Chapter 1

Algebraic Numbers and Algebraic Integers

1.1 Rings of integers

We start by introducing two essential notions: number field and algebraic integer.

Definition 1.1. A number field is a finite field extension K of $\mathbb{Q}$, i.e., a field which is a $\mathbb{Q}$-vector space of finite dimension. We note this dimension $[K : \mathbb{Q}]$ and call it the degree of K.

Examples 1.1.

1. The field
$$\mathbb{Q}(\sqrt{2}) = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$$
is a number field. It is of degree 2 over $\mathbb{Q}$. Number fields of degree 2 over $\mathbb{Q}$ are called quadratic fields. More generally, $\mathbb{Q}[X]/f(X)$ is a number field if f is irreducible. It is of degree the degree of the polynomial f.

2. Let ζ_n be a primitive nth root of unity. The field $\mathbb{Q}(\zeta_n)$ is a number field called cyclotomic field.

3. The fields $\mathbb{C}$ and $\mathbb{R}$ are not number fields.

Let K be a number field of degree n. If $\alpha \in K$, there must be a $\mathbb{Q}$-linear dependency among $\{1, \alpha, \ldots, \alpha^n\}$, since K is a $\mathbb{Q}$-vector space of dimension n. In other words, there exists a polynomial $f(X) \in \mathbb{Q}[X]$ such that $f(X) = 0$. We call α an algebraic number.

Definition 1.2. An algebraic integer in a number field K is an element $\alpha \in K$ which is a root of a monic polynomial with coefficients in $\mathbb{Z}$.

Example 1.2. Since $X^2-2=0$, $\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is an algebraic integer. Similarly, $i \in \mathbb{Q}(i)$ is an algebraic integer, since $X^2+1=0$. However, an element $a/b \in \mathbb{Q}$ is not an algebraic integer, unless b divides a.

Now that we have the concept of an algebraic integer in a number field, it is natural to wonder whether one can compute the set of all algebraic integers of a given number field. Let us start by determining the set of algebraic integers in $\mathbb{Q}$.

Definition 1.3. The minimal polynomial f of an algebraic number α is the monic polynomial in $\mathbb{Q}[X]$ of smallest degree such that $f(\alpha)=0$.

Proposition 1.1. *The minimal polynomial of α has integer coefficients if and only if α is an algebraic integer.*

Proof. If the minimal polynomial of α has integer coefficients, then by definition (Definition 1.2) α is algebraic.

Now let us assume that α is an algebraic integer. This means by definition that there exists a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha)=0$. Let $g \in \mathbb{Q}[X]$ be the minimal polyonial of α. Then $g(X)$ divides $f(X)$, that is, there exists a monic polynomial $h \in \mathbb{Q}[X]$ such that

$$g(X)h(X)=f(X).$$

(Note that h is monic because f and g are). We want to prove that $g(X)$ actually belongs to $\mathbb{Z}[X]$. Assume by contradiction that this is not true, that is, there exists at least one prime p which divides one of the denominators of the coefficients of g. Let $u>0$ be the smallest integer such that $p^u g$ does not have anymore denominators divisible by p. Since h may or may not have denominators divisible by p, let $v \geq 0$ be the smallest integer such that $p^v h$ has no denominator divisible by p. We then have

$$p^u g(X) p^v h(X) = p^{u+v} f(X).$$

The left hand side of this equation does not have denominators divisible by p anymore, thus we can look at this equation modulo p. This gives

$$p^u g(X) p^v h(X) \equiv 0 \in \mathbb{F}_p[X],$$

where $\mathbb{F}_p$ denotes the finite field with p elements. This give a contradiction, since the left hand side is a product of two non-zero polynomials (by minimality of u and v), and $\mathbb{F}_p[X]$ does not have zero divisor. □

Corollary 1.2. *The set of algebraic integers of $\mathbb{Q}$ is $\mathbb{Z}$.*

Proof. Let $\frac{a}{b} \in \mathbb{Q}$. Its minimal polynomial is $X-\frac{a}{b}$. By the above proposition, $\frac{a}{b}$ is an algebraic integer if and only $b=\pm 1$. □

Definition 1.4. The set of algebraic integers of a number field K is denoted by $\mathcal{O}_K$. It is usually called the ring of integers of K.

