Answers for sample questions:

1. Compute the minimal polynomial of $i + \sqrt{2}$ over $\mathbb{Q}$.

   Answer 1: Let $\alpha = i + \sqrt{2}$ then $\alpha^0, \ldots, \alpha^4$ are: $1, i + \sqrt{2}, 1 + 2i\sqrt{2}, 5i - \sqrt{2}, -7 + 4i\sqrt{2}$ and we find $\alpha^4 - 2\alpha^2 + 9 = 0$, we find no linear relation between $\alpha^0, \ldots, \alpha^3$ and so $f := x^4 - 2x^2 + 9$ is the minpoly.

   Answer 2: you could also compute the product of $x - \sigma(\alpha)$ for all σ in the Galois group. The set of all these $\sigma(\alpha)$ is $\{\pm i \pm \sqrt{2}\}$. First multiply $(x + \sqrt{2} + i) \cdot (x - \sqrt{2} + i)$ to obtain $x^2 + 2ix - 3$. Then multiply that by its complex conjugate and you find f.

   Fastest method: Observe that $-\alpha$ is among the conjugates of α, so $-\alpha$ has the same minpoly as α. That means that $f(-x) = f(x)$ and so $f(x) = g(x^2)$ for some g. Another way to say that is that there must be a linear relation between $\alpha^0, \alpha^2, \alpha^4$. So we don't need to compute α^3. So square α twice, and look for a linear relation between $\alpha^0, \alpha^2, \alpha^4$.

2. Suppose $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 35$. Show that $\mathbb{Q}(\alpha^3) = \mathbb{Q}(\alpha)$.

   Answer: Let $F = \mathbb{Q}(\alpha)$ and $E = \mathbb{Q}(\alpha^3)$. Since $f := x^3 - \alpha^3$ is in $E[x]$ and has α as a root, we see that d, the degree of $F = E(\alpha)$ over E, is at most 3 (equality iff f is irreducible). But d also has to divide $[F : \mathbb{Q}] = 35$. The only number ≤ 3 that divides 35 is 1. So $d = 1$.

3. Let $K = \mathbb{Q}(\zeta_{16})$ and let $G = \{\sigma_1, \sigma_3, \sigma_5, \ldots, \sigma_{15}\}$ be the Galois group of K over $\mathbb{Q}$, where σ_i maps ζ_{16} to ζ_{16}^i. For each of the following subgroups H of G, write down:
   (i) the fixed field K^H, (ii) its degree $[K^H : \mathbb{Q}]$.

   (a) G: (i): $\mathbb{Q}$, (ii): deg $= 1$

   (b) $<\sigma_1>$: (i): K, (ii) deg $= 8$

   (c) $<\sigma_3>$: This group has order 4 so deg $= 8/4 = 2$. Since that is prime, any element $\notin \mathbb{Q}$ in that field will generate it. The orbit of ζ_{16} under this group is ζ_{16} raised to the powers $1, 3, 9, 11$. The orbit of $\zeta_8 = \zeta_{16}^2$ under this group is smaller: it is ζ_8, ζ_8^3. So their sum $\zeta_8 + \zeta_8^3$ is invariant under our group. That number is equal to $\sqrt{-2}$ (recall that $\zeta_8 = (1+i)/\sqrt{2}$) so our field is $\mathbb{Q}(\sqrt{-2})$.

   (d) $<\sigma_5>$: This group has order 4, so deg $= 8/4 = 2$. The orbit of ζ_{16} under this group is ζ_{16} raised to the powers $1, 5, 9, 13$. The orbit of $i = \zeta_{16}^4$ under this group is $\{i, i^5, i^9, i^{13}\} = \{i\}$ so i is in the fixed field, which must thus be $\mathbb{Q}(i)$ (when deg is prime, any number not in the base field will generate the field).

   (e) $<\sigma_7>$: This group has order 2, so deg $= 8/2 = 4$. The orbit of ζ_{16} is $\{\zeta_{16}, \zeta_{16}^7\}$ and so $\alpha := \zeta_{16} + \zeta_{16}^7$ is in the fixed field. We can compute all conjugates of α by applying each element the quotient group $G/<\sigma_7>$ to α, and we find 4 distinct conjugates. That means that $\mathbb{Q}(\alpha)$ (which $\subseteq$ fixed field) has degree 4 and thus equals the fixed field.

