# Solutions to Homework 2

**Section 1, Exercises 8, 10, 12, 13, 16, 17** (updated), **and 18.**

**Exercise 8.** Let $\zeta = e^{2\pi i/5}$.

(a) Prove that $K = \mathbb{Q}(\zeta)$ is a splitting field for the polynomial $f(x) = x^5 - 1$ over $\mathbb{Q}$, and determine the degree $[K : \mathbb{Q}]$.

(b) Prove that $K$ is a Galois extension of $\mathbb{Q}$, and determine its Galois group.

*Solution.* For (a), note that $x^5 - 1 = (x-1)(x-\zeta)(x-\zeta^2)(x-\zeta^3)(x-\zeta^4)$, so $f$ factors into linear factors in $K$. Also, $K$ is generated by the roots of $f(x)$, so $K$ is the splitting field of $f$. Also, $g(x) = x^4 + x^3 + x^2 + x + 1$ is irreducible over $\mathbb{Q}$, since it is irreducible mod 2. It has $\zeta$ as a root, so it is the irreducible polynomial of $\zeta$. Thus $[K : \mathbb{Q}] = 4$.

For (b), any automorphism of $K$ is completely determined by how it acts on $\zeta$. Since $g(x)$ defined above is irreducible, we can send $\zeta$ to any root of $g(x)$, i.e., to $\zeta$, $\zeta^2$, $\zeta^3$, or $\zeta^4$. These are the only possible automorphisms of $K$, and they are all different, so $|G(K/\mathbb{Q})| = 4$. Hence $K/\mathbb{Q}$ is Galois. The Galois group is cyclic, generated by the automorphism $\zeta \mapsto \zeta^2$, since this element of the Galois group has order four. □

**Exercise 10.** Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Determine $[K : \mathbb{Q}]$, prove that $K$ is a Galois extension of $\mathbb{Q}$, and determine its Galois group.

*Solution.* In the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq K$, each field is a proper subset of the one that follows, and each extension is of degree at most 2, so each extension must be of degree exactly 2. Hence $[K : \mathbb{Q}] = 2 \cdot 2 \cdot 2 = 8$.

Elements of the Galois group are determined by where they send $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{5}$, and they must send each of these to their negative. Since $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{5}$ are not roots of the same irreducible polynomial, we can choose where each goes independently of where another is mapped. So

$$G(K/\mathbb{Q}) = \{\mathrm{id}, \sigma, \tau, \rho, \sigma\tau, \sigma\rho, \tau\rho, \sigma\tau\rho\}.$$

where $\sigma$, $\tau$, and $\rho$, map $\sqrt{2}, \sqrt{3}$, and $\sqrt{5}$ to $-\sqrt{2}, -\sqrt{3}$, and $-\sqrt{5}$, respectively, and fix the other field generators. In particular, $|G(K/\mathbb{Q})| = [K : \mathbb{Q}] = 8$, so the extension is Galois. Note $G(K/\mathbb{Q}) \cong C_2 \times C_2 \times C_2$. □

**Exercise 12.** Determine all automorphisms of the field $\mathbb{Q}(\sqrt[3]{2})$.

*Solution.* Note that $f(x) = x^3 - 2$ is a polynomial having $\sqrt[3]{2}$ as root, so any automorphism of $\mathbb{Q}(\sqrt[3]{2})$ would have to take $\sqrt[3]{2}$ to another root of $f$. But we know (since $f'(x) \geq 0$ for all $x$) that $f$ has only one real root, so it must have two non-real roots. But $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, so these two roots are not elements of $\mathbb{Q}(\sqrt[3]{2})$. Hence any automorphism has to map $\sqrt[3]{2}$ to itself, meaning that it is the identity.

This is an example of a field extension which is not Galois. □

**Exercise 13.** Let $K/F$ be a finite extension. Prove that the Galois group $G(K/F)$ is a finite group.

*Proof.* Since $K/F$ is a finite extension, $K$ is finitely generated as a field over $F$ (for example, it is generated by the elements of a basis). So we can write $K = F(a_1, a_2, \ldots, a_n)$. Finite extensions are algebraic, so each $a_i$ is the root of a polynomial, say of degree $d_i$. Then every transformation is determined by how it acts on the set $\{a_1, \ldots, a_n\}$, and there are at most $d_i$ choices where to send each $a_i$, so there are at most $d_1 d_2 \cdots d_n$ elements in $G(K/F)$.

