Problem 1. Let $p(x) = x^3 + x^2 + 1 \in \mathbb{Z}_5[x]$.

(a) Show that $p(x)$ is irreducible.

(b) Let $E = \mathbb{Z}_5(\alpha)$ where α is a root of $p(x)$. Show that for every $\beta \in E$ we have $\beta^{5^3} = \beta$.

(c) Let $\phi : \mathbb{Z}_5(\alpha) \to \mathbb{Z}_5(\alpha)$ be the ring automorphism $\phi(\beta) = \beta^5$. Find the order of ϕ.

Solution.

(a) We evaluate $p(x)$ at the elements of $\mathbb{Z}_5$ to obtain $p(0) = 1$, $p(1) = 3$, $p(2) = 3$, $p(3) = 2$ and $p(4) = 1$. We conclude that $p(x)$ has no roots in $\mathbb{Z}_5$. Since $p(x)$ has degree 3, it follows that $p(x)$ is irreducible.

(b) Since α is a root of $p(x)$ and $p(x)$ is irreducible by part (a), we obtain that

$$[\mathbb{Z}_5(\alpha) : \mathbb{Z}_5] = \deg(p(x)) = 3.$$

It follows that $\mathbb{Z}_5(\alpha)$ is a field with 5^3 elements. Consider the multiplicative group $\mathbb{Z}_5(\alpha)^\times = \mathbb{Z}_5(\alpha)\setminus\{0\}$. This has $5^3 - 1$ elements and so for every $\beta \in \mathbb{Z}_5(\alpha) \setminus \{0\}$ we have that $\beta^{5^3-1} = 1$. By multiplying both sides by β we obtain that $\beta^{5^3} = \beta$ for every $\beta \in \mathbb{Z}_5(\alpha) \setminus \{0\}$. Since we also have $0^{5^3} = 0$, it follows that $\beta^{5^3} = \beta$ for all $\beta \in \mathbb{Z}_5(\alpha)$.

(c) For every $\beta \in \mathbb{Z}_5(\alpha)$ we have

$$\phi^3(\beta) = \phi^2(\beta^5) = \phi(\beta^{5^2}) = \beta^{5^3} = \beta,$$

where the last equality follows by part (b). Therefore, $\phi^3 = \mathrm{id}_{\mathbb{Z}_5(\alpha)}$ and so the order of ϕ divides 3. Therefore, the order of ϕ is either 1 or 3. Assume to a contradiction that the order of ϕ is 1. Then $\beta = \mathrm{id}_{\mathbb{Z}_5(\alpha)}(\beta) = \phi(\beta) = \beta^5$ for all $\beta \in \mathbb{Z}_5(\alpha)$, implies that every $\beta \in \mathbb{Z}_5(\alpha)$ is a root of the polynomial $x^5 - x \in \mathbb{Z}_5(\alpha)$. But this is a contradiction since $x^5 - x$ has at most 5 different roots, while $\mathbb{Z}_5(\alpha)$ has 5^3 elements. Hence the order of ϕ is not 1 and so the order of ϕ is 3.

Problem 2. Let $p(x) = (x^3 - 2)(x^2 + 3) \in \mathbb{Q}[x]$. Let E be the splitting field of $p(x)$ over $\mathbb{Q}$.

(a) Show that $E = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. (Hint: the primitive third roots of unity are $\frac{-1+i\sqrt{3}}{2}$ and $\frac{-1-i\sqrt{3}}{2}$.)

(b) Show that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is not a normal field extension.

(c) Show that $[E : \mathbb{Q}] = 6$ and conclude that the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to S_3. (Hint: the only groups of order 6 are $\mathbb{Z}_6$ and S_3.)

Solution.

(a) Let ζ_3 be a primitive third root of unity. Then the roots of $p(x)$ are $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, $\zeta_3^2\sqrt[3]{2}$, $i\sqrt{3}$, and $-i\sqrt{3}$. Therefore

$$E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}, i\sqrt{3}).$$

Hence $\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) \subseteq E$. On the other hand, notice that $\zeta_3 \in \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ since $\zeta_3 = \frac{-1\pm i\sqrt{3}}{2}$. Therefore we also have $\zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2} \in \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ and so we obtain $E \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$. Since we have shown both inclusions, the claim follows.

