GIAN-CARLO ROTA, *Editor*
ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS
Volume 20

Section: Algebra
P. M. Cohn and Roger Lyndon, *Section Editors*

Finite Fields

Rudolf Lidl
University of Tasmania
Hobart, Australia

Harald Niederreiter

GIAN-CARLO ROTA, *Editor*

ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume 20

Section: Algebra
P. M. Cohn and Roger Lyndon, *Section Editors*

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

1983

Addison-Wesley Publishing Company
Advanced Book Program/World Science Division
Reading, Massachusetts

London • Amsterdam • Don Mills, Ontario • Sydney • Tokyo

Library of Congress Cataloging in Publication Data

Lidl, Rudolf
Finite fields.

(Encyclopedia of mathematics and its applications; v. 20. Section, Algebra)
Bibliography: p.
Includes indexes.
1. Finite fields (Algebra) I. Niederreiter, Harald, 1944– II. Title. III. Series: Encyclopedia of mathematics and its applications; v. 20. IV. Series: Encyclopedia of mathematics and its applications. Section, Algebra.
QA247.3.L53 1983 512'.32 83-2756
ISBN 0-201-13519-1

American Mathematical Society (MOS) Subject Classification Scheme (1980): 12CXX, 10G05, 05BXX, 51EXX, 62K10, 94BXX, 94CXX

Manufactured in the United States of America

ABCDEFGHIJ-HA-89876543

GIAN-CARLO ROTA, *Editor*
ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume		Section
1	LUIS A. SANTALÓ **Integral Geometry and Geometric Probability,** 1976 (2nd printing, with revisions, 1979)	Probability
2	GEORGE E. ANDREWS **The Theory of Partitions,** 1976 (2nd printing, 1981)	Number Theory
3	ROBERT J. McELIECE **The Theory of Information and Coding** A Mathematical Framework for Communication, 1977 (2nd printing, with revisions, 1979)	Probability
4	WILLARD MILLER, Jr. **Symmetry and Separation of Variables,** 1977	Special Functions
5	DAVID RUELLE **Thermodynamic Formalism** The Mathematical Structures of Classical Equilibrium Statistical Mechanics, 1978	Statistical Mechanics
6	HENRYK MINC **Permanents,** 1978	Linear Algebra
7	FRED S. ROBERTS **Measurement Theory** with Applications to Decisionmaking, Utility, and the Social Sciences, 1979	Mathematics and the Social Sciences
8	L. C. BIEDENHARN and J. D. LOUCK **Angular Momentum in Quantum Physics:** Theory and Application, 1981	Mathematics of Physics
9	L. C. BIEDENHARN and J. D. LOUCK **The Racah-Wigner Algebra in Quantum Theory,** 1981	Mathematics of Physics

GIAN-CARLO ROTA, *Editor*
ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume		Section
10	JOHN D. DOLLARD and CHARLES N. FRIEDMAN **Product Integration** with Application to Differential Equations, 1979	Analysis
11	WILLIAM B. JONES and W. J. THRON **Continued Fractions:** Analytic Theory and Applications, 1980	Analysis
12	NATHANIEL F. G. MARTIN and JAMES W. ENGLAND **Mathematical Theory of Entropy,** 1981	Real Variables
13	GEORGE A. BAKER, Jr. and PETER R. GRAVES-MORRIS **Padé Approximants, Part I** **Basic Theory,** 1981	Mathematics of Physics
14	GEORGE A. BAKER, Jr. and PETER R. GRAVES-MORRIS **Padé Approximants, Part II:** **Extensions and Applications,** 1981	Mathematics of Physics
15	E. C. BELTRAMETTI and G. CASSINELLI **The Logic of Quantum Mechanics,** 1981	Mathematics of Physics
16	G. D. JAMES and A. KERBER **The Representation Theory of the Symmetric Group,** 1981	Algebra
17	M. LOTHAIRE **Combinatorics on Words,** 1982	Algebra

GIAN-CARLO ROTA, *Editor*
ENCYCLOPEDIA OF MATHEMATICS AND ITS APPLICATIONS

Volume		Section
18	H. O. FATTORINI **The Abstract Cauchy Problem,** 1983	Analysis
19	G. G. LORENTZ, K. JETTER, and S. D. RIEMENSCHNEIDER **Birkhoff Interpolation,** 1983	Interpolation and Approximation
20	RUDOLF LIDL and HARALD NIEDERREITER **Finite Fields,** 1983	Algebra
21	WILLIAM T. TUTTE **Graph Theory,** 1984	Graph Theory and Combinatorics
22	JULIO R. BASTIDA **Field Extensions and Galois Theory,** 1984	Algebra

Other volumes in preparation

ENCYCLOPEDIA OF MATHEMATICS and Its Applications

GIAN-CARLO ROTA, Editor
Department of Mathematics
Massachusetts Institute of Technology
Cambridge, Massachusetts

Editorial Board

Editor's Statement

A large body of mathematics consists of facts that can be presented and described much like any other natural phenomenon. These facts, at times explicitly brought out as theorems, at other times concealed within a proof, make up most of the applications of mathematics, and are the most likely to survive change of style and of interest.

