§ 3. Ideals

1. Dedekind Domains

Theorem 3.1 (Properties of $\mathfrak{o}_K$). The ring of integers $\mathfrak{o}_K$ in a number field K is Noetherian, integrally closed, and every non-zero prime ideal is maximal.

Definition 3.2. An integral domain $\mathfrak{o}$ is called a **Dedekind domain** if it satisfies the following conditions:

1. It is **Noetherian**.
2. It is **integrally closed**.
3. Every non-zero prime ideal is **maximal**.

2. Factorization of Integral Ideals

Lemma 3.4. For every ideal $\mathfrak{a} \neq 0$ of a Dedekind domain $\mathfrak{o}$, there exist non-zero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ such that:

$$\mathfrak{a} \supseteq \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r.$$

Definition (Inverse of a Prime). Let $\mathfrak{p}$ be a prime ideal. Define the set:

$$\mathfrak{p}^{-1} = \{x \in K \mid x\mathfrak{p} \subseteq \mathfrak{o}\}.$$

Lemma 3.5. Let $\mathfrak{p}$ be a prime ideal of $\mathfrak{o}$. For every ideal $\mathfrak{a} \neq 0$:

$$\mathfrak{a}\mathfrak{p}^{-1} := \left\{ \sum a_i x_i \mid a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1} \right\} \neq \mathfrak{a}.$$

Specifically, $\mathfrak{o} \subsetneq \mathfrak{p}^{-1}$ and $\mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{o}$.

Theorem 3.3 (Unique Prime Factorization). Every ideal $\mathfrak{a}$ of $\mathfrak{o}$ different from (0) and (1) admits a factorization

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$$

into non-zero prime ideals $\mathfrak{p}_i$ of $\mathfrak{o}$, which is **unique** up to the order of the factors.

3. Fractional Ideals and the Ideal Group

Definition 3.7. A **fractional ideal** of K is a finitely generated $\mathfrak{o}$-submodule $\mathfrak{a} \neq 0$ of K.

Equivalent Definition: An $\mathfrak{o}$-submodule $\mathfrak{a} \subset K$ ($\mathfrak{a} \neq 0$) is a fractional ideal if and only if there exists a non-zero element $c \in \mathfrak{o}$ such that $c\mathfrak{a} \subseteq \mathfrak{o}$ (i.e., $c\mathfrak{a}$ is an integral ideal).

Proposition 3.8 (Ideal Group). The fractional ideals form an abelian group J_K, called the **ideal group** of K.

- **Identity:** $(1) = \mathfrak{o}$.
- **Inverse:** The inverse of $\mathfrak{a}$ is:

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{o}\}.$$

Corollary 3.9. Every fractional ideal $\mathfrak{a}$ admits a unique representation as a product:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}}$$

with $\nu_{\mathfrak{p}} \in \mathbb{Z}$ and $\nu_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$. Thus, J_K is the **free abelian group** on the set of non-zero prime ideals $\mathfrak{p}$ of $\mathfrak{o}$.

4. The Class Group

Principal Fractional Ideals (P_K). The fractional ideals of the form $(a) = a\mathfrak{o}$ for $a \in K^*$ form a subgroup of J_K denoted by P_K.

Ideal Class Group (Cl_K). The quotient group:

$$Cl_K = J_K / P_K$$

is called the **ideal class group** of K.

Fundamental Exact Sequence: The relation between numbers and ideals is captured by the exact sequence:

$$1 \longrightarrow \mathfrak{o}^* \hookrightarrow K^* \xrightarrow{a \mapsto (a)} J_K \xrightarrow{proj} Cl_K \longrightarrow 1$$