ALGEBRAIC NUMBER THEORY

Robert L. Long

Algebraic Number Theory

ROBERT L. LONG
Department of Mathematics
University of Florida

Library of Congress Cataloging in Publication Data

Long, Robert L 1940-
Algebraic number theory.

(Monographs and textbooks in pure and applied mathematics ; 41)
Bibliography: p.
Includes index.
1. Algebraic number theory. I. Title.
QA247.L59 512'.74 76-40364
ISBN 0-8247-6540-0

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Current printing (last digit):
10 9 8 7 6 5 4 3 2 1

PRINTED IN THE UNITED STATES OF AMERICA

PREFACE

As one question gives rise to another, pure mathematics arises from the conceptual framework within which man organizes his experience. The concept of number is fundamental in this framework--logically prior to most of the concepts of physics, for example--so that it is hardly surprising that number theory has had a special charm for amateur and professional mathematicians for centuries. The subject which is known today as algebraic number theory began with attempts to prove Fermat's famous "last theorem": the equation $x^n + y^n = z^n$ has no solution in integers x, y, z if n is greater than 2. In Hilbert's "Zahlbericht" these attempts were worked into an organic structure--the theory of algebraic numbers--which also encompasses other mathematics not originally motivated by Fermat's problem. Since the Zahlbericht was written, algebraic number theory has flourished. Many current investigators are primarily interested in questions which have arisen as the subject developed; others are interested in Fermat's theorem or other long-standing questions about diophantine equations: the subject exhibits a healthy mixture of "pure" and "applied" aspects. One of its charms is that it begins with questions which are easily understood. Another is that in the study of those questions a wide variety of mathematical tools are used.

It would be difficult to improve on Samuel's Algebraic Theory of Numbers for an introduction; the present book is intended to take up about where Samuel's ends. There is no single path into the subject; the sense of unity must be provided by the questions considered. Concretely in the text the exercises do most to tie together the different chapters.

The first three sections of Chapter 1 contain a very brief summary of the material with which a reader should be familiar; it is all in Samuel's book (except for the Chinese remainder theorem which is proven in full) but not everything in that book is prerequisite to this one. Chapter 1 also contains a section devoted to Hilbert's theory of ramification in Galois extensions and an optional section exposing the structure theory of finitely generated torsion-free modules over a Dedekind domain.

Chapters 2 through 5 develop basic concepts of algebraic number theory using the techniques of localization and completion. The methods in these chapters are almost exclusively algebraic. Chapters 6 through 8 make use of analytic methods and are primarily devoted to a detailed study of abelian extensions of the rationals. These are the extensions about which the most is known and which serve as prototypes for the generalization of the theory to relative and nonnormal extensions. Many of the elementary questions which have motivated the study of algebraic numbers (for example Fermat's theorem or the representation of integers by quadratic forms) lead expecially to the absolutely abelian fields. The last chapter introduces the study of normal extensions as modules over a suitable group ring.

Chapters 2 through 8 are based on notes of a first year graduate course I gave at the University of Florida in 1972-1973. That course began with the study of Samuel's book during the fall quarter so that the notes were covered in the winter and spring quarters.

There are a few comments that I should make about the style in which the book is written. I have tried to give a careful exposition of the central parts of algebraic number theory and at the same time to indicate various directions in which the theory can be pursued further. These indications, sometimes in the text and often in the exercises, are usually only sketched. Almost any chapter in the book could be expanded into an entire text, but in most cases those texts would not be about number theory. Sometimes I have repeated a definition or re-explained a notation; occasionally an entire proof has been repeated. I hope this will not unduly annoy a systematic reader and will be appreciated by those who turn to the book for reference or to refresh their memories. I have spelled out many words that are usually abbreviated; the words can be read just as quickly as the abbreviations and they look much better. There is no symbol to indicate the end of a proof. The proofs that need one are either poorly written or need to be studied more carefully.

The exercises are an important part of the book and you should read them whether or not you work on them. I exhort the student to read actively; you must ask yourself questions and try to relate different parts of the book to each other. The exercises should be of some help in this. You may also want to consult the book by Borevich and Shafarevich which has fine problem sets. Finally, if you are using the book in a class, take advantage of the teacher. You are learning best when he is talking about something to which you have given some thought; study and ask questions.

