8. Unique Factorisation of Ideals

8.1. **Finiteness of Quotient Rings.** We will look at the norm of an ideal I in $\mathcal{O}_K$. There are several descriptions of this notion. We will use the first description as the definition and prove the other descriptions are all equivalent to this one.

Definition 8.1. Let K be a number field and $\mathcal{O}_K$ its ring of integers. The *norm* of any non-zero ideal I of $\mathcal{O}_K$ is defined by

$$N(I) = \left|\frac{\Delta(I)}{\Delta_K}\right|^{\frac{1}{2}}.$$

Remark 8.2. It is worth pointing out the following things about this notion.

(1) This definition is not to be confused with the norm of an element α in the number field K; see Definition 6.14. Although they share the same terminology and notation, whether the argument is an element of an ideal should tell us which definition is in use. On the other hand, the two notions do have very close relation. We will explain that in Proposition 8.9.

(2) By Remark 7.13, we know that both $\Delta(I)$ and Δ_K are non-zero, hence the norm of the ideal I is always well-defined and a positive number. We will show that it is in fact always a positive integer; see Proposition 8.3.

Proposition 8.3. *Suppose $\omega_1, \omega_2, \cdots, \omega_n$ is an integral basis for $\mathcal{O}_K$ and $\alpha_1, \alpha_2, \cdots, \alpha_n$ is an integral basis for I. For each j, suppose $\alpha_j = \sum_{i=1}^{n} a_{ij}\omega_i$ and $M = (a_{ij})$ is the transition matrix. Then $N(I) = |\det(M)|$. In particular, $N(I)$ is a positive integer.*

Proof. Using Proposition 7.6, we have $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = (\det(M))^2\Delta(\omega_1, \omega_2, \cdots, \omega_n)$. By Definition 7.12, this is equivalent to $\Delta(I) = (\det(M))^2\Delta_K$. By Remark 7.13, $\Delta(I) \neq 0$ and $\Delta_K \neq 0$, hence we get $|\det(M)| = \left|\frac{\Delta(I)}{\Delta_K}\right|^{\frac{1}{2}} = N(I)$. Since $\omega_1, \omega_2, \cdots, \omega_n$ is an integral basis for $\mathcal{O}_K$ and each $\alpha_j \in \mathcal{O}_K$, we know that the coefficients $a_{ij} \in \mathbb{Z}$. Therefore $\det(M)$ is an integer. Since $N(I) \neq 0$, we conclude $N(I) = |\det(M)|$ is a positive integer. □

We give the third description of the norm of the ideal I. It also reveals a special property of the ring $\mathcal{O}_K$, namely, the finiteness of quotient rings.

Proposition 8.4. *For any non-zero ideal I of $\mathcal{O}_K$, the quotient ring $\mathcal{O}_K/I$ is finite and has order $N(I)$.*

Proof. (This proof is not covered in lectures and is non-examinable.) Since I is an ideal in $\mathcal{O}_K$, by forgetting the multiplication on them we know I is a subgroup of $\mathcal{O}_K$. By Proposition 7.9, $\mathcal{O}_K$ and I are both free abelian groups of rank n. By the structure

theorem of finitely generated free abelian groups in group theory, we can find an integral basis $\omega_1, \omega_2, \cdots, \omega_n$ for $\mathcal{O}_K$, such that $d_1\omega_1, d_2\omega_2, \cdots, d_n\omega_n$ is an integral basis for I, where each d_i is a positive integer. We write $d = d_1 d_2 \cdots d_n$.

We now show that the quotient ring $\mathcal{O}_K/I$ is finite of order d. In other words, there are precisely d cosets of I in $\mathcal{O}_K$. For this purpose, we will show that

$$S = \{\lambda_1\omega_1 + \lambda_2\omega_2 + \cdots + \lambda_n\omega_n \mid 0 \leqslant \lambda_i < d_i \text{ for } i = 1, 2, \cdots, n\}$$

is a complete set of representatives for cosets of I in $\mathcal{O}_K$. On one hand, for each $\beta \in \mathcal{O}_K$, let $\beta = a_1\omega_1 + a_2\omega_2 + \cdots + a_n\omega_n$ for some $a_1, a_2, \cdots, a_n \in \mathbb{Z}$. For each i, we can write $a_i = q_i d_i + r_i$ for some $0 \leqslant r_i < d_i$. Let $\gamma = r_1\omega_1 + r_2\omega_2 + \cdots r_n\omega_n$, then $\beta - \gamma = q_1 d_1\omega_1 + q_2 d_2\omega_2 + \cdots + q_n d_n\omega_n \in I$. Since $\gamma \in S$, this shows every coset is represented by some element in S. On the other hand, we need to show that elements in S represent distinct cosets. Assume $\lambda = \lambda_1\omega_1 + \lambda_2\omega_2 + \cdots + \lambda_n\omega_n \in S$ and $\delta = \delta_1\omega_1 + \delta_2\omega_2 + \cdots + \delta_n\omega_n \in S$ are in the same coset, then $\lambda - \delta \in I$, which implies $d_i \mid \lambda_i - \delta_i$ for each i. However we also have $-d_i < \lambda_i - \delta_i < d_i$, hence $\lambda_i - \delta_i = 0$ for each i, which implies $\lambda = \delta$. This concludes S is a complete set of representatives for all cosets of I in $\mathcal{O}_K$, hence $\mathcal{O}_K/I$ is finite of order $d = d_1 d_2 \cdots d_n$.

