




Contents

Preface	ix
Suggested Course Outlines.....	xiii
1 Algebraic Numbers	1
1.1 Origins and Foundations	1
1.2 Algebraic Numbers and Number Fields	13
1.3 Discriminants, Norms, and Traces	25
1.4 Algebraic Integers and Integral Bases	32
1.5 Factorization and Divisibility	48
1.6 Applications of Unique Factorization	53
1.7  Applications: Factoring in \mathbb{Z} Using Cubic Integers . . .	67
2 Arithmetic of Number Fields	73
2.1 Quadratic Fields	73
2.2 Cyclotomic Fields	81
2.3 Units in Number Rings	89
2.4 Geometry of Numbers	93
2.5 Dirichlet's Unit Theorem	108
2.6  Application: The Number Field Sieve	117
3 Ideal Theory	127
3.1 Properties of Ideals	127
3.2 PIDs and UFDs	142
3.3 Norms of Ideals	148
3.4 Ideal Classes — The Class Group	153
3.5 Class Numbers of Quadratic Fields	159
3.6 Cyclotomic Fields and Kummer's Theorem — Bernoulli Numbers and Irregular Primes	170
3.7  Cryptography in Quadratic Fields	183
4 Ideal Decomposition in Extension Fields	193
4.1 Inertia, Ramification, and Splitting	193
4.2 The Different and Discriminant	209

4.3	Galois Theory and Decomposition	232
4.4	The Kronecker-Weber Theorem	256
4.5	☞ An Application—Primality Testing	264
5	Reciprocity Laws	273
5.1	Cubic Reciprocity	273
5.2	The Biquadratic Reciprocity Law	289
5.3	The Stickelberger Relation	306
5.4	The Eisenstein Reciprocity Law	325
5.5	☞ Elliptic Curves, Factoring, and Primality	333
	Appendix A: Abstract Algebra	352
	Appendix B: Sequences and Series	383
	Appendix C: Galois Theory	393
	Appendix D: The Greek Alphabet	402
	Appendix E: Latin Phrases	403
	Solutions to Odd-Numbered Exercises	405
	Bibliography	459
	List of Symbols	464
	Index	466
	About the Author	483