Selected Titles in This Series

24 Helmut Koch, Number Theory: Algebraic Numbers and Functions, 2000
23 Alberto Candel and Lawrence Conlon, Foliations I, 2000
21 John B. Conway, A course in operator theory, 2000
20 Robert E. Gompf and András I. Stipsicz, 4-manifolds and Kirby calculus, 1999
19 Lawrence C. Evans, Partial differential equations, 1998
18 Winfried Just and Martin Weese, Discovering modern set theory. II: Set-theoretic tools for every mathematician, 1997
17 Henryk Iwaniec, Topics in classical automorphic forms, 1997
14 Elliott H. Lieb and Michael Loss, Analysis, 1997
12 N. V. Krylov, Lectures on elliptic and parabolic equations in Hölder spaces, 1996
11 Jacques Dixmier, Enveloping algebras, 1996 Printing
10 Barry Simon, Representations of finite and compact groups, 1996
9 Dino Lorenzini, An invitation to arithmetic geometry, 1996
8 Winfried Just and Martin Weese, Discovering modern set theory. I: The basics, 1996
7 Gerald J. Janusz, Algebraic number fields, second edition, 1996
6 Jens Carsten Jantzen, Lectures on quantum groups, 1996
5 Rick Miranda, Algebraic curves and Riemann surfaces, 1995
4 Russell A. Gordon, The integrals of Lebesgue, Denjoy, Perron, and Henstock, 1994
2 Jack Graver, Brigitte Servatius, and Herman Servatius, Combinatorial rigidity, 1993
1 Ethan Akin, The general topology of dynamical systems, 1993
This page intentionally left blank
Number Theory
Algebraic Numbers
and Functions
This page intentionally left blank
Number Theory
Algebraic Numbers and Functions

Helmut Koch

Translated by
David Kramer

Graduate Studies
in Mathematics
Volume 24

American Mathematical Society
Providence, Rhode Island
EDITORIAL COMMITTEE
James Humphreys (Chair)
David Saltman
David Sattinger
Ronald Stern

Originally published in the German language by Friedr. Vieweg & Sohn
Verlagsgesellschaft mbH, D-65189 Wiesbaden, Germany, under the title “Helmut Koch:
Zahlentheorie. Algebraische Zahlen und Funktionen. 1. Auflage (1st edition)”.
© by Friedr. Vieweg & Sohn Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1997
Translated from the German by David Kramer


ABSTRACT. The primary goal of this book is to present the essential elements of algebraic number
theory, including the theory of normal extensions up through a glimpse of class field theory.
Following the example set by Kronecker, Weber, Hilbert and Artin, algebraic functions are handled
on an equal footing as algebraic numbers. This is done on the one hand to demonstrate the analogy
between number fields and function fields, which is especially strong in the case where the ground
field is a finite field. On the other hand, in this way one obtains an introduction to the theory of
‘higher congruences’ as an important element of ‘arithmetic geometry’.

The book is suitable for two one-semester courses, leading from basic algebraic number theory
up to the beginning of class field theory.

Library of Congress Cataloging-in-Publication Data
Koch, Helmut, 1932-
[Zahlentheorie. English]
Number theory : algebraic numbers and functions / Helmut Koch.
   p. cm. — (Graduate studies in mathematics, ISSN 1065-7339 ; v. 24)
   Includes bibliographical references and index.
   ISBN 0-8218-2054-0 (acid-free paper)
   1. Number theory. I. Title. II. Series.
QA241. K67713   2000
512'.7—dc21   00-022320

Copying and reprinting. Individual readers of this publication, and nonprofit libraries
acting for them, are permitted to make fair use of the material, such as to copy a chapter for use
in teaching or research. Permission is granted to quote brief passages from this publication in
reviews, provided the customary acknowledgment of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication
is permitted only under license from the American Mathematical Society. Requests for such
permission should be addressed to the Assistant to the Publisher, American Mathematical Society,
P.O. Box 6248, Providence, Rhode Island 02940-6248. Requests can also be made by e-mail to
reprint-permission@ams.org.

© 2000 by the American Mathematical Society. All rights reserved.
The American Mathematical Society retains all rights
except those granted to the United States Government.
Printed in the United States of America.
The paper used in this book is acid-free and falls within the guidelines
established to ensure permanence and durability.
Visit the AMS home page at URL: http://www.ams.org/

10 9 8 7 6 5 4 3 2 1    05 04 03 02 01 00
Contents

Preface xi
Translator’s Note xvi
Notation xvii
List of Symbols xvii

Chapter 1. Introduction 1
1.1. Pythagorean Triples 1
1.2. Pell’s Equation 3
1.3. Fermat’s Last Theorem 4
1.4. Congruences 8
1.5. Public Key Cryptology 11
1.6. Quadratic Residues 12
1.7. Prime Numbers 22
1.8. The Prime Number Theorem 26
1.9. Exercises 31

Chapter 2. The Geometry of Numbers 35
2.1. Binary Quadratic Forms 35
2.2. Complete Decomposable Forms of Degree $n$ 37
2.3. Modules and Orders 39
2.4. Complete Modules in Finite Extensions of $P$ 43
2.5. The Integers of a Quadratic Field 45
2.6. Further Examples of Determining a $\mathbb{Z}$-Basis for the Ring of Integers of a Number Field 46
2.7. The Finiteness of the Class Number 47
2.8. The Group of Units 48
2.9. The Start of the Proof of Dirichlet's Unit Theorem 50
2.10. The Rank of $1(E)$ 51
2.11. The Regulator of an Order 55
2.12. The Lattice Point Theorem 55
2.13. Minkowski's Geometry of Numbers 57
2.14. Application to Complete Decomposable Forms 62
2.15. Exercises 64

