Problem 1. (a) Let F be a field. Show that the units in $F[x]$ are the nonzero constant polynomials.

(b) Let $f(x) \in \mathbb{Z}[x]$ be a polynomial. Assume that for every prime number p, the polynomial $f(x)$ is irreducible in $\mathbb{Z}_p[x]$ (that is, the polynomial $f(x)$ where we view its coefficients modulo p is irreducible in $\mathbb{Z}_p[x]$). Show that $\deg(f) = 1$.

Solution.

(a) Let $f(x) \in F[x]$ be a unit. Then there exists a polynomial $g(x) \in F[x]$ such that $f(x)g(x) = 1$. Hence clearly $f(x) \neq 0$. Moreover we obtain that

$$0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$$

and since $\deg(f) \geq 0$ and $\deg(g) \geq 0$ we conclude that $\deg(f) = 0$. Hence $f(x)$ is a nonzero constant polynomial.

On the other hand, any nonzero constant polynomial $f(x) = a$ is a unit. Indeed, we have $a^{-1} \in F$ and so for $g(x) = a^{-1} \in F[x]$ we have $f(x)g(x) = aa^{-1} = 1$, showing that $f(x)$ is a unit.

(b) We first claim that $\deg(f) \geq 1$. Indeed, assume to a contradiction that $f(x) = a_0 \in \mathbb{Z}$. Let $p \in \mathbb{Z}$ be any prime number. Then $f(x)$ is a constant polynomial in $\mathbb{Z}_p[x]$. Hence either $f(x) = 0$ or $f(x)$ is a unit in $\mathbb{Z}_p[x]$ by part (a). In either case $f(x)$ is not irreducible in $\mathbb{Z}_p[x]$ which contradicts the assumption.

Now we claim that $\deg(f) \leq 1$. Assume to a contradiction that $f(x) = a_0 + a_1x + \cdots + a_nx^n$ for some $n \geq 2$. Then there exist at most $2n$ integers $k \in \mathbb{Z}$ such that $f(k) = \pm 1$, as these are the roots of the polynomials $f(x) - 1$ and $f(x) + 1$. Let $m \in \mathbb{Z}$ be an integer with $f(m) \neq \pm 1$. Then there exists some prime divisor p of $f(m)$ and so $f(m) = 0$ in $\mathbb{Z}_p[x]$. Hence $f(x)$ is divisible by $x - p$ in $\mathbb{Z}_p[x]$. Then $f(x) = (x-p)g(x)$ in $\mathbb{Z}_p[x]$ and $\deg(f) = \deg(x-p)+\deg(g)$ gives that $\deg(g) = \deg(f)-1 = n-1 \geq 1$. By part (a) we have that $g(x)$ is not a unit and so $f(x)$ is not irreducible, which is a contradiction.

Since we have $1 \leq \deg(f) \leq 1$ we conclude that $\deg(f) = 1$ as required.

Problem 2. Let p and q be two different prime numbers. Set $E = \mathbb{Q}(\sqrt{p}, \sqrt{q})$.

(a) Show that $\mathbb{Q} \subseteq E$ is a Galois extension, that $[E : \mathbb{Q}] = 4$ and that the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Find all intermediate field extensions $\mathbb{Q} \subseteq K \subseteq E$.

Solution.

(a) We first claim that $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. The minimal polynomial of $\sqrt{p}$ over $\mathbb{Q}$ is $x^2 - p$ (it is monic, has $\sqrt{p}$ as a root and is irreducible by Eisenstein's criterion for the prime number p). Hence $\{1, p\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{p})$. Assume to a contradiction that $\sqrt{q} \in \mathbb{Q}(\sqrt{p})$. Then there exist $a, b \in \mathbb{Q}$ such that

$$\sqrt{q} = a + b\sqrt{p} \implies q = a^2 + 2ab\sqrt{p} + b^2p. \tag{1}$$

We consider three cases and reach a contradiction in each of them:

- $a = 0$. Then (1) gives $q = b^2p$ which contradicts p and q being different prime numbers.
- $b = 0$. Then (1) gives $q = a^2$ which contradicts q being a prime number.
- $ab \neq 0$. Then (1) gives $\sqrt{p} = \frac{q-a^2-b^2p}{2ab}$, which is in $\mathbb{Q}$ since $a, b, q \in \mathbb{Q}$. But then $\sqrt{p} \in \mathbb{Q}$ which contradicts $x^2 - p$ being irreducible over $\mathbb{Q}$ since $x - \sqrt{p}$ divides $x^2 - p$.