(b) The polynomial $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion for $p = 2$. Moreover it has a root in $\mathbb{Q}(\sqrt[3]{2})$, namely $\sqrt[3]{2}$. However, the other two of its roots, namely $\zeta_3\sqrt[3]{2}$ and $\zeta_3^2\sqrt[3]{2}$ are not in $\mathbb{Q}(\sqrt[3]{2})$ (since they are not real), and so the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is not normal.

(c) Consider the tower of field extensions

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) = E.$$

The degree of $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$ is 3 since the minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$. We claim that the polynomial $x^2 + 3 \in \mathbb{Q}(\sqrt[3]{2})[x]$ is also irreducible. Since it is of degree 2, it is enough to show that it has no roots in $\mathbb{Q}(\sqrt[3]{2})$. But this follows since $x^2 + 3$ has complex roots and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$. Hence $x^2 + 3$ is the minimal polynomial of $i\sqrt{3}$ over $\mathbb{Q}(\sqrt[3]{2})$. It follows that the degree of $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ is 2. Altogether we have

$$[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[3]{2}, i\sqrt{3}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6.$$

Then the Galois group $G = \mathrm{Gal}(E/\mathbb{Q})$ has order $[E : \mathbb{Q}] = 6$. Hence it is isomorphic to either $\mathbb{Z}_6$ or S_3. Assume to a contradiction that $G \cong \mathbb{Z}_6$. We have the intermediate field $K = \mathbb{Q}(\sqrt[3]{2})$ with

$$\mathbb{Q} \subseteq K \subseteq E.$$

By the FTGT we obtain a subgroup $\mathrm{Gal}(E/K)$ of $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_6$. Since $\mathbb{Z}_6$ is abelian, we have that $\mathrm{Gal}(E/K)$ is a normal subgroup of $\mathbb{Z}_6$. Then by the FTGT we obtain that $\mathbb{Q} \subseteq K$ is a normal field extension. But this contradicts part (b). Hence $G \cong S_3$.

Problem 3. Let $F \subseteq E$ be a field extension. Let $\alpha, \beta \in E$ be algebraic over F. Let $p_\alpha(x)$ be the minimal polynomial of α over F and let $p_\beta(x)$ be the minimal polynomial of β over F.

(a) Let $F \subseteq K \subseteq E$ be an intermediate field. Show that if $p_\alpha(x)$ is irreducible in $K[x]$, then $F(\alpha) \cap K = F$.

(b) Let $\deg(p_\alpha(x)) = n$ and $\deg(p_\beta(x)) = m$. Assume that $\gcd(n, m) = 1$. Show that $F(\alpha) \cap F(\beta) = F$.

Solution.

(a) Let $c \in F(\alpha) \cap K$. Then $c \in K$ and so $F(c) \subseteq K$. Since $p_\alpha(x)$ is irreducible in $K[x]$, it follows that $p_\alpha(x)$ is irreducible in $F(c)$ as well. Moreover, since $c \in F(\alpha)$, we have that $F(c) \subseteq F(\alpha)$. Since $p_\alpha(x) \in F(c)[x]$ is irreducible, it follows that

$$[F(\alpha) : F(c)] = \deg(p_\alpha(x)).$$

On the other hand we have

$$\deg(p_\alpha(x)) = [F(\alpha) : F] = [F(\alpha) : F(c)][F(c) : F].$$

We obtain that $F(c) = F$ and so $c \in F$. Since $c \in F(\alpha) \cap K$ was arbitrary, we conclude that $F(\alpha) \cap K = F$.

