

## Contents

---

<i>Preface</i>	<i>page xi</i>
<i>Acknowledgments</i>	xii
<i>Summary</i>	xiii
 <b>PART ONE PRELIMINARIES</b>	
<b>1 Finite Étale Algebras over Fields</b>	<b>3</b>
1.1 Terminology for Rings and Algebras	3
1.2 Finite Field Extensions	4
1.3 Basic Facts on Finite Étale Algebras over Fields	6
1.4 Resultants and Discriminants of Polynomials	9
1.5 Characteristic Polynomial, Trace, Norm, Discriminant	11
1.6 Integral Elements and Orders	15
<b>2 Dedekind Domains</b>	<b>17</b>
2.1 Definitions	17
2.2 Ideal Theory of Dedekind Domains	18
2.3 Discrete Valuations	20
2.4 Localization	21
2.5 Integral Closure in Finite Field Extensions	21
2.6 Extensions of Discrete Valuations	22
2.7 Norms of Ideals	24
2.8 Discriminant and Different	25
2.9 Lattices over Dedekind Domains	27
2.10 Discriminants of Lattices of Étale Algebras	30
<b>3 Algebraic Number Fields</b>	<b>34</b>
3.1 Definitions and Basic Results	34
3.1.1 Absolute Norm of an Ideal	34

3.1.2	Discriminant, Class Number, Unit Group and Regulator	35
3.1.3	Explicit Estimates	36
3.2	Absolute Values: Generalities	37
3.3	Absolute Values and Places on Number Fields	39
3.4	$S$ -integers, $S$ -units and $S$ -norm	41
3.5	Heights and Houses	44
3.6	Estimates for Units and $S$ -units	48
3.7	Effective Computations in Number Fields and Étale Algebras	50
3.7.1	Algebraic Number Fields	52
3.7.2	Relative Extensions and Finite Étale Algebras	56
<b>4</b>	<b>Tools from the Theory of Unit Equations</b>	<b>58</b>
4.1	Effective Results over Number Fields	60
4.1.1	Equations in Units of Rings of Integers	60
4.1.2	Equations with Unknowns from a Finitely Generated Multiplicative Group	61
4.2	Effective Results over Finitely Generated Domains	64
4.3	Ineffective Results, Bounds for the Number of Solutions	66
 <b>PART TWO MONIC POLYNOMIALS AND INTEGRAL ELEMENTS OF GIVEN DISCRIMINANT, MONOGENIC ORDERS</b>		
<b>5</b>	<b>Basic Finiteness Theorems</b>	<b>73</b>
5.1	Basic Facts on Finitely Generated Domains	74
5.2	Discriminant Forms and Index Forms	76
5.3	Monogenic Orders, Power Bases, Indices	78
5.4	Finiteness Results	80
5.4.1	Discriminant Equations for Monic Polynomials	80
5.4.2	Discriminant Equations for Integral Elements in Étale Algebras	83
5.4.3	Discriminant Form and Index Form Equations	85
5.4.4	Consequences for Monogenic Orders	86
<b>6</b>	<b>Effective Results over <math>\mathbb{Z}</math></b>	<b>87</b>
6.1	Discriminant Form and Index Form Equations	89
6.2	Applications to Integers in a Number Field	92
6.3	Proofs	94
6.4	Algebraic Integers of Arbitrary Degree	104

*Contents*

vii

	6.5 Proofs	106
	6.6 Monic Polynomials of Given Discriminant	108
	6.7 Proofs	109
	6.8 Notes	113
	6.8.1 Some Related Results	113
	6.8.2 Generalizations over $\mathbb{Z}$	114
	6.8.3 Other Applications	114
<b>7</b>	<b>Algorithmic Resolution of Discriminant Form and Index Form Equations</b>	<b>117</b>
	7.1 Solving Discriminant Form and Index Form Equations via Unit Equations, A General Approach	118
	7.1.1 Quintic Number Fields	121
	7.1.2 Examples	133
	7.2 Solving Discriminant Form and Index Form Equations via Thue Equations	137
	7.2.1 Cubic Number Fields	138
	7.2.2 Quartic Number Fields	138
	7.2.3 Examples	142
	7.3 The Solvability of Index Equations in Various Special Number Fields	145
	7.4 Notes	146
<b>8</b>	<b>Effective Results over the <math>S</math>-integers of a Number Field</b>	<b>148</b>
	8.1 Results over $\mathbb{Z}_S$	149
	8.2 Monic Polynomials with $S$ -integral Coefficients	152
	8.3 Proofs	157
	8.4 Integral Elements over Rings of $S$ -integers	172
	8.4.1 Integral Elements in Étale Algebras	172
	8.4.2 Integral Elements in Number Fields	178
	8.4.3 Algebraic Integers of Given Degree	179
	8.5 Proofs	182
	8.6 Notes	191
	8.6.1 Historical Remarks	191
	8.6.2 Generalizations and Analogues	192
	8.6.3 The Existence of Relative Power Integral Bases	195
	8.6.4 Other Applications	195
<b>9</b>	<b>The Number of Solutions of Discriminant Equations</b>	<b>196</b>
	9.1 Results over $\mathbb{Z}$	197
	9.2 Results over the $S$ -integers of a Number Field	200

