PrelimProb May 2, 2025 - Vignesh Nydhruva.

1. (see below pages).
2. Ok.

Contents

Acknowledgements **iv**

Preface **v**

1 Preliminaries **1**

1.1 A Short Note on Proofs 1
1.2 Sets and Equivalence Relations 3
1.3 Reading Questions 13
1.4 Exercises 14
1.5 References and Suggested Readings 16

2 The Integers **17**

2.1 Mathematical Induction 17
2.2 The Division Algorithm 20
2.3 Reading Questions 24
2.4 Exercises 24
2.5 Programming Exercises 26
2.6 References and Suggested Readings 26

3 Groups **28**

3.1 Integer Equivalence Classes and Symmetries 28
3.2 Definitions and Examples 33
3.3 Subgroups 38
3.4 Reading Questions 40
3.5 Exercises 40
3.6 Additional Exercises: Detecting Errors 43
3.7 References and Suggested Readings 45

4 Cyclic Groups **46**

4.1 Cyclic Subgroups 46
4.2 Multiplicative Group of Complex Numbers 49
4.3 The Method of Repeated Squares 53

4.4 Reading Questions 55
4.5 Exercises 55
4.6 Programming Exercises 58
4.7 References and Suggested Readings 58

5 Permutation Groups 59

5.1 Definitions and Notation 59
5.2 Dihedral Groups 65
5.3 Reading Questions 70
5.4 Exercises 71

6 Cosets and Lagrange's Theorem 74

6.1 Cosets 74
6.2 Lagrange's Theorem 76
6.3 Fermat's and Euler's Theorems 77
6.4 Reading Questions 78
6.5 Exercises 78

7 Introduction to Cryptography 81

7.1 Private Key Cryptography 81
7.2 Public Key Cryptography 83
7.3 Reading Questions 86
7.4 Exercises 87
7.5 Additional Exercises: Primality and Factoring 88
7.6 References and Suggested Readings 89

8 Algebraic Coding Theory 91

8.1 Error-Detecting and Correcting Codes 91
8.2 Linear Codes. 98
8.3 Parity-Check and Generator Matrices 101
8.4 Efficient Decoding 106
8.5 Reading Questions 109
8.6 Exercises 109
8.7 Programming Exercises 113
8.8 References and Suggested Readings 113

9 Isomorphisms 114

9.1 Definition and Examples 114
9.2 Direct Products 118
9.3 Reading Questions 121
9.4 Exercises 121

10 Normal Subgroups and Factor Groups 125

10.1 Factor Groups and Normal Subgroups. 125
10.2 The Simplicity of the Alternating Group. 127
10.3 Reading Questions 130
10.4 Exercises 130

11 Homomorphisms 133
11.1 Group Homomorphisms . . . 133
11.2 The Isomorphism Theorems . . . 135
11.3 Reading Questions . . . 138
11.4 Exercises . . . 138
11.5 Additional Exercises: Automorphisms . . . 139

12 Matrix Groups and Symmetry 141
12.1 Matrix Groups . . . 141
12.2 Symmetry . . . 148
12.3 Reading Questions . . . 154
12.4 Exercises . . . 155
12.5 References and Suggested Readings . . . 157

13 The Structure of Groups 158
13.1 Finite Abelian Groups . . . 158
13.2 Solvable Groups . . . 162
13.3 Reading Questions . . . 165
13.4 Exercises . . . 165
13.5 Programming Exercises . . . 167
13.6 References and Suggested Readings . . . 167

14 Group Actions 168
14.1 Groups Acting on Sets . . . 168
14.2 The Class Equation . . . 170
14.3 Burnside's Counting Theorem . . . 172
14.4 Reading Questions . . . 178
14.5 Exercises . . . 178
14.6 Programming Exercise . . . 180
14.7 References and Suggested Reading . . . 180

15 The Sylow Theorems 181
15.1 The Sylow Theorems . . . 181
15.2 Examples and Applications . . . 184
15.3 Reading Questions . . . 187
15.4 Exercises . . . 187
15.5 A Project . . . 188
15.6 References and Suggested Readings . . . 189

16 Rings 190
16.1 Rings. . . . 190
16.2 Integral Domains and Fields . . . 193
16.3 Ring Homomorphisms and Ideals. . . . 195
16.4 Maximal and Prime Ideals . . . 198
16.5 An Application to Software Design . . . 200
16.6 Reading Questions . . . 203
16.7 Exercises . . . 204

16.8 Programming Exercise . . . 207
16.9 References and Suggested Readings . . . 207

17 Polynomials 209

17.1 Polynomial Rings . . . 209
17.2 The Division Algorithm . . . 212
17.3 Irreducible Polynomials . . . 215
17.4 Reading Questions . . . 220
17.5 Exercises . . . 220
17.6 Additional Exercises: Solving the Cubic and Quartic Equations . . . 222

18 Integral Domains 225

18.1 Fields of Fractions . . . 225
18.2 Factorization in Integral Domains . . . 228
18.3 Reading Questions . . . 235
18.4 Exercises . . . 235
18.5 References and Suggested Readings . . . 237

19 Lattices and Boolean Algebras 238

19.1 Lattices . . . 238
19.2 Boolean Algebras . . . 241
19.3 The Algebra of Electrical Circuits . . . 246
19.4 Reading Questions . . . 248
19.5 Exercises . . . 249
19.6 Programming Exercises . . . 251
19.7 References and Suggested Readings . . . 251

20 Vector Spaces 252

20.1 Definitions and Examples . . . 252
20.2 Subspaces . . . 253
20.3 Linear Independence . . . 254
20.4 Reading Questions . . . 256
20.5 Exercises . . . 256
20.6 References and Suggested Readings . . . 259

21 Fields 260

21.1 Extension Fields . . . 260
21.2 Splitting Fields . . . 268
21.3 Geometric Constructions . . . 270
21.4 Reading Questions . . . 275
21.5 Exercises . . . 275
21.6 References and Suggested Readings . . . 277

22 Finite Fields 278

22.1 Structure of a Finite Field . . . 278
22.2 Polynomial Codes . . . 282
22.3 Reading Questions . . . 289

22.4 Exercises 289
22.5 Additional Exercises: Error Correction for BCH Codes 291
22.6 References and Suggested Readings 291

23 Galois Theory **293**

23.1 Field Automorphisms 293
23.2 The Fundamental Theorem 297
23.3 Applications 303
23.4 Reading Questions 307
23.5 Exercises 308
23.6 References and Suggested Readings 309

Appendices

A GNU Free Documentation License **311**

B Hints and Answers to Selected Exercises **318**

C Notation **336**

Back Matter

Index **339**