Graduate Texts in Mathematics

Serge Lang

Algebraic Number Theory

Second Edition

代数数论 第2版

Springer-Verlag
世界图书出版公司

Serge Lang

Algebraic Number Theory

Second Edition

Springer

世界图书出版公司

书名：Algebraic Number Theory 2nd ed.
作者：S. lang
中译名：代数数论 第 2 版
出版者：世界图书出版公司北京公司
印刷者：北京世图印刷厂
发行：世界图书出版公司北京公司（北京朝内大街 137 号　100010）
联系电话：010-64015659, 64038347
电子信箱：kjsk@vip.sina.com
开本：24 开　　印张：15.5
出版年代：2003 年 11 月
书号：7-5062-6562-1/ O · 424
版权登记：图字:01-2003-7950
定价：48.00 元

Graduate Texts in Mathematics 110

Springer
New York
Berlin
Heidelberg
Barcelona
Budapest
Hong Kong
London
Milan
Paris
Santa Clara
Singapore
Tokyo

Books of Related Interest by Serge Lang

Linear Algebra, Third Edition
1987, ISBN 96412-6

Undergraduate Algebra, Second Edition
1990, ISBN 97279-X

Complex Analysis, Third Edition
1993, ISBN 97886-0

Real and Functional Analysis, Third Edition
1993, ISBN 94001-4

Introduction to Algebraic and Abelian Functions, Second Edition
1982, ISBN 90710-6

Cyclotomic Fields I and II
1990, ISBN 96671-4

Other Books by Lang Published by Springer-Verlag

Introduction to Arakelov Theory • Riemann-Roch Algebra (with William Fulton) • Complex Multiplication • Introduction to Modular Forms • Modular Units (with Daniel Kubert) • Fundamentals of Diophantine Geometry • Introduction to Complex Hyperbolic Spaces • Elliptic Functions • Number Theory III • Algebraic Number Theory • $SL_2(R)$ • Abelian Varieties • Differential and Riemannian Manifolds • Undergraduate Analysis • Elliptic Curves: Diophantine Analysis • Introduction to Linear Algebra • Calculus of Several Variables • First Course in Calculus • Basic Mathematics • Geometry: A High School Course (with Gene Murrow) • Math! Encounters with High School Students • The Beauty of Doing Mathematics • THE FILE

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

Preface for the Second Edition

The principal change in this new edition is a complete rewriting of Chapter XVII on the Explicit Formulas. Otherwise, I have made a few additions, and a number of corrections. The need for them was pointed out to me by several people, but I am especially indebted to Keith Conrad for the list he provided for me as a result of a very careful reading of the book.

New Haven, 1994 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 $\overline{K}$ 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

1. Localization . . . 3
2. Integral closure . . . 4
3. Prime ideals . . . 8
4. Chinese remainder theorem . . . 11
5. Galois extensions . . . 12
6. Dedekind rings . . . 18
7. Discrete valuation rings . . . 22
8. Explicit factorization of a prime . . . 27
9. Projective modules over Dedekind rings . . . 29

Chapter II

Completions

1. Definitions and completions . . . 31
2. Polynomials in complete fields . . . 41
3. Some filtrations . . . 45
4. Unramified extensions . . . 48
5. Tamely ramified extensions . . . 51

Chapter III

The Different and Discriminant

1. Complementary modules . . . 57
2. The different and ramification . . . 62
3. The discriminant . . . 64

Chapter IV

Cyclotomic Fields

1. Roots of unity 71
2. Quadratic fields 76
3. Gauss sums 82
4. Relations in ideal classes 96

Chapter V

Parallelotopes

1. The product formula 99
2. Lattice points in parallelotopes 110
3. A volume computation 116
4. Minkowski's constant 119

Chapter VI

The Ideal Function

1. Generalized ideal classes 123
2. Lattice points in homogeneously expanding domains 128
3. The number of ideals in a given class 129

Chapter VII

Ideles and Adeles

1. Restricted direct products 137
2. Adeles 139
3. Ideles 140
4. Generalized ideal class groups; relations with idele classes 145
5. Embedding of k_v^* in the idele classes 151
6. Galois operation on ideles and idele classes 152

Chapter VIII

Elementary Properties of the Zeta Function and *L*-series

1. Lemmas on Dirichlet series 155
2. Zeta function of a number field 159
3. The *L*-series 162
4. Density of primes in arithmetic progressions 166
5. Faltings' finiteness theorem 170

Part Two
Class Field Theory

Chapter IX
Norm Index Computations

1. Algebraic preliminaries . . . 179
2. Exponential and logarithm functions . . . 185
3. The local norm index . . . 187
4. A theorem on units . . . 190
5. The global cyclic norm index . . . 193
6. Applications . . . 195

Chapter X
The Artin Symbol, Reciprocity Law, and Class Field Theory

1. Formalism of the Artin symbol . . . 197
2. Existence of a conductor for the Artin symbol . . . 200
3. Class fields . . . 206

Chapter XI
The Existence Theorem and Local Class Field Theory

1. Reduction to Kummer extensions . . . 213
2. Proof of the existence theorem . . . 215
3. The complete splitting theorem . . . 217
4. Local class field theory and the ramification theorem . . . 219
5. The Hilbert class field and the principal ideal theorem . . . 224
6. Infinite divisibility of the universal norms . . . 226

Chapter XII
L-series Again

1. The proper abelian *L*-series . . . 229
2. Artin (non-abelian) *L*-series . . . 232
3. Induced characters and *L*-series contributions . . . 236

Part Three
Analytic Theory

Chapter XIII

Functional Equation of the Zeta Function, Hecke's Proof

1. The Poisson summation formula 245
2. A special computation 250
3. Functional equation 253
4. Application to the Brauer-Siegel theorem 260
5. Applications to the ideal function 262
Appendix: Other applications 273

Chapter XIV

Functional Equation, Tate's Thesis

1. Local additive duality 276
2. Local multiplicative theory 278
3. Local functional equation 280
4. Local computations 282
5. Restricted direct products 287
6. Global additive duality and Riemann-Roch theorem 289
7. Global functional equation 292
8. Global computations 297

Chapter XV

Density of Primes and Tauberian Theorem

1. The Dirichlet integral 303
2. Ikehara's Tauberian theorem 304
3. Tauberian theorem for Dirichlet series 310
4. Non-vanishing of the L-series 312
5. Densities 315

Chapter XVI

The Brauer-Siegel Theorem

1. An upper estimate for the residue 322
2. A lower bound for the residue 323
3. Comparison of residues in normal extensions 325
4. End of the proofs 327
Appendix: Brauer's lemma 328

CHAPTER XVII

Explicit Formulas

1. Weierstrass factorization of the L-series 331
2. An estimate for ξ'/ξ 333
3. The Weil formula 337
4. The basic sum and the first part of its evaluation 344
5. Evaluation of the sum: Second part 348

Bibliography 353

Index 355

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