\omega_1| + |\omega_2| \le 2c^{1/2}$. The containment of the latter set in the set toward the origin from the two hyperbolas follows from the inequality $|\omega_1\omega_2|^{1/2} \leq \frac{1}{2}(|\omega_1| + |\omega_2|)$, which is a consequence of the inequality $\frac{1}{4}(|\omega_1| - |\omega_2|)^2 \geq 0$.

In the general case the inscribed convex set is described in terms of the function

$$T(\omega) = \sum_{i=1}^{r_1} |\omega|_i + 2 \sum_{i=r_1+1}^{r_1+r_2} |\omega|_i .$$

The set of ω with $T(\omega) \leq t$, t being a positive constant, is evidently a compact convex set containing 0 and closed under negatives, and the functions $T(\omega)$ and $N(\omega)$ are connected by the arithmetic–geometric mean inequality, which says that

$$N(\omega)^{1/n} \leq \frac{1}{n} T(\omega).$$

Because of this inequality the set with $T(\omega) \leq t$ is contained in the set with $N(\omega) \leq t^n/n^n$.

Since the absolute value in each $\mathbb{R}$ or $\mathbb{C}$ coordinate is canonical, so is the notion of volume, given on rectangular sets by taking products; as usual the understanding is that the set in a factor of $\mathbb{R}$ on which the absolute value is $\leq k$ contributes a factor of $2k$ to the volume, and the comparable set in a factor of $\mathbb{C}$ contributes a factor of πk^2. If V_0 denotes the volume of a fundamental parallelotope for the lattice $\Phi(J)$ in the n-dimensional Euclidean space Ω, then the Minkowski Lattice-Point Theorem says that the set with $T(\omega) \leq t$, and therefore also the set with $N(\omega) \leq t^n/n^n$, contains a nonzero lattice point as soon as the volume of the set with $T(\omega) \leq t$ is $\geq 2^n V_0$. In other words, as soon as the volume of the set with $T(\omega) \leq t$ is $\geq 2^n V_0$, there exists an $s \neq 0$ in J with $|N_{\mathbb{K}/\mathbb{Q}}(s)| \leq t^n/n^n$.

To prove Theorem 5.21, we therefore need to know two things—the volume V_0 of a fundamental parallelotope for $\Phi(J)$ and the volume of the set with $T(\omega) \leq t$. Then we can find the smallest t for which the set with $T(\omega) \leq t$ has volume $\geq 2^n V_0$, and we can sort out the details.

Let us compute the volume V_0. Let $\Gamma = (\alpha_1, \dots, \alpha_n)$ be an ordered $\mathbb{Z}$ basis of the ideal J. The easy case in which to compute V_0 is that $r_1 = n$, i.e., that all the field embeddings of $\mathbb{K}$ into $\mathbb{C}$ are real. In this case the discriminant $D(\Gamma)$ is the determinant of the n-by-n matrix $[B_{ij}]$ with

$$B_{ij} = \mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i\alpha_j) = \sum_{k=1}^{n} \sigma_k(\alpha_i)\sigma_k(\alpha_j) = \sum_{k=1}^{n} A_{ik}A^t_{jk},$$

where $[A_{ij}]$ is the matrix with $A_{ij} = \sigma_j(\alpha_i)$. We recognize $|\det[A_{ij}]|$ as the volume of a fundamental parallelotope for $\Phi(J)$, and therefore $|D(\Gamma)| = V_0^2$. By Proposition 5.1, $D(\Gamma) = N(J)^2 D_{\mathbb{K}}$, and therefore $V_0 = N(J)|D_{\mathbb{K}}|^{1/2}$.

