Introduction to finite fields and their applications

RUDOLF LIDL

University of Tasmania, Launceston, Australia

HARALD NIEDERREITER

Austrian Academy of Sciences, Vienna, Austria

Revised edition

CAMBRIDGE
UNIVERSITY PRESS

Contents

Preface *page* ix

Preface to the revised edition xi

Chapter 1 Algebraic Foundations **1**
1 Groups 2
2 Rings and Fields 11
3 Polynomials 18
4 Field Extensions 30
Notes 37
Exercises 37

Chapter 2 Structure of Finite Fields **44**
1 Characterization of Finite Fields 45
2 Roots of Irreducible Polynomials 48
3 Traces, Norms, and Bases 51
4 Roots of Unity and Cyclotomic Polynomials 60
5 Representation of Elements of Finite Fields 63
6 Wedderburn's Theorem 66
Notes 70
Exercises 70

Chapter 3 Polynomials over Finite Fields **76**
1 Order of Polynomials and Primitive Polynomials 77
2 Irreducible Polynomials 84
3 Construction of Irreducible Polynomials 89
4 Linearized Polynomials 100
5 Binomials and Trinomials 117
Notes 124
Exercises 125

Chapter 4 Factorization of Polynomials **132**
1 Factorization over Small Finite Fields 133
2 Factorization over Large Finite Fields 142
3 Calculation of Roots of Polynomials 153
Notes 162
Exercises 162

Chapter 5 Exponential Sums **166**
1 Characters 167
2 Gaussian Sums 172
Notes 185
Exercises 185

Chapter 6 Linear Recurring Sequences **189**
1 Feedback Shift Registers, Periodicity Properties 190
2 Impulse Response Sequences, Characteristic Polynomial 197
3 Generating Functions 206
4 The Minimal Polynomial 214
5 Families of Linear Recurring Sequences 219
6 Characterization of Linear Recurring Sequences 232
7 Distribution Properties of Linear Recurring Sequences 239
Notes 249
Exercises 250

Chapter 7 Theoretical Applications of Finite Fields **256**
1 Finite Geometries 257
2 Combinatorics 267
3 Linear Modular Systems 276
4 Pseudorandom Sequences 286
Notes 299
Exercises 300

Chapter 8 Algebraic Coding Theory 305
1 Linear Codes 306
2 Cyclic Codes 317
3 Goppa Codes 331
Notes 338
Exercises 339

Chapter 9 Cryptology 344
1 Background 345
2 Stream Ciphers 348
3 Discrete Logarithms 352
4 Further Cryptosystems 366
Notes 369
Exercises 370

Chapter 10 Tables 374
1 Computation in Finite Fields 374
2 Tables of Irreducible Polynomials 384
Notes 384

Bibliography 399

List of Symbols 406

Index 410