(b) By part (a) it is enough to show that $p_\alpha(x)$ is irreducible in $F(\beta)[x]$. By assumption we have that

$$[F(\alpha) : F] = \deg(p_\alpha(x)) = n \text{ and } [F(\beta) : F] = \deg(p_\beta(x)) = m.$$

Moreover, since $p_\beta(x) \in F(\alpha)[x]$ and $p_\beta(\beta) = 0$, we have that $[F(\alpha, \beta) : F(\alpha)] \leq \deg(p_\beta(x)) = m$. Similarly, we have $[F(\alpha, \beta) : F(\beta)] \leq n$. Hence

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\beta)][F(\beta) : F] = [F(\alpha, \beta) : F(\beta)] \cdot m \leq nm. \tag{1}$$

That is, we have that $m \mid [F(\alpha, \beta) : F]$ and $[F(\alpha, \beta) : F] \leq nm$. Similarly we obtain that $n \mid [F(\alpha, \beta) : F]$. Since $\gcd(n, m) = 1$, we conclude that $nm \mid [F(\alpha, \beta) : F] \leq nm$ and so $[F(\alpha, \beta) : F] = nm$. By (1) it follows that $[F(\alpha, \beta) : F(\beta)] = n$. Let $q(x)$ be the minimal polynomial of α over $F(\beta)$. Then $\deg(q(x)) = n$ and $q(x) \mid p_\alpha(x)$ since $p_\alpha(x) \in F(\beta)[x]$ and $p_\alpha(\alpha) = 0$. But since we also have that $\deg(p_\alpha(x)) = n$, we obtain that $p_\alpha(x) = uq(x)$ for some $u \in F(\beta)$. Since $q(x)$ is irreducible in $F(\beta)[x]$, we conclude that $p_\alpha(x)$ is irreducible in $F(\beta)[x]$ as well, as required.

Problem 4. Let $\omega = e^{\frac{2\pi i}{17}}$ be a primitive 17-th root of unity. Consider the cyclotomic polynomial $\Phi_{17}(x) = 1 + x + x^2 + \cdots + x^{16} \in \mathbb{Q}[x]$.

(a) Show that the splitting field of $\Phi_{17}(x)$ is $\mathbb{Q}(\omega)$.

(b) Show that the Galois group $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ of $\Phi_{17}(x)$ is isomorphic to the multiplicative group $\mathbb{Z}_{17}^{\times} = \mathbb{Z}_{17} \setminus \{0\}$.

(c) Show that there exists a sequence of field extensions

$$\mathbb{Q} = F_0 \subseteq F_1 \subseteq F_2 \subseteq F_3 \subseteq F_4 = \mathbb{Q}(\omega)$$

such that $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq 4$. You may use without a proof the fact that all groups of order 2^t for some $t \geq 1$ are solvable.

Solution.

(a) We have that

$$(x-1)\Phi_{17}(x) = (x-1)(x^{16} + \cdots + x + 1) = x^{17} - 1.$$

Hence the roots of $\Phi_{17}(x)$ are all 17-th roots of unity. Since ω is a primitive 17-th root of unity, we have that $\omega, \omega^2, \ldots, \omega^{16}, \omega^{17}$ are all distinct. On the other hand, for $1 \leq i \leq 17$ we have

$$(\omega^i)^{17} = (\omega^{17})^i = 1^i = 1,$$

and so all of $\omega, \omega^2, \ldots, \omega^{16}, \omega^{17}$ are 17-th roots of unity. Since $x^{17} - 1$ has degree 17, we obtain that $\{\omega^i \mid 1 \leq i \leq 17\}$ is the set of roots of $x^{17} - 1$. Since $\omega^{17} = 1$ is the root of $x - 1$, we conclude that $\{\omega^i \mid 1 \leq i \leq 16\}$ is the set of roots of $\frac{x^{17}-1}{x-1} = \Phi_{17}(x)$. Hence $\Phi_{17}(x)$ splits in $\mathbb{Q}(\omega)$. Clearly $\mathbb{Q}(\omega)$ is the smallest field extension of $\mathbb{Q}$ containing all the roots of $\Phi_{17}(x)$ since any such field extension must contain ω, and so we conclude that $\mathbb{Q}(\omega)$ is the splitting field of $\Phi_{17}(x)$.