Chapter 3. Dedekind's Theory of Ideals 65
3.1. Basic Definitions 66
3.2. The Main Theorem of Dedekind's Theory of Ideals 68
3.3. Consequences of the Main Theorem 71
3.4. The Converse of the Main Theorem 73
3.5. The Norm of an Ideal 74
3.6. Congruences 76
3.7. Localization 78
3.8. The Decomposition of a Prime Ideal in a Finite Separable Extension 80
3.9. The Class Group of an Algebraic Number Field 84
3.10. Relative Extensions 88
3.11. Geometric Interpretation 93
3.12. Different and Discriminant 94
3.13. Exercises 101
Chapter 4. Valuations 103
4.1. Fields with Valuation 104
4.2. Valuations of the Field of Rational Numbers and of a Field of Rational Functions 110
4.3. Completion 112
4.4. Complete Fields with Respect to a Discrete Valuation 114
4.5. Extension of a Valuation of a Complete Field to a Finite Extension 121
4.6. Finite Extensions of a Complete Field with a Discrete Valuation 124
4.7. Complete Fields with a Discrete Valuation and Finite Residue Class Field 129
4.8. Extension of the Valuation of an Arbitrary Field to a Finite Extension 132
4.9. Arithmetic in the Compositum of Two Field Extensions 137
4.10. Exercises 137

Chapter 5. Algebraic Functions of One Variable 141
5.1. Algebraic Function Fields 142
5.2. The Places of an Algebraic Function Field 144
5.3. The Function Space Associated to a Divisor 149
5.4. Differentials 154
5.5. Extensions of the Field of Constants 158
5.6. The Riemann–Roch Theorem 160
5.7. Function Fields of Genus 0 164
5.8. Function Fields of Genus 1 167
5.9. Exercises 169

Chapter 6. Normal Extensions 171
6.1. Decomposition Group and Ramification Groups 172
6.2. A New Proof of Dedekind’s Theorem on the Different 176
6.3. Decomposition of Prime Ideals in an Intermediate Field 178
6.4. Cyclotomic Fields 180
6.5. The First Case of Fermat's Last Theorem 184
6.6. Localization 188
6.7. Upper Numeration of the Ramification Group 190
6.8. Kummer Extensions 195
6.9. Exercises 199

Chapter 7. L-Series 203
7.1. From the Riemann ζ-Function to the Hecke L-Series 204
7.2. Normalized Valuations 207
7.3. Adeles 209
7.4. Ideles 212
7.5. Idele Class Group and Ray Class Group 214
7.6. Hecke Characters 217
7.7. Analysis on Local Additive Groups 219
7.8. Analysis on the Adele Group 223
7.9. The Multiplicative Group of a Local Field 227
7.10. The Local Functional Equation 230
7.11. Calculation of ρ(c) for K = ℝ 232
7.12. Calculation of ρ(c) for K = ℂ 234
7.13. Computation of the ρ-Factors for a Nonarchimedean Field 236
7.14. Relations Among the ρ-Factors 239
7.15. Analysis on the Idele Group 240
7.16. Global Zeta Functions 243
7.17. The Dedekind Zeta Function 247
7.18. Hecke L-Series 251
7.19. Congruence Zeta Functions 252
7.20. Exercises 257

Chapter 8. Applications of Hecke L-Series 259
8.1. The Decomposition of Prime Numbers in Algebraic Number Fields 259
8.2. The Nonvanishing of the L-Series at s = 1 262
8.3. The Distribution of Prime Ideals in an Algebraic Number Field  266
8.4. The Generalized Riemann Hypothesis  270
8.5. Exercises  273

Chapter 9. Quadratic Number Fields  275
9.1. Quadratic Forms and Orders in Quadratic Number Fields  275
9.2. The Class Number of Imaginary Quadratic Number Fields  282
9.3. Continued Fractions  285
9.4. Periodic Continued Fractions  290
9.5. The Fundamental Unit of an Order of a Real Quadratic Number Field  295
9.6. The Character of a Quadratic Number Field  301
9.7. The Arithmetic Class Number Formula  303
9.8. Computing the Gaussian Sum  310
9.9. Exercises  313

Chapter 10. What Next?  315
10.1. Absolutely Abelian Extensions  316
10.2. The Class Field of the Ray Class Group  317
10.3. Local Class Field Theory  321
10.4. Formulation of Class Field Theory Using Ideles  322
10.5. Exercises  324

Appendix A. Divisibility Theory  325
A.1. Divisibility in Monoids  325
A.2. Principal Ideal Domains  328
A.3. Euclidean Domains  330
A.4. Finitely Generated Modules over a Principal Ideal Domain  331
A.5. Modules over Euclidean Domains  338
A.6. The Arithmetic of Polynomials over Rings  340

Appendix B. Trace, Norm, Different, and Discriminant  341
# Contents

Appendix C. Harmonic Analysis on Locally Compact Abelian Groups 345

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.1. Topological Groups</td>
<td>345</td>
</tr>
<tr>
<td>C.2. The Pontryagin Duality Theorem</td>
<td>346</td>
</tr>
<tr>
<td>C.3. The Haar Integral</td>
<td>347</td>
</tr>
<tr>
<td>C.4. The Restricted Direct Product</td>
<td>350</td>
</tr>
<tr>
<td>C.5. The Poisson Summation Formula</td>
<td>356</td>
</tr>
</tbody>
</table>

References 359

Index 363
Preface

In writing this introduction to algebraic number theory I have been guided by several principles.

