

Contents

Preface	<i>page</i> xv
1 A Refresher on the Integers	1
1.1 Euclidean Division and the Greatest Common Divisor	1
1.2 Primes and Unique Factorization	7
1.3 Congruences	12
2 A First Look at Groups	20
2.1 Basic Properties and Examples of Groups	20
2.1.1 The Order of a Group and of Its Elements	27
2.2 The Symmetric Group	33
2.2.1 Equivalence Relations and Partitions	34
2.2.2 The Orbits and Cycles of a Permutation	35
2.2.3 Transpositions and the Parity of a Permutation	42
2.3 Subgroups and Lagrange's Theorem	50
2.3.1 Partitions of a Group by Right Cosets of a Subgroup	52
2.3.2 Subgroups of Cyclic Groups	58
2.4 Conjugation and Normal Subgroups	62
2.4.1 Conjugates in \mathcal{S}_n	65
2.4.2 Normal Subgroups of \mathcal{A}_n	67
2.4.3 Normal Subgroups of the Quaternion Group	71
2.5 Homomorphisms	73
2.5.1 The Kernel and Image of a Homomorphism	76
2.5.2 Isomorphisms	77
2.5.3 Automorphisms of Cyclic Groups	79
2.6 Quotient Groups	81
2.6.1 An Important Theorem of Cauchy	83
2.6.2 The First Isomorphism Theorem	84
2.6.3 The Correspondence Theorem	87
2.7 Products of Groups	91
2.7.1 The External Product	91
2.7.2 The Internal Product of Subgroups	94
2.8 Finite Abelian Groups	99
2.8.1 Groups of Prime Power Order	100

viii Contents

2.8.2	The Primary Decomposition	108
2.8.3	Putting the Bits Together	111
3	Groups Acting on Sets	116
3.1	Definition and Some Illustrations of Actions	116
3.1.1	A Group Action on Left Cosets	119
3.1.2	Groups of Order 6	120
3.2	Orbits and Stabilizers	122
3.2.1	An Action for the Dihedral Groups	125
3.2.2	The Symmetries of a Tetrahedron	128
3.3	The Cauchy–Frobenius–Burnside Formula	131
3.3.1	A Counting Technique Based on Burnside	133
3.4	The Class Equation and Its Implications	138
3.4.1	The Class Equation	138
3.4.2	The Class Equation and p -Groups	142
3.5	The Theorems of Cauchy and Sylow	145
3.5.1	Cauchy’s Theorem	146
3.5.2	Sylow’s Theorem	148
3.6	Semi-direct Products	159
3.6.1	Automorphism Actions of One Group on Another	159
3.6.2	Internal and Semi-direct Products	162
3.6.3	Groups of Order pq – the Full Description	163
3.7	Solvable Groups	170
3.7.1	The Second and Third Isomorphism Theorems	171
3.7.2	Subgroups and Quotients of Solvable Groups	173
3.7.3	Improving the Subnormal Chains for Solvable Groups	175
3.7.4	Commutators and the Derived Series	176
3.8	Breaking the Enigma	181
3.8.1	The Design of the Enigma Machine	181
3.8.2	The Mathematical Representation of the Enigma Machine	183
3.8.3	How the Machine Was Used	186
3.8.4	Finding the First Rotor Wiring	195
4	Basics on Rings – Mostly Commutative	203
4.1	Terminology and Examples	203
4.1.1	Compound Additions and Multiplications	206
4.1.2	Subrings	207
4.2	Units and Zero Divisors	210
4.2.1	The Group of Units	210
4.2.2	Zero Divisors	211
4.2.3	Integral Domains and Fields	213

