GALOIS THEORY: SOLUTIONS TO HOMEWORK 10

1. Let $f \in K[t] \setminus K$, and let $L : K$ be a splitting field extension for f. Assume that $K \subseteq L$.
   (a) Show that when f has a repeated root over L, then there exists $\alpha \in L$ for which $f(\alpha) = 0 = (Df)(\alpha)$.
   Solution: The situation with f is reducible simplifies to the case that f is irreducible, so we may suppose that f is irreducible with a repeated root $\alpha \in L$. Then $f = (t-\alpha)^k g$ for some $k > 1$ and $g \in L[t]$. Hence $Df = k(t-\alpha)^{k-1}g + (t-\alpha)^k Dg$, whence $(Df)(\alpha) = 0$ and $f(\alpha) = 0$.
   (b) Show that when $\alpha \in L$ satisfies $f(\alpha) = 0 = (Df)(\alpha)$, then there exists $g \in K[t]$ having the property that $\deg g \geq 1$ and g divides both f and Df.
   Solution: Suppose that there exists $\alpha \in L$ such that $f(\alpha) = (Df)(\alpha) = 0$. Then $m_\alpha(K)|f$ and $m_\alpha(K)|Df$, and so the conclusion holds with $g = m_\alpha(K)$.
   (c) Show that when $g \in K[t] \setminus K$ divides both f and Df, then f has a repeated root over L.
   Solution: Suppose that there exists $g \in K[t]$ such that $\deg g \geq 1$, having the property that $g|f$ and $g|Df$. One therefore has $f = gh$ for some $h \in K[t]$. Since f splits over L, then so does g. Let α be a root of g in L. Then $f = (t-\alpha)q$, for some $q \in L[t]$, and hence $Df = q + (t-\alpha)Dq$. But $(t-\alpha)|Df$ in $L[t]$, since $g|Df$, and so $(t-\alpha)|q$. Thus $(t-\alpha)^2|f$, and so f has a repeated root in L.
2. Suppose that $\mathrm{char}(K) = p > 0$ and f is irreducible over $K[t]$.
   (a) Show that there is an irreducible and separable polynomial $g \in K[t]$ and a non-negative integer n with the property that $f(t) = g(t^{p^n})$.
   Solution: Let n be the largest non-negative integer having the property that $f(t) \in K[t^{p^n}]$. Thus, there exists a polynomial $g \in K[t]$ having the property that $f(t) = g(t^{p^n})$. It follows from Theorem 8.2 that if g is inseparable, then $g \in K[t^p]$, which implies that $f \in K[t^{p^{n+1}}]$, contradicting the maximality of n. It follows that g is separable, and its irreducibility is an immediate consequence of that of f.
   (b) Let $L : K$ be a splitting field extension for f. Show that there exists a non-negative integer n with the property that every root of f in L has multiplicity p^n.
   Solution: From part (a) we see that $f(t) = g(t^{p^n})$ for some non-negative integer n and an irreducible separable polynomial $g \in K[t]$. Since g is separable, there exist distinct roots $\beta_1, \ldots, \beta_d \in \overline{K}$ having the property that $g(t) = (t-\beta_1)\cdots(t-\beta_d)$. Hence $f(t) = (t^{p^n} - \beta_1)\cdots(t^{p^n} - \beta_d)$. Writing $\alpha_i = \beta_i^{1/p^n} \in \overline{K}$ for $1 \leq i \leq d$, we see that the α_i are distinct elements of $\overline{K}$, and moreover a splitting field extension for f is $L : K$, where $L = K(\alpha_1, \ldots, \alpha_d)$, since we have
   $$f(t) = (t-\alpha_1)^{p^n} \cdots (t-\alpha_d)^{p^n}.$$
   Thus every root of f in L has multiplicity p^n for some non-negative integer n.