HW 5 solutions

1. Consider the following diagram of field extensions:

$$\begin{tikzcd}
& \overline{F} \arrow[d, dash] \\
\overline{E} \arrow[r, dotted, "\sigma"] \arrow[d, dash] & L \arrow[dd, dash] \\
E \arrow[d, dash] & \\
F \arrow[r, "id"] & F
\end{tikzcd}$$

Since $F \subseteq E$ is algebraic and $E \subseteq \overline{E}$ is algebraic we know $F \subseteq \overline{E}$ is algebraic.

So we can apply the isom. extension thm to say that $\exists\ \sigma : \overline{E} \to L$ an isom, where L is a subfield of $\overline{F}$.

Our goal is to show $L = \overline{F}$, so that $\sigma : \overline{E} \to \overline{F}$ is the isom. we want.

Suppose $\exists\ \alpha \in \overline{F}$, $\alpha \notin L$. let $f(x) \in L[x]$ be the min. poly. of α (Note: since $\overline{F}$ is alg./F, it is also alg / ~~any~~ any intermediate field, so we can assume α is alg. / L). Since $\alpha \notin L$, $\deg(f(x)) > 1$.

$\sigma^{-1} : L \to \overline{E}$ gives an isom $\tilde{\sigma}^{-1} : L[x] \to \overline{E}[x]$ defined by applying σ^{-1} to coefficients.

Since $\tilde{\sigma}^{-1}$ is a isom, $f(x)$ irred. in $L[x] \Rightarrow$ $\tilde{\sigma}^{-1}(f(x))$ is irred. in $\overline{E}[x]$, a contradiction since $\overline{E}$ is algebraically closed. So in fact, $L = \overline{F}$ and σ is an isom from $\overline{E}$ to $\overline{F}$

2. Let $w = \dfrac{-1 + i\sqrt{3}}{2}$. we need:

a.

$$\mathbb{Q}(\beta_1, \beta_2, \beta_3) = \mathbb{Q}(\beta_1, w) = \mathbb{Q}(\beta_1, i\sqrt{3}).$$

Note that $w^2 = \dfrac{-1 - i\sqrt{3}}{2}$.

So $\left.\begin{array}{l}\beta_2 = \beta_1 w \\ \beta_3 = \beta_1 w^2\end{array}\right\}$ this shows $\mathbb{Q}(\beta_1, \beta_2, \beta_3) \subseteq \mathbb{Q}(\beta_1, w)$.

And $\left. w = \dfrac{\beta_3}{\beta_2} \right\}$ this shows $\mathbb{Q}(\beta_1, w) \subseteq \mathbb{Q}(\beta_1, \beta_2, \beta_3)$.

therefore, the first equality holds.

Now, $\left. 2w + 1 = i\sqrt{3}. \right\}$ This shows $\mathbb{Q}(\beta_1, i\sqrt{3}) \subseteq \mathbb{Q}(\beta_1, w)$.

And $\left. \dfrac{(i\sqrt{3}) - 1}{2} = w. \right\}$ This shows $\mathbb{Q}(\beta_1, w) \subseteq \mathbb{Q}(\beta_1, i\sqrt{3})$.

so the second equality holds.

The splitting field of $x^3 - 2$ is the smallest subfield of $\overline{\mathbb{Q}}$ containing the roots of $x^3 - 2$. $\mathbb{Q}(\beta_1, \beta_2, \beta_3)$ is the smallest subfield of $\overline{\mathbb{Q}}$ containing $\beta_1, \beta_2, \beta_3$. Hence, they're the same field.

b. The ring homomorphism $\dfrac{\mathbb{Q}[x]}{(x^3 - 2)} \xrightarrow{\varphi} \mathbb{Q}(\beta_1, \beta_2, \beta_3)$ defined by sending $x + (x^3 - 2)$ to β_1 is injective, and since β_1 is in $\mathbb{R}$, any $f(x) + (x^3 - 2)$ will also be sent to a real number. So φ is not surjective. Why does this mean that the quotient field is not the splitting field? Because if $\mathbb{Q}[x]/(x^3-2)$

contained <u>three</u> roots of x^3-2, then $\mathbb{Q}(\beta_1,\beta_2,\beta_3)$ would contain <u>five</u> roots of x^3-2 : the image of $x+(x^3-2)$, which is β_1, the images of the other two roots, which are real numbers, and β_2 and β_3. But this is impossible. So $\dfrac{\mathbb{Q}[x]}{(x^3-2)}$ isn't a splitting field for x^3-2.

