JOHN SCHERK

Department of Mathematics
University of Toronto
Ontaria, Canada

ALGEBRA
A Computational Introduction

CHAPMAN & HALL/CRC

Boca Raton London New York Washington, D.C.

Contents

Preface **ix**

1 Congruences **1**
Basic Properties 1
Divisibility Tests 2
Common Divisors 6
Solving Congruences 9
The Integers Modulo n 11
Introduction to Software 13
Exercises 15

2 Permutations **19**
Permutations as Mappings 19
Cycles 20
Sign of a Permutation 23
Exercises 24

3 Permutation Groups **27**
Definition 27
Cyclic Groups 29
Generators 30
Software and Calculations 32
Exercises 36

4 Linear Groups **39**
Definitions and Examples 39
Generators 41
Software and Calculations 45
Exercises 48

5 Groups **51**
Basic Properties and More Examples 51
Homomorphisms 56
Exercises 60

6 Subgroups **63**
Definition 63
Orthogonal Groups 63
Cyclic Subgroups and Generators 65
Kernel and Image of a Homomorphism 70
Exercises 72

7 Symmetry Groups **75**
Symmetries of Regular Polygons 76
Symmetries of Platonic Solids 78
Improper Symmetries 83
Symmetries of Equations 84
Exercises 87

8 Group Actions **89**
Examples 89
Orbits and Stabilizers 90
Fractional Linear Transformations 94
Cayley's Theorem 97
Software and Calculations 98
Exercises 102

9 Counting Formulas **105**
The Class Equation 105
A First Application 110
Burnside's Counting Lemma 110
Finite Subgroups of $SO(3)$ 113
Exercises 118

10 Cosets **119**
Lagrange's Theorem 119
Normal Subgroups 123
Quotient Groups 125
The Canonical Isomorphism 126
Software and Calculations 129
Exercises 134

11 Sylow Subgroups **137**
The Sylow Theorems . . . 137
Groups of Small Order . . . 141
A List . . . 145
A Calculation . . . 146
Exercises . . . 147

12 Simple Groups **149**
Composition Series . . . 149
Simplicity of A_n . . . 151
Simplicity of $PSL(2, \mathbb{F}_p)$ . . . 153
Exercises . . . 156

13 Abelian Groups **159**
Free Abelian Groups . . . 159
Row and Column Reduction of Integer Matrices . . . 162
Classification Theorems . . . 166
Invariance of Elementary Divisors . . . 169
The Multiplicative Group of the Integers Mod n . . . 172
Exercises . . . 174

14 Polynomial Rings **177**
Basic Properties of Polynomials . . . 178
Unique Factorization into Irreducibles . . . 183
Finding Irreducible Polynomials . . . 185
Commutative Rings . . . 189
Congruences . . . 192
Factoring Polynomials over a Finite Field . . . 197
Calculations . . . 201
Exercises . . . 205

15 Symmetric Polynomials **209**
Polynomials in Several Variables . . . 209
Symmetric Polynomials and Functions . . . 210
Sums of Powers . . . 214
Discriminants . . . 215
Software . . . 216
Exercises . . . 217

16 Roots of Equations **221**
Introduction . . . 221
Extension Fields . . . 223
Degree of an Extension . . . 225
Splitting Fields . . . 228
Cubics . . . 231

Cyclotomic Polynomials 233
Finite Fields 236
Plots and Calculations 238
Exercises 241

17 Galois Groups **245**
Introduction 245
Definition 248
How Large is the Galois Group? 250
The Galois Correspondence 254
Discriminants 265
Exercises 266

18 Quartics **269**
Galois Groups of Quartics 269
The Geometry of the Cubic Resolvent 272
Software 275
Exercises 276

19 The General Equation of the *n*th Degree **279**
Examples 279
Symmetric Functions 280
The Fundamental Theorem of Algebra 282
Exercises 283

20 Solution by Radicals **285**
Formulas for a Cubic 285
Cyclic Extensions 288
Solution by Radicals in Higher Degrees 290
Calculations 294
Exercises 295

21 Ruler-and-Compass Constructions **297**
Introduction 297
Algebraic Interpretation 298
Construction of Regular Polygons 302
Periods 304
Exercises 307

Appendix: Mathematica Commands **309**

References **313**

Index **315**