It is a pleasure to acknowledge the influence and help of teachers and friends. Leon McCulloh introduced me to algebraic number theory as a graduate student, helped me through my thesis, and remains a good friend. I have also learned much from Helmut Hasse, even without having worked with him personally. His books and research papers have contributed enormously to mathematics in the twentieth century. At the same time his careful style of exposition and sensitivity to language stand as an example for all of us who write mathematics. Chapters 3 and 8 of this text derive from Hasse's treatments of the same subjects.

I had the opportunity to attend the lectures by Kenkichi Iwasawa during 1971-1972 on Z_ℓ-extensions and cyclotomic fields. Iwasawa's total command of the subject and his subtly dramatic presentation made a lasting impression on me. Many parts of my exposition, especially in Chapter 6, are based on his.

The books by Lang and Borevich and Shafarevich have also influenced my presentation. Lang's use of Lipschitz maps in the analytic theory seems to be a good idea and I have used it in Chapter 7. His book also contains an introduction to many important topics in number theory that are not touched upon in this book, for example, adeles, ideles, and classified theory.

The theory of quadratic forms, which is not touched upon in this book, has been an important part of algebraic number theory from the earliest times. (Look at the book by Dirichlet-Dedekind [6].) Borevich and Shafarevich affords an excellent account of this theory.

I am indebted to Danny Davis and Professor Robert Gold who have read parts of the manuscript and offered many useful suggestions and to Sharon Bullivant who has typed the book; I thank them all.

Robert L. Long

CONTENTS

CONTENTS

Chapter 1

DEDEKIND DOMAINS AND ALGEBRAIC NUMBER THEORY

The first three sections of this chapter are a review of the most basic facts about Dedekind domains and algebraic numbers. They contain only a few proofs. Their main purpose is to be available for reference when questions arise about notation or assumed results. I suggest that the reader skip them entirely or else skim them for items of possible interest. When you need to refer to them, the index will direct you.

The fourth section can be skipped also. The reader who chooses to read it will find a coherent account of ramification theory. Many of the results in this section appear as problems in later chapters. The fifth section is farther from the mainstream of ideas in the book and is not needed for any of the subsequent chapters. It is included because it rounds out the elementary theory of Dedekind domains nicely. It would be possible to give a systematic exposition of much of algebraic number theory using the "global" methods of Section 5.

1. Dedekind Domains

A Dedekind domain is an integral domain in which every ideal is a product of prime ideals. In a Dedekind domain the factorization of an ideal as a product of prime ideals is in fact unique. Equivalent definitions are (1) a Noetherian integrally closed domain in which every nonzero prime ideal is maximal, and (2) a domain for which every ideal is a projective module. Dedekind domains are discussed thoroughly in [37]; for the homological definition see [30].

Let A be a Dedekind domain and K be its quotient field. Any ideal in A can be written uniquely in the form $\mathfrak{a} = \Pi\, \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a})}$ where the product is over all nonzero primes p and the exponents $v_p(a)$ are almost all zero. For any prime p, we write $A_p = \{x \in K: \exists y \in A\backslash p, yx \in A\}$. This is the ring of quotients of A with respect to the multiplicatively closed set $A\backslash p$. In a Dedekind domain, the ideals are partially ordered by set theoretic inclusion and also by the relation of divisibility. The two partial orders are related:

(1.1) Lemma. Let a and b be ideals in the Dedekind domain A. Then $a \supseteq b$ if and only if $a|b$ (i.e., a divides b).

Proof: If $a|b$, then $b = ac$ for some ideal c of A. Obviously, $ac \subseteq a$. Conversely, suppose that $a \supseteq b$. To prove the divisibility relation, it is enough to show that for any nonzero prime p, $v_p(a) \leq v_p(b)$. These exponents are unchanged if a and b are replaced by the ideals they generate in A_p. Thus one may assume that a and b are both powers of p. But in that case, the result is obvious.

