Exercise 1. Let $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$. Prove that K is Galois over \mathbb{Q} . Explicitly describe the \mathbb{Q} -automorphisms of K to determine the Galois group of this extension, and draw the corresponding subgroup and subfield lattices.

K is Galois over \mathbb{Q} : Define $\theta \doteq \sqrt{2 + \sqrt{2}}$, then $\theta^2 = 2 + \sqrt{2}$ and $\theta^4 = 6 + 4\sqrt{2} = 4\theta^2 - 2$. Thus θ is a root of $f(x) = x^4 - 4x^2 + 2$. Since f(x) is irreducible over \mathbb{Q} by Eisenstein's criterion for p = 2, $[K : \mathbb{Q}] = 4$.

If we let $\theta' \doteq \sqrt{2 - \sqrt{2}}$, then we can check that $\pm \theta, \pm \theta'$ are the roots of f(x). Since these roots are all distinct, f(x) is separable. Then by §14.1 Corollary 6, if we can show that K is actually the splitting field of f(x), then K is Galois over \mathbb{Q} .

To start, note that $\theta^2 - 2 = \sqrt{2}$, so $\sqrt{2} \in K$. Also, θ^{-1} must necessarily be in K. Then

$$\sqrt{2}\theta^{-1} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} = \frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}} \frac{\sqrt{2-\sqrt{2}}}{\sqrt{2}-\sqrt{2}} = \sqrt{2-\sqrt{2}} = \theta' \in K.$$

Thus $\pm \theta$, $\pm \theta'$ (all the roots of f(x)) are in K, so K is the splitting field of a separable polynomial and thus Galois over \mathbb{Q} .

Galois Group of K **over** \mathbb{Q} : Let $G \doteq \operatorname{Gal}_{\mathbb{Q}}(K)$. Since K/\mathbb{Q} is Galois, we know $|G| = [K : \mathbb{Q}] = 4$. Then by the list on DF page 614, the only possible subgroups of S_4 with order 4 are V (the Klein four-group) and C (the cyclic group of order 4).

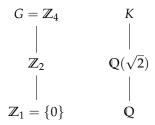
We will now show that G has an order 4 element, meaning that G = C. Since θ and θ' are roots of the same irreducible polynomial, G permutes them. Suppose $\sigma \in G$ maps $\theta \mapsto \theta'$, then since $\sqrt{2} = \theta^2 - 2$,

$$\sigma(\sigma(\theta)) = \sigma(\theta') = \sigma\left(\frac{\theta^2 - 2}{\theta}\right) = \frac{\sigma(\theta)^2 - 2}{\sigma(\theta)} = \frac{\theta'^2 - 2}{\theta'} = \frac{-\sqrt{2}}{\sqrt{2 - \sqrt{2}}} = -\theta.$$

Thus the order of θ is greater than 2, but we also know that it must divide 4 (the order of the whole group). This forces $|\theta| = 4$, so G is cyclic, i.e. $G \cong C \cong \mathbb{Z}_4$.

Subgroup and subfield lattices: We know the subgroups of \mathbb{Z}_4 , so we can use the Galois correspondence to determine the orders of the subfields of K. Since \mathbb{Z}_2 is the only nontrivial proper subgroup of \mathbb{Z}_4 and it has order 2, we know that there is only one intermediate field in the subfield lattice of K and that it has degree 2 over \mathbb{Q} .

As remarked earlier, $\sqrt{2} \in K$, so $\mathbb{Q}(\sqrt{2}) \subset K$. Since $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, we have found the subfield of K. The two lattices are then as pictured below.



Exercise 2. Let $f(x) \in \mathbb{Q}[x]$ be a cubic polynomial and let $K \subset \mathbb{C}$ be a splitting field of f over \mathbb{Q} . If $[K : \mathbb{Q}] = 3$, then all the roots of f are real.

