Problem 1.

We factor the polynomial $f(x)$ as:

$$f(x) = x^6 - 9 = (x^3 - 3)(x^3 + 3) = (x - \sqrt[3]{3})(x - \omega\sqrt[3]{3})(x - \omega^2\sqrt[3]{3})(x + \sqrt[3]{3})(x + \omega\sqrt[3]{3})(x + \omega^2\sqrt[3]{3}),$$

where ω is third root of unity. Take $E = \mathbb{Q}(\omega, \sqrt[3]{3})$. We claim that this is the splitting field of $f(x)$. By above computation, f splits over E. This field is also minimal, since it is the smallest field extension which contains $\sqrt[3]{3}$ and ω. The degree of this extension is thus 6 since adjoining ω is a degree 2 extension, and adjoining $\sqrt[3]{3}$ is a degree 3 extension.

Problem 2.

Suppose that $x^d - 1$ divides $x^n - 1$ in $\mathbb{Q}[x]$. Then every root of $x^d - 1$ is also a root of $x^n - 1$. Let ξ be a primitive $d'th$ root of unity. Then we have that $\xi^d = 1$. Since ξ is also a root of $x^n - 1$ we have that $\xi^n = 1$. Since ξ is primitive we must have that $d|n$. Conversely suppose that $d|n$. We can write

$$x^m - 1 = \prod_{b|m} \Phi_b(x).$$

Since $d|n$ every $\Phi_b(x)$ that appears in the product expansion of $x^d - 1$ will also appear in the expansion of $x^n - 1$. Therefore the quotient

$$\frac{x^n - 1}{x^d - 1} = \prod_{b|n, b \geqslant d} \Phi_b(x).$$

Since each $\Phi_b(x) \in \mathbb{Q}[x]$, the quotient is as well.

Problem 3.

Define $f(x) = x^{p^n-1} - 1$ in $\mathbb{F}_{p^n}[x]$. We compute its formal derivative as

$$Df(x) = (p^n - 1)x^{p^n-2} = -(x^{p^n-2}) = 0 \iff x = 0.$$

Therefore $f(x)$ has $p^n - 1$ distinct nonzero roots, since 0 is clearly not a root of f. We conclude that $f(x) = \prod_{x \in \mathbb{F}_{p^n}^\times}(x - u)$. Thus we have

$$f(0) = -1 = \prod_{u \in \mathbb{F}_{p^n}^\times} -u \implies (-1)^{p^n} = \prod_{u \in \mathbb{F}_{p^n}^\times} u.$$

Taking $p \neq 2$ and $n = 1$ we deduce Wilsons Theorem:

$$(-1)^p = -1 = \prod_{u \in F_p^\times} u = (p-1)(p-2)\ldots(2) = (p-1)!.$$

Problem 4.

Suppose for the sake of contradiction that $\mathsf{E}/\mathbb{Q}$ is a finite extension but contains infinitely many (distinct) roots of unity. Then there must be an infinite subset of roots of unity with distinct orders. Thus the extension $\mathsf{E}/\mathbb{Q}$ must be infinite. A contradiction.

Problem 5.

Suppose that an isomorphism $\varphi : \mathbb{Q}(\sqrt{p}) \to \mathbb{Q}(\sqrt{q})$ exists for distinct p, q. Then

$$\varphi(p) = \varphi(\overbrace{1 + \dots + 1}^{\text{p times}}) = \varphi(1) + \dots \varphi(1) = 1 + \dots + 1 = p.$$

Let $\varphi(\sqrt{p}) = x$. Then $\varphi(\sqrt{p})^2 = \varphi(p) = x^2$. So $p = x^2$ in $\mathbb{Q}(\sqrt{q})$ i.e. $x = \sqrt{p}$. This is impossible clearly.

Problem 6.

To determine the Galois group of $f(x) = x^3 - 3x + 1$ we first determine its discriminant. We have that $s_2 = -1$ and $s_2 = -3$. It follows that the discriminant is $D = -4(-3)^3 - 27(-1)^2 = 81$. This is a square over $\mathbb{Q}$ so we have that $\mathrm{Gal}(f(x)) = A_3$.