ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

EDITED BY G.-C. ROTA

Algorithmic algebraic number theory

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

6 H. Minc *Permanents*
18 H. O. Fattorini *The Cauchy problem*
19 G. G. Lorentz, K. Jetter, and S. D. Riemenschneider *Birkhoff interpolation*
22 J. R. Bastida *Field extensions and Galois theory*
23 J. R. Cannon *The one-dimensional heat equation*
25 A. Salomaa *Computation and automata*
27 N. H. Bingham, C. M. Goldie, and J. L. Teugels *Regular variation*
28 P. P. Petrushev and V. A. Popov *Rational approximation of real functions*
29 N. White (ed.) *Combinatorial geometries*
30 M. Pohst and H. Zassenhaus *Algorithmic algebraic number theory*
31 J. Aczel and J. Dhombres *Functional equations containing several variables*
32 M. Kuczma, B. Chozewski, and R. Ger *Iterative functional equations*
33 R. V. Ambartzumian *Factorization calculus and geometric probability*
34 G. Gripenberg, S.-O. Londen, and O. Staffans *Volterra integral and functional equations*
35 G. Gasper and M. Rahman *Basic hypergeometric series*
36 E. Torgersen *Comparison of statistical experiments*
37 A. Neumaier *Interval methods for systems of equations*
38 N. Korneichuk *Exact constants in approximation theory*
39 R. A. Brualdi and H. J. Ryser *Combinatorial matrix theory*
40 N. White (ed.) *Matroid applications*
41 S. Sakai *Operator algebras in dynamical systems*
42 W. Hodges *Model theory*
43 H. Stahl and V. Totik *General orthogonal polynomials*
44 R. Schneider *Convex bodies*
45 G. Da Prato and J. Zabczyk *Stochastic equations in infinite dimensions*
46 A. Bjorner, M. Las Vergnas, B. Sturmfels, N. White, and G. Ziegler *Oriented matroids*
47 E. A. Edgar and L. Sucheston *Stopping times and directed processes*
48 C. Sims *Computation with finitely presented groups*
49 T. Palmer *Banach algebras and the general theory of *-algebras I*
50 F. Borceux *Handbook of categorical algebra I*
51 F. Borceux *Handbook of categorical algebra II*
52 F. Borceux *Handbook of categorical algebra III*
54 A. Katok and B. Hasselblatt *Introduction to the modern theory of dynamical systems*
55 V. N. Sachkov *Combinatorial methods in discrete mathematics*
56 V. N. Sachkov *Probabilistic methods in combinatorial analysis*
57 P. M. Cohn *Skew fields*
58 Richard J. Gardner *Geometric tomography*
59 George A. Baker, Jr., and Peter Graves-Morris *Padé approximants*
60 Jan Krajíček *Bounded arithmetic, propositional logic, and complexity theory*
61 H. Groemer *Geometric applications of Fourier series and spherical harmonics*
62 H. O. Fattorini *Infinite dimensional optimization and control theory*
63 A. C. Thompson *Minkowski geometry*
64 R. B. Bapat and T. E. S. Raghavan *Nonnegative matrices and applications*
66 D. Cvetković, P. Rowlinson and S. Simić *Eigenspaces of graphs*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Algorithmic algebraic number theory

M. POHST
University of Düsseldorf

H. ZASSENHAUS
Late, Ohio State University

CAMBRIDGE
UNIVERSITY PRESS

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge CB2 1RP, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, United Kingdom
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1989
Reprinted 1990, 1993
First paperback edition 1997

Typeset in Times 10/13 pt

A catalogue record for this book is available from the British Library

Library of Congress Cataloguing in Publication data

Pohst, M.
Algorithmic algebraic number theory/M. Pohst and H. Zassenhaus.
p. cm. Bibliography: p.
Includes index.
ISBN 0 521 33060 2
1. Algebraic number theory. 2. Algorithms. I. Zassenhaus, Hans. II. Title
QA247.P58 1989
512′.74—dc19 88-2960 CIP

ISBN 0 521 33060 2 hardback
ISBN 0 521 59669 6 paperback

Transferred to digital printing 2002

CONTENTS

PREFACE

This book is a first step in a new direction: to modify existing theory from a constructive point of view and to stimulate the readers to make their own computational experiments. We are thoroughly convinced that their observations will help to build a new basis from which to venture into new theory on algebraic numbers. History shows that in the long run, number theory always followed the cyclic movement from theory to construction to experiment to conjecture to theory.

