Solution 1. We already know $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ is Galois with its Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ generated by ϕ and ψ, where $\phi(\sqrt{2}) = -\sqrt{2}, \phi(\sqrt{3}) = \sqrt{3}$ and $\psi(\sqrt{2}) = \sqrt{2}, \psi(\sqrt{3}) = -\sqrt{3}$.

(a). Suppose $a = c^2$ for some $c \in F = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Then $\psi(a) = \psi((2+\sqrt{2})(3+\sqrt{3})) = (2+\sqrt{2})(3-\sqrt{3})$. Consider the Galois extension $F/\mathbb{Q}(\sqrt{2})$, whose Galois group is $\{1,\psi\}$. Then

$$\begin{aligned}N_{F/\mathbb{Q}(\sqrt{2})}(a) &= a\phi(a) = (2+\sqrt{2})(2+\sqrt{3})(2+\sqrt{2})(3-\sqrt{3}) = 6(2+\sqrt{2})^2\\ &= N_{F/\mathbb{Q}(\sqrt{2})}(c^2) = (N_{F/\sqrt{2}}(c))^2.\end{aligned}$$

This implies $6(2+\sqrt{2})^2$, and hence 6, is a square in $\mathbb{Q}(\sqrt{2})$, namely,

$$6 = (a+b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$$

for some $a, b \in \mathbb{Q}$. But this cannot be true: if $a = 0$, then $6 = 2b^2$ or $b^2 = 3$, which is not possible for any $b \in \mathbb{Q}$; if $b = 0$, then $6 = a^2$, which is not possible for any $a \in \mathbb{Q}$ either; if $a \neq 0 \neq b$, then it implies $\sqrt{2}$ is rational, which is also not possible. Hence, a cannot be a square in F.

(b). Since a is not a square in F but $a \in F$, it is easily seen that $[F(\sqrt{a} = \alpha) : F] = 2$ since the minimal polynomial of $\sqrt{a} = \alpha$ over F is $x^2 - a \in F[x]$. Hence

$$[F(\alpha) : \mathbb{Q}] = [F(\alpha) : F][F : \mathbb{Q}] = 2\cdot 4 = 8.$$

Apparently, $E = \mathbb{Q}(\alpha) \subset F(\alpha)$. For the reverse inclusion, note that

$$a = \alpha^2 = (2+\sqrt{2})(3+\sqrt{3}) = 6 + 3\sqrt{2} + 2\sqrt{3} + \sqrt{6} \in E$$

and so $b = 3\sqrt{2}+2\sqrt{3}+\sqrt{6} = a-6 \in E$ and then $c = (b^2-36)/12 = \sqrt{2}+\sqrt{3}+\sqrt{6} \in E$ and then $d = b - 2c = \sqrt{2} - \sqrt{6} \in E$ and then $e = (8-d^2)/4 = \sqrt{3} \in E$ and then $\sqrt{2} = (c+d-2) \in E$. And so $F = \mathbb{Q}(\sqrt{2},\sqrt{3}) \subset E$ and $F(\alpha) \subset E$. Therefore, $E = F(\alpha)$ and $[E : \mathbb{Q}] = 8$. Keep squaring α and removing rationals, we get a polynomial rational $\alpha^8 - 24\alpha^6 + 133\alpha^4 - 288\alpha^2 + 144 = 0$. Since $[E : \mathbb{Q}] =$ deg of the minimal polynomial of α over $\mathbb{Q}$, the minimal polynomial must be $f(x) = x^8 - 24x^6 + 144 - 288x^2 + 144 \in \mathbb{Q}[x]$. $f(x)$ is irreducible and has 8 roots which can be checked directly that they are $\pm\sqrt{(2\pm\sqrt{2})(3\pm\sqrt{3})}$.

