ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

EDITED BY G.-C. ROTA

VOLUME 20

Finite fields

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

4 W. Miller, Jr. *Symmetry and separation of variables*
6 H. Minc *Permanents*
11 W. B. Jones and W. J. Thron *Continured fractions*
12 N. F. G. Martin and J. W. England *Mathematical theory of entropy*
18 H. O. Fattorini *The Cauchy problem*
19 G. G. Lorentz, K. Jetter, and S. D. Riemenschneider *Birkhoff interpolation*
21 W. T. Tutte *Graph theory*
22 J. R. Bastida *Field extensions and Galois theory*
23 J. R. Cannon *The one-dimensional heat equation*
25 A. Salomaa *Computation and automata*
26 N. White (ed.) *Theory of matroids*
27 N. H. Bingham, C. M. Goldie, and J. L. Teugels *Regular variation*
28 P. P. Petrushev and V. A. Popov *Rational aproximation 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. London, and O. Staffans *Volerra 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 appoximation 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 G. 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*
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*
57 P. M. Cohn *Skew fields*
58 R. Gardner *Geometric tomography*
60 J. Krajiček *Bounded arithmetic, propositional logic and complexity theory*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Finite fields

Rudolf Lidl
University of Tasmania
Hobart, Australia

Harald Niederreiter
Austrian Academy of Sciences
Vienna, Austria

Foreword by
P. M. Cohn
University of London
London, England

CAMBRIDGE UNIVERSITY PRESS

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

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011–4211, USA
10 Stamford Road, Oakleigh, VIC 3166, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

First published by Addison-Wesley Publishing Inc. 1983
Second edition published by Cambridge University Press 1997
Reprinted 2000

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

Library of Congress Cataloguing in Publication data available

ISBN 0 521 39231 4 hardback

Transferred to digital printing 2003

To Pamela and Gerlinde

Contents

Foreword

Most modern algebra texts devote a few pages (but no more) to finite fields. So at first it may come as a surprise to see an entire book on the subject, and even more for it to appear in the *Encyclopedia of Mathematics and Its Applications*. But the reader of this book will find that the authors performed the very timely task of drawing together the different threads of development that have emanated from the subject. Foremost among these developments is the rapid growth of coding theory which already has been treated in R. J. McEliece's volume in this series. The present volume deals with coding theory in the wider context of polynomial theory over finite fields, and also establishes the connection with linear recurring series and shift registers.

On the pure side there is a good deal of number theory that is most naturally expressed in terms of finite fields. Much of this—for example, equations over finite fields and exponential sums—can serve as a paradigm for the more general case; and the authors have gone as far in their treatment as is reasonable, using elementary algebraic methods only. As a result the book can also serve as an introduction to these topics.

But finite fields also have properties that are not shared with other types of algebra; thus they (like finite Boolean algebras) are functionally complete. This means that every mapping of a finite field can be expressed as a polynomial. While the proof is not hard (it is an immediate consequence of the Lagrange interpolation formula), practical questions arise when we try to find polynomials effecting permutations. Such permutation polynomials

are useful in several contexts, and methods of obtaining them are discussed here. True to its nature as a handbook of applications, this volume also gives various algorithms for factorizing polynomials (over both large and small finite fields).

The lengthy notes at the end of each chapter contain interesting historical perspectives, and the comprehensive bibliography helps to make this volume truly the handbook of finite fields.

P. M. COHN

Preface

The theory of finite fields is a branch of modern algebra that has come to the fore in the last 50 years because of its diverse applications in combinatorics, coding theory, and the mathematical study of switching circuits, among others. The origins of the subject reach back into the 17th and 18th century, with such eminent mathematicians as Pierre de Fermat (1601–1665), Leonhard Euler (1707–1783), Joseph-Louis Lagrange (1736–1813), and Adrien-Marie Legendre (1752–1833) contributing to the structure theory of special finite fields—namely, the so-called finite prime fields. The general theory of finite fields may be said to begin with the work of Carl Friedrich Gauss (1777–1855) and Evariste Galois (1811–1832), but it only became of interest for applied mathematicians in recent decades with the emergence of discrete mathematics as a serious discipline.

In this book, which is the first one devoted entirely to finite fields, we have aimed at presenting both the classical and the applications-oriented aspect of the subject. Thus, in addition to what has to be considered the essential core of the theory, the reader will find results and techniques that are of importance mainly because of their use in applications. Because of the vastness of the subject, limitations had to be imposed on the choice of material. In trying to make the book as self-contained as possible, we have refrained from discussing results or methods that belong properly to algebraic geometry or to the theory of algebraic function fields. Applications are described to the extent to which this can be done without too much

digression. The only noteworthy prerequisite for the book is a background in linear algebra, on the level of a first course on this topic. A rudimentary knowledge of analysis is needed in a few passages. Prior exposure to abstract algebra is certainly helpful, although all the necessary information is summarized in Chapter 1.

Chapter 2 is basic for the rest of the book as it contains the general structure theory of finite fields as well as the discussion of concepts that are used throughout the book. Chapter 3 on the theory of polynomials and Chapter 4 on factorization algorithms for polynomials are closely linked and should best be studied together. A similar unit is formed by Chapters 5 and 6. Chapters 7 and 8 can be read independently of each other and depend mostly on Chapters 2 and 3. The applications presented in Chapter 9 draw on various material in the previous chapters. Chapter 10 supplements parts of Chapters 2 and 3.

Each chapter starts with a brief description of its contents, hence it should not be necessary to give a synopsis of the book here. As this volume is part of an encyclopedic series, we have attempted to provide as much information as possible in a limited space, which meant, in particular, the omission of a few cumbersome proofs. Bibliographical references have been relegated to the notes at the end of each chapter so as not to clutter the main text. These notes also provide the researcher in the field with a survey of the literature and a summary of further results. The bibliography at the end of the volume collects all the references given in the notes.

In order to enhance the attractiveness of this monograph as a textbook, we have inserted worked-out examples at appropriate points in the text and included lists of exercises for Chapters 1–9. These exercises range from routine problems to alternative proofs of key theorems, but contain also material going beyond what is covered in the text.

With regard to cross-references, we have numbered all items in the main text consecutively by chapters, regardless of whether they are definitions, theorems, examples, and so on. Thus, "Definition 2.41" refers to item 41 in Chapter 2 (which happens to be a definition) and "Remark 6.28" refers to item 28 in Chapter 6 (which happens to be a remark). In the same vein, "Exercise 5.31" refers to the list of exercises in Chapter 5.

It is with great pleasure that we express our gratitude to Professor Gian-Carlo Rota for inviting us to write this book and for his patience in waiting for the result of our effort. We gratefully acknowledge the help of Mrs. Melanie Barton, who typed the manuscript with great care and efficiency. The staff of Addison-Wesley deserves our thanks for its professionalism in the production of the book.

R. LIDL
H. NIEDERREITER