This answer for the value of V_0 is not correct if some of the embeddings of $\mathbb{K}$ into $\mathbb{C}$ are nonreal, since $|\det[\sigma_j(\alpha_i)]|$ no longer equals V_0. To see how to adjust matters, suppose that σ is a nonreal field mapping of $\mathbb{K}$ into $\mathbb{C}$. Then the n-by-n matrix $[\sigma_j(\alpha_i)]$ contains one column $z = \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix}$ corresponding to σ and another column $\bar{z} = \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_n \end{pmatrix}$ corresponding to $\overline{\sigma}$. The entries in the k^{th} row tell how α_k is embedded in Ω, namely at some point $z_k = x_k + iy_k$ for σ and at $\bar{z}_k = x_k - iy_k$. To compute V_0 properly, we should have x_k in one column and y_k in the other, instead of z_k and $\bar{z}_k$. We can transform from the matrix with columns containing z_k and $\bar{z}_k$ to one containing x_k and y_k by first replacing the first column by the sum of the two, which is $2x_k = z_k + \bar{z}_k$, and by then replacing the second column by the difference of the second column and half the new first column, which is $\frac{1}{2}(\bar{z}_k - z_k) = -iy_k$. These operations do not change the determinant. Repeating these steps for each of the r_2 pairs of nonreal field mappings, we obtain a matrix for which the absolute value of the determinant, apart from factors of 2 in r_2 of the columns, is V_0. Consequently $V_0 = 2^{-r_2}|\det[\sigma_j(\alpha_i)]|$. Then $V_0^2 = 2^{-2r_2}|D(\Gamma)|$, and we obtain

$$V_0 = 2^{-r_2}N(J)|D_{\mathbb{K}}|^{1/2}.$$

Now let us compute the volume of the set of ω in Ω for which $T(\omega) \le t$. Write $\omega = (x_1, \dots, x_{r_1}, z_{r_1+1}, \dots, z_{r_1+r_2})$. The volume is the integral of 1 over the set on which $|x_1| + \cdots + |x_{r_1}| + 2|z_{r_1+1}| + 2|z_{r_1+r_2}| \le t$. The set for the integration is invariant under $x_i \mapsto -x_i$ and under rotation in any variable z_i, and hence the volume equals

$$2^{r_1}(2\pi)^{r_2} \int_E \rho_{r_1+1} \cdots \rho_{r_1+r_2}\, dx_1 \cdots dx_{r_1}\, d\rho_{r_1+1} \cdots d\rho_{r_1+r_2},$$

where E is the set on which all variables are ≥ 0 and

$$\sum_{i=1}^{r_1} x_i + 2 \sum_{i=r_1+1}^{r_1+r_2} \rho_i \le t.$$

For $r_1 + 1 \le i \le r_1 + r_2$, introduce $x_i = 2\rho_i$, and make the change of variables. Then the volume becomes

$$2^{r_1-r_2}\pi^{r_2} \int_{E'} x_{r_1+1} \cdots x_{r_1+r_2}\, dx_1 \cdots dx_{r_1+r_2},$$

where E' is the set of $(x_1, \dots, x_n)$ in $\mathbb{R}^{r_1+r_2}$ with all $x_i \ge 0$ and with $\sum_{i=1}^{r_1+r_2} x_i \le t$. Finally we make a change of variables that replaces each x_i by ty_i, and the result is that

$$\operatorname{volume}(\{T(\omega) \le t\}) = 2^{r_1-r_2}\pi^{r_2}t^n \int_S y_{r_1+1}\cdots y_{r_1+r_2}\,dy_1\cdots dy_{r_1+r_2},$$

where S is the standard simplex in $\mathbb{R}^{r_1+r_2}$ with all $y_i \ge 0$ and with $\sum_{i=1}^{r_1+r_2} y_i \le 1$. This definite integral is of a standard type that is evaluated by the following lemma.

Lemma 5.23. In $\mathbb{R}^m$, let S be the standard simplex with all $x_i \ge 0$ and with $\sum_{i=1}^m x_i \le 1$. If $a_1, \dots, a_m$ are positive real numbers, then

$$\int_S x_1^{a_1-1}x_2^{a_2-1}\cdots x_m^{a_m-1}\,dx_1\cdots dx_m = \frac{\Gamma(a_1)\Gamma(a_2)\cdots\Gamma(a_m)}{\Gamma(a_1+\cdots+a_m+1)}.$$

