CONTENTS

Preface

PART ONE MATHEMATICAL FOUNDATIONS:
SETS AND INTEGERS

Chapter I SETS, RELATIONS, AND FUNCTIONS

1. Terminology of Sets 3
   1.1 Set Membership 3
   1.2 Equality and Inclusion 4

2. Operations on Sets 6
   2.1 Subset Specification; the Power Set 6
   2.2 Union, Intersection, and Complement 6
   2.3 The Cartesian Product 9

3. Relations 10
   3.1 The Relation Concept 10
   3.2 Equivalence Relations 13
   3.3 Partial Orders 16

4. Functions 21
   4.1 The Function Concept 21
   4.2 Composition and Invertibility 23
   4.3 Characteristic Functions 26
   4.4 Functions and Equivalence Relations 28

Exercises 30
Notes 33
Chapter II THE INTEGERS
1. Basic Properties
2. Induction and Recursion
3. Division and Divisibility
   3.1 Equivalence and Remainders mod $m$
   3.2 Greatest Common Divisors
   3.3 Factorization into Primes
Exercises

PART TWO ALGEBRAIC SYSTEMS

Prologue to Algebra: Algebraic Systems and Abstraction
1. Levels of Abstraction
2. Heterogeneous Algebras
   Prologue Notes

Chapter III SEMIGROUPS, MONOIDS, AND GROUPS
1. Basic Definitions and Examples
   1.0 Groupoids
   1.1 Semigroups
   1.2 Monoids
   1.3 Groups
2. Basic Properties of Binary Algebraic Systems
   2.1 Identity Elements in Semigroups
   2.2 Inverses in Monoids and Groups
   2.3 Solving Equations over Groups
   2.4 Products and Powers in Semigroups and Groups
3. Subalgebras (A Universal Algebra Concept)
   3.1 Definition and Examples
   3.2 Subalgebras Generated by Subsets
   3.3 Subgroups
   3.4 Cyclic Groups; Order of Group Elements
4. Morphisms (Another Universal Algebra Concept)
   4.1 The Morphism Concept
   4.2 Structure Preserving Properties of Morphisms
Exercises

Chapter IV RINGS, INTEGRAL DOMAINS, AND FIELDS
1. The Ring Concept
   1.1 Basic Definitions and Examples
   1.2 Subrings
   1.3 Morphisms of Rings
CONTENTS

2. Integral Domains and Fields 109
   2.1 Zerodivisors and Units; Integral Domains and Fields 109
   2.2 Field of Quotients 113

3. Polynomials and Formal Power Series 115
   3.1 Algebra of Polynomials and Formal Power Series 116
   3.2 The Division Property of Polynomials 121
   3.3 Polynomials as Functions 124

4. Divisibility; Euclidean Domains 128
   4.1 Divisibility Concepts in Integral Domains 128
   4.2 Euclidean Domains 131

Exercises 137

Chapter V QUOTIENT ALGEBRAS 143

1. Universal Quotient Algebras 143
   1.1 Congruence Relations 143
   1.2 The Quotient Algebra/Morphism Theorems of Universal Algebra 145

2. Quotient Rings 148
   2.1 Ideals and Quotient Rings 148
   2.2 Isomorphism Theorem for Rings 153

3. Further Theory of Ideals 157
   3.1 Principal Ideal Domains 157
   3.2 Unital Subrings; Prime Subfields 160
   3.3 Prime and Maximal Ideals 162

Exercises 167
Notes 170

Chapter VI ELEMENTS OF FIELD THEORY 171

1. Extension Fields 171
   1.1 The Root Adjunction Problem 171
   1.2 Analysis of Simple Extension Fields 174

2. The Multiplicative Group of a Finite Field 178
   2.1 Cyclic Property of Finite Fields 179
   2.2 Finite Fields as Algebraic Extensions 180

