CAMBRIDGE

Cambridge University Press
978-1-107-16407-9 — Abstract Algebra with Applications
Audrey Terras
Table of Contents
More Information

Contents

List of Figures ix
Preface xiii

PART I GROUPS

1 Preliminaries 3
1.1 Introduction 3
1.2 Sets 6
1.3 The Integers 9
1.4 Mathematical Induction 14
1.5 Divisibility, Greatest Common Divisor, Primes, and Unique Factorization 19
1.6 Modular Arithmetic, Congruences 26
1.7 Relations 30
1.8 Functions, the Pigeonhole Principle, and Binary Operations 34

2 Groups: A Beginning 43
2.1 What is a Group? 43
2.2 Visualizing Groups 52
2.3 More Examples of Groups and Some Basic Facts 56
2.4 Subgroups 64
2.5 Cyclic Groups are Our Friends 72

3 Groups: There's More 81
3.1 Groups of Permutations 81
3.2 Isomorphisms and Cayley's Theorem 89
3.3 Cosets, Lagrange's Theorem, and Normal Subgroups 93
3.4 Building New Groups from Old, I: Quotient or Factor Groups G/H 98
3.5 Group Homomorphism 102
3.6 Building New Groups from Old, II: Direct Product of Groups 108
3.7 Group Actions 114

4 Applications and More Examples of Groups 124
4.1 Public-Key Cryptography 124
4.2 Chemistry and the Finite Fourier Transform 129
4.3 Groups and Conservation Laws in Physics 135
4.4 Puzzles 142
4.5 Small Groups 146

© in this web service Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
978-1-107-16407-9 — Abstract Algebra with Applications
Audrey Terras
Table of Contents
More Information

PART II RINGS

5 Rings: A Beginning 157
5.1 Introduction 157
5.2 What is a Ring? 158
5.3 Integral Domains and Fields are Nicer Rings 166
5.4 Building New Rings from Old: Quotients and Direct Sums of Rings 173
5.5 Polynomial Rings 180
5.6 Quotients of Polynomial Rings 185

6 Rings: There's More 189
6.1 Ring Homomorphisms 189
6.2 The Chinese Remainder Theorem 193
6.3 More Stories about $F[x]$ Including Comparisons with $\mathbb{Z}$ 198
6.4 Field of Fractions or Quotients 202

7 Vector Spaces and Finite Fields 206
7.1 Matrices and Vector Spaces over Arbitrary Fields and Rings like $\mathbb{Z}$ 206
7.2 Linear Functions or Mappings 218
7.3 Determinants 224
7.4 Extension Fields: Algebraic versus Transcendental 229
7.5 Subfields and Field Extensions of Finite Fields 233
7.6 Galois Theory for Finite Fields 239

8 Applications of Rings 244
8.1 Random Number Generators 244
8.2 Error-Correcting Codes 256
8.3 Finite Upper Half Planes and Ramanujan Graphs 265
8.4 Eigenvalues, Random Walks on Graphs, and Google 272
8.5 Elliptic Curve Cryptography 282

References 299
Index 305

© in this web service Cambridge University Press www.cambridge.org