14.2.10. *Let $f = x^8 - 3 \in \mathbb{Q}[x]$.*

5pt (a) *Find the degrees and all the conjugates of $\alpha = \sqrt[8]{3} \in \mathbb{R}$ and of $\omega = e^{2\pi i/8}$. Determine whether the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$ is normal and whether $\mathbb{Q}(\omega)/\mathbb{Q}$ is normal.*

Solution. α is a root of f, and all roots of f are $\alpha\omega^k$, $k = 0, \ldots, 7$; since f is irreducible (by Eisenstein), these are the conjugates of α.

ω is a primitive 8th root of unity, its conjugates are the primitive 8th roots of unity, which are ω, ω^3, ω^5, and ω^7.

Since $E = \mathbb{Q}(\alpha)$ doesn't contain $\alpha\omega$, $E/\mathbb{Q}$ is not normal. Since $L = \mathbb{Q}(\omega)$ contains all conjugates of ω, $L/\mathbb{Q}$ is normal (is the splitting field of the cyclotomic polynomial Φ_8).

10pt (b) *Find the splitting field K of f and find its degree.*

Solution. Since all roots of f have form $\alpha\omega^k$, $k = 0, \ldots, 7$, the splitting field of f is $K = \mathbb{Q}(\alpha, \omega)$. Let $E = \mathbb{Q}(\alpha)$ and $L = \mathbb{Q}(\omega)$, then $K = EL$. We have $[E : \mathbb{Q}] = 8$. I claim that $[K : E] = 4$, so that $[K : \mathbb{Q}] = [K : E][E : \mathbb{Q}] = 32$. Indeed, we have $\omega = \frac{1+i}{\sqrt{2}}$, so $L = \mathbb{Q}(\sqrt{2}, i)$. Now, $\deg_E \sqrt{2} = 2$: indeed, we know that the only quadratic subextensions of $E/\mathbb{Q}$ is $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$; Sbut snce $1, \sqrt{2}, \sqrt{3}$ are $\mathbb{Q}$-linearly independent, $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$, so $\sqrt{2} \notin E$. (Alternatively, if $\sqrt{2} \in E$, then $M = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ is a subfield of E of degree 4 over $\mathbb{Q}$, then α has degree 2 over M, then the only conjugate of α over M must also be real, so, is $-\alpha$, then the minimal polynomial of α over M is $x^2 - \sqrt[4]{3}$, but $\sqrt[4]{3} \notin M$ since M is normal and $\sqrt[4]{3}$ has conjugates not in M.) Also $\deg_{E(\sqrt{2})} i = 2$ since i is not real; hence, $[K : E] = 4$.

10pt (c) *Find the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$.*

Solution. Since $|G| = 32$, ω can be sent by elements of G to any of its conjugates ω^l, $l = 1, 3, 5, 7$, and α can be independently sent to any of its conjugates $\alpha\omega^k$, $k = 0, 1, \ldots, 7$. Let $\varphi_{k,l} \in G$ be the automorphism for which $\varphi_{k,l}(\omega) = \omega^l$ and $\varphi_{k,l}(\alpha) = \alpha\omega^k$. Then the product of $\varphi_{k,l}$ and $\varphi_{n,m}$ maps ω to ω^{lm} and α to $\alpha\omega^{ln+k}$, so that $\varphi_{k,l}\varphi_{n,m} = \varphi_{ln+k,lm}$. (So $G \cong \mathbb{Z}_8 \rtimes \mathbb{Z}_8^* \cong \mathbb{Z}_8 \rtimes V_4$.)

Another solution. Since $|G| = 32$, ω can be sent by elements of G to any of its conjugates ω^l, $l = 1, 3, 5, 7$, and α can be independently sent to any of its conjugates $\alpha\omega^k$, $k = 0, 1, \ldots, 7$. Define $\varphi, \psi_1, \psi_2 \in G$ by $\varphi(\alpha) = \omega\alpha$, $\varphi(\omega) = \omega$, $\psi_1(\alpha) = \psi_2(\alpha) = \alpha$, $\psi_1(\omega) = \omega^3$, $\psi_1(\omega) = \omega^5$. Then $|\varphi| = 8$, $|\psi_1| = |\psi_2| = 2$, $\psi_1\psi_2 = \psi_2\psi_1$, $\psi_1\varphi\psi_1(\alpha) = \alpha\omega^3$ and $\psi_1\varphi\psi_1(\omega) = \omega^9 = \omega$ so $\psi_1\varphi\psi_1 = \varphi^3$, and similarly $\psi_2\varphi\psi_2 = \varphi^5$. Hence, $G = \langle \varphi, \psi_1, \psi_2 \mid \varphi^8 = \psi_1^2 = \varphi_2^2 = 1,\ \psi_1\psi_2 = \psi_2\psi_1,\ \psi_1\varphi\psi_1 = \varphi^3,\ \psi_1\varphi\psi_1 = \varphi^5 \rangle$. (No more relations are needed since the obtained relations already define a group of order 32.)

