CONTENTS

Introduction 1

I. Mappings and Operations 9

1 Mappings 9
2 Composition. Invertible Mappings 15
3 Operations 19
4 Composition as an Operation 25

II. Introduction to Groups 30

5 Definition and Examples 30
6 Permutations 34
7 Subgroups 41
8 Groups and Symmetry 47

III. Equivalence. Congruence. Divisibility 52

9 Equivalence Relations 52
10 Congruence. The Division Algorithm 57
11 Integers Modulo *n* 61
12 Greatest Common Divisors. The Euclidean Algorithm 65
13 Factorization. Euler's Phi-Function 70

IV. Groups 75

14 Elementary Properties 75
15 Generators. Direct Products 81
16 Cosets 85
17 Lagrange's Theorem. Cyclic Groups 88
18 Isomorphism 93
19 More on Isomorphism 98
20 Cayley's Theorem 102
21 Appendix: RSA Algorithm 105

V. Group Homomorphisms 106

21 Homomorphisms of Groups. Kernels 106
22 Quotient Groups 110
23 The Fundamental Homomorphism Theorem 114

VI. Introduction to Rings 120

24 Definition and Examples 120
25 Integral Domains. Subrings 125
26 Fields 128
27 Isomorphism. Characteristic 131

VII. The Familiar Number Systems 137

28 Ordered Integral Domains 137
29 The Integers 140
30 Field of Quotients. The Field of Rational Numbers 142
31 Ordered Fields. The Field of Real Numbers 146
32 The Field of Complex Numbers 149
33 Complex Roots of Unity 154

VIII. Polynomials 160

34 Definition and Elementary Properties 160
Appendix to Section 34 162
35 The Division Algorithm 165
36 Factorization of Polynomials 169
37 Unique Factorization Domains 173

IX. Quotient Rings 178

38 Homomorphisms of Rings. Ideals 178
39 Quotient Rings 182
40 Quotient Rings of $F[X]$ 184
41 Factorization and Ideals 187

X. Galois Theory: Overview 193

42 Simple Extensions. Degree 194
43 Roots of Polynomials 198
44 Fundamental Theorem: Introduction 203

XI. Galois Theory 207

45 Algebraic Extensions 207
46 Splitting Fields. Galois Groups 210
47 Separability and Normality 214
48 Fundamental Theorem of Galois Theory 218
49 Solvability by Radicals 219
50 Finite Fields 223

XII. Geometric Constructions 229

51 Three Famous Problems 229
52 Constructible Numbers 233
53 Impossible Constructions 234

XIII. Solvable and Alternating Groups 237

54 Isomorphism Theorems and Solvable Groups 237
55 Alternating Groups 240

XIV. Applications of Permutation Groups 243

56 Groups Acting on Sets 243
57 Burnside's Counting Theorem 247
58 Sylow's Theorem 252

XV. Symmetry 256

59 Finite Symmetry Groups 256
60 Infinite Two-Dimensional Symmetry Groups 263
61 On Crystallographic Groups 267
62 The Euclidean Group 274

XVI. Lattices and Boolean Algebras 279

63 Partially Ordered Sets 279
64 Lattices 283
65 Boolean Algebras 287
66 Finite Boolean Algebras 291

A. Sets 296

B. Proofs 299

C. Mathematical Induction 304

D. Linear Algebra 307

E. Solutions to Selected Problems 312

Photo Credit List 326

Index of Notation 327

Index 330