First, it is my firm conviction that an area of mathematics such as number theory that has developed over a long period of time can be properly studied and understood only if one proceeds through this entire development in abbreviated form, much as an organism recapitulates its evolutionary path in abbreviated form during its embryonic development.

From this I derived the concept of allowing the reader to take part from chapter to chapter in the historical development of number theory. This holds for the first seven chapters, while the last three chapters are devoted primarily to applications and an overview.

Second, it was a discovery of Dedekind and Kronecker in the 1880s that principles that had been developed to study algebraic numbers could also be applied to the theory of algebraic functions. Dedekind wished to provide a firm foundation to Riemannian function theory. Together with H. Weber [DeWe1882] he considered the case of functions whose arguments and values are complex numbers. It later became clear that the theory of Dedekind and Weber could be extended to cover algebraic functions over an arbitrary field of constants. The most complete analogy to algebraic numbers then appears when the field of constants is finite. In fact, we find ourselves in this case in an area of number theory itself, the theory of congruences. Therefore, in this book we shall consider algebraic numbers and functions (of a single variable) together.

Lastly, this book is an introduction only to the extent that an important area of algebraic number theory, class field theory, is considered only
summarily, in the tenth, and last, chapter. Below this threshold the reader should nonetheless be able to embark on a research topic. In particular, the theory of the different and discriminant and the theory of higher ramification groups are explicated in considerable detail.

Corresponding to these three principles the book is constructed as follows: The first chapter discusses some issues of elementary number theory and encompasses the time before the development of the theory of algebraic number fields. There are two exceptions: In Section 1.5 we consider public key cryptology as an example of the application of number theory of the nineteenth century to present-day communications technology, and in Section 1.8 we prove the prime number theorem with methods that reflect the spirit of Cauchy, Riemann, and Chebyshev, though the brevity of our presentation is made possible by simplifications of recent vintage. I wish to thank F. Hirzebruch and D. Zagier for apprising me of these developments in a recent manuscript ([Za1997]).

The second chapter is concerned with the part of algebraic number theory that is applicable to arbitrary orders in algebraic number fields. This corresponds on the one hand to the state of knowledge before Dedekind, and here in particular Dirichlet’s theorem on units has its place. On the other hand, our presentation is not strictly historical; rather, it is suffused with Dedekind’s ideas. Also present here is Minkowski’s geometry of numbers, which provides the chapter its title. Number theory had its beginnings in the study of the rational integers. We therefore begin the second chapter with a discussion of complete forms, which provides the transition from questions about rational integers to questions about algebraic numbers.

With the third chapter we have finally arrived at Dedekind’s theory of ideals, which we develop in a generality that makes possible the simultaneous treatment of algebraic number fields and function fields.

The valuation-theoretic method of Chapter 4 is a supplement to the ring-theoretic method of Chapter 3.

With the machinery thus developed we present in Chapter 5 the theory of algebraic functions of one variable, basing our presentation principally on H. Hasse’s Zahlentheorie [Ha1949].

In Chapter 6 we consider the decomposition groups and ramification groups of normal extensions and thereby come to the completion of the theory of algebraic number fields of Dedekind and Hilbert. This then makes it possible to treat the important example of cyclotomic fields in an adequate manner. The Kronecker–Weber theorem is presented in the form of a series of exercises. With the upper numeration of Hasse and Herbrand we have reached the mathematics of the 1930s.
Chapter 7 is devoted primarily to a proof of the functional equation for Hecke $L$-series as presented in Tate’s thesis [Ta1950]. This result alone would hardly justify a chapter of such length, since we draw relatively few consequences from it. If I have nevertheless decided to present this in full detail, it is because on the one hand it introduces new methods of proof compared to those of the previous chapters, such as analysis on locally compact abelian groups including Pontryagin duality theory, and on the other hand the methods of Tate’s thesis allow generalizations that are of fundamental significance for the union of number theory and the representation theory of reductive groups (the Langlands conjectures).

Chapter 7 begins with a careful presentation of the relation between idele class groups and ray class groups as well as that between Hecke characters and Grössencharakters. The basic properties of ideles and adeles are proved for number fields and function fields. In proving the functional equation, however, we consider only number fields.

Chapter 8 contains applications of the analytic methods of Chapter 7 to the distribution of prime ideals in algebraic number fields. In the section on generalized Riemann hypotheses we also consider the congruence zeta functions of Artin and F.K. Schmidt. I wish to thank S. Böcherer and R. Schulze-Pillot for supplying me with extended seminar notes by P.K. Draxl on the theorem of Hecke on the distribution of primes in cones, which made possible an essential rounding off of Chapter 8.

Chapter 9 is devoted to quadratic number fields, for which many attributes can be represented more explicitly than in the general case. This holds especially for the computation of the class number and the determination of the fundamental unit. Here we also build bridges between Gauss’s theory of quadratic forms and the theory of orders in quadratic number fields.

