

On Composite Polynomials

Mohamed Ayad and Nidal Ali

Université du Littoral Côte d'Opale
50 rue F. Buisson, F-62228 Calais Cedex, France
ayad@lmpa.univ-littoral.fr
nidal@lmpa.univ-littoral.fr

Abstract

Let K be a field of characteristic $p \geq 0$. Let $f(x_1, \dots, x_\ell) \in K[x_1, \dots, x_\ell]$ such that $\frac{\partial f}{\partial x_\ell} \neq 0$. There exists at most one polynomial $P(x_1, \dots, x_{\ell-1}) \in K[x_1, \dots, x_{\ell-1}]$ such that $f(x_1, \dots, x_\ell) + P(x_1, \dots, x_{\ell-1})$ is composite and satisfying the conditions $P(0) = 0$ and $\frac{\partial P}{\partial x_i} \neq 0$ for some $i \in \{1, \dots, \ell - 1\}$ if $p > 0$. Furthermore, the use of Kronecker substitution brings back the problem to that of the composition of one polynomial in one variable. Therefore, we obtain necessary and (or) sufficient conditions for a multivariate polynomial to be composite.

Mathematics Subject Classification: 11C, 12Y05

Keywords: Composite polynomial, Kronecker's substitution, Jacobian derivation

1 Introduction

Let K be a field and let $f(x_1, \dots, x_\ell)$ be a non-constant polynomial over K . We say that f is composite over K if there exist two polynomials $u(t)$, $h(x_1, \dots, x_\ell)$ defined over K such that $\deg u \geq 2$ and $f(x_1, \dots, x_\ell) = u(h(x_1, \dots, x_\ell))$.

Let \overline{K} be an algebraic closure of K . Following the method of [1], one can prove that if K is of characteristic 0 then f is composite over K if and only if f is composite over \overline{K} .

The compositeness of polynomials is related to the reducibility by the following classical result.

Theorem 1 (*Bertini*) *Suppose that K is algebraically closed and let $f(x_1, \dots, x_\ell)$ be a non-constant polynomial over K . Then f is composite over K if and only if there exist infinitely many values of $\lambda \in K$ such that $f(x_1, \dots, x_\ell) - \lambda$ is reducible over K .*

Proof. See [4 chap. 3 §3 cor. 1].

Using Theorems 3 and 4 of [4 chap. 1 §2], one can prove that, if $f(x_1, \dots, x_\ell)$ is a polynomial over K and $f = u_1(h_1) = u_2(h_2)$, where h_1, h_2 are non-composite, then $h_1 = u(h_2)$ with $u(t) = at + b$, $a \in K^*$, $b \in K$, so the decomposition of f is unique up to a linear transformation over K .

When $f(x_1, \dots, x_\ell)$ is non-composite, the finite set of values of λ in K such that $f(x_1, \dots, x_\ell) - \lambda$ is reducible over K is called the spectrum of f . In [2], one can find an explicit method to detect if a bivariate polynomial is composite and if not to find explicitly the spectrum of f .

In order to apply Theorem 1, it is necessary to decide whether f is composite or not. Theorem 3 below, transfers the property of being composite for a multivariate polynomial to the same property for some univariate polynomial.

The second interest to detect if given a multivariate polynomial is composite is useful when factorizing this polynomial. Suppose that $f(x_1, \dots, x_\ell)$ is composite over K , $f = u(h(x_1, \dots, x_\ell))$ then $f(x_1, \dots, x_\ell) = (h - \alpha_1) \dots (h - \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the roots of u in an algebraic closure of K . Hence to factorize $f(x_1, \dots, x_\ell)$ over \overline{K} , one has to factorize the polynomials $h(x_1, \dots, x_\ell) - \alpha_i$ which are of smaller degree.

One other application of the compositeness is related to the jacobian derivation. Let K be a field, $f(x, y)$ be a polynomial over K . Let

$$d : K[x, y] \longrightarrow K[x, y]$$

be the derivation defined by

$$d(g) = \begin{vmatrix} \frac{\partial f}{\partial x} & \frac{\partial g}{\partial x} \\ \frac{\partial f}{\partial y} & \frac{\partial g}{\partial y} \end{vmatrix}$$

and let \overline{d} be its extension to $K(x, y)$ then it is known that there exists $h(x, y) \in K[x, y]$, non composite such that $\text{Ker}(d) = K[h]$ ([3] or [5]), and $\text{Ker}(\overline{d}) = K(h)$ ([5]). Since $f \in \text{Ker}(d)$ then there exists $u(t) \in K[t]$ such that $f = u(h)$.

