GALOIS THEORY: SOLUTIONS TO HOMEWORK 9

1. Suppose that $E : K$ and $F : K$ are finite extensions having the property that K, E and F are contained in a field L.

   (a) Show that $EF : K$ is a finite extension;

   Solution: Since $E : K$ and $F : K$ are both finite extensions, then for some natural number n there exist elements $\alpha_1, \ldots, \alpha_n \in E$, all algebraic over K, such that $E = K(\alpha_1, \ldots, \alpha_n)$. Thus $EF = F(\alpha_1, \ldots \alpha_n)$, and it follows from the tower law that $[EF : F] \leq \prod_{i=1}^{n} [F(\alpha_i) : F] < \infty$. But then, again by the tower law, one has $[EF : K] = [EF : F][F : K] < \infty$, and so $EF : F$ is a finite extension.

   (b) Show that when $E : K$ and $F : K$ are both normal, then $E \cap F : K$ is a normal extension;

   Solution: For any $\alpha \in E \cap F$, one sees that since E is algebraic over K, then α is algebraic over K. Hence $E \cap F : K$ is algebraic. Suppose next that $f \in K[t] \setminus K$ has the property that f is irreducible over K, and $f(\alpha) = 0$ for some $\alpha \in E \cap F$. Thus f splits over E and over F, and so f splits over $E \cap F$. Hence $E \cap F : K$ is a normal extension.

   (c) Show that when $E : K$ and $F : K$ are both normal, then $EF : E \cap F$ is a normal extension.

   Solution: Theorem 6.7 shows that $EF : K$ is normal. Since $EF : E \cap F : K$ is a tower of field extensions with $EF : K$ normal, it follows from Proposition 6.3 that $EF : E \cap F$ is also normal.

2. Suppose that $L : M$ is an algebraic extension with $M \subseteq L$. Show that when $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism, then $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$ if and only if $m_\alpha(M)$ is separable over M.

   Solution: Suppose that $\alpha \in L$ and $\sigma : M \to \overline{M}$ is a homomorphism. This homomorphism may be extended to a homomorphism $\sigma : \overline{M} \to \overline{M}$. Since $L : M$ is algebraic, we know that $m_\alpha(M)$ exists. Over $\overline{M}$, we have

   $$m_\alpha(M) = (t - \alpha_1)^{r_1} \cdots (t - \alpha_d)^{r_d},$$

   where $\alpha_1, \ldots, \alpha_d$ are distinct and $r_1, \ldots, r_d \in \mathbb{N}$. Then

   $$\sigma(m_\alpha(M)) = (t - \sigma(\alpha_1))^{r_1} \cdots (t - \sigma(\alpha_d))^{r_d},$$

   and since σ is necessarily injective, we know that $\sigma(\alpha_1), \ldots, \sigma(\alpha_d)$ are distinct. Thus $m_\alpha(M)$ has multiple roots if and only if $\sigma(m_\alpha(M))$ has multiple roots. We know that $\sigma(m_\alpha(M))$ is irreducible over $\sigma(M)$ since $m_\alpha(M)$ is irreducible over M. Hence $m_\alpha(M)$ is separable over M if and only if $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$.

3. (a) Suppose that $f \in K[t]$ is separable over K and that $L : K$ is a splitting field extension for f. Show that $L : K$ is separable.

   Solution: Assume that $K \subseteq L$. Since $L : K$ is a splitting field extension for f, we have that $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_1, \ldots, \alpha_n \in L$ are the roots of f. For each i with $1 \leq i \leq n$, we have that $m_{\alpha_i}(K)$ divides f, and since f is separable over K and $m_{\alpha_i}(K)$ is irreducible over K, we know by definition that $m_{\alpha_i}(K)$ is separable over K. Thus α_i is separable over K for each i, and hence by Theorem 7.4, the field extension $L : K$ is separable.

(b) Suppose that $L : K$ is a splitting field extension for $S \subseteq K[t]$ where each $f \in S$ is separable over K. Show that $L : K$ is a separable extension.
Solution: Let $\alpha \in L$. Then by Proposition 1.9, we have that $\alpha \in D$, where D is some finite subset of $A = \{\beta \in L : g(\beta) = 0 \text{ for some } g \in S\}$. For each $\beta \in D$, choose $g_\beta \in S$ in such a manner that β is a root of g_β. Put $h = \prod_{\beta \in D} g_\beta$, and let $M : K$ be a splitting field extension for h. We may assume here that $K \subseteq M \subseteq L$. Since g_β is separable over K for each $\beta \in D$, we deduce that h is separable over K. Thus, by part (a), we conclude that $M : K$ is separable. But $\alpha \in K(D) \subseteq M$, and so α is separable over K. Finally, since this argument holds for all $\alpha \in L$, we find that $L : K$ is separable.

