1. (a) The roots of f are $\epsilon^i\alpha$ with $i = 0, 1, 2, 3, 4$ where $\alpha = \sqrt[5]{2}$ and $\epsilon = \exp(\frac{2\pi i}{5})$. Hence $E = \mathbb{Q}(\alpha, \epsilon\alpha, \epsilon^2\alpha, \epsilon^3\alpha, \epsilon^4\alpha) = \mathbb{Q}(\alpha, \epsilon)$ is a splitting field of f inside $\mathbb{C}$.

   (b) The field E can be obtained from $\mathbb{Q}$ by two consecutive simple extensions, namely, by first adjoining α and then adjoining ϵ. The minimum polynomial of α over $\mathbb{Q}$ is $x^5 - 2$ which is irreducible by Eisenstein's criterion. Hence $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 5$. By the tower law, 5 divides the degree $(E : \mathbb{Q})$. The minimum polynomial of ϵ over $\mathbb{Q}$ is $x^4 + x^3 + x^2 + x + 1$. It is irreducible by Ex.VIII.8. Consequently, the minimum polynomial of ϵ over $\mathbb{Q}(\alpha)$ has degree at most 4, and then the tower law gives that $(E : \mathbb{Q}) \leq 20$. On the other hand, E can be obtained by fist adjoining ϵ and then α. Now, $(\mathbb{Q}(\epsilon) : \mathbb{Q}) = 4$, and hence 4 divides the degree $(E : \mathbb{Q})$. Since the only number ≤ 20 that is divisible by both 4 and 5 is 20 itself, it follows that $(E : \mathbb{Q}) = 20$. Being a splitting field in characteristic zero, E is a normal extension of $\mathbb{Q}$, and hence $|G| = (E : \mathbb{Q}) = 20$.

   (c) Since E is generated by α and ϵ, each $\mathbb{Q}$-automorphism of E is completely determined by its effect on α and ϵ. Since any such automorphism maps α to a zero of $x^5 - 2$, there are 5 possible images for α, namely $\epsilon^i\alpha$ with $i = 0, 1, 2, 3, 4$. Also, since any $\mathbb{Q}$-automorphism maps ϵ to a zero of $x^4 + x^3 + x^2 + x + 1$, the possible images for ϵ are ϵ^j with $j = 1, 2, 3, 4$. Hence there are precisely 20 possible images for the pair α, ϵ and since the order of G is 20 all 20 of these possibilities give us actual automorphisms in G. For θ and σ we have

   $$\theta^i\sigma^j(\alpha) = \epsilon^i\alpha, \qquad \theta^i\sigma^j(\epsilon) = \epsilon^{2^j}.$$

   As j runs over $0, 1, 2, 3$, the power $2^j \mod 5$ takes the values $1, 2, 4, 3$, respectively, and hence each automorphism is of the required form.

   (d) We have that θ and all of its powers fix ϵ while $\theta^i(\alpha) = \epsilon^i\alpha$. Hence the order of θ is 5. On the other hand, σ fixes α and $\sigma^j(\epsilon) = \epsilon^{2^j}$. Hence the order of σ is 4.

   (e) We have

   $$\sigma\theta\sigma^{-1}(\alpha) = \sigma\theta(\alpha) = \sigma(\epsilon\alpha) = \epsilon^2\alpha = \theta^2(\alpha)$$

   and

   $$\sigma\theta\sigma^{-1}(\epsilon) = \sigma\theta\sigma^3(\epsilon) = \sigma\theta(\epsilon^3) = \sigma(\epsilon^3) = \epsilon^6 = \epsilon = \theta^2(\epsilon).$$

   Hence $\sigma\theta\sigma^{-1} = \theta^2$. It follows that the cyclic subgroup $\langle\theta\rangle$ is normalized by the cyclic subgroup $\langle\sigma\rangle$, and hence it is normalized by $G = \langle\theta\rangle\langle\sigma\rangle$.