Consequently, this book is addressed to all lovers of number theory. On the one hand, it gives a comprehensive introduction to (constructive) algebraic number theory and is therefore especially suited as a textbook for a course on that subject. On the other hand, many parts go far beyond an introduction and make the user familiar with recent research in the field. For experimental number theoreticians we developed new methods and obtained new results (e.g., in the tables at the end of the book) of great importance for them. Both computer scientists interested in higher arithmetic and in the basic makeup of digital computers, and amateurs and teachers liking algebraic number theory will find the book of value.

Many parts of the book have been tested in courses independently by both authors. However, the outcome is not presented in the form of lectures, but, rather, in the form of developed methods and problems to be solved. Algorithms occur frequently throughout the presentation. Though we do not give a thorough definition of an algorithm (but just a rough explanation in 1.1), the underlying idea is that a definite output is obtained from prescribed input data by certain arithmetical rules in a finite number of computational steps. Clearly, an upper bound for the number of those computational steps depending on the input data should be desirable in each case. However, the bounds obtainable for many well-known, frequently used algorithms are completely unrealistic. Hence, we usually do without a complexity analysis.

(The derivation of rough estimates is a good exercise for the reader interested in that topic, however.) This approach is justified by the fact that the algorithms under consideration yield good to excellent results for number fields of small degree and not too large discriminants. In those cases O-estimates are not very helpful in general. Rather, our intention is to make the readers conscious of weak performances of (parts of) algorithms and to strengthen their ability to improve them. From our experiences those weak links in the chain of operations can be detected often only by numerical computation. Hence, we highly recommend the interaction of developing algorithms, observing their performance in practical application, followed by improving them.

Moreover, new algorithms are used to replace older proofs of theorems by means of using their output to show the existence of certain mathematical objects, such as the shortest vector in a lattice, or of a polynomial in the elementary symmetric functions representing an arbitrary symmetric function (principal theorem on symmetric functions). Any such algorithm – respectively, its performance for specified data – yields new observations, giving rise to new conjectures and thus to an improvement of the theory. That is one of the major goals of this book since many of the available numerical invariants of algebraic number fields were already obtained without the use of modern electronic computers. So there is still very little known about algebraic number fields other than abelian extensions of the rational number field.

The contents of the book are divided into six chapters. The first chapter serves as a kind of an introduction. Some basic material (e.g. the Euclidean algorithm, quadratic extensions, Gaussian integers) is to stimulate the readers and to make them curious for more systematic theory. The second chapter gives a self-contained account of Galois theory and elementary prerequisites (e.g. a good knowledge of finite field theory). The reader is introduced to E. Galois' idea of studying the algebraic relations between the roots of a given algebraic equation and thus to recognition of the algebraic background generated by the solutions. Eventually, a method of determining the Galois group of an equation is developed.

The third chapter contains an independent introduction to those parts of the geometry of numbers which will be used in later chapters. Most of Minkowski's classical theorems are presented, as well as some recent reduction methods. The fourth chapter discusses the problem of embedding an equation order into its maximal order, thereby establishing the arithmetical background of a given equation. An algorithm for the computation of an integral basis of an algebraic number field is included. A local account (using valuation theory and the theory of algebraically ordered fields) of the Hilbert–Dedekind–Krull ideal theory is part of the exposition.

The last two chapters deal with the main difference between arithmetics of the rational numbers and of the higher algebraic number fields. Chapter 5 gives a logarithm free proof of Dirichlet's famous unit theorem. It is followed by developing several methods (some new ones) for the computation of the roots of unity and of a full system of fundamental units of an order. In chapter 6 the maximal order of an algebraic number field is studied as a Dedekind ring. We then present efficient methods for the computation of the class number and the class group of an algebraic number field. Primarily they are based on a normal presentation of an ideal by two elements and a fast method for solving norm equations, both of them developed only recently. As an Appendix we present several tables with numerical data concerning the calculation of Galois groups, integral bases, unit groups and class groups.

Chapters 1–4 are essentially self-contained, using only formal results but no conceptual theory of other chapters. The last two chapters rely on the knowledge of parts of chapters 3 and 4; chapter 6 also on parts of chapter 5. Throughout this book, we only assume that the readers have a proper basic knowledge of algebra. Should they not be familiar with some topic supposed to be known they will certainly find it in the book on algebra by S. Lang to which we refer quite frequently in the early chapters. We have also provided a bibliography for each chapter at the end of the book.

