Contents

Preface v

1 **Historical Aspects of the Resolution of Algebraic Equations** 1

1.1 Approximating the Roots of an Equation 1

1.2 Construction of Solutions by Intersections of Curves 2

1.3 Relations with Trigonometry 2

1.4 Problems of Notation and Terminology 3

1.5 The Problem of Localization of the Roots 4

1.6 The Problem of the Existence of Roots 5

1.7 The Problem of Algebraic Solutions of Equations 6

Toward Chapter 2 7

2 **Resolution of Quadratic, Cubic, and Quartic Equations** 9

2.1 Second-Degree Equations 9

2.1.1 The Babylonians 9

2.1.2 The Greeks 11

2.1.3 The Arabs 11

2.1.4 Use of Negative Numbers 12

2.2 Cubic Equations 13

2.2.1 The Greeks 13

2.2.2 Omar Khayyam and Sharaf ad Din at Tusi 13

2.2.3 Scipio del Ferro, Tartaglia, Cardan 14

2.2.4 Algebraic Solution of the Cubic Equation 15

2.2.5 First Computations with Complex Numbers 16

2.2.6 Raffaele Bombelli 17

2.2.7 François Viète 18
2.3 Quartic Equations 18
Exercises for Chapter 2 19
Solutions to Some of the Exercises 22

3 Symmetric Polynomials **25**
3.1 Symmetric Polynomials 25
3.1.1 Background 25
3.1.2 Definitions 26
3.2 Elementary Symmetric Polynomials 27
3.2.1 Definition 27
3.2.2 The Product of the $X - X_i$; Relations Between Coefficients and Roots 27
3.3 Symmetric Polynomials and Elementary Symmetric Polynomials 29
3.3.1 Theorem 29
3.3.2 Proposition 31
3.3.3 Proposition 32
3.4 Newton's Formulas 32
3.5 Resultant of Two Polynomials 35
3.5.1 Definition 35
3.5.2 Proposition 35
3.6 Discriminant of a Polynomial 37
3.6.1 Definition 37
3.6.2 Proposition 37
3.6.3 Formulas 38
3.6.4 Polynomials with Real Coefficients: Real Roots and Sign of the Discriminant 38
Exercises for Chapter 3 39
Solutions to Some of the Exercises 44

4 Field Extensions **51**
4.1 Field Extensions 51
4.1.1 Definition 51
4.1.2 Proposition 52
4.1.3 The Degree of an Extension 52
4.1.4 Towers of Fields 52
4.2 The Tower Rule 53
4.2.1 Proposition 53
4.3 Generated Extensions 54
4.3.1 Proposition 54
4.3.2 Definition 55
4.3.3 Proposition 55
4.4 Algebraic Elements 55
4.4.1 Definition 55

4.4.2 Transcendental Numbers . . . 55
4.4.3 Minimal Polynomial of an Algebraic Element . . . 56
4.4.4 Definition . . . 56
4.4.5 Properties of the Minimal Polynomial . . . 57
4.4.6 Proving the Irreducibility of a Polynomial in $\mathbf{Z}[X]$. 57
4.5 Algebraic Extensions . . . 59
4.5.1 Extensions Generated by an Algebraic Element . . . 59
4.5.2 Properties of $K[a]$ . . . 59
4.5.3 Definition . . . 60
4.5.4 Extensions of Finite Degree . . . 60
4.5.5 Corollary: Towers of Algebraic Extensions . . . 61
4.6 Algebraic Extensions Generated by n Elements . . . 61
4.6.1 Notation . . . 61
4.6.2 Proposition . . . 61
4.6.3 Corollary . . . 62
4.7 Construction of an Extension by Adjoining a Root . . . 62
4.7.1 Definition . . . 62
4.7.2 Proposition . . . 62
4.7.3 Corollary . . . 63
4.7.4 Universal Property of $K[X]/(P)$ . . . 63
Toward Chapters 5 and 6 . . . 64
Exercises for Chapter 4 . . . 64
Solutions to Some of the Exercises . . . 69

