

Homework 8 Solutions.

§6.4 #1. Determine the splitting fields in \mathbb{C} for the following polynomials (over \mathbb{Q}).

- (a) $x^2 - 2$. The roots are $\{\pm\sqrt{2}\}$; hence, a splitting field is $\mathbb{Q}(\sqrt{2})$.
- (b) $x^2 + 3$. The roots are $\{\pm\sqrt{-3}\}$; hence, a splitting field is $\mathbb{Q}(\sqrt{-3})$.
- (c) $x^4 + x^2 - 6$. Since $x^4 + x^2 - 6 = (x^2 + 3)(x^2 - 2)$, a splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{-3})$.
- (d) $x^3 - 5$. The roots are $\{\sqrt[3]{5}, \zeta_3\sqrt[3]{5}, \zeta_3^2\sqrt[3]{5}\}$. Hence, a splitting field is $\mathbb{Q}(\sqrt[3]{5}, \zeta_3)$.

§6.4 #2. Determine the splitting fields in \mathbb{C} for the following polynomials (over \mathbb{Q}).

- (a) $x^3 - 1$. Since $x^3 - 1 = (x - 1)(x^2 + x + 1)$, a splitting field is $\mathbb{Q}\left(\zeta_3 = \frac{-1 + \sqrt{-3}}{2}\right)$.
- (b) $x^4 - 1$. Since $x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$, a splitting field is $\mathbb{Q}(i)$.
- (c) $x^3 + 3x^2 + 3x - 4$. We observe that

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

Therefore, it has roots $\{-1 + \sqrt[3]{5}, -1 + \zeta_3\sqrt[3]{5}, -1 + \zeta_3^2\sqrt[3]{5}\}$. It follows that a splitting field is $\mathbb{Q}(\sqrt[3]{5}, \zeta_3)$.

§6.4 #4. Let p be prime. Determine the splitting field in \mathbb{C} for $x^p - 1$ (over \mathbb{Q}).

Claim. Let F be a splitting field for $f_p(x) = x^p - 1$, and let $\zeta_p = e^{\frac{2\pi i}{p}}$. Then we have $F = \mathbb{Q}(\zeta_p)$.

Proof. The roots of $f_p(x)$ are $\{\zeta_p^j : 0 \leq j \leq p - 1\}$. It follows that $F = \mathbb{Q}(\zeta_p)$. □

§6.4 #7. Prove that if F is an extension field of K of degree 2, then F is the splitting field over K for some polynomial.

Proof. Let $u \in F \setminus K$. Then we have $[K(u) : K] \mid [F : K] = 2$. Since $u \notin K$, we must have $[K(u) : K] = 2$, and $[F : K(u)] = 1$; it follows that $F = K(u)$. Let $f_{K,u}(x)$ be the minimal polynomial of u over K . It has degree 2, and we let its second root be v . We may therefore write $f_{K,u}(x) = x^2 + ax + b = (x - u)(x - v)$. Note that $a = -(u + v)$, so $v = -(a + u)$. Since $a \in K \subseteq K(u)$ and $u \in K(u)$, we have $v \in K(u)$. As such, $K(u)$ is a splitting field of $f_{K,u}(x)$. □

§6.4 #14. (a) Show that the splitting field of $x^4 - 2$ over \mathbb{Q} is $\mathbb{Q}(\sqrt[4]{2}, i)$.

Proof. The polynomial $f(x) = x^4 - 2$ has roots $\{\sqrt[4]{2}, \zeta_4 \sqrt[4]{2}, \zeta_4^2 \sqrt[4]{2}, \zeta_4^3 \sqrt[4]{2}\}$. Noting that $\zeta_4 = i$, we see that a splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$. \square

(b) Show that $\mathbb{Q}(\sqrt[4]{2}, i)$ is also the splitting field of $x^4 + 2$ over \mathbb{Q} .

