Extra Problems Solutions

Problem 1. Let $q(x) = x^4 - 2x^2 - 2 \in \mathbb{Q}[x]$.

a) Show that q is irreducible in $\mathbb{Q}[x]$.

Proof. Applying Eisenstein's criterion for the prime 2 gives that q is irreducible in $\mathbb{Z}[x]$ and Gauss' Lemma then says that q is irreducible in $\mathbb{Q}[x]$ as well. ☐

b) The roots of q are

$$b_1 = \sqrt{1+\sqrt{3}}, \quad b_2 = \sqrt{1-\sqrt{3}}, \quad b_3 = -\sqrt{1+\sqrt{3}}, \quad \text{and } b_4 = -\sqrt{1-\sqrt{3}}.$$

Let $K_1 = \mathbb{Q}(b_1)$, $K_2 = \mathbb{Q}(b_2)$, and $F = \mathbb{Q}(\sqrt{3})$. Show that $K_1 \neq K_2$ and $K_1 \cap K_2 = F$.

Proof. If $K_1 = K_2 = K$ then K also contains $b_1 b_2 = \sqrt{1+\sqrt{3}}\sqrt{1-\sqrt{3}} = \sqrt{-2} = \sqrt{2}i$. However, $K_1, K_2 \subseteq \mathbb{R}$, so $K \subseteq \mathbb{R}$ cannot contain $\sqrt{2}i$.

Since $\sqrt{3} = b_1^2 - 1 \in K_1$, then $F \subseteq K_1$. Similarly, $\sqrt{3} = 1 - b_2^2 \in K_2$ implies $F \subseteq K_2$. Thus $F \subseteq K_1 \cap K_2$. To show the converse inclusion, note that since q is irreducible and monic it is the minimum polynomial for each one of its roots over $\mathbb{Q}$, so we have

$$[Q(b_i) : F][F : \mathbb{Q}] = [\mathbb{Q}(b_i) : \mathbb{Q}] = \deg(m_{b_i,\mathbb{Q}}) = 4 \text{ for } i = 1, 2.$$

Since

$$[F : \mathbb{Q}] = \deg m_{\sqrt{3},\mathbb{Q}} = \deg(x^2 - 3) = 2,$$

we deduce that $[Q(b_i) : F] = 2$. Moreover, since $K_1 \neq K_2$ and $K_1 \cap K_2 \neq K_i$, then

$$[K_i : K_1 \cap K_2] = [\mathbb{Q}(b_i) : K_1 \cap K_2] \geqslant 2.$$

Putting everything together we have

$$2 = [Q(b_i) : F] = [Q(b_i) : K_1 \cap K_2][K_1 \cap K_2 : F] \geqslant 2[K_1 \cap K_2 : F].$$

Therefore, $[K_1 \cap K_2 : F] = 1$ and thus $F = K_1 \cap K_2$. Note in particular that we showed that $[K_i : F] = 2$. ☐

c) Prove that K_1, K_2, and K_1K_2 are Galois over F.

Proof. Let $q_1 = x^2 - (1+\sqrt{3}) \in \mathbb{Q}(\sqrt{3})[x] = F[x]$. Then the two roots of q_1 in $\mathbb{C}$ are b_1 and $b_3 = -b_1$, and so q_1 is a separable polynomial and $K_1 = F(b_1)$ is the splitting field of q_1 over F. The splitting field of a separable polynomial over F is Galois over F, so K_1/F is Galois.

Similarly, $\sqrt{3} = -(b_1^2 - 1)$, and so $F \subseteq K_2$. The polynomial $q_2 = x^2 - (1 - \sqrt{3}) \in F[x]$ is separable, with distinct roots b_2 and $b_4 = -b_2$, and $K_2 = F(b_2)$ is the splitting field of q_2 over F. $K_1 = F(b_1)$ is the splitting field of q_1 over F. The splitting field of a separable polynomial over F is Galois over F, so K_2/F is Galois.

Finally, $K_1K_2 = K(b_1, b_2)$. Since b_1, b_2, b_3, b_4 are the four roots of the polynomial q and $b_3 = -b_1$ and $b_4 = -b_2$ are also in K_1K_2, then K_1K_2 is the splitting field of q. Moreover, q is separable (since the b_i are distinct complex numbers), and so again $K_1K_2/\mathbb{Q}$ is Galois. In particular, $K_1K_2/\mathbb{Q}$ is finite. Since $\mathbb{Q} \subseteq F \subseteq K_1K_2$, then K_1K_2/F is also Galois. ☐

d) Let $G = \mathrm{Gal}(K_1K_2/F)$. Show that G is isomorphic to $\mathbb{Z}/2 \times \mathbb{Z}/2$, and write out explicitly how this group acts on the roots of q.

Proof. Let $G = \mathrm{Gal}(K_1K_2/F)$. Consider the sucessive field extensions $\mathbb{Q} \subseteq F \subseteq K_i \subseteq K_1K_2$ for $i \in \{1, 2\}$. We already showed that $[K_i : F] = 2$ for $i \in \{1, 2\}$. Since

$$K_1K_2 = F(b_1, b_2) = (F(b_1))(b_2) = K_1(b_2)$$

and b_2 satisfies the polynomial $q_2 = x^2 - (1 - \sqrt{3}) \in K_1[x]$, then

$$[K_1K_2 : K_1] \leqslant 2.$$

Since K_2 is not contained in K_1, then $K_1K_2 \neq K_1$, and so $[K_1K_2 : K_1] \geqslant 2$. We conclude that $[K_1K_2 : K_1] = 2$.

The Degree Formula applies to give

$$[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F] = 4.$$

By definition of Galois, $|G| = |\,\mathrm{Gal}(K_1K_2/F)| = [K_1K_2 : F] = 4$.