The fact that $\mathcal{O}_K$ is a ring is not obvious. In general, if one takes a, b two algebraic integers, it is not straightforward to find a monic polynomial in $\mathbb{Z}[X]$ which has $a+b$ as a root. We now proceed to prove that $\mathcal{O}_K$ is indeed a ring.

Theorem 1.3. *Let K be a number field, and take $\alpha \in K$. The two statements are equivalent:*

1. *α is an algebraic integer.*
2. *The Abelian group $\mathbb{Z}[\alpha]$ is finitely generated (a group G is finitely generated if there exist finitely many elements $x_1, ..., x_s \in G$ such that every $x \in G$ can be written in the form $x = n_1x_1 + n_2x_2 + ... + n_sx_s$ with integers $n_1, ..., n_s$).*

Proof. Let α be an algebraic integer, and let m be the degree of its minimal polynomial, which is monic and with coefficients in $\mathbb{Z}$ by Proposition 1.1. Since all α^u with $u \geq m$ can be written as $\mathbb{Z}$-linear combination of $1, \alpha, \ldots, \alpha^{m-1}$, we have that

$$\mathbb{Z}[\alpha] = \mathbb{Z} \oplus \mathbb{Z}\alpha \oplus \ldots \oplus \mathbb{Z}\alpha^{m-1}$$

and $\{1, \alpha, \ldots, \alpha^{m-1}\}$ generate $\mathbb{Z}[\alpha]$ as an Abelian group. Note that for this proof to work, we really need the minimal polynomial to have coefficients in $\mathbb{Z}$, and to be monic!

Conversely, let us assume that $\mathbb{Z}[\alpha]$ is finitely generated, with generators $a_1, \ldots, a_m$, where $a_i = f_i(\alpha)$ for some $f_i \in \mathbb{Z}[X]$. In order to prove that α is an algebraic integer, we need to find a monic polynomial $f \in \mathbb{Z}[X]$ such that $f(\alpha) = 0$. Let N be an integer such that $N > \deg f_i$ for $i = 1, \ldots, m$. We have that

$$\alpha^N = \sum_{j=1}^{m} b_j a_j, \ b_j \in \mathbb{Z}$$

that is

$$\alpha^N - \sum_{j=1}^{m} b_j f_j(\alpha) = 0.$$

Let us thus choose

$$f(X) = X^N - \sum_{j=1}^{m} b_j f_j(X).$$

Clearly $f \in \mathbb{Z}[X]$, it is monic by the choice of $N > \deg f_i$ for $i = 1, \ldots, m$, and finally $f(\alpha) = 0$. So α is an algebraic integer. □

Example 1.3. We have that

$$\mathbb{Z}[1/2] = \left\{ \frac{a}{b} \mid b \text{ is a power of } 2 \right\}$$

is not finitely generated, since $\frac{1}{2}$ is not an algebraic integer. Its minimal polynomial is $X - \frac{1}{2}$.

Corollary 1.4. *Let K be a number field. Then $\mathcal{O}_K$ is a ring.*

Proof. Let $\alpha, \beta \in \mathcal{O}_K$. The above theorem tells us that $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated, thus so is $\mathbb{Z}[\alpha, \beta]$. Now, $\mathbb{Z}[\alpha, \beta]$ is a ring, thus in particular $\alpha \pm \beta$ and $\alpha\beta \in \mathbb{Z}[\alpha, \beta]$. Since $\mathbb{Z}[\alpha \pm \beta]$ and $\mathbb{Z}[\alpha\beta]$ are subgroups of $\mathbb{Z}[\alpha, \beta]$, they are finitely generated. By invoking again the above theorem, $\alpha \pm \beta$ and $\alpha\beta \in \mathcal{O}_K$. □

Corollary 1.5. *Let K be a number field, with ring of integers $\mathcal{O}_K$. Then $\mathbb{Q}\mathcal{O}_K = K$.*

Proof. It is clear that if $x = b\alpha \in \mathbb{Q}\mathcal{O}_K$, $b \in \mathbb{Q}$, $\alpha \in \mathcal{O}_K$, then $x \in K$.