9.3	Proof of Theorem 9.2.1	202
9.4	Proof of Theorem 9.2.2	205
9.5	Three Times Monogenic Orders over Finitely Generated Domains	209
9.6	Notes	218
<b>10</b>	<b>Effective Results over Finitely Generated Domains</b>	<b>222</b>
10.1	Statements of the Results	223
10.1.1	Results for General Domains	224
10.1.2	A Special Class of Integral Domains	226
10.2	The Main Proposition	228
10.3	Rank Estimates for Unit Groups	229
10.4	Proofs of Theorems 10.1.1 and 10.1.2	231
10.5	Proofs of Theorem 10.1.3 and Corollary 10.1.4	236
10.6	Proofs of the Results from Subsection 10.1.2	239
10.7	Supplement: Effective Computations in Finitely Generated Domains	245
10.7.1	Finitely Generated Fields over $\mathbb{Q}$	245
10.7.2	Finitely Generated Domains over $\mathbb{Z}$	249
10.8	Notes	255
<b>11</b>	<b>Further Applications</b>	<b>257</b>
11.1	Number Systems and Power Integral Bases	257
11.1.1	Canonical Number Systems in Algebraic Number Fields	258
11.1.2	Proofs	259
11.1.3	Notes	266
11.2	The Number of Generators of an $O_S$ -order	268
11.2.1	Notes	271
<b>PART THREE BINARY FORMS OF GIVEN DISCRIMINANT</b>		
<b>12</b>	<b>A Brief Overview of the Basic Finiteness Theorems</b>	<b>275</b>
<b>13</b>	<b>Reduction Theory of Binary Forms</b>	<b>278</b>
13.1	Reduction of Binary Forms over $\mathbb{Z}$	279
13.2	Geometry of Numbers over the $S$ -integers	284
13.3	Estimates for Polynomials	290
13.4	Reduction of Binary Forms over the $S$ -integers	293
<b>14</b>	<b>Effective Results for Binary Forms of Given Discriminant</b>	<b>302</b>
14.1	Results over $\mathbb{Z}$	303

*Contents*

ix

14.2	Results over the $S$ -integers of a Number Field	305
14.3	Applications	307
14.4	Proofs of the Results from Section 14.2	311
14.5	Proofs of the Results from Section 14.3	323
14.6	Bounding the Degree of Binary Forms over $\mathbb{Z}$ of Given Discriminant	327
14.7	A Consequence for Monic Polynomials	330
14.8	Relation between Binary Forms of Given Discriminant and Unit Equations in Two Unknowns	332
14.9	Decomposable Forms of Given Semi-Discriminant	333
14.10	Notes	337
14.10.1	Applications to Classical Diophantine Equations	337
14.10.2	Other Applications	338
14.10.3	Practical Algorithms	338
<b>15</b>	<b>Semi-effective Results for Binary Forms of Given Discriminant</b>	<b>339</b>
15.1	Results	340
15.2	The Basic Proposition	342
15.3	Construction of the Tuple	343
15.4	Proof of the Basic Proposition	346
15.5	Notes	356
<b>16</b>	<b>Invariant Orders of Binary Forms</b>	<b>358</b>
16.1	Algebras Associated with a Binary Form	359
16.2	Definition of the Invariant Order	361
16.3	Binary Cubic Forms and Cubic Orders	369
<b>17</b>	<b>On the Number of Equivalence Classes of Binary Forms of Given Discriminant</b>	<b>371</b>
17.1	Results over $\mathbb{Z}$	372
17.2	Results over the $S$ -integers of a Number Field	374
17.3	$\Omega$ -forms	376
17.4	Local-to-Global Results	378
17.5	Lower Bounds	384
17.6	Counting Equivalence Classes over Discrete Valuation Domains	386
17.7	Counting Equivalence Classes over Number Fields	395
17.8	Proofs of the Theorems	401
17.9	Finiteness Results over Finitely Generated Domains	403
17.10	Notes	408

<b>18</b>	<b>Further Applications</b>	409
18.1	Root Separation of Polynomials	409
18.1.1	Results for Polynomials over $\mathbb{Z}$	410
18.1.2	Results over Number Fields	411
18.1.3	Proof of Theorem 18.1.5	413
18.1.4	Proof of Theorems 18.1.6 and 18.1.7	421
18.1.5	Notes	424
18.2	An Effective Proof of Shafarevich's Conjecture for Hyperelliptic Curves	425
18.2.1	Definitions	426
18.2.2	Results	427
18.2.3	Preliminaries	429
18.2.4	Proofs	430
18.2.5	Notes	435
	<i>Glossary of Frequently Used Notation</i>	436
	<i>References</i>	440
	<i>Index</i>	454