Now we give the last application, let K be a field, $\{x_1, \dots, x_n\}$ be elements algebraically independent over K and let $E = K(\psi_1, \dots, \psi_r)$ where $\psi_1, \dots, \psi_r \in K[x_1, \dots, x_n]$. Suppose that $\text{trdeg} E/K = 1$ then it is known ([4], chap. 1 §2, thm 3 and 4) that there exists $h \in E$ such that $E = K(h)$. Consequently, for each $i = 1, \dots, r$, ψ_i is composite or it generates E .

Let $f(x_1, \dots, x_\ell)$ be a polynomial over K and let $c \in K$, then it is clear that f is composite over K if and only if $f + c$ is composite. In section 2, we fix a polynomial $f(x_1, \dots, x_\ell)$ such that $\deg_{x_\ell} f \geq 1$ and we ask for the compositeness of $f(x_1, \dots, x_\ell) + P(x_1, \dots, x_{\ell-1})$ where $P(x_1, \dots, x_{\ell-1}) \in K[x_1, \dots, x_{\ell-1}]$. In view of the preceding remark, we may suppose that $P(0) = 0$. We will prove the following result:

Theorem 2a Let $\ell \geq 2$ be an integer, K be a field of characteristic $p \geq 0$ and let $f(x_1, \dots, x_\ell)$ be a polynomial over K such that $\frac{\partial f}{\partial x_\ell} \neq 0$. There exists at most one polynomial $P(x_1, \dots, x_{\ell-1}) \in K[x_1, \dots, x_{\ell-1}]$ such that $f(x_1, \dots, x_\ell) + P(x_1, \dots, x_{\ell-1})$ is composite, satisfying $P(0) = 0$ and $\frac{\partial P}{\partial x_i} \neq 0$ for some $i \in \{1, \dots, \ell - 1\}$ if $p > 0$.

Theorem 2a can be reformulated as

Theorem 2b Keep the hypotheses of Theorem 2a and suppose that f is composite over K . Then for every $P(x_1, \dots, x_{\ell-1}) \in K[x_1, \dots, x_{\ell-1}]$ such that $\frac{\partial P}{\partial x_i} \neq 0$ for some $i \in \{1, \dots, \ell - 1\}$ if $p > 0$, $f + P$ is composite if and only if P is constant.

We omit the simple proof that Theorems 2a and 2b are equivalent.

In the following two theorems, we give necessary and sufficient conditions for a multivariate polynomial to be composite. Let K be a field, d be a positive integer and $f(x_1, \dots, x_\ell)$ be a polynomial over K for which $\deg_{x_i} f < d$ for every $i = 1, \dots, \ell - 1$, then

$$S_d : f \mapsto f(x, x^d, \dots, x^{d^{\ell-1}})$$

is called Kronecker substitution. Before stating the main result of that section, we note that a univariate polynomial $f(x) \in K[x]$ of degree at least 2 is always trivially composite. So we make the following definition. Let K be a field, the polynomial $f(x) \in K[x]$ is said to be strictly composite if there exist two polynomials over K , $u(x), g(x)$ both of them of degree at least two such that $f(x) = u(g(x))$. It is clear that if $f(x_1, \dots, x_\ell)$ is composite then $S_d(f)$ is strictly composite. The converse is false as it is shown by the following counter-example:

$$f(x_1, x_2) = x_1x_2 + 1$$

where it is seen that f is non-composite but:

$$f(x, x^3) = x^4 + 1 = u(x^2)$$

with $u(x) = x^2 + 1$, hence $f(x, x^3)$ is strictly composite. Notice that $f(x, x^4)$ is not strictly composite. Theorem 3 shows that under some assumptions the converse is true.

Theorem 3 Let K be a field, $f(x_1, \dots, x_\ell)$ be a polynomial over K depending at least on two variables and let d be an integer such that:

$$\max_{1 \leq i \leq \ell-1} \{\deg_{x_i} f\} < d.$$

Then f is composite over K if and only if $S_d(f)$ is strictly composite over K :

$$S_d(f) = u_d(h_d(x))$$

where $u_d(x)$ and $h_d(x)$ are polynomials over K of degree at least 2, and the polynomial $h_d(x) = \sum_{j=1}^s b_{i_j} x^{i_j}$ is such that the expansion in base d of each i_j takes the form:

$$i_j = c_0(i_j) + c_1(i_j)d + \dots + c_{\ell-1}(i_j)d^{\ell-1}$$

with $0 \leq c_k(i_j) \leq d - 1$ for $k = 0, \dots, \ell - 2$, and $c_k(i_j) < d/\deg u_d$ for $k = 0, \dots, \ell - 2$.