Now if $\alpha \in K$, we show that there exists $d \in \mathbb{Z}$ such that $\alpha d \in \mathcal{O}_K$ (that is $\alpha d = \beta \in \mathcal{O}_K$, or equivalently, $\alpha = \beta/d$). Let $f(X) \in \mathbb{Q}[X]$ be the minimal polynomial of α. Choose d to be the least common multiple of the denominators of the coefficients of $f(X)$, then (recall that f is monic!)

$$d^{\deg(f)} f\left(\frac{X}{d}\right) = g(X),$$

and $g(X) \in \mathbb{Z}[X]$ is monic, with αd as a root. Thus $\alpha d \in \mathcal{O}_K$. □

1.2 Norms and Traces

Definition 1.5. Let L/K be a finite extension of number fields. Let $\alpha \in L$. We consider the multiplication map by α, denoted by μ_α, such that

$$\begin{aligned} \mu_\alpha : \quad L &\to \quad L \\ x &\mapsto \quad \alpha x. \end{aligned}$$

This is a K-linear map of the K-vector space L into itself (or in other words, an endomorphism of the K-vector space L). We call the norm of α the determinant of μ_α, that is

$$\mathrm{N}_{L/K}(\alpha) = \det(\mu_\alpha) \in K,$$

and the trace of α the trace of μ_α, that is

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(\mu_\alpha) \in K.$$

Note that the norm is multiplicative, since

$$\mathrm{N}_{L/K}(\alpha\beta) = \det(\mu_{\alpha\beta}) = \det(\mu_\alpha \circ \mu_\beta) = \det(\mu_\alpha)\det(\mu_\beta) = \mathrm{N}_{L/K}(\alpha)\mathrm{N}_{L/K}(\beta)$$

while the trace is additive:

$$\mathrm{Tr}_{L/K}(\alpha+\beta) = \mathrm{Tr}(\mu_{\alpha+\beta}) = \mathrm{Tr}(\mu_\alpha+\mu_\beta) = \mathrm{Tr}(\mu_\alpha)+\mathrm{Tr}(\mu_\beta) = \mathrm{Tr}_{L/K}(\alpha)+\mathrm{Tr}_{L/K}(\beta).$$

In particular, if n denotes the degree of L/K, we have that

$$\mathrm{N}_{L/K}(a\alpha) = a^n \mathrm{N}_{L/K}(\alpha),\ \mathrm{Tr}_{L/K}(a\alpha) = a\mathrm{Tr}_{L/K}(\alpha),\ a \in K.$$

Indeed, the matrix of μ_a is given by a diagonal matrix whose coefficients are all a when $a \in K$.

Recall that the characteristic polynomial of $\alpha \in L$ is the characteristic polynomial of μ_α, that is

$$\chi_{L/K}(X) = \det(XI - \mu_\alpha) \in K[X].$$

This is a monic polynomial of degree $n = [L : K]$, the coefficient of X^{n-1} is $-\mathrm{Tr}_{L/K}(\alpha)$ and its constant term is $\pm \mathrm{N}_{L/K}(\alpha)$.

Example 1.4. Let L be the quadratic field $\mathbb{Q}(\sqrt{2})$, $K = \mathbb{Q}$, and take $\alpha \in \mathbb{Q}(\sqrt{2})$. In order to compute μ_α, we need to fix a basis of $\mathbb{Q}(\sqrt{2})$ as $\mathbb{Q}$-vector space, say

$$\{1, \sqrt{2}\}.$$

Thus, α can be written $\alpha = a + b\sqrt{2}$, $a, b \in \mathbb{Q}$. By linearity, it is enough to compute μ_α on the basis elements:

$$\mu_\alpha(1) = a + b\sqrt{2},\ \mu_\alpha(\sqrt{2}) = (a + b\sqrt{2})\sqrt{2} = a\sqrt{2} + 2b.$$

We now have that

$$\begin{pmatrix} 1, & \sqrt{2} \end{pmatrix} \underbrace{\begin{pmatrix} a & 2b \\ b & a \end{pmatrix}}_{M} = \begin{pmatrix} a + b\sqrt{2}, & 2b + a\sqrt{2} \end{pmatrix}$$

and M is the matrix of μ_α in the chosen basis. Of course, M changes with a change of basis, but the norm and trace of α are independent of the basis. We have here that

$$\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = a^2 - 2b^2,\ \mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = 2a.$$

Finally, the characteristic polynomial of μ_α is given by

$$\begin{aligned} \chi_{L/K}(X) &= \det\left(XI - \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\right) \\ &= \det\begin{pmatrix} X - a & -b \\ -2b & X - a \end{pmatrix} \\ &= (X - a)(X - a) - 2b^2 \\ &= X^2 - 2aX + a^2 - 2b^2. \end{aligned}$$

We recognize that the coefficient of X is indeed the trace of α with a minus sign, while the constant coefficient is its norm.