Therefore we have shown that $\sqrt{q} \notin \mathbb{Q}(\sqrt{p})$. We have a sequence of field extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p}) \subseteq \mathbb{Q}(\sqrt{p}, \sqrt{q}) = E, \tag{2}$$

and $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = \deg(x^2-p) = 2$. On the other hand, the polynomial $x^2-q \in \mathbb{Q}(\sqrt{p})[x]$ is irreducible over $\mathbb{Q}(\sqrt{p})$ since it is of degree 2 and we have shown that its roots $\sqrt{q}$, $-\sqrt{q}$ are not in $\mathbb{Q}(\sqrt{p})$. It follows

that x^2-q is the minimal polynomial of $\sqrt{q}$ over $\mathbb{Q}(\sqrt{p})$. Then $[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}(\sqrt{p})] = \deg(x^2-q) = 2$. Hence (2) gives

$$[\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}] = [\mathbb{Q}(\sqrt{p},\sqrt{q}):\mathbb{Q}(\sqrt{p})][\mathbb{Q}(\sqrt{p}):\mathbb{Q}] = 2\cdot 2 = 4.$$

Hence $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p},\sqrt{q})$ is a finite extension. Moreover, $\mathbb{Q}(\sqrt{p},\sqrt{q})$ is the splitting field of $f(x) = (x^2-p)(x^2-q)$. Hence $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p},\sqrt{q})$ is normal. Since $\mathbb{Q}$ is a perfect field, $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{p},\sqrt{q})$ is also separable and hence it is a Galois extension. Let $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Since E is the splitting field of $f(x)$, σ permutes the roots of $f(x)$. More precisely, we have

$$\sigma(\sqrt{p})^2 - p = \sigma(\sqrt{p})^2 - \sigma(p) = \sigma(\sqrt{p}^2 - p) = \sigma(0) = 0,$$

and so $\sigma(\sqrt{p})$ is a root of x^2-p. Therefore $\sigma(\sqrt{p}) \in \{-\sqrt{p},\sqrt{p}\}$. Similarly $\sigma(\sqrt{q}) \in \{-\sqrt{q},\sqrt{q}\}$. Therefore $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_{++},\sigma_{+-},\sigma_{-+},\sigma_{--}\}$ where

$$\sigma_{+\bullet}(\sqrt{p}) = \sqrt{p},\ \ \sigma_{-\bullet}(\sqrt{p}) = -\sqrt{p},$$

$$\sigma_{\bullet+}(\sqrt{q}) = \sqrt{q},\ \ \sigma_{\bullet-}(\sqrt{q}) = -\sqrt{q}.$$

Then $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2\times\mathbb{Z}_2$ via the map $\phi : \mathrm{Gal}(E/\mathbb{Q}) \to \mathbb{Z}_2\times\mathbb{Z}_2$, $\phi(\sigma_{++}) = (0,0)$, $\phi(\sigma_{-+}) = (1,0)$, $\phi(\sigma_{+-}) = (0,1)$, $\phi(\sigma_{--}) = (1,1)$.

(b) The non-trivial subgroups of $\mathbb{Z}_2\times\mathbb{Z}_2$ are $\{(0,0),(1,0)\}$, $\{(0,0),(1,1)\}$ and $\{(0,0),(0,1)\}$. These correspond to the subgroups

$$H_1 = \{\sigma_{++},\sigma_{-+}\},\ \ H_2 = \{\sigma_{++},\sigma_{--}\},\ \ H_3 = \{\sigma_{++},\sigma_{+-}\}$$

of $\mathrm{Gal}(E/\mathbb{Q})$. A $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{p},\sqrt{q})$ is given by $\{1,\sqrt{p},\sqrt{q},\sqrt{pq}\}$. Let

$$b = b_1 + b_1\sqrt{p} + b_2\sqrt{q} + b_3\sqrt{pq} \in \mathbb{Q}(\sqrt{p},\sqrt{q}).$$

