

H. Koch

Algebraic Number Theory



Springer

Consulting Editors of the Series:
A.A. Agrachev, A.A. Gonchar, E.F. Mishchenko,
N.M. Ostianu, V.P. Sakharova, A.B. Zhishchenko

Title of the Russian edition:
Itogi nauki i tekhniki, Sovremennye problemy matematiki,
Fundamental'nye napravleniya, Vol. 62, Teoriya chisel 2
Publisher VINITI, Moscow 1988

Second Printing 1997 of the First Edition 1992, which was originally
published as Number Theory II,
Volume 62 of the Encyclopaedia of Mathematical Sciences.

Die Deutsche Bibliothek – CIP-Einheitsaufnahme
Koch, H: Algebraic number theory / H. Koch. Ed.: A. N. Parshin; I. R. Shafarevich. – 1. ed., 2. printing. –
Berlin; Heidelberg; New York; Barcelona; Budapest; Hongkong; London; Mailand; Paris;
Santa Clara; Singapur; Tokio: Springer, 1997
ISBN 978-3-540-63003-6 ISBN 978-3-642-58095-6 (eBook)
DOI 10.1007/978-3-642-58095-6

Mathematics Subject Classification (1991):
11Rxx, 11Sxx

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1997
Originally published by Springer-Verlag Berlin Heidelberg New York in 1997
Softcover reprint of the hardcover 1st edition 1997

Typesetting: Asco Trade Typesetting Ltd., Hong Kong

SPIN: 10889896
41/3111-5 4 3 2 1 – Printed on acid-free paper.

Algebraic Number Fields

H. Koch

Contents

Preface	7
Chapter 1. Basic Number Theory	8
§ 1. Orders in Algebraic Number Fields	9
1.1. Modules and Orders	10
1.2. Module Classes	12
1.3. The Unit Group of an Order	15
1.4. The Unit Group of a Real-Quadratic Number Field	17
1.5. Integral Representations of Rational Numbers by Complete Forms	18
1.6. Binary Quadratic Forms and Complete Modules in Quadratic Number Fields	19
1.7. Representatives for Module Classes in Quadratic Number Fields	21
§ 2. Rings with Divisor Theory	22
2.1. Unique Factorization in Prime Elements	22
2.2. The Concept of a Domain with Divisor Theory	23
2.3. Divisor Theory for the Maximal Order of an Algebraic Number Field	25
§ 3. Dedekind Rings	27
3.1. Definition of Dedekind Rings	28
3.2. Congruences	29
3.3. Semilocalization	30
3.4. Extensions of Dedekind Rings	30
3.5. Different and Discriminant	33
3.6. Inessential Discriminant Divisors	36
3.7. Normal Extensions	36
3.8. Ideals in Algebraic Number Fields	40
3.9. Cyclotomic Fields	41
3.10. Application to Fermat's Last Theorem I	43

§ 4. Valuations	45
4.1. Definition and First Properties of Valuations	45
4.2. Completion of a Field with Respect to a Valuation	49
4.3. Complete Fields with Discrete Valuation	49
4.4. The Multiplicative Structure of a p -adic Number Field	51
4.5. Extension of Valuations	53
4.6. Finite Extensions of p -adic Number Fields	55
4.7. Kummer Extensions	58
4.8. Analytic Functions in Complete Non-Archimedean Valued Fields	59
4.9. The Elementary Functions in p -adic Analysis	60
4.10. Lubin-Tate Extensions	62
§ 5. Harmonic Analysis on Local and Global Fields	63
5.1. Harmonic Analysis on Local Fields, the Additive Group	64
5.2. Harmonic Analysis on Local Fields, the Multiplicative Group	65
5.3. Adeles	66
5.4. Ideles	68
5.5. Subgroups of $J(K)/K^\times$ of Finite Index and the Ray Class Groups	69
§ 6. Hecke L -Series and the Distribution of Prime Ideals	70
6.1. The Local Zeta Functions	74
6.2. The Global Functional Equation	76
6.3. Hecke Characters	77
6.4. The Functional Equation for Hecke L -Series	79
6.5. Gaussian Sums	80
6.6. Asymptotical Distribution of Ideals and Prime Ideals	82
6.7. Chebotarev's Density Theorem	84
6.8. Kronecker Densities and the Theorem of Bauer	85
6.9. The Prime Ideal Theorem with Remainder Term	87
6.10. Explicit Formulas	87
6.11. Discriminant Estimation	88
Chapter 2. Class Field Theory	90
§ 1. The Main Theorems of Class Field Theory	92
1.1. Class Field Theory for Abelian Extensions of $\mathbb{Q}$	92
1.2. The Hilbert Class Field	93
1.3. Local Class Field Theory	93
1.4. The Idele Class Group of a Normal Extension	95
1.5. Global Class Field Theory	96
1.6. The Functorial Behavior of the Norm Symbol	97
1.7. Artin's General Reciprocity Law	98
1.8. The Power Residue Symbol	99
1.9. The Hilbert Norm Symbol	101
1.10. The Reciprocity Law for the Power Residue Symbol	102