We hope to succeed in encouraging some of our readers to engage in enlightened experimentation with numbers and obtain deeper insights into their structure.

M. Pohst
H. Zassenhaus 1987

Preface to paperback edition

Since the first edition of this book in 1989 algorithmic algebraic number theory has developed rapidly. In order to keep the changes to a minimum I have mainly corrected the many typos and errors which have been found. The new developments are sketched in a new chapter with numerous references.

Unfortunately, my coauthor Hans Zassenhaus, one of the pioneers of computational algebraic number theory, passed away on 21 November, 1991. The mathematical community lost one of its outstanding members and a great person.

M. Pohst

ACKNOWLEDGEMENTS

We are much indebted to many students and colleagues for valuable suggestions, criticisms and incentives to do better. In particular we wish to acknowledge the help of D. Shanks, John McKay and J. Buchmann.

We wish to acknowledge the generous support of the production of the manuscript and the research which went into it which we received from the Department of the Ohio State University, the Mathematical Institute of the University of Düsseldorf, the National Science and Engineering Council of Canada and the Centre de Recherches Mathématiques, Université de Montréal.

Our thanks go out to the continued support and interest by the editors of Cambridge University Press, M. Gilchrist and D. Tranah, as well as to the production staff of the Encyclopedia of Mathematics and its Applications.

We would also like to acknowledge the help in proof reading we received from U. Schröter, M. Slawik, J. von Schmettow and essentially by U. Halbritter, and we thank the many secretaries who typed parts of the manuscript.

We were constantly encouraged in completing the work by the support and understanding of our wives Christel and Lieselotte.

My thanks go to Katherine Roegner and to the members of the KANT group, who helped me in locating most of the errors of the first edition. I also thank Cambridge University Press for their kind support during the preparation of the paperback edition.

SYMBOLS USED IN THE TEXT

Symbols used throughout the book are listed in connection with the mathematical terms with which they are associated in the text.

Arithmetic

δ_{ij} is Kronecker's symbol; it is one for $i = j$, zero otherwise;
sign(x) is one for $x > 0$, minus one for $x < 0$, 0 for $x = 0$, $|x| = \mathrm{sign}(x)x$;
$\lfloor x \rfloor$ denotes the largest integer less than or equal to x;
$\lceil x \rceil$ denotes the smallest integer greater than or equal to x;
$\{x\}$ denotes the integer closest to x, for $x + \frac{1}{2} \in \mathbb{Z}$ it is either $x + \frac{1}{2}$ or $x - \frac{1}{2}$;
$a|b$ means that there is an element c satisfying $b = ac$;
$a \nmid b$ means that there is no element c satisfying $b = ac$;
$p^k \| b$ means that $p^k | b$ and $p^{k+1} \nmid b$;
gcd denotes the greatest common divisor;
lcm denotes the least common multiple;
glb denotes the greatest lower bound;
$a \equiv b \bmod c$ means that $c|(a - b)$;
$a = Q(a, b)b + R(a, b)$ denotes division with remainder in a Euclidean ring;
$\gcd(a, b) = X(a, b)a + Y(a, b)b$ denotes a presentation of the *gcd* in a Euclidean ring;
$\mathrm{Re}(a), \mathrm{Im}(a)$ real, respectively imaginary part of $a \in \mathbb{C}$;
$\max\{a_1, \ldots, a_k\}$ denotes $a \in \mathbb{R}$ satisfying $a \in \{a_1, \ldots, a_k\}$ and $a \geqslant a_i$ $(1 \leqslant i \leqslant k)$.

Functions and mappings

Γ, φ, μ denote the Gamma function, Euler φ-function, Möbius μ-function, respectively;
$\mathrm{id} = \mathbf{1}$ identity mapping, $\mathbf{1}$ also the identity permutation;
ker denotes the kernel of a homomorphic mapping;
D_t derivation with respect to the variable t;

N, Tr norm, respectively trace;
ind index in finite fields.

Groups

$\mathfrak{S}_n$ symmetric group on n letters;
$\mathfrak{A}_n$ subgroup of $\mathfrak{S}_n$ consisting of all even permutations;
$\mathfrak{V}_4$ the Klein Four Group;
Hol the holomorph of a group;
$\rtimes$ denotes the semidirect product of two groups;
$\wr$ denotes the wreath product;
D_{2n} dihedral group on n letters;
ord(x) order of the group element x.

