Chapter 8: Fields, Section 1: The Galois Group of a Polynomial

1. *Solution.* $[\mathbb{F}_4 : \mathbb{F}_2] = 2$, so it immediately follows that $|\text{Gal}(\mathbb{F}_4/\mathbb{F}_2)| = 2$, which implies the result. $\square$

2. *Solution.* $\mathbb{F}_{2^3} \cong \mathbb{Z}_2[x]/\left\langle x^3 + x + 1\right\rangle$. The generator for the multiplicative group is $x + \left\langle x^3 + x + 1\right\rangle := u$. The basis for $\mathbb{F}_{2^3}$ is $\left\{1, u, u^2\right\}$.

   This Galois group is generated by the Frobenius automorphism $\phi : x \mapsto x^p = x^2$. So the Galois group consists of the automorphisms.

   $$\phi : x \mapsto x^2, \quad \phi^2 : x \mapsto x^4, \quad \text{id} : x \mapsto x. \qquad \square$$

3. Verified by direct computation.

4. Solution provided in book.

5. *Solution.* The splitting field for $x^3 - 1$ is $\mathbb{Q}(\omega)$, where $\omega = e^{\frac{2\pi}{3}i}$. We have $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2$, since we need to adjoin the roots of the polynomial x^2+x+1. Therefore $|\text{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = 2$, implying the result. $\square$

6. *Solution.* The splitting field for $(x^2 - 2)(x^2 + 2)$ is $\mathbb{Q}(\sqrt{2}, \sqrt{-2})$. We see that

   $$[\mathbb{Q}(\sqrt{2}, \sqrt{-2}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{-2}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4.$$

   We have to find automorphisms that map roots to roots. We readily find $\sqrt{2} \mapsto \pm\sqrt{2}$, $\sqrt{-2} \mapsto \pm\sqrt{-2}$, yielding 4 automorphisms with order 2. This precisely defines $\mathbb{Z}_2 \times \mathbb{Z}_2$. $\square$

7. *Solution.* To find the splitting field, we note that

   $$\begin{aligned} x^4 + 1 &= (x^2 - i)(x^2 + i) \\ &= (x - \sqrt{i})(x + \sqrt{i})(x - \sqrt{-i})(x + \sqrt{-i}) \\ &= (x - e^{\frac{\pi}{4}i})(x + e^{\frac{\pi}{4}i})(x - e^{\frac{3\pi}{4}i})(x + e^{\frac{3\pi}{4}i}). \end{aligned}$$

   Therefore the splitting field is $\mathbb{Q}(e^{\frac{\pi}{4}i}) = \mathbb{Q}(\frac{1+i}{\sqrt{2}}) = \mathbb{Q}(i, \sqrt{2})$, which has degree 4 in $\mathbb{Q}$. Again, we can map roots to roots by $\sqrt{i} \mapsto \pm\sqrt{i}$ and $\sqrt{-i} \mapsto \pm\sqrt{-i}$. So all 4 automorphisms have degree 2, defining $\mathbb{Z}_2 \times \mathbb{Z}_2$. $\square$

8. Let $f(x) = x^3 - 2$.

   a) $f(3) = 0$, so $f(x) = (x - 3)(x^2 + 3x + 4)$. We can check that this has no roots, so it is irreducible. So the splitting field has degree 2 in $\mathbb{F}_5$, and the Galois group is $\boxed{\mathbb{Z}_2}$.

   b) We can check that no roots satisfy $f(x)$. So the splitting field has degree 3 in $\mathbb{F}_7$ for some element α, and the Galois group is $\boxed{\mathbb{Z}_3}$.

c) Note that $f(-4) = -66 = 0$. So $f(x) = (x+4)(x^2 - 4x + 5)$. We can check that $x^2 - 4x + 5$ is irreducible, the Galois group is $\boxed{\mathbb{Z}_2}$.

9. *Solution.* Let $f(x) = x^4 - 1$. We see that $f(1) = 0$, $f(-1) = 0$, so $f(x) = (x-1)(x+1)(x^2+1)$. (x^2+1) is irreducible, so the Galois group is $\boxed{\mathbb{Z}_2}$. $\square$

10. *Proof.* Let $\phi : E \to F$ be an isomorphism. Let

$$\Phi : \mathrm{Gal}(E/K) \to \mathrm{Gal}(F/K), \quad \tau \mapsto \phi \circ \tau \circ \phi^{-1}$$

For any automorphism $\tau : E \to E \in \mathrm{Gal}(E/K)$, we have $\phi\circ\tau\circ\phi^{-1} : F \to F$ is an automorphism as well (since it is composed of isomorphisms). Clearly, this composition also fixes K. Therefore $\phi \circ \tau \circ \phi^{-1} \in \mathrm{Gal}(F/K)$.

To show Φ is injective, let $\phi \circ \tau_1 \circ \phi^{-1} = \phi \circ \tau_2 \circ \phi^{-1}$. Then

$$\begin{gathered} \phi^{-1} \circ (\phi \circ \tau_1 \circ \phi^{-1}) \circ \phi = \phi^{-1}(\circ\phi \circ \tau_2 \circ \phi^{-1}) \circ \phi \\ \tau_1 = \tau_2. \end{gathered}$$

For Φ to be surjective, for any $\pi \in \mathrm{Gal}(F/K)$, we can take $\phi^{-1}\circ\pi\circ\phi : E \to E$ to get an automorphism of E that clearly fixes K. So Φ is bijective. $\square$

$$\begin{tikzcd} E \arrow[r, hook, two heads, "\phi"] \arrow[loop below, "\tau"] & F \arrow[loop below, "\pi"] \end{tikzcd}$$

$$\begin{tikzcd} \mathrm{Gal}(E/K) \arrow[r, hook, two heads, "\Phi"] & \mathrm{Gal}(F/K) \end{tikzcd}$$

If I've made any errors or you have any other comments on these solutions, message me on Mathstodon.

Notation

- I write the Galois Field $\mathrm{GF}(p^n)$ as $\mathbb{F}_{p^n}$.