

# Contents

<b>Preface.....</b>	<b>vii</b>
<b>Contents.....</b>	<b>ix</b>
<b>0 Preliminaries.....</b>	<b>1</b>
0.1 Lattices.....	1
0.2 Groups.....	2
0.3 The Symmetric Group.....	10
0.4 Rings.....	10
0.5 Integral Domains.....	14
0.6 Unique Factorization Domains.....	16
0.7 Principal Ideal Domains.....	16
0.8 Euclidean Domains.....	17
0.9 Tensor Products.....	17
Exercises.....	19
<b>Part I—Field Extensions</b>	
<b>1 Polynomials.....</b>	<b>23</b>
1.1 Polynomials over a Ring.....	23
1.2 Primitive Polynomials and Irreducibility.....	24
1.3 The Division Algorithm and Its Consequences.....	27
1.4 Splitting Fields.....	32
1.5 The Minimal Polynomial.....	32
1.6 Multiple Roots.....	33
1.7 Testing for Irreducibility.....	35
Exercises.....	38
<b>2 Field Extensions.....</b>	<b>41</b>
2.1 The Lattice of Subfields of a Field.....	41
2.2 Types of Field Extensions.....	42
2.3 Finitely Generated Extensions.....	46
2.4 Simple Extensions.....	47
2.5 Finite Extensions.....	53
2.6 Algebraic Extensions.....	54

2.7 Algebraic Closures.....	56
2.8 Embeddings and Their Extensions.....	58
2.9 Splitting Fields and Normal Extensions.....	63
Exercises.....	66
<b>3 Embeddings and Separability.....</b>	<b>73</b>
3.1 Recap and a Useful Lemma.....	73
3.2 The Number of Extensions: Separable Degree.....	75
3.3 Separable Extensions.....	77
3.4 Perfect Fields.....	84
3.5 Pure Inseparability.....	85
*3.6 Separable and Purely Inseparable Closures.....	88
Exercises.....	91
<b>4 Algebraic Independence.....</b>	<b>93</b>
4.1 Dependence Relations.....	93
4.2 Algebraic Dependence.....	96
4.3 Transcendence Bases.....	100
*4.4 Simple Transcendental Extensions.....	105
Exercises.....	108
<b>Part II—Galois Theory</b>	
<b>5 Galois Theory I: An Historical Perspective.....</b>	<b>113</b>
5.1 The Quadratic Equation.....	113
5.2 The Cubic and Quartic Equations.....	114
5.3 Higher-Degree Equations.....	116
5.4 Newton's Contribution: Symmetric Polynomials.....	117
5.5 Vandermonde.....	119
5.6 Lagrange.....	121
5.7 Gauss.....	124
5.8 Back to Lagrange.....	128
5.9 Galois.....	130
5.10 A Very Brief Look at the Life of Galois.....	135
<b>6 Galois Theory II: The Theory.....</b>	<b>137</b>
6.1 Galois Connections.....	137
6.2 The Galois Correspondence.....	143
6.3 Who's Closed?.....	148
6.4 Normal Subgroups and Normal Extensions.....	154
6.5 More on Galois Groups.....	159
6.6 Abelian and Cyclic Extensions.....	164
*6.7 Linear Disjointness.....	165
Exercises.....	168
<b>7 Galois Theory III: The Galois Group of a Polynomial.....</b>	<b>173</b>
7.1 The Galois Group of a Polynomial.....	173
7.2 Symmetric Polynomials.....	174
7.3 The Fundamental Theorem of Algebra.....	179

7.4 The Discriminant of a Polynomial.....	180
7.5 The Galois Groups of Some Small-Degree Polynomials.....	182
Exercises.....	193
<b>8 A Field Extension as a Vector Space.....</b>	<b>197</b>
8.1 The Norm and the Trace.....	197
*8.2 Characterizing Bases.....	202
*8.3 The Normal Basis Theorem.....	206
Exercises.....	208
<b>9 Finite Fields I: Basic Properties.....</b>	<b>211</b>
9.1 Finite Fields Redux.....	211
9.2 Finite Fields as Splitting Fields.....	212
9.3 The Subfields of a Finite Field.....	213
9.4 The Multiplicative Structure of a Finite Field.....	214
9.5 The Galois Group of a Finite Field.....	215
9.6 Irreducible Polynomials over Finite Fields.....	215
*9.7 Normal Bases.....	218
*9.8 The Algebraic Closure of a Finite Field.....	219
Exercises.....	223
<b>10 Finite Fields II: Additional Properties.....</b>	<b>225</b>
10.1 Finite Field Arithmetic.....	225
*10.2 The Number of Irreducible Polynomials.....	232
*10.3 Polynomial Functions.....	234
*10.4 Linearized Polynomials.....	236
Exercises.....	238
<b>11 The Roots of Unity.....</b>	<b>239</b>
11.1 Roots of Unity.....	239
11.2 Cyclotomic Extensions.....	241
*11.3 Normal Bases and Roots of Unity.....	250
*11.4 Wedderburn's Theorem.....	251
*11.5 Realizing Groups as Galois Groups.....	253
Exercises.....	257
<b>12 Cyclic Extensions.....</b>	<b>261</b>
12.1 Cyclic Extensions.....	261
12.2 Extensions of Degree $\text{Char}(F)$ .....	265
Exercises.....	266
<b>13 Solvable Extensions.....</b>	<b>269</b>
13.1 Solvable Groups.....	269
13.2 Solvable Extensions.....	270
13.3 Radical Extensions.....	273
13.4 Solvability by Radicals.....	274
13.5 Solvable Equivalent to Solvable by Radicals.....	276
13.6 Natural and Accessory Irrationalities.....	278
13.7 Polynomial Equations.....	280

Exercises.....	282
<b>Part III—The Theory of Binomials</b>	
<b>14    Binomials.....</b>	<b>289</b>
14.1 Irreducibility.....	289
14.2 The Galois Group of a Binomial.....	296
*14.3 The Independence of Irrational Numbers.....	304
Exercises.....	307
<b>15    Families of Binomials.....</b>	<b>309</b>
15.1 The Splitting Field.....	309
15.2 Dual Groups and Pairings.....	310
15.3 Kummer Theory.....	312
Exercises.....	316
<b>Appendix: Möbius Inversion.....</b>	<b>319</b>
Partially Ordered Sets.....	319
The Incidence Algebra of a Partially Ordered Set.....	320
Classical Möbius Inversion.....	324
Multiplicative Version of Möbius Inversion.....	325
<b>References.....</b>	<b>327</b>
<b>Index.....</b>	<b>329</b>