Chapter 10 finally provides a glimpse of class field theory.

In writing this book I have had before me the image of a reader who possesses a good knowledge of linear algebra. This must be supplemented by knowledge of field theory, particularly Galois theory, along the lines of what is covered in E. Kunz’s *Algebra*, which has also appeared in Vieweg Verlag’s series “Aufbaukurs Mathematik.” In some ways this book builds directly on Kunz’s *Algebra*, which we have cited at many points. If at the beginning of this book we spoke of an “abbreviated development,” such an abbreviation has been made possible by the developments of modern algebra, which have simplified many a difficult proof by one of the older masters.

In the planning of this book I have had before me as examples the long series of texts on algebraic number theory, above all the books by H. Hasse [Ha1949] and Borevich and Shafarevich [BoSh1966]. The idea for treating
simultaneously the cases of number fields and function fields is to be found in, aside from the above-mentioned books, the books of Eichler [Ei1963], Artin [Ar1967], and Weil [We1967]. For various reasons these books seem to me unsuitable for the beginner.

My colleagues S. Böge, G. Frei, W. Hoffmann, S. Kukkuk, W. Narkiewicz, and F. Nicolae have read drafts of individual chapters of this book and have suggested very valuable improvements and corrections. I offer them my heartfelt thanks, which I offer also to C. Hadan, B. Wüst, and again S. Kukkuk and F. Nicolae for preparing the TeX files.

Some of the greatest mathematicians of the past—I name here only David Hilbert and Hermann Weyl—have seen in algebraic number theory one of the most outstanding creations of mathematics. The task of this book will have been fulfilled if some of this enthusiasm is transmitted to the reader.

Berlin, March 1997

Translator’s Note

This English translation is generally faithful to the German text, the only changes being the correction of a few small errors and the enlargement of the index. I hope that I have not introduced too many new errors.

The German edition of this book is part of the series Vieweg Studium, Aufbaukurs Mathematik. Thus it was natural for the author to cite as a source for results on abstract algebra the text in the same series by E. Kunz [Ku]. Since this book has appeared only in German, in this edition it has been replaced as a reference by Serge Lang’s Algebra [La], which is known to a worldwide English-language readership. Most of these references are to standard results in field theory. The reader who is familiar with another introductory algebra text, that of van der Waerden [Wa1966, Wa1967], for example, will certainly find the requisite background material for the study of algebraic number theory.

I would like to thank Helmut Koch for his kind assistance with the translation. He answered a large number of queries about notation and terminology and then looked over the entire English manuscript. I would also like to express my gratitude to Walter Neumann and Lawrence Washington for their help with terminology and in clarifying a few sticky points.
Notation

We use the standard Bourbaki notation $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. The elements of $\mathbb{Z}$ are in general denoted by lowercase Latin letters, as are also the elements of the ring $\Gamma$ that appears as a generalization of $\mathbb{Z}$ and of $P_0[x]$, the polynomial ring over the field $P_0$.

Fields are designated by uppercase Latin letters: $K$, $L$, $M$, $N$, $P$, while $O$, $R$ are reserved for rings. The elements of fields that appear as extensions $Q(\Gamma)$ are denoted by lowercase Greek letters, while the elements of $P = Q(\Gamma)$ are denoted by Latin letters.

We let

$$E = \begin{pmatrix} 1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \end{pmatrix}$$

denote the identity matrix. Matrices are denoted by uppercase boldface Latin letters: $A$, $B$, $C$, \ldots.

The notation $A \subset B$ for sets $A$, $B$ means that $A$ is properly contained in $B$. The usual subset relation is denoted by $A \subseteq B$. We let $|A|$ denote the number of elements in the set $A$.

In Chapter 2, modules in $K$ will generally be denoted by lowercase fraktur letters $a$, $b$, $c$, $d$, \ldots. Ideals and divisors in Chapter 3, on the other hand, are denoted by uppercase fraktur letters.

Field isomorphisms will be indicated by lowercase Latin letters.

List of Symbols

$\mathcal{A}_K$ the adele ring of $K$
char($K$) characteristic of the field $K$
Cl(K)  ideal class group of K
deg    degree of a polynomial
Δ(𝒜)  discriminant of the module 𝒜
d_K = Δ(O_K) discriminant of the algebraic number field K
Δ_K/F discriminant (as an ideal)
Δ_K/F  different
GL     general linear group
gcd    greatest common divisor
h_K    class number of the number field K
I_O    group of fractional ideals of O
I_K    group of fractional ideals of O_K
I_K    idele ring of K
ℑ      imaginary part of a complex number
ker    kernel of a mapping
1      see Section 2.9
lcm    least common multiple
L(s,χ) Dirichlet or Hecke L-series
Λ    group of invertible elements of the ring Λ
N      (absolute) norm
N_K/F relative norm
ℙ      projective space
Pic     Picard group
Q(O)   quotient field of the ring O
ℜ      real part of a complex number
rank   rank of a module
R_K    regulator of the number field K
S_1    group of complex numbers with absolute value 1
Spec   spectrum of a ring
A^t    transpose of the matrix A
tr     trace
U^n    group of principal units of level n
V(K)   set of places of K
V_f(K) set of finite places of K
V_∞(K) set of infinite places of K
ζ(s)   Riemann zeta function
ζ_K(s) Dedekind zeta function
References


