Contents

Introduction **1**
What is Algebra? . . . 1
Number Systems . . . 4

1 The Integers **7**
1.1 Introduction . . . 7
1.2 Divisibility . . . 8
1.3 The Euclidean Algorithm, First Version . . . 11
1.4 The Greatest Common Divisor . . . 14
1.5 The Division Algorithm . . . 18
1.6 The Euclidean Algorithm, Second Version . . . 20
1.7 The Extended Euclidean Algorithm . . . 26
1.8 Application 1: Linear Diophantine Equations . . . 33
1.8.1 The GCD-criterion . . . 35
1.8.2 How to solve $mx + ny = c$ . . . 38
1.8.3 Solving $mx + ny + \ldots + kz = c$ . . . 44
1.9 Application 2: Unique Factorization . . . 49
1.9.1 Questions about prime numbers . . . 49
1.9.2 The Unique Factorization Theorem . . . 51
1.9.3 Application 1 of Unique Factorization: Prime Exponents . . . 54
1.9.4 Application 2 of Unique Factorization: Irrationality . . . 54
1.9.5 Application 3: A “formula” for the GCD . . . 55
1.10 Review Exercises . . . 58

2 Modular Arithmetic **61**
2.1 Introduction . . . 61
2.2 The Calculus of Remainders . . . 63
2.3 The Cancellation Law . . . 70
2.4 Solving the Congruence Equation $ax \equiv b \pmod{m}$ . . . 72
2.5 The Ring $\mathbb{Z}/m\mathbb{Z}$ and the Field $\mathbb{F}_p$ . . . 76
2.6 The Chinese Remainder Theorem . . . 78
2.7 Fermat’s (Little) Theorem . . . 86

2.8 Public Key Cryptography 95
2.9 Review Exercises 103

3 Polynomials 107
3.1 Introduction 107
3.2 Review of Complex Numbers 109
3.3 Polynomials: first properties 123
3.4 The Division Algorithm 126
3.5 The Remainder Theorem 129
3.6 The Euclidean Algorithm 134
3.7 Unique Factorization 139
3.8 Factoring Methods 148
3.9 Review Exercises 160

4 Interpolation and Approximation and the Geometry of $\mathbb{R}^n$ 163
4.1 Introduction 163
4.2 The Lagrange Interpolation Formula 166
4.3 The Least Square Method 174
4.4 Review of the Geometry of $\mathbb{R}^n$ 179
4.5 A distance problem 185
4.6 Orthogonal Vectors and the Gram-Schmidt Procedure 194
4.7 Function spaces and Fourier Approximation 200
4.8 Review Exercises 209

5 Matrix Polynomials and Discrete Linear Systems 211
5.1 Introduction 211
5.2 Matrix Polynomials: First Properties 214
5.3 Evaluating Matrix Polynomials – Method I
(Diagonable Case) 215
5.4 Review of Diagonalization 217
5.5 Evaluating Matrix Polynomials — Method I
(Non-diagonable Case) 223
5.6 Evaluating Matrix Polynomials — Method II 229
5.7 The Generalized Remainder Theorem 233
5.8 Evaluating Matrix Polynomials — Method III 243
5.9 Application to Discrete Linear Systems 250
5.9.1 Homogeneous Discrete Linear Systems 250
5.9.2 Difference Equations as Discrete Linear Systems 253
5.9.3 Markov Chains as Discrete Linear Systems 258
5.9.4 Non-homogeneous Discrete Linear Systems 262
5.10 Review Exercises 268

6 The Jordan Canonical Form 273
6.1 Introduction . . . 273
6.2 Algebraic and geometric multiplicities of eigenvalues . . . 274
6.3 How to find P such that $P^{-1}AP = J$ (for $m \leq 3$) . . . 284
6.4 Generalized Eigenvectors and the JCF . . . 290
6.5 A procedure for finding P such that $P^{-1}AP = J$ . . . 298
6.6 A Proof of the Cayley–Hamilton Theorem . . . 302
6.7 Appendix: Proof of the Jordan Canonical Form . . . 304
6.8 Review Exercises . . . 308

7 Powers of Matrices 311
7.1 Introduction . . . 311
7.2 Powers of Numbers . . . 312
7.3 Sequences of powers of matrices . . . 315
7.4 Finding $\lim\limits_{n\to\infty} A^n$ (when A is power convergent) . . . 320
7.5 The spectral radius and Geršgorin's theorem . . . 327
7.6 Geometric Series . . . 336
7.7 Stochastic matrices and Markov chains . . . 342
7.8 Application: Finding approximate eigenvalues of a matrix . . . 354
7.9 Review Exercises . . . 362

8 Permutation Groups 369
8.1 Introduction . . . 369
8.2 Permutations . . . 372
8.3 Orbits and cycles . . . 375
8.4 Rigid Motions . . . 379
8.5 Permutation Groups . . . 386
8.6 Application to counting problems . . . 391
8.7 Restricted Colour Frequencies . . . 399
8.8 A Proof of Burnside's Theorem . . . 401
8.9 Review Exercises . . . 404

Solutions to Part A of the Review Problems 409

Index 415