Then

$$b \in E_{H_1} \iff \sigma_{-+}(b) = b \iff b_0 - b_1\sqrt{p} + b_2\sqrt{q} - b_3\sqrt{pq} = b_1 + b - 1\sqrt{p} + b_2\sqrt{q} + b_3\sqrt{q} \iff b_1 = 0 \text{ and } b_3 = 0.$$

Hence $E_{H_1} = \{b_0 + b_2\sqrt{q} \mid b_0, b_2 \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{q})$. Similarly we obtain that $E_{H_2} = \mathbb{Q}(\sqrt{pq})$ and $E_{H_3} = \mathbb{Q}(\sqrt{p})$. By the FTGT, these are all the intermediate fields between $\mathbb{Q}$ and E.

Problem 3. Let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 3. Let G be the Galois group of $f(x)$.

(a) Show that $|G| \geq 3$.

(b) Show that if G is cyclic, then $G \cong \mathbb{Z}_3$.

(c) Show that if $z \in \mathbb{C}$ is a root of $f(x)$, then its complex conjugate $\overline{z}$ is also a root of $f(x)$. Conclude that if G is cyclic, then all of the roots of $f(x)$ are real.

Solution.

(a) Let $\alpha_1,\alpha_2,\alpha_3 \in \mathbb{C}$ be the roots of $f(x)$. Then $\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$ is the splitting field of $f(x)$. Then by the FTGT we have

$$|G| = [\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3):\mathbb{Q}] \geq [\mathbb{Q}(\alpha_1):\mathbb{Q}] = \deg(f) = 3,$$

where the equality $[\mathbb{Q}(\alpha_1):\mathbb{Q}] = \deg(f)$ holds since $f(x) \in \mathbb{Q}[x]$ is an irreducible polynomial with α_1 as a root.

(b) Recall that the elements of the Galois group act as permutations on $\{\alpha_1,\alpha_2,\alpha_3\}$. Hence $G < S_3$. Since G is a subgroup of S_3, we have that $|G| \mid |S_3| = 6$. Hence $|G| \in \{1,2,3,6\}$. Since G is a cyclic group and S_3 is not a cyclic group, we have that $G \neq S_3$ and so $|G| \neq 6$. We conclude that $|G| \in \{1,2,3\}$. Since by part (a) we have that $|G| \geq 3$, we obtain that $|G| = 3$. Since G is a cyclic group with three elements, it readily follows that $G \cong \mathbb{Z}_3$.

(c) Assume that z is a complex root of $f(x)$. Let $\phi : \mathbb{C} \to \mathbb{C}$ denote the complex conjugation, that is $\phi(a+bi) = a-bi$. Then ϕ is an automorphism of $\mathbb{C}$ which acts as the identity on $\mathbb{Q}$ and so

$$0 = \phi(0) = \phi(f(z)) = f(\phi(z)) = f(\overline{z}),$$

showing that $\overline{z}$ is also a root of $f(x)$. Hence complex roots of $f(x)$ come in pairs.

Now assume that G is cyclic, so that $G \cong \mathbb{Z}_3$ by part (b). Since the degree of $f(x)$ is 3 and complex roots come in pairs, we conclude that $f(x)$ has at least one real root, say α_1. On the other hand, for every $i \in \{1,2,3\}$ we have

$$3 = [\mathbb{Q}(\alpha_i) : \mathbb{Q}] \leq [\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) : \mathbb{Q}(\alpha_i)][\mathbb{Q}(\alpha_i) : \mathbb{Q}] = [\mathbb{Q}(\alpha_1,\alpha_2,\alpha_3) : \mathbb{Q}] = |G| = |\mathbb{Z}_3| = 3,$$

and so we conclude that $\mathbb{Q}(\alpha_i) = \mathbb{Q}(\alpha_1,\alpha_2,\alpha_3)$. Hence

$$\alpha_2 \in \mathbb{Q}(\alpha_2) = \mathbb{Q}(\alpha_1) \subseteq \mathbb{R} \text{ and } \alpha_3 \in \mathbb{Q}(\alpha_3) = \mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$$

as required.

