

Contents

Preface	v
Notation	xix
PART I POLYNOMIALS	
Chapter 1 Cubic Equations	3
1.1 Cardan's Formulas	3
Historical Notes	8
1.2 Permutations of the Roots	10
A Permutations	10
B The Discriminant	11
C Symmetric Polynomials	13
Mathematical Notes	14
Historical Notes	14
1.3 Cubic Equations over the Real Numbers	15
A The Number of Real Roots	15
B Trigonometric Solution of the Cubic	18
Historical Notes	19
References	23

Chapter 2 Symmetric Polynomials	25
2.1 Polynomials of Several Variables	25
A The Polynomial Ring in n Variables	25
B The Elementary Symmetric Polynomials	27
Mathematical Notes	29
2.2 Symmetric Polynomials	30
A The Fundamental Theorem	30
B The Roots of a Polynomial	34
C Uniqueness	35
Mathematical Notes	37
Historical Notes	37
2.3 Computing with Symmetric Polynomials (Optional)	41
A Using <i>Mathematica</i>	42
B Using <i>Maple</i>	43
2.4 The Discriminant	46
Mathematical Notes	48
Historical Notes	50
References	53
Chapter 3 Roots of Polynomials	55
3.1 The Existence of Roots	55
Mathematical Notes	59
Historical Notes	61
3.2 The Fundamental Theorem of Algebra	62
Mathematical Notes	66
Historical Notes	67
References	70
PART II FIELDS	
Chapter 4 Extension Fields	73
4.1 Elements of Extension Fields	73
A Minimal Polynomials	74
B Adjoining Elements	75
Mathematical Notes	79
Historical Notes	79

4.2	Irreducible Polynomials	81
A	Using <i>Maple</i> and <i>Mathematica</i>	81
B	Algorithms for Factoring	83
C	The Schönemann–Eisenstein Criterion	84
D	Prime Radicals	85
	Historical Notes	87
4.3	The Degree of an Extension	88
A	Finite Extensions	89
B	The Tower Theorem	91
	Mathematical Notes	93
	Historical Notes	93
4.4	Algebraic Extensions	94
	Mathematical Notes	97
	References	98

Chapter 5 Normal and Separable Extensions 101

5.1	Splitting Fields	101
A	Definitions and Examples	101
B	Uniqueness	103
5.2	Normal Extensions	107
	Historical Notes	108
5.3	Separable Extensions	109
A	Fields of Characteristic 0	112
B	Fields of Characteristic p	113
C	Computations	114
	Mathematical Notes	116
5.4	The Theorem of the Primitive Element	119
	Mathematical Notes	122
	Historical Notes	122
	References	123

Chapter 6 The Galois Group 125

6.1	Definition of the Galois Group	125
	Historical Notes	128
6.2	Galois Groups of Splitting Fields	130
6.3	Permutations of the Roots	132
	Mathematical Notes	134
	Historical Notes	135

6.4	Examples of Galois Groups	136
A	The p th Roots of 2	136
B	The Universal Extension	137
C	A Polynomial of Degree 5	138
	Mathematical Notes	139
	Historical Notes	141
6.5	Abelian Equations (Optional)	143
	Historical Notes	144
	References	146
Chapter 7 The Galois Correspondence		147
7.1	Galois Extensions	147
A	Splitting Fields of Separable Polynomials	147
B	Finite Separable Extensions	150
C	Galois Closures	151
	Historical Notes	152
7.2	Normal Subgroups and Normal Extensions	154
A	Conjugate Fields	154
B	Normal Subgroups	155
	Mathematical Notes	159
	Historical Notes	160
7.3	The Fundamental Theorem of Galois Theory	161
7.4	First Applications	167
A	The Discriminant	167
B	The Universal Extension	169
C	The Inverse Galois Problem	170
	Historical Notes	172
7.5	Automorphisms and Geometry (Optional)	173
A	Groups of Automorphisms	173
B	Function Fields in One Variable	176
C	Linear Fractional Transformations	178
D	Stereographic Projection	180
	Mathematical Notes	183
	References	188

PART III APPLICATIONS

Chapter 8 Solvability by Radicals	191
8.1 Solvable Groups	191
Mathematical Notes	194
8.2 Radical and Solvable Extensions	196
A Definitions and Examples	196
B Compositums and Galois Closures	198
C Properties of Radical and Solvable Extensions	198
Historical Notes	200
8.3 Solvable Extensions and Solvable Groups	201
A Roots of Unity and Lagrange Resolvents	201
B Galois's Theorem	204
C Cardan's Formulas	207
Historical Notes	208
8.4 Simple Groups	210
Mathematical Notes	214
Historical Notes	214
8.5 Solving Polynomials by Radicals	215
A Roots and Radicals	215
B The Universal Polynomial	217
C Abelian Equations	217
D The Fundamental Theorem of Algebra Revisited	218
Historical Notes	219
8.6 The <i>Casus Irreducibilis</i> (Optional)	220
A Real Radicals	220
B Irreducible Polynomials with Real Radical Roots	222
C The Failure of Solvability in Characteristic p	224
Historical Notes	226
References	227
Chapter 9 Cyclotomic Extensions	229
9.1 Cyclotomic Polynomials	229
A Some Number Theory	229
B Definition of Cyclotomic Polynomials	231
C The Galois Group of a Cyclotomic Extension	233
Historical Notes	235

