A note on separable polynomials

Bassel Mannaa

February 10, 2013

Fact 0.1. *For a field K, let $p, q \in K[X]$. We can find $r, s, g, p_1, q_1 \in K[X]$ such that $p = p_1 g, q = q_1 g, rp_1 + sq_1 = 1$. We call g the greatest common divisor (gcd) of f and q, we write $g = \langle f, q \rangle$.*

Definition 0.2 (Separable associate)**.** *Let K be a field. Let $f \in K[X]$ be a nonzero polynomial of degree n and f' the derivative of f. The* separable associate *of f is* the *-unique up to polynomial equivalence- polynomial h such that $f = hg, f' = qg$ where $g = \langle f, f' \rangle$.*

The following two propositions are usually proved with the assumption of existence of a factorization algorithm (equivalently, an irreducibility test) of polynomials over a field. We give a proof without this assumption.

Proposition 0.3. *Let K be a field of characteristic 0 and $f \in K[X]$ a nonzero polynomial. Let h be the separable associate of f. Then $f \mid h^n$.*

Proof. Let $g = \langle f, f' \rangle$, thus $f = hg$. We prove $f \mid h^n$ by induction on the degree of g. Let degree of g be 0. Then if $deg(f) = 0$ we get $f \mid h^0 = 1$. Otherwise, $f \mid h$. Assuming the statement is true for $deg(g) \leqslant m$. Now Let $f = hg, h' = qg, rh + sq = 1$ and degree of g is $m+1$. Let g' be the derivative of g we can find $l_1, l_2, d, , r_1, r_2$ such that $g = l_1 d, g' = l_2 d, r_1 l_1 + r_2 l_2 = 1$. Since $deg(d) < deg(g) = m + 1$, then by induction hypothesis we get that $g \mid l_1^{m+1}$. Let $ge = l_1^{m+1}$. We have $f' = qg = h'g + hg'$, substituting we get $h' l_1 d + h l_2 d = q l_1 d$. We know that $d \neq 0$, hence $h' l_1 + h l_2 = q l_1$. From this and $r_1 l_1 + r_2 l_2 = 1$ we get $r_2 h' l_1 + h - h r_1 l_1 = r_2 q l_1$. Thus $l_1(r_2 q + h r_1 - r_2 h') = l_1 c = h$. Now $f = hg$ then $f e c^{m+1} = h(ge)c^{m+1} = h l_1^{m+1} c^{m+1} = h^{m+2}$. □

Proposition 0.4. *Let K be a field of any characteristic. The separable associate of a polynomial over $K[X]$ is separable.*

Proof. Let $f \in K[X]$ a nonzero polynomial. Let $g = \langle f, f' \rangle$ and h the separable associate of f. We show that if $\langle h, h' \rangle = 1$. By fact 0.1 we can

find $r_1, r_2, a, l_1, l_2, r3, r_4, d, l_3, l_4$ such that $h = l_1 a, h' = l_2 a, r_1 l_1 + r_2 l_2 = 1, a = l_3 d, a' = l_4 d, r_3 l_3 + r_4 l_4 = 1$. We now prove that for $n \in \mathbb{N}$, if $a^{n+1} \mid g$ then $a^{n+2} \mid g$. Let $g = m a^{n+1}$ then $g' = m' a^{n+1} + (n+1) m a^n a' = m' a^n l_3 d + (n+1) m a^n l_4 d$ and $a^n d \mid g'$. Let $g' = a^n dy$. We have $h' = l_2 l_3 d = l_1' l_3 d + l_1 l_4 d$ if we multiply both sides by r_4 and substitute for $r_4 l_4 = 1 - r_3 l_3$ we get $l_3 d(r_4 l_2 - r_4 l_1' + r_3 l_1) = l_1 d$. Multiplying by l_3 we get $a l_3 (r_4 l_2 - r_4 l_1' + r_3 l_1) = h$. Let $z = (r_4 l_2 - r_4 l_1' + r_3 l_1)$ and we have $h = a l_3 z$. Hence, $hg' = (a l_3 z)(a^n dy) = a^{n+2} yz$ and we already have $h' g = l_2 m a^{n+2}$. Multiply $h' g + h g' = qg$ by s we get $s h' g + s h g' = g - grh$. Hence, $g = a^{n+2}(s l_2 m + syz + rml_1)$ and the statement is proven.

It is easy to prove that $a \mid g$ because we have $g = s h' g + s h g' + grh = a(s l_2 g + s l_1 g' + gr l_1)$. So now we have that $\forall n \in \mathbb{N}.\ a^n \mid g$. Hence, a is a unit and we choose $t = r_1 a^{-1}, r = r_2 a^{-1}$ to get $th + rh' = 1$. $\square$