Problem 4. Let $F = \mathrm{GF}(7)$ be a field with 7 elements and let $f(x) = x^{49} - x \in F[x]$.

(a) Let E be the splitting field of $f(x)$. Show that $E = \mathrm{GF}(7^2)$ is a field with 49 elements and conclude that $[E : F] = 2$.

(b) Let $g(x) \in F[x]$ be a monic irreducible polynomial of degree n. Show that $g(x)$ divides $f(x)$ if and only if $n = 1$ or $n = 2$.

(c) Show that there are 21 monic irreducible polynomials of degree 2 in $F[x]$.

Solution.

(a) Let $\alpha \in E$ be a root of $f(x)$. Since $f'(x) = 49x - 1 = -1$, we have $f'(\alpha) = -1 \neq 0$ and so α is a simple root of $f(x)$. It follows that $f(x)$ has 49 distinct roots. Let $E' \subseteq E$ be the set of all roots of $f(x)$ in E. Then $|E'| = 49$. Let $\alpha, \beta \in E'$ be two roots of $f(x)$ with $\alpha \neq 0$. Then $\alpha^{49} = \alpha$ and $\beta^{49} = \beta$ and so

$$\begin{aligned}(\alpha+\beta)^{49} - (\alpha+\beta) &= \alpha^{49} + \beta^{49} - \alpha - \beta = \alpha^{49} - \alpha + \beta^{49} - \beta = 0 + 0 = 0\\ (\alpha\beta)^{49} - \alpha\beta &= \alpha^{49}\beta^{49} - \alpha\beta = \alpha\beta - \alpha\beta = 0\\ (-\alpha)^{49} - (-\alpha) &= -(\alpha^{49}) + \alpha = -\alpha + \alpha = 0\\ (\alpha^{-1})^{49} - \alpha^{-1} &= (\alpha^{49})^{-1} - \alpha^{-1} = \alpha^{-1} - \alpha^{-1} = 0,\end{aligned}$$

which show that $\alpha+\beta, \alpha\beta, -\alpha, \alpha^{-1} \in E'$. Hence E' is a field comprising all roots of $f(x)$ by definition. It follows that $E' = E$ is the splitting field of $f(x)$, containing exactly $|E'| = 49$ elements. Then we obtain

$$[E : F] = [\mathrm{GF}(7^2) : \mathrm{GF}(7)] = 2.$$

(b) Assume first that $g(x)$ divides $f(x)$. Let α be a root of $g(x)$. Then $[F(\alpha) : F] = \deg(g) = n$ since $g(x)$ is irreducible. Moreover, $f(\alpha) = 0$ since α is a root of $g(x)$ and so $\alpha \in E$. Hence we obtain field extensions $F \subseteq F(\alpha) \subseteq E$. Then

$$2 = [E : F] = [E : F(\alpha)][F(\alpha) : F] = [E : F(\alpha)]n$$

gives that $n \mid 2$ and so $n = 1$ or $n = 2$.

For the other direction we need to show that all roots of $g(x)$ are roots of $f(x)$. In other words, it is enough to show that E contains all roots of $g(x)$.

Assume first that $n = 1$. Then $g(x) = x - a$ for some $a \in \mathrm{GF}(7)$. In particular $a \in E$ as required.

Assume now that $n = 2$. Let L be the splitting field of $g(x)$ and let $\alpha \in L$ be a root of $g(x)$. Then $[F(\alpha) : F] = \deg(g) = 2$ and so $F(\alpha)$ is a field with 7^2 elements. By uniqueness of finite fields with the same number of elements we have that $F(\alpha)$ is isomorphic to E. Hence $g(x)$ has a root $\alpha' \in E$. Then $x - \alpha'$ divides $g(x)$ in $E[x]$ and since $g(x)$ is of degree 2, it follows that $g(x)$ has its other root in E as well.

(c) The monic polynomial $f(x)$ can be written as the product of all monic irreducible polynomials that divide it. By part (b) these are all the monic irreducible polynomials of degree 1 and 2. There are exactly 7 monic irreducible polynomials of degree 1 in GF(7). Say there are k monic irreducible polynomials of degree 2 in GF(7). Then $f(x)$ is the product of 7 polynomials of degree 1 and k polynomials of degree 2. Hence

$$49 = \deg(f) = 7 \cdot 1 + k \cdot 2$$

which gives that $k = \frac{49-7}{2} = 21$.