We now would like to give another equivalent definition of the trace and norm of an algebraic integer α in a number field K, based on the different roots of the minimal polynomial of α. Since these roots may not belong to K, we first need to introduce a bigger field which will contain all the roots of the polynomials we will consider.

Definition 1.6. The field $\bar{F}$ is called an algebraic closure of a field F if all the elements of $\bar{F}$ are algebraic over F and if every polynomial $f(X) \in F[X]$ splits completely over $\bar{F}$.

We can think that $\bar{F}$ contains all the elements that are algebraic over F, in that sense, it is the largest algebraic extension of F. For example, the field of complex numbers $\mathbb{C}$ is the algebraic closure of the field of reals $\mathbb{R}$ (this is the fundamental theorem of algebra). The algebraic closure of $\mathbb{Q}$ is denoted by $\bar{\mathbb{Q}}$, and $\bar{\mathbb{Q}} \subset \mathbb{C}$.

Lemma 1.6. *Let K be number field, and let $\bar{K}$ be its algebraic closure. Then an irreducibe polynomial in $K[X]$ cannot have a multiple root in $\bar{K}$.*

Proof. Let $f(X)$ be an irreducible polynomial in $K[X]$. By contradiction, let us assume that $f(X)$ has a multiple root α in $\bar{K}$, that is $f(X) = (X-\alpha)^m g(X)$ with $m \geq 2$ and $g(\alpha) \neq 0$. We have that the formal derivative of $f'(X)$ is given by

$$\begin{aligned} f'(X) &= m(X-\alpha)^{m-1} g(X) + (X-\alpha)^m g'(X) \\ &= (X-\alpha)^{m-1}(mg(X) + (X-\alpha)g'(X)), \end{aligned}$$

and therefore $f(X)$ and $f'(X)$ have $(X-\alpha)^{m-1}$, $m \geq 2$, as a common factor in $\bar{K}[X]$. In other words, α is root of both $f(X)$ and $f'(X)$, implying that the minimal polynomial of α over K is a common factor of $f(X)$ and $f'(X)$. Now since $f(X)$ is irreducible over $K[X]$, this common factor has to be $f(X)$ itself, implying that $f(X)$ divides $f'(X)$. Since $\deg(f'(X)) < \deg(f(X))$, this forces $f'(X)$ to be zero, which is not possible with K of characteristic 0. □

Thanks to the above lemma, we are now able to prove that an extension of number field of degree n can be embedded in exactly n different ways into its algebraic closure. These n embeddings are what we need to redefine the notions of norm and trace. Let us first recall the notion of field monomorphism.

Definition 1.7. Let L_1, L_2 be two field extensions of a field K. A field monomorphism σ from L_1 to L_2 is a field homomorphism, that is a map from L_1 to L_2 such that, for all $a, b \in L_1$,

$$\begin{aligned} \sigma(ab) &= \sigma(a)\sigma(b) \\ \sigma(a+b) &= \sigma(a) + \sigma(b) \\ \sigma(1) &= 1 \\ \sigma(0) &= 0. \end{aligned}$$

A field homomorphism is automatically an injective map, and thus a field monomorphism. It is a field K-monomorphism if it fixes K, that is, if $\sigma(c) = c$ for all $c \in K$.

Example 1.5. We consider the number field $K = \mathbb{Q}(i)$. Let $x = a + ib \in \mathbb{Q}(i)$. If σ is field $\mathbb{Q}$-homomorphism, then $\sigma(x) = a + \sigma(i)b$ since it has to fix $\mathbb{Q}$. Furthermore, we need that

$$\sigma(i)^2 = \sigma(i^2) = -1,$$

so that $\sigma(i) = \pm i$. This gives us exactly two $\mathbb{Q}$-monomorphisms of K into $\bar{K} \subset \mathbb{C}$, given by:

$$\sigma_1 : a + ib \mapsto a + ib,\ \sigma_2 : a + ib \mapsto a - ib,$$

that is the identity and the complex conjugation.

