Let F be a number field and let $\alpha \in F$ be an algebraic integer for which $F = \mathbf{Q}(\alpha)$. We describe a criterion, due to Dedekind, for $\mathbf{Z}[\alpha]$ to be the ring of integers of F. We start with a local theorem.

Proposition 1. *Let A be a 1-dimensional local Noetherian domain with maximal ideal $\mathfrak{m}$. Then the following are equivalent*
(a) A is a PID;
(b) A is integrally closed;
(c) $\mathfrak{m}$ is principal;
(d) $\mathfrak{m}/\mathfrak{m}^2$ is a 1-dimensional $A/\mathfrak{m}$-vector space.

Proof. (a) $\Rightarrow$ (b). Let $x \in \mathrm{Frac}(A)$ be integral over A. Write $x = r/s$ with $r, s \in A$ having gcd 1. Let $f = X^n + \ldots + a_1 X + a_0 \in A[X]$ vanish in r/s. Then we have $r^n + \ldots + a_1 r s^{n_1} + a_0 s^n = 0$. So s divides r^n. Since s and r^n are coprime, it follows that s is a unit and $x = r/s$ is in A.

(b) $\Rightarrow$ (c). Since $\dim A = 1$, its maximal ideal is not zero. Let $0 \neq x \in \mathfrak{m}$. Since the only prime ideal of $A/(x)$ is $\mathfrak{m}/(x)$, it is also its nilradical. The fact that A is Noetherian implies then that $\mathfrak{m}^n \subset (x)$ for some $n > 0$. Let n be minimal with this property and choose $y \in \mathfrak{m}^{n-1} - (x)$. Then we have $y\mathfrak{m} \subset \mathfrak{m}^n \subset (x)$ and hence $(y/x)\mathfrak{m}$ is an ideal of A. Since $y/x \notin A$, it is not integral over A. Since $\mathfrak{m}$ is finitely generated, this implies $(y/x)\mathfrak{m} \not\subset \mathfrak{m}$. It follows that $(y/x)\mathfrak{m} = A$ and hence also $\mathfrak{m} = (x/y)$.

(c) $\Leftrightarrow$ (d). In one direction this is obvious. In the other direction this follows from Nakayama's lemma.

(c) $\Rightarrow$ (a). Let $I \subset A$ be an ideal that is neither A or (0). Then we have $I \subset \mathfrak{m}$. Let $\mathfrak{m} = (\pi)$ for some $\pi \in A$. Since $\mathfrak{m}/I$ is the only prime ideal of A/I, we have $\pi^n \in I$ for some n. For every $k \geq 0$ multiplication by π^k induces an isomorphism $A/\mathfrak{m} \cong \mathfrak{m}^k/\mathfrak{m}^{k+1}$. IN particolar, $\mathfrak{m}^{k+1}$ is strictly smaller than $\mathfrak{m}^k$. This implies that there is a maximal n for which $I \subset \mathfrak{m}^n$. Let $x \in I - \mathfrak{m}^{n+1}$. Then $x = u\pi^n$ for some $u \in A$. Since we have $x \notin \mathfrak{m}^{n+1}$, the element u is a unit. The ideal I is generated by x. Indeed, for $y \in I$ we have $y = v\pi^n = vu^{-1}x$ for some $v \in A$.

This proves the proposition.

Lemma 2. *Let A be a 1-dimensional Noetherian domain and let $\mathfrak{p}$ be a prime ideal of A. Let $\mathfrak{q} = \mathfrak{p}A_\mathfrak{p}$ denote the maximal ideal of the local ring $A_\mathfrak{p}$. Then $A_\mathfrak{p}$ is Noetherian and 1-dimensional. The natural maps $A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{q}$ and $\mathfrak{p}/\mathfrak{p}^2 \to \mathfrak{q}/\mathfrak{q}^2$ are bijective.*

Proof. Since $I = (I \cap A)A_\mathfrak{p}$ for every ideal I of $A_\mathfrak{p}$, it is clear that $A_\mathfrak{p}$ is Noetherian. To see that $A_\mathfrak{p}$ has Krull dimension 1, let $\mathfrak{q} \subset A_\mathfrak{p}$ be a non-zero prime ideal. Then $\mathfrak{q} \subset \mathfrak{p}A_\mathfrak{p}$ and $\mathfrak{q} \cap A$ is a non-zero prime ideal of A containing $\mathfrak{p}$. Therefore it is equal to $\mathfrak{p}$. This implies that $\mathfrak{q}$ is also maximal. Indeed, the natural map $A/\mathfrak{p} \to A_\mathfrak{p}/\mathfrak{q}$ is an isomorphism. Similarly, the map $\mathfrak{p}/\mathfrak{p}^2 \to \mathfrak{q}/\mathfrak{q}^2$ is an isomorphism of $A/\mathfrak{p}$-vector spaces.