Problem 5. Let $\omega = e^{\frac{2\pi i}{7}}$ be a primitive 7-th root of unity. Consider the cyclotomic polynomial $\Phi_7(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \in \mathbb{Q}[x]$.

(a) Show that $\Phi_7(x)$ is irreducible in $\mathbb{Q}[x]$.

(b) Show that the splitting field of $\Phi_7(x)$ is $\mathbb{Q}(\omega)$.

(c) Show that the Galois group $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ of $\Phi_7(x)$ is isomorphic to the multiplicative group $\mathbb{Z}_7^\times = \mathbb{Z}_7 \setminus \{0\}$.

(d) Let $\rho = \omega + \omega^2 + \omega^4 \in \mathbb{Q}(\omega)$. Find the minimal polynomial of ρ over $\mathbb{Q}$ and the subgroup $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\rho))$ of $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$.

Solution.

(a) We have that $\Phi_7(x)$ is irreducible in $\mathbb{Q}[x]$ if and only if $\Phi_7(x+1)$ is irreducible in $\mathbb{Q}[x]$ as well. Notice that $x^7 - 1 = (x-1)\Phi_7(x)$ and so we compute

$$\begin{aligned}\Phi_7(x+1) = \frac{(x+1)^7 - 1}{(x+1) - 1} &= \frac{x^7 + 7x^6 + 21x^5 + 35x^4 + 35x^3 + 21x^2 + 7x + 1 - 1}{x} \\ &= x^6 + 7x^5 + 21x^4 + 35x^3 + 35x^2 + 21x + 7.\end{aligned}$$

This last polynomial is irreducible by applying Eisenstein criterion for $p = 7$. We conclude that $\Phi_7(x)$ is irreducible as well.

(b) We have that

$$(x-1)\Phi_7(x) = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x^7 - 1.$$

Hence the roots of $\Phi_7(x)$ are all 7-th roots of unity. Since ω is a primitive 7-th root of unity, we have that $\omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7$ are all distinct. On the other hand, for $1 \leq i \leq 7$ we have

$$(\omega^i)^7 = (\omega^7)^i = 1^i = 1,$$

and so all of $\omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6, \omega^7$ are 7-th roots of unity. Since $x^7 - 1$ has degree 7, we obtain that $\{\omega^i \mid 1 \leq i \leq 7\}$ is the set of roots of $x^7 - 1$. Since $\omega^7 = 1$ is the root of $x - 1$, we conclude that $\{\omega^i \mid 1 \leq i \leq 6\}$ is the set of roots of $\frac{x^7-1}{x-1} = \Phi_7(x)$. Hence $\Phi_7(x)$ splits in $\mathbb{Q}(\omega)$. Clearly $\mathbb{Q}(\omega)$ is the smallest field extension of $\mathbb{Q}$ containing all the roots of $\Phi_7(x)$ since any such field extension must contain ω, and so we conclude that $\mathbb{Q}(\omega)$ is the splitting field of $\Phi_7(x)$.

(c) Let $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$. Then σ is a field automorphism $\sigma : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ such that $\sigma\big|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. A $\mathbb{Q}$-basis of $\mathbb{Q}(\omega)$ is given by $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$ and so σ is determined uniquely by its value $\sigma(\omega)$. We have

$$\Phi_7(\sigma(\omega)) = 1 + \sigma(\omega) + \sigma(\omega)^2 + \sigma(\omega)^3 + \sigma(\omega)^4 + \sigma(\omega)^5 + \sigma(\omega)^6 = \sigma(1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6) = \sigma(0) = 0,$$

and so $\sigma(\omega)$ is a root of $\Phi_7(x)$. Therefore $\sigma(\omega) = \omega^i$ for some $1 \leq i \leq 6$. Clearly any choice of i gives rise to a $\mathbb{Q}$-automorphism σ_i of $\mathbb{Q}(\omega)$ by defining $\sigma_i\big|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$ and $\sigma_i(\omega) = \omega^i$ and extending bilinearly through the $\mathbb{Q}$-basis of $\mathbb{Q}(\omega)$. Hence $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\sigma_i \mid 1 \leq i \leq 6\}$. Define a map

$$\begin{aligned}\Psi : G &\longrightarrow \mathbb{Z}_7^\times \\ \sigma_i &\longmapsto \bar{i}.\end{aligned}$$

