GALOIS THEORY 2019: HW 4 SOLUTIONS

For assessment: Problems 1, 2, 3

Due by noon Tuesday, week 9 of the term

1. (Here you are to prove Proposition 7.2.) Suppose that $L : M$ is an algebraic field extension, and let $\overline{M}$ be an algebraic closure of M; suppose that $M \subseteq L \subseteq \overline{M}$. Also suppose $\alpha \in L$ (so $m_\alpha(M)$ exists), and suppose $\sigma : M \to \overline{M}$ is a homomorphism. Show that if $m_\alpha(M)$ is separable over M then $\sigma(m_\alpha(M))$ is separable over $\sigma(M)$.

   Solution: First, since $m_\alpha(M)$ is separable and irreducible over M, over $\overline{M}$, we have

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

   where $\alpha_1, \ldots, \alpha_d \in \overline{M}$ are distinct. Next, since $\overline{M} : L$ is an algebraic extension, by Theorem 4.5 we can extend σ to a homomorphism $\tau : \overline{M} \to \overline{M}$. Then

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

   and since τ is necessarily injective, we know that $\tau(\alpha_1), \ldots, \tau(\alpha_d)$ are distinct. Thus $\sigma(m_\alpha(M))$ has no multiple roots in $\overline{M}$. We know that $\sigma(m_\alpha(M))$ is irreducible over $\sigma(M)$ since $m_\alpha(M)$ is irreducible over M, so $\sigma(m_\alpha(M))$ is separable over M.

2. (Here you are to prove Corollary 8.6.) Suppose $\mathrm{char}K = p > 0$ and K is algebraic over its prime subfield. Then all polynomials in $K[t] \setminus K$ are separable over K.

   Solution: Take $f \in K[t]$ so that f is irreducible over K; for the sake of contradiction, suppose f is inseparable over K. Then by Theorem 8.2, $f(t) = g(t^p)$ for some $g \in K[t]$. By Corollary 8.5, every element of K is a pth power, so $f(t) = g(t^p) = (g(t))^p$, contradicting the assumption that f is irreducible over K. Hence every irreducible element of $K[t]$ is separable, and thus every element of $K[t] \setminus K$ are separable over K.

   ALTERNATIVELY: Let $\overline{K}$ be an algebraic closure of K; assume that $K \subseteq \overline{K}$. Take irreducible $f \in K[t]$. Over $\overline{K}$, we have

   $$f = \lambda \prod_{i=1}^{d}(t - \alpha_i)^{r_i}$$

   where $\lambda \in K, \alpha_1, \ldots, \alpha_d \in \overline{K}, r_1, \ldots, r_d \in \mathbb{Z}_+$. Set $E = F(\alpha_1, \ldots, \alpha_d)$. As K is algebraic over F, we know that $\overline{K}$ is an algebraic closure of F, and so $\alpha_1, \ldots, \alpha_d$ are algebraic over F and hence $[E : F] < \infty$. Let $m = [E : F]$; so $|E| = p^m$ and each element of E is a root of $t^{p^m} - t$ [recall that $E^\times$ is a group under multiplication with order $p^m - 1$]. We have $t^{p^m} - t, f \in K[t]$ with f irreducible over K and α_1 a root of both polynomials; thus f must divide $t^{p^m} - t$. As $t^{p^m} - t$

has no multiple roots, neither does f, and hence f is separable over K.

3. (Proposition 10.1) Let K, M, L be fields so that $K \subseteq L$ and $M \subseteq L$. Suppose G and H are subgroups of $Aut(L)$. Prove the following.
   (a) If $K \subseteq M$ then $Gal(L : K) \supseteq Gal(L : M)$.
   (b) If G is a subgroup of H, then $Fix_L(G) \supseteq Fix_L(H)$.
   (c) $K \subseteq Fix_L(Gal(L : K))$.
   (d) $G \subseteq Gal(L : Fix_L(G))$.
   (e) $Gal(L : K) = Gal(L : Fix_L(Gal(L : K)))$.
   (f) $Fix_L(G) = Fix_L(Gal(L : Fix_L(G)))$.