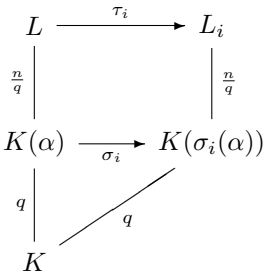
Proposition 1.7. *Let K be a number field, L be a finite extension of K of degree n, and $\bar{K}$ be an algebraic closure of K. There are n distinct K-monomorphisms of L into $\bar{K}$.*

Proof. This proof is done in two steps. In the first step, the claim is proved in the case when $L = K(\alpha)$, $\alpha \in L$. The second step is a proof by induction on the degree of the extension L/K in the general case, which of course uses the first step. The main idea is that if $L \neq K(\alpha)$ for some $\alpha \in L$, then one can find such intermediate extension, that is, we can consider the tower of extensions $K \subset K(\alpha) \subset L$, where we can use the first step for $K(\alpha)/K$ and the induction hypothesis for $L/K(\alpha)$.

Step 1. Let us consider $L = K(\alpha)$, $\alpha \in L$ with minimal polynomial $f(X) \in K[X]$. It is of degree n and thus admits n roots $\alpha_1, \ldots, \alpha_n$ in $\bar{K}$, which are all distinct by Lemma 1.6. For $i = 1, \ldots, n$, we thus have a K-monomorphism $\sigma_i : L \to \bar{K}$ such that $\sigma_i(\alpha) = \alpha_i$.

Step 2. We now proceed by induction on the degree n of L/K. Let $\alpha \in L$ and consider the tower of extensions $K \subset K(\alpha) \subset L$, where we denote by q, $q > 1$, the degree of $K(\alpha)/K$. We know by the first step that there are q distinct K-monomomorphisms from $K(\alpha)$ to $\bar{K}$, given by $\sigma_i(\alpha) = \alpha_i$, $i = 1, \ldots, q$, where α_i are the q roots of the minimal polynomial of α.

Now the fields $K(\alpha)$ and $K(\sigma_i(\alpha))$ are isomorphic (the isomorphism is given by σ_i) and one can build an extension L_i of $K(\sigma_i(\alpha))$ and an isomorphism $\tau_i : L \to L_i$ which extends σ_i (that is, τ_i restricted to $K(\alpha)$ is nothing else than σ_i):



Now, since

$$[L_i : K(\sigma_i(\alpha))] = [L : K(\alpha)] = \frac{n}{q} < n,$$

we have by induction hypothesis that there are $\frac{n}{q}$ distinct $K(\sigma_i(\alpha))$-monomorphisms θ_{ij} of L_i into $\bar{K}$. Therefore, $\theta_{ij} \circ \tau_i$, $i = 1, \ldots, q$, $j = 1, \ldots, \frac{n}{q}$ provide n distinct K-monomorphisms of L into $\bar{K}$. □

Corollary 1.8. *A number field K of degree n over $\mathbb{Q}$ has n embeddings into $\mathbb{C}$.*

Proof. The proof is immediate from the proposition. It is very common to find in the literature expressions such as "let K be a number field of degree n, and $\sigma_1, \ldots, \sigma_n$ be its n embeddings", without further explanation. □

Definition 1.8. Let L/K be an extension of number fields, and let $\alpha \in L$. Let $\sigma_1, \ldots, \sigma_n$ be the n field K-monomorphisms of L into $\bar{K} \subset \mathbb{C}$ given by the above proposition. We call $\sigma_1(\alpha), \ldots, \sigma_n(\alpha)$ the conjugates of α.

Proposition 1.9. *Let L/K be an extension of number fields. Let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of L into $\mathbb{C}$ which fix K. For all $\alpha \in L$, we have*

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha), \ \mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha).$$

Proof. Let $\alpha \in L$, with minimal polynomial $f(X) \in K[X]$ of degree m, and let $\chi_{K(\alpha)/K}(X)$ be its characteristic polynomial.

