Contents

Preface xi
Acknowledgments xiv

1 Euclidean Arithmetic 1
1.1 Divisors and Primes 2
1.2 The Form of the gcd 5
1.3 The Prime Divisor Property 8
1.4 Irrational Numbers 10
1.5 The Equation $x^2 - 2y^2 = 1$ 13
1.6 Rings 15
1.7 Fields 19
1.8 Factors of Polynomials 22
1.9 Discussion 24

2 Diophantine Arithmetic 33
2.1 Rational versus Integer Solutions 34
2.2 Fermat’s Last Theorem for Fourth Powers 36
2.3 Sums of Two Squares 38
2.4 Gaussian Integers and Primes 41
2.5 Unique Gaussian Prime Factorization 43
2.6 Factorization of Sums of Two Squares 45
2.7 Gaussian Primes 47
2.8 Primes that Are Sums of Two Squares 48
2.9 The Equation $y^3 = x^2 + 2$ 50
2.10 Discussion 53

3 Quadratic Forms 59
3.1 Primes of the Form $x^2 + ky^2$ 60
3.2 Quadratic Integers and Quadratic Forms 61
3.3 Quadratic Forms and Equivalence 63
## Contents

3.4 Composition of Forms
3.5 Finite Abelian Groups
3.6 The Chinese Remainder Theorem
3.7 Additive Notation for Abelian Groups
3.8 Discussion

4 Rings and Fields
4.1 Integers and Fractions
4.2 Domains and Fields of Fractions
4.3 Polynomial Rings
4.4 Algebraic Number Fields
4.5 Field Extensions
4.6 The Integers of an Algebraic Number Field
4.7 An Equivalent Definition of Algebraic Integer
4.8 Discussion

5 Ideals
5.1 “Ideal Numbers”
5.2 Ideals
5.3 Quotients and Homomorphisms
5.4 Noetherian Rings
5.5 Noether and the Ascending Chain Condition
5.6 Countable Sets
5.7 Discussion

6 Vector Spaces
6.1 Vector Space Basis and Dimension
6.2 Finite-Dimensional Vector Spaces
6.3 Linear Maps
6.4 Algebraic Numbers as Matrices
6.5 The Theorem of the Primitive Element
6.6 Algebraic Number Fields and Embeddings in \( \mathbb{C} \)
6.7 Discussion

7 Determinant Theory
7.1 Axioms for the Determinant
7.2 Existence of the Determinant Function
7.3 Determinants and Linear Equations
7.4 Basis Independence
7.5 Trace and Norm of an Algebraic Number
7.6 Discriminant
7.7 Discussion
## Contents

8 **Modules**  
8.1 From Vector Spaces to Modules 171  
8.2 Algebraic Number Fields and Their Integers 174  
8.3 Integral Bases 176  
8.4 Bases and Free Modules 179  
8.5 Integers over a Ring 182  
8.6 Integral Closure 184  
8.7 Discussion 186  

9 **Ideals and Prime Factorization**  
9.1 To Divide Is to Contain 189  
9.2 Prime Ideals 190  
9.3 Products of Ideals 192  
9.4 Prime Ideals in Algebraic Number Rings 194  
9.5 Fractional Ideals 196  
9.6 Prime Ideal Factorization 197  
9.7 Invertibility and the Dedekind Property 199  
9.8 Discussion 201  

**References** 211  
**Index** 217