Internat. J. Math. & Math. Sci.
Vol. 23, No. 11 (2000) 777–781
S0161171200002830

ON THE DECOMPOSITION OF $x^d + a_e x^e + \cdots + a_1 x + a_0$

JAVIER GOMEZ-CALDERON

(Received 9 July 1998 and in revised form 28 March 1999)

Abstract. Let K denote a field. A polynomial $f(x) \in K[x]$ is said to be decomposable over K if $f(x) = g(h(x))$ for some polynomials $g(x)$ and $h(x) \in K[x]$ with $1 < \deg(h) < \deg(f)$. Otherwise $f(x)$ is called indecomposable. If $f(x) = g(x^m)$ with $m > 1$, then $f(x)$ is said to be trivially decomposable. In this paper, we show that $x^d + ax + b$ is indecomposable and that if e denotes the largest proper divisor of d, then $x^d + a_{d-e-1}x^{d-e-1} + \cdots + a_1 x + a_0$ is either indecomposable or trivially decomposable. We also show that if $g_d(x,a)$ denotes the Dickson polynomial of degree d and parameter a and $g_d(x,a) = f(h(x))$, then $f(x) = g_t(x-c,a)$ and $h(x) = g_e(x,a)+c$

Keywords and phrases. Polynomials and fields.

2000 Mathematics Subject Classification. Primary 11T06.

Let K denote a field. A polynomial $f(x) \in K[x]$ is said to be *decomposable* over K if

$$f(x) = g(h(x)) \tag{1}$$

for some polynomials $g(x)$ and $h(x) \in K[x]$ with $1 < \deg(h(x)) < \deg(f(x))$. Otherwise $f(x)$ is called *indecomposable*.

Examples. (a) $f(x) = x^{mn}$, m and $n > 1$, is decomposable because $f(x) = g(h(x))$ where $h(x) = x^m + c$ and $g(x) = (x-c)^n$.

(b) $f(x) = x^p$, p a prime, is indecomposable because p does not have proper divisors.

(c) $f(x) = \sum_{i=0}^{n} a_i x^{mi}$ is decomposable because $f(x) = g(h(x))$ where $h(x) = x^m$ and $g(x) = \sum_{i=0}^{n} a_i x^i$.

Decompositions such as the one given in (c) are trivial and consequently we say that $f(x)$ is *trivially decomposable* if $f(x) = g(x^m)$ for some polynomial $g(x)$ with $m > 1$.

In this paper, we show that $x^d + ax + b$ is indecomposable and that if e denotes the largest proper divisor of d, then $x^d + a_{d-e-1}x^{d-e-1} + \cdots + a_1 x + a_0$ is either indecomposable or trivially decomposable. We will also show that if $g_d(x,a)$ denotes the Dickson polynomial of degree d and parameter a and $g_d(x,a) = f(h(x))$, then $f(x) = g_t(x-c,a)$ and $h(x) = g_e(x,a)+c$. More precisely, we prove the following.

Theorem 1. *Let K be a field. Let d be a positive integer. If K has a positive characteristic p, assume that $(d,p) = 1$.*

(a) $x^d + ax + b$, $a \neq 0$, is decomposable.

(b) If e denotes the largest proper divisor of d, then $x^d + a_{d-e-1}x^{d-e-1} + \cdots + a_1 x + a_0$ is either indecomposable or trivially decomposable.

(c) If $x^d = f(h(x))$ for some polynomials $f(x)$ and $h(x)$ in $K[x]$, then $f(x) = (x-c)^t$ and $h(x) = x^e + c$ for some $c \in K$ and $d = et$.

(d) If $g_d(x,a)$ denotes the Dickson polynomial of degree d and parameter a and $g_d(x,a) = f(h(x))$, then $f(x) = g_t(x-c,a)$ and $h(x) = g_e(x,a)+c$ for some $c \in K$.

The proof of the theorem need the following lemmas.

Lemma 2. *Let $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$ denote a monic polynomial over a field K. If K has a positive characteristic p, assume that $(p,d) = 1$. Let the irreducible factorization of $f(x)-f(y)$ be given by*

$$f(x)-f(y) = \prod_{i=1}^{s} f_i(x,y) \tag{2}$$

Let

$$f_i(x,y) = \sum_{j=0}^{n_i} g_{ij}(x,y) \tag{3}$$

be the homogeneous decomposition of $f_i(x,y)$ so that $n_i = \deg(f_i(x,y))$ and $g_{ij}(x,y)$ is homogeneous of degree j. Assume $a_{d-1} = a_{d-2} = \cdots = a_{d-r} = 0$ for some $r \geq 1$. Then,

$$g_{i,n_i-1}(x,y) = g_{i,n_i-2}(x,y) = \cdots = g_{i,R_i}(x,y) = 0 \tag{4}$$

where

$$R_i = \begin{cases} n_i - r & \text{if } n_i \geq r_i \\ 0 & \text{if } n_i < r_i \end{cases} \tag{5}$$

