7. The Ring of Integers in a Number Field

We introduce the ring of integers $\mathcal{O}_K$ in a number field K and determine the additive structure of $\mathcal{O}_K$.

7.1. **The ring of integers.** We first introduce the central object that we will study.

Let K be a number field. We consider the set of all algebraic integers in K. By Corollary 6.7 and the fact that K is a field, this set is closed under addition, multiplication and inverse, hence is a subring of the ring of all algebraic integers. This ring is called the *ring of (algebraic) integers* in K, denote by $\mathcal{O}_K$. The remaining part of this course will be devoted to study various properties of this ring.

The first obvious question, is to understand the elements in $\mathcal{O}_K$. We study this question in two concrete examples.

Proposition 7.1. *A rational number $\alpha \in \mathbb{Q}$ is an algebraic integer iff $\alpha \in \mathbb{Z}$.*

Proof. If $\alpha \in \mathbb{Z}$, it is clearly an algebraic integer. For the other direction, if α is an algebraic integer, by Proposition 6.19, we have $T(\alpha) \in \mathbb{Z}$ and $N(\alpha) \in \mathbb{Z}$. By Example 6.17, in this case $T(\alpha) = N(\alpha) = \alpha$, hence $\alpha \in \mathbb{Z}$. □

Proposition 7.2. *Let $d \neq 1$ be a square-free integer and $K = \mathbb{Q}(\sqrt{d})$ the corresponding quadratic field. The elements in the ring of integers $\mathcal{O}_K$ is given by $\{a + b\omega \mid a, b \in \mathbb{Z}\}$, where*

$$\omega = \begin{cases} \sqrt{d} & \text{if } d \equiv 2 \text{ or } 3 \pmod 4; \\ \frac{1}{2}(1 + \sqrt{d}) & \text{if } d \equiv 1 \pmod 4. \end{cases}$$

Proof. We first show that for any $a, b \in \mathbb{Z}$, $a + b\omega$ is an algebraic number. By Proposition 6.6, it suffices to show ω is an algebraic integer. If $d \equiv 2$ or $3 \pmod 4$, ω is a root of $x^2 - d$ hence is an algebraic integer. If $d \equiv 1 \pmod 4$, ω is a root of $x^2 - x - \frac{d-1}{4}$ hence is also an algebraic integer.

It remains to show that every algebraic integer in K has the given form. Let $\alpha = r + s\sqrt{d}$ is an algebraic integer for some $r, s \in \mathbb{Q}$. By Example 6.17 and Proposition 6.19, we know $T(r + s\sqrt{d}) = 2r \in \mathbb{Z}$ and $N(r + s\sqrt{d}) = r^2 - s^2 d \in \mathbb{Z}$. Thus $(2r)^2 - (2s)^2 d \in 4\mathbb{Z}$ and $(2s)^2 d \in \mathbb{Z}$. Since d is square-free, this implies $2s \in \mathbb{Z}$.

Now we consider the case $d \equiv 2$ or $3 \pmod 4$. If both $2r$ and $2s$ are odd, then $(2r)^2 \equiv 1 \pmod 4$ and $(2s)^2 d \equiv d \pmod 4$, which contradicts $(2r)^2 - (2s)^2 d \in 4\mathbb{Z}$. Hence at least one of them is even. Then by $(2r)^2 \equiv (2s)^2 d \pmod 4$ again and $4 \nmid d$ we conclude that both $2r$ and $2s$ are even; i.e. $r, s \in \mathbb{Z}$. So $\alpha = r + s\sqrt{d}$ has the given form.

Now we consider the other case $d \equiv 1 \pmod 4$. By $(2r)^2 \equiv (2s)^2 d \equiv (2s)^2 \pmod 4$ we know that $2r$ and $2s$ are either both even or both odd; i.e. $r - s \in \mathbb{Z}$. Then $\alpha = r + s\sqrt{d} = (r-s) + s(1+\sqrt{d}) = (r-s) + 2s \cdot \omega$ has the given form. $\square$

Now we turn to the notion of the discriminant.

