

Answers to Problem Sheet 11

1. $K = \mathbb{Q}$, since both roots lie in \mathbb{Q} , so $|G| = [\mathbb{Q} : \mathbb{Q}] = 1$ and $G = \{id\}$ (the trivial group). There is only one subgroup, and one intermediate field.

| | |
|--------------------|-----------------|
| $f = x^2 - 5x + 6$ | |
| subgroup | subfield |
| G | \mathbb{Q} |

2. $K = \mathbb{Q}(\sqrt{2})$, and $[K : \mathbb{Q}] = 2$ (since $\deg(\sqrt{2}, \mathbb{Q}) = 2$). $G = C_2$, the cyclic group of order 2 (it being the only group of order 2). The cyclic group of order 2 has no proper subgroups.

| | |
|-----------------------------------|---------------------------|
| $f = x^2 - 2$ | |
| subgroup of G | intermediate field |
| G | \mathbb{Q} |
| $\{id\}$ | K |

3. $x^4 - x^2 - 2 = (x^2 - 2)(x^2 + 1)$, so the splitting field is $K = \mathbb{Q}(\sqrt{2}, i)$. The Galois group is $G = C_2 \times C_2$ (a.k.a. the Klein 4-group). G is generated by the two \mathbb{Q} -automorphisms of K

$$\sigma : K \rightarrow K \quad \text{determined by} \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(i) = i$$

$$\tau : K \rightarrow K \quad \text{determined by} \quad \tau(\sqrt{2}) = \sqrt{2}, \quad \tau(i) = -i$$

Then $G = \{id, \sigma, \tau, \sigma\tau\}$ has three subgroups of order 2, one subgroup of order 1, and one subgroup of order 4.

| | |
|----------------------|-------------------------|
| $f = x^4 - x^2 - 2$ | |
| subgroup | subfield |
| G | \mathbb{Q} |
| $\{id, \sigma\}$ | $\mathbb{Q}(i)$ |
| $\{id, \tau\}$ | $\mathbb{Q}(\sqrt{2})$ |
| $\{id, \sigma\tau\}$ | $\mathbb{Q}(i\sqrt{2})$ |
| $\{id\}$ | K |

Since G is abelian, all subgroups are normal, and therefore all the intermediate fields are Galois extensions of \mathbb{Q} (which also follows from the fact that all the (proper) intermediate fields are all quadratic extensions of \mathbb{Q}).

4. The roots of $x^3 - 7$ are $\alpha_1 = 7^{\frac{1}{3}}$, $\alpha_2 = \zeta 7^{\frac{1}{3}}$ and $\alpha_3 = \zeta^2 7^{\frac{1}{3}}$ where $\zeta = e^{\frac{2\pi i}{3}}$. The splitting field is $K = \mathbb{Q}(7^{\frac{1}{3}}, \zeta 7^{\frac{1}{3}}, \zeta^2 7^{\frac{1}{3}}) = \mathbb{Q}(7^{\frac{1}{3}}, \zeta)$. Then $\mathbb{Q} \subsetneq \mathbb{Q}(7^{\frac{1}{3}}) \subsetneq \mathbb{Q}(7^{\frac{1}{3}}, \zeta) = K$. Noting that $\mathbb{Q} \neq \mathbb{Q}(7^{\frac{1}{3}})$ because $7^{\frac{1}{3}}$ is irrational, and $\mathbb{Q}(7^{\frac{1}{3}}) \neq \mathbb{Q}(7^{\frac{1}{3}}, \zeta)$ because $\mathbb{Q}(7^{\frac{1}{3}}) \subset \mathbb{R}$ and $\zeta \notin \mathbb{R}$. Then

$$\begin{aligned} |G| &= [K : \mathbb{Q}] && \text{(since it's a splitting field)} \\ &= [K : \mathbb{Q}(7^{\frac{1}{3}})][\mathbb{Q}(7^{\frac{1}{3}}) : \mathbb{Q}] \\ &= [K : \mathbb{Q}(7^{\frac{1}{3}})] \times 3 && \text{(since } \deg(7^{\frac{1}{3}}, \mathbb{Q}) = 3) \\ &\geq 2 \times 3 && \text{(since } \mathbb{Q}(7^{\frac{1}{3}}) \neq K) \end{aligned}$$

on the other hand,

$$|G| \leq |S_3| = 6 \quad \text{(since each element of } G \text{ permutes the roots of } f.)$$

It follows that $|G| = 6$, and G is isomorphic to S_3 . Any permutation of the roots is therefore realisable by a \mathbb{Q} -automorphism of K (unlike the previous example). We label each element of G by the corresponding permutation, e.g. (12) represents the automorphism determined by swapping α_1 and α_2 but leaving α_3 fixed.

| $f = x^2 - 7$ | |
|----------------------------|-------------------------|
| subgroup | subfield |
| $G = S_3$ | \mathbb{Q} |
| $H = \{id, (123), (132)\}$ | $L = \mathbb{Q}(\zeta)$ |
| $\{id, (12)\}$ | $\mathbb{Q}(\alpha_3)$ |
| $\{id, (13)\}$ | $\mathbb{Q}(\alpha_2)$ |
| $\{id, (23)\}$ | $\mathbb{Q}(\alpha_1)$ |
| $\{id\}$ | K |

The determination of L needs some explanation. Note that $\mathbb{Q}(\zeta)$ satisfies $\mathbb{Q} \subsetneq \mathbb{Q}(\zeta) \subsetneq K$ and so must appear on the list of intermediate fields. Since $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, the corresponding subgroup must be index 2 in G . Since H is the only such subgroup, its fixed subfield must be $\mathbb{Q}(\zeta)$.