One could believe that if $S_d(f)$ is strictly composite over K for all large d , then f is composite, but this claim is not true. Consider for example the polynomial:

$$f(x_1, \dots, x_\ell) = x_1^2 + \dots + x_\ell^2$$

Then

$$f(x, x^d, \dots, x^{d^{\ell-1}}) = x^2 + x^{2d} + \dots + x^{2d^{\ell-1}} = u_d(x^2)$$

where $u_d(t) = t^{d^{\ell-1}} + \dots + t^d + t$, hence $S_d(f)$ is strictly composite for all $d \geq 2$, although f is not composite over any field of characteristic not equal to 2. Even if we suppose that for all large d , $S_d(f)$ is strictly composite over K and decomposes in the form $S_d(f)(x) = u(g_d(x))$, where u and g_d are polynomials over K of degree at least 2 and u is independent of d , we cannot deduce that f is composite. For instance, let $\ell \geq 3$ and

$$A(t) = t(t + 1) \dots (t + \ell - 2) = t^{\ell-1} + a_{\ell-2}t^{\ell-2} + \dots + a_1t$$

and consider:

$$f(x_1, \dots, x_\ell) = x_1^{(\ell-1)a} x_2^{a_1} x_3^{a_2} \dots x_{\ell-1}^{a_{\ell-2}} x_\ell,$$

where a is a non negative integer. Then:

$$S_d(f) = x^{(\ell-1)a+A(d)} = [x^{a+A(d)/(\ell-1)!}]^{(\ell-1)!}$$

hence $S_d(f)$ is strictly composite for all $d \geq 2$ and decomposes in the form $S_d(f)(x) = u(g_d(x))$ where the polynomial $u(t) = t^{(\ell-1)!}$ is independent of d . Suppose now that $\ell = 2$ and let

$$f(x, y) = A_0(x)y^n + A_1(x)y^{n-1} + \dots + A_n(x)$$

be a polynomial over K . The next theorem shows that the claim hereafter is true if $A_0(x) \in K^*$:

Claim If there exists an integer $m \geq 2$ such that, for all large d , $S_d(f)$ is strictly composite, and can be decomposed in the form $f(x, x^d) = u_d(g_d(x))$ where u_d is a polynomial of degree m , then $f(x, y)$ is composite.

Theorem 4 Let K be a field and let $f(x, y)$ be a polynomial over K of the form:

$$f(x, y) = a_0y^n + A_1(x)y^{n-1} + \dots + A_n(x) \tag{1}$$

where $a_0 \in K^*$ and $A_i(x) \in K[x]$ for $i = 1, \dots, n$. Suppose that there exists some positive integer $d > \deg_x f$ such that $f(x, x^d)$ is strictly composite over K and takes the form:

$$f(x, x^d) = u(g(x)) \tag{2}$$

where u and g are polynomials defined over K , $\deg u = m$ and $\gcd(m, d) = 1$. Moreover, suppose that the characteristic of K is zero or prime to m and that one of the following cases holds.

- (i) $\frac{n}{m} < m$ and $\deg A_i(x) < \frac{d}{m}$, for $i = 1, \dots, \frac{n}{m}$.
- (ii) $\frac{n}{m} \geq m$ and $\deg A_i < \frac{id}{n}$ for $i = 1, \dots, \frac{n}{m}$.

Then $f(x, y)$ is composite over K .

Theorem 4 is not going to work out if we remove the condition on the characteristic of the field K . Indeed, consider the following counter examples, where the first one satisfies (i) and the second one (ii).

- (a) $K = \mathbb{F}_2$, $f(x, y) = y^2 + xy + 1$, $d = 3$, $f(x, x^3) = u(g(x))$ with $u(x) = x^2$ and $g(x) = x^3 + x^2 + 1$.
- (b) $K = \mathbb{F}_2$, $f(x, y) = y^4 + xy + 1$, $d = 3$, $f(x, x^3) = u(g(x))$ with $u(x) = x^2$ and $g(x) = x^6 + x^2 + 1$.

The authors believe that in the general case the claim preceding Theorem 4 may be formulated in the following:

Conjecture Let K be a field and let $f(x, y)$ be a polynomial over K ,

$$f(x, y) = A_0(x)y^n + A_1(x)y^{n-1} + \dots + A_n(x)$$

Suppose that there exist two large integers d_1, d_2 such that $S_{d_1}(f)$ and $S_{d_2}(f)$ are strictly composite over K and can be decomposed in the form $f(x, x^{d_i}) = u_i(g_i(x))$ for some polynomials u_1, g_1, u_2, g_2 defined over K , $\deg u_1 = \deg u_2 = m$, $m|d_1$ and $\gcd(m, d_2) = 1$. Suppose also that the characteristic of K is zero or prime to m , then $f(x, y)$ is composite over K .

