Contents

1 Identification Numbers and Modular Arithmetic 1
   1.1 Examples of Identification Numbers 1
   1.2 Modular Arithmetic 4
   1.3 Error Detection with Identification Numbers 16

2 Error Correcting Codes 19
   2.1 Basic Notions 19
   2.2 Gaussian Elimination 22
   2.3 The Hamming Code 29

3 Rings and Fields 31
   3.1 The Definition of a Ring 31
   3.2 First Properties of Rings 35
   3.3 Fields 40

4 Linear Algebra 43
   4.1 Vector Spaces 43
   4.2 Linear Independence, Spanning, and Bases 48
   4.3 Linear Codes 51

5 Quotient Rings and Field Extensions 53
   5.1 Arithmetic of Polynomial Rings 53
   5.2 Ideals and Quotient Rings 56

6 Cyclic Codes 65
   6.1 BCH Codes 65
   6.2 Reed-Solomon Codes 65

7 Cryptography and Group Theory 67
   7.1 The RSA encryption system 67
   7.2 Groups 69
   7.3 Secure Signatures with RSA 75