6.2. **Number fields.** We introduce the notion of number fields as follows:

Definition 6.8. An *(algebraic) number field* is a field K, such that $\mathbb{Q} \subseteq K \subseteq \mathbb{C}$, and K has finite degree (dimension as a vector space) over $\mathbb{Q}$.

Example 6.9. Simple example: the field $\mathbb{Q}$ itself is a number field of degree 1 over $\mathbb{Q}$.

We recall a useful result in Algebra 2B which gives a lot of examples of number fields.

Proposition 6.10. *Let $\Bbbk \subseteq K$ be a field extension, and let $\alpha \in K$ be a root of some non-zero polynomial $g(x) \in \Bbbk[x]$. Then the set $\{f(\alpha) \in K \mid f \in \Bbbk[x]\}$ is a field, denoted by $\Bbbk[\alpha]$ or $\Bbbk(\alpha)$, satisfying $\Bbbk \subseteq \Bbbk(\alpha) \subseteq K$.*

Moreover, assume $g(x)$ is irreducible and $\deg g(x) = n$, then $\Bbbk(\alpha)$ has degree n over $\Bbbk$ and $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ is a basis of $\Bbbk(\alpha)$ over $\Bbbk$.

Proof. See Proposition 2.23 (2013) or Theorem 4.8 (2014) in Algebra 2B. □

Remark 6.11. We point out two things.

(1) In Algebra 2B, we used the notation $\Bbbk[\alpha]$. But in literature (especially in literature on field theory) the notation $\Bbbk(\alpha)$ seems to be used more often. We will use the latter.

(2) Roughly speaking, if an element α in the large field is the root of a polynomial with coefficients in the small field, then we can "add" α to the small field to generate an intermediate field, which has a finite degree over the small field, with a basis given by powers of α. If the small and large fields are $\mathbb{Q}$ and $\mathbb{C}$ respectively, we can get lots of examples of number fields.

Example 6.12. In Proposition 6.10, we take $\Bbbk = \mathbb{Q}$ and $K = \mathbb{C}$.

(1) For any square-free integer $d \neq 1$, $\sqrt{d}$ is a root of the irreducible polynomial $x^2 - d \in \mathbb{Q}[x]$. Therefore $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ is number field of degree 2 over $\mathbb{Q}$. A number field of this form is called a *quadratic field*. It is called a *real quadratic field* if $d > 0$, or an *imaginary quadratic field* if $d < 0$. For instance, $\mathbb{Q}(\sqrt{2})$ is a real quadratic fields and $\mathbb{Q}(i)$ is an imaginary quadratic field.

(2) We have that $\sqrt[3]{2}$ is a root of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$. Therefore $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$ is a number field of degree 3 over $\mathbb{Q}$. This is an example of the so-called *cubic field*.

(3) We have that $\zeta = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ is the root of an irreducible polynomial $x^4 + x^3 + x^2 + x + 1$. Therefore $\mathbb{Q}(\zeta)$ is a number field of degree 4 over $\mathbb{Q}$. This is an example of the so-called *cyclotomic field*.

The following lemma justifies the name.

Lemma 6.13. *Every element in a number field is an algebraic number.*

Proof. Let K be a number field of degree n over $\mathbb{Q}$ and $\alpha \in K$. Then $1, \alpha, \alpha^2, \cdots, \alpha^n$ must be linearly dependent over $\mathbb{Q}$; i.e. $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_n\alpha^n = 0$, where $a_i \in \mathbb{Q}$ for each i and all a_i's are not simultaneously zero. This implies α is a root of a polynomial with rational coefficients, hence is an algebraic number. □

We then introduce the notions of traces and norms.

Definition 6.14. Let K be a number field. Every $\alpha \in K$ defines a $\mathbb{Q}$-linear transformation

$$L_\alpha : K \to K, \quad \gamma \mapsto \alpha\gamma.$$

The trace of the linear transformation L_α is called the *trace* of α in K, denoted by $T_K(\alpha)$. The determinant of the linear transformation L_α is called the *norm* of α in K, denoted by $N_K(\alpha)$.

Remark 6.15. We make the following comments about this definition.