(f) $<\sigma_9>$: This group has order 2, so deg $= 8/2 = 4$. The group sends ζ_{16} to $\pm\zeta_{16}$ so we see that $\zeta_8 = \zeta_{16}^2$ is invariant. We already know that ζ_8 has degree 4 over $\mathbb{Q}$ so the fixed field is $\mathbb{Q}(\zeta_8) = \mathbb{Q}(i, \sqrt{2})$. Another way we could have concluded this is because $<\sigma^9>\subseteq<\sigma_3>$ but also $\subseteq<\sigma_5>$, so our fixed field must contain the fixed fields from exercises (c) and (d). Combining their generators gives $\mathbb{Q}(\sqrt{-2}, i) = \mathbb{Q}(i, \sqrt{2})$ and since this has degree 4 it must be the field that we are looking for.

(g) $<\sigma_{15}>$: This group has order 2, so the degree of the fixed field is $8/2 = 4$. The orbit of ζ_{16} is $\{\zeta_{16}, \zeta_{16}^{-1}\}$ and so $\beta := \zeta_{16} + \zeta_{16}^{-1}$ is in the fixed field. We can compute all conjugates of this (apply each element the quotient group $G/<\sigma_{15}>$ to β) and we find 4 distinct conjugates. That means that $\mathbb{Q}(\beta)$ ($\subseteq$ fixed field) has degree 4 and thus equals the fixed field.

(h) Which of the field(s) in questions (a)–(g) contains i?

Recall from item (d) that i is fixed by $<\sigma_5>= \{\sigma_1, \sigma_5, \sigma_9, \sigma_{13}\}$ so i is the fixed field of a group H if and only if $H \subseteq \{\sigma_1, \sigma_5, \sigma_9, \sigma_{13}\}$, which was the case for questions (b),(d),(f).

(i) Which of the field(s) in questions (a)–(g) is contained in $\mathbb{R}$?

Conjugation is σ_{15} so for K^H to be $\subseteq \mathbb{R}$ it needs to be invariant under σ_{15}, in other words $\sigma_{15} \in H$. That was true for (a) and (g).

Note: not all subgroups were listed in this exercise, there is another subgroup $H := \{\sigma_1, \sigma_7, \sigma_9, \sigma_{15}\}$. Since this group contains σ_{15}, its fixed field must be inside $\mathbb{R}$. But it must also be inside the subfields from exercises (e) and (f) because H contains σ_7 and σ_9. Intersecting $\mathbb{R}$ with the field from (f) we get $\mathbb{Q}(\sqrt{2})$ and thus $\sqrt{2}$ must also be an element of the field from (e). So if you (try this) compute a minpoly for exercise (e), then that minpoly has to factor (deg 2 times deg 2) over $\mathbb{Q}(\sqrt{2})$. To get such a degree 2 factor in $\mathbb{Q}(\sqrt{2})[x]$, multiply $x - \alpha$ by $x - \sigma_{15}(\alpha)$ To explain why that works: The orbit of $x - \alpha$ under H is $\{x - \alpha, x - \sigma_{15}(\alpha)\}$ (although H has order 4, this orbit has only 2 elements because $x - \alpha$ is invariant under σ_7). So the product $(x - \alpha)(x - \sigma_{15}(\alpha))$ is invariant under H, which means that its coefficients are in the fixed field, $\mathbb{Q}(\sqrt{2})$, of H.

4. Let $K = \mathbb{Q}(i, \sqrt[4]{3})$.

(a) What is the Galois group G of K over $\mathbb{Q}$? $D_{2\cdot 4}$ where complex conjugation (denote this with τ) acts as a reflection on the set of four complex roots of $x^4 - 3$ while σ (which we define by sending i to i and $\sqrt[4]{3}$ to $i\sqrt[4]{3}$) acts as a rotation on the set of roots.