Matrices

I_n denotes the $n \times n$ unit matrix;
diag$(a_1, \ldots, a_n)$ denotes the $n \times n$ matrix $(a_{ij})_{1 \leqslant i,j \leqslant n}$ with $a_{ii} = a_i$ $(1 \leqslant i \leqslant n)$ and $a_{ij} = 0$ for $i \neq j$;
det(M) determinant of the matrix M;
$H(M)$ Hermite normal form of the matrix M;
$GL(r, \mathbb{Z})$, $SL(r, \mathbb{Z})$ general linear group, special linear group of degree r.

Orders

$\mathfrak{D}(\Lambda/R)$ discriminant ideal of the R-order Λ;
$\mathfrak{D}_0(\Lambda/R)$ reduced discriminant ideal;
AR(Λ) arithmetic radical;
$\mathfrak{E}_i(\Lambda/R)$ elementary ideals $(i \in \mathbb{Z}^{\geqslant 0})$;
$\mathfrak{N}(\Lambda/R)$ exponent ideal;
$(\Lambda :_R \tilde{\Lambda})$ index ideal;
$(\Lambda :_R 0)$ order ideal;
Tor(Λ/R) set of all x of Λ for which there exists a non-zero divisor $\lambda \in R$ such that $\lambda x = 0$.

Polynomials

$d(f)$ discriminant of the polynomial f;
deg(f) degree of f;
$l(f)$ denotes the coefficient of the term of f of highest degree;
Res(f, g) resultant of the polynomials f, g;
$P_{\xi/\mathbb{Q}}$ principal polynomial of ξ over $\mathbb{Q}$;
$M_{\xi/\mathbb{Q}}$ minimal polynomial of ξ over $\mathbb{Q}$.

Rings and fields

$C(R)$ center of the ring R;
$\mathfrak{Q}(R)$ quotient ring of R;
$J(R)$ Jacobson radical;
$\mathrm{NR}(R)$ nilradical;
PID principal ideal domain;
$[A/B] = \{x \in R \mid xB \subseteq A\}$ for subsets A, B of the ring R;
$\simeq_R$ R-isomorphic;
$\dot{+}$ inner direct sum (see 1. (3.8));
$\oplus$ direct sum;
$\otimes_R$ tensor product over R;
$F^\times = F \backslash \{0\}$ for fields F.

Algebraic number fields F

$o_F = \mathrm{Cl}(\mathbb{Z}, F)$ ring of algebraic integers of F;
d_F discriminant of F (respectively of o_F);
$\beta^{(j)}$ jth conjugate of $\beta \in F$;
$U(R)$ unit group of the order R of F, $U_F := U(o_F)$;
$TU(R)$ torsion subgroup (elements of finite order) of $U(R)$;
$\mathrm{Reg}(U(R))$ regulator of $U(R)$, $\mathrm{Reg}_F = \mathrm{Reg}(U_F)$;
I_R semigroup of R-fractional ideals of the order R of F;
H_R group of principal R-fractional ideals;
h_R class number of R, $h_F := h_{o_F}$;
Cl_F class group of F;
$\alpha \sim \beta \Leftrightarrow \alpha/\beta \in U(R)$;
$R_A := \{\beta \in o_F \mid \beta A \subseteq A\}$ for subsets A of o_F.

Special sets of numbers

$\mathbb{N}, \mathbb{P}, \mathbb{Z}$ natural numbers, prime numbers, rational integers, respectively;
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ rational numbers, real numbers, complex numbers, respectively;
$\mathbb{F}_q$ finite field of $q = p^n$ elements ($p \in \mathbb{P}, n \in \mathbb{N}$); $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/p$;
$\mathbb{Z}^{\leqslant m}$ all $x \in \mathbb{Z}$ subject to $x \leqslant m$ (analogously $\mathbb{Z}^{\geqslant m}, \mathbb{Z}^{<m}, \mathbb{Z}^{>m}$);
$[a, b]$ interval of real numbers x satisfying $a \leqslant x \leqslant b$.

Other

$|S| = \#S$ denotes the number of elements of the set S;
$\| \ \|$ denotes the norm of a vector;
$\langle S \rangle$ denotes the generation of a subgroup, subring, etc. by the elements of the set S;
$\lim\limits_{t \to 1} = \lim\limits_{\substack{t \to 1 \\ t > 1}}$;
$\square$ marks the end of a proof.

We refer to a formula or theorem of the same chapter by its number $(m.n)$, where m denotes the number of the corresponding section and n the number within that section. Formulae of different chapters are referred to by also listing the number of that chapter, for example 2 (11.12).