

Contents

Preface	v
How to Use This Book	xi
List of Algorithms	xxi
0 Basics	1
0.1 Natural Numbers and Integers	1
0.2 Maps	5
0.3 Mathematical Algorithms	9
Notes	12
1 Commutative Rings with Unity	15
1.1 Why Abstract Algebra?	15
1.2 Groups	16
1.3 Rings	19
1.4 Subrings and Homomorphisms	22
1.5 Ideals and Residue Class Rings	25
1.6 The Homomorphism Theorem	32
1.7 Gcd's, Lcm's, and Principal Ideal Domains	38
1.8 Maximal and Prime Ideals	47
1.9 Prime Rings and Characteristic	49
1.10 Adjunction, Products, and Quotient Rings	51
Notes	58
2 Polynomial Rings	61
2.1 Definitions	61
2.2 Euclidean Domains	78
2.3 Unique Factorization Domains	87
2.4 The Gaussian Lemma	92
2.5 Polynomial Gcd's	97
2.6 Squarefree Decomposition of Polynomials	99
2.7 Factorization of Polynomials	109
2.8 The Chinese Remainder Theorem	114
Notes	116

3	Vector Spaces and Modules	119
3.1	Vector Spaces	119
3.2	Independent Sets and Dimension	129
3.3	Modules	133
	Notes	138
4	Orders and Abstract Reduction Relations	141
4.1	The Axiom of Choice and Some Consequences in Algebra	141
4.2	Relations	149
4.3	Foundedness Properties	155
4.4	Some Special Orders	167
4.5	Reduction Relations	173
4.6	Computing in Algebraic Structures	178
	Notes	183
5	Gröbner Bases	187
5.1	Term Orders and Polynomial Reductions	188
5.2	Gröbner Bases—Existence and Uniqueness	204
5.3	Gröbner Bases—Construction	210
5.4	Standard Representations	218
5.5	Improved Gröbner Basis Algorithms	222
5.6	The Extended Gröbner Basis Algorithm	237
	Notes	241
6	First Applications of Gröbner Bases	243
6.1	Computation of Syzygies	243
6.2	Basic Algorithms in Ideal Theory	256
6.3	Dimension of Ideals	270
6.4	Uniform Word Problems	276
	Notes	291
7	Field Extensions and the Hilbert Nullstellensatz	293
7.1	Field Extensions	293
7.2	The Algebraic Closure of a Field	306
7.3	Separable Polynomials and Perfect Fields	309
7.4	The Hilbert Nullstellensatz	312
7.5	Height and Depth of Prime Ideals	323
7.6	Implicitization of Rational Parametrizations	327
7.7	Invertibility of Polynomial Maps	330
	Notes	332
8	Decomposition, Radical, and Zeroes of Ideals	335
8.1	Preliminaries	335
8.2	The Radical of a Zero-Dimensional Ideal	340
8.3	The Number of Zeroes of an Ideal	346

8.4	Primary Ideals	350
8.5	Primary Decomposition in Noetherian Rings	358
8.6	Primary Decomposition of Zero-Dimensional Ideals	366
8.7	Radical and Decomposition in Higher Dimensions	388
8.8	Computing Real Zeroes of Polynomial Systems	399
	Notes	419
9	Linear Algebra in Residue Class Rings	423
9.1	Gröbner Bases and Reduced Terms	423
9.2	Computing in Finitely Generated Algebras	433
9.3	Dimensions and the Hilbert Function	441
	Notes	451
10	Variations on Gröbner Bases	453
10.1	Gröbner Bases over PID's and Euclidean Domains	453
10.2	Homogeneous Gröbner Bases	466
10.3	Homogenization	477
10.4	Gröbner Bases for Polynomial Modules	485
10.5	Systems of Linear Equations	488
10.6	Standard Bases and the Tangent Cone	496
10.7	Symmetric Functions	501
	Notes	508
	Appendix: Outlook on Advanced and Related Topics	511
	Complexity of Gröbner Basis Constructions	511
	Term Orders and Universal Gröbner Bases	514
	Comprehensive Gröbner Bases	515
	Gröbner Bases and Automatic Theorem Proving	518
	Characteristic Sets and Wu-Ritt Reduction	520
	Term Rewriting	523
	Standard Bases in Power Series Rings	525
	Non-Commutative Gröbner Bases	526
	Gröbner Bases and Differential Algebra	528
	Selected Bibliography	531
	Conference Proceedings	531
	Books and Monographs	533
	Articles	536
	List of Symbols	561
	Index	567