Alternatively, note that $[L : \mathbb{Q}] = [G : H]$ by the Main Theorem, so $[L : \mathbb{Q}] = 2$. Now let $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$. Then $\delta \in L = K^H$ since it is fixed by the automorphism corresponding to the permutation (123). Therefore $\mathbb{Q}(\delta) \subseteq L$. Also, $\delta \notin \mathbb{Q}$ since it is not fixed by the automorphism corresponding to (12) (it sends δ to $-\delta$). Then $[\mathbb{Q}(\delta) : \mathbb{Q}] \geq 2$, and $2 = [L : \mathbb{Q}] = [L : \mathbb{Q}(\delta)][\mathbb{Q}(\delta) : \mathbb{Q}] \geq [L : \mathbb{Q}(\delta)] \times 2$ which implies that $[L : \mathbb{Q}(\delta)] = 1$ and $L = \mathbb{Q}(\delta)$. Note that $\mathbb{Q}(\delta) = \mathbb{Q}(\zeta)$ since $\delta = 2(1 - \zeta)^3 = -6(1 + 2\zeta)$.

The subfields $\mathbb{Q}(\alpha_1)$, $\mathbb{Q}(\alpha_2)$ and $\mathbb{Q}(\alpha_3)$ are not Galois extensions of \mathbb{Q} because the order 2 subgroups of S_3 are not normal (since, for example, $(23)(12)(23)^{-1} = (13)$).

5. This is a quadratic extension, as in question 2.
6. The roots of $x^5 - 1$ are $1, \xi, \xi^2, \xi^3$, and ξ^4 where $\xi = e^{\frac{2\pi i}{5}}$. The splitting field is $K = \mathbb{Q}(1, \xi, \xi^2, \xi^3, \xi^4) = \mathbb{Q}(\xi)$, and $[K : \mathbb{Q}] = 4$ since $\deg(\xi, \mathbb{Q}) = 4$. Any \mathbb{Q} -automorphism of K is determined by its affect on ξ . Since ξ and ξ^2 are both roots of the irreducible polynomial $\text{irr}(\xi, \mathbb{Q}) = \xi^4 + \xi^3 + \xi^2 + \xi + 1$, there is a \mathbb{Q} -automorphism sending ξ to ξ^2 . Let $\varphi \in G$ be such that $\varphi(\xi) = \xi^2$. Then $\varphi^2(\xi) = \xi^4$, $\varphi^3(\xi) = \xi^3$ and $\varphi^4(\xi) = \xi$. Therefore φ has order 4, and $G = C_4$ the cyclic group of order 4.

| $f = x^5 - 1$ | |
|---|---------------------------|
| subgroup | subfield |
| $G = \{id, \varphi, \varphi^2, \varphi^3\}$ | \mathbb{Q} |
| $\{id, \varphi^2\}$ | $\mathbb{Q}(\xi + \xi^4)$ |
| $\{id\}$ | K |

7. $f = x^4 + 1$ has roots $\zeta, -\zeta, \zeta^3, -\zeta^3$ where $\zeta = e^{\frac{\pi i}{4}}$. $K = \mathbb{Q}(\zeta)$ and $[K : \mathbb{Q}] = 4$. The four elements of G are determined by the four choices of image of ζ (namely $\zeta, -\zeta, \zeta^3$ or $-\zeta^3$). Each has order ≤ 2 in G . It follows that G is the group $C_2 \times C_2$. Since G is abelian, all its subgroups are normal. Therefore, all intermediate fields are Galois extensions of \mathbb{Q} .
8. $f = x^4 - 2$ has roots $2^{\frac{1}{4}}, i2^{\frac{1}{4}}, -2^{\frac{1}{4}}$ and $-i2^{\frac{1}{4}}$. The splitting field is $K = \mathbb{Q}(2^{\frac{1}{4}}, i)$. So $[K : \mathbb{Q}] = [\mathbb{Q}(2^{\frac{1}{4}}, i) : \mathbb{Q}(2^{\frac{1}{4}})][\mathbb{Q}(2^{\frac{1}{4}}) : \mathbb{Q}] = 2 \times 4 = 8$. That $[\mathbb{Q}(2^{\frac{1}{4}}) : \mathbb{Q}] = 4$ follows from the fact that $\deg(2^{\frac{1}{4}}, \mathbb{Q}) = 4$ since f is irreducible. Also, $\deg(i, \mathbb{Q}(2^{\frac{1}{4}})) = 2$ since i is a root of $x^2 + 1$ and this polynomial is irreducible over $\mathbb{Q}(2^{\frac{1}{4}})$ as it is quadratic and neither of its roots lie in $\mathbb{Q}(2^{\frac{1}{4}}) \subseteq \mathbb{R}$. So $|G| = 8$. The intermediate field $\mathbb{Q}(2^{\frac{1}{4}})$ is not a Galois extension of \mathbb{Q} .

To decide which group of order 8 we have, consider the \mathbb{Q} -automorphisms σ determined by $\sigma(2^{\frac{1}{4}}) = i2^{\frac{1}{4}}$ and $\sigma(i) = i$, and τ determined by $\tau(2^{\frac{1}{4}}) = 2^{\frac{1}{4}}$ and $\tau(i) = -i$. Then σ has order 4, τ has order 2 and $\tau\sigma\tau^{-1} = \sigma^{-1}$. It follows that the group is D_4 the dihedral group of a square. The subgroup of G generated by τ is not normal in G . Its fixed field $\mathbb{Q}(2^{\frac{1}{4}})$ is not a Galois extension of \mathbb{Q} .