GALOIS THEORY 2019: Bonus Exercise for Section 8

Here you complete the proof of Theorem 8.7. Assume that K is a field with $\mathrm{char}K = p > 0$,

$$f = a_0 + a_1 t^p + \cdots + a_n t^{np}$$

where $a_0, \ldots, a_n \in K$ with $n \geq 1$ and $a_n = 1$. Set $g = a_0 + a_1 t + \cdots + a_n t^n$.

(a) Suppose that $f = h_1 h_2$ where $h_1, h_2 \in K[t] \setminus K$ are monic, and $\lambda_1, \lambda_2 \in K[t]$ so that $\lambda_1 h_1 + \lambda_2 h_2 = 1$. [We can choose such $h_1, h_2, \lambda_1, \lambda_2$ when f has at least two distinct irreducible factors in $K[t]$.]

(i) Use that $0 = Df = D(h_1 h_2)$ and that $Dh_1 = (Dh_1)(\lambda_1 h_1 + \lambda_2 h_2$ to deduce that h_1 divides Dh_1, and conclude that $Dh_1 = 0$.

(ii) Suppose that $Dh_1 = 0 = Dh_2$. Show that g is reducible in $K[t]$.

(b) Suppose that $f = f_1^m$ where f_1 is a monic, irreducible element of $K[t]$ and $m > 1$.

(i) Suppose that $p|m$. Show that all coefficients of f are powers of p.

(ii) Suppose that $p \nmid m$. Show that $Df_1 = 0$, and deduce that $g = g_1^m$ for some $g_1 \in K[t] \setminus K$.

Solutions:

(a)(i) We have $0 = Df = D(h_1 h_2) = (Dh_1)h_2 + h_1(Dh_2)$, so $(Dh_1)h_2 = -h_1(Dh_2)$. Hence

$$Dh_1 = (Dh_1)(\lambda_1 h_1 + \lambda_2 h_2) = \lambda_1 (Dh_1) h_1 - \lambda_2 (Dh_2) h_1.$$

If $Dh_1 \neq 0$ then $\deg Dh_1 < \deg h_1$; but the above computation shows that h_1 divides Dh_1. So we must have $Dh_1 = 0$.

(a)(ii) Since $Dh_1 = 0 = Dh_2$, we know that $h_1 = c_0 + c_1 t^p + \cdots + c_j t^{jp}$ and $h_2 = d_0 + d_1 t^p + \cdots + d_k t^{kp}$ for some $j, k \in \mathbb{Z}_+$ and $c_0, \ldots, c_j, d_0, \ldots, d_k \in K$ with $c_j = d_k = 1$. Since $g(t^p) = f(t) = h_1 h_2$, we have

$$g(t) = (c_0 + c_1 t + \cdots + c_j t^j)(d_0 + d_1 t + \cdots + d_k t^k)$$

and since $c + j = 1 = d_k$, this shows that g is reducible in $K[t]$.

(b)(i) Suppose that $p|m$; set $h_1 = (f_1)^{m/p}$. Note that h_1 is monic, and h_1 cannot be constant as $f = h_1^p$ is not constant. Write $h_1 = c_0 + c_1 t + \cdots + c_k t^k$, some $k \in \mathbb{Z}_+$ and $c_0, \ldots, c_k \in K$ with $c_k = 1$. Then

$$f = (c_0 + c_1 t + \cdots + c_k t^k)^p = c_0^p + c_1^p t^p + \cdots + c_k^p t^{kp},$$

showing that all coefficients of f are powers of p.

(b)(ii) Suppose that $p \nmid m$. We have

$$0 = Df = m(Df_1)f_1;$$

as $m \neq 0$ in K and $f_1 \neq 0$ in $K[t]$, we must have $Df_1 = 0$ [recall that $K[t]$ is an integral domain, so it has no zero divisors]. Thus for some $d_0, \ldots, d_k \in K$ with $k \geq 1$ and $d_k = 1$, we have

$$f_1 = d_0 + d_1 t^p + \cdots + d_k t^{kp} = g_1(t^p)$$

where $g_1 \in K[t] \setminus K$. As $g(t^p) = f = f_1^m = (g_1(t^p))^m$, we have $g(t) = (g(t))^m$. Since $m > 1$, this shows that $g = g(t)$ is reducible in $K[t]$.