(b) Give a subgroup H of G whose fixed field is:

i. $\mathbb{Q}(i)$: $<\sigma>$ which is a group of order 4.

ii. $\mathbb{Q}(\sqrt[4]{3})$: $<\tau>$ which is a group of order 2.

iii. $\mathbb{Q}(i\sqrt[4]{3})$: Comparing this with (b) we see that $i\sqrt[4]{3}$ is another root of the same irreducible polynomial x^4-3. So the fields in (b),(c) are isomorphic and thus the group for (c) should be a conjugate of the group for (b). But the group $<\tau>$ from (b) only has one conjugate not equal to itself, and to find it, we should conjugate with something that doesn't commute with τ, we can take σ. Result: $<\tau'>$ where $\tau' = \sigma\tau\sigma^{-1}$. Indeed, applying τ' to $i\sqrt[4]{3}$ (apply σ^{-1}, then τ, then σ) sends that number to itself.

5. Let $K := \mathbb{Q}(\zeta_{16})$ and let G be its Galois group. For each of the following subfields E, write down an explicit group $H \leq G$ such that E is the fixed field of H. You do not need to explain your answers for (a)–(f).

(a) $E_1 := K$. $H_1 = \{1\}$.

(b) $E_2 := \mathbb{Q}$. $H_2 = G = (\mathbb{Z}/(16))^* = \{1,3,5,7,9,11,13,15\}$.

(c) $E_3 := K \bigcap \mathbb{R}$. $H_3 = \{1,15\} = \{1,-1\}$.

(d) $E_4 := \mathbb{Q}(\zeta_{16} + \zeta_{16}^7)$. $H_4 = \{1,7\}$, which is a group since $7^2 \equiv 1 \bmod 16$.

(e) $E_5 := \mathbb{Q}(\zeta_8)$. $H_5 = \{1,9\}$,which is a group since $9^2 \equiv 1 \bmod 16$. The "9" in H_5 sends $\zeta_8 = \zeta_{16}^2$ to $(\zeta_{16}^9)^2 = \zeta_8$.

(f) $E_6 := \mathbb{Q}(\zeta_4)$. This is a subfield of E_5 so the group should become larger than H_5. We find $H_6 = \{1,5,9,13\}$ since they send $\zeta_4 = (\zeta_{16})^4$ to ζ_4^i (with $i \in \{1,5,9,13\}$) all of which are equal to ζ_4.

(g) $E_7 :=$ The intersection of E_3 and E_5. This group should contain H_3 and H_5. We find $H_7 = <-1,9> = \{1,7,9,15\}$.

(h) What is $[E_7 : \mathbb{Q}]$? This equals $[K : \mathbb{Q}]/|H_7| = 8/4 = 2$.

(i) Is $E_7 \subseteq E_4$? Yes, because $H_4 \subseteq H_7$.

6. Let $K = \mathbb{Q}(i, \sqrt[4]{3})$ and let $G = <\tau, \sigma>$ where τ is complex conjugation, $\tau : i \mapsto -i$, and σ sends i to i and $\sqrt[4]{3}$ to $i\sqrt[4]{3}$. Let $h = \tau\sigma^2$ and $H = <h>$. What is K^H?

h sends i to $-i$ and sends $\sqrt[4]{3}$ to $-\sqrt[4]{3}$ so it keeps $\alpha := i\sqrt[4]{3}$ invariant. The degree of α over $\mathbb{Q}$ is 4 (minpoly is x^4-3) so it generates K^H. Answer: $\mathbb{Q}(\alpha)$.

7. Suppose that $K/\mathbb{Q}$ is Galois and that its Galois group G is a simple group. Suppose that E is a proper subfield, i.e. $\mathbb{Q} \subsetneq E \subsetneq K$. Show that $E/\mathbb{Q}$ is not Galois.

The group E is the fixed field of some subgroup H of G. Since E is a proper subfield, H is a proper subgroup (not equal to G or to $\{1\}$) but in a simple group, there are no normal proper subgroups. So H is not a normal subgroup, which is equivalent to saying that its fixed field is not Galois over $\mathbb{Q}$.

