GALOIS THEORY: SOLUTIONS TO HOMEWORK 8

1. Recall the splitting field L over $\mathbb{Q}$ that you constructed in question 4(b) of Problem Sheet 7 for the polynomial $t^8 - 16$. Determine the subgroup of S_4 to which $\mathrm{Gal}(L : \mathbb{Q})$ is isomorphic.
Solution: Recall that $L = \mathbb{Q}(\alpha, \zeta)$, where $\alpha = \sqrt{2}$ and $\zeta = (1+i)/\alpha$. Thus in fact $L = \mathbb{Q}(\alpha, i)$. Take $\tau \in \mathrm{Gal}(L : \mathbb{Q})$. Then τ is determined by its action on $\alpha = \sqrt{2}$ and $i = \sqrt{-1}$. We begin by constructing $\mathbb{Q}$-homomorphisms $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha, i)$. We know that $\sigma(\alpha)$ must be a root of $m_\alpha(\mathbb{Q}) = t^2 - 2$, so $\sigma(\alpha) = \pm\alpha$. We can extend σ to $\tau : \mathbb{Q}(\alpha, i) \to \mathbb{Q}(\alpha, i)$ by taking $\tau|_{\mathbb{Q}(\alpha)} = \sigma$ and $\tau(i) = \pm i$, with the choice of sign independent of the previous choice. Here, since $m_i(\mathbb{Q}(\alpha)) = t^2 + 1$, we find that $\tau(i)$ must be one of the roots of $t^2 + 1$, explaining the previous assertion. We thus conclude that τ is one of the permutations τ_{lm} $(l, m \in \{0, 1\})$, where $\tau_{lm}(\alpha) = (-1)^l\alpha$ and $\tau_{lm}(i) = (-1)^m i$. Thus τ acts as one of the four permutations
$$(\alpha\ \ -\alpha)(i\ \ -i), \quad (\alpha\ \ -\alpha), \quad (i\ \ -i), \quad \mathrm{id}.$$
The group $\mathrm{Gal}(L : \mathbb{Q})$ is therefore isomorphic to the group of permutations
$$\{(1), (1\ 2), (3\ 4), (1\ 2)(3\ 4)\}.$$

2. Suppose that K is a field and that $L : K$ is a splitting field extension for an irreducible polynomial $f \in K[t]$ of degree n. Assume that $K \subseteq L$.
   (a) Show that whenever α and β are roots of f in L, and σ is a K-automorphism of L, then $\sigma(\alpha) = \sigma(\beta)$ if and only if $\alpha = \beta$;
   Solution: Since σ is a K-automorphism of L, it is bijective and hence invertible. Then $\sigma(\alpha) = \sigma(\beta)$ if and only if $\sigma^{-1}(\sigma(\alpha)) = \sigma^{-1}(\sigma(\beta))$, which is to say, if and only if $\alpha = \beta$.
   (b) Show that the elements of $\mathrm{Gal}(L : K)$ act as permutations on the n roots of f, and hence deduce that $\mathrm{Gal}(L : K)$ has order dividing $n!$;
   Solution: Let $\alpha \in L$ be a root of f, and consider $\tau \in \mathrm{Gal}(L : K)$. Then $\tau(f(\alpha)) = f(\tau(\alpha))$. Thus, under the action of any element τ of $\mathrm{Gal}(L : K)$, a root α of f is taken to another root β of f. Since this mapping is bijective, it follows that σ acts as a permutation on the set of roots of f. A permutation group on a set of n objects is a subset of S_n (the permutation group on n letters), and hence by Lagrange's theorem has order dividing $n!$.
   (c) Let g be a degree m polynomial in $K[t]$, not necessarily irreducible, and let $M : K$ be a splitting field extension for g. Show that $|\mathrm{Gal}(M : K)|$ divides $m!$.
   Solution: Let $\alpha \in M$ be a root of g, and consider $\tau \in \mathrm{Gal}(M : K)$. Then again $\tau(g(\alpha)) = g(\tau(\alpha))$. Thus, just as in the discussion for part (b), the mapping τ acts as a permutation on the distinct roots of g. If the number of distinct roots of g is n, then it follows that $|\mathrm{Gal}(M : K)|$ divides $n!$. But $n \leq m$, so $n!$ divides $m!$, whence $|\mathrm{Gal}(M : K)|$ divides $m!$.

3. Suppose that $L : K$ is a normal extension, and that $K \subseteq L \subseteq \overline{K}$. Recall that since $L : K$ is algebraic, then any algebraic closure of K is an algebraic closure of L.
   (a) Show that for any K-homomorphism $\tau : L \to \overline{K}$, one has $\tau(L) = L$;

Solution: Let $\tau : L \to \overline{K}$ be a K-homomorphism. Let $\alpha \in L$. Then since $L : K$ is algebraic, one sees that α is algebraic over K, and so $m_\alpha(K)$ exists. Write $g = m_\alpha(K)$. Then on noting that g is a K-homomorphism, we deduce that $0 = \tau(g(\alpha)) = g(\tau(\alpha))$. But $L : K$ is normal, so $\tau(\alpha) \in L$. Since this holds for all $\alpha \in L$, we infer that $\tau(L) \subseteq L$. Finally, since $L : K$ is algebraic, it follows from Theorem 3.4 that $\tau(L) = L$.

