Galois theory, Problems 4

To be handed in by 1:00 pm, 22 November 2017 **SOLUTIONS**

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.

   (i) 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 $E = K(\alpha_1, \ldots, \alpha_m)$. 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.

   (ii) 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 $E \cap F$. [Note that we can suppose that $K \subseteq E \subseteq \overline{K}$ and $K \subseteq F \subseteq \overline{K}$; let A be the set of roots of f in $\overline{K}$. Since $\overline{K}[t]$ is a UFD, f splits over E if and only if $A \subseteq E$ and f splits over F if and only if $A \subseteq F$.] Hence $E \cap F : K$ is a normal extension.

   (iii) 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. As Proposition 6.3 was left as an exercise, let us quickly prove that $EF : E \cap F$ is normal. As $EF : K$ is a finite, normal extension, it is a splitting field extension for some polynomial $f \in K[t]$. Thus $EF : E \cap F$ is also a splitting field extension for f, and hence $EF : E \cap F$ is a normal extension.

2. Which of the following field extensions are normal?

   (i) $\mathbb{Q}(\sqrt{3}) : \mathbb{Q}$
   Solution: 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.

   (ii) $\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}$
   Solution: 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 the remaining roots $\sqrt[3]{3}\omega$ and $\sqrt[3]{3}\omega^2$ over $\overline{\mathbb{Q}}$ are not real, and cannot lie in $\mathbb{Q}(\sqrt[3]{3})$.

   (iii) $\mathbb{Q}(\sqrt{-1}) : \mathbb{Q}$
   Solution: Normal: this is a splitting field extension for $t^2 + 1$ over $\mathbb{Q}$, since $t^2 + 1 = (t - \sqrt{-1})(t + \sqrt{-1})$ splits over $\mathbb{Q}(\sqrt{-1})$, and splitting field extensions are normal extensions.

   (iv) $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$
   Solution: 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 $\mathbb{Q}(\sqrt{3}, \sqrt[3]{3})$.

(v) $\mathbb{Q}(\sqrt{-1}, \sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}$.
Solution: 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.

Justify your answers.

3. 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 $\alpha \in L$ 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

$$m_\alpha(M) = \prod_{i=1}^{d} (t-\alpha_i)^{r_i},$$

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

$$\sigma(m_\alpha(M)) = \prod_{i=1}^{d} (t-\sigma(\alpha_i))^{r_i},$$

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 $\sigma(M)$.

4. (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.

5. Let p be a prime number, let $\mathbb{F}_p$ denote the finite field of p elements, and let $K = \mathbb{F}_p(t)$ where t is transcendental over $\mathbb{F}_p$. 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: Without loss of generality, assume that $J \subseteq E$. Take $\xi \in E$ so that ξ is a root of $x^p - t$. Then since $\mathrm{char}K = \mathrm{char}\mathbb{F}_p$, by the Binomial Theorem we have $(x - \xi)^p = x^p - t$ [recall that for any prime p, in $\mathbb{F}_p$ we have $(-1)^p = -1$]. Hence $E = J(\xi)$. To show that $[E : J] = p$, we show that $x^p - t$ is irreducible over $J[x]$. By Theorem 8.7, $x^p - t$ is irreducible over J if t is not a pth power in J. For the sake of contradiction, suppose that $t = \alpha^p$ for some $\alpha \in J$. Thus $\alpha = \beta/\gamma$ for some $\beta, \gamma \in \mathbb{F}_p[t, s]$ [as J is the field of fractions of $\mathbb{F}_p[t, s]$]. If $\beta \notin \mathbb{F}_p[t]$ or $\gamma \notin \mathbb{F}_p[t]$, then $t\gamma^p - \beta^p = 0$ shows that s satisfies a nontrivial algebraic relation over $\mathbb{F}_p(t)$, contradicting that s is transcendental over $\mathbb{F}_p(t)$. So suppose that $\beta, \gamma \in \mathbb{F}_p[t]$; then $1 = \deg_t(\beta^p) - \deg_t(\gamma^p) = p(\deg_t \beta - \deg_t \gamma)$, which is impossible. [Note that for $\beta \in \mathbb{F}_p[t]$, $\deg_t \beta$ is well-defined as t is transcendental over $\mathbb{F}_p$.] Hence $x^p - t = m_t(J)$ and so $[E : J] = [J(\xi) : J] = p$.