We have shown that b_1 is a root of the monic polynomial $q_1 = x^2 - (1 + \sqrt{3}) \in F[x]$, and since we have $[K_1 : F] = 2$ it follows that $q_1 = m_{b_1,F}$ and q_1 is irreducible in $F[x]$. Similarly, $q_2 = x^2 - (1 - \sqrt{3}) = m_{b_2,F}$ is irreducible in $F[x]$. Now $q = q_1q_2$ and from the proof of (c-ii) K_1K_2 is the splitting field of q.

By a theorem from class, the orbits of the action of G on the roots of q are the sets of roots of the same irreducible factors; that is, the orbits are $\{b_1, b_3\}$ and $\{b_2, b_4\}$. Then the elements of G either swap b_1 and b_3 or fix both of them, and similarly they either swap b_2 and b_4 or fix both of them. Hence $G \cong C_2 \times C_2$, and the images of the elements of G in S_4 are e, $(1\ 3)$, $(2\ 4)$, and $(1\ 3)(2\ 4)$. □

e) Determine all of the subgroups $H \leq G$ and determine their corresponding fixed subfields $(K_1K_2)^H$.

Proof. Let $g_{(1\ 3)} \in G$ be the element that swaps b_1 and b_3 and fixes b_2 and b_4, meaning it corresponds to the permutation $(1\ 3) \in S_4$. Similarly, let $g_{(2\ 4)}, g_{(1\ 3)(2\ 4)} \in G$ be the elements corresponding to $(2\ 4)$ and $(1\ 3)(2\ 4)$. The subgroups of G are: $H_1 = \{e\}$, $H_2 = \{e, g_{(1\ 3)}\}$, $H_3 = \{e, g_{(2\ 4)}\}$, $H_4 = \{e, g_{(1\ 3)(2\ 4)}\}$, and $H_5 = G$.

Since q_1 is irreducible in $F[x]$ with degree 2 and root b_1, then $\{1, b_1\}$ is a basis for the F-vector space K_1. Similarly, q_2 is irreducible in $K_1[x]$ with degree 2 and root b_2, and so $\{1, b_2\}$ is a basis for the K_1-vector space K_1K_2. Then $\{1, b_1, b_2, b_1b_2\}$ is a basis for the F-vector space K_1K_2 as shown in the proof of the Degree Formula.

Let $k \in K_1K_2$; then $k = r + sb_1 + tb_2 + ub_1b_2$ for some $r, s, t, u \in F$. Since $e(k) = k$, then $(K_1K_2)^{H_1} = K_1K_2$.

Next

$$g_{(1\ 3)}(k) = r + sb_3 + tb_2 + ub_3b_2 = r - sb_1 + tb_2 - ub_1b_2,$$

and so $g_{(1\ 3)}(k) = k$ iff $s = u = 0$ and $k = r + tb_2 \in K_2$. Therefore, $(K_1K_2)^{H_2} = K_2$.

Similarly

$$g_{(2\ 4)}(k) = r + sb_1 + tb_4 + ub_1b_4 = r + sb_1 - tb_2 - ub_1b_2,$$

and so $g_{(2\ 4)}(k) = k$ if and only if $t = u = 0$ and $k = r + sb_1 \in K_1$. Therefore, $(K_1K_2)^{H_3} = K_1$. Also

$$g_{(1\ 3)(2\ 4)}(k) = r + sb_3 + tb_4 + ub_3b_4 = r - sb_1 - tb_2 + ub_1b_2,$$

and so $g_{(1\ 3)(2\ 4)}(k) = k$ if and only if $s = t = 0$ and $k = r + ub_1b_2$. This shows that $(K_1K_2)^{H_4} \subseteq F(b_1b_2)$. Note that $b_1b_2 = \sqrt{1+\sqrt{3}}\sqrt{1-\sqrt{3}} = \sqrt{-2}$ has minimal polynomial $x^2 + 2$ over the subfield $F = \mathbb{Q}(\sqrt{3})$ and so

$$[F(b_1b_2) : F] = 2 = [G : H_4] = [(K_1K_2)^{H_4} : F],$$

where the last equality follows from the Fundamental Theorem of Galois Theory. Now the Degree Formula gives

$$2 = [F(b_1b_2) : F] = [F(b_1b_2) : (K_1K_2)^{H_4}][(K_1K_2)^{H_4} : F] = [F(b_1b_2) : (K_1K_2)^{H_4}]2$$

and forces $(K_1K_2)^{H_4} = F(b_1b_2)$.

Finally, the element $k \in K_1K_2$ lies in $(K_1K_2)^{H_5} = (K_1K_2)^G$ if and only if $s = t = u = 0$ and $k = r \in F$. Therefore, $(K_1K_2)^{H_5} = (K_1K_2)^G = F$. □

f) Prove that the splitting field L of q over $\mathbb{Q}$ satisfies $[L : \mathbb{Q}] = 8$, and $\mathrm{Gal}(L/Q)$ is isomorphic to the dihedral group of order 8.

Hint: D_8 is the only non Hamiltonian group of order 8, meaning that D_8 is the only group of order 8 that has nonnormal subgroups.

Proof. Recall that $L = K_1K_2$ from the arguments above. Notice that $K_1 = \mathbb{Q}(b_1)$ is not Galois over $\mathbb{Q}$ because for example it does not contain all the roots of the minimal polynomial $q = m_{\beta_1,\mathbb{Q}}$ contradicting Corollary 4.74. It follows by the FTGT that the subgroup $H = \mathrm{Gal}(L/K_1)$ is a non normal subgroup of G, hence using the tip $G \cong D_8$. □