This ENCYCLOPEDIA will attempt to present the factual body of all mathematics. Clarity of exposition, accessibility to the non-specialist, and a thorough bibliography are required of each author. Volumes will appear in no particular order, but will be organized into sections, each one comprising a recognizable branch of present-day mathematics. Numbers of volumes and sections will be reconsidered as times and needs change.

It is hoped that this enterprise will make mathematics more widely used where it is needed, and more accessible in fields in which it can be applied but where it has not yet penetrated because of insufficient information.

GIAN-CARLO ROTA

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

Contents

Chapter 1

Algebraic Foundations

This introductory chapter contains a survey of some basic algebraic concepts that will be employed throughout the book. Elementary algebra uses the operations of arithmetic such as addition and multiplication, but replaces particular numbers by symbols and thereby obtains formulas that, by substitution, provide solutions to specific numerical problems. In modern algebra the level of abstraction is raised further: instead of dealing with the familiar operations on real numbers, one treats general operations —processes of combining two or more elements to yield another element—in general sets. The aim is to study the common properties of all systems consisting of sets on which are defined a fixed number of operations interrelated in some definite way—for instance, sets with two binary operations behaving like $+$ and $\cdot$ for the real numbers.

Only the most fundamental definitions and properties of algebraic systems—that is, of sets together with one or more operations on the set—will be introduced, and the theory will be discussed only to the extent needed for our special purposes in the study of finite fields later on. We state some standard results without proof. With regard to sets we adopt the naive standpoint. We use the following sets of numbers: the set $\mathbb{N}$ of natural numbers, the set $\mathbb{Z}$ of integers, the set $\mathbb{Q}$ of rational numbers, the set $\mathbb{R}$ of real numbers, and the set $\mathbb{C}$ of complex numbers.

1. GROUPS

In the set of all integers the two operations addition and multiplication are well known. We can generalize the concept of operation to arbitrary sets. Let S be a set and let $S \times S$ denote the set of all ordered pairs (s, t) with $s \in S$, $t \in S$. Then a mapping from $S \times S$ into S will be called a (*binary*) *operation* on S. Under this definition we require that the image of $(s, t) \in S \times S$ must be in S; this is the *closure property* of an operation. By an *algebraic structure* or *algebraic system* we mean a set S together with one or more operations on S.

In elementary arithmetic we are provided with two operations, addition and multiplication, that have associativity as one of their most important properties. Of the various possible algebraic systems having a single associative operation, the type known as a group has been by far the most extensively studied and developed. The theory of groups is one of the oldest parts of abstract algebra as well as one particularly rich in applications.

1.1. Definition. A *group* is a set G together with a binary operation $*$ on G such that the following three properties hold:

1. $*$ is *associative*; that is, for any $a, b, c \in G$,
$$a * (b * c) = (a * b) * c.$$
2. There is an *identity* (or *unity*) *element* e in G such that for all $a \in G$,
$$a * e = e * a = a.$$
3. For each $a \in G$, there exists an *inverse element* $a^{-1} \in G$ such that
$$a * a^{-1} = a^{-1} * a = e.$$

If the group also satisfies

4. For all $a, b \in G$,
$$a * b = b * a,$$

then the group is called *abelian* (or *commutative*).

It is easily shown that the identity element e and the inverse element a^{-1} of a given element $a \in G$ are uniquely determined by the properties above. Furthermore, $(a * b)^{-1} = b^{-1} * a^{-1}$ for all $a, b \in G$. For simplicity, we shall frequently use the notation of ordinary multiplication to designate the operation in the group, writing simply ab instead of $a * b$. But it must be emphasized that by doing so we do not assume that the operation actually is ordinary multiplication. Sometimes it is also convenient to write $a + b$ instead of $a * b$ and $-a$ instead of a^{-1}, but this additive notation is usually reserved for abelian groups.