

# Contents

|  |            |
|--|------------|
| <b>Preface</b>                                   | <b>vii</b> |
| <b>Chapter 1 Algebraic Foundations</b>           | <b>1</b>   |
| 1 Groups   | 2          |
| 2 Rings and Fields                               | 11         |
| 3 Polynomials                                    | 18         |
| 4 Field Extensions                               | 30         |
| Exercises  | 37         |
| <b>Chapter 2 Structure of Finite Fields</b>      | <b>43</b>  |
| 1 Characterization of Finite Fields              | 44         |
| 2 Roots of Irreducible Polynomials               | 47         |
| 3 Traces, Norms, and Bases                       | 50         |
| 4 Roots of Unity and Cyclotomic Polynomials      | 59         |
| 5 Representation of Elements of Finite Fields    | 62         |
| 6 Wedderburn's Theorem                           | 65         |
| Exercises  | 69         |
| <b>Chapter 3 Polynomials over Finite Fields</b>  | <b>74</b>  |
| 1 Order of Polynomials and Primitive Polynomials | 75         |
| 2 Irreducible Polynomials                        | 82         |

|                  |   |            |
|------------------|---|------------|
| 3                | Construction of Irreducible Polynomials               | 87         |
| 4                | Linearized Polynomials                                | 98         |
| 5                | Binomials and Trinomials                              | 115        |
|                  | Exercises   | 122        |
| <b>Chapter 4</b> | <b>Factorization of Polynomials</b>                   | <b>129</b> |
| 1                | Factorization over Small Finite Fields                | 130        |
| 2                | Factorization over Large Finite Fields                | 139        |
| 3                | Calculation of Roots of Polynomials                   | 150        |
|                  | Exercises   | 159        |
| <b>Chapter 5</b> | <b>Exponential Sums</b>                               | <b>162</b> |
| 1                | Characters  | 163        |
| 2                | Gaussian Sums   | 168        |
|                  | Exercises   | 181        |
| <b>Chapter 6</b> | <b>Linear Recurring Sequences</b>                     | <b>185</b> |
| 1                | Feedback Shift Registers, Periodicity Properties      | 186        |
| 2                | Impulse Response Sequences, Characteristic Polynomial | 193        |
| 3                | Generating Functions                                  | 202        |
| 4                | The Minimal Polynomial                                | 210        |
| 5                | Families of Linear Recurring Sequences                | 215        |
| 6                | Characterization of Linear Recurring Sequences        | 228        |
| 7                | Distribution Properties of Linear Recurring Sequences | 235        |
|                  | Exercises   | 245        |
| <b>Chapter 7</b> | <b>Theoretical Applications of Finite Fields</b>      | <b>251</b> |
| 1                | Finite Geometries                                     | 252        |
| 2                | Combinatorics   | 262        |
| 3                | Linear Modular Systems                                | 271        |
| 4                | Pseudorandom Sequences                                | 281        |
|                  | Exercises   | 294        |
| <b>Chapter 8</b> | <b>Algebraic Coding Theory</b>                        | <b>299</b> |
| 1                | Linear Codes  | 300        |
| 2                | Cyclic Codes  | 311        |
| 3                | Goppa Codes   | 325        |
|                  | Exercises   | 332        |
| <b>Chapter 9</b> | <b>Cryptography</b>                                   | <b>338</b> |
| 1                | Background  | 339        |

|                   |                                   |            |
|-------------------|-----------------------------------|------------|
| 2                 | Stream Ciphers                    | 342        |
| 3                 | Discrete Logarithms               | 346        |
| 4                 | Further Cryptosystems             | 360        |
|                   | Exercises                         | 363        |
| <b>Chapter 10</b> | <b>Tables</b>                     | <b>367</b> |
| 1                 | Computation in Finite Fields      | 367        |
| 2                 | Tables of Irreducible Polynomials | 377        |
|                   | <b>Bibliography</b>               | <b>392</b> |
|                   | <b>List of Symbols</b>            | <b>397</b> |
|                   | <b>Index</b>                      | <b>401</b> |