of *some* monic polynomial in $\mathbb{Z}[x]$, a condition which seems difficult to check. The next proposition gives a simple criterion for α to be an algebraic integer in terms of the minimal polynomial for α.

Proposition 28. An element α in some field extension of $\mathbb{Q}$ is an algebraic integer if and only if α is algebraic over $\mathbb{Q}$ and its minimal polynomial $m_{\alpha,\mathbb{Q}}(x)$ has integer coefficients. In particular, the algebraic integers in $\mathbb{Q}$ are the integers $\mathbb{Z}$, i.e., $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$.

Proof: If α is algebraic over $\mathbb{Q}$ with $m_{\alpha,\mathbb{Q}}(x) \in \mathbb{Z}[x]$, then by definition α is integral over $\mathbb{Z}$. Conversely, assume α is integral over $\mathbb{Z}$, and let $f(x)$ be a monic polynomial in $\mathbb{Z}[x]$ of minimum degree having α as a root. If f were reducible in $\mathbb{Q}[x]$, then by Gauss' Lemma $f(x) = g(x)h(x)$ for some monic polynomials $g(x)$, $h(x)$ in $\mathbb{Z}[x]$ of degree smaller than the degree of f. But then α would be a root of either g or h, contradicting the minimality of f. Hence f is irreducible in $\mathbb{Q}[x]$, so $f(x) = m_{\alpha,\mathbb{Q}}(x)$ and so the minimal polynomial for α has coefficients in $\mathbb{Z}$. Finally, the minimal polynomial of $\alpha = a/b \in \mathbb{Q}$ (a/b reduced to lowest terms and $b > 0$) is $bx - a$, which is monic if and only if $b = 1$, so $\alpha \in \mathbb{Q}$ is an algebraic integer if and only if $\alpha \in \mathbb{Z}$.

Because the integers $\mathbb{Z}$ are the algebraic integers in $\mathbb{Q}$, for emphasis (and clarity) the elements of $\mathbb{Z}$ are sometimes referred to as the "rational integers" to distinguish them from the "integers" in extensions of finite degree over $\mathbb{Q}$ (called *number fields*). The next result gives some of the basic structure of the ring of integers in a general number field.

Theorem 29. Let K be a number field of degree n over $\mathbb{Q}$.

(1) The ring $\mathcal{O}_K$ of integers in K is a Noetherian ring and is a free $\mathbb{Z}$-module of rank n.

(2) For every $\beta \in K$ there is some nonzero $d \in \mathbb{Z}$ such that $d\beta$ is an algebraic integer. In particular, K is the field of fractions of $\mathcal{O}_K$.

(3) If $\beta_1, \beta_2, \ldots, \beta_n$ is any $\mathbb{Q}$-basis of K, then there is an integer d such that $d\beta_1, d\beta_2, \ldots, d\beta_n$ is a basis for a free $\mathbb{Z}$-submodule of $\mathcal{O}_K$ of rank n. Any basis of the $\mathbb{Z}$-module $\mathcal{O}_K$ is also a basis for K as a vector space over $\mathbb{Q}$.

Proof: Note first that any $\mathbb{Z}$-linear dependence relation among elements in $\mathcal{O}_K$ is a $\mathbb{Q}$-linear dependence relation in K, and multiplying a $\mathbb{Q}$-linear dependence relation of elements of $\mathcal{O}_K$ in K by a common denominator for the coefficients yields a $\mathbb{Z}$-linear dependence relation in $\mathcal{O}_K$. Let β be any element of K and let $x^k + a_{k-1}x^{k-1} + \cdots + a_0$ be the minimal polynomial of β over $\mathbb{Q}$. If d is a common denominator for the coefficients, then multiplying through by d^k shows that

$$(d\beta)^k + da_{k-1}(d\beta)^{k-1} + \cdots + d^{k-1}a_1(d\beta) + d^k a_0 = 0,$$

and $d^k a_0, d^{k-1}a_1, \ldots, da_{k-1} \in \mathbb{Z}$. Hence $d\beta$ is an algebraic integer, which proves the first part of (2) and then the second statement in (2) follows immediately.

If $\beta_1, \ldots, \beta_n$ are a $\mathbb{Q}$-basis for K over $\mathbb{Q}$, then there is a nonzero integer d such that $d\beta_1, \ldots, d\beta_n$ all lie in $\mathcal{O}_K$. These elements are still linearly independent over $\mathbb{Q}$, so in particular are independent over $\mathbb{Z}$, hence generate a free submodule of $\mathcal{O}_K$ of rank n,

which proves the first statement in (3).

