7.2. **Integral bases of ideals.** We focus on the additive structure of the ring $\mathcal{O}_K$, then $\mathcal{O}_K$ is an (additive) abelian group, and every ideal I of $\mathcal{O}_K$ is an abelian subgroup. We are aiming to show that every ideal I is a free abelian group.

Lemma 7.7. *For any $\beta \in K$, there exists some $b \in \mathbb{Z}$, $b \neq 0$, such that $b\beta \in \mathcal{O}_K$.*

Proof. By Lemma 6.13, β is an algebraic number. Therefore β satisfies an equation

$$a_0\beta^m + a_1\beta^{m-1} + a_2\beta^{m-2} + \cdots + a_m = 0$$

where $a_i \in \mathbb{Z}$ for each i and $a_0 \neq 0$. Multiply both sides by a_0^{m-1} to get

$$(a_0\beta)^m + a_1(a_0\beta)^{m-1} + a_2a_0(a_0\beta)^{m-2} + \cdots + a_ma_0^{m-1} = 0.$$

This shows that $a_0\beta$ is an algebraic integer since $a_ia_0^{i-1} \in \mathbb{Z}$ for each i. □

Lemma 7.8. *Every non-zero ideal I of $\mathcal{O}_K$ contains a basis for K over $\mathbb{Q}$.*

Proof. Assume the degree of K over $\mathbb{Q}$ is n. Pick any $\mathbb{Q}$-basis $\beta_1, \beta_2, \cdots, \beta_n$ of K. By Lemma 7.7 we can find some $b \in \mathbb{Z}$, $b \neq 0$, such that $b\beta_1, b\beta_2, \cdots, b\beta_n \in \mathcal{O}_K$. Indeed, there is some non-zero $b_i \in \mathbb{Z}$ for each β_i such that $b_i\beta_i \in \mathcal{O}_K$. Then take b to be any common multiple all b_i's.

We choose any $\alpha \in I$, $\alpha \neq 0$. Then $b\beta_1\alpha, b\beta_2\alpha, \cdots, b\beta_n\alpha$ are in I and form a $\mathbb{Q}$-basis of K. Indeed, for any $a_1, a_2, \cdots, a_n \in \mathbb{Q}$, if

$$a_1b\beta_1\alpha + a_2b\beta_2\alpha + \cdots + a_nb\beta_n\alpha = 0,$$

then since $b\alpha \neq 0$ we have

$$a_1\beta_1 + a_2\beta_2 + \cdots + a_n\beta_n = 0,$$

which implies $a_i = 0$ for each i. Hence $b\beta_1\alpha, b\beta_2\alpha, \cdots, b\beta_n\alpha$ are $\mathbb{Q}$-independent and is a $\mathbb{Q}$-basis for K. □

In other words, the above proposition says we can find a $\mathbb{Q}$-basis for K which entirely consists of algebraic integers. There are in general many choices for the $\mathbb{Q}$-basis of K in $\mathcal{O}_K$, but the follow result shows that some of them are much preferred.

Proposition 7.9. *Let I be a non-zero ideal of $\mathcal{O}_K$. Then we can find $\alpha_1, \alpha_2, \cdots, \alpha_n \in I$ such that they form a $\mathbb{Q}$-basis for K, and for every element α in the field K, $\alpha \in I$ iff $\alpha = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_n\alpha_n$ for some $a_1, a_2, \cdots, a_n \in \mathbb{Z}$.*

Proof. By Lemma 7.8, I contains $\mathbb{Q}$-bases for K. By Remark 7.4 and Proposition 7.5, the discriminant of any such basis is a non-zero integer. Therefore we can always find a $\mathbb{Q}$-basis for $\mathcal{O}_K$ in I such that $|\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)|$ minimal.