4. Let p be a prime number, let $\mathbb{F}_p$ denote the finite field of p elements, and let $K = \mathbb{F}_p(t)$. Suppose that $L : K$ is a field extension, and $s \in L$ is transcendental over K.
(a) Write $J = K(s)$, and let E denote a splitting field for the polynomial $x^p - t \in J[x]$. Show that for some $\xi \in E$, one has $x^p - t = (x - \xi)^p$, and deduce that $[E : J] = p$.
Solution: Let E denote a splitting field for $x^p - t$ over J. Write $h(x) = x^p - t$. Since E is a splitting field for h, there exists some $\xi \in E$ with $h(\xi) = 0$. In particular, one has $\xi^p = t$. But since the binomial coefficients $\binom{p}{r}$ are divisible by p, and hence zero in $\mathbb{F}_p$ for $1 \le r < p$, we have $(x - \xi)^p = x^p - \xi^p = x^p - t$, as desired.
We next show that h is irreducible over J. If $(x - \xi)^p = x^p - t = fg$, with $f, g \in J[x]$ monic polynomials of degree at least one, then since $E[x]$ is a UFD, one finds that $f = (x - \xi)^u$ and $g = (x - \xi)^{p-u}$ for some integer u with $1 \le u \le p - 1$. Since p and u are coprime, so too are $p - u$ and u, and hence there exist $a, b \in \mathbb{Z}$ with $au + b(p - u) = 1$. Thus $x - \xi = f^a g^b \in J[x]$, whence $\xi \in J$. But then there exist $c, d \in \mathbb{F}_q[s, t] \setminus \{0\}$ with $\xi = c/d$. Hence $t = \xi^p = c^p/d^p$, so that $c^p = td^p$. The degree of the polynomial on the left hand side of the last relation is divisible by p, while on the right hand side the degree is congruent to 1 modulo p, a contradiction. Thus, the hypothesised factorisation does not exist, and so h is irreducible over J. Finally, since h is irreducible over $J[x]$, one has $h = m_\xi(J)$. Since $E = J(\xi)$, we deduce that $[E : J] = \deg(m_\xi(J)) = p$, as desired.
(b) Let $U : J$ be a splitting field extension for the polynomial $(x^p - t)(x^p - s)$. By considering a splitting field extension F for the polynomial $x^p - s \in E[x]$, show that $[U : J] = p^2$.
Solution: We have $E = J(\xi) \subseteq \mathbb{F}_p(\xi, s)$. The same argument as in part (a), in all essentials, shows that $[F : E] = p$. For some $\eta \in U$ we have $x^p - s = (x - \eta)^p$. Were $x^p - s$ to fail to be irreducible over $E[x]$, then for some integer v with $1 \le v \le p-1$, we would have $\eta^v = s$. But then we deduce as before that $\eta \in E$. Then the relation $\eta^p = s$ implies the existence of polynomials $c', d' \in \mathbb{F}_p(\xi)[s]$ with $(c')^p = s(d')^p$, leading to a contradiction (on considering the degrees of left and right hand sides as polynomials in s). Then $x^p - s$ is irreducible over $E[x]$. Since $F = E(\eta)$, we obtain $[F : E] = \deg(m_\eta(E)) = p$, as required. Finally, by the Tower Law, we have $[F : J] = [F : E][E : J] = p^2$. But $E \subsetneq U \subseteq F$. Then by the Tower Law we see that $[U : J]$ is a divisor of p^2 exceeding p, which is to say that $[U : J] = p^2$.

5. With the same notation as in the previous question:
(a) Show that if $\gamma \in U$, then $\gamma^p \in J$.
Solution: The field U contains elements ξ and η with $\xi^p = t$ and $\eta^p = s$, and one has $(x^p - t)(x^p - s) = (x - \xi)^p(x - \eta)^p$, so that $U = J(\xi, \eta)$. Then if $\gamma \in U$, we may find non-zero polynomials $q, r \in J[x_1, x_2]$ for which $\gamma = q(\xi, \eta)/r(\xi, \eta)$.

But then by our earlier observation concerning pth powers, one finds that $\gamma^p = q(\xi^p, \eta^p)/r(\xi^p, \eta^p) = q(t, s)/r(t, s) \in J$.

(b) What is the degree of the field extension $J(\gamma) : J$? Explain.
Solution: Let $\delta = \gamma^p \in J$. Then the minimal polynomial of γ over J divides $t^p - \delta$, hence has degree at most p. In particular, one has $1 \leq [J(\gamma) : J] \leq p$. On the other hand, since $J \subseteq J(\gamma) \subseteq U$, it follows from the Tower Law that $[J(\gamma) : J]$ divides $[U : J] = p^2$. Thus we conclude that $[J(\gamma) : J] = 1$ or p.

(c) Deduce that $U : J$ is a finite field extension which is not simple.
Solution: Suppose that $U : J$ is a simple extension, so that for some element $\gamma \in U$, one has $U = J(\gamma)$. Then from part (b) we have $[U : J] = [J(\gamma) : J] = 1$ or p, yet from 4(b) we must have $[U : J] = p^2$. This yields a contradiction, and so the finite field extension $U : J$ is not simple.