Since $\mathcal{O}_K$ is a subring of the field K, it is a torsion free $\mathbb{Z}$-module. If $\mathcal{O}_K$ were contained in some finitely generated $\mathbb{Z}$-module it would follow that $\mathcal{O}_K$ is also finitely generated over $\mathbb{Z}$, hence is a free $\mathbb{Z}$-module. If L is the Galois closure of K, then $\mathcal{O}_K \subseteq \mathcal{O}_L$ and so it suffices to see that $\mathcal{O}_L$ is contained in a finitely generated $\mathbb{Z}$-module. Let $\alpha_1, \ldots, \alpha_m$ be a $\mathbb{Q}$-basis for L. Multiplying by an integer $d \in \mathbb{Z}$, if necessary, we may assume that each α_i is an algebraic integer, i.e., $\alpha_1, \ldots, \alpha_m \in \mathcal{O}_L$. For each fixed $\theta \neq 0$ in L, the map

$$T_\theta : L \to \mathbb{Q} \quad \text{defined by} \quad T_\theta(\alpha) = \mathrm{Tr}_{L/\mathbb{Q}}(\theta\alpha)$$

(where $\mathrm{Tr}_{L/\mathbb{Q}}$ denotes the trace map from L to $\mathbb{Q}$, cf. Exercise 18 in Section 14.2) is a $\mathbb{Q}$-linear transformation from L to $\mathbb{Q}$. This linear transformation is nonzero because $T_\theta(\theta^{-1}) = \mathrm{Tr}_{L/\mathbb{Q}}(1) = m$. It follows that the map from L to $\mathrm{Hom}_{\mathbb{Q}}(L, \mathbb{Q})$ mapping θ to T_θ is an injective homomorphism of vector spaces over $\mathbb{Q}$. Since both spaces have the same dimension over $\mathbb{Q}$, the map is an isomorphism. Put another way, every linear functional on L is of the form T_θ for some $\theta \in L$. In particular, there are elements $\alpha_1', \ldots, \alpha_m'$ in L whose corresponding linear transformations $T_{\alpha_i'}$ give the dual basis of $\alpha_1, \ldots, \alpha_m$, i.e.,

$$\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i'\alpha_j) = \begin{cases} 1, & \text{if } i = j \\ 0, & \text{otherwise.} \end{cases}$$

Since $\alpha_1', \ldots, \alpha_m'$ are linearly independent, they give a basis for L over $\mathbb{Q}$. Hence every element $\beta \in \mathcal{O}_L$ can be written

$$\beta = a_1\alpha_1' + \cdots + a_i\alpha_i' + \cdots + a_m\alpha_m'$$

with $a_1, \ldots, a_m \in \mathbb{Q}$. Multiplying by α_j and taking the trace shows that

$$\mathrm{Tr}_{L/\mathbb{Q}}(\beta\alpha_j) = a_1\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_1'\alpha_j) + \cdots + a_i\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_i'\alpha_j) + \cdots + a_m\mathrm{Tr}_{L/\mathbb{Q}}(\alpha_m'\alpha_j) = a_j.$$

But β and α_j are both elements of $\mathcal{O}_L$, so also $\beta\alpha_j$ is an element of $\mathcal{O}_L$, and this implies that $a_j = \mathrm{Tr}_{L/\mathbb{Q}}(\beta\alpha_j)$ is an element of $\mathbb{Z}$ (cf. Exercise 18(d) of Section 14.2). It follows that

$$\mathcal{O}_L \subseteq \mathbb{Z}\alpha_1' + \cdots + \mathbb{Z}\alpha_m'$$

so that $\mathcal{O}_L$ is contained in a finitely generated $\mathbb{Z}$-module, proving that $\mathcal{O}_K$ (and also $\mathcal{O}_L$) is a free $\mathbb{Z}$-module.

Since K has dimension n as a vector space over $\mathbb{Q}$, it follows that $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank at most n (by Theorem 5 of Section 12.1). Because $\mathcal{O}_K$ also contains a free $\mathbb{Z}$-submodule of rank n, it follows that the $\mathbb{Z}$-rank of $\mathcal{O}_K$ is precisely n, proving (1), and then the second statement in (3) follows by the remarks on $\mathbb{Z}$-linear and $\mathbb{Q}$-linear dependence relations.

Finally, any ideal I in $\mathcal{O}_K$ is a $\mathbb{Z}$-submodule of a free $\mathbb{Z}$-module of rank n, so is a free $\mathbb{Z}$-module of rank at most n, and a set of $\mathbb{Z}$-module generators for I is also a set of $\mathcal{O}_K$-generators. Hence every ideal of $\mathcal{O}_K$ can be generated by at most n elements, which implies that $\mathcal{O}_K$ is a Noetherian ring and completes the proof.

Definition. An *integral basis* for the number field K is a basis of the ring of integers in K considered as a free $\mathbb{Z}$-module of rank $[K : \mathbb{Q}]$.