	Contents	ix
4.3	Polynomials	216
4.3.1	The Definition of Polynomial Rings	217
4.3.2	Properties of the Degree	222
4.3.3	Polynomials in Several Variables	224
4.3.4	The Ring of Formal Power Series	224
4.4	Homomorphisms and Ideals	226
4.4.1	Ring Homomorphisms	227
4.4.2	The Kernel	231
4.4.3	Ideals	232
4.5	Ideals in \mathbb{Z} and in Polynomial Rings	237
4.5.1	Finite Groups of Units in a Field	240
4.6	Quotient Rings and the Isomorphism Theorem	244
4.6.1	The First Isomorphism Theorem for Rings	245
4.6.2	Computing the Euler Function	248
4.6.3	The Correspondence Theorem	249
4.7	Maximal and Prime Ideals	252
4.7.1	Maximal Ideals and the Construction of Fields	253
4.7.2	Existence of Maximal Ideals	254
4.7.3	Prime Ideals and Integral Domains	255
4.7.4	Building Fields from Polynomial Rings	256
4.8	Fractions	259
4.8.1	Localizations at Denominator Sets	259
4.8.2	Uniqueness of Localizations	261
4.8.3	Existence of Localizations	262
5	Primes and Unique Factorization	268
5.1	Primes, Irreducibles and Factoring	268
5.2	Principal Ideal and Noetherian Domains	274
5.2.1	Noetherian Domains	275
5.3	Euclidean Domains	278
5.4	Gaussian Primes and Sums of Squares	281
5.5	Greatest Common Divisors	285
5.6	Polynomials over Unique Factorization Domains	294
5.6.1	Gauss' Lemma	294
5.6.2	The Primes of $A[X]$ and Its Unique Factorization	297
5.7	Irreducible Polynomials	300
5.7.1	The Rational Root Test	301
5.7.2	Using a Natural Extension of Homomorphisms	304
5.7.3	Eisenstein's Criterion	305
5.8	Polynomials over Noetherian Rings	308
5.8.1	Hilbert's Basis Theorem: a Source of Noetherian Rings	309

x	Contents	
	5.8.2 Eisenstein's Criterion for Noetherian Domains	311
	5.8.3 Primes in Rings Coming from Algebraic Integers	314
	5.8.4 A Principal Ideal Domain that Is Not Euclidean	317
6	Algebraic Field Extensions	322
6.1	Algebraic Elements and Degrees of Extensions	322
6.1.1	The Degree of a Field Extension	322
6.1.2	Algebraic Elements	323
6.1.3	The Minimal Polynomial of an Algebraic Element	325
6.1.4	A Basis for a Singly Generated Algebraic Extension	327
6.1.5	Algebraic Elements with the Same Minimal Polynomial	329
6.1.6	The Tower Theorem	330
6.1.7	Fields Generated by Several Algebraic Elements	331
6.1.8	The Algebraic Closure inside a Field Extension	334
6.1.9	The Tower Theorem and Composite Fields	335
6.1.10	The Tower Theorem Used in Conjunction with Eisenstein for Noetherian Domains	337
6.2	Splitting Fields	341
6.2.1	The Synthesis of Algebraic Elements	341
6.2.2	What Is a Splitting Field?	343
6.2.3	Lifting Isomorphisms to Splitting Fields	346
6.2.4	The Uniqueness of Splitting Fields	349
6.2.5	Finite Fields of Equal Size Are Isomorphic	349
6.2.6	Splitting Fields Are Rich with Automorphisms	350
6.2.7	Fixed Fields, F -Maps and F -Conjugates	351
6.2.8	The Normality Theorem	352
6.2.9	A Control on the Degree of a Splitting Field	355
6.2.10	Quadratic Extensions Are Splitting Fields	356
6.3	Separability	360
6.3.1	Derivatives of Polynomials and Repeated Roots	360
6.3.2	Separable Polynomials and the Derivative	362
6.3.3	Finite Fields of All Possible Sizes	364
6.3.4	Factoring $X^{p^n} - X$ in $\mathbb{Z}_p[X]$	365
6.3.5	Perfect Fields	366
6.4	The Galois Group	371
6.4.1	Roots, Generators and Galois Groups	372
6.4.2	Some Examples of Galois Groups	374
6.5	The Core of Galois Theory	379
6.5.1	The Independence of Characters	379
6.5.2	A Bound on the Order of a Galois Group	381
6.5.3	The Fixed Field of an Automorphism Group	382