2 Compositeness of $f(x_1, \dots, x_\ell) + P(x_1, \dots, x_{\ell-1})$

Proof of Theorem 2a. Suppose that there exists two polynomials $P_1(x_1, \dots, x_{\ell-1}), P_2(x_1, \dots, x_{\ell-1})$ over K such that $P_1 - P_2 \notin K$ and $f + P_1, f + P_2$ are composite over K . Set:

$$P_1(x_1, \dots, x_{\ell-1}) - P_2(x_1, \dots, x_{\ell-1}) = P(x_1, \dots, x_{\ell-1}) \tag{3}$$

$$f(x_1, \dots, x_\ell) + P_1(x_1, \dots, x_{\ell-1}) = u_1(h_1(x_1, \dots, x_\ell)) \tag{4}$$

$$f(x_1, \dots, x_\ell) + P_2(x_1, \dots, x_{\ell-1}) = u_2(h_2(x_1, \dots, x_\ell)) \tag{5}$$

where u_1, u_2, h_1, h_2 are polynomials defined over K , with $\deg u_1 \geq 2$ and $\deg u_2 \geq 2$. From (3), (4), (5) we deduce that

$$P(x_1, \dots, x_{\ell-1}) = u_1(h_1(x_1, \dots, x_\ell)) - u_2(h_2(x_1, \dots, x_\ell)) \tag{6}$$

Differentiating (6) with respect to each x_i we obtain the following system of ℓ linear equations where $u'_1(h_1), -u'_2(h_2)$ are the unknowns:

$$\begin{aligned} u'_1(h_1) \frac{\partial h_1}{\partial x_\ell} - u'_2(h_2) \frac{\partial h_2}{\partial x_\ell} &= 0 \\ u'_1(h_1) \frac{\partial h_1}{\partial x_1} - u'_2(h_2) \frac{\partial h_2}{\partial x_1} &= \frac{\partial P}{\partial x_1} \\ \dots & \\ u'_1(h_1) \frac{\partial h_1}{\partial x_{\ell-1}} - u'_2(h_2) \frac{\partial h_2}{\partial x_{\ell-1}} &= \frac{\partial P}{\partial x_{\ell-1}} \end{aligned} \tag{7}$$

Denote by $J(h_1, h_2)$ the matrix of this system, then $J(h_1, h_2)$ is the Jacobian matrix of (h_1, h_2) and:

$$J(h_1, h_2) = \begin{pmatrix} \frac{\partial h_1}{\partial x_\ell} & \frac{\partial h_2}{\partial x_\ell} \\ \frac{\partial h_1}{\partial x_1} & \frac{\partial h_2}{\partial x_1} \\ \dots & \dots \\ \frac{\partial h_1}{\partial x_{\ell-1}} & \frac{\partial h_2}{\partial x_{\ell-1}} \end{pmatrix} \tag{8}$$

Since $\frac{\partial f}{\partial x_\ell} \neq 0$, the first row of $J(h_1, h_2)$ is different from zero. Consequently, the rank of this matrix is equal to one or two. We distinguish two cases.

- (a) Suppose that $\text{rank } J(h_1, h_2) = 1$, then the non-zero vector $(0, \frac{\partial P}{\partial x_1}, \dots, \frac{\partial P}{\partial x_{\ell-1}})$ is proportional to $(\frac{\partial h_1}{\partial x_\ell}, \frac{\partial h_1}{\partial x_1}, \dots, \frac{\partial h_1}{\partial x_{\ell-1}})$ which implies $\frac{\partial h_1}{\partial x_\ell} = 0$. As a result, $f(x_1, \dots, x_\ell) \in K[x_1, \dots, x_{\ell-1}]$, hence we get a contradiction.

- (b) Suppose that $\text{rank } J(h_1, h_2) = 2$. For $i = 1, \dots, \ell$ put $V_i = (\frac{\partial h_1}{\partial x_i}, \frac{\partial h_2}{\partial x_i})$. Since $V_\ell \neq (0, 0)$ there exists $i \in \{1, \dots, \ell - 1\}$ such that V_ℓ and V_i are linearly independent over K , hence the determinant

$$D = \begin{vmatrix} \frac{\partial h_1}{\partial x_\ell} & \frac{\partial h_2}{\partial x_\ell} \\ \frac{\partial h_1}{\partial x_i} & \frac{\partial h_2}{\partial x_i} \end{vmatrix} \tag{9}$$

is non zero. Solving the system (7) we obtain:

$$D \cdot u'_1(h_1) = \begin{vmatrix} 0 & \frac{\partial h_2}{\partial x_\ell} \\ \frac{\partial P}{\partial x_i} & \frac{\partial h_2}{\partial x_i} \end{vmatrix} = -\frac{\partial P}{\partial x_i} \frac{\partial h_2}{\partial x_\ell} \tag{10}$$

$$-D \cdot u'_2(h_2) = \begin{vmatrix} \frac{\partial h_1}{\partial x_\ell} & 0 \\ \frac{\partial h_1}{\partial x_i} & \frac{\partial P}{\partial x_i} \end{vmatrix} = \frac{\partial P}{\partial x_i} \frac{\partial h_1}{\partial x_\ell} \tag{11}$$