c. An isomorphism $\dfrac{\mathbb{Q}[x]}{(x^3-2)} \xhookrightarrow{\tau} \mathbb{C}$ is determined by its value on $\alpha = x+(x^3-2)$. And $\tau(\alpha)$ must have x^3-2 as its minimal polynomial. So there are three possibilities, and the conjugation isomorphisms

$$\psi_{x+(x^3+2),\beta_1} : \frac{\mathbb{Q}[x]}{(x^3-2)} \hookrightarrow \mathbb{C}$$

$$\psi_{x+(x^3+2),\beta_2} : \frac{\mathbb{Q}[x]}{(x^3-2)} \hookrightarrow \mathbb{C}$$

$$\psi_{x+(x^3+2),\beta_3} : \frac{\mathbb{Q}[x]}{(x^3-2)} \hookrightarrow \mathbb{C}$$

tell you that all three are realized.

c. Since $\mathbb{Q}(\beta_1,\beta_2,\beta_3)$ is separable over $\mathbb{Q}$, we know

$$\{\mathbb{Q}(\beta_1,\beta_2,\beta_3):\mathbb{Q}\} = [\mathbb{Q}(\beta_1,\beta_2,\beta_3):\mathbb{Q}],$$ and we know $\mathbb{Q}(\beta_1) \subseteq \mathbb{Q}(\beta_1, i\sqrt{3})$ is a <u>proper</u> extension, and since x^2+3 has $i\sqrt{3}$ as a root, this extension can only have degree 2 (not 1, since it's proper). So

$$\underbrace{\mathbb{Q}\subseteq\mathbb{Q}(\beta_1)}_{3} \underbrace{\subseteq \mathbb{Q}(\beta_1, i\sqrt{3})}_{2}$$ tells us that the index $\{\mathbb{Q}(\beta_1,\beta_2,\beta_3):\mathbb{Q}\}$ is 6.

so there are 6 isomorphisms from $\mathbb{Q}(\beta_1, \beta_2, \beta_3)$ to a subfield of $\mathbb{C}$, but since it's a splitting field, they're all automorphisms.

d. an automorphism of $\mathbb{Q}(\beta_1, \beta_2, \beta_3)$ fixing $\mathbb{Q}$ is determined by its values on $\beta_1, \beta_2, \beta_3$. But these 3 elements can only be sent to their conjugates, i.e. each other. So the six permutations of the roots of $x^3 - 2$ determine the six automorphisms of $\mathbb{Q}(\beta_1, \beta_2, \beta_3)$ that fix $\mathbb{Q}$.

e. If σ is an automorphism that fixes $i\sqrt{3}$ (and $\mathbb{Q}$), then

$$\sigma(w) = \sigma\left(\frac{-1+i\sqrt{3}}{2}\right) = \frac{\sigma(-1) + \sigma(i\sqrt{3})}{\sigma(2)} = \frac{-1+i\sqrt{3}}{2} = w,$$

so σ fixes w. Similarly, σ fixes w^2. Then σ is determined by its values on $\beta_1, \beta_2, \beta_3$, or, equivalently, by its values on $\beta_1, \beta_1 w, \beta_1 w^2$. By the above, these values will be

$$\sigma(\beta_1)$$
$$\sigma(\beta_1 w) = \sigma(\beta_1) w$$
$$\sigma(\beta_1 w^2) = \sigma(\beta_1) w^2.$$

So the (three) automorphisms fixing $i\sqrt{3}$ are determined by:

$\beta_1 \mapsto \beta_1$

$\beta_2 = \beta_1 w \mapsto \beta_1 w = \beta_2$

$\beta_3 = \beta_1 w^2 \mapsto \beta_1 w^2 = \beta_2$

(id)

$\beta_1 \mapsto \beta_2$

$\beta_2 = \beta_1 w \mapsto \beta_2 w = \beta_1 w^2 = \beta_3$

$\beta_3 = \beta_1 w^2 \mapsto \beta_2 w^2 = \beta_1$

(σ)