5pt **14.2.13.** *Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is cyclic of order 3 then all roots of the cubic are real.*

Solution. We can prove more: if $K \subset \mathbb{C}$ and $K/\mathbb{Q}$ is a Galois extension of odd degree, then $K \subseteq \mathbb{R}$. Indeed, (the restriction of) the complex conjugation $\varphi(z) = \bar{z}$, $z \in K$, is an automorphism of K with $\varphi^2 = 1$, so $\varphi \in G = \mathrm{Gal}(K/\mathbb{Q})$ with order 1 or 2. Since G has an odd order, φ cannot have order 2 in G, so φ has order 1 in G, that is, acts trivially on K.

Another solution. Let K be the splitting field of the cubic f, the $[K : F] = 3$. f has no roots in $\mathbb{Q}$, since otherwise K would have degree at most 2 over $\mathbb{Q}$. Let α be a real root of f. Then $\mathbb{Q}(\alpha)$ is a subfield of K; but then $1 < [\mathbb{Q}(\alpha) : \mathbb{Q}] \,\big|\, [K : \mathbb{Q}] = 3$, so $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$, so $K = \mathbb{Q}(\alpha) \subseteq \mathbb{R}$.

10pt **14.2.14.** *Let $K = \mathbb{Q}\big(\sqrt{2 + \sqrt{2}}\big)$; prove that $K/\mathbb{Q}$ is a Galois extension and that $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathbb{Z}_4$.*

Solution. Let $\alpha = \sqrt{2 + \sqrt{2}}$; the minimal polynomial of α is $(x^2 - 2)^2 - 2 = x^4 - 4x^2 + 2$ (which is irreducible by Eisenstein's criterion). Using our classification of Galois groups of irreducible biquadratic polynomials, we check that $\sqrt{b} = \sqrt{2} \notin \mathbb{Q}$, $\delta = \sqrt{(-4)^2 - 4 \cdot 2} = 2\sqrt{2}$ so $\sqrt{2}/\delta \in \mathbb{Q}$, so $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathbb{Z}_4$. We also see that the degree of the splitting field of f is 4, so $K = \mathbb{Q}(\alpha)$ is the splitting field of f, and so, $K/\mathbb{Q}$ is Galois with $\mathrm{Gal}(K/\mathbb{Q}) = \mathrm{Gal}(f/\mathbb{Q})$.

Another solution. The conjugates of α over $\mathbb{Q}$ are $\beta = \sqrt{2-\sqrt{2}}$, $-\alpha$, and $-\beta$. We have $\alpha\beta = \sqrt{2} \in \mathbb{Q}(\alpha)$, so $\beta \in \mathbb{Q}(\alpha)$, and also $-\alpha, -\beta \in \mathbb{Q}(\alpha)$, so $K/\mathbb{Q} = \mathbb{Q}(\alpha)/\mathbb{Q}$ is normal, and so, is a Galois extension of degree 4. Thus, $G = \mathrm{Gal}(K/\mathbb{Q})$ is (isomorphic to) either $\mathbb{Z}_4$ or V_4; we have $G \cong \mathbb{Z}_4$ iff there is an element of order 4 in G.

Let φ be an automorphism of K such that $\varphi(\alpha) = \beta$. (Such an automorphism exists, and is unique since K is generated by α.) Then $\varphi(\sqrt{2}) = \varphi(\alpha^2 - 2) = \beta^2 - 2 = -\sqrt{2}$. So,

$$\varphi(\beta) = \varphi(\sqrt{2}/\alpha) = (-\sqrt{2})/\beta = -\alpha.$$

Hence, $\varphi^2(\alpha) = \varphi(\beta) = -\alpha$, $\varphi^3(\alpha) = \varphi(-\alpha) = -\beta$, and $\varphi^4(\alpha) = \varphi(-\beta) = \alpha$. So, φ is an element of G of order 4, and $G = \langle\varphi\rangle \cong \mathbb{Z}_4$.