References


References


References


Index

Abel, N., 305
abelian extension, 171, 183
absolute degree, 145, 159, 164
absolute norm, 74, 175
adele, 299
principal, 210
affine set, 93
algebraic
function, 39, 40, 141
integral, 40
integer, 39
number, 39
analytic class number formula, 303
analytic number theory, 203
annihilator, 337
approximation theorem, 107, 189, 215
Archimedean axiom, 107
archimedean valuation, 107
Archimedes, 3
arithmetic class number formula, 301, 303
arithmetic geometry, 272
Artin, E., xv, xvi, 136, 199, 205, 253, 317
Artin mapping, 317
associate, 326
associated
divisor, 156, 163
function, 146
system of divisors, 163
asymptotically equivalent, 25

Bachet de Méziriac, C.G., 4
Bauer’s theorem, 261
binary quadratic form, 35
Böcherer, S., xv
Böge, S., xvi
Bombieri, E., 272

Borevich, Z.I., xv
Brill, A., 64
cancellation rule, 325
canonical correspondence, 281
canonical divisor class, 157
Cauchy, A., xiv
Cauchy sequence, 113, 345
centrally symmetric, 55
character, 346
Dirichlet, 301
group, 346
primitive, 302, 306
characteristic
function, 349
polynomial, 343
Chebyshev, P.L., xiv, 27
Chevalley, C., 136, 205, 214, 321
Chinese remainder theorem, 8, 76, 329
class field theory, 316
class group, 84, 280
narrow, 214, 280
class number, 84
analytic formula, 303
arithmetic formula, 301, 303
complementary
basis, 94, 96, 162, 343
ideal, 161
module, 94
complete
decomposable form, 37, 62
field, 112
module, 43
completely ramified
extension field, 124
completion, of a field, 112, 113
Index

conductor, 46, 96, 207, 217, 222, 291, 295, of a sequence of elements, 341
318
congruence, 1, 8, 76
discriminant theorem
congruence subgroup, 215
Dedekind's, 60, 100, 159
congruence zeta function, 252
Hermite's, 60
congruence function, see also field of constants
Minkowski's, 59, 101
content, 340
divisor, 326
continued fraction, 285
associated, 156, 163
corvergent, 286
chain condition, 326
corvergent
class group, 148
corvergent of a continued fraction, 286
degree of, 148
cyclotomic field, 180, 194
effective divisor, 145, 160
decomposable polynomial, 37
eichler, M., xvi
decomposition field, 173
Eisenstein number, 6
decomposition group, 172, 189, 190
Eisenstein polynomial, 156
dedekind, R., xiii, xiv, 7, 41, 47, 65, 94, 100,
with respect to p, 91
to 101, 142, 171, 204, 275, 315
dedekind domain, 66
Eisenstein's irreducibility criterion, 92
dedekind zeta function, 204, 247
element different, 176, 181
dedekind's
elementary divisor, 337
differential theorem, 60, 100, 159
elementary transformation, 338
discriminant theorem, 96
effective, 145
dedekind's theorem on the different, 98, 128, 163,
elementary divisor, 337
176, 177
dedekind's second main theorem, 96
equivalent quadratic forms, 276
dedekind's theorem on the different, 96
dedekind's third main theorem, 98
euclid, 22, 330
defining module, 214, 218
euclidean algorithm, 286, 330
degree
euclidean domain, 330
definite, 145
euler factor, 24
define, 148
euler product, 24
definition, 112
euler summation formula, 25
development, 25

euler, L., 4-6, 8, 9, 12, 22-24, 36, 291
equation, 145
euler, L., 4-6, 8, 9, 12, 22-24, 36, 291
exact sequence, 332
euler's generalization of, 9
explicit formula for \( \pi(x) \), 25
extension
extension of a valuation, 113
of a valuation, 113
evaluation, 112
extension of the field of constants, 158