Using (10) (resp. (11)) we will obtain the following inequality: $\deg_{x_\ell} h_2 > \deg_{x_\ell} h_1$ (resp $\deg_{x_\ell} h_1 > \deg_{x_\ell} h_2$). But these inequalities are contradictory, hence the second case is excluded and the proof of the theorem is complete. We now prove the above claims in the case $p > 0$, the case $p = 0$ is similar and simpler. Set

$$h_1 = a_1(x_1, \dots, x_{\ell-1}, x_\ell^p) + b_1(x_1, \dots, x_\ell)$$

and

$$h_2 = a_2(x_1, \dots, x_{\ell-1}, x_\ell^p) + b_2(x_1, \dots, x_\ell)$$

where $a_1, a_2 \in K[x_1, \dots, x_{\ell-1}, x_\ell^p]$ and $b_1, b_2 \in K[x_1, \dots, x_\ell] \setminus K[x_1, \dots, x_\ell^p]$ then by (10) we have $\deg_{x_\ell} b_2 - 1 = \deg u'_1 \cdot \deg_{x_\ell} h_1 + \deg D \geq \deg_{x_\ell} h_1$ so $\deg_{x_\ell} h_2 > \deg_{x_\ell} h_1$ and by (11), $\deg_{x_\ell} h_1 > \deg_{x_\ell} h_2$.

Remarks.

- (a) Theorem 2a is false if we remove the condition on the characteristic of the field K . Indeed, Let K be any field of characteristic $p > 0$, $f(x_1, x_2, x_3) = x_3^p$, $P_1(x_1, x_2) = x_1^p$, $P_2(x_1, x_2) = x_1^p + x_2^p$, then $f + P_1$ and $f + P_2$ are composite over K .
- (b) Theorem 2a no longer holds if we replace the word composite by the word reducible as it is shown by the following example: $f(x_1, x_2) = (x_1^2 + x_2^2)$, $P_1(x_1) = -x_1^2$ and $P_2(x_1) = -2x_1^2$. Here $f + P_1$ and $f + P_2$ are reducible.

Examples. Consider the set $K[x_1, \dots, x_\ell]/K[x_1, \dots, x_{\ell-1}]$. Theorem 2a implies that every non zero class of this set contains at most one polynomial $f(x_1, \dots, x_\ell)$ such that $f(0) = 0$ and f is composite over K . So the non trivial classes are of two types:

First type: class which contains exactly one element f such that $f(0) = 0$ and f is composite.

Second type: class such that no polynomial belonging to this class is composite. It is easy to construct representatives of classes of the first type. Here we give two examples of classes belonging to the second type.

- (a) Let $f(x_1, \dots, x_\ell)$ be a polynomial over K such that $\deg_{x_\ell} f = 1$, then it is clear that f represents a class of the second type.
- (b) Let q be a prime number, K be a field of characteristic $p \geq 0$ such that $(p, q) = 1$ if $p > 0$ and let

$$f(x_1, \dots, x_\ell) = x_\ell^q + a_{q-2}(x_1, \dots, x_{\ell-1})x_\ell^{q-2} + \dots + a_0(x_1, \dots, x_{\ell-1})$$

where $a_i(x_1, \dots, x_{\ell-1}) \in K[x_1, \dots, x_{\ell-1}]$ for $i = 0, \dots, q-2$. Suppose that there exists $i \in \{1, \dots, q-2\}$ such that $\deg a_i > 0$, then f represents a class of the second type.

Proof. Suppose that $f + P$ is composite for some $P(x_1, \dots, x_{\ell-1}) \in K[x_1, \dots, x_{\ell-1}]$. Set

$$f(x_1, \dots, x_\ell) + P(x_1, \dots, x_{\ell-1}) = u(h(x_1, \dots, x_\ell))$$

where u and h are polynomials over K such that $\deg u \geq 2$, then it is clear that $\deg u = q$ and $\deg_{x_\ell} h = 1$. Set

$$u(t) = c_q t^q + \dots + c_0$$

$$h(x_1, \dots, x_\ell) = a(x_1, \dots, x_{\ell-1}) + x_\ell b(x_1, \dots, x_{\ell-1})$$

Then:

$$\begin{aligned} & x_\ell^q + a_{q-2}(x_1, \dots, x_{\ell-1})x_\ell^{q-2} + \dots + a_0(x_1, \dots, x_{\ell-1}) + P(x_1, \dots, x_{\ell-1}) = \\ & c_q [a(x_1, \dots, x_{\ell-1}) + x_\ell b(x_1, \dots, x_{\ell-1})]^q + c_{q-1} [a(x_1, \dots, x_{\ell-1}) + \\ & x_\ell b(x_1, \dots, x_{\ell-1})]^{q-1} + \dots + c_0. \end{aligned}$$