8. Suppose that $K/\mathbb{Q}$ is Galois with group G. Suppose that $\alpha \in K$ and that $\sigma \in Z(G)$, the center of G. Show that $\sigma(\alpha) \in \mathbb{Q}(\alpha)$.

   Let $E := \mathbb{Q}(\alpha)$ and let $H \leq G$ with $E = K^H$. Let $h \in H$. Then $h(\sigma(\alpha)) = \sigma(h(\alpha))$ because σ, h commute. But $h(\alpha) = \alpha$. Hence h leaves $\sigma(\alpha)$ invariant. This is true for every $h \in H$, hence $\sigma(\alpha)$ is an element of the fixed field of H, which is $\mathbb{Q}(\alpha)$.

9. Let E be a subfield of $\mathbb{Q}(\zeta_{17})$, not equal to $\mathbb{Q}(\zeta_{17})$. Show that $E \subset \mathbb{R}$.

   The Galois group G is cyclic of order 16, and the cyclic group of order 16 has a very simple subgroup structure: $C_1 \subset C_2 \subset C_4 \subset C_8 \subset C_{16}$. So if $K = \mathbb{Q}(\zeta_{17})$ and $E \neq K$ is a subfield, then $E = K^H$ where H is one of these groups: $C_2 \subset C_4 \subset C_8 \subset C_{16}$. In particular, H will contain the unique element of G with order 2. That element is complex conjugation. So $E = K^H$ is invariant under complex conjugation, and thus $\subseteq \mathbb{R}$.

   Bonus exercise: Show that $E \subseteq \mathbb{Q}(\cos(2\pi/17))$.

10. Let $K := \mathbb{Q}(\zeta_{16}) \bigcap \mathbb{R}$. Show that K is Galois over $\mathbb{Q}$, and give its Galois group.

    Let $F = \mathbb{Q}(\zeta_{16})$. This F is a splitting field over $\mathbb{Q}$ (e.g. for $x^{16} - 1$, or for $x^8 + 1$) and so it is a Galois over $\mathbb{Q}$. The Galois group is the group of units in $\mathbb{Z}/(16)$, which is $G := (\mathbb{Z}/(16))^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ and is isomorphic to $C_2 \times C_4$. The field K is the fixed field of $H := \{1, 15\}$, which is a normal subgroup of G (all subgroups of an abelian group are normal) and thus K must be Galois over $\mathbb{Q}$ with group G/H which is isomorphic to C_4 (to see this, note that 3 still has order 4 even when you work mod H).

11. Let $K = \mathbb{Q}(\zeta_{13})$.

    (a) Is K Galois over $\mathbb{Q}$?.

    Yes, $\mathbb{Q}(\zeta_n)$ is Galois, with Galois group $(\mathbb{Z}/(n))^*$. With $n = 13$, we find $G := (\mathbb{Z}/(13))^* \cong C_{12}$.

    (b) How many subfields does K have.

    In general, the subgroups of C_N are in 1-1 correspondence with the divisors of N. The divisors of 12 are: 1,2,3,4,6,12. So there are 6 subgroups, and hence, 6 subfields by the Galois correspondence.

    (c) How many of subfields of K are inside $\mathbb{R}$?

    A subfield $E \subseteq K$ is inside $\mathbb{R}$ if and only if the elements of E are fixed under complex conjugation. Now complex conjugation sends ζ_{13} to $\zeta_{13}^{-1} = \zeta_{13}^{12}$. So complex conjugation corresponds to the element

$[-1] = [12] \in G$.

Complex conjugation is the only element in G of order 2, because a cyclic group of even order has only 1 element of order 2. So the subgroups of G that contain this element of order 2 are precisely the subgroups of even order: C_2, C_4, C_6, and C_{12}. Therefore, the fixed fields of these four subgroups are the subfields of $K \bigcap \mathbb{R}$. Hence K has 4 subfields inside $\mathbb{R}$.

(d) Does there exist an element $a \in K$ with $a \notin \mathbb{R}$ and $\mathbb{Q}(a) \neq K$? If so, then write down an example of such a.

