Graduate Texts in Mathematics

Serge Lang

# Algebraic Number Theory

代数数论［英］

Springer-Verlag
World Publishing Corp

Serge Lang

# Algebraic Number Theory

Springer-Verlag
World Publishing Corp

Serge Lang
Department of Mathematics
Yale University
New Haven, CT 06520
U.S.A.

AMS Classifications: 1065, 1250

With 7 Illustrations

Library of Congress Cataloging in Publication Data
Lang, Serge
Algebraic number theory.
(Graduate texts in mathematics; 110)
Bibliography: p.
Includes index.
1. Algebraic number theory. 2. Class field theory.
I. Title. II. Series.
QA247.L32 1986 512'.74 86-6627

ISBN 7-5062-0733-8

ISBN 0-387-96375-8 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-96375-8 Springer-Verlag Berlin Heidelberg New York

# Foreword

The present book gives an exposition of the classical basic algebraic and analytic number theory and supersedes my *Algebraic Numbers*, including much more material, e.g. the class field theory on which I make further comments at the appropriate place later.

For different points of view, the reader is encouraged to read the collection of papers from the Brighton Symposium (edited by Cassels-Frohlich), the Artin-Tate notes on class field theory, Weil's book on *Basic Number Theory*, Borevich-Shafarevich's *Number Theory*, and also older books like those of Weber, Hasse, Hecke, and Hilbert's *Zahlbericht*. It seems that over the years, everything that has been done has proved useful, theoretically or as examples, for the further development of the theory. Old, and seemingly isolated special cases have continuously acquired renewed significance, often after half a century or more.

The point of view taken here is principally global, and we deal with local fields only incidentally. For a more complete treatment of these, cf. Serre's book *Corps Locaux*. There is much to be said for a direct global approach to number fields. Stylistically, I have intermingled the ideal and idelic approaches without prejudice for either. I also include two proofs of the functional equation for the zeta function, to acquaint the reader with different techniques (in some sense equivalent, but in another sense, suggestive of very different moods). Even though a reader will prefer some techniques over alternative ones, it is important at least that he should be aware of all the possibilities.

*New York*
*June 1970*

SERGE LANG

# Prerequisites

Chapters I through VII are self-contained, assuming only elementary algebra, say at the level of Galois theory.

Some of the chapters on analytic number theory assume some analysis. Chapter XIV assumes Fourier analysis on locally compact groups. Chapters XV through XVII assume only standard analytical facts (we even prove some of them), except for one allusion to the Plancherel formula in Chapter XVII.

In the course of the Brauer-Siegel theorem, we use the conductor-discriminant formula, for which we refer to Artin-Tate where a detailed proof is given. At that point, the use of this theorem is highly technical, and is due to the fact that one does not know that the zeros of the zeta function don't occur in a small interval to the left of 1. If one knew this, the proof would become only a page long, and the $L$-series would not be needed at all. We give Siegel's original proof for that in Chapter XIII.

My *Algebra* gives more than enough background for the present book. In fact, *Algebra* already contains a good part of the theory of integral extensions, and valuation theory, redone here in Chapters I and II. Furthermore, *Algebra* also contains whatever will be needed of group representation theory, used in a couple of isolated instances for applications of the class field theory, or to the Brauer-Siegel theorem.

The word **ring** will always mean commutative ring without zero divisors and with unit element (unless otherwise specified).

If $K$ is a field, then $K^*$ denotes its multiplicative group, and $\bar{K}$ its algebraic closure. Occasionally, a bar is also used to denote reduction modulo a prime ideal.

We use the $o$ and $O$ notation. If $f$, $g$ are two functions of a real variable, and $g$ is always $\geqq 0$, we write $f = O(g)$ if there exists a constant $C > 0$ such that $|f(x)| \leqq Cg(x)$ for all sufficiently large $x$. We write $f = o(g)$ if $\lim_{x\to\infty} f(x)/g(x) = 0$. We write $f \sim g$ if $\lim_{x\to\infty} f(x)/g(x) = 1$.