Dirichlet
Fermat field, 169
L-series, 204
Fermat prime, 5
discriminant, 45, 95, 148
Fermat's last theorem, 4, 6, 84, 184, 185
differential, 154
first case, 7, 184
different, 95, 148, 176
different, 95, 148, 176
different and
of an element, 341
do not include
of the first kind, 163
different and
differential
Diophantus, 4
Dirichlet's
Diophantus, 4
Dirichlet's
discriminant theorem
Dirichlet, P. G. L., 7, 35, 48, 49, 204, 267
discriminant, 45, 95, 148
of a polynomial, 344
of a quadratic form, 276
discriminant, 45, 95, 148
Dirichlet, P. G. L., 7, 35, 48, 49, 204, 267
discriminant, 45, 95, 148
inecessary divisor of, 101, 126
discriminant, 45, 95, 148
discriminant, 45, 95, 148
inecessary divisor of, 101, 126
discriminant, 45, 95, 148
inecessary divisor of, 101, 126
of a polynomial, 344
of a quadratic form, 276
extension
extension of a valuation, 113
of the field of constants, 158
Fermat field, 169
Fermat prime, 5
Fermat's last theorem, 4, 6, 84, 184, 185
field
fine case, 7, 184
second case, 7
Fermat's little theorem, 6, 78
Euler's generalization of, 9
Fermat, P., 4, 5, 36
Fermat, Pierre de, 3
field
complete, 112
cycloptic, 180, 194
of coefficients, 142
of constants, 143, 147
extension of, 158
of formal power series, 120
with valuation, 104
first supplementary theorem, see also quadratic reciprocity
form, 38
complete, 39
irreducible, 37
quadratic, see also quadratic form
reducible, 37
formal Laurent series, 120
formal power series, 120
Fourier transform, 349
fractional ideal, 68
Frei, G., xvi
Frobenuis automorphism, 176, 182, 199, 316
function field
algebraic, 142
equadratic, 168
function space
associated to a divisor, 149
functional equation
for Hecke L-series, 219
local, 231
fundamental
group, 315
parallelepiped, 55
system of units, 55
unit, 295
Galois, E., 294
Gauss, C. F., xv, 6, 8, 12, 17, 25, 36, 84, 197, 275, 276, 340
Gaussian sum, 8, 14, 304
Gauss's lemma, 18
general point, 93
general reciprocity law, 199
generalized Riemann hypothesis, 270, 271
generic point, 93
genus, 158, 159, 320
gometric point, 159
gometry of numbers, 35, 48
global class field theory
main theorem, 323
global field, 207
Goldbach, C., 5
greatest common divisor, 327, 331
of ideals, 72
Grössencharakter, 204, 205, 206, 218
 equivalence of -s, 207
primitive, 207
Grothendieck, A., 93, 272
group of principal units, 190
group of units, 326
Haar integral, 347
Haar measure
normalized, 347
Hadamard, J., 25
Hadam, C., xvi
half system, 17
Hase, H., xiv, xv, 103, 136, 142, 190, 272, 321
Hecke character, 218
Hecke L-series, 204, 251
Hecke, E., xv
Heegner, K., 285
height, 330
Hensel's lemma, 115, 125
Hensel, K., 103, 115, 133, 136
Herbrand function, 190
Herbrand, J., xiv, 190
Hermite's discriminant theorem, 60
Hilbert, D., xiv, xvi, 171, 183, 317, 318
Hilbert class field, 318
Hirzebruch, F., xiv
Hoffmann, W., xvi
Hurwitz, A, 170
ideal, 328
fractional, 68
ideal numbers, 7
idele, 212
class group, 205, 212
principal, 212
identity
in a monoid, 325
index, 337
of a to base g, 31
index table, 31
inert, 83
inertia
degree, 67, 92
of an extension field, 124
field, 156, 173
group, 173
inesential divisor of the discriminant, 101, 126
inesential prime ideal, 83
infinite
component, 214
descent, 5
place, 112
integral
algebraic function, 40
closure, 42
domain, 325
element, 40
ideal, 68
integarlly closed, 42
inversion
formula, 349
theorem, 349
irreducible, 326
isomorphism
  complex, 48
  real, 48
Jacobi symbol, 17, 18
jump, 194
Krasner’s lemma, 124
Kronecker, L., xiii, 1, 183, 315
Kronecker–Weber theorem, xiv, 200, 316
Kukkuk, S., xvi
Kummer, E., 7, 84, 184, 262
Kummer extension, 195
Kürschak, J., 103
Lagrange, J.-L., 3, 36, 291
Lamé, G., 7
Langlands, R., xv
Langlands conjectures, xv, 262
lattice, 55
least common multiple, 327
  of ideals, 72
Legendre, A.-M., 7
Legendre symbol, 13, 14, 183, 199
Leibniz, G., 303
Lessing, Gotthold, 3
limit, of a sequence, 113
little Fermat theorem, 78
local
  class field theory, 321
  functional equation, 231
  zeta function, 230
localization, 188
logarithmic component, 50
lower integral, 348
$L$-series, 204
  Dirichlet, 204
  Hecke, 204, 251
maximal order, 45
maximal tamely ramified extension, 131
measurable set, 349
Minkowski, H., xiv, 35, 48, 54, 56
Minkowski’s discriminant theorem, 59, 101, 317