(b) 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 and powers of ω and so σ is determined uniquely by its value $\sigma(\omega)$. We have

$$\Phi_{17}(\sigma(\omega)) = 1 + \sigma(\omega) + \sigma(\omega)^2 + \cdots + \sigma(\omega)^{16} = \sigma(1 + \omega + \omega^2 + \cdots + \omega^{17}) = \sigma(0) = 0,$$

and so $\sigma(\omega)$ is a root of $\Phi_{17}(x)$. Therefore $\sigma(\omega) = \omega^i$ for some $1 \leq i \leq 16$. 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 $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\sigma_i \mid 1 \leq i \leq 16\}$. Define a map

$$\begin{aligned} \Psi : G &\longrightarrow \mathbb{Z}_{17}^{\times} \\ \sigma_i &\longmapsto \overline{i}. \end{aligned}$$

Clearly Ψ is a bijective map. We claim that it is also a ring homomorphism. Let $1 \leq i, j \leq 16$. Write $ij = 17p + q$ for some $0 \leq q \leq 16$. Then

$$\sigma_i \circ \sigma_j(\omega) = \sigma_i(\omega^j) = \omega^{ij} = \omega^{17p+q} = (\omega^{17})^p \omega^q = 1 \cdot \omega^q = \omega^q = \sigma_q(\omega),$$

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

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

while

$$\Psi(\sigma_i) \cdot \Psi(\sigma_j) = \overline{i} \cdot \overline{j} = \overline{ij} = \overline{17p + q} = \overline{q}.$$

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 $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_{17}^{\times}$.

(c) The group $G \coloneqq \mathrm{Gal}(\mathbb{Q}(\omega)/$ has $16 = 2^4$ elements by part (b). Therefore by the statement in the problem we know that G is solvable. Therefore there exists a sequence

$$\{e\} = G_k \lhd G_{k-1} \lhd \cdots \lhd G_1 \lhd G_0 = G$$

of subgroups of G such that G_i/G_{i+1} is cyclic of prime order for any $0 \leq i \leq k-1$. In particular we have that

$$\left|\frac{G_0}{G_1}\right| = \frac{|G_0|}{|G_1|} = \frac{16}{|G_1|}$$

and since $|\frac{G_0}{G_1}|$ is prime, we conclude that $|\frac{G_0}{G_1}| = 2$. It follows that $|G_1| = 8$. Continuing this way, we obtain that $|G_0| = 16$, $|G_1| = 8$, $|G_2| = 4$, $|G_3| = 2$ and $|G_4| = 1$ which we can write more generally as $|G_i| = 2^{4-i}$. Hence we have a sequence

$$\{e\} = G_4 \triangleleft G_3 \triangleleft G_2 \triangleleft G_1 \triangleleft G_0 = G$$

with $\left|\frac{G_i}{G_{i+1}}\right| = 2$ for $0 \leq i \leq 3$. By the FTGT we obtain a sequence of field extensions

$$F_0 \subseteq F_1 \subseteq F_2 \subseteq F_3 \subseteq F_4$$

where $F_i = \mathbb{Q}(\omega)_{G_i}$ for $0 \leq i \leq 4$. In particular, we have

$$F_0 = \mathbb{Q}(\omega)_{G_0} = \mathbb{Q}(\omega)_G = \mathbb{Q}(\omega)_{\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})} = \mathbb{Q}$$

and

$$F_4 = \mathbb{Q}(\omega)_{G_4} = \mathbb{Q}(\omega)_{\{e\}} = \mathbb{Q}(\omega).$$

Finally, again by the FTGT, we have for $0 \leq i \leq 4$ that

$$[F_i : F_0] = \frac{|\mathrm{Gal}(F_4/F_0)|}{|\mathrm{Gal}(F_4/F_i)|} = \frac{|\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})|}{|\mathrm{Gal}(\mathbb{Q}(\omega)/F_i)|} = \frac{16}{|G_i|} = \frac{16}{2^{4-i}} = 2^i.$$

Hence

$$2^i = [F_i : F_0] = [F_i : F_{i-1}][F_{i-1} : F_0] = [F_i : F_{i-1}] \cdot 2^{i-1}$$

implies that $[F_i : F_{i-1}] = 2$, as required.