Equating the coefficients of x_ℓ^q in both sides of this equation and also the coefficients of x_ℓ^{q-1} , we obtain:

$$c_q b^q(x_1, \dots, x_{\ell-1}) = 1$$

$$c_{q-1} b^{q-1}(x_1, \dots, x_{\ell-1}) + q c_q a(x_1, \dots, x_{\ell-1}) b^{q-1}(x_1, \dots, x_{\ell-1}) = 0$$

The first equation implies that $b \in K^*$ and the second one implies $a \in K$, hence $h \in K[x_\ell]$, and $f + P \in K[x_\ell]$ contradicting the hypothesis.

3 Kronecker substitution and compositeness

Let K be a field and let $d \geq 2$ be an integer, the application

$$S_d : K[x_1, \dots, x_\ell] \mapsto K[x]$$

$$f \mapsto f(x, x^d, \dots, x^{d^{\ell-1}})$$

is a morphism of rings and is called Kronecker substitution.

Lemma 1 *The application S_d is one to one from the set of polynomials $f(x_1, \dots, x_\ell)$ such that $\deg_{x_i} f < d$, for $i = 1, \dots, \ell - 1$, onto $K[x]$.*

Proof. See [4 chap. 1, §6, cor. 1]. In fact, we have made a slight modification of the presentation given in this book.

Proof of theorem 3.

Suppose that f is composite over K and decomposes in the form: $f(x_1, \dots, x_\ell) = u(h(x_1, \dots, x_\ell))$ where u and h are polynomials over K such that $m = \deg u \geq 2$ and $\deg h \geq 1$, then $S_d(f) = u(S_d(h))$. Set $g(x) = S_d(h)$, then $\deg g \geq 2$ (because h depends on at least two variables) and $S_d(f)(x) = u(g(x))$ hence $S_d(f)$ is strictly composite over K . We must show now that $g(x)$ has the particular form indicated in the theorem. Set:

$$h(x_1, \dots, x_\ell) = a_k(x_1, \dots, x_{\ell-1})x_\ell^k + \dots + a_1(x_1, \dots, x_{\ell-1})x_\ell + a_0(x_1, \dots, x_{\ell-1})$$

The hypothesis show that for all $i = 1, \dots, \ell - 1$, $\deg_{x_i} f = m \deg_{x_i} h < d$, hence $\deg_{x_i} h < \frac{d}{m}$ for all $i = 1, \dots, \ell - 1$. It follows that $\deg_{x_i} a_j(x_1, \dots, x_{\ell-1}) < \frac{d}{m}$ for all $i = 1, \dots, \ell - 1$ and $j = 0, \dots, k$. Using the following form of a_j :

$$a_j(x_1, \dots, x_{\ell-1}) = \sum b_{i_1 \dots i_{\ell-1}}^{(j)} x_1^{i_1(j)} \dots x_{\ell-1}^{i_{\ell-1}(j)}$$

where each exponent $i_i(j)$ satisfies: $i_i(j) < \frac{d}{m}$, leads to the equations:

$$\begin{aligned} g(x) = S_d(h(x)) &= S_d(a_k)x^{k \cdot d^{\ell-1}} + \dots + S_d(a_1)x^{d^{\ell-1}} + S_d(a_0) \\ &= x^{k \cdot d^{\ell-1}} \sum b_{i_1 \dots i_{\ell-1}}^{(k)} x^{i_1(k)+di_2(k)+\dots+d^{\ell-2}i_{\ell-1}(k)} + \dots \\ &+ x^{d^{\ell-1}} \sum b_{i_1 \dots i_{\ell-1}}^{(1)} x^{i_1(1)+di_2(1)+\dots+d^{\ell-2}i_{\ell-1}(1)} \\ &+ \sum b_{i_1 \dots i_{\ell-1}}^{(0)} x^{i_1(0)+di_2(0)+\dots+d^{\ell-2}i_{\ell-1}(0)} \end{aligned}$$

hence $g(x)$ has the required form.

Conversely, suppose that $S_d(f)$ is strictly composite over K and $S_d(f) = u(g(x))$ where u and g are polynomials over K of degree at least 2 and g has the particular form described in the theorem.

