

Contents

1	Unique Factorisation in the Natural Numbers	1
1.1	The Natural Numbers	2
1.2	Euclid's Algorithm	3
1.3	The Fundamental Theorem of Arithmetic	8
1.4	The Gaussian Integers	9
1.5	Another Application of the Gaussian Integers	14
2	Number Fields	17
2.1	Algebraic Numbers	17
2.2	Minimal Polynomials	20
2.3	The Field of Algebraic Numbers	21
2.4	Number Fields	25
2.5	Integrality	28
2.6	The Ring of All Algebraic Integers	31
2.7	Rings of Integers of Number Fields	35
3	Fields, Discriminants and Integral Bases	39
3.1	Embeddings	40
3.2	Norms and Traces	44
3.3	The Discriminant	47
3.4	Integral Bases	51
3.5	Further Theory of the Discriminant	53
3.6	Rings of Integers in Some Cubic and Quartic Fields	57
3.6.1	$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$	57
3.6.2	$K = \mathbb{Q}(\sqrt{-2}, \sqrt{-5})$	59
3.6.3	$K = \mathbb{Q}(\sqrt[3]{2})$	60
3.6.4	$K = \mathbb{Q}(\sqrt[3]{175})$	61
4	Ideals	65
4.1	Uniqueness of Factorisation Revisited	66
4.2	Non-unique Factorisation in Quadratic Number Fields	67
4.3	Kummer's Ideal Numbers	71
4.4	Ideals	73
4.5	Generating Sets for Ideals	76

4.6	Ideals in Quadratic Fields	79
4.7	Unique Factorisation Domains and Principal Ideal Domains	81
4.8	The Noetherian Property	84
5	Prime Ideals and Unique Factorisation	87
5.1	Some Ring Theory	87
5.2	Maximal Ideals	94
5.3	Prime Ideals.	96
5.4	Unique Factorisation into Prime Ideals	99
5.5	Coprimality	102
5.6	Norms of Ideals	104
5.7	The Class Group	105
5.8	Splitting of Primes	107
5.9	Primes in Quadratic Fields.	112
6	Imaginary Quadratic Fields	113
6.1	Units.	113
6.1.1	$d \equiv 2, 3 \pmod{4}$	114
6.1.2	$d \equiv 1 \pmod{4}$	114
6.1.3	Summary.	115
6.2	Euclidean Imaginary Quadratic Fields.	116
6.2.1	$d \equiv 2, 3 \pmod{4}$	116
6.2.2	$d \equiv 1 \pmod{4}$	117
6.3	Quadratic Forms.	120
6.4	Reduction Theory.	123
6.5	Class Numbers and Quadratic Forms	131
6.5.1	$d \equiv 2, 3 \pmod{4}$	134
6.5.2	$d \equiv 1 \pmod{4}$	142
6.6	Counting Quadratic Forms.	143
7	Lattices and Geometrical Methods	149
7.1	Lattices	149
7.2	Geometry of Number Fields.	153
7.3	Finiteness of the Class Number	158
7.4	Dirichlet's Unit Theorem.	164
8	Other Fields of Small Degree	169
8.1	Continued Fractions	170
8.2	Continued Fractions of Square Roots	176
8.3	Real Quadratic Fields	180
8.4	Biquadratic Fields.	184
8.5	Cubic Fields	188

9 Cyclotomic Fields and the Fermat Equation 191

9.1 Definitions 191

9.2 Discriminants and Integral Bases 195

9.3 Gauss Sums and Quadratic Reciprocity 198

9.4 Remarks on Fermat’s Last Theorem 202

10 Analytic Methods 207

10.1 The Riemann Zeta Function 207

10.2 The Functional Equation of the Riemann Zeta Function 211

10.3 Zeta Functions of Number Fields 214

10.4 The Analytic Class Number Formula 215

10.5 Explicit Class Number Formulae 223

10.6 Other Embeddings 226

11 The Number Field Sieve 231

11.1 The RSA Cryptosystem and the Problem of Factorisation 231

11.2 The Quadratic Sieve 233

11.3 The Number Field Sieve: A First Example 237

11.4 Index Calculus 238

11.5 Prime Ideals and the Algebraic Factorbase 241

11.6 Further Obstructions 244

11.7 The General Case 248

11.8 Closing Comments 253

Appendix A: Solutions and Hints to Exercises 257

Index 289



<http://www.springer.com/978-3-319-07544-0>

Algebraic Number Theory

Jarvis, F.

2014, XIII, 292 p. 3 illus., Softcover

ISBN: 978-3-319-07544-0