Problem 5. Let $R = \{f(x) \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}$ be the integral domain of rational polynomials with integer constant term.

(a) Show that the units of R are -1 and 1.

(b) Let $f(x) \in R$ be a constant polynomial. Show that $f(x)$ is irreducible in R if and only if $f(x) = -p$ or $f(x) = p$ for some prime number $p \in \mathbb{Z}$.

(c) Let $f(x) \in R$ be a polynomial with $\deg(f(x)) \geq 1$. Show that $f(x)$ is irreducible in R if and only if $f(0) \in \{-1, 1\}$ and $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(d) Is the element $x \in R$ irreducible? Is R a unique factorization domain (UFD)?

Solution.

(a) Let $p(x) \in R$ be a unit. Then there exists a polynomial $q(x) \in R$ such that $p(x)q(x) = 1$. Clearly $q(x) \neq 0$. If $\deg(p(x)) > 0$ then

$$0 < \deg(p(x)) \leq \deg(p(x)q(x)) = \deg(1) = 0,$$

which is impossible. Hence $\deg(p(x)) = 0$ and so $p(x) = p_0$ is a constant polynomial. Since $p(0) \in \mathbb{Z}$ by assumption, we conclude that $p_0 \in \mathbb{Z}$. Similary we have that $q(x) = q_0 \in \mathbb{Z}$. Then $p_0 q_0 = p(x)q(x) = 1$ and $p_0, q_0 \in \mathbb{Z}$ implies that $p_0 \in \{-1, 1\}$.

(b) Since $f(x) \in R$ is a constant polynomial, we have that $f(x) = f_0 \in \mathbb{Z}$. Moreover $f(x) = g(x)h(x)$ with $g(x), h(x) \in R$ implies that $g(x) = g_0 \in \mathbb{Z}$ and $h(x) = h_0 \in \mathbb{Z}$, since the polynomials $g(x)$ and $h(x)$ cannot be non-constant. Since the units of R and $\mathbb{Z}$ are the same, it follows that $f(x)$ is irreducible in R if and only if f_0 is irreducible in $\mathbb{Z}$. But an element in $\mathbb{Z}$ is irreducible if and only if it is of the form $\pm p$ for some prime number p, which proves the claim.

(c) Since $\deg(f(x)) \geq 1$ and since units in R are $\{-1, 1\}$ and units in $\mathbb{Q}[x]$ are $\mathbb{Q} \setminus \{0\}$, it follows that $f(x)$ is not a unit neither in R nor in $\mathbb{Q}[x]$. Let $f(x) = f_0 + f_1 x + \cdots + f_n x^n$ for some $n \geq 1$.

Assume first that $f(x)$ is irreducible in $\mathbb{Q}[x]$ and $f(0) \in \{-1, 1\}$. Let $f(x) = g(x)h(x)$ for some $g(x), h(x) \in R$ and it is enough to show that one of $g(x)$ and $h(x)$ is a unit in R. Since $f(x) = g(x)h(x)$ holds in $\mathbb{Q}[x]$ as well, and since $f(x)$ is irreducible in $\mathbb{Q}[x]$, we have that $g(x)$ or $h(x)$ is a unit in $\mathbb{Q}[x]$. Without loss of generality, let us say that $g(x)$ is a unit in $\mathbb{Q}[x]$. Then $g(x) = g_0$ for some $g_0 \in \mathbb{Q} \setminus \{0\}$. Since $g(x) \in R$, we have that $g(0) = g_0 \in \mathbb{Z}$. On the other hand, we have that $f(0) = g(0)h(0)$. Since $f(0) = \pm 1$, $g(0) = g_0 \in \mathbb{Z}$ and $h(0) \in \mathbb{Z}$ (as $h(x) \in R$ as well), we conclude that $g_0 = \pm 1$ as well. By part (a) we have that $g(x) = g_0 = \pm 1$ is a unit, which shows that $f(x)$ is irreducible in R.