9.2	Gauss and Roots of Unity (Optional)	238
A	The Galois Correspondence	238
B	Periods	239
C	Explicit Calculations	242
D	Solvability by Radicals	246
	Mathematical Notes	248
	Historical Notes	249
	References	254

Chapter 10 Geometric Constructions 255

10.1	Constructible Numbers	255
	Mathematical Notes	263
	Historical Notes	266
10.2	Regular Polygons and Roots of Unity	269
	Historical Notes	271
10.3	Origami (Optional)	273
A	Origami Constructions	274
B	Origami Numbers	276
C	Marked Rulers and Intersections of Conics	279
	Mathematical Notes	281
	Historical Notes	282
	References	287

Chapter 11 Finite Fields 289

11.1	The Structure of Finite Fields	289
A	Existence and Uniqueness	289
B	Galois Groups	292
	Mathematical Notes	294
	Historical Notes	295
11.2	Irreducible Polynomials over Finite Fields (Optional)	299
A	Irreducible Polynomials of Fixed Degree	299
B	Cyclotomic Polynomials Modulo p	301
C	Berlekamp's Algorithm	303
	Historical Notes	305
	References	308

PART IV FURTHER TOPICS

Chapter 12 Lagrange, Galois, and Kronecker	313
12.1 Lagrange	313
A Resolvent Polynomials	314
B Similar Functions	318
C The Quartic	321
D Higher Degrees	324
E Lagrange Resolvents	326
Historical Notes	327
12.2 Galois	332
A Beyond Lagrange	333
B Galois Resolvents	333
C Galois's Group	336
D Natural and Accessory Irrationalities	337
E Galois's Strategy	339
Historical Notes	341
12.3 Kronecker	346
A Algebraic Quantities	346
B Module Systems	347
C Splitting Fields	349
Historical Notes	352
References	354
Chapter 13 Computing Galois Groups	357
13.1 Quartic Polynomials	357
Mathematical Notes	362
Historical Notes	365
13.2 Quintic Polynomials	367
A Transitive Subgroups of S_5	367
B Galois Groups of Quintics	370
C Examples	375
D Solvable Quintics	376
Mathematical Notes	377
Historical Notes	379
13.3 Resolvents	384
A Jordan's Strategy	384
B Relative Resolvents	388

C Factoring Resolvents	389
Mathematical Notes	391
13.4 Other Methods	394
A Kronecker's Analysis	394
B Dedekind's Theorem	398
Mathematical Notes	401
References	404
Chapter 14 Solvable Permutation Groups	407
14.1 Polynomials of Prime Degree	407
Mathematical Notes	410
Historical Notes	411
14.2 Imprimitive Polynomials of Prime-Squared Degree	412
A Primitive and Imprimitive Groups	413
B Wreath Products	414
C The Solvable Case	417
Mathematical Notes	419
Historical Notes	419
14.3 Primitive Permutation Groups	422
A Doubly Transitive Permutation Groups	423
B Affine Linear and Semilinear Groups	424
C Minimal Normal Subgroups	425
D The Solvable Case	427
Mathematical Notes	431
Historical Notes	433
14.4 Primitive Polynomials of Prime-Squared Degree	438
A The First Two Subgroups	438
B The Third Subgroup	439
C The Solvable Case	444
Mathematical Notes	451
Historical Notes	452
References	455
Chapter 15 The Lemniscate	457
15.1 Division Points and Arc Length	458
A Division Points	458

B Arc Length of the Lemniscate	460
Mathematical Notes	462
Historical Notes	463
15.2 The Lemniscatic Function	465
A A Periodic Function	465
B Addition Laws	467
C Multiplication by Integers	470
Historical Notes	473
15.3 The Complex Lemniscatic Function	476
A A Doubly Periodic Function	477
B Zeros and Poles	479
Mathematical Notes	481
Historical Notes	482
15.4 Complex Multiplication	483
A The Gaussian Integers	485
B Multiplication by Gaussian Integers	485
C Multiplication by Gaussian Primes	492
Mathematical Notes	495
Historical Notes	496
15.5 Abel's Theorem	499
A The Lemniscatic Galois Group	499
B Straightedge-and-Compass Constructions	500
Mathematical Notes	503
Historical Notes	504
References	507

Appendix A Abstract Algebra	509
A.1 Basic Algebra	509
A Groups	509
B Rings	513
C Fields	514
D Polynomials	515
A.2 Complex Numbers	518
A Addition, Multiplication, and Division	518
B Roots of Complex Numbers	519
A.3 Polynomials with Rational Coefficients	522

A.4	Group Actions	523
A.5	More Algebra	526
A	The Sylow Theorems	526
B	The Chinese Remainder Theorem	527
C	The Multiplicative Group of a Field	527
D	Unique Factorization Domains	528
Appendix B Hints to Selected Exercises		529
References		543
A	Books and Monographs on Galois Theory	543
B	Books on Abstract Algebra	544
C	Collected Works	544
Index		547