# Contents

## Part One

## General Basic Theory

### Chapter I

### Algebraic Integers

### Chapter II

### Completions

### Chapter III

### The Different and Discriminant

# Part Two
# Class Field Theory

## Chapter IX

### Norm Index Computations

## Chapter X

### The Artin Symbol, Reciprocity Law, and Class Field Theory

## Chapter XI

### The Existence Theorem and Local Class Field Theory

## Chapter XII

### *L*-series Again

## Part Three

## Analytic Theory

### Chapter XIII

### Functional Equation of the Zeta Function, Hecke's Proof

### Chapter XIV

### Functional Equation, Tate's Thesis

### Chapter XV

### Density of Primes and Tauberian Theorem

### Chapter XVI

### The Brauer-Siegel Theorem

## Chapter XVII

## Explicit Formulas

# PART ONE

# BASIC THEORY

CHAPTER I

# Algebraic Integers

This chapter describes the basic aspects of the ring of algebraic integers in a number field (always assumed to be of finite degree over the rational numbers $\mathbf{Q}$). This includes the general prime ideal structure.

Some proofs are given in a more general context, but only when they could not be made shorter by specializing the hypothesis to the concrete situation we have in mind. It is not our intention to write a treatise on commutative algebra.

## *§1. Localization*

Let $A$ be a ring. By a **multiplicative subset** of $A$ we mean a subset containing 1 and such that, whenever two elements $x$, $y$ lie in the subset, then so does the product $xy$. We shall also assume throughout that 0 does not lie in the subset.

Let $K$ be the quotient field of $A$, and let $S$ be a multiplicative subset of $A$. By $S^{-1}A$ we shall denote the set of quotients $x/s$ with $x$ in $A$ and $s$ in $S$. It is a ring, and $A$ has a canonical inclusion in $S^{-1}A$.

If $M$ is an $A$-module contained in some field $L$ (containing $K$), then $S^{-1}M$ denotes the set of elements $v/s$ with $v \in M$ and $s \in S$. Then $S^{-1}M$ is an $S^{-1}A$-module in the obvious way. We shall sometimes consider the case when $M$ is a ring containing $A$ as subring.

Let $\mathfrak{p}$ be a prime ideal of $A$ (by definition, $\mathfrak{p} \neq A$). Then the complement of $\mathfrak{p}$ in $A$, denoted by $A - \mathfrak{p}$, is a multiplicative subset $S = S_{\mathfrak{p}}$ of $A$, and we shall denote $S^{-1}A$ by $A_{\mathfrak{p}}$.

A **local ring** is a ring which has a unique maximal ideal. If $\mathfrak{o}$ is such a ring, and $\mathfrak{m}$ its maximal ideal, then any element $x$ of $\mathfrak{o}$ not lying in $\mathfrak{m}$ must be a unit, because otherwise, the principal ideal $x\mathfrak{o}$ would be contained in a maximal ideal unequal to $\mathfrak{m}$. Thus $\mathfrak{m}$ is the set of non-units of $\mathfrak{o}$.

The ring $A_{\mathfrak{p}}$ defined above is a local ring. As can be verified at once, its maximal ideal $\mathfrak{m}_{\mathfrak{p}}$ consists of the quotients $x/s$, with $x$ in $\mathfrak{p}$ and $s$ in $A$ but not in $\mathfrak{p}$.

We observe that $\mathfrak{m}_{\mathfrak{p}} \cap A = \mathfrak{p}$. The inclusion $\supset$ is clear. Conversely, if an element $y = x/s$ lies in $\mathfrak{m}_{\mathfrak{p}} \cap A$ with $x \in \mathfrak{p}$ and $s \in S$, then $x = sy \in \mathfrak{p}$ and $s \notin \mathfrak{p}$. Hence $y \in \mathfrak{p}$.

Let $A$ be a ring and $S$ a multiplicative subset. Let $\mathfrak{a}'$ be an ideal of $S^{-1}A$. Then

$$\mathfrak{a}' = S^{-1}(\mathfrak{a}' \cap A).$$

The inclusion $\supset$ is clear. Conversely, let $x \in \mathfrak{a}'$. Write $x = a/s$ with some $a \in A$ and $s \in S$. Then $sx \in \mathfrak{a}' \cap A$, whence $x \in S^{-1}(\mathfrak{a}' \cap A)$.

Under multiplication by $S^{-1}$, the multiplicative system of ideals of $A$ is mapped homomorphically onto the multiplicative system of ideals of $S^{-1}A$. This is another way of stating what we have just proved. If $\mathfrak{a}$ is an ideal of $A$ and $S^{-1}\mathfrak{a}$ is the unit ideal, then it is clear that $\mathfrak{a} \cap S$ is not empty, or as we shall also say, $\mathfrak{a}$ **meets** $S$.