(c). Since $\mathbb{Q}$ is perfect, all finite extensions are separable and so we need to check $E/\mathbb{Q}$ is normal, which can be done via checking that all the roots of $f(x)$ lie in E and E is a splitting field of $f(x)$ and so is normal. This is straightforward.

$$\alpha\sqrt{(2-\sqrt{2})(3+\sqrt{3})} = \sqrt{(2+\sqrt{2})(3+\sqrt{3})(2-\sqrt{2})(3+\sqrt{3})} = (3+\sqrt{3})\sqrt{2} \in E$$

and therefore, $\sqrt{(2-\sqrt{2})(3+\sqrt{3})} = (3+\sqrt{3})\sqrt{2}/\alpha \in E$. Similarly,

$$\alpha\sqrt{(2+\sqrt{2})(3-\sqrt{3})} = \sqrt{(2+\sqrt{2})(3+\sqrt{3})(2+\sqrt{2})(3-\sqrt{3})} = (2+\sqrt{2})\sqrt{6} \in E$$

and therefore, $\sqrt{(2+\sqrt{2})(3-\sqrt{3})} = (2+\sqrt{2})\sqrt{6}/\alpha \in E$. Finally,

$$\alpha\sqrt{(2-\sqrt{2})(3-\sqrt{3})} = \sqrt{(2+\sqrt{2})(3+\sqrt{3})(2-\sqrt{2})(3-\sqrt{3})} = 2\sqrt{3} \in E$$

and therefore, $\sqrt{(2-\sqrt{2})(3-\sqrt{3})} = 2\sqrt{3}/\alpha \in E$. The rest of them are the negatives of these four and hence also are in E. So indeed, E is a splitting field of $f(x)$ over $\mathbb{Q}$ and normal.

(d). Since $E = \mathbb{Q}(\alpha)$, an element in the Galois group is entirely determined by its action on α. For convenience, we write $\beta = \sqrt{(2-\sqrt{2})(3+\sqrt{3})}$ and $\gamma = \sqrt{(2+\sqrt{2})(3-\sqrt{3})}$. Then from part (c), wee that $\alpha\beta = \sqrt{2}(3+\sqrt{3})$ and $\alpha\gamma = \sqrt{6}(2+\sqrt{2})$. Now $\sigma(\alpha^2) = \beta^2$, namely,

$$\sigma(\alpha^2) = \sigma((2+\sqrt{2})(3+\sqrt{3})) = (2-\sqrt{2})(3+\sqrt{3}).$$

Note that $\alpha^2 = a \in F$ and $\sigma|_F \in \text{Gal}(F/\mathbb{Q}) = \langle \phi, \psi \rangle$. So we must have $\sigma|_F = \phi$. More precisely, consider the canonical surjection from the fundamental theorem on Galois theory

$$\pi : \text{Gal}(E/\mathbb{Q}) \to \text{Gal}(F/\mathbb{Q}), \tau \mapsto \tau|_L.$$

Then $\ker(\pi) = \text{Gal}(E/F)$ and $\pi(\sigma) = \phi$. And so

$$\sigma(\alpha\beta) = \sigma(\sqrt{2}(3+\sqrt{3})) = -\sqrt{2}(3+\sqrt{3}) = -\alpha\beta.$$

It follows immediately that $\sigma(\beta) = -\alpha$ and so σ is of order 4.

(e). Similar arguments apply on τ. We see that $\tau(\alpha^2) = \gamma^2$, namely,

$$\tau(\alpha^2) = \tau((2+\sqrt{2})(3+\sqrt{3})) = \gamma^2 = (2+\sqrt{2})(3-\sqrt{3}).$$

Hence $\pi(\tau) = \psi$. And then

$$\tau(\alpha\gamma) = \tau(\sqrt{6}(2+\sqrt{2})) = -\sqrt{6}(2+\sqrt{2}) = -\alpha\gamma.$$

Therefore, $\tau(\gamma) = -\alpha$ and τ is of order 4. If $\text{Gal}(E/\mathbb{Q})$ is cyclic, it cannot have two elements of order 4. Thus $\text{Gal}(E/\mathbb{Q})$ is not cyclic. Now consider $\langle\sigma\rangle$, which is a cyclic group of order 4. We note that $\sigma^2(\alpha) = -a$ and $\sigma^3(\alpha) = -\beta$. Since $\langle\sigma\rangle$ is of index 2 and $\tau \notin \langle\sigma\rangle$, $\text{Gal}(E/\mathbb{Q})$ is partitioned by $\langle\sigma\rangle$ and $\tau\langle\sigma\rangle$. Hence, $\text{Gal}(E/\mathbb{Q}) = \langle\sigma, \tau\rangle$. Note that $\sigma^2(\alpha) = -\alpha = \tau^2(\alpha)$, so $\sigma^2 = \tau^2$. Note that