10pt **14.3.8.** *Determine the splitting field and the Galois group of the polynomial $f(x) = x^p - x - a \in \mathbb{F}_p[x]$, where $a \in \mathbb{F}_p \setminus \{0\}$.*

Solution. (The solution partially repeats arguments of the solution to exercise 13.5.5.) No element b of $\mathbb{F}_p$ is a root of f, since $b^p = b$. If α is a root of f, then for any $b \in \mathbb{F}_p$,

$$f(\alpha + b) = (\alpha + b)^p - (\alpha + b) - a = \alpha^p - \alpha - a + b^p - b = 0,$$

so $\alpha + b$ is also a root of f, and we therefore have $p = \deg f$ distinct roots of f in $\mathbb{F}_p(\alpha)$. Thus, $K = \mathbb{F}_p(\alpha)$ is the splitting field of f, and is separable over $\mathbb{F}_p$. Since f has no roots in $\mathbb{F}_p$, $K \neq \mathbb{F}_p$, and so, $K/\mathbb{F}_p$ is a nontrivial Galois extension of degree $\leq \deg f = p$. (If we use the result of 13.5.5 that f is irreducible, we can claim that $[K : F(\alpha)] = p$; but we don't need this.)

Since $\alpha \notin \mathbb{F}_p$, its minimal polynomial has degree ≥ 2; so α has conjugates distinct from itself, and we know that all conjugates of α must be of the form $\alpha + b$, $b \in \mathbb{F}_p$. Let $\alpha + b$, with $b \neq 0$, be one of them, and let $\varphi \in \mathrm{Gal}(K/\mathbb{F}_p)$ be such that $\varphi(\alpha) = \alpha + b$. (Such φ exists and is unique, since K is generated by α.) The elements α, $\varphi(\alpha) = \alpha + b$, $\varphi^2(\alpha) = \alpha + 2b$, ..., and $\varphi^{p-1}(\alpha) = \alpha + (p-1)b$ are all distinct, so the automorphisms $\mathrm{Id}, \varphi, \varphi^2, \ldots, \varphi^{p-1}$ are all distinct, so $\mathrm{Gal}(K/\mathbb{F}_p)$ is cyclic, $\cong \mathbb{Z}_p$, generated by φ. (It now follows, by the way, that $\deg_{\mathbb{F}_p} \alpha = p$, so f is irreducible, and $K = \mathbb{F}_{p^p}$.)

10pt **Cf. 14.2.3.** *Let $f = (x^2-2)(x^2-3)(x^2-5) \in \mathbb{Q}[x]$; find the splitting field K of f and $\mathrm{Gal}(f/\mathbb{Q}) = \mathrm{Gal}(K/\mathbb{Q})$. List all 16 subgroups of G and for every subgroup $H \leq G$ find the subfield $\mathrm{Fix}(H)$ of K.*

Solution. The group $G = \mathrm{Gal}(K/F)$ is isomorphic to $\mathbb{Z}_2^3$. Indeed, $K = \mathbb{Q}\big(\sqrt{2}, \sqrt{3}, \sqrt{5}\big)$ has degree 8 over $\mathbb{Q}$, since, as it is easy to see, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ and $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Thus, each of the 8 mappings $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{3} \mapsto \pm\sqrt{3}$, $\sqrt{5} \mapsto \pm\sqrt{5}$, defines an automorphism of $K/\mathbb{Q}$. These mappings commute and have order 2, thus form a group isomorphic to $\mathbb{Z}_2^3$.

$G \cong \mathbb{Z}_2^3$ is a 3-dimensional $\mathbb{Z}_2$ vector space; "a basis" of G is formed by the automorphisms $\varphi_1, \varphi_2, \varphi_3$ defined by

$$\varphi_1 : \begin{matrix} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{matrix} \qquad \varphi_2 : \begin{matrix} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \\ \sqrt{5} \mapsto \sqrt{5} \end{matrix} \qquad \varphi_3 : \begin{matrix} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \\ \sqrt{5} \mapsto -\sqrt{5} \end{matrix}$$

G has the following subgroups:
the subgroup $1 = \{\mathrm{Id}_K\}$,
seven "one-dimensional" subgroups of the form $\langle\varphi\rangle$ for $\varphi \in G \setminus \{1\}$,
seven "two dimensional" subgroups of the form $\langle\varphi, \psi\rangle$ for distinct $\varphi, \psi \in G \setminus \{1\}$,
and G itself.