Let $m = \deg u$ and set

$$g(x) = \sum b_j x^{i_j} \quad \text{and} \quad u(x) = a(x - \alpha_1) \dots (x - \alpha_m)$$

where $a \in K$ and $\alpha_1, \dots, \alpha_m \in \overline{K}$ and the exponents i_j have the particular form, then

$$\begin{aligned} S_d(f) = u(g(x)) &= a(g(x) - \alpha_1) \dots (g(x) - \alpha_m) \\ &= a(\sum b_j x^{i_j} - \alpha_1) \dots (\sum b_j x^{i_j} - \alpha_m). \end{aligned}$$

For $i = 1, \dots, m$ consider the polynomial:

$$h_i(x_1, \dots, x_\ell) = \sum b_j x_1^{c_0(i_j)} x_2^{c_1(i_j)} \dots x_\ell^{c_{\ell-1}(i_j)} - \alpha_i.$$

Then $\deg_{\mathbb{S}_{x_k}} h_i < \frac{d}{m}$ for all $k = 1, \dots, \ell - 1$ and all $i = 1, \dots, m$ and

$$S_d(f) = a \prod_{i=1}^m S_d(h_i) = S_d(a \prod_{i=1}^m h_i).$$

Since $\deg_{x_k}(a \prod_{i=1}^m h_i) < d$ for all $k = 1, \dots, \ell - 1$, we can use Lemma 1 and conclude that:

$$f(x_1, \dots, x_\ell) = a \prod_{i=1}^m h_i(x_1, \dots, x_\ell)$$

hence f is composite.

Notice that, when $\ell = 2$, the condition on $h_d(x)$ in Theorem 3 may be formulated as follows. Write $h_d(x)$ in the x^d -adic expansion

$$h_d(x) = b_0(x) + b_1(x)x^d + \dots + b_k(x)x^{kd},$$

where $\deg b_i(x) < d$, for all $i = 0, \dots, k$, then $\deg b_i(x) < d/\deg u_d$ for $i = 0, \dots, k$.

Proof of Theorem 4. Since $d > \deg_x f$, we have in the two cases (i), (ii), $\deg A_i(x) < d$ for $i = 1, \dots, n$. Set

$$A_i(x) = a_{id-d+1}x^{d-1} + \dots + a_{id}, C_i(x) = c_{id-d+1}x^{d-1} + \dots + c_{id} \tag{12}$$

and let $e_i = \deg A_i(x)$, with $e_i = -\infty$ if $A_i(x) = 0$. We may suppose in (2) that g is monic and $g(0) = 0$. Write $g(x)$ in the form:

$$g(x) = C_0(x)x^{kd} + C_1(x)x^{(k-1)d} + \dots + C_k(x) \tag{13}$$

with $C_i(x) \in K[x]$, $\deg C_i(x) < d$, $C_0(x) \neq 0$, $C_k(0) = 0$. From (2) and (13) we obtain:

$$\deg f(x, x^d) = nd = m(kd + \deg C_0(x))$$

hence m divides n and $\frac{n}{m}d = kd + \deg C_0(x)$. It follows that $k = n/m$ and $C_0(x) = 1$. So $g(x)$ takes the form:

$$g(x) = x^{\frac{n}{m}d} + x^{(\frac{n}{m}-1)d}(c_1x^{d-1} + \dots + c_d) + \dots + (c_{\frac{n}{m}d-d+1}x^{d-1} + \dots + c_{\frac{n}{m}d-1}x) \tag{14}$$

Set:

$$u(x) = b_0x^m + b_1x^{m-1} + \dots + b_m \tag{15}$$

Identifying in (2) the coefficients of $x^{nd}, x^{nd-1}, \dots, x^{(n-\frac{n}{m})d+1}$, we obtain the following equations:

$$a_0 = b_0 \tag{16}$$

$$a_1 = mb_0c_1 \tag{17}$$

$$\dots \dots \dots \tag{18}$$

$$a_q = b_0(mc_q + \sum_{(i_1, \dots, i_m)} \ell_{i_1 \dots i_m} c_{i_1} \dots c_{i_m}) \tag{18}$$

for all integers q , $2 \leq q \leq \frac{n}{m}d - 1$ and where $\ell_{i_1 \dots i_m}$ is a positive integer and the sum runs over all tuples of positive integers $(i_1 \dots i_m)$ such that $1 \leq i_1 \leq \dots \leq i_m < q$ and $i_1 + \dots + i_m = q$.

(a) Suppose that (i) holds. We show that $c_q = \frac{a_q}{ma_0}$ for $q = 1, \dots, \frac{n}{m}d - 1$. Equations (16) and (17) show that this is true for $q = 1$. Suppose that $c_k = \frac{a_k}{ma_0}$ for every $k = 1, \dots, q-1$. This implies that if we write k in the form $k = \lambda d - \mu$ where λ is a positive integer and $\mu \in \{0, 1, \dots, d-1\}$ then $c_k = 0$ if $\mu > e_\lambda$. In order to prove the above formula, we use (18) and show that the sum appearing in (18) is zero. Suppose that some term $\ell_{i_1 \dots i_m} c_{i_1} \dots c_{i_m}$ in \sum is non zero. Set $q = \alpha d - \beta$ and $i_j = \alpha_j d - \beta_j$ with $\beta, \beta_j \in \{0, 1, \dots, d-1\}$ and $\alpha_j \leq \alpha \leq \frac{n}{m}$, then for each $j = 1, \dots, m$, $\beta_j \leq e_{\alpha_j}$. Using (i), we deduce that: $\sum_{j=1}^m \beta_j \leq \sum_{j=1}^m e_{\alpha_j} < \frac{d}{m} \cdot m = d$. It follows that: $\alpha = \sum_{j=1}^m \alpha_j$ and $\beta = \sum_{j=1}^m \beta_j$

