Scanned by TapScanner

Contents

Preface xi

PART 1 Integers and Equivalence Relations 1

0 Preliminaries 3

Properties of Integers 3 | Modular Arithmetic 6 | Complex Numbers 13 | Mathematical Induction 14 | Equivalence Relations 17 | Functions (Mappings) 20

Exercises 23

PART 2 Groups 29

1 Introduction to Groups 31

Symmetries of a Square 31 | The Dihedral Groups 34

Exercises 37

Biography of Niels Abel 41

2 Groups 42

Definition and Examples of Groups 42 | Elementary Properties of Groups 50 | Historical Note 53

Exercises 54

3 Finite Groups; Subgroups 60

Terminology and Notation 60 | Subgroup Tests 61 | Examples of Subgroups 65

Exercises 68

4 Cyclic Groups 77

Properties of Cyclic Groups 77 | Classification of Subgroups of Cyclic Groups 82

Scanned by TapScanner

Exercises 87
Biography of James Joseph Sylvester 93
Supplementary Exercises for Chapters 1–4 95

5 Permutation Groups 99
Definition and Notation 99 | Cycle Notation 102 | Properties of Permutations 104 | A Check-Digit Scheme Based on D_5 115
Exercises 118
Biography of Augustin Cauchy 126

6 Isomorphisms 127
Motivation 127 | Definition and Examples 127 | Cayley's Theorem 131 | Properties of Isomorphisms 133 | Automorphisms 134
Exercises 138
Biography of Arthur Cayley 143

7 Cosets and Lagrange's Theorem 144
Properties of Cosets 144 | Lagrange's Theorem and Consequences 147 | An Application of Cosets to Permutation Groups 151 | The Rotation Group of a Cube and a Soccer Ball 153 | An Application of Cosets to the Rubik's Cube 155
Exercises 156
Biography of Joseph Lagrange 161

8 External Direct Products 162
Definition and Examples 162 | Properties of External Direct Products 163 | The Group of Units Modulo n as an External Direct Product 166 | Applications 168
Exercises 174
Biography of Leonard Adleman 180
Supplementary Exercises for Chapters 5–8 181

9 Normal Subgroups and Factor Groups 185
Normal Subgroups 185 | Factor Groups 187 | Applications of Factor Groups 193 | Internal Direct Products 195
Exercises 200
Biography of Évariste Galois 207

Scanned by TapScanner

10 Group Homomorphisms 208
Definition and Examples 208 | Properties of Homomorphisms 210 | The First Isomorphism Theorem 214
Exercises 219
Biography of Camille Jordan 225

11 Fundamental Theorem of Finite Abelian Groups 226
The Fundamental Theorem 226 | The Isomorphism Classes of Abelian Groups 226 | Proof of the Fundamental Theorem 231
Exercises 234
Supplementary Exercises for Chapters 9–11 238

PART 3 Rings 243

12 Introduction to Rings 245
Motivation and Definition 245 | Examples of Rings 246 | Properties of Rings 247 | Subrings 248
Exercises 250
Biography of I. N. Herstein 254

13 Integral Domains 255
Definition and Examples 255 | Fields 256 | Characteristic of a Ring 258
Exercises 261
Biography of Nathan Jacobson 266

14 Ideals and Factor Rings 267
Ideals 267 | Factor Rings 268 | Prime Ideals and Maximal Ideals 272
Exercises 274
Biography of Richard Dedekind 279
Biography of Emmy Noether 280
Supplementary Exercises for Chapters 12–14 281

15 Ring Homomorphisms 285
Definition and Examples 285 | Properties of Ring Homomorphisms 288 | The Field of Quotients 290
Exercises 292

Scanned by TapScanner

16 Polynomial Rings 298
Notation and Terminology 298 | The Division Algorithm and Consequences 301
Exercises 305
Biography of Saunders Mac Lane 310

17 Factorization of Polynomials 311
Reducibility Tests 311 | Irreducibility Tests 314 | Unique Factorization in $Z[x]$ 319 | Weird Dice: An Application of Unique Factorization 320
Exercises 322
Biography of Serge Lang 327

