Homework 8

1. i) K finite normal $/F \Rightarrow K$ is a splitting field over F and K is separable over F.

Let $X \subseteq F[x]$ be the set of polynomials that F is the splitting field of. Since $F[x] \subseteq E[x]$ we see that $X \subseteq E[x]$, so K is a splitting field over E.

Since $F \subseteq E \subseteq K$ and K is separable over F, Theorem 51.9 tells us that K is separable over E.

So K is a finite normal extension of E.

ii) Elements of $G(K/E)$ are automorphisms of K that fix E. Since $F \subseteq E$, there automorphisms fix F, too. So we can write $G(K/E) \leq G(K/F)$.

Let H be the subgroup of $G(K/F)$ defined to be

$$H = \{\sigma \in G(K/F) : \sigma \text{ fixes } E\} \leq G(K/F).$$

We need to show that $H = G(K/E)$.

Actually we don't need to show this, it's true by definition.

iii) if $\sigma|_E = \tau|_E$, then $(\sigma|_E)^{-1} \circ (\tau|_E)$ is the identity on E, which means $\sigma^{-1} \circ \tau|_E$ = identity on E, so $\sigma^{-1} \circ \tau \in G(K/E)$, so $\sigma^{-1} \circ \tau\, G(K/E) = G(K/E)$,

so $\tau\, G(K/E) = \sigma\, G(K/E)$.

2: $\quad x^4 - x^2 - 2 = (x^2-2)(x^2+1)$,

which has roots $\pm\sqrt{2}, \pm i$, so its splitting field over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, i)$.

Since $\mathbb{Q}$ is perfect, $\mathbb{Q}(\sqrt{2}, i)$ is a separable extension of $\mathbb{Q}$, so

$$4 = [\mathbb{Q}(\sqrt{2},i):\mathbb{Q}] = \{\mathbb{Q}(\sqrt{2},i):\mathbb{Q}\} = \left| G\left(\mathbb{Q}(\sqrt{2},i)/\mathbb{Q}\right)\right|$$

Automorphisms of $K = \mathbb{Q}(\sqrt{2}, i)$ that fix $\mathbb{Q}$ are determined by their values on $\sqrt{2}$ and on i. Since elements can only be sent to their conjugates, we know that for $\sigma \in G(K/\mathbb{Q})$, $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(i) = \pm i$. This describes all four elements of $G(K/\mathbb{Q})$:

$$\left\{ id,\ \left(\sigma_1 : \begin{matrix}\sqrt{2}\mapsto -\sqrt{2} \\ i \mapsto i\end{matrix}\right),\ \left(\sigma_2 : \begin{matrix}\sqrt{2}\mapsto \sqrt{2} \\ i \mapsto -i\end{matrix}\right),\ \left(\sigma_3 : \begin{matrix}\sqrt{2}\mapsto -\sqrt{2} \\ i \mapsto -i\end{matrix}\right) \right\}.$$

with subgroups

$$\begin{tikzcd}
 & \boxed{G(K/\mathbb{Q})} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
\boxed{\langle\sigma_1\rangle} \arrow[dr, dash] & \boxed{\langle\sigma_2\rangle} \arrow[d, dash] & \boxed{\langle\sigma_3\rangle} \arrow[dl, dash] \\
 & \boxed{\langle id\rangle} &
\end{tikzcd}$$

fixes $\mathbb{Q}$

fixes $\mathbb{Q}(\sqrt{2})$ $\quad$ fixes $\mathbb{Q}(i\sqrt{2})$

fixes $\mathbb{Q}(i)$

fixes $\mathbb{Q}(\sqrt{2}, i)$

3. $$x^7 - 1 = (x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

this has roots $\alpha = e^{\frac{2\pi i}{7}} = \cos\left(\frac{2\pi}{7}\right) + i \sin\left(\frac{2\pi}{7}\right)$,

as well as $\alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6$.

The splitting field of $x^7 - 1$ over $\mathbb{Q}$ is therefore $\mathbb{Q}(\alpha)$, which is a degree 6 extension of $\mathbb{Q}$.

Since $\mathbb{Q}$ is perfect, $\mathbb{Q}(\alpha)$ is separable $/\mathbb{Q}$, so

$$6 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \{\mathbb{Q}(\alpha) : \mathbb{Q}\} = |G(\mathbb{Q}(\alpha)/\mathbb{Q})|.$$

Any $\sigma \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$ is determined by $\sigma(\alpha)$, which must be in $\{\alpha^1, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$. the 6 automorphisms σ_i determined by $\sigma_i(\alpha) = \alpha^i$ (for $1 \leq i \leq 6$) give the full group of automorphisms of $\mathbb{Q}(\alpha)$ fixing $\mathbb{Q}$.

the composition $\sigma_i \circ \sigma_j$ sends α to $(\alpha^j)^i$ $= \alpha^{ji} = \alpha^{ji \bmod 7}$, since $\alpha^7 = 1$. so the group $\{\sigma_1, \ldots, \sigma_6\}$ with composition is isomorphic to the group $\{1, 2, \ldots, 6\}$ with multiplication mod 7.