Remark: Let A be any commutative ring and S be a multiplicatively closed subset of A. The ring of quotients of A with respect to S, denoted $S^{-1}A$, is a ring whose underlying set is the set of equivalence classes of pairs $(a,s) \in A \times S$ under the relation $(a,s) \sim (a',s')$ if and only if there is a $t \in S$ such that $t(s'a - sa') = 0$. The operations in $S^{-1}A$ are defined by $[a,s] + [a',s'] = [as' + a's, ss']$ and $[a,s][a',s'] = [aa',ss']$ (where $[a,s]$ denotes the equivalence class of the pair (a,s)). The homomorphism $\theta: A \to S^{-1}A$ defined by $\theta(a) = [sa,s]$ (where s is any element of S) induces an inclusion preserving correspondence between ideals of A and ideals of $S^{-1}A$. The restriction of this correspondence to the set of prime ideals of A which do not meet S is a bijection onto the set of all prime ideals of $S^{-1}A$. More details can be found in [37, Chapter IV, Sections 9 and 10].

In the study of Dedekind domains, it is often possible to reduce a problem about A to a problem about one of the rings A_p (p is a nonzero prime ideal). Because the ring A_p has a unique maximal ideal (generated by p), the following result may then be useful:

(1.2) Nakayama's Lemma. Let A be a commutative ring and a be an ideal which is contained in every maximal ideal of A. If X is a finitely generated A-module and $\mathfrak{a}X = X$, then $X = 0$.

Proof: If $X \neq 0$, then, being finitely generated, it has a maximal proper submodule Y. X/Y is a simple A-module and is therefore isomorphic to $A/\mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. Thus $\mathfrak{m}X \subseteq Y$. But then $X = \mathfrak{a}X \subseteq \mathfrak{m}X \subseteq Y$, which is impossible. Therefore $X = 0$.

Returning now to the ideal theory in a Dedekind domain one can see, using (1.1), that the greatest common divisor of two ideals is the smallest ideal which contains both and that the least common multiple is the largest ideal contained in both. In terms of the $v_{\mathfrak{p}}$'s:

(1.3) Lemma. For any ideals $\mathfrak{a}$ and $\mathfrak{b}$ and for every nonzero prime ideal $\mathfrak{p}$,

$$v_{\mathfrak{p}}(\mathfrak{a} + \mathfrak{b}) = \min\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$$
$$v_{\mathfrak{p}}(\mathfrak{a} \cap \mathfrak{b}) = \max\{v_{\mathfrak{p}}(\mathfrak{a}), v_{\mathfrak{p}}(\mathfrak{b})\}$$

(1.4) Proposition. Let $\mathfrak{a}$, $\mathfrak{b}$, and $\mathfrak{c}$ be ideals in a Dedekind domain, then

$$\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) = (\mathfrak{a} \cap \mathfrak{b}) + (\mathfrak{a} \cap \mathfrak{c})$$
$$\mathfrak{a} + (\mathfrak{b} \cap \mathfrak{c}) = (\mathfrak{a} + \mathfrak{b}) \cap (\mathfrak{a} + \mathfrak{c})$$

The reader can prove this result by calculating $v_{\mathfrak{p}}$ on both sides using (1.3).

(1.5) Chinese Remainder Theorem. Let A be a Dedekind domain, $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ ideals in A, and $x_1, \ldots, x_n \in A$. The system of congruences, $x \equiv x_i \bmod \mathfrak{a}_i$ $(i=1,\ldots,n)$ admits a solution $x \in A$ if and only if $x_i \equiv x_j \bmod \mathfrak{a}_i + \mathfrak{a}_j$ for each pair (i,j).

Proof: If x is a solution, then $x_i \equiv x \equiv x_j \bmod \mathfrak{a}_i + \mathfrak{a}_j$. The converse will be proved by induction on n. When $n = 2$, $x_1 - x_2 = a_1 - a_2$ for suitable $a_i \in \mathfrak{a}_i$. Thus $x = x_1 - a_1 = x_2 - a_2$ is a solution. Now assume the theorem has been shown for n-1 simultaneous congruences. Then there is an x' with $x' \equiv x_i \bmod \mathfrak{a}_i$ for $i=1,\ldots,n-1$. We seek an x, $x \equiv x' \bmod \bigcap_{i=1}^{n-1} \mathfrak{a}_i$, $x \equiv x_n \bmod \mathfrak{a}_n$. These two congruences can be solved if $x_n \equiv x' \bmod \bigcap_{i<n} a_i + a_n$. By the distributive law, the last ideal equals $\bigcap_{i<n}(a_i + a_n)$. For $i=1,\ldots,n-1$, $x_n \equiv x_i \equiv x' \bmod a_i$; thus a solution exists.

