

CONTENTS

<i>Preface</i>	vii
List of symbols used in the text	xi
1 Basics of constructive algebraic number theory	1
1.1 Introduction	1
1.2 The main task of constructive algebra	4
1.3 On the construction of overmodules and overrings	7
1.4 The ring of an equation	13
1.5 The Gaussian integer ring $\mathbb{Z}[i]$	15
1.6 Factorial monoids and divisor cascades	23
2 The group of an equation	29
2.1 Splitting rings	29
2.2 The fixed subring of the permutation automorphisms	37
2.3 Symmetric polynomials	48
2.4 Indecomposable splitting rings	63
2.5 Finite fields	69
2.6 The main theorem of Galois theory	87
2.7 Minimal splitting fields	91
2.8 The Lagrange resolvent	97
2.9 The group of an equation	108
2.10 How to determine the group of a separable equation over a field	135
2.11 The cyclotomic equation	157
2.12 Normal bases	163
3 Methods from the geometry of numbers	177
3.1 Introduction	177
3.2 Free modules over principal entire rings	177
3.3 Lattices and basis reduction	186
3.4 Minkowski's convex body theorem	212

4	Embedding of commutative orders into the maximal order	219
4.1	Introduction	219
4.2	The algebraic background	222
4.3	Valuation theory	230
4.4	Eisenstein polynomials	255
4.5	Dedekind rings and orders	264
4.6	Embedding algorithm	313
5	Units in algebraic number fields	327
5.1	Introduction	327
5.2	The Dirichlet theorem	329
5.3	On solving norm equations I	336
5.4	Computation of roots of unity	343
5.5	Computation of independent units	350
5.6	Regulator bounds and index estimates	359
5.7	Computation of fundamental units	367
5.8	Remarks on computerization	372
6	The class group of algebraic number fields	377
6.1	Introduction	377
6.2	The ring \mathcal{o}_F of algebraic integers as a Dedekind ring	381
6.3	Ideal calculus	396
6.4	On solving norm equations II	408
6.5	Computation of the class group	413
7	Recent developments	427
7.1	Introduction	427
7.2	Galois groups	428
7.3	Integral basis	429
7.4	Unit group and class group	429
7.5	Examples and applications	434
7.6	Relative extensions I: Kummer extensions	436
7.7	Relative extensions II: Hilbert class fields	443
7.8	Computation of subfields	445
7.9	KANT and the KANT shell KASH	450
7.10	Examples	453
	Appendix: Numerical tables	459
	Algorithms	487
	References	488
	Index	493