1. *Determine the degree of the splitting field of the polynomial* $f = x^4 - 2$ *over the following fields:*
$$\mathbf{C}, \quad \mathbf{R}, \quad \mathbf{Q}, \quad \mathbf{Q}(\sqrt{2}), \quad \mathbf{Q}(\sqrt[4]{2}).$$

Sol.: The polynomial f decomposes as

$$x^4 - 2 = (x^2 + \sqrt{2})(x^2 - \sqrt{2}) = (x + i\sqrt[4]{2})(x - i\sqrt[4]{2})(x + \sqrt[4]{2})(x - \sqrt[4]{2}).$$

(a) The splitting field is $\mathbf{C}_f = \mathbf{C}$ (all roots of f are already in $\mathbf{C}$) and $[\mathbf{C}_f : \mathbf{C}] = 1$;

(b) The splitting field is $\mathbf{R}_f = \mathbf{R}(\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}) = \mathbf{R}(i) = \mathbf{C}$ and $[\mathbf{C} : \mathbf{R}] = 2$;

(c) The splitting field $\mathbf{Q}_f = \mathbf{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbf{Q}(\sqrt[4]{2}, i)$.
Let's show that $\mathbf{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbf{Q}(\sqrt[4]{2}, i)$:
the inclusion $\mathbf{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) \subset \mathbf{Q}(\sqrt[4]{2}, i)$ is clear; to prove the opposite one it is sufficient to note that $i = i\sqrt[4]{2}/\sqrt[4]{2} \in \mathbf{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2})$.
The degree $[\mathbf{Q}_f : \mathbf{Q}] = 8$:
$[\mathbf{Q}_f : \mathbf{Q}] = [\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}(\sqrt[4]{2})][\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}]$, where $[\mathbf{Q}(\sqrt[4]{2}) : \mathbf{Q}] = 4$, because the polynomial $x^4 - 1$, which is the minimum polynomial of $\sqrt[4]{2}$ over $\mathbf{Q}$, irreducible over $\mathbf{Q}$, and $[\mathbf{Q}_f : \mathbf{Q}(\sqrt[4]{2})] = 2$, because the polynomial $x^2 + 1$, which is the minimum polynomial of i over $\mathbf{Q}(\sqrt[4]{2})$, is irreducible.

(d) One has $\sqrt{2} = (\sqrt[4]{2})^2$. Hence $\mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt[4]{2})$. Since $x^2 - \sqrt{2}$, which is the minimum polynomial of $\sqrt[4]{2}$ is irreducible over $\mathbf{Q}(\sqrt{2})$, the inclusion $\mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\sqrt[4]{2})$ is a quadratic extension. We already observed in (c) that $[\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}(\sqrt[4]{2})] = 2$. Then $[\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}(\sqrt{2})] = 4$.

(e) We already observed in (c) that $[\mathbf{Q}(\sqrt[4]{2}, i) : \mathbf{Q}(\sqrt[4]{2})] = 2$.

2. (a) *Show that there exist trascendental elements* $\alpha, \beta \in \mathbf{C}$ *such that their product is algebraic over* $\mathbf{Q}$.
   (b) *Show that there exist trascendental elements* $\alpha, \beta \in \mathbf{C}$ *such that both their sum is algebraic over* $\mathbf{Q}$.
   (c) *Let* $\alpha, \beta \in \mathbf{C}$ *have the property that both their sum and their product are algebraic over* $\mathbf{Q}$. *Show that* α *and* β *themselves are algebraic over* $\mathbf{Q}$.

