CAMBRIDGE STUDIES IN
ADVANCED MATHEMATICS 27

ALGEBRAIC NUMBER THEORY

Already published

1 W.M.L. Holcombe *Algebraic automata theory*
2 K. Petersen *Ergodic theory*
3 P.T. Johnstone *Stone spaces*
4 W.H. Schikhof *Ultrametric calculus*
5 J.-P. Kahane *Some random series of functions, 2nd edition*
6 H. Cohn *Introduction to the construction of class fields*
7 J. Lambek & P.J. Scott *Introduction to higher-order categorical logic*
8 H. Matsumura *Commutative ring theory*
9 C.B. Thomas *Characteristic classes and the cohomology of finite groups*
10 M. Aschbacher *Finite group theory*
11 J.L. Alperin *Local representation theory*
12 P. Koosis *The logarithmic integral I*
13 A. Pietsch *Eigenvalues and s-numbers*
14 S.J. Patterson *An introduction to the theory of the Riemann zeta-function*
15 H.J. Baues *Algebraic homotopy*
16 V.S. Varadarajan *Introduction to harmonic analysis on semisimple Lie groups*
17 W. Dicks & M. Dunwoody *Groups acting on graphs*
18 L.J. Corwin & F.P. Greenleaf *Representations of nilpotent Lie groups and their applications*
19 R. Fritsch & R. Piccinini *Cellular structures in topology*
20 H Klingen *Introductory lectures on Siegel modular forms*
21 P. Koosis *The logarithmic integral II*
22 M.J. Collins *Representations and characters of finite groups*
24 H. Kunita *Stochastic flows and stochastic differential equations*
25 P. Wojtaszczyk *Banach spaces for analysts*
26 J.E. Gilbert & M.A.M. Murray *Clifford algebras and Dirac operators in harmonic analysis*
28 K. Goebel & W.A. Kirk *Topics in metric fixed point theory*
29 J.F. Humphreys *Reflection groups and Coxeter groups*
30 D.J. Benson *Representations and cohomology I*
31 D.J. Benson *Representations and cohomology II*
33 C. Soulé, D. Abramovich, J.-F. Burnol & J. Kramer *Lectures on Arakelov Geometry*

ALGEBRAIC NUMBER THEORY

A. Fröhlich, FRS
Imperial College, London and
Robinson College, Cambridge

M. J. Taylor
UMIST, Manchester

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1991
First paperback edition 1993, 1994

Library of Congress cataloguing in publication data available
British Library cataloguing in publication data available

ISBN 0 521 36664 X hardback
ISBN 0 521 43834 9 paperback

Transferred to digital printing 2000

To our long suffering wives,
Ruth and Sharon

Contents

Preface

There are many attractive and instructive topics which can, and should, be included in an introductory, but moderately ambitious, text book on algebraic number theory. But – as if by a conspiracy of silence – they are usually either omitted altogether, or, at best, are treated inadequately in the existing array of texts available. One of our aims in writing this book has been to try to break free from this standard mould, and to fill these gaps. As instances we mention cubic and biquadratic fields, Gaussian periods, Brauer relations, module theory over a Dedekind domain, an algebraic number theoretic treatment of binary quadratic forms, tame ramification and the two-classgroup of a quadratic field.

Conceptually the book breaks fairly neatly into two parts: the first four chapters and the final chapter are, for the most part, of a theoretical nature, though we always take care to fix abstract ideas by means of worked examples; the remaining three chapters are devoted to giving a detailed study of various arithmetic objects in situations of particular interest.

Throughout the text we have laid great stress on worked examples; it is a depressing fact that many number theorists have never acquired sufficient technique to perform number theoretic calculations in anything but a quadratic field. Again, this is, to some extent, the fault of the existing literature, where scant emphasis is placed on calculations.

On the whole we have opted for schematic exposition, rather than attempting an evolutionary or historical development of the subject mat-

ter. Thus, for instance, Diophantine equations now become an application of the theory; whereas, of course, historically they were the principal motivation for the development of the theory.

This book has its origins in various lecture courses given by the authors at Cambridge Part III and M.Sc. level; however, in its later sections, we go beyond these courses. What we require is roughly the knowledge of a third year undergraduate. More precisely, somewhere along the line the reader will be supposed to have some familiarity with elementary point set topology, with elementary Galois theory, and with basic module theory, including tensor products and the structure theorem for finitely generated modules over a principal ideal domain.

In its undiluted form, the book is best suited to a two semester course at Masters level. We therefore now describe how it may be used for a more minimal, one semester course. Needless to say, in general the prospective lecturer should concentrate on the main theorems and omit much of the other surrounding material.