It remains to show that $d = N(I)$. We apply Proposition 8.3 for the particular bases we chose at the beginning of the proof. Under these bases the matrix M is diagonal with diagonal entries $d_1, d_2, \cdots, d_n$ which are positive integers, hence $N(I) = |\det(M)| = d_1 d_2 \cdots d_n = d$. It follows that the order of $\mathcal{O}_K/I$ is $N(I)$. □

The following is an interesting consequence. $N(I) \in \mathbb{Z}$ implies $N(I) \in \mathcal{O}_K$. In fact, we have

Corollary 8.5. *For any non-zero ideal I in $\mathcal{O}_K$, $N(I) \in I$.*

Proof. Since $1 \in \mathcal{O}_K$, we consider the coset $1 + I$. By Proposition 8.4, the sum of $N(I)$ copies of $1 + I$ is the zero element in $\mathcal{O}_K/I$; i.e. the coset $N(I) + I$ is $0 + I$. It follows $N(I) \in I$. □

Corollary 8.6. *For any non-zero ideal I in $\mathcal{O}_K$, $N(I) = 1$ iff $I = \mathcal{O}_K$.*

Proof. Both conditions $N(I) = 1$ and $I = \mathcal{O}_K$ are equivalent to the condition that there is only one coset of I in $\mathcal{O}_K$, hence they are equivalent. □

In other words, the norm of any other non-zero ideal is a positive integer larger than 1.

Remark 8.7. We have understood the norm of an ideal $N(I)$ from three points of views: in terms of discriminants (Definition 8.1); in terms of integral basis and transition matrix (Proposition 8.3); in terms of the quotient ring (Proposition 8.4).

The following consequence of Proposition 8.4 is called the *ascending chain condition*. Recall that a similar result was required to show that every PID is a UFD.

Proposition 8.8 (Ascending Chain Condition)**.** *Let K be a number field. In the ring of integers $\mathcal{O}_K$, every ascending chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ stabilises. In other words, there is a positive integer N such that $I_m = I_{m+1}$ for all $m \geqslant N$.*

Proof. For each $m \in \mathbb{Z}^+$, suppose $d_m = N(I_m)$ which is the order of $\mathcal{O}_K/I_m$ by Proposition 8.4. If $I_m \subsetneq I_{m+1}$, then for any $a \in \mathcal{O}_K$, we have $a + I_m \subsetneq a + I_{m+1}$; i.e. every coset of I_m is contained in some coset of I_{m+1} while every coset of I_{m+1} contains more than one coset of I_m. It follows that $d_m \geqslant d_{m+1}$ and the equality holds iff $I_m = I_{m+1}$. The increasing chain of ideals gives $d_1 \geqslant d_2 \geqslant d_3 \geqslant \cdots$. Since all d_m's are positive integers, there exists some $N > 0$ such that $d_m = d_{m+1}$ for $m \geqslant N$, hence $I_m = I_{m+1}$ for every $m \geqslant N$. □

To provide a convenient tool for computing the norm of a principal ideal, we will explain the relation between the two norms: the norm of an element and the norm of an ideal. If the ideal $I = (\alpha)$ is generated by a single element α, it is natural to expect that $N(\alpha)$ and $N(I)$ are closely related. It is true by the following result.

Proposition 8.9. *Let $I = (\alpha)$ for some non-zero element $\alpha \in \mathcal{O}_K$. Then $N(I) = |N(\alpha)|$.*

Proof. We will follow the definitions to interpret the two norms by determinants of certain matrices. We fix an integral basis $\omega_1, \omega_2, \cdots, \omega_n$ for $\mathcal{O}_K$. It is also a $\mathbb{Q}$-basis for K. For each $j = 1, 2, \cdots, n$, write $\alpha\omega_j = \sum_{i=1}^{n} a_{ij}\omega_i$, then the linear transformation L_α under this basis is given by the matrix $M = (a_{ij})$. Hence $N(\alpha) = \det(M)$.

To compute $N(I)$, we first need to write down an integral basis for I. By Exercise 7.4, we know that $\alpha\omega_1, \alpha\omega_2, \cdots, \alpha\omega_n$ is such an integral basis. Using this integral basis, we apply Proposition 8.3 and get that $N(I) = |\det(M)|$. It follows that $N(I) = |N(\alpha)|$. □