## §2. *Integral closure*

Let $A$ be a ring and $x$ an element of some field $L$ containing $A$. We shall say that $x$ is **integral** over $A$ if either one of the following conditions is satisfied.

**INT 1.** *There exists a finitely generated non-zero A-module $M \subset L$ such that $xM \subset M$.*

**INT 2.** *The element $x$ satisfies an equation*

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

*with coefficients $a_i \in A$, and an integer $n \geqq 1$.* (Such an equation will be called an **integral equation.**)

The two conditions are actually equivalent. Indeed, assume **INT 2.** The module $M$ generated by $1, x, \ldots, x^{n-1}$ is mapped into itself by the element $x$. Conversely, assume there exists $M = \langle v_1, \ldots, v_n \rangle$ such that $xM \subset M$, and $M \neq 0$. Then

$$\begin{aligned} xv_1 &= a_{11}v_1 + \cdots + a_{1n}v_n \\ &\vdots \\ xv_n &= a_{n1}v_1 + \cdots + a_{nn}v_n \end{aligned}$$

with coefficients $a_{ij}$ in $A$. Transposing $xv_1, \ldots, xv_n$ to the right-hand side of these equations, we conclude that the determinant

$$\begin{vmatrix} x - a_{11} & & & -a_{ij} \\ & x - a_{22} & & \\ -a_{ij} & & \ddots & \\ & & & x - a_{nn} \end{vmatrix}$$

is equal to 0. In this way we get an integral equation for $x$ over $A$.

***Proposition 1.*** *Let $A$ be a ring, $K$ its quotient field, and $x$ algebraic over $K$. Then there exists an element $c \neq 0$ of $A$ such that $cx$ is integral over $A$.*

*Proof.* There exists an equation

$$a_n x^n + \cdots + a_0 = 0$$

with $a_i \in A$ and $a_n \neq 0$. Multiply it by $a_n^{n-1}$. Then

$$(a_n x)^n + \cdots + a_0 a_n^{n-1} = 0$$

is an integral equation for $a_n x$ over $A$.

Let $B$ be a ring containing $A$. We shall say that $B$ is **integral** over $A$ if every element of $B$ is integral over $A$.

***Proposition 2.*** *If $B$ is integral over $A$ and finitely generated as an $A$-algebra, then $B$ is a finitely generated $A$-module.*

*Proof.* We may prove this by induction on the number of ring generators, and thus we may assume that $B = A[x]$ for some element $x$ integral over $A$. But we have already seen that our assertion is true in that case.

***Proposition 3.*** *Let $A \subset B \subset C$ be three rings. If $B$ is integral over $A$ and $C$ is integral over $B$, then $C$ is integral over $A$.*

*Proof.* Let $x \in C$. Then $x$ satisfies an integral equation

$$x^n + b_{n-1}x^{n-1} + \cdots + b_0 = 0$$

with $b_i \in B$. Let $B_1 = A[b_0, \ldots, b_{n-1}]$. Then $B_1$ is a finitely generated $A$-module by Proposition 2, and $B_1[x]$ is a finitely generated $B_1$-module, whence a finitely generated $A$-module. Since multiplication by $x$ maps $B_1[x]$ into itself, it follows that $x$ is integral over $A$.

***Proposition 4.*** *Let $A \subset B$ be two rings, and $B$ integral over $A$. Let $\sigma$ be a homomorphism of $B$. Then $\sigma(B)$ is integral over $\sigma(A)$.*

*Proof.* Apply $\sigma$ to an integral equation satisfied by any element $x$ of $B$. It will be an integral equation for $\sigma(x)$ over $\sigma(A)$.

The above proposition is used frequently when $\sigma$ is an isomorphism and is particularly useful in Galois theory.

***Proposition 5.*** *Let $A$ be a ring contained in a field $L$. Let $B$ be the set of elements of $L$ which are integral over $A$. Then $B$ is a ring, called the* **integral closure** *of $A$ in $L$.*

*Proof.* Let $x$, $y$ lie in $B$, and let $M$, $N$ be two finitely generated $A$-modules such that $xM \subset M$ and $yN \subset N$. Then $MN$ is finitely generated, and is mapped into itself by multiplication with $x \pm y$ and $xy$.

