Paulo Ribenboim

Classical Theory of Algebraic Numbers

Springer

Paulo Ribenboim
Department of Mathematics
Queen's University
Kingston, Ontario K7L 3N6
Canada

Editorial Board
(North America):

S. Axler
Mathematics Department
San Francisco State University
San Francisco, CA 94132
USA

F.W. Gehring
Mathematics Department
East Hall
University of Michigan
Ann Arbor, MI 48109-1109
USA

K.A. Ribet
Mathematics Department
University of California at Berkeley
Berkeley, CA 94720-3840
USA

Mathematics Subject Classification (2000): 11-01, 11Sxx

Library of Congress Cataloging-in-Publication Data
Ribenboim, Paulo.
Classical theory of algebraic numbers / Paulo Ribenboim. — 1st ed.
p. cm. — (Universitext)
Rev. ed. of: Algebraic numbers. 1972.
Includes bibliographical references and indexes.

ISBN 978-1-4419-2870-2 ISBN 978-0-387-21690-4 (eBook)
DOI 10.1007/978-0-387-21690-4

1. Algebraic number theory. I. Ribenboim, Paulo. Algebraic Numbers. II. Title.
QA247.R465 2001
512′.74—dc21 00-040044

Printed on acid-free paper.

© 2001 Springer Science+Business Media New York
Originally published by Springer-Verlag New York, Inc. in 2001
Softcover reprint of the hardcover 2rd edition 2001
All rights reserved. This work may not be translated or copied in whole or in part without the written permission of the publisher (Springer Science+Business Media, LLC), except for brief excerpts in connection with reviews or scholarly analysis. Use in connection with any form of information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed is forbidden.
The use of general descriptive names, trade names, trademarks, etc., in this publication, even if the former are not especially identified, is not to be taken as a sign that such names, as understood by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone.

Production managed by Lesley Poliner; manufacturing supervised by Jerome Basma.
Typeset in TEX by Sławomir Browkin.

9 8 7 6 5 4 3 2 1

SPIN 10770500

Contents

Preface v

Acknowledgments ix

Index of Notations xix

INTRODUCTION 1

CHAPTER 1. Unique Factorization Domains, Ideals, and Principal Ideal Domains 5

1.1. Unique Factorization Domains 5

1.2. Ideals 6

1.3. Principal Ideal Domains 8

Exercises 8

CHAPTER 2. Commutative Fields 13

2.1. Algebraic Elements 13

2.2. Algebraic Extensions, Algebraically Closed Fields 14

2.3. Algebraic Number Fields 15

2.4. Characteristic and Prime Fields 15

2.5. Normal Extensions, Splitting Fields 15

2.6. Separable Extensions 16

2.7. Galois Extensions 17

2.8. Roots of Unity 18

2.9. Finite Fields 19

2.10. Trace and Norm of Elements 19

2.11. The Discriminant 20

2.12. Discriminant and Resultant of Polynomials 21

2.13. Inseparable Extensions 23

2.14. Perfect Fields 23

2.15. The Theorem of Steinitz 24

2.16. Orderable Fields 24

2.17. The Theorem of Artin 25
Exercises 25

PART ONE **33**

CHAPTER 3. Residue Classes **37**
3.1. Congruences 37
3.2. The Group of Invertible Residue Classes 41
3.3. Finite Abelian Groups 45
Exercises 49

CHAPTER 4. Quadratic Residues **61**
4.1. The Legendre Symbol and Gauss' Reciprocity Law 61
4.2. Gaussian Sums 70
4.3. The Jacobi Symbol 73
Exercises 76

PART TWO **83**

CHAPTER 5. Algebraic Integers **85**
5.1. Integral Elements, Integrally Closed Domains 85
5.2. Rings of Algebraic Integers 91
5.3. Arithmetic in the Field of Gaussian Numbers 92
5.4. Integers of Quadratic Number Fields 97
5.5. Integers of Cyclotomic Fields 100
Exercises 101

CHAPTER 6. Integral Basis, Discriminant **107**
6.1. Finitely Generated Modules 107
6.2. Integral Basis 114
6.3. The Discriminant 116
6.4. Discriminant of Quadratic Fields 117
6.5. Discriminant of Cyclotomic Fields 118
Exercises 119

CHAPTER 7. The Decomposition of Ideals **123**
7.1. Dedekind's Theorem 123
7.2. Dedekind Domains 128
Exercises 133

CHAPTER 8. The Norm and Classes of Ideals **141**
8.1. The Norm of an Ideal 141
8.2. Classes of Ideals 145
Exercises 148

CHAPTER 9. Estimates for the Discriminant 153
9.1. The Theorem of Minkowski 153
9.2. Estimates of the Discriminant 158
Exercises 165

CHAPTER 10. Units 167
10.1. Roots of Unity 167
10.2. Units of Quadratic Fields 169
10.3. Units of Cyclotomic Fields 175
10.4. Dirichlet's Theorem 177
Exercises 184

CHAPTER 11. Extension of Ideals 189
11.1. Extension of Ideals 189
11.2. Decomposition of Prime Numbers in Quadratic Fields 198
11.3. Decomposition of Prime Numbers in Cyclotomic Fields 202
Exercises 204

CHAPTER 12. Algebraic Interlude 207
12.1. Rings of Fractions 207
12.2. Traces and Norms in Ring Extensions 213
12.3. Discriminant of Ring Extensions 226
Exercises 231

CHAPTER 13. The Relative Trace, Norm, Discriminant, and Different 233
13.1. The Relative Trace and Norm of an Ideal 233
13.2. Relative Discriminant and Different of Algebraic Number Fields 237
Exercises 256