5 Constructions with Straightedge and Compass 79
5.1 Constructible Points . . . 79
5.2 Examples of Classical Constructions . . . 80
5.2.1 Projection of a Point onto a Line . . . 80
5.2.2 Construction of an Orthonormal Basis from Two Points 80
5.2.3 Construction of a Line Parallel to a Given Line Passing Through a Point . . . 81
5.3 Lemma . . . 82
5.4 Coordinates of Points Constructible in One Step . . . 82
5.5 A Necessary Condition for Constructibility . . . 83
5.6 Two Problems More Than Two Thousand Years Old . . . 84
5.6.1 Duplication of the Cube . . . 85
5.6.2 Trisection of the Angle . . . 85
5.7 A Sufficient Condition for Constructibility . . . 85
Exercises for Chapter 5 . . . 87
Solutions to Some of the Exercises . . . 90

6 K-Homomorphisms 93
6.1 Conjugate Numbers . . . 93
6.2 K-Homomorphisms . . . 94
6.2.1 Definitions . . . 94

6.2.2 Properties 94
6.3 Algebraic Elements and K-Homomorphisms 95
6.3.1 Proposition 95
6.3.2 Example 96
6.4 Extensions of Embeddings into $\mathbb{C}$ 97
6.4.1 Definition 97
6.4.2 Proposition 97
6.4.3 Proposition 98
6.5 The Primitive Element Theorem 99
6.5.1 Theorem and Definition 99
6.5.2 Example 100
6.6 Linear Independence of K-Homomorphisms 101
6.6.1 Characters 101
6.6.2 Emil Artin's Theorem 101
6.6.3 Corollary: Dedekind's Theorem 102
Exercises for Chapter 6 102
Solutions to Some of the Exercises 103

7 Normal Extensions **107**
7.1 Splitting Fields 107
7.1.1 Definition 107
7.1.2 Splitting Field of a Cubic Polynomial 108
7.2 Normal Extensions 108
7.3 Normal Extensions and K-Homomorphisms 109
7.4 Splitting Fields and Normal Extensions 109
7.4.1 Proposition 109
7.4.2 Converse 110
7.5 Normal Extensions and Intermediate Extensions 110
7.6 Normal Closure 111
7.6.1 Definition 111
7.6.2 Proposition 111
7.6.3 Proposition 111
7.7 Splitting Fields: General Case 112
Toward Chapter 8 113
Exercises for Chapter 7 113
Solutions to Some of the Exercises 115

8 Galois Groups **119**
8.1 Galois Groups 119
8.1.1 The Galois Group of an Extension 119
8.1.2 The Order of the Galois Group of a Normal Extension of Finite Degree 120
8.1.3 The Galois Group of a Polynomial 120
8.1.4 The Galois Group as a Subgroup of a Permutation Group 120

8.1.5 A Short History of Groups 121
8.2 Fields of Invariants 122
8.2.1 Definition and Proposition 122
8.2.2 Emil Artin's Theorem 122
8.3 The Example of $\mathbf{Q}\left[\sqrt[3]{2}, j\right]$: First Part 124
8.4 Galois Groups and Intermediate Extensions 126
8.5 The Galois Correspondence 126
8.6 The Example of $\mathbf{Q}\left[\sqrt[3]{2}, j\right]$: Second Part 128
8.7 The Example $X^4 + 2$ 128
8.7.1 Dihedral Groups 128
8.7.2 The Special Case of D_4 129
8.7.3 The Galois Group of $X^4 + 2$ 130
8.7.4 The Galois Correspondence 130
8.7.5 Search for Minimal Polynomials 132
Toward Chapters 9, 10, and 12 133
Exercises for Chapter 8 133
Solutions to Some of the Exercises 139

9 Roots of Unity **149**
9.1 The Group $U(n)$ of Units of the Ring $\mathbb{Z}/n\mathbb{Z}$ 149
9.1.1 Definition and Background 149
9.1.2 The Structure of $U(n)$ 150
9.2 The Möbius Function 151
9.2.1 Multiplicative Functions 151
9.2.2 The Möbius Function 151
9.2.3 Proposition 151
9.2.4 The Möbius Inversion Formula 152
9.3 Roots of Unity 153
9.3.1 n-th Roots of Unity 153
9.3.2 Proposition 153
9.3.3 Primitive Roots 153
9.3.4 Properties of Primitive Roots 153
9.4 Cyclotomic Polynomials 153
9.4.1 Definition 153
9.4.2 Properties of the Cyclotomic Polynomial 153
9.5 The Galois Group over $\mathbf{Q}$ of an Extension of $\mathbf{Q}$ by a Root of Unity 156
Exercises for Chapter 9 157
Solutions to Some of the Exercises 163