$$\sigma\tau(\gamma) = \sigma(-\alpha) = -\sigma(\alpha) = -\beta$$

and

$$\tau\sigma^3(\beta) = \tau\sigma^2(-\alpha) = \tau(\alpha) = \gamma.$$

By a similar argument as part (d), we then see that $\tau\sigma^3(\gamma) = -\beta = \sigma\tau(\gamma)$. And hence $\sigma\tau = \tau\sigma^3$, or equivalently, $\tau\sigma = \sigma^{-1}\tau$ by the conjugation of σ^{-1}.

One of the standard presentation (as per Wikipedia) of Q_8 is

$$\langle a, b | a^4 = e, a^2 = b^2, ba = a^{-1}b\rangle.$$

The isomorphism between $\mathrm{Gal}(E/\mathbb{Q})$ and Q_8 is then trivially by $\sigma \mapsto a$ and $\tau \mapsto b$.

Solution 2. By Eisenstein's Criterion, $f(x) = x^4 + px + p \in \mathbb{Q}[x]$ is irreducible for any prime p. So we can safely apply the classification about the Galois groups of quartics. The resolvent of $f(x)$ is then

$$r(x) = x^3 - 4px - p^2 \in \mathbb{Q}[x].$$

And the discriminant is

$$\Delta = -4(-4p)^3 - 27(-p^2)^2 = p^3(256 - 27p).$$

Note that if p is odd, then $p^3 \mid \Delta$ but $p^4 \nmid \Delta$ since $p \nmid (256 - 27p)$. So Δ is never a square in $\mathbb{Q}$ when p is an odd prime. If $p = 2$, then $\Delta = 2^3(256 - 27 \cdot 2) = 1616$ is not a square in $\mathbb{Q}$ either. Therefore, Δ is never a square in $\mathbb{Q}$ whatever the prime p is.

The thing left is to determine the irreducibility of $r(x)$. If $r(x)$ is reducible, then it has a rational root as being a cubic. By the rational root test, if the rational root is a/b in the lowest form, then $b \mid 1$ and $a \mid -p^2$. And so the only possible roots are $\pm 1, \pm p, \pm p^2$. But $r(1) = 1 - 4p - p^2 < 0$, so 1 is never a root. And $r(-1) = 1 + 4p - p^2 = 5 - (p-2)^2$ can never be 0 since 5 is not a square. Now

$$r(p^2) = p^6 - 4p^3 - p^2 > p^2(p^4 - 4p - 1) > p^2(8p - 4p - 1) > 3p^3 > 0.$$

And

$$r(-p^2) = -p^6 + 4px^3 - p^2 = -p^2(p^4 - 4p + 1) < -p^2(p^4 - p^2 + (p-2)^2) < -p^2 < 0.$$

And so $\pm p^2$ can never be roots of $r(x)$. Thus we only to check whether $\pm p$ are roots of $r(x)$. Note that

$$r(p) = p^3 - 4p^2 - p^2 = p^2(p - 5)$$

has roots $p = 0, 5$ and

$$r(-p) = -p^3 + 4p^2 - p^2 = (3 - p)p^2$$

has roots $p = 0, 3$.

Therefore, when $p \neq 3, 5$, $r(x)$ is irreducible. Combining the fact that Δ is never a square, we see that the Galois group $G_f \cong S_5$.

If $p = 3$, then $r(x) = x^3 - 12x - 9 = (x+3)(x^2 - 3x - 3)$. The roots of $r(x)$ are $-3, (3 \pm \sqrt{21})/2$. So the splitting field of $r(x)$ is $L = \mathbb{Q}(\sqrt{21})$. The polynomial to be tested to determine the Galois group is $h(x) = (x^2 + 3x + 3)(x^2 + 3)$. We see that $\sqrt{i\sqrt{3}}$ does not lie in L and so $h(x)$ does not split over L and so $G_f \cong D_4$.

