Algebraic Number Fields Second Edition

Gerald J. Janusz

Graduate Studies in Mathematics

Volume 7



American Mathematical Society

Other Titles in This Series

- 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
- 3 William W. Adams and Philippe Loustaunau, An introduction to Gröbner bases, 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

Algebraic Number Fields

Second Edition

Gerald J. Janusz

Graduate Studies in Mathematics

Volume 7



American Mathematical Society

Editorial Board James E. Humphreys Lance W. Small

1991 Mathematics Subject Classification. Primary 11-01, 11R04, 11R29, 11R37.

Library of Congress Cataloging-in-Publication Data Janusz. Gerald J. Algebraic number fields / Gerald J. Janusz. — 2nd ed. p. cm. —(Graduate studies in mathematics, ISSN 1065-7339; v. 7) Includes bibliographical references. (p. -) and index. ISBN 0-8218-0429-4 (alk. paper) 1. Algebraic fields. 2. Class field theory. I. Title. II. Series. QA 247.J353 1996 512'.74—dc20 95-41431 CIP

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 (including abstracts) 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.

© Copyright 1996 by the American Mathematical Society. All rights reserved. Printed in the United States of America.

First edition © 1973 by Academic Press The American Mathematical Society retains all rights except those granted to the United States Government. © The paper used in this book is acid-free and falls within the guidelines established to ensure permanence and durability.

10 9 8 7 6 5 4 3 2 01 00 99 98 97

To Gregory and Julie

—who have made their parents very proud.

This page intentionally left blank

Contents

Prefaces	ix
Chapter I. Subrings of Fields	1
1. Localization	1
2. Integral Dependence	4
3. Discrete Valuation Rings and Dedekind Rings	7
4. Fractional Ideals and the Class Group	16
5. Norms and Traces	19
6. Extensions of Dedekind Rings	25
7. Ramification and the Discriminant	33
8. Norms of Ideals	42
9. Algebraic Integers	46
10. Cyclotomic Fields	52
11. Quadratic Reciprocity	59
12. Lattices in Real Vector Spaces	62
13. The Class Number and the Unit Theorem	67
Chapter II. Complete Fields	83
1. Valuations	83
2. Completions	90
3. Extensions of Nonarchimedean Valuations	100
4. Completions of Archimedean Valuations	108
5. The Topology of Completions of Number Fields	111
6. Local Norms and Traces and the Product Formula	114
Chapter III. Decomposition Groups and the Artin Map	121
1. Decomposition and Inertia Groups	121
2. The Frobenius Automorphism	125
3. The Artin Map for Abelian Extensions	130

CONTENTS

Chapter IV Analytic Methods and Bay Classes	135
1. Moduli and Bay Classes	135
2 Dirichlet Series	141
3 Characters of Abelian Groups	154
4 L-Series and Product Representations	156
5. The Frobenius Density Theorem	162
Chapter V. Class Field Theory	169
1. Cohomology of Cyclic Groups	169
2. Preparations for the Second Inequality	172
3. A Norm Index Computation	177
4. The Fundamental Equality for Cyclic Extensions	184
5. The Reciprocity Theorem	190
6. Ideal Groups, Conductors, and Class Fields	199
7. Reduction Steps toward the Existence Theorem	203
8. Kummer Extensions and the S-unit Theorem	205
9. The Existence Theorem	208
10. Some Consequences of the Classification Theorem	215
11. Norm Residues and the Conductor	218
12. The Hilbert Class Field	228
Chapter VI. Quadratic Fields	233
1. The Conductor of $\mathbf{Q}(\sqrt{d})$	233
2. Two Hilbert Class Fields	236
3. The Extended Class Group	241
4. The Class Number and L-functions	249
Appendix	261
A. Normal Basis Theorem and Hilbert's Theorem 90	261
B. Modules over Principal Ideal Domains	263
C. Representation of Permutation Groups and Gauss Sums	266
References	273
Index	275

viii

PREFACE TO THE SECOND EDITION

The main objective of this new edition remains the same as that of the first edition: to give an exposition of the introductory material and the main theorems about class fields of algebraic number fields while placing the minimum prerequisite demands on the reader. Although the basic outline remains the same, some new material has been added, many proofs have been expanded, and corrections have been made where errors in the first edition were found. Some of the additions to this edition are new treatments of some examples, emphasizing the use of the regular representation to do some calculations, a theorem determining the ring of integers in a number field with a finite amount of computation. The section on the topology of complete fields has been enlarged to correct a common error found in several texts regarding the existence of completions. A new section has been added giving the class number formula for quadratic fields. Some new exercises have been added. This edition was rekeyed (since no electronic version of the first edition exists) so that every line was rewritten.