REMARKS. The expression $\Gamma(\,\cdot\,)$ is understood to be the usual gamma function, whose value at positive integers is given by $\Gamma(n+1)=n!$. We merely sketch the proof; the details can be found in many books that treat changes of variables for multiple integrals.[22]

SKETCH OF PROOF. Let I be the unit cube, given by $0 \le u_i \le 1$ for $1 \le i \le m$. We make the change of variables $x = \varphi(u)$ that carries the points u of the cube I one-one onto the points x of the simplex S and that is given by

$$\begin{aligned} x_1 &= u_1, \\ x_2 &= (1-u_1)u_2, \\ &\vdots \\ x_m &= (1-u_1)\cdots(1-u_{m-1})u_m. \end{aligned}$$

The volume element transforms by the absolute value of the Jacobian determinant, specifically by

$$dx = |\varphi'(u)|\,du = (1-u_1)^{m-1}(1-u_2)^{m-2}\cdots(1-u_{m-1})\,du,$$

and the result of the change of variables is that the given integral equals

$$\prod_{i=1}^m \int_0^1 u_i^{a_i-1}(1-u_i)^{\sum_{k=i+1}^m a_k}\,du_i.$$

The factors here can be evaluated by means of Euler's formula

$$\int_0^1 u^{a-1}(1-u)^{b-1} = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)},$$

and the lemma follows. □

[22] One such is the author's *Basic Real Analysis*; the details appear in the problems at the end of Chapter VI of that book. Another such book is Rudin's *Principles of Mathematical Analysis*.

For the integral of interest to us, we have $m = r_1 + r_2$, $a_1 = \cdots = a_{r_1} = 1$, and $a_{r_1+1} = \cdots = a_{r_1+r_2} = 2$. Thus $a_1 + \cdots + a_m = r_1 + 2r_2 = n$, and we obtain

$$\text{volume}(\{T(\omega) \le t\}) = 2^{r_1-r_2}\pi^{r_2}t^n \frac{\Gamma(1)^{r_1}\Gamma(2)^{r_1+r_2}}{\Gamma(n+1)} = \frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!}.$$

Finally we can put everything together. We are to solve for t such that this expression is equal to $2^n V_0$, and then there exists an element $s \ne 0$ in J with $|N_{\mathbb{K}/\mathbb{Q}}(s)| \le t^n/n^n$. Since $V_0 = 2^{-r_2}N(J)|D_{\mathbb{K}}|^{1/2}$, the equation to solve for t is

$$\frac{2^{r_1-r_2}\pi^{r_2}t^n}{n!} = 2^n 2^{-r_2} N(J)|D_{\mathbb{K}}|^{1/2}.$$

Thus $t^n = \left(\frac{4}{\pi}\right)^{r_2} n! N(J)|D_{\mathbb{K}}|^{1/2}$, and the element $s \ne 0$ in J satisfies

$$|N_{\mathbb{K}/\mathbb{Q}}(s)| \le \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} |D_{\mathbb{K}}|^{1/2} N(J).$$

This completes the proof of Theorem 5.21.

7. Problems

1. Take as known that the discriminant of a cubic polynomial $F(X) = X^3 + pX + q$ is $-(4p^3 + 27q^2)$. In each of the following cases, let $\mathbb{K} = \mathbb{Q}[X]/(F(X))$ with $F(X)$ as indicated, and verify that the field discriminant $D_{\mathbb{K}}$ is as indicated:
   (a) $F(X) = X^3 - X - 1$, $D_{\mathbb{K}} = -23$.
   (b) $F(X) = X^3 + X + 1$, $D_{\mathbb{K}} = -31$.

2. Let $\mathbb{K} = \mathbb{Q}[X]/(F(X))$, where $F(X) = X^3 - 2X^2 + 2$.
   (a) Use the formula of the previous problem to show that the discriminant of the polynomial $F(X)$ is -44.
   (b) Using Proposition 5.2, show that $D_{\mathbb{K}}$ cannot be -11, and conclude that $D_{\mathbb{K}} = -44$.