(1) The $\mathbb{Q}$-linearity of L_α can be easily checked by observing $\alpha(\gamma_1 + \gamma_2) = \alpha\gamma_1 + \alpha\gamma_2$ for any $\gamma_1, \gamma_2 \in K$, and $\alpha(\lambda\gamma) = \lambda(\alpha\gamma)$ for any $\gamma \in K$ and $\lambda \in \mathbb{Q}$.

(2) The trace and norm depends on both K and α. The same algebraic number α, when considered as an element of different number fields, could have different traces and norms. If there is only one number field K in consideration, we often omit the reference to K and write $T(\alpha)$ and $N(\alpha)$ for simplicity.

(3) In practice we can choose any $\mathbb{Q}$-basis of K and write the linear transformation L_α as a matrix to compute $T(\alpha)$ and $N(\alpha)$. We know that the trace and determinant of a linear transformation are independent of the choice of the basis, but choosing the basis wisely can make the computation easier.

The following properties can be easily proved using the language of linear transformations and matrices.

Lemma 6.16. *Let K be a number field of degree n over $\mathbb{Q}$, $\alpha, \beta \in K$ and $a \in \mathbb{Q}$. Then*

(1) $T(\alpha + \beta) = T(\alpha) + T(\beta)$, $N(\alpha\beta) = N(\alpha)N(\beta)$;

(2) $T(a\alpha) = aT(\alpha)$, $N(a\beta) = a^n N(\beta)$;

(3) $T(1) = n$, $N(1) = 1$;

(4) $N(\alpha) = 0$ *iff* $\alpha = 0$.

Proof. We leave them as exercises. See Exercise 6.3. □

We show two examples of computation of traces and norms.

Example 6.17. Consider the number field $K = \mathbb{Q}$. For any $\alpha \in K$, we compute its trace and norm. We choose a $\mathbb{Q}$-basis $\{1\}$ for K, then the matrix of L_α under this basis is a 1×1 matrix with the only entry α. Hence $T(\alpha) = \alpha$ and $N(\alpha) = \alpha$.

Example 6.18. Consider the quadratic field $K = \mathbb{Q}(\sqrt{d})$ where $d \neq 1$ is a square-free integer. For any $\alpha = a + b\sqrt{d} \in K$, we compute its trace and norm. We choose a $\mathbb{Q}$-basis $\{1, \sqrt{d}\}$ for K. Since $L_\alpha(1) = a + b\sqrt{d}$ and $L_\alpha(\sqrt{d}) = bd + a\sqrt{d}$, the matrix of L_α under this basis is $\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$. Therefore $T(\alpha) = 2a$ and $N(\alpha) = a^2 - b^2 d$.

A crucial property of the trace and the norm is the following:

Proposition 6.19. *Let K be a number field and α an algebraic integer in K, then $T(\alpha), N(\alpha) \in \mathbb{Z}$.*

Sketch of proof. The proof of this result will be left in Exercise 6.4. Here we explain briefly the motivation and main idea in the proof and give some hints step by step.

By Definition 6.14, if we can find a $\mathbb{Q}$-basis for K, under which the matrix of the linear transformation L_α has integral entries, then $T(\alpha)$ and $N(\alpha)$ are integers. Therefore the proof contains two steps: find a $\mathbb{Q}$-basis for K; show that the matrix of L_α under this basis has integer entries.

More precisely, we consider an intermediate field $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq K$ as in Proposition 6.10. Then for some $m > 0$, we know $\{1, \alpha, \alpha^2, \cdots, \alpha^{m-1}\}$ is a basis of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. On the other hand, we choose any basis of K over $\mathbb{Q}(\alpha)$, say $\{\beta_0, \beta_1, \cdots, \beta_{n-1}\}$. We can prove that the set

$$S = \left\{\alpha^i \beta_j \mid 0 \leqslant i \leqslant m-1, 0 \leqslant j \leqslant n-1\right\}$$

is a basis of K over $\mathbb{Q}$. For this purpose, we need to show that S is a spanning set and elements in S are independent. Then we write down the matrix for L_α under this basis and conclude all entries are integers. □