3. Uniqueness and Existence of Finite Fields 184
   3.1 Uniqueness of GF(p^n) 184
   3.2 Existence of GF(p^n) 186

Exercises 187
Notes 189
<table>
<thead>
<tr>
<th>PART THREE</th>
<th>ALGEBRAIC COMPUTING</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter VII</td>
<td>ARITHMETIC IN EUCLIDEAN DOMAINS</td>
</tr>
<tr>
<td>1.</td>
<td>Complexity of Integer and Polynomial Arithmetic</td>
</tr>
<tr>
<td>1.1</td>
<td>Polynomial Arithmetic</td>
</tr>
<tr>
<td>1.2</td>
<td>Integer Arithmetic</td>
</tr>
<tr>
<td>2.</td>
<td>Computation of Greatest Common Divisors</td>
</tr>
<tr>
<td>2.1</td>
<td>Derivation of Euclid's Algorithm</td>
</tr>
<tr>
<td>2.2</td>
<td>Analysis of Euclid's Algorithm over ( \mathbb{Z} ) and ( F[x] )</td>
</tr>
<tr>
<td>2.3</td>
<td>Euclid's Extended Algorithm</td>
</tr>
<tr>
<td>3.</td>
<td>Computation of ( \text{mod} \ m ) Inverses</td>
</tr>
<tr>
<td>3.1</td>
<td>Theory of ( \text{mod} \ m ) Inverses</td>
</tr>
<tr>
<td>3.2</td>
<td>Computation of ( \text{mod} \ m ) Inverses</td>
</tr>
<tr>
<td>Appendix: The Invariant Relation Theorem</td>
<td></td>
</tr>
<tr>
<td>Exercises</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter VIII</th>
<th>COMPUTATION BY HOMOMORPHIC IMAGES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>Computation by a Single Homomorphic Image</td>
</tr>
<tr>
<td>1.1</td>
<td>( \Omega )-Expressions and their Evaluation</td>
</tr>
<tr>
<td>1.2</td>
<td>Solutions to an Integer Congruence</td>
</tr>
<tr>
<td>1.3</td>
<td>The Homomorphc Image Scheme for ( \mathbb{Z} )</td>
</tr>
<tr>
<td>2.</td>
<td>Chinese Remainder and Interpolation Algorithms</td>
</tr>
<tr>
<td>2.1</td>
<td>A CRA for Euclidean Domains</td>
</tr>
<tr>
<td>2.2</td>
<td>A CRA for ( \mathbb{Z} )</td>
</tr>
<tr>
<td>2.3</td>
<td>A CRA for ( F[x] ): Interpolation</td>
</tr>
<tr>
<td>3.</td>
<td>Computation by Multiple Homomorphic Images</td>
</tr>
<tr>
<td>3.1</td>
<td>The MHI Scheme for ( \mathbb{Z} )</td>
</tr>
<tr>
<td>3.2</td>
<td>The MHI Scheme for ( F[x] )</td>
</tr>
<tr>
<td>3.3</td>
<td>The MHI Scheme for ( \mathbb{Z}[x] )</td>
</tr>
<tr>
<td>Appendix 1: Computing Lists of Primes</td>
<td></td>
</tr>
<tr>
<td>Appendix 2: &quot;Adjoint Solution&quot; to ( Ax = b )</td>
<td></td>
</tr>
<tr>
<td>Exercises</td>
<td></td>
</tr>
<tr>
<td>Notes</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter IX</th>
<th>THE FAST FOURIER TRANSFORM: ITS ROLE IN COMPUTER ALGEBRA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>What is the Fast Fourier Transform?</td>
</tr>
<tr>
<td>1.1</td>
<td>The Forward Transform: Fast Multipoint Evaluation</td>
</tr>
<tr>
<td>1.2</td>
<td>The Inverse Transform: Fast Interpolation</td>
</tr>
<tr>
<td>1.3</td>
<td>Feasibility of ( \text{mod} \ p ) FFTs</td>
</tr>
</tbody>
</table>
CONTENTS

2. Fast Algorithms for Multiplying Polynomials and Integers 307
   2.1 Fast Polynomial Multiplication 307
   2.2 Fast Integer Multiplication 308

3. Fast Algorithms for Manipulating Formal Power Series 312
   3.1 Truncated Power Series Revisited 312
   3.2 Fast Power Series Inversion; Newton's Method 313
   3.3 Polynomial Root-Finding over Power Series Domains 318

Exercises 325
Notes 327

SELECTED BIBLIOGRAPHY 330

INDEX TO NOTATION 333

INDEX 337