   Alternatively: one could show that $x^p - t$ is irreducible over $\mathbb{F}_p[t, s]$ using Eisenstein's Criterion, and then by Gauss' Lemma, one has that $x^p - t$ is irreducible over J. To show t is irreducible in $\mathbb{F}_p[t, s]$, suppose that $t = gh$ for some (nonzero) $g, h \in \mathbb{F}_p[t, s]$. [Note: since t and s are transcendental over $\mathbb{F}_p$, g is a unit in $\mathbb{F}_p[t, s]$ if and only if $g \in \mathbb{F}_p^\times$.] So $0 = \deg_x t = \deg_s g + \deg_s h$. [Since s is transcendental over $\mathbb{F}_p(t)$, $\deg_s f$ makes sense for any $f \in \mathbb{F}_p[t, s]$.] Thus $g, h \in \mathbb{F}_p[t]$, and $1 = \deg_t g + \deg_t h$. [Since t is transcendental over $\mathbb{F}_p$, $\deg_t f$ makes sense for any $f \in \mathbb{F}_p[t]$.] Hence either g or h is a unit in $\mathbb{F}_p[t]$, meaning that g or h lies in $\mathbb{F}_p^\times$. Thus t is irreducible in $\mathbb{F}_p[t, s]$ and so by Eisenstein's Criterion, $x^p - t$ is irreducible over $\mathbb{F}_p[t, s]$.

   (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: Assume that $E \subseteq U$. Take $\zeta \in U$ so that ζ is a root of $x^p - s$. Hence $(x - \zeta)^p = x^p - s$, and $U = E(\zeta)$. (Note that E is the field of fractions of $\mathbb{F}_p[\xi, s]$.) For the sake of contradiction, suppose that $s = (\beta/\gamma)^p$ where $\beta, \gamma \in \mathbb{F}_p[\xi, s]$. Since $\xi^p = t$, we have $\beta^p, \gamma^p \in \mathbb{F}_p[t, s]$, and as polynomials in s, β^p, γ^p have degrees divisible by p; hence $s \neq (\beta/\gamma)^p$. Thus $x^p - s = m_s(E)$ so $[U : E] = [E(\zeta) : E] = p$. Thus by the Tower Law, $[E : J] = p^2$.

   Alternatively: one could show that $x^p - s$ is irreducible over $\mathbb{F}_p[\xi, s]$ using Eisenstein's Criterion. To argue as in (a), we need to first show that ξ is transcendental over $\mathbb{F}_p(s)$. For the sake of contradiction, suppose that ξ is the root of some $g \in \mathbb{F}_p(s)[x]$. If $g \in \mathbb{F}_p[x]$ then ξ is algebraic over $\mathbb{F}_p$ and hence $t = \xi^p$ is algebraic over $\mathbb{F}_p$, a contradiction. So suppose $g \notin \mathbb{F}_p[x]$. Write $g = (a_0/b_0) + (a_1/b_1)x + \cdots + (a_n/b_n)x^n$ where $a_i, b_i \in \mathbb{F}_p[s]$, $b_i \neq 0$ $(0 \leq i \leq n)$; also, $g \notin \mathbb{F}_p(s)$ so $a_n \neq 0$ with $n > 0$. Set $h = (b_0 \cdots b_n)g$; so h is a nonzero element of $\mathbb{F}_p[s, x]$ with $h(\xi) = 0$. Also,

$$0 = (h(\xi))^p = h^p(t) \in \mathbb{F}_p[t, s].$$

   If $\deg_s h^p(t) > 0$ then s is algebraic over $\mathbb{F}_p(t)$, a contradiction. If $\deg_s h^p(t) = 0$ then t is algebraic over $\mathbb{F}_p$, a contradiction. Thus ξ must be transcendental over $\mathbb{F}_p(s)$, and hence arguing as in (a) [with ξ playing the role of s and s playing the role of t], we see that s is irreducible in $\mathbb{F}_p[\xi, s]$.

6. 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 ζ with $\xi^p = t$ and $\zeta^p = s$, and one has $(x^p - t)(x^p - s) = (x - \xi)^p(x - \zeta)^p$, so that $U = J(\xi, \zeta)$. Then if $\gamma \in U$, we may find non-zero polynomials $q, r \in J[x_1, x_2]$ for which $\gamma = q(\xi, \zeta)/r(\xi, \zeta)$. But then by our earlier observation concerning pth powers, one finds that $\gamma^p = q(\xi^p, \zeta^p)/r(\xi^p, \zeta^p) = q(t, s)/r(t, s) \in J$.

   (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 5(b) we must have $[U : J] = p^2$. This yields a contradiction, and so the finite field extension $U : J$ is not simple.