Proof. The polynomial $f(x) = x^4 + 2$ has roots $\{\sqrt[4]{-2}, \zeta_4 \sqrt[4]{-2}, \zeta_4^2 \sqrt[4]{-2}, \zeta_4^3 \sqrt[4]{-2}\}$. Hence, a splitting field is $\mathbb{Q}(\sqrt[4]{-2}, i)$. We note that

$$\sqrt[4]{-1} = i^{1/2} = e^{\frac{\pi i}{4}} = \frac{\sqrt{2} + i\sqrt{2}}{2} = \frac{(1+i)\sqrt{2}}{2}.$$

It follows that

$$\sqrt[4]{-2} = \sqrt[4]{2} \cdot \sqrt[4]{-1} = \sqrt[4]{2} \cdot \frac{(1+i)(\sqrt[4]{2})^2}{2} = \frac{(1+i)(\sqrt[4]{2})^3}{2} \in \mathbb{Q}(\sqrt[4]{2}, i).$$

I.e., the field $\mathbb{Q}(\sqrt[4]{2}, i)$ is a splitting field. \square

§8.1 #4. In Example 8.1.2, find $\{x \in \mathbb{Q}(\sqrt{2} + \sqrt{3}) : \theta_2(x) = x\}$ and show that it is a subfield of $\mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Proof. Let $F = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. We showed that $F = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Define $\theta_2, \theta_3 \in G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$\begin{aligned} \theta_2 : \sqrt{2} &\mapsto -\sqrt{2}, \quad \sqrt{3} \mapsto \sqrt{3}; \\ \theta_3 : \sqrt{2} &\mapsto \sqrt{2}, \quad \sqrt{3} \mapsto -\sqrt{3}. \end{aligned}$$

The set $F^{\langle \theta_2 \rangle} = \{x \in F : \theta_2(x) = x\}$ is the fixed field of the subgroup $\langle \theta_2 \rangle \subseteq G_{F/\mathbb{Q}}$; hence, it is a field. Since F is a splitting field of the separable polynomial $(x^2 - 2)(x^2 - 3)$, we may apply the Galois correspondence to conclude that $[G_{F/\mathbb{Q}} : \langle \theta_2 \rangle] = 2 = [F^{\langle \theta_2 \rangle} : \mathbb{Q}]$. Moreover, since $\theta_2(\sqrt{3}) = \sqrt{3}$, we have $\mathbb{Q}(\sqrt{3}) \subseteq F^{\langle \theta_2 \rangle}$; since $[F^{\langle \theta_2 \rangle} : \mathbb{Q}] = 2$, it follows that $\mathbb{Q}(\sqrt{3}) = F^{\langle \theta_2 \rangle}$. \square

§8.1 #6. Show that the Galois group of $(x^2 - 2)(x^2 + 2)$ over \mathbb{Q} is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. We note that the roots of $f_1(x) = x^2 - 2$ are $\{\pm\sqrt{2}\}$; the roots of $f_2(x) = x^2 + 2$ are $\{\pm\sqrt{-2}\}$. Therefore, $F = \mathbb{Q}(\sqrt{2}, \sqrt{-2} = i\sqrt{2}) = \mathbb{Q}(\sqrt{2}, i)$ is a splitting field of $g(x) = f_1(x) \cdot f_2(x)$. We now verify that $[F : \mathbb{Q}] = 4$. Since $f_1(x) \in \mathbb{Q}[x]$ is 2-Eisenstein, it is irreducible over \mathbb{Q} ; we conclude that $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. We observe that $x^2 + 1$ has two non-real roots $\{\pm i\}$. On the other hand, we have $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$. It follows that $x^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt{2})$. Therefore, we have $[F : \mathbb{Q}(\sqrt{2})] = 2$, from which we deduce that $[F : \mathbb{Q}] = 4$.

Now, since F is a splitting field over \mathbb{Q} of the separable polynomial $g(x)$, we have $|G_{F/\mathbb{Q}}| = [F : \mathbb{Q}] = 4$; hence, $G_{F/\mathbb{Q}} \cong \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. To identify $G_{F/\mathbb{Q}}$, note that it contains two elements

$$\begin{aligned}\phi : \sqrt{2} &\mapsto \sqrt{2}, & i &\mapsto -i \\ \psi : \sqrt{2} &\mapsto -\sqrt{2}, & i &\mapsto i.\end{aligned}$$

The elements ϕ and ψ are distinct elements of order 2 in $G_{F/\mathbb{Q}}$, which implies that $G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. \square

§8.2 #5. Show that if $F \supseteq E \supseteq K$ are fields and F is separable over K , then F is separable over E .

