Contents

Sections marked with an asterisk are optional.

Preface vii

Chapter 0

Preliminaries 1

0.1 Lattices 1
0.2 Groups 3
0.3 Rings 12
0.4 Integral Domains 15
0.5 Unique Factorization Domains 17
0.6 Principal Ideal Domains 17
0.7 Euclidean Domains 18
0.8 Tensor Products 19

Part 1 Basic Theory 23

Chapter 1

Polynomials 25

1.1 Polynomials Over a Ring 25
1.2 Primitive Polynomials 26
1.3 The Division Algorithm 28
1.4 Splitting Fields 31
1.5 The Minimal Polynomial 32
1.6 Multiple Roots 33
1.7 Testing for Irreducibility 35

Chapter 2
Field Extensions 39
2.1 The Lattice of Subfields of a Field 39
2.2 Distinguished Extensions 40
2.3 Finitely Generated Extensions 41
2.4 Simple Extensions 42
2.5 Finite Extensions 43
2.6 Algebraic Extensions 45
2.7 Algebraic Closures 46
2.8 Embeddings 48
2.9 Splitting Fields and Normal Extensions 52

Chapter 3
Algebraic Independence 61
3.1 Dependence Relations 61
3.2 Algebraic Dependence 64
3.3 Transcendence Bases 67
*3.4 Simple Transcendental Extensions 73

Chapter 4
Separability 79
4.1 Separable Polynomials 79
4.2 Separable Degree 81
4.3 The Simple Case 82
4.4 The Finite Case 84
4.5 The Algebraic Case 87
4.6 Pure Inseparability 88
4.7 Separable and Purely Inseparable Closures 91
4.8 Perfect Fields 94

Part 2 Galois Theory 99

Chapter 5
Galois Theory I 101
5.1 Galois Connections 101
5.2 The Galois Correspondence 104
5.3 Who's Closed? 109
5.4 Normal Subgroups and Normal Extensions 112
5.5 More on Galois Groups 113

*5.6 Linear Disjointness 117
*5.7 The Krull Topology 120

Chapter 6

Galois Theory II 127

6.1 The Galois Group of a Polynomial 127
6.2 Symmetric Polynomials 128
6.3 The Discriminant of a Polynomial 132
6.4 The Galois Groups of Some Small Degree Polynomials 134

Chapter 7

A Field Extension as a Vector Space 147

7.1 The Norm and the Trace 147
*7.2 The Discriminant of Field Elements 151
*7.3 Algebraic Independence of Embeddings 155
*7.4 The Normal Basis Theorem 156

Chapter 8

Finite Fields I: Basic Properties 161

8.1 Finite Fields 161
8.2 Finite Fields as Splitting Fields 162
8.3 The Subfields of a Finite Field 163
8.4 The Multiplicative Structure of a Finite Field 163
8.5 The Galois Group of a Finite Field 165
8.6 Irreducible Polynomials over Finite Fields 165
*8.7 Normal Bases 169
*8.8 The Algebraic Closure of a Finite Field 170

Chapter 9

Finite Fields II: Additional Properties 175

9.1 Finite Field Arithmetic 175
*9.2 The Number of Irreducible Polynomials 178
*9.3 Polynomial Functions 180
*9.4 Linearized Polynomials 182

Part 3 The Theory of Binomials 187

Chapter 10

The Roots of Unity 189

10.1 Roots of Unity 189
10.2 Cyclotomic Extensions 191
***10.3 Normal Bases and Roots of Unity 198**
***10.4 Wedderburn's Theorem 200**
***10.5 Realizing Groups as Galois Groups 201**

Chapter 11

Cyclic Extensions 209

11.1 Cyclic Extensions 210
11.2 Extensions of Degree Char(F) 212

Chapter 12

Solvable Extensions 215

12.1 Solvable Groups 215
12.2 Solvable Extensions 216
12.3 Solvability by Radicals 219
12.4 Polynomial Equations 222

Chapter 13

Binomials 227

13.1 Irreducibility 228
13.2 The Galois Group of a Binomial 232
***13.3 The Independence of Irrational Numbers 241**

Chapter 14

Families of Binomials 247

14.1 The Splitting Field 247
***14.2 Kummer Theory 249**

Appendix

Möbius Inversion 257

References 265

Index of Symbols 267

Index 269