It is clear that every integral linear combination of $\alpha_1, \alpha_2, \cdots, \alpha_n$ is in I since I is an ideal. For the other direction, for any $\alpha \in I$, we can write $\alpha = \gamma_1\alpha_1 + \gamma_2\alpha_2 + \cdots + \gamma_n\alpha_n$ with $\gamma_i \in \mathbb{Q}$. We need to show that every $\gamma_i \in \mathbb{Z}$. If not, then some $\gamma_i \notin \mathbb{Z}$ and by relabeling if necessary we can assume $\gamma_1 \notin \mathbb{Z}$. We write $\gamma_1 = m + \theta$ where $m \in \mathbb{Z}$ and $0 < \theta < 1$. Let $\beta_1 = \alpha - m\alpha_1, \beta_2 = \alpha_2, \cdots, \beta_n = \alpha_n$. Then $\beta_1, \beta_2, \cdots, \beta_n \in I$ and is a $\mathbb{Q}$-basis of K. And the transition matrix between the two basis is

$$\begin{pmatrix} \theta & 0 & \cdots & 0 \\ \gamma_2 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \gamma_n & 0 & \cdots & 1 \end{pmatrix}.$$

By Proposition 7.6, we find $\Delta(\beta_1, \beta_2, \cdots, \beta_n) = \theta^2\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)$, which contradicts the minimality of $|\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n)|$ since $0 < \theta < 1$. Therefore $\gamma_i \in \mathbb{Z}$ for every i, which means every element in I is an integral linear combination of $\alpha_1, \alpha_2, \cdots, \alpha_n$. □

Remark 7.10. We make some comments.

(1) For $\alpha_1, \alpha_2, \cdots, \alpha_n$ satisfying the conditions in Proposition 7.9, we say they form an *integral basis* for I. This is very useful in the sense that every element in K can be uniquely written as a rational linear combination of them, and every element in I can be uniquely written as an integral linear combination of them. We sometimes write $I = \mathbb{Z}\alpha_1 \oplus \mathbb{Z}\alpha_2 \oplus \cdots \oplus \mathbb{Z}\alpha_n$ to indicate the second condition.

(2) As a special case of Proposition 7.9, we think of $\mathcal{O}_K$ as a non-zero ideal in itself. Then there is a $\mathbb{Q}$-basis of K, $\omega_1, \omega_2, \cdots, \omega_n$, such that every element $\alpha \in K$ is a $\mathbb{Q}$-linear combination of $\omega_1, \omega_2, \cdots, \omega_n$, and α is an algebraic integer iff all coefficients in this linear combination are in $\mathbb{Z}$. As an example, if K is a quadratic field, we can choose $\omega_1 = 1$ and $\omega_2 = \omega$ as in Proposition 7.2.

Proposition 7.9 shows the existence of an integral basis for I, but the integral basis for I may not be unique. Although there could be many choices, they all have the same discriminants. We look at the following result:

Lemma 7.11. *Suppose* $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ *and* $\{\beta_1, \beta_2, \cdots, \beta_n\}$ *are two integral bases for* I. *Then* $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = \Delta(\beta_1, \beta_2, \cdots, \beta_n)$.

Proof. We leave it as an exercise. See Exercise 7.2. □

By Lemma 7.11, the discriminant of an integral basis of an ideal I in $\mathcal{O}_K$ is independent of the choice of the integral basis. We have the following definition:

Definition 7.12. For any non-zero ideal I in $\mathcal{O}_K$, the discriminant of any integral basis of I is called the *discriminant of the ideal* I, written as $\Delta(I)$. In particular, the discriminant of $\mathcal{O}_K$ is called the *discriminant of the number field* K, written as $\Delta(\mathcal{O}_K)$, or simply Δ_K.

Remark 7.13. By Remark 7.4 and Proposition 7.5, we know that $\Delta(I)$ (hence Δ_K) is always a non-zero integer.

The discriminant of a number field is an important quantity associated to a number field. In the following example we give the values for quadratic fields. We need to remember them because they will be used extensively later.

Proposition 7.14. *Let $d \neq 1$ be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$ a quadratic field. Then*

$$\Delta_K = \begin{cases} 4d & \text{if } d \equiv 2 \text{ or } 3 \pmod 4; \\ d & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. We leave it as an exercise. See Exercise 7.3. □