The author expresses his thanks to the students and faculty at the University of Illinois, as well as many others, who have used this text and made comments regarding its improvement. Special thanks to Steve Ullom, Kurt Foster, Gennadii V. Matveev, and the late Irving Reiner, who sent comments and corrections to the first edition.

> –GJJ August 1995

Preface to the First Edition

This book contains an exposition of the main theorems of the class field theory of algebraic number fields along with the necessary introductory material. An attempt is made to keep the exposition self-contained. The only material presupposed is that which would be used in elementary Galois theory. The structure theorem for finitely generated modules over a principal ideal domain is used, but a proof is included in the appendix.

We use the direct approach to the subject by congruence subgroups of the ideal group rather than the more subtle description involving the cohomology of groups. This may be considered the historical approach to the subject, but we have presented it because it seems most useful for mathematicians who are specialists in other areas but wish to use it. From the student's point of view, this approach seems to require less background preparation and so is desirable for them.

PREFACES

The student who is not particularly interested in the theory of class fields can profitably read the first three chapters for an introduction to the study of arithmetic in fields, Dedekind domains, valuations, and general background material necessary for further work in several directions.

The first chapter contains an introduction to the algebra of number theory. The basic properties of Dedekind domains are presented using rather general ring theoretic arguments as much as possible. Emphasis is placed on local methods and proofs by localization. The results are given for rather general fields except in the last three sections. There we discuss cyclotomic extensions of the rational field and prove the unit theorem and the finiteness of the class number for algebraic number fields.

Valuations and complete fields are discussed in the second chapter. This depends partly on the previous chapter.

Chapter three contains material connecting Galois groups and ramification. The last section gives properties of the Artin map, which are of fundamental importance for the rest of the book.

In Chapter four the material becomes more specialized. We work exclusively with algebraic number fields and their completions. The analytic theorems proved include the Frobenius density theorem and Dirichlet's theorem on primes in arithmetic progression.

Chapter five contains the main results on class fields. A small amount of cohomology is developed here. We use only H^0 and H^1 and then only for cyclic groups. In this case a concrete description of the cohomology groups is used so the reader is not carried far from the fields and Galois groups. The approach to the main theorems makes systematic use of the Artin map and the Artin reciprocity theorem. We close the chapter with a discussion of the Hilbert class field and Artin's reduction of the principal ideal theorem.

The last chapter is intended primarily for illustration of the concepts introduced in the earlier chapters. We study mainly quadratic fields and prove a result which goes back to Gauss giving information about the class group of a quadratic number field. A few calculations are made to illustrate the use of the norm residue symbols.

The material in this text was used in a year-long course at the University of Illinois in 1970-1971. The first three chapters were covered in the first semester and the balance in the second semester.

REFERENCES

- 1. E. Artin, Theory of Algebraic Numbers, Lecture Notes, Göttingen, 1959.
- 2. E. Artin and J. Tate, Class Field Theory, Benjamin, New York, 1967.
- 3. A. Baker, Linear forms in the logarithms of algebraic numbers, Mathematika 13 (1966), 204–216.
- Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York, 1967.
- J. Cassels & A. Fröhlich, Eds., Algebraic Number Theory, Thompson Publ., Washington, D.C., 1967.
- Ph. Furtwangler, Beweis des Hauptidealsatzes f
 ür Klassenkörper algebraischer Zahlenkörper, Abhand. Math. Seminar Hamburg 7 (1930), 14–36.
- L. J. Goldstein, Analytic Number Theory, Prentice-Hall, Englewood Cliffs, N. J., 1971.
- 8. H. Hasse, Vorlesungen über Klassenkörpertheorie, Physica, Wurzburg, 1967.
- E. S. Golod and I. R. Shafarevich, On the class-field tower, Izvestiya Akad. Nauk. SSSR 28 (1964), 261–272. (Russian)
- Neal Koblitz, p-adic Numbers, p-adic Analysis, and Zeta-Functions, Springer-Verlag, Berlin, Heidelberg, and New York, 1977.
- 11. Serge Lang, Algebra, Addison-Wesley, Reading, Mass., 1965.
- 12. Serge Lang, Algebraic Number Theory, Addison-Wesley, Reading, Mass., 1970.
- 13. James Munkres, Topology, Prentice Hall, Englewood Cliffs, NJ, 1975.
- 14. J. Neukirch, Klassenkörpertheorie, Universität Bonn, Bonn, 1967.
- 15. J. P. Serre, Corps Locaux, Hermann, Paris, 1962.
- Andreas Speiser, Die Zerlegungsgruppe, J. f
 ür die Reine und Angew. Math. 149 (1919), 174–188.
- 17. H. M. Stark, A complete determination of complex quadratic fields of class number one, Mich. Math J. 14 (1967), 1–27.
- 18. A. Weil, *Basic Number Theory*, Springer-Verlag, Berlin, Heidelberg, and New York, 1967.
- 19. E. Weiss, Algebraic Number Theory, McGraw Hill, New York, 1963.

