1. *Let p be a prime. Show that $X^p - X \in \mathbf{F}_p[X]$ is separable, while $X^p - 1 \in \mathbf{F}_p[X]$ is not. How many zeroes do these polynomials have in $\mathbf{F}_p$?*

Sol.: Recall that by definition a polynomial is separable if all its zeros are distinct in any splitting field. Equivalently, if $\gcd(f, f') = 1$ (see Milne, Prop. 2.13). Since $f'(X) = pX^{p-1} - 1 = -1 \in \mathbf{F}_p[X]$, it is clear that $\gcd(f, f') = 1$ and f is separable. If we write $f(X) = X(X^{p-1} - 1)$, we see that the p elements of $\mathbf{F}_p$ are the distinct zeros of f in $\mathbf{F}_p$: by Little Fermat's theorem, one has in fact that $a^{p-1} - 1 = 0$, for every $a \in \mathbf{F}_p \setminus \{0\}$.
Since $g'(X) = pX^p = 0 \in \mathbf{F}_p[X]$, we have that $\gcd(g', g) = g \neq 1$. Hence g is not separable. One can also see directly that $g(X) = X^p - 1 = (X - 1)^p$ has 1 as a unique zero of multiplicity p.

2. *Let $n \geq 3$.*
   (a) Let α be a zero of $X^n - 1 \in \mathbf{Q}[X]$. Show that $\mathbf{Q}(\alpha)$ is a normal extension of $\mathbf{Q}$.
   (b) Let β be a zero of $X^n - 2 \in \mathbf{Q}[X]$. Show that $\mathbf{Q}(\beta)$ is not a normal extension of $\mathbf{Q}$.

Sol.: (a) Let α be a zero of $X^n - 1 \in \mathbf{Q}[X]$ and let d be its order. Then α is a primitive root of $X^d - 1$ and all other zeroes are powers of α. Therefore $\mathbf{Q}(\alpha)$ is a splitting field of the separable polynomial $X^d - 1$ and hence it is normal over $\mathbf{Q}$.
(b) For example take $\beta = \sqrt[n]{2}$. Then $\mathbf{Q}(\beta)$ is strictly contained in the splitting field of $f(X) = X^n - 2$, which is given by $\mathbf{Q}_f = \mathbf{Q}(\sqrt[n]{2}, \zeta_n)$, where ζ_n is a primitive n^{th} root of 1. Note that while $\mathbf{Q}(\sqrt[n]{2})$ can be embedded in $\mathbf{R}$, the field $\mathbf{Q}(\sqrt[n]{2}, \zeta_n)$ cannot.

3. *Let $\zeta_9 \in \mathbf{C}$ denote a primitive 9-th root of unity and let $\mathbf{F} = \mathbf{Q}(\zeta_9)$.*
   (a) Show that the factorization into irreducible factors of $x^9 - 1$ over $\mathbf{Q}$ is given by

$$(x^9 - 1) = (x - 1)(x^2 + x + 1)(x^6 + x^3 + 1).$$

   (b) Show that $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{F})$ is isomorphic to $\mathbf{Z}/9\mathbf{Z}^* \cong \mathbf{Z}/6\mathbf{Z}$.
   (c) Exhibit $\gamma \in \mathbf{F}$ so that $[\mathbf{Q}(\gamma) : \mathbf{Q}] = 3$.

Sol.: (a) The factor $x^2 + x + 1$ is irreducible over $\mathbf{Q}$ because it does not vanish in ± 1, which are the only potental rational roots. To check that $x^6 + x^3 + 1$ is irreducible, we perform the change of variable $x = y + 1$ and obtain

$$(y + 1)^6 + (y + 1)^3 + 1 = y^6 + 6y^5 + 15y^4 + 21y^3 + 18y^2 + 9y + 3.$$

By the Eisenstein criterion for $p = 3$, we can conclude that $y^6 + 6y^5 + 15y^4 + 21y^3 + 18y^2 + 9y + 3$ and therefore $x^6 + x^3 + 1$ is irreducible.
(b) Since ζ_9 is a zero of the degree 6 irreducible polynomial $x^6 + x^3 + 1$, we deduce that $[\mathbf{Q}(\zeta_9) : \mathbf{Q}] = 6$. The group $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{F}) = \mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}(\zeta_9), \mathbf{Q}(\zeta_9))$ is in 1-1 correspondence with the zeros of $x^6 + x^3 + 1$ in $\mathbf{Q}(\zeta_9)$, namely the powers of ζ_9 with exponent coprime with 9

$$\zeta_9,\ \zeta_9^2,\ \zeta_9^4,\ \zeta_9^5,\ \zeta_9^7,\ \zeta_9^8.$$

Each of the above zeros determines the automorphism $\phi_i(\zeta_9) = \zeta_9^i$ and an isomorphism $(\mathrm{Aut}_{\mathbf{Q}}(\mathbf{F}), \circ) \to (\mathbf{Z}/9\mathbf{Z}^*, \cdot)$ is given by $\phi_i \mapsto i$. One can check that $\phi_i \circ \phi_j \mapsto i \cdot j$.

(c) Consider the automorphism determined by $\phi_8(\zeta_9) = \zeta_9^8 = \overline{\zeta}_9$. Then ϕ_8 is an element of order two in $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{F})$. In fact $\phi_8(\phi_8(\zeta_9)) = \zeta_9^{64} = \zeta_9$. Denote by G the subgroup of $\mathrm{Aut}_{\mathbf{Q}}(\mathbf{F})$ generated by ϕ_8. Then $[\mathbf{Q}(\zeta_9) : \mathbf{Q}(\zeta_9)^G] = \#G = 2$ and $[\mathbf{Q}(\zeta_9)^G : \mathbf{Q}] = 3$. Now it is clear that as the element γ we can take $\zeta_9 + \overline{\zeta}_9$. It remains to observe that $\zeta_9 + \overline{\zeta}_9 = 2\cos 2\pi/9 \notin \mathbf{Q}$.

4. *Let R be the ring $\mathbf{Q}[X]/(X^4 + X + 1)$. For a polynomial $g(X) \in \mathbf{Q}[X]$, we write $\overline{g(X)}$ for its canonical image in R.*

(a) *Show that every element of R can be represented by a polynomial in $\mathbf{Q}[X]$ of degree ≤ 3.*

(b) *Let $g(X) = X^2+1$. Compute $\overline{g(X)}^2$ and represent the result by a polynomial in $\mathbf{Q}[X]$ of degree ≤ 3.*

Sol.: (a) Every element $f \in R$ can be represented by the remainder of the division of f by g, which is a polynomial in $\mathbf{Q}[X]$ of degree ≤ 3.

(b) One has $g(X)^2 = (X^2+1)(X^2+1) = X^4 + 2X^2 + 1$. Using the relation $X^4 = -1$, one obtains $\overline{g(X)^2} = -1 + 2X^2 + 1 = 2X^2$.