$\beta_1 \mapsto \beta_3$

$\beta_2 = \beta_1 w \mapsto \beta_3 w = \beta_1$

$\beta_3 = \beta_1 w^2 \mapsto \beta_3 w^2 = \beta_2$

(σ^2)

3\. a $x^3 - 1 = (x-1)(x^2+x+1)$

has splitting field $\mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\right)$

$$= \mathbb{Q}\left(\frac{-1+i\sqrt{3}}{2}\right)$$

$$= \mathbb{Q}(i\sqrt{3}) \quad \text{by prev. problem.}$$

this extension has degree 2, since x^2+3 is the minimal polynomial of $i\sqrt{3}$ over $\mathbb{Q}$.

b. $x^4 - 1 = (x^2+1)(x+1)(x-1)$ has splitting field $\mathbb{Q}(i)$, which is degree 2 over $\mathbb{Q}$.

c. using 2, we know the splitting field will be $\mathbb{Q}(\beta_1, \beta_2, \beta_3, \sqrt{2})$. The question is, is $\sqrt{2}$ in $\mathbb{Q}(\beta_1, \beta_2, \beta_3)$ already, or is this a proper extension?

Note that $\mathbb{Q}(\beta_1, \beta_2, \beta_3) = \mathbb{Q}(\sqrt[3]{2}, i\sqrt{3})$ and has basis

$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, i\sqrt{3}, (\sqrt[3]{2})(i\sqrt{3}), (\sqrt[3]{2})^2(i\sqrt{3})\}$. If we write

$$\sqrt{2} = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 + d(i\sqrt{3}) + e(\sqrt[3]{2})(i\sqrt{3}) + f(\sqrt[3]{2})^2(i\sqrt{3}),$$

RHS has imaginary part $(d\sqrt{3} + e\sqrt[3]{2}\sqrt{3} + f(\sqrt[3]{2})^2\sqrt{3})$

$$= \sqrt{3}\left(d + e\sqrt[3]{2} + f(\sqrt[3]{2})^2\right)$$

$$= 0 \iff d = e = f = 0.$$

So we have $\sqrt{2} = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$

$$\Rightarrow \quad 2 = (a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2)$$

$$= a^2 + ab\sqrt[3]{2} + ac(\sqrt[3]{2})^2$$

$$+ ba\sqrt[3]{2} + b^2(\sqrt[3]{2})^2 + bc(\sqrt[3]{2})^3$$

$$+ ac(\sqrt[3]{2})^2 + bc(\sqrt[3]{2})^3 + c^2(\sqrt[3]{2})^4$$

$$= (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)(\sqrt[3]{2})^2$$

$$\Rightarrow \quad a^2 + 4bc = 2$$

$$2ab + 2c^2 = 0$$

$$2ac + b^2 = 0,$$ which has no rational solutions.

So $\mathbb{Q}(\beta_1, \beta_2, \beta_3) \subseteq \mathbb{Q}(\beta_1, \beta_2, \beta_3, \sqrt{2})$ is a proper extension of degree 2. So the splitting field of $(x^2-2)(x^3-2)$ is degree 12.

4. Since $F \subseteq E$ is a finite extension, we can assume $E = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some algebraic $\alpha_i \in E$. Let $f_i(x)$ be the minimal polynomial of α_i over F. Since E is a splitting field, E contains all roots of each $f_i(x)$. Now set $g(x) = \prod_{i=1}^{n} f_i(x)$.

Any field containing all roots of $g(x)$ ~~also~~ must contain $\{\alpha_1, \ldots, \alpha_n\}$, so contains E. So E is the smallest field containing all roots of $g(x)$. So E is the splitting field of $g(x)$.

5. E is a splitting field if and only if for every isomorphism τ from E to a subfield of $\overline{F}$ leaving F fixed, τ is actually an automorphism.

Let $f(x)$ be a polynomial with a root $\alpha \in E$. then for any root β of $f(x)$, $\beta \in \overline{F}$, we want to show $\beta \in E$, too.

consider $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$. By isom. extension, $\exists\ \tau$, $\tau : E \to$ a subfield of $\overline{F}$, with $\tau\big|_{F(\alpha)} = \psi_{\alpha,\beta}$. But since E is a splitting field, τ is an automorphism. So $\tau(\alpha) = \psi_{\alpha,\beta}(\alpha) = \beta$ is in E. So E contains all roots of $f(x)$.