Sol.: (a) $\alpha = \pi$ is a trascendental element over $\mathbf{Q}$ and so is $\beta = \pi^{-1}$. On the othet hand $\alpha/\beta = 1$ is algebraic over $\mathbf{Q}$.
(b) $\alpha = \pi$ is a trascendental element over $\mathbf{Q}$ and so is $\beta = -\pi$. On the othet hand $\alpha + \beta = 0$ is algebraic over $\mathbf{Q}$.
(c) The elements α and β are roots of the degree 2 polynomial $(x - \alpha)(x - \beta) = x^2 - (\alpha + \beta)x + \alpha\beta$. If $\alpha, \beta \in \mathbf{C}$ have the property that both their sum and their product are algebraic over $\mathbf{Q}$, then they are roots of a polynomial with algebraic coefficients, precisely in the finite degree extension $\mathbf{Q}(\alpha + \beta, \alpha\beta)$ of $\mathbf{Q}$. Then

$$\mathbf{Q} \subset \mathbf{Q}(\alpha + \beta, \alpha\beta) \subset \mathbf{Q}(\alpha + \beta, \alpha\beta)(\alpha, \beta)$$

is a chain of finite degree extensions and therefore algebraic. In particular, and α and β are themselves algebraic over $\mathbf{Q}$.

3. *Let* $\zeta_8 = e^{\frac{2\pi i}{8}} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2} \in \mathbf{C}$.
   (a) *Show that* ζ_8 *is a primitive 8-th root of unity and determine its minimum polynomial over* $\mathbf{Q}$.
   (b) *Show that* $\mathbf{Q}(i) \subset \mathbf{Q}(\zeta_8)$ *and that* $\mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\zeta_8)$.
   (c) *How many elements do the following sets have?*

$$\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}(\sqrt{2}), \mathbf{C}), \quad \mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}(\zeta_8), \mathbf{C}), \quad \mathrm{Hom}_{\mathbf{Q}(\sqrt{2})}(\mathbf{Q}(\zeta_8), \mathbf{C})$$

Sol.: (a) For simplicity set $\xi = \zeta_8$. All eight roots of 1, namely ± 1, $\pm i$, $\pm\frac{\sqrt{2}}{2} \pm i\frac{\sqrt{2}}{2}$ are powers of ξ:

$$\xi = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \quad \xi^2 = i, \quad \xi^3 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \quad \xi^4 = -1,$$

$$\xi^5 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \quad \xi^6 = -i, \quad \xi^7 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \quad \xi^8 = 1.$$

From the factorization $x^8 - 1 = (x^4+1)(x^2+1)(x+1)(x-1)$, it follows that ξ is a zero of x^4+1, which is irreducible over $\mathbf{Q}$. Hence x^4+1 is the minimum polynomial of ξ.
(b) From $\xi^2 = i$, it follows that $i \in \mathbf{Q}(\xi)$ and $\mathbf{Q}(i) \subset \mathbf{Q}(\xi)$;
from $\xi + \xi^7 = \sqrt{2}$, it follows that $\sqrt{2} \in \mathbf{Q}(\xi)$ and $\mathbf{Q}(\sqrt{2}) \subset \mathbf{Q}(\xi)$.
(c) $\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}(\sqrt{2}), \mathbf{C})$ is in 1-1 correspondence with the zeros of $x^2 - 2$ (the minimum polynomial of $\sqrt{2}$ over $\mathbf{Q}$) in $\mathbf{C}$. Hence it has 2 elements.
$\mathrm{Hom}_{\mathbf{Q}}(\mathbf{Q}(\zeta_8), \mathbf{C})$ is in 1-1 correspondence with the zeros of x^4+1 (the minimum polynomial of $\sqrt{2}$ over $\mathbf{Q}$) in $\mathbf{C}$. Hence it has 4 elements.
$\mathrm{Hom}_{\mathbf{Q}(\sqrt{2})}(\mathbf{Q}(\zeta_8), \mathbf{C})$ is in 1-1 correspondence with the zeros of $x^2 - \sqrt{2}x + 1$ (the minimum polynomial of ξ over $\mathbf{Q}(\sqrt{2})$) in $\mathbf{C}$. Hence it has 2 elements.