Supopse $c \in \mathbb{C} - \mathbb{R}$ is a complex root of f(x), then its complex conjugate \overline{c} is known to also be a root of f(x). Since odd degree polynomials always have at least one root, this forces the third root to be real. Thus we can represent f(x) by

$$f(x) = (x - c)(x - \overline{c})(x - \alpha),$$

where α is the real root. This shows f is separable, so by §14.1 Corollary 6, K is Galois over \mathbb{Q} . Let $G \doteq \operatorname{Gal}_{\mathbb{Q}}(K)$, then by the Galois correspondence, since $[K : \mathbb{Q}] = 3$, we know |G| = 3.

If f had complex roots, then $c \mapsto \overline{c}$ would be a Q-automorphism and thus belong to G. But this particular map has order 2, and the order of a group element must divide the order of the group, so this is impossible. Thus all the roots of f(x) are real.

Exercise 3. Let K be a splitting field of $f(x) = x^4 - 5$ over \mathbb{Q} . Show that there cannot be a \mathbb{Q} -automorphism of K that fixes exactly one root of f.

Let $\theta \doteq \sqrt[4]{5}$, then the roots of f(x) are θ , $\theta \zeta_4$, $\theta \zeta_4^2$, $\theta \zeta_4^3$, so its splitting field is $K = \mathbb{Q}(\theta, \zeta_4)$. But by the list on DF page 540, $\zeta_4 = i$, so the splitting field is really $K = \mathbb{Q}(\theta, i)$.

Since f(x) is irreducible over Q by Eisenstein's criterion for p=5, we know $[Q(\theta):Q]=4$. Since each ζ^n is either complex or an integer, $\pm\sqrt{2}\not\in Q(\theta)$. This means the polynomial x^2-2 has no roots in $Q(\theta)$, but since this polynomial is quadratic, that's equivalent to it being irreducible over $Q(\theta)$. Then since $\sqrt{2}$ is a root of this polynomial, $[K:Q(\theta)]=2$. Then since degrees multiply in towers, [K:Q]=8. Since f(x) has four distinct roots (i.e. is separable), by §14.1 Corollary 6, its splitting field K is Galois over Q. Then by the Galois correspondence, we know its Galois group has 8 elements.

If we define maps that permute the roots of f(x) by

$$\sigma: \zeta^n \mapsto \zeta^{n+1}, \quad \tau: \zeta^n \mapsto \zeta^{n+2}, \quad \pi: \zeta^n \mapsto \zeta^{n+3},$$

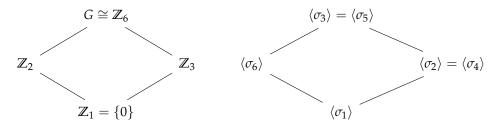
(where $\theta = \theta \zeta^0$), then the subgroup they generate is

$$\langle \sigma, \tau, \pi \rangle = \left\{1, \sigma, \sigma^2, \sigma^3, \tau, \pi, \pi^2, \pi^3\right\}.$$

Furthermore, since each ζ is complex and the ζ 's are all that change, each of these maps is a Q-automorphism. But since there are 8 of these and we know that the Galois group has 8 elements, we have found all possible Q-automorphisms. Since none of these fix only one root of f(x), we are done.

Exercise 4. Determine the Galois group of $\mathbb{Q}(\zeta_7)$ over \mathbb{Q} and find all intermediate fields. What is the minimal polynomial of $\zeta_7 + \zeta_7^{-1}$ over \mathbb{Q} ?

Galois group and subfields: Let $\zeta \doteq \zeta_7$. The §14.5 Theorem 26, $G \doteq \text{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta)) \cong$ $\mathbb{Z}_7^{\times} \cong \mathbb{Z}_6$. We know that the subgroups of \mathbb{Z}_n correspond to the divisors of n, which gives us the structure of the subgroup lattice of *G*. Using the map $\sigma_a : \zeta \mapsto \zeta^a$ (this map was defined for a relatively prime to 7, but 7 is prime so any a < 7 will work), we get an isomorphic copy of the lattice.