Minkowski’s lattice point theorem, 56
module, 391
  basis of, 332
  finitely generated, 332
  in a quadratic number field, 277
  rank of, 333
torsion, 333
torsion-free, 333
unitary, 331
monic polynomial, 329
monoid, 325
  reduced, 326
monotonically
  decreasing, 348
  increasing, 348
Mordell–Weil theorem, 169
multiplicity, 146, 149
Möbius
  function, 32
  inversion formula, 33
Narkiewicz, W., xvi
narrow class group, 280
natural number, 1
Newman, D., 25
Nicolaue, F., xvi
Noether, E., 66, 68, 142
Noetherian ring, 66
nonarchimedean valuation, 107
norm, 341
  absolute, 74
  of an element, 74
  of an ideal, 74
  relative, 74, 172
norm form, 38
norm residue symbol, 321
normal basis, 150
Olbers, H., 6
order, 46, 337
  of a pole, 146
Ostrowski, A., 103
Ostrowski’s theorem, 113, 121
$p$-adic rational number, 115
partial denominator
  of a continued fraction, 286
Pell’s equation, 3
periodic continued fraction, 290
$\mathfrak{p}$-exponent of an ideal, 71
Picard group, 148, 169, 214
pigeonhole principle, 48, 52
place, 112
  infinite, 112, 144
  of a field, 144
Poisson summation formula, 356
pole, 146, 149
  order of, 146
polynomial
  characteristic, 343
decomposable, 37
discriminant of, 344
monic, 329
Pontryagin duality theorem, 346
prime
  discriminant, 310
element, 110, 326
<table>
<thead>
<tr>
<th>Term</th>
<th>Page(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>factorization, uniqueness of</td>
<td>1</td>
</tr>
<tr>
<td>ideal theorem</td>
<td>271</td>
</tr>
<tr>
<td>number function</td>
<td>25</td>
</tr>
<tr>
<td>number theorem</td>
<td>25, 26</td>
</tr>
<tr>
<td>residue class</td>
<td>9</td>
</tr>
<tr>
<td>primitive</td>
<td></td>
</tr>
<tr>
<td>character</td>
<td>302, 306</td>
</tr>
<tr>
<td>root</td>
<td>9</td>
</tr>
<tr>
<td>principal</td>
<td></td>
</tr>
<tr>
<td>adele</td>
<td>210</td>
</tr>
<tr>
<td>divisor</td>
<td>146</td>
</tr>
<tr>
<td>genus</td>
<td>320</td>
</tr>
<tr>
<td>ideal domain</td>
<td>328</td>
</tr>
<tr>
<td>order</td>
<td>45</td>
</tr>
<tr>
<td>unit</td>
<td></td>
</tr>
<tr>
<td>group of $-s$, 190, 139</td>
<td></td>
</tr>
<tr>
<td>of level n, 130, 138</td>
<td></td>
</tr>
<tr>
<td>product</td>
<td></td>
</tr>
<tr>
<td>of modules</td>
<td>41</td>
</tr>
<tr>
<td>product theorem for valuations</td>
<td>208</td>
</tr>
<tr>
<td>projective line</td>
<td>112</td>
</tr>
<tr>
<td>projectively generate</td>
<td>37, 38</td>
</tr>
<tr>
<td>public key cryptography</td>
<td>11</td>
</tr>
<tr>
<td>purely cubic number field</td>
<td>64</td>
</tr>
<tr>
<td>Pythagorean</td>
<td></td>
</tr>
<tr>
<td>theorem</td>
<td>1</td>
</tr>
<tr>
<td>triple</td>
<td>1</td>
</tr>
<tr>
<td>quadratic form</td>
<td></td>
</tr>
<tr>
<td>associated matrix</td>
<td>276</td>
</tr>
<tr>
<td>discriminant of</td>
<td>276</td>
</tr>
<tr>
<td>equivalence of $-s$</td>
<td>276</td>
</tr>
<tr>
<td>properly equivalent $-s$</td>
<td>276</td>
</tr>
<tr>
<td>quadratic irrationality</td>
<td>291</td>
</tr>
<tr>
<td>reduced</td>
<td>292</td>
</tr>
<tr>
<td>quadratic nonresidue</td>
<td>12</td>
</tr>
<tr>
<td>quadratic reciprocity</td>
<td>8, 12, 14, 183</td>
</tr>
<tr>
<td>first supplementary theorem</td>
<td>14, 21</td>
</tr>
<tr>
<td>second supplementary theorem</td>
<td>16, 21</td>
</tr>
<tr>
<td>quadratic residue</td>
<td>12</td>
</tr>
<tr>
<td>quasi-character</td>
<td>227, 351, 352</td>
</tr>
<tr>
<td>quotient field</td>
<td>325</td>
</tr>
<tr>
<td>ramification group</td>
<td>173</td>
</tr>
<tr>
<td>upper numeration</td>
<td>190</td>
</tr>
<tr>
<td>ramification index</td>
<td>76, 90, 92</td>
</tr>
<tr>
<td>of an extension field</td>
<td>124</td>
</tr>
<tr>
<td>ramification index shifting theorem</td>
<td>126</td>
</tr>
<tr>
<td>ramified</td>
<td>83, 90</td>
</tr>
<tr>
<td>tamely</td>
<td>100</td>
</tr>
<tr>
<td>wildly</td>
<td>100</td>
</tr>
<tr>
<td>ramified prime ideal</td>
<td>94</td>
</tr>
<tr>
<td>ray class field</td>
<td>317</td>
</tr>
<tr>
<td>ray class group</td>
<td>214, 317</td>
</tr>
<tr>
<td>ray group</td>
<td>214</td>
</tr>
<tr>
<td>reduced monoid</td>
<td>326</td>
</tr>
<tr>
<td>regulator</td>
<td>55</td>
</tr>
<tr>
<td>relative extension</td>
<td>88</td>
</tr>
<tr>
<td>relative norm</td>
<td>74, 90, 172</td>
</tr>
<tr>
<td>remainder</td>
<td></td>
</tr>