φ_1 fixes $\sqrt{3}$ and $\sqrt{5}$, so the subgroup $\langle\varphi_1\rangle$ fixes the subfield $\mathbb{Q}(\sqrt{3}, \sqrt{5})$ of K; since the degree of this field over $\mathbb{Q}$ equals 4 equals the index of $\langle\varphi_1\rangle$ in G, we have $\mathrm{Fix}(\langle\varphi_1\rangle) = Q(\sqrt{3}, \sqrt{5})$. We similarly find the fixed fields of the other "one-dimensional" subgroups of G. For the "two-dimensional" subgroup $\langle\varphi_1, \varphi_2\rangle$, its fixed field is the intersection $\mathrm{Fix}(\langle\varphi_1\rangle) \cap \mathrm{Fix}(\langle\varphi_2\rangle) = \mathbb{Q}(\sqrt{5})$. Similarly, we find the fixed fields of other "two-dimensional" subgroups, and get the following correspondence table:

$$\begin{gathered}1 \longrightarrow K\\ \langle\varphi_1\rangle \longrightarrow \mathbb{Q}(\sqrt{3},\sqrt{5}),\quad \langle\varphi_2\rangle \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{5}),\quad \langle\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{3}),\\ \langle\varphi_1\varphi_2\rangle \longrightarrow \mathbb{Q}(\sqrt{5},\sqrt{6}),\quad \langle\varphi_1\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{3},\sqrt{10}),\quad \langle\varphi_2\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{2},\sqrt{15}),\\ \langle\varphi_1\varphi_2\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{6},\sqrt{10}),\\ \langle\varphi_1,\varphi_2\rangle \longrightarrow \mathbb{Q}(\sqrt{5}),\quad \langle\varphi_1,\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{3}),\quad \langle\varphi_2,\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{2}),\\ \langle\varphi_1\varphi_2,\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{6}),\quad \langle\varphi_1\varphi_3,\varphi_2\rangle \longrightarrow \mathbb{Q}(\sqrt{10}),\quad \langle\varphi_2\varphi_3,\varphi_1\rangle \longrightarrow \mathbb{Q}(\sqrt{15}),\\ \langle\varphi_1\varphi_2,\varphi_2\varphi_3\rangle \longrightarrow \mathbb{Q}(\sqrt{30}),\\ \text{and } G \longrightarrow \mathbb{Q}\end{gathered}$$

5pt **14.5.10.** *Prove that $\sqrt[3]{2}$ is not contained in any cyclotomic field.*

Solution. Let $K/\mathbb{Q}$ be a cyclotomic extension. Then $K/\mathbb{Q}$ is Galois with abelian $\mathrm{Gal}(K/\mathbb{Q})$ (namely, $\mathbb{Z}_n^*$ for some n). Thus every subextension of $K/\mathbb{Q}$ is normal; but $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal.

Another solution. Assume that $K/\mathbb{Q}$ is a cyclotomic extension containing $\alpha = \sqrt[3]{2}$. Then $K/\mathbb{Q}$ is Galois, so K contains the splitting field of the minimal polynomial $f = x^3 - 2$ of α, so $\mathrm{Gal}(f/\mathbb{Q})$ is a quotient group of $\mathrm{Gal}(K/\mathbb{Q})$. But $\mathrm{Gal}(K/\mathbb{Q})$ is abelian, whereas $\mathrm{Gal}(f/\mathbb{Q}) \cong S_3$ is not, contradiction.

5pt **A1.** *Prove that there are no biquadratic extensions of finite fields.*

Solution. Finite fields are perfect, so any algebraic extension of a finite field is separable. A (separable) biquadratic extension has Galois group isomorphic to V_4, whereas any finite extension of a finite field is cyclic (has cyclic Galois group).

5pt **A2.** *Let K/F be a Galois extension, let $G = \mathrm{Gal}(K/F)$. For every prime p and every $r \in \mathbb{N}$ such that $p^r \,\big|\, |G|$, prove that there is a subfield L of K with $[K : L] = p^r$.*

Solution. By Sylow's theorem, if a prime p and $r \in \mathbb{N}$ are such that $p^r \,\big|\, |G|$, then G contains a subgroup H with $|H| = p^r$. Let $L = \mathrm{Fix}(H)$; then $[K : L] = |H| = p^r$.