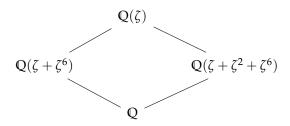


By the Galois correspondence, we know there are two proper subfields of $\mathbb{Q}(\zeta_7)$: the fixed fields of $\langle \sigma_6 \rangle$ and $\langle \sigma_2 \rangle = \langle \sigma_4 \rangle$ (from now on, I work with $\langle \sigma_2 \rangle$ instead of $\langle \sigma_4 \rangle$ since it doesn't matter which one I choose).

Following example 2 on DF page 597, since 7 is odd and we're working with $\mathbb{Q}(\zeta_7)$, we know that the fixed fields of $\langle \sigma_6 \rangle$ and $\langle \sigma_2 \rangle$ are given by $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$, respectively, where

$$lpha = \sum_{ au \in \langle \sigma_6
angle} au \zeta
onumber \ eta = \sum_{ au \in \langle \sigma_2
angle} au \zeta.$$

Since $\langle \sigma_6 \rangle = \{ \sigma_1, \sigma_6 \}$ and $\langle \sigma_2 \rangle = \{ \sigma_1, \sigma_2, \sigma_4 \}$, these evaluate to $\alpha = \zeta + \zeta^6$ and $\beta = \zeta + \zeta^2 + \zeta^4$. Thus the subfields of $\mathbb{Q}(\zeta)$ are $\mathbb{Q}(\zeta + \zeta^6)$ and $\mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$. The subfield lattice is pictured below.



Minimal polynomial: Let $\alpha \doteq \zeta + \zeta^{-1} = \zeta + \zeta^6$. Then we manually calculate $\alpha^2 = \zeta^5 + \zeta^2 + 5$ and $\alpha^3 = 3\zeta^6 + \zeta^4 + \zeta^3 + 3\zeta$. Now ζ is a root of the 7th cyclotomic polynomial, which we can express in terms of α , α^2 , and α^3 . We have

$$0 = \Phi_7(\zeta) = \zeta^6 + \zeta^5 + \dots + \zeta^1 + 1 = \alpha^3 + \alpha^2 - 2\alpha - 1,$$

so $\alpha = \zeta + \zeta^{-1}$ is a root of the polynomial $x^3 + x^2 - 2x - 1$. Since this is irreducible over Q by the rational root test, it is the minimal polynomial of $\zeta + \zeta^{-1}$ over Q.

Exercise 5. Construct (with justification) an example of a Galois extension whose Galois group is $Z_2 \times Z_6$.

Before constructing the extension, we note that such an extension must exist. This is because $Z_2 \times Z_6$, as the product of finite abelian groups, is itself finite abelian. Then by §14.5 Corollary 28, there is some subfield of a cyclotomic extension whose Galois group is $Z_2 \times Z_6$.

Now consider $\mathbb{Q}(\zeta_{21})$, which we know to be Galois over \mathbb{Q} . Since 21 has prime decomposition $21 = 3 \cdot 7$, by §14.5 Corollary 27,

$$\begin{split} \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{21})) & \cong \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{3})) \times \operatorname{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_{7})) \\ & \cong \mathbb{Z}_{3}^{\times} \times \mathbb{Z}_{7}^{\times} \\ & \cong Z_{2} \times Z_{6}. \end{split}$$

Thus $Q(\zeta_{21})$ is a Galois extension whose Galois group is $Z_2 \times Z_6$.

Exercise 6. If *K* is a root extension of *F* and *E* is an intermediate field, then *K* is a root extension of *E*.

By assumption,

$$F = K_0 \subset K_1 \subset \cdots \subset K_s = K$$
,

for some s, where $K_{i+1} = K_i \left(\sqrt[n_i]{a_i} \right)$ for some $a_i \in K_i$. If we let $\theta_i \doteq \sqrt[n_i]{a_i}$, then

$$K = K_s = F(\theta_1, \ldots, \theta_s).$$

Now suppose *E* is an intermediate field, i.e. $F \subset E \subset K$. If *E* happens to be one of the K_i above, then *K* is a root extension of *E*: we just append to *E* all θ_i for i > i.