Clearly Ψ is a bijective map. We claim that it is also a ring homomorphism. Let $1 \leq i, j \leq 6$. Write $ij = 7p + q$ for some $0 \leq q \leq 6$. Then

$$\sigma_i \circ \sigma_j(\omega) = \sigma_i(\omega^j) = \omega^{ij} = \omega^{7p+q} = (\omega^7)^p \omega^q = 1 \cdot \omega^q = \omega^q = \sigma_q(\omega),$$

and so $\sigma_i \circ \sigma_j = \sigma_q$. Therefore we have

$$\Psi(\sigma_i \circ \sigma_j) = \Psi(\sigma_q) = \overline{q}$$

while

$$\Psi(\sigma_i) \cdot \Psi(\sigma_j) = \overline{i} \cdot \overline{j} = \overline{ij} = \overline{7p + q} = \overline{q}.$$

Hence we conclude that $\Psi(\sigma_i \circ \Psi_j) = \Psi(\sigma_i) \cdot \Psi(\sigma_j)$ and so Ψ is a group homomorphism. Since it is also bijective, Ψ is a group isomorphism and so $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_7^\times$.

(d) Using

$$1 + \omega + \omega^2 + \omega^3 + \omega^4 + \omega^5 + \omega^6 = 0,$$

we obtain that $1 + \rho + \omega^3 + \omega^5 + \omega^6 = 0$. Using this we compute

$$\begin{aligned}
\rho^2 &= (\omega + \omega^2 + \omega^4)^2 \\
&= \omega + \omega^2 + 2\omega^3 + \omega^4 + 2\omega^5 + 2\omega^6 \\
&= (\omega + \omega^2 + \omega^4) + 2(\omega^3 + \omega^5 + \omega^6) \\
&= \rho + 2(-\rho - 1) \\
&= -\rho - 2.
\end{aligned}$$

We conclude that ρ is a root of $x^2 + x + 2$. This is a monic polynomial over $\mathbb{Q}$ and none of the integer divisors of the constant term 2 is a root. Hence $x^2 + x + 2$ has no root in $\mathbb{Q}$. Since it is of degree 2, we conclude that it is irreducible and hence it is the minimal polynomial of ρ.

To find the group $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\rho)) < \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ we need to find all $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}))$ such that $\sigma\big|_{\mathbb{Q}(\rho)} = \mathrm{id}_{\mathbb{Q}(\rho)}$. Since for every $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ we have that $\sigma\big|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$, we only need to find for which $\sigma \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ we have $\sigma(\rho) = \rho$. By part (c) we have that

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\sigma_i \mid 1 \leq i \leq 6\},$$

where $\sigma_i(\omega) = \omega^i$. Then $\sigma_i(\rho) = \rho$ gives

$$\omega^i + \omega^{2i} + \omega^{4i} = \omega + \omega^2 + \omega^4.$$

Since $\{1, \omega, \omega^2, \omega^3, \omega^4, \omega^5, \omega^6\}$ are $\mathbb{Q}$-linearly independent, and since both sides are just sums of terms in this $\mathbb{Q}$-basis of $\mathbb{Q}(\omega)$, we conclude that ω^i must be equal to one of ω, ω^2 and ω^4. We can see that this is possible only for $i \in \{1, 2, 4\}$. Checking these i we see that

$$\sigma_1(\rho) = \omega + \omega^2 + \omega^4 = \rho, \;\; \sigma_2(\rho) = \omega^2 + \omega^4 + \omega = \rho, \;\; \sigma_4(\rho) = \omega^4 + \omega + \omega^2 = \rho,$$

showing that $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}(\rho)) = \{\sigma_1, \sigma_2, \sigma_4\}$ (which is isomorphic to the subgroup $\{\overline{1}, \overline{2}, \overline{4}\}$ of $\mathbb{Z}_7^\times$, which in turn is isomorphic to $\mathbb{Z}_3$).