Proof. Let e_i denote the second highest degree of $f_i(x,y)$ defined by

$$e_i = \begin{cases} \deg\left(f_i(x,y) - g_{i,n_i}(x,y)\right) & \text{if } f_i(x,y) \neq g_{i,n_i}(x,y) \\ -\infty & \text{if } f_i(x,y) = g_{i,n_i}(x,y) \end{cases} \tag{6}$$

Assume, without loss of generality, that $n_1 - e_1 \leq n_2 - e_2 \leq \cdots \leq n_s - e_s$. Let b denote the largest integer i such that $N = n_1 - e_1 = n_2 - e_2 = \cdots = n_i - e_i$. Our goal is to show that $N > r$. So, assume that N is finite. Hence, $g_{i,e_i}(x,y) \neq 0$ for all i, $1 \leq i \leq b$ and

$$a_{d-N}\left(x^{d-N} - y^{d-N}\right) = \sum_{i=1}^{b} g_{i,e_i}(x,y) \prod_{\substack{j=1 \\ j \neq i}}^{s} g_{j,n_j}(x,y) \tag{7}$$

On the other hand, we have

$$x^d - y^d = \prod_{i=1}^{s} g_{i,n_i}(x,y) \tag{8}$$

Therefore,

$$a_{d-N}\frac{x^{d-N} - y^{d-N}}{x^d - y^d} = \sum_{i=1}^{b} \frac{g_{i,e_i}(x,y)}{g_{i,n_i}(x,y)} \tag{9}$$

As $(d,p) = 1$, $x^d - y^d$ has no multiple divisors in the algebraic closure of K. So, the denominators in the right-hand side of the above formula are relatively prime to each other, and if the denominator and numerator of each summand have a common factor, it can be canceled out. Hence, the right-hand side of (9) does not vanish. Thus, $a_{d-N} \neq 0$ and consequently $d - N < d - r$. Therefore, $N > r$ and the proof of the lemma is complete. □

Lemma 3. *Let $f(x)$ be a monic polynomial over a field K. If K has a positive characteristic p, assume that p does not divide the degree of $f(x)$. Let N denote the number of linear factors of $f(x) - f(y)$ over $\bar{\mathbf{K}}$, the algebraic closure of K. Then, there exists a constant b in K such that*

$$f(x) = g\big((x+b)^N\big) \tag{10}$$

for some polynomial $g(x) \in K[x]$.

Proof. Choose b in F such that $f(x-b) = F(x) = x^d + a_{d-2}x^{d-2} + \cdots + a_1 x + a_0$. Hence, by Lemma 2, all linear factors of $F(x) - F(y)$ have the form $x - a_i y$ for $i = 1, 2, \ldots, N$. Thus, $F(a_i x) = F(x)$ for all i, and consequently $F(a_i a_j x) = F(a_j x) = F(x)$ for all i and j. Therefore, $a_1, a_2, \ldots, a_N$ form a multiplicative cyclic group of order N and $\prod_{i=1}^{N}(x - a_i x) = x^N - y^N$.
Now write

$$F(x) = f_0(x) + f_1(x)x^N + f_2(x)x^{2N} + \cdots + f_m(x)x^{mN} \tag{11}$$

with $\deg(f_i(x)) < N$ for all i. This decomposition is clearly unique. Thus,

$$\begin{aligned} F(x) &= f_0(x) + f_1(x)x^N + f_2(x)x^{2N} + \cdots + f_m(x)x^{mN} \\ &= f_0(a_i x) + f_1(a_i x)(a_i x)^N + f_2(a_i x)(a_i x)^{2N} + \cdots + f_m(a_i x)(a_i x)^{mN} \\ &= f_0(a_i x) + f_1(a_i x)x^N + f_2(a_i x)x^{2N} + \cdots + f_m(a_i x)x^{mN} \end{aligned} \tag{12}$$

for $i = 1, 2, \ldots, N$ implies that $f_j(x) = c_j \in K$ for all $0 \le j \le m$.
Therefore,

$$F(x) = \sum_{i=0}^{m} c_i x^{Ni} = g(x^N) \tag{13}$$

where $g(x) = \sum_{i=0}^{m} c_i x^i \in K[x]$. This completes the proof of the lemma. □

