

Galois Theory

Fifth Edition

Ian Stewart
University of Warwick, UK



CRC Press

Taylor & Francis Group

Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
A CHAPMAN & HALL BOOK

Contents

Acknowledgements	xiii
Preface to the Fifth Edition	xv
Historical Introduction	xix
1 Classical Algebra	1
1.1 Complex Numbers	2
1.2 Subfields and Subrings of the Complex Numbers	3
1.3 Solving Equations	7
1.4 Solution by Radicals	8
2 The Fundamental Theorem of Algebra	19
2.1 Polynomials	19
2.2 Fundamental Theorem of Algebra	22
2.3 Implications	26
3 Factorisation of Polynomials	31
3.1 The Euclidean Algorithm	31
3.2 Irreducibility	36
3.3 Gauss’s Lemma	38
3.4 Eisenstein’s Criterion	40
3.5 Reduction Modulo p	42
3.6 Zeros of Polynomials	43
4 Field Extensions	49
4.1 Field Extensions	49
4.2 Rational Expressions	53
4.3 Simple Extensions	54

5	Simple Extensions	59
5.1	Algebraic and Transcendental Extensions	59
5.2	The Minimal Polynomial	60
5.3	Simple Algebraic Extensions	62
5.4	Classifying Simple Extensions	64
6	The Degree of an Extension	69
6.1	Definition of the Degree	69
6.2	The Tower Law	70
6.3	Primitive Element Theorem	74
7	Ruler-and-Compass Constructions	79
7.1	Approximate Constructions and More General Instruments	81
7.2	Constructions in $\mathbb{C}$	83
7.3	Specific Constructions	88
7.4	Impossibility Proofs	92
7.5	Construction from a Given Set of Points	94
8	The Idea behind Galois Theory	101
8.1	A First Look at Galois Theory	102
8.2	Galois Groups According to Galois	102
8.3	How to Use the Galois Group	105
8.4	The Abstract Setting	106
8.5	Polynomials and Extensions	107
8.6	The Galois Correspondence	109
8.7	Diet Galois	111
8.8	Natural Irrationalities	116
9	Normality and Separability	123
9.1	Splitting Fields	123
9.2	Normality	126
9.3	Separability	127
10	Counting Principles	131
10.1	Linear Independence of Monomorphisms	131

11 Field Automorphisms	139
11.1 K -Monomorphisms	139
11.2 Normal Closures	140
12 The Galois Correspondence	145
12.1 The Fundamental Theorem of Galois Theory	145
13 Worked Examples	149
13.1 Examples of Galois Groups	149
13.2 Discussion	158
14 Solubility and Simplicity	161
14.1 Soluble Groups	161
14.2 Simple Groups	164
14.3 Cauchy's Theorem	167
15 Solution by Radicals	171
15.1 Radical Extensions	171
15.2 An Insoluble Quintic	176
15.3 Other Methods	178
16 Abstract Rings and Fields	181
16.1 Rings and Fields	182
16.2 General Properties of Rings and Fields	184
16.3 Polynomials Over General Rings	186
16.4 The Characteristic of a Field	187
16.5 Integral Domains	189
17 Abstract Field Extensions and Galois Groups	195
17.1 Minimal Polynomials	195
17.2 Simple Algebraic Extensions	196
17.3 Splitting Fields	197
17.4 Normality	199
17.5 Separability	200
17.6 Galois Theory for Abstract Fields	204
17.7 Conjugates and Minimal Polynomials	205
17.8 The Primitive Element Theorem	208
17.9 Algebraic Closure of a Field	209

18 The General Polynomial Equation	215
18.1 Transcendence Degree	215
18.2 Elementary Symmetric Polynomials	218
18.3 The General Polynomial	220
18.4 Cyclic Extensions	221
18.5 Solving Equations of Degree Four or Less	225
18.6 Explicit Formulas	227
19 Finite Fields	233
19.1 Structure of Finite Fields	233
19.2 The Multiplicative Group	234
19.3 Counterexample to the Primitive Element Theorem	236
19.4 Application to Solitaire	237
20 Regular Polygons	241
20.1 What Euclid Knew	241
20.2 Which Constructions are Possible?	244
20.3 Regular Polygons	245
20.4 Fermat Numbers	249
20.5 How to Construct a Regular 17-gon	249
21 Circle Division	257
21.1 Genuine Radicals	258
21.2 Fifth Roots Revisited	260
21.3 Vandermonde Revisited	263
21.4 The General Case	265
21.5 Cyclotomic Polynomials	268
21.6 Galois Group of $\mathbb{Q}(\zeta)/\mathbb{Q}$	271
21.7 Constructions Using a Trisector	274
22 Calculating Galois Groups	283
22.1 Transitive Subgroups	283
22.2 Bare Hands on the Cubic	285
22.3 The Discriminant	287
22.4 General Algorithm for the Galois Group	288

23 Algebraically Closed Fields	293
23.1 Ordered Fields and Their Extensions	293
23.2 Sylow's Theorem	295
23.3 The Algebraic Proof	297
24 Transcendental Numbers	301
24.1 Irrationality	302
24.2 Transcendence of e	304
24.3 Transcendence of π	305
25 What Did Galois Do or Know?	311
25.1 List of the Relevant Material	312
25.2 The First Memoir	312
25.3 What Galois Proved	313
25.4 What is Galois up to?	315
25.5 Alternating Groups, Especially A_5	317
25.6 Simple Groups Known to Galois	318
25.7 Speculations about Proofs	319
25.8 A_5 is Unique	324
26 Further Directions	327
26.1 Inverse Galois Problem	327
26.2 Differential Galois Theory	329
26.3 p -adic Numbers	333
References	337
Index	345