Let us first prove that $f(X) = \chi_{K(\alpha)/K}(X)$. Note that both polynomials are monic by definition. Now the K-vector space $K(\alpha)$ has dimension m, thus m is also the degree of $\chi_{K(\alpha)/K}(X)$. By Cayley-Hamilton theorem (which states that every square matrix over the complex field satisfies its own characteristic equation), we have that

$$\chi_{K(\alpha)/K}(\mu_\alpha) = 0.$$

Now since

$$\chi_{K(\alpha)/K}(\mu_\alpha) = \mu_{\chi_{K(\alpha)/K}(\alpha)},$$

(see Example 1.7), we have that α is a root of $\chi_{K(\alpha)/K}(X)$. By minimality of the minimal polynomial $f(X)$, $f(X) \mid \chi_{K(\alpha)/K}(X)$, but knowing that both polynomials are monic of same degree, it follows that

$$f(X) = \chi_{K(\alpha)/K}(X). \tag{1.1}$$

We now compute the matrix of μ_α in a K-basis of L. We have that

$$\{1, \alpha, \ldots, \alpha^{m-1}\}$$

is a K-basis of $K(\alpha)$. Let k be the degree $[L : K(\alpha)]$ and let $\{\beta_1, \ldots, \beta_k\}$ be a $K(\alpha)-$basis of L. The set $\{\alpha^i \beta_j\}$, $0 \leq i < m$, $1 \leq j \leq k$ is a K-basis of L. The multiplication μ_α by α can now be written in this basis as

$$\mu_\alpha = \underbrace{\begin{pmatrix} B & 0 & \ldots & 0 \\ 0 & B & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & \ldots & B \end{pmatrix}}_{k \text{ times}}, \ B = \begin{pmatrix} 0 & 1 & \ldots & 0 \\ 0 & 0 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \\ a_0 & a_1 & \ldots & a_{m-1} \end{pmatrix}$$

where a_i, $i = 0, \ldots, m-1$ are the coefficients of the minimal polynomial $f(X)$ (in other words, B is the companion matrix of f). We conclude that

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha) &= \mathrm{N}_{K(\alpha)/K}(\alpha)^k, \\ \mathrm{Tr}_{L/K}(\alpha) &= k\mathrm{Tr}_{K(\alpha)/K}(\alpha), \\ \chi_{L/K}(X) &= (\chi_{K(\alpha)/K})^k = f(X)^k, \end{aligned}$$

where last equality holds by (1.1). Now we have that

$$\begin{aligned} f(X) &= (X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_m) \in \bar{\mathbb{Q}}[X] \\ &= X^m - \sum_{i=1}^{m} \alpha_i X^{m-1} + \ldots \pm \prod_{i=1}^{m} \alpha_i \in \mathbb{Q}[X] \\ &= X^m - \mathrm{Tr}_{K(\alpha)/K}(\alpha) X^{m-1} + \ldots \pm \mathrm{N}_{K(\alpha)/K}(\alpha) \in \mathbb{Q}[X] \end{aligned}$$

where last equality holds by (1.1), so that

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha) &= \left(\prod_{i=1}^{m} \alpha_i \right)^k, \\ \mathrm{Tr}_{L/K}(\alpha) &= k \sum_{i=1}^{m} \alpha_i. \end{aligned}$$

To conclude, we know that the embeddings of $K(\alpha)$ into $\bar{\mathbb{Q}}$ which fix K are determined by the roots of α, and we know that there are exactly m distinct such roots (Lemma 1.6). We further know (see Proposition 1.7) that each of these embeddings can be extended into an embedding of L into $\bar{\mathbb{Q}}$ in exactly k ways. Thus

$$\begin{aligned} \mathrm{N}_{L/K}(\alpha) &= \prod_{i=1}^{n} \sigma_i(\alpha), \\ \mathrm{Tr}_{L/K}(\alpha) &= \sum_{i=1}^{n} \sigma_i(\alpha), \end{aligned}$$

which concludes the proof. □

Example 1.6. Consider the field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. It has two embeddings

$$\sigma_1 : a + b\sqrt{2} \mapsto a + b\sqrt{2}, \ \sigma_2 : a + b\sqrt{2} \mapsto a - b\sqrt{2}.$$

Take the element $\alpha = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. Its two conjugates are $\sigma_1(\alpha) = \alpha = a + b\sqrt{2}$, $\sigma_2(\alpha) = a - b\sqrt{2}$, thus its norm is given by

$$\mathrm{N}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = a^2 - 2b^2,$$

while its trace is

$$\mathrm{Tr}_{\mathbb{Q}(\sqrt{2})/\mathbb{Q}}(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha).$$

It of course gives the same answer as what we computed in Example 1.4.

