special reducible polynomials over a field with positive characteristic

Canonical name	SpecialReduciblePolynomialsOverAFieldWithPositiveCharacteristic
Date of creation	2013-03-22 18:31:05
Last modified on	2013-03-22 18:31:05
Owner	joking (16130)
Last modified by	joking (16130)
Numerical id	10
Author	joking (16130)
Entry type	Theorem
Classification	msc 13F07

Let k be an arbitrary field such that $\mathrm{char}(k) = p > 0$. We will assume that $0 \notin \mathbb{N}$.

Proposition. Let $m \in \mathbb{N}$. Then for any $a \in k$ the polynomial $W(X) = X^{p^m} - a$ is reducible if and only if there exist $c \in k$ and $n \in \mathbb{N}$ such that $c^{p^n} = a$. Moreover the factorization of $W(X)$ is given by the formula

$$W(X) = (X^{p^{m-n}} - c)^{p^n},$$

where n is a maximal natural number such that $0 \leq n \leq m$ and $a = c^{p^n}$ for some $c \in k$.

Proof. "$\Leftarrow$" Assume that $a = c^{p^n}$ for some $c \in k$ and $n \in \mathbb{N}$. It is well known that if $\mathrm{char}(k) = p > 0$ and $t \in \mathbb{N}$ then for any $x, y \in k$ we have $(x+y)^{p^t} = x^{p^t} + y^{p^t}$. Therefore

$$W(X) = X^{p^m} - a = X^{p^m} - c^{p^n} = (X^{p^{m-1}})^p - (c^{p^{n-1}})^p = (X^{p^{m-1}} - c^{p^{n-1}})^p = (V(X))^p.$$

Note that $p^m > \deg(V(X)) = p^{m-1} > 0$ and therefore $W(X)$ is reducible. $\square$

"$\Rightarrow$" Assume that $W(X)$ is reducible. Therefore there exist $V(X), U(X) \in k[X]$ such that $W(X) = V(X) \cdot U(X)$ and both $\deg(V(X)) > 0$ and $\deg(U(X)) > 0$.

Recall that there exists an algebraically closed field $\overline{k}$ such that k is a subfield of $\overline{k}$ (generally it is true for any field). Therefore there exists $c_0 \in \overline{k}$ such that $c_0^{p^m} = a$ and thus we have:

$$W(X) = X^{p^m} - a = X^{p^m} - c_0^{p^m} = (X - c_0)^{p^m}$$

in $\overline{k}[X]$. Now $V(X) \cdot U(X) = W(X) = (X - c_0)^{p^m}$ and since $\overline{k}[X]$ is a unique factorization domain then for $n = \deg(V(X)) > 0$ we have:

$$V(X) = (X - c_0)^n.$$

But $V(X) \in k[X]$ (the factorization was assumed to be over k) and therefore $c_0^n \in k$. It is easy to see that since $c_0^n \in k$ and $c_0^{p^m} \in k$ then $c_0^{\gcd(n,p^m)} \in k$, but $\gcd(n, p^m) = p^s$ for some $s \in \mathbb{N}$. Thus if we put $c = c_0^{p^s}$ we gain that $c^{p^{m-s}} = a$. But $m > s$ (since $n < p^m$ because we assumed that both $\deg(V(X)) > 0$ and $\deg(U(X)) > 0$), which completes the proof of the first part. $\square$

Now let $n \in \mathbb{N}$ be a maximal natural number such that $n \leq m$ and $a = c^{p^n}$ for some $c \in k$. Then we have

$$W(X) = (X^{p^{m-n}} - c)^{p^n}.$$

Note that the polynomial $X^{p^{m-n}} - c$ is irreducible. Indeed, assume that $X^{p^{m-n}} - c$ is reducible. Then (due to first part of the proposition) $c = u^{p^k}$ for some $k \in \mathbb{N}$ and $u \in k$. But then $a = (u^{p^k})^{p^n} = u^{p^{n+k}}$. Contradiction, since $n + k > n$ and n was assumed to be maximal. $\square$