1. Show that the splitting field of $f(x) = x^4+1$ is $F = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$ where $\alpha = e^{\pi i/4} = (\sqrt{2} + \sqrt{2}i)/2$. Determine the Galois group $G = \mathrm{Gal}(F/\mathbb{Q})$ and the correspondence between subfields of F and subgroups of G.

   ▶ **Solution.** Since $\alpha^4 = (e^{\pi i/4})^4 = e^{\pi i} = -1$ it follows that α is a root of $x^4 + 1$. Similarly, any odd power of α satisfies $(\alpha^{2k+1})^4 = (\alpha^4)^{2k+1} = (-1)^{2k+1} = -1$. Thus, roots of $x^4 + 1$ are $\alpha = (\sqrt{2} + \sqrt{2}i)/2$, $\alpha^3 = e^{3\pi i/4} = (-\sqrt{2} + \sqrt{2}i)/2$, $\alpha^5 = e^{5\pi i/4} = -\alpha = (-\sqrt{2} - \sqrt{2}i)/2$ and $\alpha^7 = e^{7\pi i/4} = -\alpha^3 = (\sqrt{2} - \sqrt{2}i)/2$. Therefore, all roots are in $\mathbb{Q}(\alpha)$ so the splitting field of $x^4 + 1$ is $F = \mathbb{Q}(\alpha)$. Note that $\alpha + \alpha^7 = \sqrt{2}$ so $\sqrt{2} \in F$ and $\alpha - \alpha^7 = \sqrt{2}i \in F$ so $i = \sqrt{2}i/\sqrt{2} \in F$. Hence, $\mathbb{Q}(\sqrt{2}, i) \subseteq F$. Moreover, $\alpha = (\sqrt{2} + \sqrt{2}i)/2 \in \mathbb{Q}(\sqrt{2}, i)$ so $F = \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Hence, the splitting field of $x^4 + 1$ is $F = \mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{2}, i)$.

   Since $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \times 2 = 4$, it follows that the Galois group of $x^4 + 1$ has order 4. Any $\phi \in \mathrm{Gal}(F/\mathbb{Q})$ must take $\sqrt{2}$ to $\pm\sqrt{2}$ and i to $\pm i$. Since $\mathrm{Gal}(F/\mathbb{Q})$ has order 4, each of these 4 possible outcomes actually occurs. Thus, there are elements $\phi_1 = \mathrm{id}$, ϕ_2, ϕ_3, and ϕ_4 of $\mathrm{Gal}(F/\mathbb{Q})$ such that:

	$\sqrt{2}$	i
ϕ_1	$\sqrt{2}$	i
ϕ_2	$-\sqrt{2}$	i
ϕ_3	$\sqrt{2}$	$-i$
ϕ_4	$-\sqrt{2}$	$-i$

   The group operation is composition, so it follows from the above table that the group multiplication table for $\mathrm{Gal}(F/\mathbb{Q})$ is

$\cdot$	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	ϕ_1	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

   Since $\phi_1 = \mathrm{id}$ it follows that every nonidentity element has order 2, so this group is isomorphic to the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

   The subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ are $\langle \mathrm{id} \rangle$, $H_1 = \langle \phi_2 \rangle$, $H_2 = \langle \phi_3 \rangle$, $H_3 = \langle \phi_4 \rangle$, and $G = \mathrm{Gal}(F/\mathbb{Q})$. The corresponding subfields of F are given by the fixed fields of the subgroups of G: $F = F^{\langle \mathrm{id} \rangle} = F$, $F^{H_1} = \mathbb{Q}(i)$, $F^{H_2} = \mathbb{Q}(\sqrt{2})$, $F^{H_3} = \mathbb{Q}(\sqrt{2}i)$, and $F^G = \mathbb{Q}$. ◀

2. Determine the splitting field F of $x^4 - x^2 - 6$ over $\mathbb{Q}$. Determine the Galois group $G = \mathrm{Gal}(F/\mathbb{Q})$ and the correspondence between subfields of F and subgroups of G.