Example 1.7. Consider again the field extension $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Take the element $\alpha = a+b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, whose characteristic polynomial is given by, say, $\chi(X) = p_0 + p_1X + p_2X^2$. Thus $\chi(\alpha) = p_0 + p_1(a + b\sqrt{2}) + p_2(a^2 + 2ab\sqrt{2} + 2b^2) = (p_0 + p_1a + p_2a^2 + p_2 2b^2) + (p_1b + p_2 2ab)\sqrt{2}$, and

$$\mu_{\chi(\alpha)} = \begin{pmatrix} p_0 + p_1a + p_2a^2 + p_2 2b^2 & 2bp_1 + 4p_2ab \\ p_1b + p_2 2ab & p_0 + p_1a + p_2a^2 + p_2 2b^2 \end{pmatrix}$$

(see Example 1.4). On the other hand, we have that

$$\chi(\mu_\alpha) = p_0 I + p_1 \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} + p_2 \begin{pmatrix} a & 2b \\ b & a \end{pmatrix}^2.$$

Thus we have that $\mu_{\chi(\alpha)} = \chi(\mu_\alpha)$.

Example 1.8. Consider the number field extensions $\mathbb{Q} \subset \mathbb{Q}(i) \subset \mathbb{Q}(i, \sqrt{2})$. There are four embeddings of $\mathbb{Q}(i, \sqrt{2})$, given by

$$\begin{array}{lll} \sigma_1 : & i \mapsto i, & \sqrt{2} \mapsto \sqrt{2} \\ \sigma_2 : & i \mapsto -i, & \sqrt{2} \mapsto \sqrt{2} \\ \sigma_3 : & i \mapsto i, & \sqrt{2} \mapsto -\sqrt{2} \\ \sigma_4 : & i \mapsto -i, & \sqrt{2} \mapsto -\sqrt{2} \end{array}$$

We have that

$$N_{\mathbb{Q}(i)/\mathbb{Q}}(a + ib) = \sigma_1(a + ib)\sigma_2(a + ib) = a^2 + b^2,\ a, b \in \mathbb{Q}$$

but

$$\begin{aligned} N_{\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}}(a + ib) &= \sigma_1(a + ib)\sigma_2(a + ib)\sigma_3(a + ib)\sigma_4(a + ib) \\ &= \sigma_1(a + ib)\sigma_2(a + ib)\sigma_1(a + ib)\sigma_2(a + ib) \\ &= \sigma_1(a + ib)^2\sigma_2(a + ib)^2 \\ &= (a^2 + b^2)^2 \end{aligned}$$

since $a, b \in \mathbb{Q}$.

Corollary 1.10. *Let K be a number field, and let $\alpha \in K$ be an algebraic integer. The norm and the trace of α belong to $\mathbb{Z}$.*

Proof. The characteristic polynomial $\chi_{K/\mathbb{Q}}(X)$ is a power of the minimal polynomial (see inside the proof of the above theorem), thus it belongs to $\mathbb{Z}[X]$. □

Corollary 1.11. *The norm $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ of an element α of $\mathcal{O}_K$ is equal to ± 1 if and only if α is a unit of $\mathcal{O}_K$.*

Proof. Let α be a unit of $\mathcal{O}_K$. We want to prove that its norm is ± 1. Since α is a unit, we have that by definition $1/\alpha \in \mathcal{O}_K$. Thus

$$1 = \mathrm{N}_{K/\mathbb{Q}}(1) = \mathrm{N}_{K/\mathbb{Q}}(\alpha)\mathrm{N}_{K/\mathbb{Q}}(1/\alpha)$$

by multiplicativity of the norm. By the above corollary, both $\mathrm{N}_{K/\mathbb{Q}}(\alpha)$ and its inverse belong to $\mathbb{Z}$, meaning that the only possible values are ± 1.

Conversely, let us assume that $\alpha \in \mathcal{O}_K$ has norm ± 1, which means that the constant term of its minimal polynomial $f(X)$ is ± 1:

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots \pm 1.$$

Let us now consider $1/\alpha \in K$. We see that $1/\alpha$ is a root of the monic polynomial

$$g(X) = 1 + a_{n-1}X + \cdots \pm X^n,$$

with $g(X) \in \mathbb{Z}[X]$. Thus $1/\alpha$ is an algebraic integer. □

Let us prove a last result on the structure of the ring of integers. Recall that a group G is finitely generated if there exist finitely many elements $x_1, \ldots, x_s \in G$ such that every $x \in G$ can be written in the form $x = n_1x_1 + \ldots + n_sx_s$, with $n_1, \ldots, n_s$ integers. Such a group is called free if it is isomorphic to $\mathbb{Z}^r$, $r \geq 0$, called the rank of G. We now prove that $\mathcal{O}_K$ is not only a ring, but it is furthermore a free Abelian group of rank the degree of the corresponding number field.