(f) $\langle\theta\rangle$ has order 5, and hence $\Phi(\langle\theta\rangle)$ is a degree 4 extension of $\mathbb{Q}$. Since θ fixes ϵ, and $(\mathbb{Q}(\epsilon) : \mathbb{Q}) = 4$, it follows that $\Phi(\langle\theta\rangle) = \mathbb{Q}(\epsilon)$.

$\langle\sigma\rangle$ has order 4, and hence $\Phi(\langle\sigma\rangle)$ is a degree 5 extension of $\mathbb{Q}$. Since σ fixes α, and $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 5$, it follows that $\Phi(\langle\sigma\rangle) = \mathbb{Q}(\alpha)$.

The subgroup H od G that is generated by θ and σ^2 has order 10 (in fact, since $\sigma^2\theta\sigma^{-2} = \theta^4 = \theta^{-1}$, H is isomorphic to the dihedral group of order 10). Hence $\Phi(H)$ is a degree 2 extension of $\mathbb{Q}$. Since both θ and σ^2 fix $\epsilon + \epsilon^4 = \epsilon + \sigma^2(\epsilon)$, it follows that $\Phi(H) = \mathbb{Q}(\epsilon + \epsilon^4)$ (Note that $\epsilon+\epsilon^4 \notin \mathbb{Q}$ because it it is not fixed by σ: $\sigma(\epsilon+\epsilon^4) = \epsilon^2+\epsilon^3$ which is a negative real number whereas $\epsilon + \epsilon^4$ is a positive real number).

2. (a) The roots of f are $\epsilon^i\alpha$ with $i = 0, 1, 2, 3, 4, 5$ where $\alpha = \sqrt[6]{2}$ and $\epsilon = \exp(\frac{2\pi i}{6})$. Hence $E = \mathbb{Q}(\alpha, \epsilon\alpha, \epsilon^2\alpha, \ldots, \epsilon^5\alpha) = \mathbb{Q}(\alpha, \epsilon)$ is a splitting field of f inside $\mathbb{C}$.

(b) The field E can be obtained from $\mathbb{Q}$ by two consecutive simple extensions, namely, by first adjoining α and then adjoining ϵ. The minimum polynomial of α over $\mathbb{Q}$ is $x^6 - 2$ which is irreducible by Eisenstein's criterion. Hence $(\mathbb{Q}(\alpha) : \mathbb{Q}) = 6$. The minimum polynomial of $\epsilon = \exp(\frac{2\pi i}{6}) = \frac{1}{2}(1 + i\sqrt{3})$ over $\mathbb{Q}$ is $x^2 - x + 1$. This stays irreducible over $\mathbb{Q}(\alpha)$ since its two roots are non-real complex numbers and $\mathbb{Q}(\alpha)$ consists entirely of real numbers. Consequently, $(E : \mathbb{Q}(\alpha)) = 2$, and then the tower law gives that $(E : \mathbb{Q}) = 12$. Being a splitting field in characteristic zero, E is a normal extension of $\mathbb{Q}$, and hence $|G| = (E : \mathbb{Q}) = 12$.

(c) Since E is generated by α and ϵ, each $\mathbb{Q}$-automorphism of E is completely determined by its effect on α and ϵ. Since any such automorphism maps α to a zero of $x^6 - 2$, there are 6 possible images for α, namely $\epsilon^i\alpha$ with $i = 0, 1, 2, 3, 4, 5$. Also, since any $\mathbb{Q}$-automorphism maps ϵ to a zero of $x^2 - x + 1$, the possible images for ϵ are ϵ and $\epsilon^5 = \bar{\epsilon}$. Hence there are precisely 12 possible images for the pair α, ϵ and since the order of G is 12 all 12 of these possibilities give us actual automorphisms in G. For θ and σ we have

$$\theta^i(\alpha) = \epsilon^i\alpha, \qquad \theta^i(\epsilon) = \epsilon.$$

and

$$\theta^i\sigma(\alpha) = \epsilon^i\alpha, \qquad \theta^i\sigma(\epsilon) = \bar{\epsilon}.$$

Hence each automorphism in G is a product of powers of α and ϵ, and so these automorphisms generate G.

