Number Theory

K

June 22, 2022

Contents

Part I

Field Theory

Chapter 1

Overview

1.1 Definitions and Theorems

1.2 Proofs, Remarks, and Examples

Theorem 1. Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of factors.
In other words, if $n \in \mathbb{Z}$, then there are prime numbers $p_1, \ldots, p_k \in \mathbb{Z}$ and positive integers $r_1, \ldots, r_k \in \mathbb{N}^+$ such that

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

is unique, up to the order of factors.

Remark. This theorem is also called the unique factorization theorem and prime factorization theorem.

Definition 2. A field extension is a pair of fields $E \subset F$, such that the operations of E are those of F restricted to E. In this case, F is an extension field of E and E is a subfield of F. Such a field extension is denoted F/E (read as "F over E").

Definition 3. Let F/E be a field extension and $\alpha \in F$. We say α is algebraic over E if α is a root of a non-zero polynomial with coefficients in E. Moreover, if all elements of the extension field is algebraic, we say algebraic extension.

Definition 4. A number field is an an algebraic extension of $\mathbb{Q}$ of finite degree.

Definition 5. Let K be a number field. An algebraic integer α in K is a root of a monic polynomial with integer coefficients, i.e.

$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0, \tag{1.1}$$

with $c_0, \ldots, c_{n-1} \in \mathbb{Z}$.
The ring of integers of a number field K, denoted by $\mathcal{O}_K$, is the ring of all algebraic integers.

Example 5.1. Let $K = \mathbb{Q}(\sqrt{5})$. What is $\mathcal{O}_K$? Generalize this to $\sqrt{d}$.

Definition 6. Let A be a ring. A non-unit element $a \in A$ is irreducible if $a = xy$ implies that x or y is a unit in A.

Theorem 7. Let K be a number field and $\mathcal{O}_K$ its ring of integers. Then, for any $x \in \mathcal{O}_K$ we have

$$x = y_1^{r_1} \cdot \ldots \cdot y_k^{r_k}$$

where $y_1, \ldots, y_k$ are irreducible.

Definition 8. Let A be a ring. Then, an ideal factor $\mathfrak{a} \subset A$ is a subset of A with (some properties) but its just an ideal.

Theorem 9. Let $\mathcal{O}_K$ be the ring of integers and let $\mathfrak{a}$ an ideal, then

$$\mathfrak{a} = \mathfrak{p}_1^{r_1} \cdot \ldots \cdot \mathfrak{p}_k^{r_k}$$

where $\mathfrak{p}_i$ are prime ideals and this decomposition is basically unique.

1.3 Exercises and Notes

Part II

Ring Theory

Part III

Number Theory

Chapter 2

Ring of Integers

2.1 Definitions and Theorems

2.2 Proofs, Remarks, and Examples

Definition 10. Let $K/\mathbb{Q}$ be a number field.

1. An algebraic integer α in K is a root of a monic polynomial with integer coefficients, i.e.
$$\alpha^n + c_{n-1}\alpha^{n-1} + \cdots + c_0 = 0, \tag{2.1}$$
with $c_0, \dots, c_{n-1} \in \mathbb{Z}$.

2. The ring of integers of a number field K, denoted by $\mathcal{O}_K$, is the ring of all algebraic integers of K.

Proof. We show $\mathcal{O}_K$ is indeed a ring. Fix an α and β in $\mathcal{O}_K$, then there are monic polynomials $p, q \in \mathbb{Z}[X]$, such that $p(\alpha) = 0$ and $q(\beta) = 0$.

1.

$\square$

Corollary 1. Let K be a number field and $\mathcal{O}_K$ its ring of integers. The fraction field of $\mathcal{O}_K$ is the number field K.

2.3 Exercises and Notes

Chapter 3

Ring of Integers

3.1 Definitions and Theorems

3.2 Proofs, Remarks, and Examples

3.3 Exercises and Notes