1.11. The Principal Ideal Theorem	103
1.12. Local-Global Relations	104
1.13. The Zeta Function of an Abelian Extension	105
§ 2. Complex Multiplication	107
2.1. The Main Polynomial	107
2.2. The First Main Theorem	108
2.3. The Reciprocity Law	109
2.4. The Construction of the Ray Class Field	109
2.5. Algebraic Theory of Complex Multiplication	111
2.6. Generalization	112
§ 3. Cohomology of Groups	112
3.1. Definition of Cohomology Groups	112
3.2. Functoriality and the Long Exact Sequence	113
3.3. Dimension Shifting	114
3.4. Shapiro's Lemma	115
3.5. Corestriction	115
3.6. The Transgression and the Hochschild-Serre-Sequence	116
3.7. Cup Product	117
3.8. Modified Cohomology for Finite Groups	119
3.9. Cohomology for Cyclic Groups	120
3.10. The Theorem of Tate	121
§ 4. Proof of the Main Theorems of Class Field Theory	121
4.1. Application of the Theorem of Tate to Class Field Theory ...	121
4.2. Class Formations	122
4.3. Cohomology of Local Fields	124
4.4. Cohomology of Ideles and Idele Classes	125
4.5. Analytical Proof of the Second Inequality	129
4.6. The Canonical Class for Global Extensions	130
§ 5. Simple Algebras	131
5.1. Simple Algebras over Arbitrary Fields	131
5.2. The Reduced Trace and Norm	132
5.3. Splitting Fields	133
5.4. The Brauer Group	133
5.5. Simple Algebras over Local Fields	134
5.6. The Structure of the Brauer Group of an Algebraic Number Field	135
5.7. Simple Algebras over Algebraic Number Fields	136
§ 6. Explicit Reciprocity Laws and Symbols	137
6.1. The Explicit Reciprocity Law of Shafarevich	138
6.2. The Explicit Reciprocity Law of Brückner and Vostokov	139
6.3. Application to Fermat's Last Theorem II	141
6.4. Symbols	142
6.5. Symbols of p -adic Number Fields	143
6.6. Tame and Wild Symbols	144
6.7. Remarks about Milnor's K -Theory	144