(d) We have that θ and all of its powers fix ϵ while $\theta^i(\alpha) = \epsilon^i\alpha$. Hence the order of θ is 6. On the other hand, σ fixes α and $\sigma^2(\epsilon) = \epsilon$. Hence the order of σ is 2.

(e) We have

$$\sigma\theta\sigma^{-1}(\alpha) = \sigma\theta(\alpha) = \sigma(\epsilon\alpha) = \bar{\epsilon}\alpha = \epsilon^5\alpha = \theta^5(\alpha)$$

and

$$\sigma\theta\sigma^{-1}(\epsilon) = \sigma\theta\sigma(\epsilon) = \sigma\theta(\bar{\epsilon}) = \sigma(\bar{\epsilon}) = \epsilon = \theta^5(\epsilon).$$

Hence $\sigma\theta\sigma^{-1} = \theta^5$. It follows that the cyclic subgroup $\langle\theta\rangle$ is normalized by the cyclic subgroup $\langle\sigma\rangle$, and hence it is normalized by $G = \langle\theta\rangle\langle\sigma\rangle$. Moreover, G is generated by θ of order 6 and σ of order 2 and $\sigma\theta\sigma^{-1} = \theta^{-1}$. So G is isomorphic to the dihedral group of order 12.

(f) $\langle\theta\rangle$ has order 6, and hence $\Phi(\langle\theta\rangle)$ is a degree 2 extension of $\mathbb{Q}$. Since θ fixes ϵ, and $(\mathbb{Q}(\epsilon):\mathbb{Q}) = 2$, it follows that $\Phi(\langle\theta\rangle) = \mathbb{Q}(\epsilon)$.

$\langle\sigma\rangle$ has order 2, and hence $\Phi(\langle\sigma\rangle)$ is a degree 6 extension of $\mathbb{Q}$. Since σ fixes α, and $(\mathbb{Q}(\alpha):\mathbb{Q}) = 6$, it follows that $\Phi(\langle\sigma\rangle) = \mathbb{Q}(\alpha)$.

$\langle\theta^3\rangle$ has order 2, and hence $\Phi(\langle\theta^3\rangle)$ is a degree 6 extension of $\mathbb{Q}$. Since θ^3 fixes ϵ and $\alpha^2 = \sqrt[3]{2}$, and since $(\mathbb{Q}(\epsilon, \sqrt[3]{2}):\mathbb{Q}) = 6$, it follows that $\Phi(\langle\theta\rangle) = \mathbb{Q}(\epsilon, \sqrt[3]{2})$.

3. (a) The roots of f are $\epsilon^i\alpha$ with $i = 0, 1, \ldots, 7$ where $\alpha = \sqrt[8]{2}$ and $\epsilon = \exp(\frac{2\pi i}{8})$. Hence $E = \mathbb{Q}(\alpha, \epsilon\alpha, \epsilon^2\alpha, \ldots, \epsilon^7\alpha) = \mathbb{Q}(\alpha, \epsilon)$ is a splitting field of f inside $\mathbb{C}$.

(b) It is not true that $x^4 + 1$ stays irreducible over $\mathbb{Q}(\alpha)$. In fact,

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2} + 1),$$

and since $\sqrt{2} = \alpha^4 \in \mathbb{Q}(\alpha)$, this is a factorization over $\mathbb{Q}(\alpha)$.

(c) We have $\epsilon^2 = i \in E$. Hence $E = \mathbb{Q}(\alpha, \epsilon, i)$. But $\epsilon = \frac{\sqrt{2}}{2}(1+i) = \frac{\alpha^4}{2}(1+i)$. Consequently, $E = \mathbb{Q}(\alpha, i)$, as required.