The reader may find it worthwhile to write down the special case of the theorem in which $A = \mathbb{Z}$. Of the many possible corollaries, only one will be stated here.

(1.6) Corollary. If $m_1,\ldots,m_r$ are integers which are relatively prime in pairs, then

$$\mathbb{Z}/(m_1 m_2 \cdots m_r) \cong \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2) \times \cdots \times \mathbb{Z}/(m_r).$$

Given integers $x_1,\ldots,x_r$, there is an $x \equiv x_i \bmod m_i$ $(i = 1,\ldots,r)$, and x is unique modulo $m_1 m_2 \cdots m_r$.

Proof: Because the m_i are relatively prime in pairs, the kernel of the homomorphism $\mathbb{Z} \to \prod_i \mathbb{Z}/(m_i)$, which is $\bigcap_i (m_i)$ in any case, equals $(m_1 m_2 \cdots m_r)$. The theorem asserts that the homomorphism is surjective.

An A-submodule of K which is finitely generated is called a fractional ideal. Equivalently, a submodule M of K is a fractional ideal if and only if $aM \subseteq A$ for some $a \in A$. The fractional ideals constitute a free abelian group of which a basis is the set of nonzero prime ideals of A. The ideal A is the identity element of this group. For any fractional ideal a, the inverse is $a^{-1} = \{x \in K: xa \subseteq A\}$. The ideals of A are often referred to as integral ideals. For fractional ideals a and b, a divides b, written $a|b$, means that $b = ac$ for some integral ideal c.

2. Extensions of Dedekind Domains

Let L/K be a field extension of finite degree n. An element $x \in L$ is integral over A provided that x is a root of a monic polynomial in A[X]. The elements of L which are integral over A form a subring $B \subseteq L$ called the integral closure of A in L. (For details see [31] or [20].) It is easy to see that for any $x \in L$ there is an $a \in A$ such that $ax \in B$; for example, one can choose a so that it clears the denominators of the coefficients of the minimal polynomial of x over

K. In particular, L is the quotient field of B, and one can always find a basis for L/K consisting of elements of B. A very important result in the theory of Dedekind domains is the following:

(2.1) Theorem. The integral closure of a Dedekind domain in a finite extension of its quotient field is a Dedekind domain.

If L/K is a separable extension, then B is not only a Dedekind domain, but it is also finitely generated as an A-module. This is proved in [31]; for a proof of the theorem see [37] or [17].

Let p be a nonzero prime of A. Being an ideal in the Dedekind domain B, pB has a factorization into prime ideals, $pB = P_1^{e_1}P_2^{e_2}\cdots P_g^{e_g}$. For each i, B/P_i is an extension of the field A/p whose degree, denoted f_i or $f(P_i/p)$, is at most n. When L/K is separable, $\Sigma_{i=1}^{g} e_i f_i = n$. This is proved by Samuel [31]. In general $\Sigma e_i f_i \le n$; see Chapter 2, Section 4 of this text. The prime P is called ramified in L/K if it occurs with exponent $e > 1$ in pB ($p = P \cap A$), P is called unramified in L/K if $e = 1$ and B/P is a separable extension of A/p. (The requirement of separability is related to the different ideal, which will be defined in Chapter 5. Especially see exercise 17 of Chapter 5.) Finally, P is totally ramified in L/K if $pB = P^n$. In Section 4, there is a more detailed study, including proofs, of Galois extensions L/K.

3. Algebraic Numbers

An algebraic number field is a finite extension of the rational field; such an extension is necessarily separable. The ring of integers in a number field K is the integral closure of the rational integers in K; it will usually be denoted A. Because $\mathbb{Z}$ is a principal ideal domain, A has a $\mathbb{Z}$ basis. Such a basis is called an integral basis of K. If L/K is a finite extension, then the integral closure B of A in L is a Dedekind domain and coincides with the ring of integers of L. B may or may not have a basis as an A-module. If it does, this basis is called a relative integral basis. The adjective "relative" (relative norm, relative degree, etc.) is used when the base field is a number field; when the adjective "absolute" is used the base field is Q. Usually norms and traces are subscripted (e.g., $N_{L/K}$, $tr_{L/K}$) unless the context defys misunderstanding. The unadorned N denotes the absolute norm of an algebraic number or of an ideal.