   ▶ **Solution.** Since $x^4 - x^2 - 6 = (x^2 - 3)(x^2 + 2)$ the roots of $x^4 - x^2 - 6$ are $\pm\sqrt{3}$ and $\pm\sqrt{2}i$. Thus, the splitting field F is $F = \mathbb{Q}(\sqrt{3}, \sqrt{2}i)$ and this is essentially equivalent to exercise 1. Since $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt{2}i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4$, it follows

that the Galois group of $x^4 - x^2 - 6$ has order 4. Any $\phi \in \mathrm{Gal}(F/\mathbb{Q})$ must take $\sqrt{3}$ to $\pm\sqrt{3}$ and $\sqrt{2}i$ to $\pm\sqrt{2}i$. Since $\mathrm{Gal}(F/\mathbb{Q})$ has order 4, each of these 4 possible outcomes actually occurs. Thus, there are elements $\phi_1 = \mathrm{id}$, ϕ_2, ϕ_3, and ϕ_4 of $\mathrm{Gal}(F/\mathbb{Q})$ such that:

	$\sqrt{3}$	$\sqrt{2}i$
ϕ_1	$\sqrt{3}$	$\sqrt{2}i$
ϕ_2	$-\sqrt{3}$	$\sqrt{2}i$
ϕ_3	$\sqrt{3}$	$-\sqrt{2}i$
ϕ_4	$-\sqrt{3}$	$-\sqrt{2}i$

The group operation is composition, so it follows from the above table that the group multiplication table for $\mathrm{Gal}(F/\mathbb{Q})$ is

$\cdot$	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_1	ϕ_1	ϕ_2	ϕ_3	ϕ_4
ϕ_2	ϕ_2	ϕ_1	ϕ_4	ϕ_3
ϕ_3	ϕ_3	ϕ_4	ϕ_1	ϕ_2
ϕ_4	ϕ_4	ϕ_3	ϕ_2	ϕ_1

Since $\phi_1 = \mathrm{id}$ it follows that every nonidentity element has order 2, so this group is isomorphic to the Klein 4-group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The subgroups of $\mathrm{Gal}(F/\mathbb{Q})$ are $\langle \mathrm{id} \rangle$, $H_1 = \langle \phi_2 \rangle$, $H_2 = \langle \phi_3 \rangle$, $H_3 = \langle \phi_4 \rangle$, and $G = \mathrm{Gal}(F/\mathbb{Q})$. The corresponding subfields of F are given by the fixed fields of the subgroups of G: $F = F^{\langle \mathrm{id} \rangle} = F$, $F^{H_1} = \mathbb{Q}(\sqrt{2}i)$, $F^{H_2} = \mathbb{Q}(\sqrt{3})$, $F^{H_3} = \mathbb{Q}(\sqrt{6}i)$, and $F^G = \mathbb{Q}$. ◀

3. Show that $F = \mathbb{Z}_2(u)$ where u is a root of $f(x) = x^4 + x + 1$ is the splitting field of $f(x)$ over $\mathbb{Z}_2$. Determine the Galois group $G = \mathrm{Gal}(F/\mathbb{Z}_2)$ and the correspondence between subfields of F and subgroups of G.

► **Solution.** Since $f(x)$ has no roots in $\mathbb{Z}_2$, the only irreducible quadratic over $\mathbb{Z}_2$ is $x^2 + x + 1$, and $x^4 + x + 1 \neq (x^2 + x + 1)^2$, it follows that $f(x)$ is irreducible. Thus, $F = \mathbb{Z}_2(u)$ has degree 4 over $\mathbb{Z}_2$. The group $\mathrm{Gal}(F/\mathbb{Z}_2)$ is thus cyclic of order 4 and generated by the Frobenius map $\phi : F \to F$ with $\phi(x) = x^2$ (Theorem 8.1.8). Since any automorphism of F over $\mathbb{Z}_2$ must take a root of $x^4 + x + 1$ to another root, we can look for additional roots by applying ϕ to known roots. One root is given as u. Thus, additional roots are $\phi(u) = u^2$, $\phi(u^2) = u^4 = u + 1$ and $\phi(u + 1) = u^2 + 1$. Thus, we have found all 4 roots of $f(x)$ in F so F is the splitting field of $f(x)$ over $\mathbb{Z}_2$.