Proposition 1.12. *Let K be a number field. Then $\mathcal{O}_K$ is a free Abelian group of rank $n = [K : \mathbb{Q}]$.*

Proof. We know by Corollary 1.5 that there exists a $\mathbb{Q}$-basis $\{\alpha_1, \ldots, \alpha_n\}$ of K with $\alpha_i \in \mathcal{O}_K$ for $i = 1, \ldots, n$ (take a basis of K with elements in K, and multiply the elements by the proper factors to obtain elements in $\mathcal{O}_K$ as explained in Corollary 1.5). Thus, an element $x \in \mathcal{O}_K$ can be written as

$$x = \sum_{i=1}^{n} c_i\alpha_i, \ c_i \in \mathbb{Q}.$$

Our goal is now to show that the denominators of c_i are bounded for all c_i and all $x \in \mathcal{O}_K$. To prove this, let us assume by contradiction that this is not the case, that is, that there exists a sequence

$$x_j = \sum_{i=1}^{n} c_{ij}\alpha_i, \ c_{ij} \in \mathbb{Q}$$

such that the greatest denominator of c_{ij}, $i = 1, \ldots, n$ goes to infinity when $j \to \infty$. Let us look at the norm of such an x_j. We know that $N_{K/\mathbb{Q}}(x_j)$ is the determinant of an $n \times n$ matrix with coefficients in $\mathbb{Q}[c_{ij}]$ (that is coefficients are $\mathbb{Q}$-linear combinations of c_{ij}). Thus the norm is a homogeneous polynomial

in c_{ij}, whose coefficients are determined by the field extension considered. Furthermore, it belongs to $\mathbb{Z}$ (Corollary 1.10). Since the coefficients are fixed and the norm is in $\mathbb{Z}$, the denominators of c_{ij} cannot grow indefinitely. They have to be bounded by a given constant B. Thus we have shown that

$$\mathcal{O}_K \subset \frac{1}{B} \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i.$$

Since the right hand side is a free Abelian group, $\mathcal{O}_K$ is free. Furthermore, $\mathcal{O}_K$ contains n elements which are linearly independent over $\mathbb{Q}$, thus the rank of $\mathcal{O}_K$ is n. □

Example 1.9. Let ζ_p be a primitive pth root of unity. One can show that the ring of integers of $\mathbb{Q}(\zeta_p)$ is

$$\mathbb{Z}[\zeta_p] = \mathbb{Z} \oplus \mathbb{Z}\zeta_p \cdots \oplus \mathbb{Z}\zeta_p^{p-2}.$$

Proposition 1.13. *Let K be a number field. Let $\alpha \in K$. If α is the zero of a monic polynomial f with coefficients in $\mathcal{O}_K$, then $\alpha \in \mathcal{O}_K$. We say that $\mathcal{O}_K$ is integrally closed.*

Proof. Let us write $f(X) = X^m + a_{m-1}X^{m-1} + \ldots + a_0$, with $a_i \in \mathcal{O}_K$. We know by the above proposition that $\mathcal{O}_K$ is a free abelian group which is finitely generated. Since

$$\alpha^m = -a_{m-1}\alpha^{m-1} - \cdots - a_0,$$

we have that $\mathcal{O}_K[\alpha]$ is finitely generated as Abelian group. Thus $\mathbb{Z}[\alpha] \subset \mathcal{O}_K[\alpha]$ is also finitely generated, and α is an algebraic integer by Theorem 1.3. □

The main definitions and results of this chapter are

- Definition of a number field K of degree n and its ring of integers $\mathcal{O}_K$.
- Properties of $\mathcal{O}_K$: it is a ring with a $\mathbb{Z}$-basis of n elements, and it is integrally closed.
- The fact that K has n embeddings into $\mathbb{C}$.
- Definition of norm and trace, with their characterization as respectively product and sum of the conjugates.