   Solutions:

   (a) Suppose $K \subseteq M$. Take $\sigma \in Gal(L : M)$. Thus $\sigma \in Aut(L)$ and σ fixes M pointwise. Since $K \subseteq M$, σ fixes K pointwise. Hence $\sigma \in Gal(L : K)$. Thus $Gal(L : K) \supseteq Gal(L : M)$.

   (b) Suppose G is a subgroup of H. Take $\alpha \in Fix_L(H)$. Thus for all $\sigma \in H$, we have $\sigma(\alpha) = \alpha$. Since $G \subseteq H$, this means that for all $\sigma \in G$, we have $\sigma(\alpha) = \alpha$. Thus $\alpha \in Fix_L(G)$, and hence $Fix_L(G) \supseteq Fix_L(H)$.

   (c) Suppose $\alpha \in K$. Recall that $K \subseteq L$, so $\alpha \in L$. Then for all $\sigma \in Gal(L : K)$, we have $\sigma(\alpha) = \alpha$, so $\alpha \in Fix_L(Gal(L : K))$. Hence $K \subseteq Fix_L(Gal(L : K))$.

   (d) Take $\sigma \in G$. So $\sigma \in Aut(L)$. Also, for every $\alpha \in Fix_L(G)$, we have $\sigma(\alpha) = \alpha$. Thus $\sigma \in Gal(L : Fix_L(G))$. Hence $G \subseteq Gal(L : Fix_L(G))$.

   (e) We know that the elements of $Gal(L : K)$ are necessarily K-homomorphisms; hence $K \subseteq Fix_L(Gal(L : K))$. Then by (a) [taking $M = Fix_L(Gal(L : K))$], we have

   $$Gal(L : K) \supseteq Gal(L : Fix_L(Gal(L : K)).$$

   By (d) [taking $G = Gal(L : K)$], we have

   $$Gal(L : K) \subseteq Gal(L : Fix_L(Gal(L : K))).$$

   Hence $Gal(L : K) = Gal(L : Fix_L(Gal(L : K)))$.

   (f) By (d), $G \subseteq Gal(L : Fix_L(G))$, so by (b) we have

   $$Fix_L(G) \supseteq Fix_L(Gal(L : Fix_L(G))).$$

   Also, by (c) [taking $K = Fix_L(G)$], we have

   $$Fix_L(G) \subseteq Fix_L(Gal(L : Fix_L(G))).$$

   Hence $Fix_L(G) = Fix_L(Gal(L : Fix_L(G)))$.

4. (This is Corollary 7.6 (b)) Suppose that $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$.
   (a) Show that if $L : K$ is a separable extension then each $f \in S$ is separable over K.
   (b) Show that if each $f \in S$ is separable over K then $L : K$ is a separable extension.

Solution:

Assume that $K \subseteq L$.

(a) Suppose $L : K$ is a splitting field extension for $S \subseteq K[t] \setminus K$ and $L : K$ is a separable extension. Thus for any $f \in S$, the roots of f are separable over K, and hence f is separable over K.

(b) Conversely, suppose that each element of S is separable over K. Take $\alpha \in L$. Thus by Proposition 1.9, $\alpha \in D$ 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 $g_\beta \in S$ so that β is a root of g_β. Set $h = \prod_{\beta \in D} g_\beta$, and let $M : K$ be a splitting field extension for h; assume that $K \subseteq M \subseteq L$. Since each g_β is separable over K ($\beta \in D$), h is separable over K. Thus by the first part of this Corollary, $M : K$ is separable. Since $\alpha \in K(D) \subseteq M$, we have that α is separable over K. As this argument holds for all $\alpha \in L$, we have that $L : K$ is separable.

5. (This is Theorem 8.1) Let $f \in K[t]$, $f \neq 0$, and let $L : K$ be a splitting field extension for f. Show that the following are equivalent:
   (i) f has a multiple root in L.
   (ii) There is some $\alpha \in L$ so that $f(\alpha) = 0 = (Df)(\alpha)$.
   (iii) There is some $g \in K[t]$ so that $\deg g \geq 1$ and g divides both f and Df.

   Solution: Write $f = \sum_{k=0}^{n} a_k t^k$.

