

Contents

Preface	v
1 Identification Numbers and Modular Arithmetic	1
1.1 Examples of Identification Numbers	1
1.1.1 The USPS Zip Code	1
1.1.2 The Universal Product Code	2
1.1.3 International Standard Book Numbers	3
1.2 Modular Arithmetic	4
1.2.1 Arithmetic Operations in \mathbb{Z}_n	8
1.2.2 Greatest Common Divisors	11
1.2.3 The Euclidean Algorithm	13
1.3 Error Detection with Identification Numbers	18
References	21
2 Error Correcting Codes	23
2.1 Basic Notions	23
2.2 Gaussian Elimination	27
2.3 The Hamming Code	34
2.4 Coset Decoding	36
2.5 The Golay Code	39
References	40
3 Rings and Fields	41
3.1 The Definition of a Ring	41
3.2 First Properties of Rings	45
3.3 Fields	52
References	55
4 Linear Algebra and Linear Codes	57
4.1 Vector Spaces	57
4.2 Linear Independence, Spanning, and Bases	62
4.3 Linear Codes	67
References	72
5 Quotient Rings and Field Extensions	73
5.1 Arithmetic of Polynomial Rings	73

5.2	Ideals and Quotient Rings	76
5.3	Field Extensions	83
5.4	Algebraic Elements and Minimal Polynomials	88
	References	91
6	Ruler and Compass Constructions	93
6.1	Constructing a Coordinate System	94
6.2	The Field of Constructible Numbers	95
6.3	A Criterion for Constructibility	97
6.4	Classical Construction Problems	100
6.4.1	Angle Trisection	100
6.4.2	Duplicating a Cube	101
6.4.3	Squaring the Circle	101
6.4.4	Constructible Polygons	102
	References	104
7	Cyclic Codes	105
7.1	Introduction to Cyclic Codes	105
7.2	Finite Fields	108
7.3	Minimal Polynomials and Roots of Polynomials	110
7.4	Reed–Solomon Codes	113
7.5	Error Correction for Reed–Solomon Codes	116
	References	120
8	Groups and Cryptography	121
8.1	Definition and Examples of Groups	121
8.1.1	Subgroups	125
8.1.2	Lagrange’s Theorem	127
8.2	Cryptography and Group Theory	130
8.2.1	The RSA Encryption System	130
8.2.2	Secure Signatures with RSA	132
	References	134
9	The Structure of Groups	135
9.1	Direct Products	138
9.2	Normal Subgroups, Quotient Groups, and Homomorphisms	140
	References	144
10	Symmetry	145
10.1	Isometries	145
10.1.1	Origin-Preserving Isometries	149
10.1.2	Compositions of Isometries	152
10.2	Structure of the Group $\text{Isom}(\mathbb{R}^2)$	153
10.2.1	Semidirect Products	154
10.3	Symmetry Groups	156
10.3.1	Examples of Symmetry Groups	157
10.4	The Seven Frieze Groups	160
10.5	Point Groups of Wallpaper Patterns	163
10.5.1	Symmetry Groups of Bounded Plane Figures	163
10.5.2	Point Groups of Wallpaper Patterns	165

10.5.3	Equivalence Versus Isomorphism	167
10.5.4	The Five Lattice Types	169
10.6	The 17 Wallpaper Groups	178
	References	181
List of Symbols	183
Index	185