Note: A stronger statement is true: $|G(K/F)| \leq [K : F]$. In other words, there can never be more automorphisms that the degree of the extension. □

**Exercise 16.** Prove or disprove: Let $f(x)$ be an irreducible cubic polynomial in $\mathbb{Q}[x]$ with one real root $\alpha$. Show that the other roots form a complex conjugate pair $\beta, \overline{\beta}$, so the field $L = \mathbb{Q}(\beta)$ has an automorphism $\sigma$ which interchanges $\beta, \overline{\beta}$.

*Solution.* While the first part is true, the second part is false. Since $\beta$ is a root of the irreducible cubic polynomial $f(x)$, we have $[\mathbb{Q}(\beta) : \mathbb{Q}] = 3$. So the order of $G(\mathbb{Q}(\beta)/\mathbb{Q})$ divides 3. Now, $\sigma$ has even order, so it cannot be in $G(\mathbb{Q}(\beta)/\mathbb{Q})$. □

**Exercise 17.** Let $K$ be a Galois extension of a field $F$ such that $G(K/F) \cong C_2 \times C_{12}$. How many intermediate fields $L$ are there such that **(a)** $[L : F] = 4$, **(b)** $[L : F] = 9$, **(c)** $G(K/L) \cong C_4$.

*Solution.*

**(a)** By the main Galois theorem, there is exactly one intermediate field $L$ with $[L : F] = 4$ for each subgroup of $C_2 \times C_{12}$ of index 4 (i.e. of order 6). Since every subgroup of $C_2 \times C_{12}$ is abelian and every abelian group of order 6 is cyclic, we only have to check the number of cyclic subgroups of order 6. Using additive notation with $(1, 0)$ and $(0, 1)$ as generators of $C_2 \times C_{12}$, the three subgroups of order 6 are generated by $(0, 2)$, $(1, 2)$, and $(1, 4)$, respectively. Therefore there are 3 such intermediate fields.

**(b)** Again, we are counting subgroups of index 9. Since 9 does not divide 24, there are no such intermediate fields.

**(c)** By the Galois correspondence, $G(K/L)$ is equal to the subgroup of $G(K/F)$ that corresponds to $L$. So we need to find the number of subgroups

of $C_2 \times C_{12}$ that are isomorphic to $C_4$. There are two, generated by $(0,3)$, and $(1,3)$ respectively. $\square$

**Exercise 18.** Let $f(x) = x^4 + bx^2 + c \in F[x]$, and let $K$ be the splitting field of $f$. Prove that $G(K/F)$ is contained in a dihedral group.

*Proof.* By the quadratic formula, $x$ must satisfy

$$x^2 = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

So the roots of $f$ are $\{\alpha, -\alpha, \beta, -\beta\}$, where

$$\alpha = \sqrt{\frac{-b + \sqrt{b^2 - 4c}}{2}} \qquad \beta = \sqrt{\frac{-b - \sqrt{b^2 - 4c}}{2}}.$$

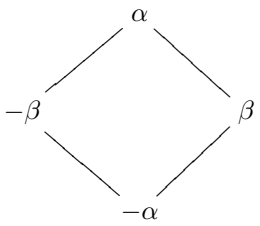
Therefore $K = F(\alpha, \beta)$. Any automorphism is completely determined by how it acts on $\alpha$ and $\beta$, and it must send each of $\alpha$ and $\beta$ to one of $\{\pm\alpha, \pm\beta\}$. We have four choices for where $\alpha$ should go, and since this choice determines where $-\alpha$ goes, we have two choices for where $\beta$ goes. So there are at most eight automorphisms of $K/F$:

id : the identity $\quad r : \alpha \mapsto \beta \mapsto -\alpha \quad r^2 : \alpha \mapsto -\alpha, \beta \mapsto -\beta \quad r^3 : \alpha \mapsto -\beta \mapsto -\alpha$

$s : \alpha \mapsto -\alpha, \beta$ fixed $\quad sr : \alpha \mapsto \beta \mapsto \alpha \quad sr^2 : \alpha$ fixed, $\beta \mapsto -\beta \quad sr^3 : \alpha \mapsto -\beta \mapsto \alpha$

This group is isomorphic to $D_4$. Of course, there may be more relations on $\alpha$ and $\beta$ (for example perhaps $\alpha \in F$), in which case not all of these maps correspond to elements of $G(K/F)$. But $G(K/F)$ is a subset, and hence a subgroup of this group, which is isomorphic to $D_4$, as desired.

It may be easier to visualize the group above as the group of symmetries of the following diagram:




Here the map $r$ is rotation clockwise by 90 degrees, and the map $s$ is a flip across the horizontal line of symmetry.

$\square$