10 Cyclic Extensions **179**
10.1 Cyclic and Abelian Extensions 179
10.2 Extensions by a Root and Cyclic Extensions 179
10.3 Irreducibility of $X^p - a$ 180
10.4 Hilbert's Theorem 90 181

10.4.1 The Norm 181
10.4.2 Hilbert's Theorem 90 182
10.5 Extensions by a Root and Cyclic Extensions: Converse . . . 182
10.6 Lagrange Resolvents 183
10.6.1 Definition 183
10.6.2 Properties 183
10.7 Resolution of the Cubic Equation 184
10.8 Solution of the Quartic Equation 186
10.9 Historical Commentary 188
Exercises for Chapter 10 188
Solutions to Some of the Exercises 190

11 Solvable Groups **195**
11.1 First Definition 195
11.2 Derived or Commutator Subgroup 196
11.3 Second Definition of Solvability 196
11.4 Examples of Solvable Groups 197
11.5 Third Definition 197
11.6 The Group A_n Is Simple for $n \geq 5$ 198
11.6.1 Theorem 198
11.6.2 A_n Is Not Solvable for $n \geq 5$, Direct Proof 199
11.7 Recent Results 199
Exercises for Chapter 11 200
Solutions to Some of the Exercises 203

12 Solvability of Equations by Radicals **207**
12.1 Radical Extensions and Polynomials Solvable by Radicals . 207
12.1.1 Radical Extensions 207
12.1.2 Polynomials Solvable by Radicals 208
12.1.3 First Construction 208
12.1.4 Second Construction 208
12.2 If a Polynomial Is Solvable by Radicals, Its Galois Group Is Solvable 209
12.3 Example of a Polynomial Not Solvable by Radicals 209
12.4 The Converse of the Fundamental Criterion 210
12.5 The General Equation of Degree n 210
12.5.1 Algebraically Independent Elements 210
12.5.2 Existence of Algebraically Independent Elements . . 211
12.5.3 The General Equation of Degree n 211
12.5.4 Galois Group of the General Equation of Degree n . 211
Exercises for Chapter 12 212
Solutions to Some of the Exercises 214

13 The Life of Évariste Galois **219**

14 Finite Fields **227**

14.1 Algebraically Closed Fields 227

14.1.1 Definition 227

14.1.2 Algebraic Closures 228

14.1.3 Theorem (Steinitz, 1910) 228

14.2 Examples of Finite Fields 229

14.3 The Characteristic of a Field 229

14.3.1 Definition 229

14.3.2 Properties 229

14.4 Properties of Finite Fields 230

14.4.1 Proposition 230

14.4.2 The Frobenius Homomorphism 231

14.5 Existence and Uniqueness of a Finite Field with p^r Elements 231

14.5.1 Proposition 231

14.5.2 Corollary 232

14.6 Extensions of Finite Fields 233

14.7 Normality of a Finite Extension of Finite Fields 233

14.8 The Galois Group of a Finite Extension of a Finite Field . . 233

14.8.1 Proposition 233

14.8.2 The Galois Correspondence 234

14.8.3 Example 234

Exercises for Chapter 14 235

Solutions to Some of the Exercises 243

15 Separable Extensions **257**

15.1 Separability 257

15.2 Example of an Inseparable Element 258

15.3 A Criterion for Separability 258

15.4 Perfect Fields 259

15.5 Perfect Fields and Separable Extensions 259

15.6 Galois Extensions 260

15.6.1 Definition 260

15.6.2 Proposition 260

15.6.3 The Galois Correspondence 260

Toward Chapter 16 260

16 Recent Developments **261**

16.1 The Inverse Problem of Galois Theory 261

16.1.1 The Problem 261

16.1.2 The Abelian Case 262

16.1.3 Example 262

16.2 Computation of Galois Groups over $\mathbb{Q}$ for Small-Degree Polynomials 262

16.2.1 Simplification of the Problem 263

16.2.2 The Irreducibility Problem 263

16.2.3 Embedding of G into S_n 263
16.2.4 Looking for G Among the Transitive Subgroups of S_n 264
16.2.5 Transitive Subgroups of S_4 264
16.2.6 Study of $\Phi(G) \subset A_n$ 265
16.2.7 Study of $\Phi(G) \subset D_4$ 266
16.2.8 Study of $\Phi(G) \subset \mathbb{Z}/4\mathbb{Z}$ 267
16.2.9 An Algorithm for $n = 4$ 268

Bibliography **271**

Index **277**