3. This problem computes the class number of $\mathbb{K} = \mathbb{Q}(\sqrt[3]{3})$.
   (a) Show that every equivalence class of nonzero ideals contains an ideal with norm ≤ 4.
   (b) Show that the prime ideals whose norm is a power of 2 are $P_1 = (2, \sqrt[3]{3} - 1)$, whose norm is 2, and $P_2 = (2, \sqrt[3]{9} + \sqrt[3]{3} + 1)$, whose norm is 4.
   (c) Show for P_1 that 2 is a multiple of $\sqrt[3]{3} - 1$, and show for P_2 that 2 is a multiple of $\sqrt[3]{9} + \sqrt[3]{3} + 1$.
   (d) Show that the only prime ideal whose norm is 3 is $(\sqrt[3]{3})$.
   (e) Deduce that the class number of $\mathbb{K}$ is 1.

4. Let R be the ring of algebraic integers in the number field $\mathbb{K} = \mathbb{Q}(\sqrt[3]{7})$, and let I be the doubly generated ideal $I = (2, 1 + \sqrt[3]{7})$ in R.
   (a) Prove that $N(I) = 2$.
   (b) Prove that I is not a principal ideal.

Problems 5–9 give an example of a nontrivial finite extension $\mathbb{L}/\mathbb{K}$ of number fields in which no prime ideal for $\mathbb{K}$ ramifies in passing to $\mathbb{L}$. By contrast, Corollary 5.22 says that there always exists a prime that ramifies in passing from $\mathbb{Q}$ to a nontrivial finite extension. The example has $\mathbb{L} = \mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ and $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$. Let $\mathbb{K}' = \mathbb{Q}(\sqrt{5})$ and $\mathbb{K}'' = \mathbb{Q}(\sqrt{-1})$. Observe that $\mathbb{L}/\mathbb{Q}$ is a Galois extension, and so are all the various quadratic extensions of $\mathbb{L}$ over $\mathbb{K}$, $\mathbb{K}'$, and $\mathbb{K}''$, as well as of $\mathbb{K}$, $\mathbb{K}'$, and $\mathbb{K}''$ over $\mathbb{Q}$. The problems make use of the fact that ramification indices multiply in passing to an extension in stages, and so do residue class degrees.

5. Show that the minimal polynomial of $\sqrt{-1} + \sqrt{-5}$ over $\mathbb{Q}$ is $X^4 + 12X^2 + 16$, and deduce that the elements $\frac{1}{2}(\pm\sqrt{-1} \pm \sqrt{-5})$ are algebraic integers in $\mathbb{L}$.

6. By making use the formula for $D(\xi)$ in terms of $\mathcal{D}(\xi)$, where ξ is an element in $\mathbb{L}$, prove that $|D(\frac{1}{2}(\sqrt{-1} + \sqrt{-5}))| = 2^4 5^2$. Consequently $D_{\mathbb{L}}$ divides $2^4 5^2$.

7. Verify the following decompositions of the ideals (2) and (5) when extended from $\mathbb{Z}$ to the rings R, R', and R'' of algebraic integers in $\mathbb{K}$, $\mathbb{K}'$, and $\mathbb{K}''$:
   (a) $(2)R = \wp^2$ with $f = 1$, and $(5)R = \wp^2$ with $f = 1$.
   (b) $(2)R' = \wp$ with $f = 2$, and $(5)R' = \wp^2$ with $f = 1$.
   (c) $(2)R'' = \wp^2$ with $f = 1$, and $(5)R'' = \wp_1\wp_2$ with $f = 1$.

8. Let T be the ring of algebraic integers in $\mathbb{L}$. Since $\mathbb{L}/\mathbb{Q}$ is a Galois extension, the only possible decompositions of $(p)T$, when p is a prime number, have (e, f, g) equal to $(4, 1, 1)$ or $(2, 2, 1)$ or $(2, 1, 2)$ or $(1, 4, 1)$ or $(1, 2, 2)$ or $(1, 1, 4)$. Here e is the ramification index, f is the residue class degree, and g is the number of distinct prime factors. Using the product formulas for ramification degrees and comparing what happens for the passage $\mathbb{Q} \subseteq \mathbb{K}' \subseteq \mathbb{L}$ with what happens for the passage $\mathbb{Q} \subseteq \mathbb{K}'' \subseteq \mathbb{L}$, show that the only possibilities for $(p)T$ with $p = 2$ and $p = 5$ are
   (a) $(e, f, g) = (2, 2, 1)$ for $(2)T$, i.e., $(2)T = P^2$ with $\dim_{\mathbb{F}_2}(T/P) = 2$.
   (b) $(e, f, g) = (2, 1, 2)$ for $(5)T$, i.e., $(5)T = P_1^2 P_2^2$ with $\dim_{\mathbb{F}_5}(T/P_1) = \dim_{\mathbb{F}_5}(T/P_2) = 1$.