If $p = 5$, then $r(x) = x^3 - 20x - 25 = (x - 5)(x^2 + 5x + 5)$ with roots $5, (-5 + \sqrt{5})/2$. SO the splitting field of $r(x)$ is $\mathbb{Q}(\sqrt{5})$. The polynomial to be tested to determine the Galois group is $h(x) = (x^2 + 5x + 5)(x^2 - 5)$, which has roots $\pm\sqrt{5}, (-5 \pm \sqrt{5})/2$ all in L. So $h(x)$ splits over L. Therefore, the Galois group $G_f \cong \mathbb{Z}/4\mathbb{Z}$.

Solution 3. Let a be a real root of f and $b \neq 0$ a complex root. Since complex roots appear in pair by conjugation, we see $\bar{b}$ is also a root. Let L be the splitting field of f over $\mathbb{Q}$ and we further require $\mathbb{Q} \subset \overline{\mathbb{Q}} \subset \mathbb{C}$. Then $L \subset \mathbb{C}$. Denote the complex conjugation on $\mathbb{C}$ by $\phi : \mathbb{C} \to \mathbb{C}, x \mapsto \overline{x}$. Then $\phi|_L$ is a homomorphism from L to $\mathbb{C}$ fixing $\mathbb{Q}$. But L as the splitting field is normal and so indeed we have $\phi|_L \in \mathrm{Gal}(L/\mathbb{Q}) = G_f$. Since f is irreducible, the Galois group G_f is transitive and so we can find an element $\tau \in G_f$ such that $\tau(a) = b$. But then $\phi|_L$ and τ do not commute in the sense that

$$\tau\phi|_L(a) = \tau(a) = b \neq \phi|_L\tau(a) = \phi|_L(b) = \bar{b}.$$

Therefore, G_f is not an abelian group.

We cannot drop the assumption that f is irreducible since we need the transitivity of G_f. As a counter example, $f(x) = (x - 1)(x^2 + 1)$ and $f(x)$ has the obvious Galois group $G_f \cong \mathbb{Z}/2\mathbb{Z}$ consisting of the identity map and the complex conjugation map.

Solution 4. I think this is a problem on the lower bound of the Euler function $\varphi(n)$.

Claim: $\varphi(n) \geq \sqrt{n/2}$.

With this claim, suppose $E/\mathbb{Q}$ is a finite extension. Then we can find a positive integer n such that $[E : \mathbb{Q}] < \sqrt{n/2}$. Then E cannot contain any primitive m-th root for any $m > n$. Otherwise,

$$[E : \mathbb{Q}] \geq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m) \geq \sqrt{m/2} > \sqrt{n/2} > [E : \mathbb{Q}],$$

which is a contradiction. But there are only finitely many q-th primitive root of unity for $q \leq n$.

Proof of Claim: Let $n = p_1^{e_1} \dots p_k^{e_k}$, where p_i are distinct primes and $e_i \geq 1$. Then we have

$$\begin{aligned}
\varphi(n)^2 &= (n\prod_{i=1}^{k}(1 - \frac{1}{p_i}))(\prod_{i=1}^{k} p_i^{e_i-1}(p_i - 1)) \\
&= n\prod_{i=1}^{k}(1 - \frac{1}{p_i})p_i^{e_i-1}(p_i - 1) \\
&\geq n\prod_{i=1}^{k}\frac{(p_i - 1)^2}{p_i} \\
&\geq \frac{n}{2},
\end{aligned}$$

because if $p_i = 2$, then $(p_i - 1)^2/p_i = 1/2$ and if $p_i \geq 3$, then $(p_i - 1)^2/p_i \geq 1$. Therefore, we have the desired inequality.

