Rudolf Lidl Günter Pilz

Applied Abstract Algebra

Second Edition

With 112 illustrations

Springer

Contents

Preface **vii**

List of Symbols **xv**

1 Lattices **1**

1 Properties and Examples of Lattices 1

2 Distributive Lattices 16

3 Boolean Algebras 19

4 Boolean Polynomials 26

5 Ideals, Filters, and Equations 34

6 Minimal Forms of Boolean Polynomials 40

Notes 51

2 Applications of Lattices **55**

7 Switching Circuits 55

8 Applications of Switching Circuits 62

9 More Applications of Boolean Algebras 78

Notes 93

3 Finite Fields and Polynomials **95**

10 Some Group Theory 95

11 Rings and Polynomials 109

12 Fields 124
13 Finite Fields 138
14 Irreducible Polynomials over Finite Fields 153
15 Factorization of Polynomials over Finite Fields 166
Notes 176

4 Coding Theory **183**
16 Introduction to Coding 183
17 Linear Codes 192
18 Cyclic Codes 205
19 Special Cyclic Codes 222
20 Decoding BCH Codes 229
Notes 236

5 Cryptology **239**
21 Classical Cryptosystems 240
22 Public Key Cryptosystems 255
23 Discrete Logarithms and Other Ciphers 266
Notes 279

6 Applications of Groups **283**
24 Fast Adding 284
25 Pólya's Theory of Enumeration 287
26 Image Understanding 302
27 Symmetry Groups 314
Notes 329

7 Further Applications of Algebra **331**
28 Semigroups 333
29 Semigroups and Automata 342
30 Semigroups and Formal Languages 350
31 Semigroups and Biology 356
32 Semigroups and Sociology 360
33 Linear Recurring Sequences 365
34 Fast Fourier Transforms 379
35 Latin Squares 388
36 Block Designs 399
37 Hadamard Matrices, Transforms, and Networks 413

38 Gröbner Bases for Algebraic and Differential Equations . 426
39 Systems Theory 434
40 Abstract Data Types 447
Notes 458

Bibliography **459**

Index **475**