If P is a nonzero prime ideal in the ring of integers $\mathcal{O}_K$ of a number field K then $P \cap \mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. If $\alpha \in P$, then the constant term of the minimal polynomial for α over $\mathbb{Q}$ is then an element in $P \cap \mathbb{Z}$, which shows that $P \cap \mathbb{Z} = p\mathbb{Z}$ is also a nonzero prime ideal in $\mathbb{Z}$. By Theorem 26, every prime ideal (p) in $\mathbb{Z}$ arises in this way. Since $p\mathbb{Z}$ is a maximal ideal, it also follows from (2) in Theorem 26 that *nonzero prime ideals in $\mathcal{O}_K$ are maximal*, and then by Corollary 27, there are finitely many prime ideals P in $\mathcal{O}_K$ with $P \cap \mathbb{Z} = p\mathbb{Z}$. We shall see later (Corollary 16 in Section 16.3) that *every nonzero ideal in the ring of integers of a number field can be written uniquely as the product of prime ideals*, and in the case of the ideal $p\mathcal{O}_K$ the distinct prime factors are precisely the finitely many ideals P in $\mathcal{O}_K$ with $P \cap \mathbb{Z} = p\mathbb{Z}$. This property replaces the unique factorization of *elements* in $\mathcal{O}_K$ into primes (which need not hold since $\mathcal{O}_K$ *need not be a U.F.D.*). We shall also see that primary ideals in $\mathcal{O}_K$ are powers of prime ideals (in fact this is equivalent to the unique factorization of ideals of $\mathcal{O}_K$ into products of prime ideals, cf. the exercises).

Example: (The Ring of Integers in Quadratic Extensions of $\mathbb{Q}$)

If K is a quadratic extension of $\mathbb{Q}$ then $K = \mathbb{Q}(\sqrt{D})$ for some squarefree integer D. Then

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \omega,$$

with integral basis $1, \omega$, where

$$\omega = \begin{cases} \sqrt{D}, & \text{if } D \equiv 2, 3 \bmod 4 \\ \dfrac{1+\sqrt{D}}{2}, & \text{if } D \equiv 1 \bmod 4. \end{cases}$$

This is the quadratic integer ring introduced in Section 7.1. Since ω satisfies $\omega^2 - D = 0$ (respectively, $\omega^2 - \omega + (1 - D)/4$) for $D \equiv 2, 3 \bmod 4$ (respectively, $D \equiv 1 \bmod 4$), it follows that ω is an algebraic integer in K and so $\mathbb{Z}[\omega] \subseteq \mathcal{O}_K$. To prove that this is the full ring of integers in K, let $\alpha = a + b\sqrt{D}$ with $a, b \in \mathbb{Q}$, and suppose that α is an algebraic integer. If $b = 0$, then $\alpha \in \mathbb{Q}$ and so $a \in \mathbb{Z}$. If $b \neq 0$, the minimal polynomial of α is $x^2 - 2ax + (a^2 - b^2D)$. Then Proposition 28 shows that $2a$ and $a^2 - b^2D$ are elements of $\mathbb{Z}$. Then $4(a^2 - b^2D) = (2a)^2 - (2b)^2D \in \mathbb{Z}$, hence $4b^2D \in \mathbb{Z}$. Since D is squarefree it follows that $2b$ is an integer. Write $a = x/2$ and $b = y/2$ for some integers x, y. Since $a^2 - b^2D$ is an integer, $x^2 - y^2D \equiv 0 \pmod 4$. Since 0 and 1 are the only squares mod 4 and D is not divisible by 4, it is easy to check that the only possibilities are the following:

(i) $D \equiv 2$ or $3 \pmod 4$ and x, y are both even, or

(ii) $D \equiv 1 \pmod 4$ and x, y are both even or both odd.

In case (i), $a, b \in \mathbb{Z}$ and $\alpha \in \mathbb{Z}[\omega]$. In case (ii), $a + b\sqrt{D} = r + s\omega$ where $r = (x - y)/2$ and $s = y$ are both integers, so again $\alpha \in \mathbb{Z}[\omega]$.

Example: (The Ring of Integers in Cyclotomic Fields)

The ring of integers in the cyclotomic field $\mathbb{Q}(\zeta_n)$ of n^{th} roots of unity is $\mathbb{Z}[\zeta_n]$, where ζ_n is any primitive n^{th} root of 1. The elements $1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}$ are an integral basis. It is clear that ζ_n is an algebraic integer since it is a root of $x^n - 1$, so the ring $\mathbb{Z}[\zeta_n]$ is contained in the ring of integers. The proof that this is the full ring of algebraic integers in $\mathbb{Q}(\zeta_n)$ involves techniques from algebraic number theory beyond the scope of the material here.