4. *Let* p *be a prime and let* $\mathbf{F}$ *be a field of characteristic* p.
   (a) *Show that* $\mathbf{F}^p = \{x^p : x \in \mathbf{F}\}$ *is a subfield of* $\mathbf{F}$.
   (b) *When* $\mathbf{F} = \mathbf{Z}/p\mathbf{Z}(x)$ *is the field of rational functions in the variable* x, *compute* $[\mathbf{F} : \mathbf{F}^p]$.

Sol.: (a) We need to show that $\mathbf{F}^p$ is closed for addition, multiplication and inverse:
by the "freshman's dream", one has $x^p + y^p = (x+y)^p$, proving that sum of p^{th} powers is a p^{th} power; also $-x^p = (-x)^p$, proving that the opposite of a p^{th} power is a p^{th} power;
$x^p y^p = (xy)^p$ shows that product of p^{th} powers is a p^{th} power; finally, $(x^p)^{-1} = x^{-p}$ shows that the multiplicative inverse of a p^{th} power is a p^{th} power.
(b) By definition $\mathbf{F} = \mathbf{Z}/p\mathbf{Z}(x) = \{\frac{f(x)}{g(x)},\ f, g \in \mathbf{Z}/p\mathbf{Z}[x]\}$ and $\mathbf{F}^p = \{\frac{f(x)^p}{g(x)^p},\ f, g \in \mathbf{Z}/p\mathbf{Z}[x]\}$. By the "freshman's dream" and the fact that $\forall a \in \mathbf{Z}/p\mathbf{Z}$ one has $a^p = a$ (for example by Little Fermat Theorem), given a polynomial $h(x) = a_n x^n + \ldots + a_1 x + a_0$, with $a_i \in \mathbf{Z}/p\mathbf{Z}$, then

$$h(x)^p = (a_n x^n + \ldots + a_1 x + a_0)^p = a_n^p x^{np} + \ldots + a_1^p x^p + a_0^p = a_n x^{np} + \ldots + a_1 x^p + a_0.$$

Hence, $h(x)^p = h(x^p)$ and

$$\mathbf{F}^p = \{\frac{f(x^p)}{g(x^p)},\ f, g \in \mathbf{Z}/p\mathbf{Z}[x]\} = \mathbf{Z}/p\mathbf{Z}(x^p).$$

To compute the degree $[\mathbf{F} : \mathbf{F}^p] = [\mathbf{Z}/p\mathbf{Z}(x) : \mathbf{Z}/p\mathbf{Z}(x^p)]$, set $y = x^p$ and compute the degree

$$[\mathbf{Z}/p\mathbf{Z}(\sqrt[p]{y}) : \mathbf{Z}/p\mathbf{Z}(y)].$$

As $\sqrt[p]{y}$ is a zero of the degree p polynomial $Z^p - y$, we have that $[\mathbf{Z}/p\mathbf{Z}(\sqrt[p]{y}) : \mathbf{Z}/p\mathbf{Z}(y)] = p$ provided that $Z^p - y$ is *irreducible* in $\mathbf{Z}/p\mathbf{Z}(y)[Z]$.

It was not required to prove the irreducibility of $F(Z) = Z^p - y$, however here is an argument: let $y^{1/p}$ denote a root of $Z^p - y$ in a splitting field $\mathbf{L}$ over $\mathbf{F} = \mathbf{F}_p(y)$. Then $Z^p - y = (Z - y^{1/p})^p$ in $\mathbf{L}[Z]$. Let $g \in \mathbf{F}[Z]$ be a monic irreducible divisor of $Z^p - y$. Then $g = (Z - y^{1/p})^i \in \mathbf{L}[Z]$, for some $1 \leq i \leq p$. By Newton's formula, $g = Z^p - i * y^{1/p} * Z^{(p-1)} + \ldots$. However, g is in $\mathbf{F}[Z]$. But the coefficient $i * y^{1/p}$ is not in $\mathbf{F}$, unless $i \equiv 0 \bmod p$. So, $1 \leq i \leq p$ and p divides $i \Rightarrow i = p$ and $g = Z^p - y$. So, $Z^p - y$ is irreducible.