

# An Introduction to Algebraic Number Theory

**Takashi Ono**

*The Johns Hopkins University  
Baltimore, Maryland*

Plenum Press • New York and London

# Contents

|  |           |
|--|-----------|
| <b>Notation and Conventions</b> . . . . .                            | <b>xi</b> |
| <b>1. To the Gauss Reciprocity Law</b> . . . . .                     | <b>1</b>  |
| 1.1. Basic Facts . . . . .   | 2         |
| 1.2. Modules in $\mathbb{Z}$ . . . . .                               | 4         |
| 1.3. Euclidean Algorithm and Continued Fractions . . . . .           | 8         |
| 1.4. Continued-Fraction Expansion of Irrational<br>Numbers . . . . . | 12        |
| 1.5. Concept of Groups . . . . .                                     | 16        |
| 1.6. Subgroups and Quotient Groups . . . . .                         | 21        |
| 1.7. Ideals and Quotient Rings . . . . .                             | 23        |
| 1.8. Isomorphisms and Homomorphisms . . . . .                        | 25        |
| 1.9. Polynomial Rings . . . . .                                      | 28        |
| 1.10. Primitive Roots . . . . .                                      | 30        |
| 1.11. Algebraic Integers . . . . .                                   | 34        |
| 1.12. Characters of Abelian Groups . . . . .                         | 37        |
| 1.13. The Gauss Reciprocity Law . . . . .                            | 41        |
| <b>2. Basic Concepts of Algebraic Number Fields</b> . . . . .        | <b>44</b> |
| 2.1. Field Extensions . . . . .                                      | 44        |
| 2.2. Galois Theory . . . . .   | 48        |
| 2.3. Norm, Trace, and Discriminant . . . . .                         | 53        |
| 2.4. Gauss Sum and Jacobi Sum . . . . .                              | 55        |

|           |   |            |
|-----------|---|------------|
| 2.5.      | Construction of a Regular $l$ -gon . . . . .                                | 58         |
| 2.6.      | Subfields of the $l$ th Cyclotomic Field . . . . .                          | 60         |
| 2.7.      | Cohomology of Cyclic Groups . . . . .                                       | 63         |
| 2.8.      | Finite Fields . . . . .   | 68         |
| 2.9.      | Ring of Integers, Ideals, and Discriminant . . . . .                        | 69         |
| 2.10.     | Fundamental Theorem of Ideal Theory . . . . .                               | 74         |
| 2.11.     | Residue Class Rings . . . . .   | 78         |
| 2.12.     | Decomposition of Primes in Number Fields . . . . .                          | 81         |
| 2.13.     | Discriminant and Ramification . . . . .                                     | 86         |
| 2.14.     | Hilbert Theory . . . . .  | 89         |
| 2.15.     | Artin Map . . . . .   | 93         |
| 2.16.     | Artin Maps of Subfields of the $l$ th Cyclotomic Field . . . . .            | 97         |
| 2.17.     | The Artin Map in Quadratic Fields . . . . .                                 | 100        |
| <b>3.</b> | <b>Analytic Methods . . . . .</b>   | <b>105</b> |
| 3.1       | Lattices in $\mathbb{R}^n$ . . . . .  | 105        |
| 3.2.      | Minkowski's Theorem . . . . .   | 109        |
| 3.3.      | Dirichlet's Unit Theorem . . . . .  | 113        |
| 3.4.      | Pre-Zeta Functions . . . . .  | 119        |
| 3.5.      | Dedekind Zeta Function . . . . .  | 123        |
| 3.6.      | The $m$ th Cyclotomic Field . . . . .                                       | 132        |
| 3.7.      | Dirichlet $L$ -Functions . . . . .  | 134        |
| 3.8.      | Dirichlet's Theorem on Arithmetical Progressions . . . . .                  | 140        |
| <b>4.</b> | <b>The <math>l</math>th Cyclotomic Field and Quadratic Fields . . . . .</b> | <b>143</b> |
| 4.1.      | Determination of Gauss Sums . . . . .                                       | 144        |
| 4.2.      | $L$ -Functions and Gauss Sums . . . . .                                     | 149        |
| 4.3.      | Class Numbers of Subfields of the $l$ th Cyclotomic<br>Field . . . . .      | 152        |
| 4.4.      | Class Number of $\mathbb{Q}(\sqrt{l^*})$ . . . . .                          | 155        |
| 4.5.      | Ideal Class Groups of Quadratic Fields . . . . .                            | 159        |
| 4.6.      | Cohomology of Quadratic Fields . . . . .                                    | 166        |
| 4.7.      | Gauss Genus Theory . . . . .  | 173        |
| 4.8.      | Quadratic Irrationals . . . . .   | 179        |
| 4.9.      | Real Quadratic Fields and Continued Fractions . . . . .                     | 186        |

|   |            |
|---|------------|
| <b>Answers and Hints to Exercises</b> . . . . .   | <b>195</b> |
| <b>Notes</b> . . . . .                            | <b>210</b> |
| A. Peano Axioms . . . . .                         | 210        |
| B. Fundamental Theorem of Algebra . . . . .       | 211        |
| C. Zorn's Lemma . . . . .                         | 212        |
| D. Quadratic Fields and Quadratic Forms . . . . . | 212        |
| <b>List of Mathematicians.</b> . . . . .          | <b>215</b> |
| <b>Bibliography</b> . . . . .                     | <b>216</b> |
| Comments on the Bibliography . . . . .            | 220        |
| <b>Index</b> . . . . .                            | <b>221</b> |