(d) The field E can be obtained from $\mathbb{Q}$ by two consecutive simple extensions, namely, by first adjoining α and then adjoining i. The minimum polynomial of α over $\mathbb{Q}$ is $x^8 - 2$ which is irreducible by Eisenstein's criterion. Hence $(\mathbb{Q}(\alpha):\mathbb{Q}) = 8$. The minimum polynomial of i over $\mathbb{Q}$ is x^2+1. This stays irreducible over $\mathbb{Q}(\alpha)$ since its two roots $\pm i$ are non-real complex numbers and $\mathbb{Q}(\alpha)$ consists entirely of real numbers. Consequently, $(E:\mathbb{Q}(\alpha)) = 2$, and then the tower law gives that $(E:\mathbb{Q}) = 16$. Being a splitting field in characteristic zero, E is a normal extension of $\mathbb{Q}$, and hence $|G| = (E:\mathbb{Q}) = 16$.

(e) Since E is generated by α and i, each $\mathbb{Q}$-automorphism of E is completely determined by its effect on α and i. Since any such automorphism maps α to a zero of $x^8 - 2$, there are 8 possible images for α, namely $\epsilon^i\alpha$ with $j = 0, 1, \ldots, 7$. Also, since any $\mathbb{Q}$-automorphism maps i to a zero of x^2+1, the possible images for i are $\pm i$. Hence there are precisely 16 possible images for the pair α, i and since the order of G is 16, all 16 of these possibilities give us actual automorphisms in G. In particular, G contains the automorphisms θ and σ as required.

(f) We have

$$\begin{aligned}\theta(\epsilon) &= \theta\left(\frac{\sqrt{2}}{2}(1+i)\right) = \theta\left(\frac{\alpha^4}{2}(1+i)\right) = \frac{\theta(\alpha)^4}{2}(1+i) \\ &= \frac{(\epsilon\alpha)^4}{2}(1+i) = \frac{(\epsilon)^4(\alpha)^4}{2}(1+i) = \frac{(-1)\sqrt{2}}{2}(1+i) = -\epsilon.\end{aligned}$$

(g) We have

$$\theta(\alpha) = \epsilon\alpha, \qquad \theta^2(\alpha) = -\epsilon^2\alpha, \qquad \theta^3(\alpha) = \epsilon^7\alpha, \qquad \theta^4(\alpha) = -\alpha,$$

$$\theta^5(\alpha) = -\epsilon\alpha, \qquad \theta^6(\alpha) = \epsilon^2\alpha, \qquad \theta^7(\alpha) = -\epsilon^7\alpha, \qquad \theta^8(\alpha) = \alpha$$

while i is fixed by θ and all its powers. It follows that θ has order 8.

(h) Of course, σ is just complex conjugation and therefore of order 2.

(i) We have

$$\sigma\theta\sigma^{-1}(\alpha) = \sigma\theta\sigma(\alpha) = \sigma\theta(\alpha) = \sigma(\epsilon\alpha) = \bar{\epsilon}\alpha = \epsilon^7\alpha = \theta^3(\alpha)$$

and

$$\sigma\theta\sigma^{-1}(i) = \sigma\theta\sigma(i) = \sigma\theta(-i) = \sigma(-i) = i = \theta^3(i).$$

Hence $\sigma\theta\sigma^{-1} = \theta^3$. From here we easily calculate

$$\sigma\theta^2\sigma^{-1} = \theta^6, \;\; \sigma\theta^3\sigma^{-1} = \theta, \;\; \sigma\theta^4\sigma^{-1} = \theta^4,$$

$$\sigma\theta^5\sigma^{-1} = \theta^7, \;\; \sigma\theta^6\sigma^{-1} = \theta^3, \;\; \sigma\theta^7\sigma^{-1} = \theta^5.$$

It follows that the cyclic subgroup $\langle\theta\rangle$ is normalized by the cyclic subgroup $\langle\sigma\rangle$, and hence it is normalized by $G = \langle\theta\rangle\langle\sigma\rangle$.