Solution 5. One direction shall be easy, suppose n is not square free, say $n = p^2 q$ for some prime p. Let ζ_n be a primitive n-th root. Then ζ_n^{pq} is a primitive p-th root of unity. Hence

$$\Phi_p(\zeta_n^{pq}) = 1 + \zeta_n^{pq} + (\zeta_n^{pq})^2 + \cdots + (\zeta_n^{pq})^{p-1} = 0.$$

Multiplying both sides by ζ_n, we get

$$\zeta_n + \zeta_n^{pq+1} + \zeta_n^{2pq+1} + \cdots + \zeta_n^{(p-1)pq+1} = 0.$$

Note that $\gcd(p^2 q, ipq + 1) = 1$, so each element ζ_n^{pq+1} is also a primitive n-th root. Hence we get a nontrivial linear dependence relation between the n-th primitive roots. So they cannot form a basis.

For the other direction, I did not really find a way to apply the normal basis theorem. Maybe you can explain to me after the presentation.

Solution 6. One direction is clear. Let $\{\sigma(a) : \sigma \in G\}$ be a normal basis for some $a \in L$. Then we claim that $\{a\}$ is a basis of L as a KG-module and so L is a cyclic hence free KG-module. We only need to prove the claim. Since $\{\sigma(a) : \sigma \in G\}$ is a K-basis for L, any element $x \in L$ can be expressed as $x = \sum_{\sigma\in G} k_\sigma \sigma(a)$, where $k_\sigma \in K$. But then take the element $s_x = \sum_{\sigma\in G} k_\sigma \sigma \in KG$. We see that $s_x a = (\sum_{\sigma\in G} k_\sigma)a = \sum_{\sigma\in G} k_\sigma \sigma(a) = x$. So $\{a\}$ is a spanning set. To see $\{a\}$ is linearly independent, we assume there is a linear dependence relation

$$0 = (\sum_{\sigma\in G} k_\sigma \sigma)a = \sum_{\sigma\in G} k_\sigma \sigma(a).$$

But $\{\sigma(a) : \sigma \in G\}$ is a K-basis, then we must have $k_\sigma = 0$ for all $\sigma \in G$ and so $(\sum_{\sigma\in G} k_\sigma \sigma) = 0$.

For the other direction, suppose L is a free KG-module, namely, $L = \langle a_1 \rangle \oplus \cdots \oplus \langle a_k \rangle$, where $\langle a_i \rangle \cong KG$ for each direct summand. Note that KG, hence $\langle a_i \rangle$, has a K-vector space structure with $\dim_K(KG) = |G| = [L : K]$. So by counting the dimension, L is necessarily a cyclic KG-module, say, $L = \langle a \rangle$. Then $\{\sigma(a) : \sigma \in G\}$ is a normal basis. Again by counting dimension, we only need to show it is a spanning set. Now since $L = \langle a \rangle$, for any $x \in L$ we can find $s_x = \sum_{\sigma\in G} k_\sigma \in KG$, where $k_\sigma \in K$, such that $x = (\sum_{\sigma\in G} k_\sigma)a = \sum_{\sigma\in G} k_\sigma \sigma(a)$. In other words, x is a K-linear combination of $\{\sigma(a) : \sigma \in G\}$.

Solution 7. Let $[L : K] = m$. Then $L = \mathbb{F}_{q^m}$ (up to isomorphism), where $q = p^n$, and the Galois group is cyclic and generated by the Frobenius map $\phi : L \to L, x \mapsto x^q$. By Hilbert 90, $N_{L/K}(\alpha) = 1$ if and only if we can find $a \in L$ such that $\alpha = \phi(a)/a$. Hence

$$\ker(N_{L/K}) = \{\phi(a)/a : a \in L\}.$$

To find the cardinality of $\{\phi(a)/a : a \in L\}$, we need to eliminate the duplicity. Now consider the map

$$f : L^* \to L^*, x \mapsto \phi(x)/x = x^p/x.$$

Since both phi and inverse map are group homomorphisms, so is f. Hence by group isomorphism theorem, we have

$$L^*/\ker(f) \cong \mathrm{im}(f) = \{\phi(a)/a : a \in L\}.$$

Now $x \in \ker(f)$ if and only if $\phi(x) = x$, namely, x is fixed by ϕ and then by the Galois group, so if and only if $x \in K^*$. And hence

$$|\ker(N_{L/K})| = |L^*/\ker(f)| = |L^*|/|K^*| = (q^m - 1)/(q - 1),$$

where $m = [L : K]$ and $q = p^n$.