Exercise 1 (Gauss Lemma)**.** Let A be a principal ideal domain, and K its fraction field. When $P \in A[X]$ is a polynomial, we define its *content* $\mathrm{cont}(P)$ as the ideal generated in A by its coefficients.

(i) Let $R \in A[X]$. Show that there exists $\alpha \in A$ and $\widetilde{R} \in A[X]$ such that $\mathrm{cont}(R) = \alpha A$ and $R = \alpha\widetilde{R}$.

(ii) Let $P, Q \in A[X]$ be such that $\mathrm{cont}(P) = \mathrm{cont}(Q) = A$. Show that $\mathrm{cont}(PQ) = A$. (Hint: Consider a prime ideal $\mathfrak{p}$ of A, and show that $PQ \notin \mathfrak{p}A[X]$.)

(iii) Let $P, Q \in A[X]$. Show that $\mathrm{cont}(PQ) = \mathrm{cont}(P)\,\mathrm{cont}(Q)$.

(iv) Let K be the fraction field of A, and $P \in A[X]$ be such that $\mathrm{cont}(P) = A$. Deduce that P is irreducible in $A[X]$ if and only if it is irreducible in $K[X]$.

Exercise 2. Let A be an integrally closed domain with fraction field K. Let L/K be a finite field extension. Consider an element $\alpha \in L$, and let $P \in K[X]$ be its minimal polynomial over K. Show that α is integral over A if and only if $P \in A[X]$.

Exercise 3. Let $a, b \in \mathbb{Q}$ be such that the polynomial $P = X^n + aX + b$ is irreducible in $\mathbb{Q}[X]$. Let $\alpha \in \mathbb{C}$ be a root of P, and $K = \mathbb{Q}(\alpha)$. Show that

$$\mathrm{D}_{K/\mathbb{Q}}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}}(n^n b^{n-1} + a^n(1-n)^{n-1}).$$

Exercise 4. Let $P = X^3 + X + 1 \in \mathbb{Z}[X]$.

(i) Show that the polynomial P is irreducible in $\mathbb{Q}[X]$.

(ii) Let $\alpha \in \mathbb{C}$ be a root of P, and consider the subfield $K = \mathbb{Q}(\alpha) \subset \mathbb{C}$. Show that $[K : \mathbb{Q}] = 3$ and that $\alpha \in \mathcal{O}_K$.

(iii) Show that $(1, \alpha, \alpha^2)$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. (Hint: Use the previous exercise.)

Exercise 5. (Optional) Let $n \geq 2$ be an integer, and $\xi \in \mathbb{C}$ a primitive n-th root of unity. Let $P \in \mathbb{Q}[X]$ be the minimal polynomial of ξ over $\mathbb{Q}$. Let

$$\Phi_n = \prod_{k \in S}(X - \xi^k),$$

where $S \subset \{1, \ldots, n\}$ is the set of elements k with $\gcd(k, n) = 1$. We are going to prove that $P = \Phi_n$

We let p be prime number, and denote $Q \mapsto \overline{Q}$ the reduction modulo p map $\mathbb{Z}[X] \to \mathbb{F}_p[X]$. Let $F \in \mathbb{Q}[X]$ be the minimal polynomial of ξ^p over $\mathbb{Q}$.

(i) Show that $P, F \in \mathbb{Z}[X]$.

(ii) Show that $\overline{F}$ and $\overline{P}$ have a common irreducible divisor in $\mathbb{F}_p[X]$. (Hint: consider the polynomial $G = P(X^p) \in \mathbb{Z}[X]$.)

(iii) Assume that the prime number p does not divide n. Show that $F = P$.

(iv) Deduce that $\Phi_n \mid P$ in $\mathbb{Q}[X]$.

(v) Show that

$$\Phi_n = \prod_{d|n} \Phi_d$$

and deduce that $\Phi_n \in \mathbb{Z}[X]$.

(vi) Conclude.