9. Return to the situation with $\mathbb{Q} \subseteq \mathbb{K} \subseteq \mathbb{L}$, where $\mathbb{K} = \mathbb{Q}(\sqrt{-5})$. According to Problem 7a, the prime decompositions of $(2)R$ and $(5)R$ are $(2)R = \wp_2^2$ and $(5)R = \wp_5^2$.
   (a) Using the results of Problem 8, show that $\wp_2 T = P$ and $\wp_5 T = P_1 P_2$, i.e., $\wp_2 T$ is prime, and $\wp_5 T$ is the product of two distinct prime ideals.

(b) Show how to conclude from these facts and from Theorem 5.6 that no prime ideal in R ramifies in T. (Educational note: The field $\mathbb{L}$ is the "Hilbert class field" of $\mathbb{K}$ in the sense of Section 1; the order of the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ matches the class number of $\mathbb{K}$.)

Problems 10–16 concern the cyclotomic field $\mathbb{K} = \mathbb{Q}(e^{2\pi i/p})$, where $p > 2$ is a prime number. They show that the discriminant is given by $D_{\mathbb{K}} = p^{p-2}$ and that a $\mathbb{Z}$ basis of the ring R of algebraic integers in $\mathbb{K}$ consists of $\{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$, where $\zeta = e^{2\pi i/p}$.

10. Show that $\mathbb{K}$ has no real-valued field mappings into $\mathbb{C}$, and deduce that $N_{\mathbb{K}/\mathbb{Q}}(x)$ is positive for every $x \neq 0$ in $\mathbb{K}$.

11. Let $F(X) = X^{p-1} + X^{p-2} + \cdots + 1$ be the minimal polynomial of ζ over $\mathbb{Q}$, and let $G(X) = F(X+1)$. Suppose that k is an integer with $\mathrm{GCD}(k, p) = 1$.
   (a) Prove that $G(X)$ is the minimal polynomial of $\zeta^k - 1$, and deduce that the norm of $\zeta^k - 1$ is given by $F(1) = p$.
   (b) Why does it follow that $N_{\mathbb{K}/\mathbb{Q}}(1 - \zeta^k) = p$?
   (c) Prove that $(1 - \zeta^k)/(1 - \zeta)$ is a unit of R.

12. With notation as in the previous problem, prove that the different $\mathcal{D}(\zeta^k)$ of ζ^k has $|\mathcal{D}(\zeta^k)| = p\big/|\zeta^k - 1|$.

13. Deduce from the previous problem that $D(\zeta) = (-1)^{(p-1)(p-2)/2} p^{p-2}$.

14. Let $\lambda = 1 - \zeta$. Problem 11b shows that $N_{\mathbb{K}/\mathbb{Q}}(\lambda) = p$. Prove that
   (a) the $\mathbb{Z}$ span of $\{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$ equals the $\mathbb{Z}$ span of $\{1, \lambda, \lambda^2, \dots, \lambda^{p-2}\}$.
   (b) an equality $p = \prod_{k=1}^{p-1} (1 - \zeta^k)$ holds.
   (c) there exists a unit ε of R such that $p = \varepsilon(1 - \zeta)^{p-1} = \varepsilon\lambda^{p-1}$.

15. Using Problem 14c, prove that the principal ideals $(p)R$ and (λ) in R are related by $(p)R = (\lambda)^{p-1}$, and deduce from this fact that (λ) is a prime ideal.