hence $\alpha = \sum_{j=1}^m \alpha_j \geq m$, which contradicts our assumptions $\alpha \leq \frac{n}{m} < m$. So

the formula $c_q = \frac{a_q}{ma_0}$ is proved. From this, we deduce that if $c_{\alpha d - \beta} x^\beta$ is any term in the polynomial $C_\alpha(x)$ and if $\beta > e_\alpha$ then since $a_{\alpha d - \beta} = 0$, we have $c_{\alpha d - \beta} = 0$, hence $\deg C_\alpha(x) \leq e_\alpha < \frac{d}{m}$.

(b) Suppose that (ii) holds. Let $\delta = \max\{\frac{n}{i}e_i; i = 1, \dots, \frac{n}{m}\}$, then for each $i = 0, 1, \dots, \frac{n}{m}$, $e_i \leq \frac{i}{n}\delta$. We show inductively that

$$\deg C_i(x) \leq \frac{i}{n}\delta \tag{19}$$

for $i = 0, 1, \dots, \frac{n}{m}$. Now (19) is satisfied for $i = 0$. Suppose that (19) holds for $i = 0, \dots, \alpha - 1$. We will show that $\deg C_\alpha(x) \leq \frac{\alpha}{n}\delta$. Let $c_{\alpha d - \beta}x^\beta$, where $\beta \in \{0, \dots, d-1\}$, be any term in $C_\alpha(x)$ and suppose that $\beta > \frac{\alpha}{n}\delta$. According to (ii) we have $a_{\alpha d - \beta} = 0$, hence by (18),

$$m c_{\alpha d - \beta} + \sum \ell_{i_1 \dots i_m} c_{i_1} \dots c_{i_m} = 0 \quad (20)$$

Suppose that some term $\ell_{i_1 \dots i_m} c_{i_1} \dots c_{i_m}$ in this sum is non zero and set $i_j = \alpha_j d - \beta_j$, for $j = 1, \dots, m$. It is clear that $\beta_j \leq \deg C_{\alpha_j}(x)$ (otherwise $c_{i_j} = 0$). We deduce from (ii) that, for $j = 1, \dots, m$, $\alpha_j \delta / n \leq \delta / m < d / m$, hence by (19):

$$\sum_{j=1}^m \beta_j \leq \sum_{j=1}^m \deg C_{\alpha_j}(x) \leq \sum_{j=1}^m \frac{\alpha_j}{n} \delta < d.$$

Since $\alpha d - \beta = \sum_j (\alpha_j d - \beta_j)$, it follows that $\alpha = \sum_{j=1}^m \alpha_j$ and $\beta = \sum_{j=1}^m \beta_j$

and by (19) again,

$$\beta = \sum_{j=1}^m \beta_j \leq \sum_{j=1}^m \deg C_{\alpha_j}(x) \leq \sum_{j=1}^m \frac{\alpha_j}{n} \delta = \frac{\alpha}{n} \delta$$

and this contradicts our assumptions. It follows that the sum in (20) is zero and $c_{\alpha d - \beta} = 0$ for $\beta > \frac{\alpha}{n}\delta$ hence $\deg C_\alpha(x) \leq \frac{\alpha}{n}\delta < \frac{d}{m}$.

In case (i) or (ii), we have proved that $\deg C_\alpha(x) < \frac{d}{m}$ for $\alpha = 0, \dots, \frac{n}{m}$. The conclusion of Theorem 4 now follows from Theorem 3.

References

- [1] M. Ayad, Sur les polynômes f tels que $K[f]$ est intégralement fermé dans $K[x, y]$, Acta. Arithmetica, 105 (2002), 9-28.
- [2] M. Ayad, P. Ryckelynck, On the spectrum of bivariate polynomials, Preprint L.M.P.A.
- [3] A. Nowicki, N. Nagata, Rings of constants for k -derivations in $K[x_1, \dots, x_n]$, J. Math. Kyoto Univ. 28 (1998), 111-118.
- [4] A. Schinzel, Polynomials with special regards to reducibility, Cambridge Univ. Press (2000).
- [5] Y. Stein, The total reducibility order of polynomials in two variables, Israel J. Math. 68 (1999), 109-122.

Received: November 7, 2007