

Contents

Preface.....	ix
About the Author.....	xiii
Suggested Course Outlines.....	xv
1 Integral Domains, Ideals, and Unique Factorization	1
1.1 Integral Domains	1
1.2 Factorization Domains	7
1.3 Ideals	15
1.4 Noetherian and Principal Ideal Domains	20
1.5 Dedekind Domains	25
1.6 Algebraic Numbers and Number Fields	35
1.7 Quadratic Fields	44
2 Field Extensions	55
2.1 Automorphisms, Fixed Points, and Galois Groups	55
2.2 Norms and Traces	65
2.3 Integral Bases and Discriminants	70
2.4 Norms of Ideals	83
3 Class Groups	87
3.1 Binary Quadratic Forms	87
3.2 Forms and Ideals	96
3.3 Geometry of Numbers and the Ideal Class Group	108
3.4 Units in Number Rings	122
3.5 Dirichlet's Unit Theorem	130
4 Applications: Equations and Sieves	139
4.1 Prime Power Representation	139
4.2 Bachet's Equation	145
4.3 The Fermat Equation	149
4.4 Factoring	165
4.5 The Number Field Sieve	174
5 Ideal Decomposition in Number Fields	181
5.1 Inertia, Ramification, and Splitting of Prime Ideals	181
5.2 The Different and Discriminant	196
5.3 Ramification	213
5.4 Galois Theory and Decomposition	221

5.5	Kummer Extensions and Class-Field Theory	233
5.6	The Kronecker-Weber Theorem	244
5.7	An Application—Primality Testing	255
6	Reciprocity Laws	261
6.1	Cubic Reciprocity	261
6.2	The Biquadratic Reciprocity Law	278
6.3	The Stickelberger Relation	294
6.4	The Eisenstein Reciprocity Law	311
	Appendix A: Abstract Algebra	319
	Appendix B: Sequences and Series	345
	Appendix C: The Greek Alphabet	355
	Appendix D: Latin Phrases	357
	Bibliography	359
	Solutions to Odd-Numbered Exercises	365
	Index	407