If *E* is not one of the K_i , then *K* is still a root extension of *E*. If we append all θ_i to *E*, we get the chain

$$E=E_0\subset E_1\subset\cdots\subset E_s,$$

where $E_{i+1} = E_i(\theta_i)$. Since $E \subset K$ and $\theta_i \in K$ for all i, we know $E_s \subset K$. Conversely, since $F \subset E$, we get $K = F_s = F(\theta_1, \dots, \theta_s) \subset E(\theta_1, \dots, \theta_s) = E_s$. Thus $E_s = K$, so K is a root extension of *E*.

Exercise 7. If $f: A \to A$ is an R-module homomorphism such that ff = f, then $A = \ker f \oplus \operatorname{im} f$.

Let $a \in A$ be arbitrary, then consider a - f(a). Mapping this under f and using the condition $f \circ f = f$ along with the fact that f is a homomorphism gives

$$f(a - f(a)) = f(a) - f(f(a)) = f(a) - f(a) = 0.$$

Thus $a - f(a) \in \ker f$. But a = a - f(a) + f(a), so we have written a as a sum of an element of the kernel of f and an element of the image of f. Thus $A = \ker f + \operatorname{im} f$.

Now we show that $\ker f$ and $\operatorname{im} f$ have trivial intersection. Suppose $\tilde{a} \in \ker f \cap \operatorname{im} f$, then $f(\tilde{a}) = 0$ and $\tilde{a} = f(a)$ for some $a \in A$. Then since $f \circ f = f$,

$$\tilde{a} = f(a) = f(f(a)) = f(\tilde{a}) = 0.$$

Thus \tilde{a} is 0, so the intersection of ker f and im f is trivial. This shows that $A = \ker f \oplus \operatorname{im} f$.

Exercise 8. Let *R* be a commutative ring with 1 and let *M* be a left *R*-module. Show that $\operatorname{Hom}_R(R,M) \cong M$ (as R-modules).

Define the map

$$\phi: \operatorname{Hom}_R(R, M) \to M$$

$$f \mapsto f(1).$$

This is well-defined since R is assumed to have 1. We claim that ϕ is an isomorphism.

Homomorphism: By the definitions of function addition and the R action on $\operatorname{Hom}_R(R, M)$, for $r \in R$, $f, g \in \operatorname{Hom}_R(R, M)$,

$$\phi(rf + g) = (rf + g)(1)$$

$$= (rf)(1) + g(1)$$

$$= rf(1) + g(1)$$

$$= r\phi(f) + \phi(g).$$

Thus ϕ is an *R*-module homomorphism.

Bijective: Let $m \in M$ be arbitrary and consider the map $f_m(r) = rm$. By the definition of a module, for $s, r_1, r_2 \in R$,

$$f_m(sr_1 + r_2) = (sr_1 + r_2)m$$

$$= (sr_1)m + r_2m$$

$$= s(r_1m) + r_2m$$

$$= sf_m(r_1) + f_m(r_2),$$

so $f_m \in \operatorname{Hom}_R(R, M)$. Since $\phi(f_m) = f_m(1) = m$ and m was arbitrary, this means ϕ is surjective.

Now suppose $g \in \ker \phi$, i.e. $\phi(g) = g(1) = 0$. Then since g is by assumption a homomorphism, for all $r \in R$,

$$g(r) = g(1 \cdot r) = g(1) \cdot g(r) = 0 \cdot g(r) = 0.$$

Thus *g* is the trivial homomorphism, so the kernel of ϕ is trivial, so ϕ is injective. This shows that ϕ is a bijective *R*-module homomorphism, i.e. an *R*-module isomorphism, so $\operatorname{Hom}_R(R, M) \cong M$.