16. Apply Proposition 5.2 to the $\mathbb{Q}$ basis $\{1, \lambda, \lambda^2, \dots, \lambda^{p-2}\}$ of $\mathbb{K}$ lying in R to show that no factor of p^2 can be eliminated from $D(\lambda) = D(\zeta)$; take into account the highest powers of λ that divide each term. Conclude that $D_{\mathbb{K}} = D(\zeta)$ and that $\{1, \zeta, \zeta^2, \dots, \zeta^{p-2}\}$ is a $\mathbb{Z}$ basis of R.

Problems 17–18 use the same notation as in the text of the chapter: $\mathbb{K}$ is a number field of degree n over $\mathbb{Q}$, R is its ring of algebraic integers, $D_{\mathbb{K}}$ is its field discriminant, the field mappings of $\mathbb{K}$ into $\mathbb{C}$ are denoted by σ_i for $1 \leq i \leq n$, r_1 of the σ_i's are real-valued, and r_2 complex-conjugate pairs of the σ_i's are nonreal.

17. Prove that the sign of $D_{\mathbb{K}}$ is $(-1)^{r_2}$.

18. **(Stickelberger's condition)** Let $\Gamma = (\alpha_1, \dots, \alpha_n)$ be an ordered n-tuple of members of R linearly independent over $\mathbb{Q}$, and suppose that $\mathbb{K}/\mathbb{Q}$ is a Galois extension. Write $\det[\sigma_j(\alpha_i)] = P - N$, where P is the sum of all the terms of

the determinant corresponding to even permutations and N is the sum corresponding to even permutations. Using Galois theory, prove that $P+N$ and PN are in $\mathbb{Z}$. Then write $D(\Gamma)=(\det[\sigma_j(\alpha_i)])^2=(P+N)^2-4PN$, and deduce that the integer $D(\Gamma)$ is congruent to 1 or 0 modulo 4. (Educational note: A variant of this argument proves the same conclusion about $D(\Gamma)$ without the assumption that $\mathbb{K}/\mathbb{Q}$ is a Galois extension. One makes use of the smallest normal extension of $\mathbb{Q}$ containing $\mathbb{K}$; this is the splitting field of the minimal polynomial of any primitive element of $\mathbb{K}$.)

Problems 19–23 continue with the notation of Problems 17–18. It is to be proved that a suitable localization $S^{-1}R$ of R is a principal ideal domain for which the group of units is finitely generated as an abelian group. Let h be the class number of $\mathbb{K}$.

19. Let $I_1,\dots,I_h$ be ideals representing all the equivalence classes of ideals in R. For each I_j, let u_j be a nonzero element of I_j, and put $u=u_1\cdots u_h$. Define $S=\{1,u,u^2,\dots\}$. Prove that $S^{-1}R$ is a principal ideal domain.

20. (a) Prove that if a member a of R divides u^k within R for some $k\geq 0$, then a is a unit in $S^{-1}R$, i.e., a^{-1} is in $S^{-1}R$.
    (b) Prove conversely that if a member a of R has the property that au^{-m} is a unit in $S^{-1}R$ for some $m\geq 0$, then a divides u^k within R for some integer $k\geq 0$.

21. Let $P_1,\dots,P_l$ be the distinct prime ideals appearing in the unique factorization of (u), and suppose that $P_j^h=(b_j)$ for $1\leq j\leq l$. Let au^{-m} and k be as in Problem 20b, and write $u^k=ab$ with $b\in R$.
    (a) Why must each b_j necessarily be a unit in $S^{-1}R$?
    (b) Prove that there exist integers $n_j\geq 0$ for $1\leq j\leq l$ such that the element $d=\prod_j b_j^{n_j}$ has $(a)=(d)P_1^{t_1}\cdots P_l^{t_l}$ for some integers t_j with $0\leq t_j\leq h-1$.
    (c) In this case, why must $P_1^{e_1}\cdots P_l^{e_l}$ be a principal ideal?