Proof. Let $u \in F$. It suffices to show that $f_{E,u}(x)$ is separable. First, we observe that since $E \supseteq K$, we have $f_{E,u}(x) \mid f_{K,u}(x)$. Now, since F is separable over K , the polynomial $f_{K,u}(x)$ is separable: it has only simple roots in a splitting field. Since $f_{E,u}(x) \mid f_{K,u}(x)$, the polynomial $f_{E,u}(x)$ has only simple roots in a splitting field. Therefore, it is separable. \square

§8.3 #3. Find the Galois group of $x^4 + 1$ over \mathbb{Q} .

Claim. Let F be a splitting field for $f(x) = x^4 + 1$. Then we have $G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. The polynomial $f(x)$ has roots $\{\sqrt[4]{-1}, \zeta_4 \sqrt[4]{-1}, \zeta_4^2 \sqrt[4]{-1}, \zeta_4^3 \sqrt[4]{-1}\}$. We observe that

$$\sqrt[4]{-1} = i^{\frac{1}{2}} = e^{\frac{\pi i}{4}} = \frac{\sqrt{2} + i\sqrt{2}}{2} = \frac{(1+i)\sqrt{2}}{2}.$$

Since $\zeta_4 = i$, a splitting field for $f(x)$ is $F = \mathbb{Q}(\sqrt{2}, i)$. Problem §8.1, #6 now shows that $G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. \square

§8.3 #4. Find the Galois group of $x^4 - x^2 - 6$ over \mathbb{Q} .

Claim. Let F be a splitting field for $f(x) = x^4 - x^2 - 6$ over \mathbb{Q} . Then we have $G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. We first observe that $f(x) = (x^2 - 3)(x^2 + 2)$. It follows that $F = \mathbb{Q}(\sqrt{-2}, \sqrt{3})$. The polynomial $x^2 - 3$ is 3-Eisenstein, and hence, irreducible over \mathbb{Q} ; therefore, we have $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$. Now, note that $x^2 + 2$ has non-real roots $\{\pm\sqrt{-2}\}$. Since $\mathbb{Q}(\sqrt{3}) \subseteq \mathbb{R}$, the polynomial $x^2 + 2$ is irreducible over $\mathbb{Q}(\sqrt{3})$. Hence, we have $[F : \mathbb{Q}(\sqrt{3})] = 2$; we conclude that $[F : \mathbb{Q}] = 4$. Since F is a splitting field of a separable polynomial, we have $|G_{F/\mathbb{Q}}| = 4$. Two elements of $G_{F/\mathbb{Q}}$ are:

$$\begin{aligned}\phi : \sqrt{3} &\mapsto \sqrt{3}, & \sqrt{-2} &\mapsto -\sqrt{-2}, \\ \psi : \sqrt{3} &\mapsto -\sqrt{3}, & \sqrt{-2} &\mapsto \sqrt{-2}.\end{aligned}$$

These are distinct elements of order 2; we conclude that $G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. \square

§8.3 #5. Find the Galois group of $x^8 - 1$ over \mathbb{Q} .

Claim. Let F be a splitting field of $f(x) = x^8 - 1$ over \mathbb{Q} . Then we have $G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Proof. We first note that $f(x)$ factors into irreducibles in $\mathbb{Q}[x]$ as $f(x) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$. By §8.3, #3, the field $F = \mathbb{Q}(\sqrt{2}, i)$ is a splitting field for $x^4 + 1$; the field $E = \mathbb{Q}(i)$ is a splitting field for $x^2 + 1$. Since $\mathbb{Q}(i) \subseteq F$, it follows that F is a splitting field for $f(x)$. Appealing again to §8.3, #3, we find that $G_{F/\mathbb{Q}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. \square