18 Divisibility in Integral Domains 328
Irreducibles, Primes 328 | Historical Discussion of Fermat's Last Theorem 331 | Unique Factorization Domains 334 | Euclidean Domains 337
Exercises 341
Biography of Sophie Germain 345
Biography of Andrew Wiles 346
Supplementary Exercises for Chapters 15–18 347

PART 4 Fields 349

19 Vector Spaces 351
Definition and Examples 351 | Subspaces 352 | Linear Independence 353
Exercises 355
Biography of Emil Artin 358
Biography of Olga Taussky-Todd 359

20 Extension Fields 360
The Fundamental Theorem of Field Theory 360 | Splitting Fields 362 | Zeros of an Irreducible Polynomial 368
Exercises 372
Biography of Leopold Kronecker 375

21 Algebraic Extensions 376
Characterization of Extensions 376 | Finite Extensions 378 | Properties of Algebraic Extensions 382

Scanned by TapScanner

Exercises 384

Biography of Irving Kaplansky 387

22 Finite Fields 388

Classification of Finite Fields 388 | Structure of Finite Fields 389 | Subfields of a Finite Field 393

Exercises 395

Biography of L. E. Dickson 398

23 Geometric Constructions 399

Historical Discussion of Geometric Constructions 399 | Constructible Numbers 400 | Angle-Trisectors and Circle-Squarers 402

Exercises 402

Supplementary Exercises for Chapters 19–23 405

PART 5 Special Topics 407

24 Sylow Theorems 409

Conjugacy Classes 409 | The Class Equation 410 | The Probability That Two Elements Commute 411 | The Sylow Theorems 412 | Applications of Sylow Theorems 417

Exercises 421

Biography of Ludwig Sylow 427

25 Finite Simple Groups 428

Historical Background 428 | Nonsimplicity Tests 433 | The Simplicity of A_5 437 | The Fields Medal 438 | The Cole Prize 438

Exercises 439

Biography of Michael Aschbacher 442

Biography of Daniel Gorenstein 443

Biography of John Thompson 444

26 Generators and Relations 445

Motivation 445 | Definitions and Notation 446 | Free Group 447 | Generators and Relations 448 | Classification of Groups of Order Up to 15 452 | Characterization of Dihedral Groups 454 | Realizing the Dihedral Groups with Mirrors 455

Exercises 457

Biography of Marshall Hall, Jr. 460

Scanned by TapScanner

27 Symmetry Groups 461

Isometries 461 | Classification of Finite Plane Symmetry Groups 463 | Classification of Finite Groups of Rotations in R^3 464

Exercises 466

28 Frieze Groups and Crystallographic Groups 469

The Frieze Groups 469 | The Crystallographic Groups 475 | Identification of Plane Periodic Patterns 481

Exercises 487

Biography of M. C. Escher 492

Biography of George Pólya 493

Biography of John H. Conway 494

29 Symmetry and Counting 495

Motivation 495 | Burnside's Theorem 496 | Applications 498 | Group Action 501

Exercises 502

Biography of William Burnside 505

30 Cayley Digraphs of Groups 506

Motivation 506 | The Cayley Digraph of a Group 506 | Hamiltonian Circuits and Paths 510 | Some Applications 516

Exercises 519

Biography of William Rowan Hamilton 524

Biography of Paul Erdős 525

31 Introduction to Algebraic Coding Theory 526

Motivation 526 | Linear Codes 531 | Parity-Check Matrix Decoding 536 | Coset Decoding 539 | Historical Note: The Ubiquitous Reed–Solomon Codes 543

Exercises 545

Biography of Richard W. Hamming 550

Biography of Jessie MacWilliams 551

Biography of Vera Pless 552

32 An Introduction to Galois Theory 553

Fundamental Theorem of Galois Theory 553 | Solvability of Polynomials by Radicals 560 | Insolvability of a Quintic 564

Exercises 565

Biography of Philip Hall 569

Scanned by TapScanner

33 Cyclotomic Extensions 570

Motivation 570 | Cyclotomic Polynomials 571 |
The Constructible Regular *n*-gons 575

Exercises 577

Biography of Carl Friedrich Gauss 579

Biography of Manjul Bhargava 580

Supplementary Exercises for Chapters 24–33 581

Selected Answers A1

Index of Mathematicians A45

Index of Terms A47

Scanned by TapScanner