22. Suppose that there are N tuples $(e_1,\dots,e_l)$ with $0\leq e_j\leq h-1$ for all j such that $P_1^{e_1}\cdots P_l^{e_l}$ is a principal ideal. For the i^{th} such tuple, let the principal ideal be denoted by (c_i), $1\leq i\leq N$. Prove that if k, a, and b are as in the previous problem and if the principal ideal in (c) of that problem is (c_i), then $a=bc_i\varepsilon$ for some ε in $R^\times$.

23. Conclude from the three previous problems that the group of units of $S^{-1}R$ is finitely generated as an abelian group.

Problems 24–32 complete the discussion in Section 4 of Dedekind's example of a cubic extension of $\mathbb{Q}$ with a common index divisor. The field is $\mathbb{K}=\mathbb{Q}(\xi)$, where ξ is a root of $F(X)=X^3+X^2-2X+8$, and it was shown in Section 4 that $D(\xi)=-2^2\cdot 503$. Let R be the ring of algebraic integers in $\mathbb{K}$. It will be shown that R is a principal ideal domain.

24. Show that $\eta = 4/\xi$ is a root of the polynomial $G(X) = X^3 - X^2 + 2X + 8$, and conclude that η is in R.

25. (a) By rewriting $F(\xi)/\xi$ in terms of ξ and η, show that $\xi^2 + \xi - 2 + 2\eta = 0$.
    (b) By rewriting $G(\eta)/\eta$ in terms of ξ and η, show that $2\xi + 2 - \eta + \eta^2 = 0$. Conclude from this formula and (a) that products of ξ and η may be simplified according to the table
$$\xi^2 = -\xi + 2 - 2\eta, \qquad \eta^2 = -2\xi - 2 + \eta, \qquad \xi\eta = 4.$$
    (c) Using the first formula in (b), deduce the containment of abelian groups given by $\mathbb{Z}(\{1, \xi, \xi^2\}) \subseteq \mathbb{Z}(\{1, \xi, \eta\})$.
    (d) Using the first formula in (b), deduce that η does not lie in $\mathbb{Z}(\{1, \xi, \xi^2\})$.
    (e) Conclude from the above facts that $\{1, \xi, \eta\}$ and $\big\{1, \xi, \frac{1}{2}(\xi^2 + \xi)\big\}$ are $\mathbb{Z}$ bases of R.

26. Let P be a prime ideal in R containing $(2)R$, write $\mathbb{F}$ for the field R/P, let $\varphi : R \to \mathbb{F}$ be the quotient homomorphism, and let $\overline{\xi} = \varphi(\xi)$ and $\overline{\eta} = \varphi(\eta)$. By applying φ to the table in Problem 25b and using the fact that the additive group generated by $\{1, \xi, \eta\}$ is all of R, prove that $\mathbb{F}$ has only two elements, i.e., that the residue class degree is $f = 1$, and that the only possibilities for φ are the following:
$$\begin{aligned} \varphi &= \varphi_{0,0} \quad \text{with} \quad \varphi_{0,0}(\xi) = 0, \quad \varphi_{0,0}(\eta) = 0,\\ \varphi &= \varphi_{1,0} \quad \text{with} \quad \varphi_{1,0}(\xi) = 1, \quad \varphi_{1,0}(\eta) = 0,\\ \varphi &= \varphi_{0,1} \quad \text{with} \quad \varphi_{0,1}(\xi) = 0, \quad \varphi_{0,1}(\eta) = 1.\end{aligned}$$

27. Conversely show that the three functions $\varphi_{0,0}, \varphi_{1,0}, \varphi_{0,1}$ defined on ξ and η in the previous problem extend to well-defined ring homomorphisms of R onto $\mathbb{F}_2$.

28. Let $P_{0,0}$, $P_{1,0}$, and $P_{0,1}$ be the kernels of the ring homomorphisms in the previous problem. Prove that these ideals all have norm 2 and that $(2)R = P_{0,0}P_{1,0}P_{0,1}$.

29. (a) Prove that $P_{0,0} = (2, \xi, \eta)$, $P_{1,0} = (2, \xi + 1, \eta)$, and $P_{0,1} = (2, \xi, \eta + 1)$.
    (b) Exhibit η as a member of the ideal $(2, \xi + 1)$, and show therefore that $P_{1,0} = (2, \xi + 1)$.
    (c) Similarly show that $P_{0,1} = (2, \eta + 1)$ and that $P_{0,0} = (2, \xi - \eta)$.