Definition 7.3. Let K be a number field of degree n over $\mathbb{Q}$ and $\alpha_1, \alpha_2, \cdots, \alpha_n$ an n-tuple of elements of K. We define the *discriminant* of the n-tuple to be

$$\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = \det \begin{pmatrix} T(\alpha_1\alpha_1) & T(\alpha_1\alpha_2) & \cdots & T(\alpha_1\alpha_n) \\ T(\alpha_2\alpha_1) & T(\alpha_2\alpha_2) & \cdots & T(\alpha_2\alpha_n) \\ \vdots & \vdots & \ddots & \vdots \\ T(\alpha_n\alpha_1) & T(\alpha_n\alpha_2) & \cdots & T(\alpha_n\alpha_n) \end{pmatrix}. \tag{7.1}$$

Remark 7.4. If $\alpha_1, \alpha_2, \cdots, \alpha_n \in \mathcal{O}_K$, then each entry of the matrix is an integer by Proposition 6.19, hence the discriminant $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) \in \mathbb{Z}$.

Proposition 7.5. *The n-tuple $\alpha_1, \alpha_2, \cdots, \alpha_n$ is a $\mathbb{Q}$-basis for K iff $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0$.*

Proof. We first show that if $\{\alpha_i \mid 1 \leqslant i \leqslant n\}$ are linearly dependent over $\mathbb{Q}$, then $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = 0$. By assumption we can find $a_1, a_2, \cdots, a_n \in \mathbb{Q}$, not all zero, such that $\sum_{i=1}^n a_i\alpha_i = 0$. Multiply this equation by α_j and take the trace. By Lemma 6.16 we get $\sum_{i=1}^n a_i T(\alpha_i\alpha_j) = 0$ for each $j = 1, 2, \cdots, n$. This shows that the rows of the matrix in (7.1) are linearly dependent, so its determinant is zero.

We then show that if $\{\alpha_i \mid 1 \leqslant i \leqslant n\}$ is a $\mathbb{Q}$-basis for K, then $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) \neq 0$. Assume on the contrary that $\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = 0$, then the rows of the matrix in (7.1) are linearly dependent, so we can find $a_1, a_2, \cdots, a_n \in \mathbb{Q}$, not all zero, such that $\sum_{i=1}^n a_i T(\alpha_i\alpha_j) = 0$ for each $j = 1, 2, \cdots, n$. Let $\alpha = \sum_{i=1}^n a_i\alpha_i$. By Lemma 6.16 we get $T(\alpha\alpha_j) = 0$ for each $j = 1, 2, \cdots, n$. Assume on the contrary that $\{\alpha_i \mid 1 \leqslant i \leqslant n\}$ is a basis, then $\alpha \neq 0$, and there exist $b_1, b_2, \cdots, b_n \in \mathbb{Q}$ such that $\alpha^{-1} = \sum_{j=1}^n b_j\alpha_j$. By Lemma 6.16 again we have $T(\alpha\alpha^{-1}) = \sum_{j=1}^n b_j T(\alpha\alpha_j) = 0$. Contradiction to $T(1) = n \neq 0$. $\square$

Proposition 7.6. *Suppose $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$ and $\{\beta_1, \beta_2, \cdots, \beta_n\}$ are both n-tuples in K. Assume that for each j, $\alpha_j = \sum_{i=1}^n a_{ij}\beta_i$ for some $a_{ij} \in \mathbb{Q}$ and $M = (a_{ij})$ the transition matrix, then*

$$\Delta(\alpha_1, \alpha_2, \cdots, \alpha_n) = (\det M)^2 \, \Delta(\beta_1, \beta_2, \cdots, \beta_n).$$

Proof. (This proof is not covered in lecture and is non-examinable.) We have $\alpha_j\alpha_l = \sum_i \sum_k a_{ij}a_{kl}\beta_i\beta_k$. Taking the traces of both sides we get $T(\alpha_j\alpha_l) = \sum_i \sum_k a_{ij}a_{kl}T(\beta_i\beta_k)$. Let $A = (T(\alpha_j\alpha_l))$, $B = (T(\beta_i\beta_k))$ be $n \times n$ matrices. Then we find the matrix identity $A = M'BM$ where M' is the transpose of M. Take the determinant on both sides to get $\det A = (\det M)^2 \det B$, as desired. $\square$