	Contents	xi
6.5.4	Galois Extensions	383
6.5.5	Artin's Theorem	386
6.5.6	The Galois Correspondence	387
6.5.7	The Fundamental Theorem of Galois Theory	388
6.5.8	The Normality Connection	389
7	Applications of Galois Theory	397
7.1	Three Classical Theorems	397
7.1.1	The Primitive Generator Theorem	397
7.1.2	The Fundamental Theorem of Algebra	399
7.1.3	The Symmetric Function Theorem	399
7.2	Special Extensions and Their Galois Groups	403
7.2.1	The Galois Correspondence in Finite Fields	403
7.2.2	The Galois Groups of Cubics	405
7.2.3	Cyclotomic Extensions	408
7.3	Solvability of Equations by Radicals	414
7.3.1	Cardano's Formula	414
7.3.2	Extensions by a Single Radical and Cyclic Galois Groups	418
7.3.3	Radical Towers	420
7.3.4	Solvable Polynomials Have Solvable Galois Groups	424
7.3.5	Polynomials with Solvable Galois Groups Are Solvable	426
7.4	Ruler and Compass Constructions	428
7.4.1	Constructible Points, Lines and Circles	429
7.4.2	Constructible Real Numbers	433
7.4.3	Constructible Real Numbers and Field Towers	435
7.4.4	Constructible Complex Numbers	440
7.5	The Inverse Galois Problem over \mathbb{Q}	444
8	Modules over Principal Ideal Domains	450
8.1	The Language and Tools of Modules	450
8.1.1	Examples of Modules	451
8.1.2	Module Homomorphisms	452
8.1.3	Submodules	453
8.1.4	Free Modules	454
8.1.5	Quotient Modules and the First Isomorphism Theorem	457
8.1.6	Cyclic Modules and Annihilator Ideals	459
8.1.7	Direct Sums of Submodules	460
8.1.8	Free Modules Are Projective	462
8.2	Modules over Integral Domains	464
8.2.1	Torsion Elements and Modules	465
8.2.2	Rank	466

xii Contents

8.3	Modules over Principal Ideal Domains	468
8.3.1	Splitting Torsion from Torsion-Free	469
8.3.2	Torsion Modules over a Principal Ideal Domain	471
8.3.3	Primary Modules over a Principal Ideal Domain	475
8.3.4	Structure of Finitely Generated Modules over a Principal Ideal Domain	479
8.4	Linear Algebra and Modules	488
9	Division Algorithms	507
9.1	Well-Partial Orders	508
9.1.1	Well-Ordered Sets: Total and Partial	508
9.1.2	The Dickson Basis	513
9.1.3	Extensions of Well-Partial Orders	514
9.2	Gröbner Domains	520
9.2.1	Gröbner Functions	520
9.2.2	The Gröbner Basis of an Ideal	522
9.2.3	Polynomials in Several Variables Are Gröbner Domains	524
9.2.4	A Division Algorithm for Complete Reductions	527
9.3	Buchberger's Algorithm	539
9.3.1	Detecting Gröbner Bases via S -Polynomials	539
9.3.2	Buchberger's Algorithm	545
9.4	Applications of Gröbner Bases	553
9.4.1	Gröbner Bases for Ideal Intersections	554
9.4.2	Units and Zero Divisors in Finitely Generated Algebras	559
9.4.3	Normal Forms	563
9.4.4	Finite Varieties	570
9.4.5	Hilbert's Nullstellensatz and Idempotents	575
A	Infinite Sets	593
A.1	Zorn's Lemma	593
A.1.1	Choice Functions	593
A.1.2	Chains of Subsets	593
A.1.3	Chain Maximality in Partially Ordered Sets	595
A.1.4	Choice Implies Zorn	597
A.1.5	The Well-Ordering Principle	597
A.1.6	Zorn Implies Choice	599
A.2	The Size of Infinite Sets	600
A.2.1	Infinite Sets and the Positive Integers	600
A.2.2	Comparing Sets	601
A.2.3	Countable Sets	602
A.2.4	The Cantor–Schröder–Bernstein Theorem	603

	Contents	xiii
A.2.5	Total Ordering by Cardinality	604
A.2.6	The Unboundedness of Cardinality	605
A.2.7	A Bit of Cardinal Arithmetic	606
A.3	The Algebraic Closure of a Field	611
	Index	617