Fields.

1. Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 5 and let $g \in \mathbb{Q}[x]$ be an irreducible polynomial of degree 7. Let $\alpha \in \mathbb{C}$ be a root of f and $\beta \in \mathbb{C}$ be a root of g. Let $K_1 = \mathbb{Q}(\alpha)$, $K_2 = \mathbb{Q}(\beta)$ and $K_3 = \mathbb{Q}(\alpha, \beta)$.

   (a) Give: $[K_1 : \mathbb{Q}]$, $[K_2 : \mathbb{Q}]$, $[K_3 : \mathbb{Q}]$, $[K_3 : K_1]$ and $[K_3 : K_2]$.

   ANSWER: 5, 7, 35, $[K_3 : \mathbb{Q}]/[K_1 : \mathbb{Q}] = 35/5 = 7$, $[K_3 : \mathbb{Q}]/[K_2 : \mathbb{Q}] = 35/7 = 5$.
   The reason that $[K_3 : \mathbb{Q}]$ is 35 is because it must be divisible by $[K_1 : \mathbb{Q}]$ and $[K_2 : \mathbb{Q}]$ since K_1 and K_2 are subfields of K_3. So it must be divisible by 35. It can not be larger than 35 because that would make $[K_3 : K_1]$ larger than 7, so that would make the minpoly of β over K_1 have higher degree than its minpoly over $\mathbb{Q}$, which can not be.

   (b) Is f reducible or irreducible in $K_1[x]$? Why?

   ANSWER: Reducible because it has a root in K_1.

   (c) Is f reducible or irreducible in $K_2[x]$? Why?

   ANSWER: Irreducible because $[K_2(\alpha) : K_2] = 5$ (see part (a)), so the minpoly of α over K_2 has degree 5. Then this minpoly can only be f. But a minpoly is always irreducible.

2. Let p be a prime number, let $S = \{f(x) \in \mathbb{Q}[x] \,|\, f(x) \notin \mathbb{Q},\ \deg(f) < p\}$. Let $m(x)$ be any irreducible polynomial in $\mathbb{Q}[x]$ of degree p, and let $f(x)$ be any element of S. Show that there exists a unique $g(x) \in S$ for which $g(f(x)) - x$ is divisible by $m(x)$.
   Start as follows: Let α be a root of $m(x)$, let $\beta = f(\alpha)$, now prove that there exists a polynomial $g(x) \in S$ with $g(\beta) = \alpha$.

   ANSWER: Since $f(x)$ is not divisible by $m(x)$, the number β is not 0, but it is also not in $\mathbb{Q}$ because $f(x)$ is not a constant. So $\mathbb{Q}(\beta) \neq \mathbb{Q}$, but it is a subfield of $\mathbb{Q}(\alpha)$ since $\beta \in \mathbb{Q}(\alpha)$. Now $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a prime number, so there can not be a proper intermediate field. So when $\mathbb{Q} \neq \mathbb{Q}(\beta) \subseteq \mathbb{Q}(\alpha)$ then $\mathbb{Q}(\beta)$ must be $\mathbb{Q}(\alpha)$, so $\alpha \in \mathbb{Q}(\beta)$. Then there must exist a polynomial g of degree $< p$ with $g(\beta) = \alpha$. So $g(f(\alpha)) - \alpha = 0$ and so α is a root of $g(f(x)) - x$. Then $g(f(x)) - x$ must be dvisible by the minpoly of α.

3. Let K be the splitting field of the polynomial $x^6 - 2$ over $\mathbb{Q}$. The Galois group G is isomorphic to $D_{2 \cdot 6}$ and can be written using two generators as follows $G = <\sigma, \tau>$, where σ is defined by $\sigma(\sqrt[6]{2}) = \zeta_6 \sqrt[6]{2}$, $\sigma(\zeta_6) = \zeta_6$, and τ is defined by $\tau(\sqrt[6]{2}) = \sqrt[6]{2}$, $\tau(\zeta_6) = \zeta_6^5$ (note: τ is complex conjugation). For each of the following subgroups H of G, write down the corresponding subfield K_H, the fixed field of H. You do not need to give proofs.

   (a) $H_1 = G$ (a group of order 12)

   ANSWER: $\mathbb{Q}$

(b) $H_2 = \{1\}$ (a group of order 1)

ANSWER: K

(c) $H_3 = < \sigma >$ (a group of order 6)

ANSWER: $\mathbb{Q}(\zeta_6)$ (this equals $\mathbb{Q}(\sqrt{-3})$).

(d) $H_4 = < \tau >$ (a group of order 2)

ANSWER: $\mathbb{Q}(\sqrt[6]{2})$.

(e) $H_5 = < \sigma^2 >$ (a group of order 3)

ANSWER: $\mathbb{Q}((\sqrt[6]{2})^3, \zeta_6) = \mathbb{Q}(\sqrt{2}, \sqrt{-3})$.

(f) $H_6 = < \sigma^2, \tau\sigma >$ (a group of order 6)

ANSWER: The degree-2 subfields of the field in exercise (e) are: $\mathbb{Q}((\sqrt[6]{2})^3) = \mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\sqrt{-3})$, and $\mathbb{Q}(\sqrt{-6})$. Now $\tau\sigma$ sends $(\sqrt[6]{2})^3$ to $-(\sqrt[6]{2})^3$, and sends ζ_6 to its complex conjugate, so those first two fields are not the fixed fields. Then the only remaining option is that the fixed field is $\mathbb{Q}(\sqrt{-6})$.

4. Let K and G be as in the previous question. What is the group $H \leq G$ belonging to the subfield $\mathbb{Q}(\sqrt{2})$?
Hint: If $\sqrt{2}$ is an element of one of the fields you computed in the previous question, then the group H_i in that question will be a subgroup of the group H you need to find for this question. First check if this hint already gives you enough elements of H to generate H, if so, then write down those generators and you're done, if not, then you need to find more generators.

ANSWER: $\sqrt{2}$ is fixed by σ^2 but also by complex conjugation τ, so $H = < \sigma^2, \tau >$.