30. The previous problem exhibited $P_{0,0}$, $P_{1,0}$, and $P_{0,1}$ explicitly as doubly generated. In fact, use of the norm map $N_{\mathbb{K}/\mathbb{Q}}$ will ultimately show them to be principal ideals.
    (a) Show that if $H(X)$ is the field polynomial over $\mathbb{Q}$ of an element θ in $\mathbb{K}$, then $N_{\mathbb{K}/\mathbb{Q}}(\theta) = -H(0)$ and $N_{\mathbb{K}/\mathbb{Q}}(\theta - q) = -H(q)$ for every $q \in \mathbb{Q}$.
    (b) Prove that $N_{\mathbb{K}/\mathbb{Q}}(\xi) = N_{\mathbb{K}/\mathbb{Q}}(\eta) = -8 = -2^3$, that $|N_{\mathbb{K}/\mathbb{Q}}(\xi + 3)| = 2^2$, that $|N_{\mathbb{K}/\mathbb{Q}}(\xi - 1)| = |N_{\mathbb{K}/\mathbb{Q}}(\xi + 2)| = 2^3$, and that $|N_{\mathbb{K}/\mathbb{Q}}(\xi - 2)| = 2^4$.

(c) Prove that $(\xi) = P_{0,0}^a P_{1,0}^b P_{0,1}^c$ for unique exponents ≥ 0 whose sum is 3, and that $(\eta) = P_{0,0}^\alpha P_{1,0}^\beta P_{0,1}^\gamma$ for unique exponents ≥ 0 whose sum is 3.

(d) Using the fact that $\xi\eta = 4$, prove that $a + \alpha = b + \beta = c + \gamma = 2$.

(e) Using the definitions of $P_{0,0}$, $P_{1,0}$, and $P_{0,1}$ as kernels, prove that $b = 0$ and $\gamma = 0$.

(f) Conclude that $(\xi) = P_{0,0}P_{0,1}^2$ and that $(\eta) = P_{0,0}P_{1,0}^2$.

31. This problem uses the norm computations in Problem 30b.

(a) Using the defining homomorphisms, show that if l is an odd integer, then $P_{1,0}$ contains $(\xi + l)$, but $P_{0,0}$ and $P_{0,1}$ do not.

(b) Show that $(\xi + 3) = P_{1,0}^2$ and that $(\xi - 1) = P_{1,0}^3$.

(c) Using the defining homomorphisms, show that if l is an even integer, then $P_{0,1}$ contains $(\xi + l)$, but $P_{1,0}$ does not.

(d) Show that $(2, \xi) = P_{0,0}P_{0,1}$.

(e) Show that if l is an even integer not divisible by 4, then $P_{0,1}^2$ does not contain $(\xi + l)$.

(f) Show that $(\xi + 2) = P_{0,0}^2 P_{0,1}$ and that $(\xi - 2) = P_{0,0}^3 P_{0,1}$.

32. (a) From the identity $(\xi + 2)P_{0,0} = (\xi - 2)$ that results from Problem 31f, deduce that $r_{0,0} = \frac{\xi-2}{\xi+2}$ is in R and that $P_{0,0} = (r_{0,0})$.

(b) Deduce similarly that $P_{1,0}$ and $P_{0,1}$ are principal ideals.

(c) Using Theorem 5.6, show that R contains no ideals of norm 3.

(d) Using Theorem 5.6, show that the only ideal in R of norm 5 is $(5, 1 + \xi)$.

(e) Show that $|N_{\mathbb{K}/\mathbb{Q}}(1 + \xi)| = 10$, and deduce that $(1 + \xi) = (5, 1 + \xi)P$, where P is one of the three ideals $P_{0,0}$, $P_{1,0}$, and $P_{0,1}$.

(f) Why does it follow that $(5, 1 + \xi)$ is a principal ideal?

(g) Prove that R is a principal ideal domain.