   To show (i) implies (ii): Suppose f is not separable over K. So over L, we have

$$f = \lambda \prod_{i=0}^{m} (t - \alpha_i)^{r_i}$$

   where $\lambda \in K$, $\alpha_i \in L$, and $r_i \in \mathbb{Z}_+$ with $r_j > 1$ for some j ($1 \leq j \leq m$). Thus $t - \alpha_j$ is a factor of both f and Df, so $f(\alpha_j) = 0 = (Df)(\alpha_j)$.

   To show (ii) implies (iii): Suppose there is some $\alpha \in L$ so that $f(\alpha) = 0 = (Df)(\alpha)$. Let $g = m_\alpha(K)$. So $g \in K[t]$ with $\deg g \geq 1$, and

$$(g) = \{h \in K[t] : \ h(\alpha) = 0 \ \}.$$

   So $f, Df \in (g)$, and hence g divides both f and Df.

   To show (iii) implies (i): Suppose there is some $g \in K[t]$ so that $\deg g \geq 1$ and g divides both f and Df. Since f splits over L, so does g. Hence there is some and take $\alpha \in L$ so that $g(\alpha) = 0$. Over L, we have $f = (t - \alpha)h$, some $h \in L[t]$. We have

$$Df = h + (t - \alpha)(Dh).$$

   Since $g | Df$, we must have that $(t - \alpha) | Df$. Hence $(t - \alpha) | h$, and since $f = (t - \alpha)h$, we have $(t - \alpha)^2 | f$. Thus f is not separable over K.

6. (Part of Theorem 9.1) Suppose that K is an infinite field, α, β are algebraic over K, and $L : K$ is a splitting field extension for

$$m_\alpha(K) \cdot m_\beta(K).$$

Suppose that $\varphi_1, \ldots, \varphi_r$ are **distinct** monomorphisms from $K(\alpha, \beta)$ into L that fix K pointwise.

(a) Show that $f \neq 0$, where

$$f = \prod_{i \neq j} \big((\varphi_i(\alpha) - \varphi_j(\alpha)) + (\varphi_i(\beta) - \varphi_j(\beta))t\big).$$

(b) Show that there is some $\delta \in K$ so that $f(\delta) \neq 0$.

(c) With δ as above, set $\gamma = \alpha + \beta\delta$. Show that for $i \neq j$ $(1 \leq i, j \leq r)$, we have $\varphi_j(\gamma) \neq \varphi_j(\gamma)$.

Solution: (a) Suppose that $f = 0$. Then for some i, j with $i \neq j$, we have

$$(\varphi_i(\alpha) - \varphi_j(\alpha)) + (\varphi_i(\beta) - \varphi_j(\beta))t = 0.$$

Thus $\varphi_i(\alpha) = \varphi_j(\alpha)$ and $\varphi_i(\beta) = \varphi_j(\beta)$. We know that every element of $K(\alpha, \beta)$ is a K-linear combination of products of powers of α and β. Since φ_i, φ_j are homomorphisms that fix K pointwise and $\varphi_i(\alpha) = \varphi_j(\alpha)$, $\varphi_i(\beta) = \varphi_j(\beta)$, this means $\varphi_i = \varphi_j$, contradicting that φ_i, φ_j are distinct.

(b) Since $f \neq 0$, f has finitely many roots in K. Since K is infinite, not every element of K can be a root of f, so there is some $\delta \in K$ so that $f(\delta) \neq 0$.

(c) Suppose there are s, t with$1 \leq s, t \leq r$, $s \neq t$ and $\varphi_s(\gamma) = \varphi_t(\gamma)$. Then

$$\big(\varphi_s(\alpha) - \varphi_t(\alpha)\big) + \big(\varphi_s(\beta) - \varphi_t(\beta)\big)\delta = \varphi_s(\alpha + \beta)\delta - \varphi_t(\alpha + \beta)\delta$$

and so

$$f(\gamma) = f(\alpha + \beta\delta) = \prod_{i \neq j} \big((\varphi_i(\alpha) - \varphi_j(\alpha)) + (\varphi_i(\beta) - \varphi_j(\beta))\delta\big) \neq 0.$$