This group is cyclic, generated by σ_3. It has two proper non-trivial subgroups: $\langle \sigma_2 \rangle = \{\sigma_1, \sigma_2, \sigma_4\}$ and $\langle \sigma_6 \rangle = \{\sigma_1, \sigma_6\}$, with subgroup diagram

$$\begin{tikzcd}
 & \boxed{G(\mathbb{Q}(\alpha)/\mathbb{Q})} \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \text{fixes } \mathbb{Q} \arrow[l] \\
\mathbb{Q}(\alpha+\alpha^2+\alpha^4) \arrow[r, dash] & & \mathbb{Q}(\alpha+\alpha^6) \arrow[d, dash] \\
\boxed{\langle \sigma_2 \rangle} \arrow[dr, dash, "2"'] & & \boxed{\langle \sigma_6 \rangle} \arrow[dl, dash, "3"] \\
 & \boxed{\langle \sigma_1 \rangle} & \text{fixes } \mathbb{Q}(\alpha) \arrow[l]
\end{tikzcd}$$

(explained below)

The fixed fields of the full Galois group and its trivial subgroup are straightforward. But what about the intermediate subgroups? Consider what σ^2 does to the roots of $x^7 - 1$:

$$\sigma_2 : \quad \begin{aligned} \alpha &\longrightarrow \alpha^2 \\ \alpha^2 &\longrightarrow \alpha^4 \\ \alpha^3 &\longrightarrow \alpha^6 \\ \alpha^4 &\longrightarrow \alpha^1 \\ \alpha^5 &\longrightarrow \alpha^3 \\ \alpha^6 &\longrightarrow \alpha^5 \end{aligned}$$

Note that $\alpha^1 \to \alpha^2 \to \alpha^4$. This means that

$\alpha^1 + \alpha^2 + \alpha^4$ is fixed by σ^2. We'd like to show that $\mathbb{Q}(\alpha + \alpha^2 + \alpha^4)$ is a degree 2 extension of $\mathbb{Q}$, because then we'll have found the entire fixed field of $\langle \sigma_2 \rangle$ (by degree consideration, using main thm here).

Let $\beta = \alpha + \alpha^2 + \alpha^4$.

then $\beta^2 = \alpha^2 + \alpha^3 + \alpha^5 + \alpha^3 + \alpha^4 + \alpha^6 + \alpha^5 + \alpha^6 + \underbrace{\alpha^8}_{=\alpha}$.

$= \alpha^2 + 2\alpha^3 + \alpha^4 + 2\alpha^5 + 2\alpha^6 + \alpha$

[Recall that $\alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 = -1$] $\circledast$

$= -1 + \alpha^3 + \alpha^5 + \alpha^6$

Then $\beta^2 + \beta$

$= -1 + \alpha^3 + \alpha^5 + \alpha^6 + \alpha + \alpha^2 + \alpha^4$ (rearrange:)

$= -1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6$

$= -2$ by above $\circledast$.

so $\beta^2 + \beta + 2 = 0$. Since $x^2 + x + 2$ is irred./$\mathbb{Q}$, this shows $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$ and thus it is the entire fixed field of $\langle \sigma_2 \rangle$.

σ_6 acts on α by

$$\begin{aligned} \alpha^1 &\longrightarrow \alpha^6 \\ \alpha^2 &\longrightarrow \alpha^5 \\ \alpha^3 &\longrightarrow \alpha^4 \\ \alpha^4 &\longrightarrow \alpha^3 \\ \alpha^5 &\longrightarrow \alpha^2 \\ \alpha^6 &\longrightarrow \alpha^1. \end{aligned}$$

we note that $\alpha^1 \rightleftarrows \alpha^6$. so $\alpha^1 + \alpha^6$

is fixed by σ_6.

Let $\gamma = \alpha^1 + \alpha^6$. By a similar ~~[illegible]~~ computation as with β, we can show that $\gamma^3 + \gamma - 2\gamma - 1 = 0$.

so $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 3$ (since $x^3 + x - 2x - 1$ is irreducible.)

Again, since the fixed field of $\langle \sigma_6 \rangle$ is degree $3/\mathbb{Q}$, this proves that $\mathbb{Q}(\gamma)$ is the fixed field of this subgroup.

4. As we've seen on previous HW, the splitting field of $x^3 - 2$ is a degree 6 extension of $\mathbb{Q}$, and its Galois group $G(\mathbb{Q}(\sqrt[3]{2}, \frac{-1+i\sqrt{3}}{2})/\mathbb{Q})$ is isomorphic to S_3.

Meanwhile, $x^3-1 = (x-1)(x^2+x+1)$ has splitting field $\mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right)$, a degree 2 extension of $\mathbb{Q}$, with Galois group cyclic of order 2, generated by complex conjugation

$$\frac{-1+i\sqrt{3}}{2} \longmapsto \frac{-1-i\sqrt{3}}{2}.$$

x^3-1 has a splitting field of lower degree and a smaller automorphism group.

My expectation is that the Galois group of and splitting field x^3-5 would look like that of x^3-2, But x^3-8 would look like x^3-1. This is because x^3-3 and x^3-5 are irreducible $/\mathbb{Q}$, while x^3-1 and x^3-8 factor over $\mathbb{Q}$ in similar ways.