The concept of discriminant is very important in algebraic number theory. Let $x_1,\ldots,x_n \in L$; the discriminant $d_{L/K}(x_1,\ldots,x_n)$ is defined as the determinant of the matrix whose (i,j)-entry is $tr_{L/K}(x_i x_j)$. If the x_i's are not linearly independent over K, then their discriminant is zero. The discriminant ideal, denoted $d_{L/K}$, is the ideal in A generated by the elements $d_{L/K}(x_1,\ldots,x_n)$ as the x_i range over B ($n = [L:K]$). In this book discriminants are always denoted by lower case letters, elements by Roman, and ideals by script. The corresponding upper case notations refer to the different. Keep in mind that the discriminant belongs to the "lower" field K; differents will be seen to belong to the "upper" field L. When the base field is Q, the discriminant notation is usually shortened to $d_K(x_1,\ldots,x_n)$ or even $d(x_1,\ldots,x_n)$. In the absolute case, the discriminant ideal is generated by the discriminant of an integral basis. Changing the integral basis does not alter the generator. Consequently, for extensions of Q, one usually uses the finer invariant d_K, which equals discriminant of any integral basis of K instead of the ideal (d_K). Finally, $d_{L/K}(1,\theta,\theta^2,\ldots,\theta^{n-1})$ is usually shortened to $d_{L/K}(\theta)$ or, in the absolute case, $d_K(\theta)$.

The reader should be aware that $d_{L/K}(x_1,\ldots,x_n)$ is equal to the square of the determinant of the matrix with (i,j)-entry $\sigma_i(x_j)$ where $\sigma_1,\ldots,\sigma_n$ are the embeddings of L into a normal extension of K. A simple consequence of this is the fact that if L/K is normal of odd degree, then $d_{L/K}(x_1,\ldots,x_n)$ is a square in K. The importance of the discriminant in algebraic number theory is displayed in the following theorem which will be proved in Chapter 5.

(3.1) Theorem. Let L/K be a finite extension of number fields. A prime p of K has a ramified factor in L if and only if p divides $d_{L/K}$.

Let I(K) denote the group of (fractional) ideals of K. Every element of K generates a principal ideal, and these principal ideals constitute a subgroup of I(K) denoted P(K). The quotient I(K)/P(K) is the ideal class group of K.

(3.2) Theorem. The ideal class group of an algebraic number field is finite.

The group P(K) is isomorphic to the quotient $K^{\cdot}/E(K)$ where E(K) is the group of units in A (which are usually called the units of K). The structure of E(K) is described in the following famous theorem of Dirichlet:

(3.3) Dirichlet's Unit Theorem. Let K be an algebraic number field, let r_1 be the number of embeddings of K in $\mathbb{R}$, and let r_2 be the number of conjugate pairs of embeddings of K in $\mathbb{C}$. Then E(K) is isomorphic to the product of the (finite) group of roots of unity in K by a free abelian group of rank $r_1 + r_2 - 1$.

Theorems (3.2) and (3.3) are proved in most books about algebraic number theory. Samuel's exposition in [31] is especially recommended. Minkowski proved in [27] that if K/Q is normal, then there is a system of $r_1 + r_2$ conjugate units in A of which any $r_1 + r_2 - 1$ are linearly independent over $\mathbb{Z}$. However, his result offers no hint for deciding whether these units generate E(K) modulo the roots of unity.

4. Theory of Ramification in Galois Extensions

Throughout this section, A is a Dedekind domain, L/K is a finite Galois extension, and B is the integral closure of A in L. The "number field case" is that in which A is the ring of integers in a number field K. Let G = Gal(L/K) and n = [L:K].

(4.1) Proposition. Let p be a nonzero prime of A, and let $P_1,\ldots,P_g$ be the primes of B above p. Then G permutes $\{P_1,\ldots,P_g\}$ transitively.

Proof: Let $P|p$. For any $\sigma \in G$, $\sigma(P)|\sigma(p)$. As $\sigma(p) = p$, it follows that G permutes $\{P_i : i = 1,\ldots,g\}$. Suppose now that $Q|p$ and that Q is not a conjugate of P. Say $P_1,\ldots,P_r$ are the distinct