Assume now that $f(x)$ is irreducible in R. We first show that $f(0) = \pm 1$. Assume to a contradiction that $f(0) = 0$. Then we can write $f(x) = 2\frac{f(x)}{2}$ and we have both $2 \in R$ and $\frac{f(x)}{2} \in R$ since $\frac{f(0)}{2} = 0$. Since $f(x)$ is irreducible, we have that one of 2 and $\frac{f(x)}{2}$ is a unit. But this contradicts part (a) (since $f(x)$ has degree at least 1). Hence $f(0) = f_0 \neq 0$. Then we can write $f(x) = f_0 \frac{f(x)}{f_0}$ and we have both $f_0 \in R$ and $\frac{f(x)}{f_0} \in R$ since $\frac{f(0)}{f_0} = \frac{f_0}{f_0} = 1$. Since $f(x)$ is irreducible, we have that one of f_0 and $\frac{f(x)}{f_0}$ is a unit. Again by part (a) we have that $\frac{f(x)}{f_0}$ is not a unit and so $f_0 = \pm 1$. It remains to show that $f(x)$ is irreducible in $\mathbb{Q}[x]$. Assume to a contradiction that $f(x)$ is not irreducible in $\mathbb{Q}[x]$. Then there exist polynomials $g(x), h(x) \in \mathbb{Q}[x]$ which are not units in $\mathbb{Q}[x]$ and such that $f(x) = g(x)h(x)$. Let

$$g(x) = g_0 + g_1 x + \cdots + g_k x^k, \text{ and } h(x) = h_0 + h_1 x + \cdots + h_m x^m.$$

In particular, since these are not units, we have that $k, m \geq 1$. Since $g_0 h_0 = f_0 = \pm 1$, we have that $g_0 h_0 = \pm 1$. Then

$$\begin{aligned} f(x) &= g(x)h(x) \\ &= (g_0 + g_1 x + \cdots + g_k x^k)(h_0 + h_1 x + \cdots + h_m x^m) \\ &= g_0 \left(1 + \frac{g_1}{g_0} x + \cdots + \frac{g_k}{g_0} x^k\right)(h_0 + h_1 x + \cdots + h_m x^m) \\ &= \left(1 + \frac{g_1}{g_0} x + \cdots + \frac{g_k}{g_0} x^k\right)(g_0 h_0 + g_0 h_1 x + \cdots + g_0 h_m x^m), \end{aligned}$$

with both $1 + \frac{g_1}{g_0} x + \cdots + \frac{g_k}{g_0} x^k \in R$ and $g_0 h_0 + g_0 h_1 x + \cdots + g_0 h_m x^m \in R$ (since $g_0 h_0 = \pm 1 \in \mathbb{Z}$). But then this contradicts that $f(x)$ is irreducible in R since both of these polynomials are not units (because $k \geq 1$ and $m \geq 1$). Hence $f(x)$ is irreducible in $\mathbb{Q}[x]$.

(d) The element $x \in R$ can be written as

$$x = 2 \cdot \left(\frac{1}{2} x\right),$$

where both $2 \in R$ and $\frac{1}{2} x \in R$ hold, but neither of these two polynomials is a unit by part (a). Hence x is not irreducible in R. On the other hand, we claim that x cannot be written as a product of irreducible elements in R. Indeed, assume to a contradiction that

$$x = f_1(x) \cdots f_k(x)$$

for some irreducible $f_1(x), \ldots, f_k(x) \in R$. Since x is not irreducible, we have that $k \geq 2$. Then by comparing degrees it follows that exactly one of $f_1(x), \ldots, f_k(x)$ is of degree 1 and the rest are constant. Say $f_1(x) = a + bx$ and $f_2(x), \ldots, f_k(x)$ are constant. By part (b) we have that $f_2(x) = \pm p_2, \ldots, f_k(x) = \pm p_k$ for some prime numbers $p_2, \ldots, p_k$. By part (c) we have that $f_1(0) = \pm 1$ and so $a = \pm 1$. Then

$$x = (\pm 1 + bx)(\pm p_2) \cdots (\pm p_k)$$

is impossible since the constant terms do not match. Since x cannot be written as a product of irreducible elements in R, we conclude that R is not a UFD.