(b) Suppose that M is a field satisfying $K \subseteq M \subseteq L$. Show that $L : M$ is a normal extension.

Solution: Assume $K \subseteq M \subseteq L$, and let $f \in M[t] \setminus M$ be irreducible. Suppose that $\alpha \in L$ is a root of f. Then $f = \lambda m_\alpha(M)$ for some $\lambda \in M^\times$. But $m_\alpha(M)$ divides $m_\alpha(K)$, and since $L : K$ is normal, one has that $m_\alpha(K)$ splits over L. Hence $m_\alpha(M)$ also splits over L, and thus f splits over L. Then $L : M$ is a normal extension.

4. Which of the following field extensions are normal? Justify your answers.
   (a) $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$
   (b) $\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}$
   (c) $\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}$
   (d) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$
   (e) $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$.

Solution: (a) Normal: this is a splitting field extension for $t^2 - 3$ over $\mathbb{Q}$, since $t^2 - 3 = (t - \sqrt{3})(t + \sqrt{3})$ splits over $\mathbb{Q}(\sqrt{3})$, and splitting field extensions are normal extensions.
(b) Not normal: the polynomial $t^3 - 3$ has one root $\sqrt[3]{3}$ lying in $\mathbb{Q}(\sqrt[3]{3})$, yet does not split over the latter field. For writing $\omega = e^{2\pi i/3}$, the remaining roots $\sqrt[3]{3}\omega$ and $\sqrt[3]{3}\omega^2$ over $\overline{\mathbb{Q}}$ are not real, and cannot lie in $\mathbb{Q}(\sqrt[3]{3})$.
(c) Normal: this is a splitting field extension for $t^2 + 1$ over $\mathbb{Q}$, since the polynomial $t^2 + 1 = (t - \sqrt{-1})(t + \sqrt{-1})$ splits over $\mathbb{Q}(\sqrt{-1})$, and splitting field extensions are normal extensions.
(d) Not normal: the polynomial $t^3 - 3$ has one root $\sqrt[3]{3}$ lying in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$, yet does not split over the latter field, for the remaining roots $\sqrt[3]{3}\omega$ and $\sqrt[3]{3}\omega^2$ over $\overline{\mathbb{Q}}$ are not real, and cannot lie in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$.
(e) Normal: this is a splitting field extension for $(t^2 + 1)(t^3 - 3)$ over $\mathbb{Q}$, since

$$(t^2 + 1)(t^3 - 3) = (t - \sqrt{-1})(t + \sqrt{-1})(t - \sqrt[3]{3})(t - \omega\sqrt[3]{3})(t - \omega^2\sqrt[3]{3}),$$

with $\omega = \frac{1}{2}(-1 + \sqrt{-1}\sqrt{3}) \in \mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3})$. Here, we confirm that this satisfies the minimality condition on noting that $\sqrt{3} = (1 + 2\omega\sqrt[3]{3}/\sqrt[3]{3})/\sqrt{-1} \in \mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3})$. Moreover, splitting field extensions are normal extensions.

5. Let $K = \mathbb{F}_5(t)$. Find an algebraic field extension $L : K$ which is not normal, and justify your answer.

Solution: Let $\overline{K}$ denote an algebraic closure of K with $K \subset \overline{K}$, and consider the element $t^{1/3} \in \overline{K}$ that is a root of the polynomial $X^3 - t \in K[X]$. We claim that the algebraic extension $L : K$, where $L = K(t^{1/3})$, is not a normal extension. If $\alpha \in \overline{K}$ satisfies the equation $\alpha^3 - t = 0$, then we have $(\alpha/t^{1/3})^3 = 1$, so that $\alpha = \beta t^{1/3}$ with $\beta^3 = 1$. Thus, we find that β satisfies the equation $(\beta - 1)(\beta^2 + \beta + 1) = 0$. Then either $\beta = 1$, or else $(2\beta + 1)^2 = -3$. There is no element $\gamma \in \mathbb{F}_5$ with $\gamma^2 = -3$, since $1^2 \equiv 4^2 \equiv 1 \pmod 5$ and $2^2 \equiv 3^2 \equiv -1 \pmod 5$. Observe that $K(t^{1/3}) = \mathbb{F}_5(t^{1/3})$. Then if $\gamma \in \mathbb{F}_5(t^{1/3}) \setminus \mathbb{F}_5$ satisfies $\gamma^2 = -3$, then there is a non-constant polynomial $h \in \mathbb{F}_5[X]$ having the property that $h(t^{1/3}) = 0$. The existence of such a polynomial would show that $t^{1/3}$, and hence also t, are algebraic over $\mathbb{F}_5$, contradicting the (implicit) assumption that t is transcendental over $\mathbb{F}_5$. Then no element $\gamma \in K(t^{1/3})$ satisfies the equation $\gamma^2 = -3$, and thus the only solution $\beta \in K(t^{1/3})$ of $\beta^3 = 1$ is $\beta = 1$. The only linear factor of $X^3 - t$ over $L[X]$ is therefore $X - t^{1/3}$. Finally, since $X^3 - t \neq (X - t^{1/3})^3$, we conclude that $X^3 - t$ does not split over $K(t^{1/3})$, whence $L : K$ is not a splitting field extension, and consequently is not normal.