Since $G = \mathrm{Gal}(F/\mathbb{Z}_2) = \langle \phi \rangle$ where $\phi(x) = x^2$ and $\phi^4 = \mathrm{id}$, it follows that the only proper subgroup of G is the cyclic group of order two $\langle \phi^2 \rangle$. The map $\phi^2(x) = \phi(\phi(x)) = \phi(x^2) = \phi(x)^2 = x^4$. Thus, the fixed field of $\langle \phi^2 \rangle$ is the set of all elements v of F such the $v^4 = v$. Since a basis for F over $\mathbb{Z}_2$ is $\{1, u, u^2, u^3\}$, a typical element of v is $v = a_0 + a_1 v + a_2 v^2 + a_3 v^3$. Then, using the fact that $u^4 + u + 1 = 0$ implies $u^4 = u + 1$

gives

$$\begin{aligned} v^4 &= a_1 + a_1u^4 + a_2u^8 + a_3u^{12} \\ &= a_0 + a_1(u+1) + a_2(u^2+1) + a_3(u^3+u^2+u+1) \\ &= (a_0+a_1+a_2+a_3) + (a_1+a_3)u + (a_2+a_3)u^2 + a_3u^3. \end{aligned}$$

Setting $v^4 = v$ gives a system of equations:

$$\begin{aligned} a_0 &= a_0 + a_1 + a_2 + a_3 \\ a_1 &= a_1 + a_3 \\ a_2 &= a_2 + a_3 \\ a_3 &= a_3. \end{aligned}$$

Solving these equations gives $a_3 = 0$ and $a_1 + a_2 = 0$ so that $a_1 = a_2$. Thus, the fixed field of ϕ^2 consists of the elements of the form $a_0 + a_1(u + u^2)$. These are the elements $\{0,\ 1,\ u+u^2,\ u+u^2+1\}$. This is the only subfield of F other than F and $\mathbb{Z}_2$ since the Galois group has only one subgroup other than $\langle \mathrm{id} \rangle$ and G. ◀

Do the following exercises from Beachy-Blair:

Page 391: 3, 4

3. Find the Galois group of $x^5 - 1$ over $\mathbb{Q}$.

▶ **Solution.** We have the factorization $x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$, where the second factor is irreducible by Corollary 4.4.7. It follows that the splitting field F of $x^5 - 1$ over $\mathbb{Q}$ has degree at least 4, and since $x^5 - 1$ has no repeated roots over $\mathbb{Q}$, Theorem 8.1.6 implies that the Galois group G of $x^5 - 1$ over $\mathbb{Q}$ has order at least 4. On the other hand, the proof of Theorem 8.4.2 implies that G is isomorphic to a subgroup of $\mathbb{Z}_5^* \cong \mathbb{Z}_4$, and so we must have $G \cong \mathbb{Z}_4$. ◀

4. Find the Galois group of $x^9 - 1$ over $\mathbb{Q}$.

▶ **Solution.** The proof of Theorem 8.4.2 implies that the Galois group G of $x^9 - 1$ over $\mathbb{Q}$ is isomorphic to a subgroup of $\mathbb{Z}_9^* \cong \mathbb{Z}_6$. We can factor $x^9 - 1$ as

$$x^9 - 1 = (x^3-1)(x^6+x^3+1) = (x-1)(x^2+x+1)(x^6+x^3+1).$$

To see that $x^6 + x^3 + 1$ is irreducible, note that a polynomial $f(x)$ is irreducible if and only if the polynomial $g(x) = f(x+r)$ is irreducible. But if $f(x) = x^6 + x^3 + 1$ and $r = 1$, then $g(x) = f(x+1)$ so

$$g(x) = (x+1)^6 + (x+1)^3 + 1 = x^6 + 6x^5 + 15x^4 + 21x^3 + 18x^2 + 9x + 3.$$

Note that 3 divides every coefficient except for x^6 and 3^2 does not divide the constant term, so Eisenstein's criterion applies to conclude that $g(x)$ is irreducible. Then also $f(x)$ is irreducible.

Since $f(x)$ is a factor of $x^9 - 1$, it follows that the splitting field of $x^9 - 1$ over $\mathbb{Q}$ has degree at least 6 and hence the order of the Galois group is at least 6. Since G is isomorphic to a subgroup of $\mathbb{Z}_6$ we conclude that $G \cong \mathbb{Z}_6$. ◀