§ 7. Further Results of Class Field Theory	145
7.1. The Theorem of Shafarevich-Weil	145
7.2. Universal Norms	145
7.3. On the Structure of the Ideal Class Group	146
7.4. Leopoldt's Spiegelungssatz	147
7.5. The Cohomology of the Multiplicative Group	149
Chapter 3. Galois Groups	150
§ 1. Cohomology of Profinite Groups	151
1.1. Inverse Limits of Groups and Rings	151
1.2. Profinite Groups	153
1.3. Supernatural Numbers	154
1.4. Pro- p -Groups and p -Sylow Groups	154
1.5. Free Profinite, Free Prosolvable, and Free Pro- p -Groups	154
1.6. Discrete Modules	155
1.7. Inductive Limits in C	156
1.8. Galois Theory of Infinite Algebraic Extensions	157
1.9. Cohomology of Profinite Groups	159
1.10. Cohomological Dimension	159
1.11. The Dualizing Module	160
1.12. Cohomology of Pro- p -Groups	161
1.13. Presentation of Pro- p -Groups by Means of Generators and Relations	162
1.14. Poincaré Groups	164
1.15. The Structure of the Relations and the Cup Product	165
1.16. Group Rings and the Theorem of Golod-Shafarevich	166
§ 2. Galois Cohomology of Local and Global Fields	168
2.1. Examples of Galois Cohomology of Arbitrary Fields	168
2.2. The Algebraic Closure of a Local Field	169
2.3. The Maximal p -Extension of a Local Field	171
2.4. The Galois Group of a Local Field	173
2.5. The Maximal Algebraic Extension with Given Ramification ..	175
2.6. The Maximal p -Extension with Given Ramification	177
2.7. The Class Field Tower Problem	180
2.8. Discriminant Estimation from Above	181
2.9. Characterization of an Algebraic Number Field by its Galois Group	182
§ 3. Extensions with Given Galois Groups	182
3.1. Embedding Problems	183
3.2. Embedding Problems for Local and Global Fields	185
3.3. Extensions with Prescribed Galois Group of l -Power Order ..	186
3.4. Extensions with Prescribed Solvable Galois Group	188
3.5. Extensions with Prescribed Local Behavior	188
3.6. Realization of Extensions with Prescribed Galois Group by Means of Hilbert's Irreducibility Theorem	190

Chapter 4. Abelian Fields	192
§ 1. The Integers of an Abelian Field	193
1.1. The Coordinates	193
1.2. The Galois Module Structure of the Ring of Integers of an Abelian Field	194
§ 2. The Arithmetical Class Number Formula	195
2.1. The Arithmetical Class Number Formula for Complex Abelian Fields	195
2.2. The Arithmetical Class Number Formula for Real Quadratic Fields	197
2.3. The Arithmetical Class Number Formula for Real Abelian Fields	198
2.4. The Stickelberger Ideal	200
2.5. On the p -Component of the Class Group of $\mathbb{Q}(\zeta_{p^m})$	203
2.6. Application to Fermat's Last Theorem III	205
§ 3. Iwasawa's Theory of Γ -Extensions	206
3.1. Class Field Theory of Γ -Extensions	206
3.2. The Structure of $\mathcal{A}$ -Modules	207
3.3. The p -Class Group of a Γ -Extension	208
3.4. Iwasawa's Theorem	209
§ 4. p -adic L -Functions	211
4.1. The Hurwitz Zeta Function	212
4.2. p -adic L -Functions	213
4.3. Congruences for Bernoulli Numbers	214
4.4. Generalization to Totally Real Number Fields	215
4.5. The p -adic Class Number Formula	215
4.6. Iwasawa's Construction of p -adic L -Functions	216
4.7. The Main Conjecture	218
Chapter 5. Artin L -Functions and Galois Module Structure	219
§ 1. Artin L -Functions	222
1.1. Representations of Finite Groups	222
1.2. Artin L -Functions	224
1.3. Cyclotomic Fields with Class Number 1	226
1.4. Imaginary-Quadratic Fields with Small Class Number	227
1.5. The Artin Representation and the Artin Conductor	228
1.6. The Functional Equation for Artin L -Functions	230
1.7. The Conjectures of Stark about Artin L -Functions at $s = 0$..	231
§ 2. Galois Module Structure and Artin Root Numbers	234
2.1. The Class Group of $\mathbb{Z}[G]$	235
2.2. The Galois Module Structure of Tame Extensions	236
2.3. Further Results on Galois Module Structure	236

Appendix 1. Fields, Domains, and Complexes	237
1.1. Finite Field Extensions	237
1.2. Galois Theory	238
1.3. Domains	238
1.4. Complexes	239
Appendix 2. Quadratic Residues	240
Appendix 3. Locally Compact Groups	241
3.1. Locally Compact Abelian Groups	241
3.2. Restricted Products	243
Appendix 4. Bernoulli Numbers	243
Tables	245
References	251
Author Index	263
Subject Index	266