<tr>
<td>of a continued fraction</td>
<td>286</td>
</tr>
<tr>
<td>residue class characteristic</td>
<td>114</td>
</tr>
<tr>
<td>residue class field</td>
<td>109</td>
</tr>
<tr>
<td>residue symbol</td>
<td></td>
</tr>
<tr>
<td>$n$th-power</td>
<td>199</td>
</tr>
<tr>
<td>restricted direct product</td>
<td>350</td>
</tr>
<tr>
<td>$\rho$-factor</td>
<td>236, 239</td>
</tr>
<tr>
<td>Riemann</td>
<td></td>
</tr>
<tr>
<td>hypothesis</td>
<td>25, 27</td>
</tr>
<tr>
<td>generalized</td>
<td>270, 271</td>
</tr>
<tr>
<td>sphere</td>
<td>144</td>
</tr>
<tr>
<td>surface</td>
<td>90, 94, 141, 142, 144</td>
</tr>
<tr>
<td>zeta function</td>
<td>24</td>
</tr>
<tr>
<td>Riemann, B., xiv</td>
<td>24, 25, 142</td>
</tr>
<tr>
<td>Riemann–Roch theorem</td>
<td>142, 149, 160, 162</td>
</tr>
<tr>
<td>ring</td>
<td></td>
</tr>
<tr>
<td>adele</td>
<td>209</td>
</tr>
<tr>
<td>root number</td>
<td>238</td>
</tr>
<tr>
<td>Schmidt, F. K., xv</td>
<td>142, 164</td>
</tr>
<tr>
<td>Schulze-Pillot, R., xv</td>
<td></td>
</tr>
<tr>
<td>second supplementary theorem</td>
<td>see also quadratic reciprocity</td>
</tr>
<tr>
<td>self-dual measure</td>
<td>222</td>
</tr>
<tr>
<td>semilocalization</td>
<td>80</td>
</tr>
<tr>
<td>separating element</td>
<td>144</td>
</tr>
<tr>
<td>Shafarevich, I. R., xv</td>
<td></td>
</tr>
<tr>
<td>similar in the narrow sense</td>
<td>279</td>
</tr>
<tr>
<td>solvable extension</td>
<td>171</td>
</tr>
<tr>
<td>Spec</td>
<td>93</td>
</tr>
<tr>
<td>specialization of a polynomial</td>
<td>141</td>
</tr>
<tr>
<td>split completely</td>
<td>83, 90, 259</td>
</tr>
<tr>
<td>Stark, H.</td>
<td>285</td>
</tr>
<tr>
<td>Stepanov, A.</td>
<td>272</td>
</tr>
<tr>
<td>Stickelberger, L.</td>
<td>64</td>
</tr>
<tr>
<td>strong approximation theorem</td>
<td>77</td>
</tr>
<tr>
<td>summable function</td>
<td>348</td>
</tr>
<tr>
<td>surface</td>
<td>93</td>
</tr>
<tr>
<td>symmetric group</td>
<td>179</td>
</tr>
<tr>
<td>Takagi, T., 317</td>
<td></td>
</tr>
<tr>
<td>Tamagawa measure</td>
<td>356</td>
</tr>
<tr>
<td>tamely ramified</td>
<td>100</td>
</tr>
<tr>
<td>tamely ramified measure</td>
<td>129</td>
</tr>
<tr>
<td>maximal</td>
<td>151</td>
</tr>
<tr>
<td>Tate, J., xv, 205</td>
<td></td>
</tr>
<tr>
<td>Taylor, R., 4</td>
<td></td>
</tr>
<tr>
<td>theorem</td>
<td></td>
</tr>
<tr>
<td>Bauer’s, 261</td>
<td></td>
</tr>
<tr>
<td>Chinese remainder</td>
<td>329</td>
</tr>
<tr>
<td>Dedekind’s – on the different</td>
<td>98, 128, 163, 176, 177</td>
</tr>
<tr>
<td>Dedekind’s discriminant</td>
<td>60, 100, 159</td>
</tr>
<tr>
<td>Dedekind’s first main</td>
<td>96</td>
</tr>
</tbody>
</table>
Dedekind's second main, 96
Dedekind's third main, 98
Dirichlet's, 266
Dirichlet's unit, 48, 50
Fermat's last, see also Fermat's last theorem
Fermat's little, 78
Hermite's discriminant, 60
Kronecker–Weber, xiv, 200, 316
main – of global class field theory, 323
main – of local class field theory, 321
Minkowski's discriminant, 59, 101, 317
Minkowski's lattice point, 56
Mordell–Weil, 169
of Hasse–Arf, 195
of Landau, 265
of Peter and Weyl, 268
Ostrowski's, 113, 121
Pontryagin duality, 346
prime ideal, 271
prime number, 25, 26
product – for valuations, 208
ramification index shifting, 126
Riemann–Roch, 142, 149, 160, 162
strong approximation, 77
Tychonoff product, 350
topological group, 345, 346
torsion
  element, 333
  module, 333
totally positive, 214
tower of differentials theorem, 95, 177, 192
trace, 341
transcendental, 143
triangle inequality, 104
trivial valuation, 104
Tychonoff product theorem, 350

uniformizing parameter, 110
unit
  fundamental system of −s, 55
unitarity, 331
unramified, 181, 196
  extension field, 124
upper integral, 348
upper numeration, 190, 191
Urysohn's lemma, 268

Vallée Poussin, C.-J. de la, 25, 27
valuation, 104, 113
  archimedean, 107
  discrete, 109
  equivalent −s, 104
  exponential, 109
  group, 113
  nonarchimedean, 107
  ring, 109
  valuation ring, 147
  value
    m-fold, 147
  variable, 143

Weber, H., xiii, 142, 183
Weierstrass normal form, 168
Weil, A., xvi, 3, 272
Weyl, H., xvi
  wildly ramified, 100
    extension field, 129
Wiles, A., 4
Wilson's theorem, 31
Wüst, B., xvi

Zagier, D., xiv
zeta function
  congruence, 252, 253
  Dedekind, 204, 247
  local, 230
  Riemann, 24