Lemma 4. *Let d be a positive integer and assume that K contains a primitive nth root ζ of unity. Put*

$$B_k = \zeta^k + \zeta^{-k}, \qquad C_k = \zeta^k - \zeta^{-k}. \tag{14}$$

Then for each $a \in K$ we have

(a) *If $d = 2n+1$ is odd*

$$g_d(x,a) - g_d(y,a) = (x-y)\prod_{i=1}^{n}\left(x^2 - B_k xy + y^2 + aC_k^2\right) \tag{15}$$

(b) *If $d = 2n$ is even*

$$g_d(x,a) - g_d(y,a) = (x^2 - y^2)\prod_{i=1}^{n-1}(x^2 - A_k xy + y^2 + aC_k^2) \tag{16}$$

Moreover for $a \neq 0$ the quadratic factors are different from each other and are irreducible in $K[x,y]$.

Proof. See [1, page 46]. □

Proof of the theorem. (a) Assume $x^d + ax + b = f(h(x))$ with $1 < \deg(h(x)) < d$ and $a \neq 0$. Let $\bar{\mathbf{K}}$ denote the algebraic closure of K. Let the irreducible factorization of $f(x) - f(y)$ over $\bar{\mathbf{K}}$ be given by

$$f(x) - f(y) = (x - y)\prod_{i=1}^{m} G_i(x,y). \tag{17}$$

Then,

$$x^d + ax - y^d - ay = (h(x) - h(y))\prod_{i=1}^{m} G_i(h(x),h(y)) = \prod_{i=1}^{r} f_i(x,y) \tag{18}$$

for some irreducible polynomials $f_i(x,y) \in \bar{\mathbf{K}}[x,y]$ with $\deg(f_i(x,y)) \leq d-2$ for $1 \leq i \leq r$. Hence, applying Lemma 2, each of the factors $f_i(x,y)$ has a second highest degree of $-\infty$. Therefore, considering only the highest degree terms in (18),

$$x^d - y^d = \prod_{i=1}^{r} f_i(x,y) \tag{19}$$

and consequently $ax - ay = 0$. Since this is clearly a contradiction, then $h(x)$ has either degree 1 or d.

(b) Let e denotes the largest proper divisor of d. Assume that the polynomial $g_e(x) = x^d + a_{d-e-1}x^{d-e-1} + \cdots + a_1 x + a_0$ is decomposable. So, $g_e(x) = f(h(x))$ for some $h(x) \in K[x]$ with $1 < \deg(h(x)) \leq e$. Let the irreducible factorization of $f(x) - f(y)$ over $\bar{\mathbf{K}}$ be given by

$$f(x) - f(y) = (x - y)\prod_{i=1}^{r} f_i(x,y). \tag{20}$$

Then

$$g_e(x) - g_e(y) = (h(x) - h(y))\prod_{i=1}^{r} f_i(h(x),h(y)). \tag{21}$$

Hence, by Lemma 2, $h(x) - h(y)$ is homogeneous and consequently a factor of $x^d - y^d$. So, $h(x) - h(y)$ is a product of homogeneous linear factors and, by Lemma 3, $h(x) = x^m + c$ for some $c \in K$. Thus, $g_e(x) = f(x^m + c) = f_2(x^m)$ where $f_2(x) = f(x + c)$. Therefore, $g_e(x)$ is either indecomposable or trivially decomposable.

(c) If $x^d = f(h(x))$ then, we did this before,

$$\begin{aligned} x^d - y^d &= f(h(x)) - f(h(y)) \\ &= (h(x) - h(y)) \prod_{i=1}^{m} G_i(h(x), h(y)) = \prod_{i=0}^{d-1} (x - \zeta^i y) \end{aligned} \tag{22}$$

for some dth primitive root of unity ζ in $\mathbf{K}$. Thus, $h(x) = x^e + c$ for some $c \in K$ and $e \mid d$.

Therefore,

$$\begin{aligned} f(h(x)) - f(h(y)) = (x^e)^{d/e} - (y^e)^{d/e} &= \prod_{j=1}^{d/e} (x^e - \zeta^{ej} y^e) \\ &= \prod_{j=1}^{d/e} (h(x) - c - \zeta^{ej}(h(y) - c)) \end{aligned} \tag{23}$$

and $f(x) = (x - c)^{d/e}$.

(d) Similar to (c) using Lemma 4. $\square$

Acknowledgement. The author thanks the referee for his suggestions which improved the final version of the paper.

References

[1] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson Polynomials*, Longman Scientific & Technical, Harlow, 1993. MR 94i:11097. Zbl 823.11070.

Calderon: Department of Mathematics, New Kensington Campus, Pennsylvania State University, New Kensington, PA, 15068, USA