(j) Any element in G has a unique expression as a product $\theta^i\sigma^j$ where $0 \le i \le 7$ and $j = 0, 1$. From (i) we have that $\sigma\theta = \theta^3\sigma$. Using this, we easily calculate

$$(\theta\sigma)^2 = \theta\sigma\theta\sigma = \theta\theta^3\sigma\sigma = \theta^4,$$

$$(\theta\sigma)^3 = \theta^4\theta\sigma = \theta^5\sigma,$$

and, finally,

$$(\theta\sigma)^4 = ((\theta\sigma)^2)^2 = (\theta^4)^2 = \theta^8 = 1.$$

Hence the order of $\theta\sigma$ is 4. So G has at least three elements of order 4, namely $\theta\sigma$, θ^2 and θ^6. Hence it cannot be isomorphic to the dihedral group D_{16} which has only two elements of order 4 (all elements outside the cyclic normal subgroup of order 8 in D_{12} have order 2).

(k) $\langle\theta\rangle$ has order 8, and hence $\Phi(\langle\theta\rangle)$ is a degree 2 extension of $\mathbb{Q}$. Since θ fixes i, and $(\mathbb{Q}(i):\mathbb{Q}) = 2$, it follows that $\Phi(\langle\theta\rangle) = \mathbb{Q}(i)$.

$\langle\theta^2\rangle$ has order 4, and hence $\Phi(\langle\theta^2\rangle)$ is a degree 4 extension of $\mathbb{Q}$. Since θ^2 fixes $\alpha^4 = \sqrt{2}$ and i, and $(\mathbb{Q}(\sqrt{2}, i):\mathbb{Q}) = 4$, it follows that $\Phi(\langle\sigma\rangle) = (\mathbb{Q}(\sqrt{2}, i):\mathbb{Q}) = 4$.

$\langle\theta^4\rangle$ has order 2, and hence $\Phi(\langle\theta^4\rangle)$ is a degree 8 extension of $\mathbb{Q}$. Since θ^4 fixes $\alpha^2 = \sqrt[4]{2}$ and i , and since $(\mathbb{Q}(\sqrt[4]{2}, i):\mathbb{Q}) = 8$ (see Ex.VII.1), it follows that $\Phi(\langle\theta^2\rangle) = \mathbb{Q}(\sqrt[4]{2}, i)$.

$\langle\sigma\rangle$ has order 2, and hence $\Phi(\langle\sigma\rangle)$ is a degree 8 extension of $\mathbb{Q}$. Since σ fixes α, and since $(\mathbb{Q}(\alpha):\mathbb{Q}) = 8$, it follows that $\Phi(\langle\theta^2\rangle) = \mathbb{Q}(\alpha)$.

The group $H = \langle\theta^4, \sigma\rangle$ is generated by two commuting elements of order 2, so it is a Klein four group of order 4. Hence $\Phi(H)$ is a degree 4 extension of $\mathbb{Q}$. Since both θ^4 and σ fix $\alpha^2 = \sqrt[4]{2}$, and $(\mathbb{Q}(\sqrt[4]{2}):\mathbb{Q}) = 4$, it follows that $\Phi(H) = \mathbb{Q}(\sqrt[4]{2})$.

4. Let σ be an automorphisms of $\mathbb{R}$ that fixed all rational numbers (in fact, since $\mathbb{Q}$ is the prime subfield, any automorphism of $\mathbb{R}$ will be a $\mathbb{Q}$-automorphism). Let $\alpha \in \mathbb{R}$ with $\alpha > 0$. Then $\sqrt{\alpha} \in \mathbb{R}$, and we have $\sigma(\alpha) = \sigma(\sqrt{\alpha}\sqrt{\alpha}) = (\sigma(\sqrt{\alpha}))^2 > 0$. It follows that if $\alpha > \beta$ then $\sigma(\alpha) > \sigma(\beta)$. Consequently, if $\{a_n\}$ and $\{b_n\}$ are sequences of rational numbers converging to α such that $a_n > \alpha > b_n$ for all n, we get that $a_n = \sigma(a_n) > \sigma(\alpha) > \sigma(b_n) = b_n$ for all n, and hence $\sigma(\alpha) = \alpha$, i.e. σ is the identity map.