This page intentionally left blank

Index

Abelian extension, 128 Absolute norm, 44 Absolute values, 82 equivalent, 82 Algebraic integer, 46 Algebraic number field, 46 Approximation Theorem, 135 Archimedean valuation, 83 Artin map, 128 local, 219 nonabelian case, 213 product formula, 223 Artin Reciprocity Theorem, 194 Artin's Lemma, 191 Cauchy sequence, 89,100 Centrally symmetric, 65 Character, 152 principal, 152 Characteristic polynomial, 21 Class field, 199 Class group, 19, 199 extended, 238 Class number, 19, 72, 249 Classification Theorem, 211 Cohomology groups, 167 Cokernel, 182 Complete DVR, 103 Complete field, 89 Complete ring, 101 Completely split prime, 125 Completion theorem, 92 Completion, 92 Complex prime, 109 Composite field, 49 Conductor, 199 local, 221 Congruence subgroup, 196 Convex set, 65 Counting norm, 44 Cyclotomic extension, 188 Cyclotomic field, 52 Cyclotomic polynomials, 163

Decomposition group, 119, 216 Dedekind ring, 8 Dirichlet density, 158 Dirichlet series, 139 Dirichlet's Theorem, 164 Dirichlet-Chevalley-Hasse Unit Theorem, 204 Discrete valuation ring, 7, 86 Discriminant, 33, 39 Division, 160 Dual basis, 25 DVR, 7, 86

Equivalent absolute values, 82 Euler function, 52 Exact Hexagon Lemma, 167 Exponent, 202 Exponential valuation, 85 Extended class group, 238 Extended genus field, 240

Finite prime, 88
First Fundamental Inequality, 163
First Inequality, 163
Fractional ideal, 16
Frobenius automorphism, 123, 128 density theorem, 160
Full lattice, 63
Fundamental parallelepiped, 63
Fundamental unit, 78

Gauss sum, 250, 265 with real characters, 268 Genus field, 240

Hasse Norm Theorem, 186 failure of, 212 Hensel's lemma, 104 Herbrand quotient, 168 Hilbert Class Field, 73, 225 extended, 238

INDEX

Ideal group, 19, 199 Inertia field, 122 Inertia group, 121 Infinite prime, 88 Integral closure, 5 Integral dependence, 4 Integral ideal, 16, 143 Integral normal basis, 196 Inverse ideal, 16 Invertible, 17

Kronecker-Weber Theorem, 195 Kummer extension, 202

L-series, 154 Lattice, 63 Laurent series, 118 Legendre symbol, 59 Linearly disjoint, 57 Local Artin map, 219 Local class field theory, 225 Local norm, 185 Local ring, 3 Localization, 2, 3

Minimum polynomial, 6 Minkowski's Theorem, 65 Modulus, 134 Multiplicative congruence, 134 Multiplicative set, 1

Nakayama's Lemma, 4 Nonarchimedean valuation, 83 Nondegenerate form, 21 Norm residue symbol, 219 Norm, 20, 111 local, 185 of an ideal, 42

Permutation groups, 262 Permutation module, 262 PID, 6 Prime ideal, 2 Prime, of a field, 88, 109 Primitive character, 265 Principal ideal domain, 6 Principal Ideal Theorem, 226 of group theory, 227Product formula, for Artin maps, 223 for valuations, 88, 116

Quadratic character, 247 Quadratic reciprocity, 59 Quotient field, 2

Ramification index, 29 Ramified prime, 33 Ray class group, 135 Ray classes, 135 Real prime, 109 Reciprocity law, 187 Regular representation, 19, 263 Regulator, 150 of a number field, 78 Relative degree, 30 Riemann ζ -function, 139, 248

S-units, 171 Second inequality, 163

Tchebotarev Density Theorem, 214 Totally positive, 238 Totally ramified, 32, 121 Trace, 20 Transfer, 226 Triangle inequality, 83

UFD, 6 Unique factorization, 6

Valuation, 83 p-adic, 85 discrete, 86 exponential, 85 Van der Monde matrix, 23, 39 Volume of a lattice, 63

Zeta function of K, 143 Riemann's, 139, 248

276