Corollary 3. *Let A be a 1-dimensional Noetherian domain. Then A is integrally closed (and hence is a Dedekind domain) if and only if $\mathfrak{p}/\mathfrak{p}^2$ is a 1-dimensional $A/\mathfrak{p}$-vector space for every non-zero prime ideal $\mathfrak{p}$ of A.*

Proof. If A is integrally closed so are its localizations $A_{\mathfrak{p}}$ and we apply Proposition 1 and Lemma 2. Conversely, suppose that $x \in \mathrm{Frac}(A)$ is integral over A. By Proposition 1, the ring $A_{\mathfrak{p}}$ is integrally closed and we have $x \in A_{\mathfrak{p}}$. Writing $x = r/s$ with $r, s \in A$, we have therefore for every maximal ideal $\mathfrak{p}$ that $rv = us$ for certain $u, v \in A$ with $v \notin \mathfrak{p}$. The A-ideal generated by the various v is equal to A. It follows that that s divides r and hence $x = r/s$ is in A. This proves the corollary.

Finally we specialize to ring of the form $\mathbf{Z}[\alpha]$. Here α is an algebraic integer with minimum polynomial $f \in \mathbf{Z}[X]$. The ring $\mathbf{Z}[\alpha]$ is contained in the ring of integers O_F of $F = \mathbf{Q}(\alpha)$. Evaluating in α induces a ring isomorphism $\mathbf{Z}[X]/(f) \cong \mathbf{Z}[\alpha]$. The non-zero prime ideals of $\mathbf{Z}[\alpha]$ are maximal. They have the form $\mathfrak{p} = (p, \phi(\alpha)$, where p is a prime and $\phi \in \mathbf{F}_p[X]$ is an irreducible divisor of f. The counterimage of $\mathfrak{p}$ in $\mathbf{Z}[X]$ is the maximal ideal $(p, \phi(X))$. It follows from the Nulstellensatz that every maximal ideal of $\mathbf{Z}[X]$ is of this form.

Proposition 4. *Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial and let α be a zero of f. Let p be a prime and let $\phi \in \mathbf{F}_p[X]$ be an irreducible divisor of f. Put $\mathfrak{p} = (p, \phi(\alpha))$ and $\mathfrak{m} = (p, \phi(X))$. Then the following are equivalent:*
(a) $f \in \mathfrak{m}^2$;
(b) $f \equiv \phi^2\psi$ modulo p for some $\psi \in \mathbf{Z}[X]$ and ϕ divides $(f - \phi^2\psi)/p$;
(c) The dimension of the $\mathbf{Z}[\alpha]/\mathfrak{p}$-vector space $\mathfrak{p}/\mathfrak{p}^2$ is not 1.

Proof. The natural maps $\mathbf{Z}[X]/\mathfrak{m} \to \mathbf{Z}[\alpha]/\mathfrak{p}$ and $\mathfrak{m}/(\mathfrak{m}^2 + (f)) \to \mathfrak{p}/\mathfrak{p}^2$ are bijective. Since $\mathfrak{m}/\mathfrak{m}^2$ has dimension 2 over $\mathbf{Z}[X]/\mathfrak{m}$, this implies that (a) and (c) are equivalent. Condition (a) means that $f = gp^2 + hp\phi + \psi\phi^2$ for certain polynomials $g, h, \psi \in \mathbf{Z}[X]$. It follows that ϕ^2 divides $f \pmod p$ and that ϕ divides $(f - \phi^2\psi)/p \pmod p$. In other words, (b) holds. Conversely, if the conditions in (b) hold, we must have $f \in \mathfrak{m}^2$. This proves Proposition 4.

Corollary 5. *If f is Eisenstein at p, then $\mathfrak{p} = (p, \alpha)$ is the unique prime of $\mathbf{Z}[\alpha]$ dividing p and the local ring $\mathbf{Z}[\alpha]_{\mathfrak{p}}$ is integrally closed.*

Proof. We may assume that $d = \deg f$ is at least 1. We have $f \equiv X^d \pmod p$. Put $\phi = X$ and $\psi = \phi^{d-2}$. Then ϕ^2 divides f modulo p. However, by the Eisenstein condition the polynomial $(f - \phi^2\psi)/p$ has constant term prime to p. Therefore it is not divisible by X in the ring $\mathbf{F}_p[X]$. By Proposition 4 the $\mathbf{F}_p$-dimension of $\mathfrak{p}/\mathfrak{p}^2$ is 1. So Proposition 1 and Lemma 2 imply the result.

Corollary. *(Dedekind criterion) Let $f \in \mathbf{Z}[X]$ be a monic irreducible polynomial and let α denote a zero of f. Put $F = \mathbf{Q}(\alpha)$. Then the following are equivalent*
(a) we have $\mathbf{Z}[\alpha] = O_F$.
(b) $f \notin \mathfrak{m}^2$ for all maximal ideals $\mathfrak{m}$ of $\mathbf{Z}[X]$;
(c) For all primes p and for every irreducible polynomial $\phi \in \mathbf{F}_p[X]$ for which $f = \phi^2\psi$ in $\mathbf{F}_p[X]$, we have

$$\phi \quad \textit{does not divide} \quad \frac{f - \phi^2\psi}{p};$$