CHAPTER 14. The Decomposition of Prime Ideals in Galois Extensions 259
14.1. Decomposition and Inertia 259
14.2. The Ramification 264
Exercises 271

CHAPTER 15. The Fundamental Theorem of Abelian Extensions 273
15.1. The Theorem of Kronecker and Weber 273
15.2. Class Field Theory 282
15.2.1. The Theory of Hilbert 283
15.2.2. The Theory of Takagi 283
Exercises 287

CHAPTER 16. Complements and Miscellaneous Numerical Examples 291
16.1. Some Algorithms 291
16.1.1. Calculation of the Minimal Polynomial, Trace and Norm of an Element 292
16.1.2. Calculation of the Discriminant of a Set $\{x_1, \ldots, x_n\}$ 293
16.1.3. Determination of an Integral Basis, Ring of Integers and Discriminant 293
16.1.4. Decomposition into Prime Ideals 294
16.2. Complements on Cyclotomic Fields 294
16.3. Some Cubic Fields 300
16.4. Biquadratic Fields 311
16.5. Binomial Extensions 314
16.6. Relative Binomial Extensions 320
16.7. The Class Number of Quadratic Extensions 325
16.8. Prime Producing Polynomials 330
Exercises 333

PART THREE 337

CHAPTER 17. Local Methods for Cyclotomic Fields 339
17.1. p-Adic and λ-Adic Numbers 339
17.1.1. The p-Adic Numbers 339
17.1.2. The λ-Adic Numbers 343
17.2. The λ-Adic Exponential and Logarithm 344
17.2.1. Formal Power Series 344
17.2.2. The λ-Adic Exponential and Logarithm 349
17.3. The λ-Adic Integers 355
Exercises 363

CHAPTER 18. Bernoulli Numbers 367
18.1. Algebraic Properties 367
18.1.1. Recurrence for the Bernoulli Numbers 367
18.1.2. Relations of Bernoulli Numbers with Trigonometric Functions 370
18.1.3. Bernoulli Numbers and the Zeta Function 372
18.1.4. Sums of Equal Powers of Successive Natural Numbers 377
18.1.5. Quadratic Identities 380
18.2. Arithmetical Properties 384
18.2.1. The Denominator of the Bernoulli Numbers 384
18.2.2. The Numerator of the Bernoulli Numbers 390
18.2.3. The Congruence of Kummer 392

Exercises 394

CHAPTER 19. Fermat's Last Theorem for Regular Prime Exponents 399
19.1. Regular Primes and the Lemma of Units 399
19.2. Kummer's Theorem 409
19.3. Irregular Primes 418
Exercises 425

CHAPTER 20. More on Cyclotomic Extensions 429
20.1. Resolution by Radicals of the Cyclotomic Equation 429
20.2. The Gaussian Periods 434
20.3. Lagrange Resolvents and the Jacobi Cyclotomic Function 438
20.4. On the Decomposition into Prime Ideals of the Cyclotomic Field 447
20.5. Generation of the Class Group of the Cyclotomic Field 454
Exercises 458

PART FOUR 461

CHAPTER 21. Characters and Gaussian Sums 463
21.1. Characters of Finite Abelian Groups 463
21.2. Modular Characters 472
21.3. Gaussian Sums 478
Exercises 482

CHAPTER 22. Zeta-Functions and *L*-Series 487
22.1. The Riemann Zeta-Function 487
22.2. *L*-Series 493
Exercises 498

CHAPTER 23. The Dedekind Zeta-Function 505
23.1. Asymptotic Expression for the Class Number 505
23.2. The Dedekind Zeta-Series 513
23.3. Hecke *L*-Series 518
Exercises 519

CHAPTER 24. Primes in Arithmetic Progressions 523
24.1. Proof of Dirichlet's Theorem 523
24.2. Special Cases 529
Exercises 541

CHAPTER 25. The Frobenius Automorphism and the Splitting of Prime Ideals 543

25.1. The Frobenius Automorphism 543
25.2. Density Results on the Decomposition of Prime Ideals 548
25.3. The Theorem of Chebotarev 552
25.4. Bauerian Extensions of Fields 563
Exercises 564

CHAPTER 26. Class Number of Quadratic Fields 567
26.1. The Quadratic Character Attached to the Quadratic Field 568
26.2. The L-Series and the Gaussian Sum of the Quadratic Character 573
26.3. The Class Number Formula and the Distribution of Quadratic Residues 583
Exercises 592

CHAPTER 27. Class Number of Cyclotomic Fields 595
27.1. The Class Number Formula 595
27.2. The Two Factors of the Class Number 599
Exercises 616

CHAPTER 28. Miscellaneous Results About the Class Number of Quadratic Fields 617
28.1. Divisibility Properties 617
28.2. Quadratic Fields with Class Number 1 636

CHAPTER 29. Miscellaneous Results About the Class Number of Cyclotomic Fields 639
29.1. Miscellanea About the Relative Class Number of $\mathbb{Q}(\zeta_p)$ 639
29.1.1. Determinantal Formulas for the Relative Class Number 640
29.1.2. Upper and Lower Bounds for the Relative Class Number 648
29.1.3. Cyclotomic Fields with Class Number 1 652
29.1.4. Growth of the Relative Class Number 653
29.1.5. Some Divisibility Properties of the Relative Class Number 656
29.2. Miscellanea About the Real Class Number of Cyclotomic Fields 659
29.3. The Class Number of $\mathbb{Q}(\zeta_m)$, $m > 2$ and Miscellaneous Results 661
29.3.1. The Class Number Formula 661
29.3.2. Divisibility Properties 662
29.3.3. Fields with Class Number 1 663

A Guide for Further Study 665

Bibliography **667**
Index of Names **673**
Subject Index **677**