In part (c) we showed that if $\mathbb{Q}(a) \subseteq K$, and $\mathbb{Q}(a) \not\subseteq \mathbb{R}$, then $\mathbb{Q}(a)$ must the fixed field of a subgroup of G with odd order, i.e., C_1 or C_3. We can rule out C_1 because $\mathbb{Q}(a) \neq K$. Hence $\mathbb{Q}(a)$ is the fixed field of C_3. Here C_3 is the set of elements of order 1 and 3 in G, we need to find those elements. Now $[1]$ has order 1, with some computation one finds that $[2]$ has order 12, so $[2]^4$ must then have order $12/4 = 3$. Now $[2]^4 = [3]$. So $C_3 =< [3] >= \{[1], [3], [9]\} \subseteq (\mathbb{Z}/(13))^*$. Now $a \in K$ must be invariant under this group. We can take $a := \zeta_{13}^1 + \zeta_{13}^3 + \zeta_{13}^9$. This a is in the fixed field of C_3. In particular $\mathbb{Q}(a) \neq K$. Drawing these three powers of ζ_{13} on the unit circle, one sees that $\mathrm{Im}(\zeta_{13}^3 + \zeta_{13}^9)$ is slightly more than 0. The imaginary part of ζ_{13} is also positive. Hence $\mathrm{Im}(a) > 0$, so $a \notin \mathbb{R}$.

12. Let $\zeta = e^{2\pi i/31}$ be a primitive 31'th root of unity, and let

$$\alpha = \zeta + \zeta^2 + \zeta^4 + \zeta^8 + \zeta^{16}.$$

Let $K = \mathbb{Q}(\zeta)$ and $E = \mathbb{Q}(\alpha)$. Let G be the Galois group of K over $\mathbb{Q}$.

(a) Write down the group G and the order of G.

$G \cong (\mathbb{Z}/(31))^*$ is a cyclic group of order 30.

(b) Explain why E must be Galois over $\mathbb{Q}$.

By Galois correspondence, the subfields of K correspond to the subgroups of G, and a subfield is Galois over $\mathbb{Q}$ iff the corresponding subgroup is a normal subgroup. But G is abelian, so every subgroup is normal, and hence every subfield of K is Galois over $\mathbb{Q}$.

(c) Prove that $[E : \mathbb{Q}] \leq 6$ (hint: Write down a subgroup $H \leq G$ such that α is in the fixed field of H).

The group G is isomorphic to $(\mathbb{Z}/(31))^*$ which is cyclic of order 30, and this isomorphism is as follows, if $i \in (\mathbb{Z}/(31))^*$ then the corresponding isomorphism $\sigma_i : K \to K$ is the isomorphism that sends ζ to ζ^i. Now let $H =<2> = \{\sigma_1, \sigma_2, \sigma_4, \sigma_8, \sigma_{16}\} \subseteq G = (\mathbb{Z}/(31))^*$. Then $\alpha = \sum_{h \in H} h(\zeta)$ which is clearly invariant under H, and hence α is in the fixed field K^H of H. Now $[K : K^H]$ equals the order of

H, which is 5, and hence $[K^H : \mathbb{Q}] = 30/5 = 6$. Since α, and hence E, sits in K^H, we get $[E : \mathbb{Q}] \leq 6$.

(d) Prove that $[E : \mathbb{Q}] = 6$.

We have to show that α is algebraic over $\mathbb{Q}$ of degree 6, which is equivalent to saying that α has 6 distinct conjugates. Applying the σ_i to α (take one σ_i from each coset mod H) (so one σ_i for each element of G/H) one can find 6 distinct conjugates (one of them, $\sigma_3(\alpha)$, can be seen in the next question).

(e) Let $\beta = \zeta^3 + \zeta^6 + \zeta^{12} + \zeta^{24} + \zeta^{48}$ (note: $\zeta^{48} = \zeta^{17}$). Prove that $\beta \in E$.

Method 1: This number is $\beta = \sigma_3(\alpha)$ so it is a conjugate of α. But $E = \mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$, and this implies that any conjugate of any element of E is again an element of E.
Method 2: β is invariant under σ_2 (the generator of H) and so β is in K^H. But using the previous question we see that K^H is the same as E.