In all cases we would suggest that Chapter 1 be used as background material; it is only intended to serve as a ready source of reference for a number of elementary algebraic facts which may be new to the reader. By contrast, (II, §1) up to and including Theorem 5 and then (II.1.31, 32) are fundamental; they contain the genesis of a whole host of ideas which are basic to the subject. The notions of valuation and absolute value in (II, §2) are used repeatedly throughout; and from (II, §3) one needs the basic definitions together with Theorems 10 and 11; however, the final section on module theory for Dedekind domains can, for the most part, be omitted without serious disadvantage.

In Chapter III we consider the behaviour of many of the concepts introduced in the previous chapter when they are extended from a given number field to an extension field. Again much of the material can be omitted for the purposes of a short course. In §1, Theorem 18 can certainly be omitted. In §2 the minimalist may omit the general definition of a discriminant, and get by with the absolute discriminant of (II, §1); on the other hand, Theorem 22 (Dedekind's theorem on the ramification of divisors of the discriminant) and Theorem 23 (Kummer's criterion for the decomposition of prime ideals in an extension) are quite important. All of §4 can be omitted, and the only results of §3 which are essential are those that concern cyclotomic extensions.

Chapter IV concerns the application of convex body theory to the study of classgroups and units, i.e. the topic usually referred to as Minkowski methods. This is the most standard chapter in the book; it is also the briefest and some form of it will be required.

Having dealt with the basic theory, the reader is then in the agreeable position of being faced with a kind of Smørgasbord of choices of applications and further developments. We therefore list some of the options available. Chapter V begins with the important and traditional theory of quadratic fields. This would seem to us to be an essential ingredient of any course in algebraic number theory. The chapter then concludes with sections on biquadratic and cubic number fields. Chapter VI is devoted to the theory of cyclotomic fields. In our opinion, this is the most elegant chapter of the book. In Chapter VII we consider various kinds of Diophantine equations: Fermat's Last Theorem, quadratic forms and finally various cubic results. The main text then concludes with sections on Dedekind zeta-functions and L-functions. Since these are the most powerful methods in the whole book, it would be regrettable if too much of this chapter were omitted.

As additional aids to the reader we also include an Appendix on the character theory of Abelian groups, and a wide range of exercises.

The authors wish to express their thanks to Robin Chapman for his detailed reading of the initial manuscript of the book: his comments and suggestions have been of great help. Thanks also go to David Burns for his mathematical reading of the proof script, and to Jean Cougnard for giving us access to his tables of biquadratic number fields. In addition we wish to thank Bryan Birch for permission to use many of the exercises from his Oxford question sheets.

Last – but by no means least – it is a pleasure to acknowledge the help and co-operation that David Tranah has provided, on behalf of Cambridge University Press, in the production of this text.

Notation

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the natural numbers, the integers, the rational numbers, the real numbers, the complex numbers respectively.

For two sets A and B, $A \subset B$ means A is contained in B, and $A \subsetneqq B$ denotes strict containment. The number of elements in a finite set A will be denoted by $|A|$ or by $\mathrm{card}(A)$.

The term ring is always to be understood as meaning a commutative ring with a multiplicative identity; S will be called a subring of a ring R if, in addition to the usual requirements, their multiplicative identities coincide. The group of units of a ring R, i.e. the group of multiplicatively invertible elements in R, will be denoted by R^*. Ideals of R will also be referred to as R-ideals. Our use of the term prime is slightly non-standard and therefore deserves special mention: unless stated to the contrary, we always use this term to mean non-zero prime ideal.

The sequence $A \xrightarrow{f} B \xrightarrow{g} C$ is aid to be exact if $\mathrm{im}(f) = \ker(g)$, where A, B, C are modules over a given ring R, and f, g are R-homomorphisms. Thus, in particular $0 \to A \xrightarrow{f} B$ is exact at A if f is injective; $B \xrightarrow{g} C \to 0$ is exact at C if g is surjective. With the same notation the triangle

$$\begin{tikzcd} & B \arrow[dr, "g"] & \\ A \arrow[ur, "f"] \arrow[rr, "h"] & & C \end{tikzcd}$$

is said to *commute* if $g \circ f = h$. Similar terminology applies to commutative squares etc.

Given two groups $H \subset G$, of finite index, we write $[G: H]$ for that index. The degree of a finite extension of fields L/K is denoted by $(L: K)$; if the extension is Galois, we write $\mathrm{Gal}(L/K)$ for the Galois group of L/K. Finally, we remark that in general we use the abbreviation iff for "if, and only if".