***Corollary.*** *Let $A$ be a ring, $K$ its quotient field, and $L$ a finite separable extension of $K$. Let $x$ be an element of $L$ which is integral over $A$. Then the norm and trace of $x$ from $L$ to $K$ are integral over $A$, and so are the coefficients of the irreducible polynomial satisfied by $x$ over $K$.*

*Proof.* For each isomorphism $\sigma$ of $L$ over $K$, $\sigma x$ is integral over $A$. Since the norm is the product of $\sigma x$ over all such $\sigma$, and the trace is the sum of $\sigma x$ over all such $\sigma$, it follows that they are integral over $A$. Similarly, the coefficients of the irreducible polynomial are obtained from the elementary symmetric functions of the $\sigma x$, and are therefore integral over $A$.

A ring $A$ is said to be **integrally closed in a field** $L$ if every element of $L$ which is integral over $A$ in fact lies in $A$. It is said to be **integrally closed** if it is integrally closed in its quotient field.

***Proposition 6.*** *Let $A$ be a Noetherian ring, integrally closed. Let $L$ be a finite separable extension of its quotient field $K$. Then the integral closure of $A$ in $L$ is finitely generated over $A$.*

*Proof.* It will suffice to show that the integral closure of $A$ is contained in a finitely generated $A$-module, because $A$ is assumed to be Noetherian.

Let $w_1, \ldots, w_n$ be a linear basis of $L$ over $K$. After multiplying each $w_i$ by a suitable element of $A$, we may assume without loss of generality that the $w_i$ are integral over $A$ (Proposition 1). The trace Tr from $L$ to $K$ is a $K$-linear map of $L$ into $K$, and is non-degenerate (i.e. there exists an element $x \in L$ such that $\mathrm{Tr}(x) \neq 0$). If $\alpha$ is a non-zero element of $L$, then the function $\mathrm{Tr}(\alpha x)$ on $L$ is an element of the dual space of $L$ (as $K$-vector space), and induces a homomorphism of $L$ into its dual space. Since the kernel is trivial, it follows that $L$ is isomorphic to its dual under the bilinear form

$$(x, y) \mapsto \mathrm{Tr}(xy).$$

Let $w_1', \dots, w_n'$ be the dual basis of $w_1, \dots, w_n$, so that

$$\operatorname{Tr}(w_i'w_j) = \delta_{ij}.$$

Let $c \neq 0$ be an element of $A$ such that $cw_i'$ is integral over $A$. Let $z$ be in $L$, integral over $A$. Then $zcw_i'$ is integral over $A$, and so is $\operatorname{Tr}(czw_i')$ for each $i$. If we write

$$z = b_1w_1 + \cdots + b_nw_n$$

with coefficients $b_i \in K$, then

$$\operatorname{Tr}(czw_i') = cb_i,$$

and $cb_i \in A$ because $A$ is integrally closed. Hence $z$ is contained in

$$Ac^{-1}w_1 + \cdots + Ac^{-1}w_n.$$

Since $z$ was selected arbitrarily in the integral closure of $A$ in $L$, it follows that this integral closure is contained in a finitely generated $A$-module, and our proof is finished.

***Proposition 7.*** *If $A$ is a unique factorization domain, then $A$ is integrally closed.*

*Proof.* Suppose that there exists a quotient $a/b$ with $a, b \in A$ which is integral over $A$, and a prime element $p$ in $A$ which divides $b$ but not $a$. We have, for some integer $n \geqq 1$,

$$(a/b)^n + a_{n-1}(a/b)^{n-1} + \cdots + a_0 = 0,$$

whence

$$a^n + a_{n-1}ba^{n-1} + \cdots + a_0b^n = 0.$$

Since $p$ divides $b$, it must divide $a^n$, and hence must divide $a$, contradiction.

***Theorem 1.*** *Let $A$ be a principal ideal ring, and $L$ a finite separable extension of its quotient field, of degree $n$. Let $B$ be the integral closure of $A$ in $L$. Then $B$ is a free module of rank $n$ over $A$.*

*Proof.* As a module over $A$, the integral closure is torsion-free, and by the general theory of principal ideal rings, any torsion-free finitely generated module is in fact a free module. It is obvious that the rank is equal to the degree $[L:K]$.

Theorem 1 is applied to the ring of ordinary integers $\mathbf{Z}$. A finite extension of the rational numbers $\mathbf{Q}$ is called a **number field.** The integral closure of $\mathbf{Z}$ in a number field $K$ is called the ring of **algebraic integers** of that field, and is denoted by $\mathfrak{o}_K$.