Applications of Abstract Algebra with MAPLE

Richard E. Klima
Neil Sigmon
Ernest Stitzinger

Contents

Preface v

1 Preliminary Mathematics 1

1.1 Permutation Groups 1

1.2 Cosets and Quotient Groups 6

1.3 Rings and Euclidean Domains 9

1.4 Finite Fields 13

1.5 Finite Fields with Maple 16

1.6 The Euclidean Algorithm 18

2 Block Designs 27

2.1 General Properties of Block Designs 27

2.2 Hadamard Matrices 31

2.3 Hadamard Matrices with Maple 33

2.4 Difference Sets 36

2.5 Difference Sets with Maple 39

3 Error-Correcting Codes 43

3.1 General Properties of Codes 43

3.2 Hadamard Codes 46

3.3 Reed-Muller Codes 48

3.4 Reed-Muller Codes with Maple 48
3.5 Linear Codes 53
3.6 Hamming Codes with Maple 60

4 BCH Codes **67**
4.1 Construction of BCH Codes 67
4.2 Error Correction in BCH Codes 70
4.3 BCH Codes with Maple 77
4.3.1 Construction of the Generator Polynomial 78
4.3.2 Error Correction 80

5 Reed-Solomon Codes **91**
5.1 Construction of Reed-Solomon Codes 91
5.2 Error Correction in Reed-Solomon Codes 93
5.3 Proof of Reed-Solomon Error Correction 97
5.4 Binary Reed-Solomon Codes 101
5.5 Reed-Solomon Codes with Maple 102
5.5.1 Construction of the Codewords 103
5.5.2 Error Correction 105
5.6 Reed-Solomon Codes in Voyager 2 111

6 Algebraic Cryptography **115**
6.1 Some Elementary Cryptosystems 115
6.2 The Hill Cryptosystem 119
6.3 The Hill Cryptosystem with Maple 124
6.4 Generalizations of the Hill Cryptosystem 129
6.5 The Two-Message Problem 131

7 The RSA Cryptosystem **139**
7.1 Mathematical Prerequisites 140

7.2 RSA Encryption and Decryption 142
7.3 The RSA Cryptosystem with Maple 147
7.4 A Note on Modular Exponentiation 150
7.5 A Note on Primality Testing 152
7.6 A Note on Integer Factorization 153
7.7 A Note on Digital Signatures 154
7.8 The Diffie-Hellman Key Exchange 155

8 Elliptic Curve Cryptography **163**
8.1 The ElGamal Cryptosystem 163
8.2 The ElGamal Cryptosystem with Maple 166
8.3 Elliptic Curves 168
8.4 Elliptic Curves with Maple 175
8.5 Elliptic Curve Cryptography 178
8.6 Elliptic Curve Cryptography with Maple 182

9 Polya Theory **189**
9.1 Group Actions 190
9.2 Burnside's Theorem 192
9.3 The Cycle Index 195
9.4 The Pattern Inventory 198
9.5 The Pattern Inventory with Maple 203
9.6 Switching Functions 205
9.7 Switching Functions with Maple 208

Appendices

A Basic Maple Tutorial **213**
A.1 Introduction to Maple 213
A.2 Arithmetic 214

A.3 Defining Variables and Functions 216
A.4 Algebra 217
A.5 Case Sensitivity 218
A.6 Help File 219
A.7 Arrays and Loops 219
A.8 Conditional Statements 221
A.9 Maple Procedures 223

B Some Maple Linear Algebra Commands **225**

C User-Written Maple Procedures **231**
C.1 Chapter 5 Procedures 231
C.2 Chapter 7 Procedures 234
C.3 Chapter 8 Procedures 235
C.4 Chapter 9 Procedures 236

Hints and Solutions to Selected Written Exercises **243**

Index **248**