CONTENTS

CHAPTER

I. Divisibility
1. Uniqueness of factorization 1
2. A general problem 5
3. The Gaussian integers 7
Problems 11

II. The Gaussian Primes
1. Rational and Gaussian primes 14
2. Congruences 14
3. Determination of the Gaussian primes 18
4. Fermat's theorem for Gaussian primes 21
Problems 23

III. Polynomials over a field
1. The ring of polynomials 25
2. The Eisenstein irreducibility criterion 30
3. Symmetric polynomials 35
Problems 40

IV. Algebraic Number Fields
1. Numbers algebraic over a field 44
2. Extensions of a field 46
3. Algebraic and transcendental numbers 51
Problems 56

V. Bases
1. Bases and finite extensions 59
2. Properties of finite extensions 62
3. Conjugates and discriminants 64
4. The cyclotomic field 68
Problems 70

VI. Algebraic Integers and Integral Bases
1. Algebraic integers 74
2. The integers in a quadratic field 77
3. Integral bases 79
4. Examples of integral bases 82
Problems 86

CHAPTER

VII. Arithmetic in Algebraic Number Fields
1. Units and primes 88
2. Units in a quadratic field 90
3. The uniqueness of factorization 93
4. Ideals in an algebraic number field 95
Problems 98

VIII. The Fundamental Theorem of Ideal Theory
1. Basic properties of ideals 102
2. The classical proof of the unique factorization theorem 107
3. The modern proof 112
Problems 116

IX. Consequences of the Fundamental Theorem
1. The highest common factor of two ideals 120
2. Unique factorization of integers 123
3. The problem of ramification 125
4. Congruences and norms 128
5. Further properties of norms 132
Problems 135

X. Ideal Classes and Class Numbers
1. Ideal classes 139
2. Class numbers 140
Problems 144

XI. The Fermat Conjecture
1. Pythagorean triples 146
2. The Fermat conjecture 147
3. Units in cyclotomic fields 150
4. Kummer's theorem 155
Problems 158

References 159
List of Symbols 160
Index 161