International Journal of Algebra, Vol. 5, 2011, no. 7, 309 - 314

Indecomposability of Multivariate Polynomials over Finite Extensions

Salah Najib

Université Hassan 1er - Settat
Faculté Polydisciplinaire de Khouribga
Al Hay El Jadid - El Biout "OCP" - BP: 145
Khouribga, Morocco
salah.najib@math.univ-lille1.fr, najibm@voila.fr

Abstract. Let K be a field of characteristic 0 and L be a finite extension of K. Let $F \in L[\underline{x}]$ be a non-constant multivariate polynomial with coefficients in L. The first main result in this paper shows an equivalence between decomposability of F as a composition of two polynomials with one having coefficients in K and the existence of infinitely many $a \in L$ with $F - a$ having a non-constant divisor in $K[\underline{x}]$. As an example of application of the first result, the second main result dealing with decomposability of the product FG of F and one of its K-conjugates. Moreover, we close this paper by a criterion for monic decomposable polynomials.

Mathematics Subject Classification: Primary 12D05, 12E05; Secondary 12F05, 11C08

Keywords: Irreducible and composite polynomial, Spectrum of a polynomial, Field extension

1. Introduction.

Let K be a field, $\overline{K}$ be an algebraic closure of K, $n \geq 2$ be an integer and $F(\underline{x}) := F(x_1, \ldots, x_n)$ be a polynomial with coefficients in K.

The polynomial F is said to be *composite* over K (or $K-$*composite*), if there exist two polynomials $Q(\underline{x}) \in K[\underline{x}]$ and $u(t) \in K[t]$ of degree $\deg(u) \geq 2$ such that $F(\underline{x}) = u(Q(\underline{x}))$. It is well-known that in the case of characteristic 0: F is composite over K if and only if F is composite over any extension of K; see for example [1; Théorème 7]. However, in positive characteristic case, this

equivalence is not always true; see [1; Section 8]. We refer to [3; Section 4] for some recent developements of this question.

Recall that the *spectrum* of the polynomial F, that one notes $\sigma(F)$, is the subset of $\overline{K}$ given by

$$\sigma(F) = \{\lambda \in \overline{K} : F(\underline{x}) - \lambda \text{ is reducible over } \overline{K}\}.$$

By a theorem of Bertini-Krull, we have: F is non-composite over $\overline{K}$ if and only if the spectrum of F is finite or empty; see [6; Chap. 3, §3, Cor. 1] or [5; Théorème 1.1]. More precisely, in [4] we showed that: if $F \in K[\underline{x}]$ is non-composite then the cardinality of $\sigma(F)$ is at most equal to $\deg(F) - 1$; see also [5] and [7].

This paper offers some new results in this context. More precisely, let K be a field of characteristic 0 and L be a finite extension of K. Let $F \in L[\underline{x}]$ be a non-constant multivariate polynomial with coefficients in L. The main results of this article are:

first: we prove an equivalence between decomposability of F as a composition of two polynomials with one having coefficients in K and the existence of infinitely many $a \in L$ with $F - a$ having a non-constant divisor in $K[\underline{x}]$ (see Theorem 1);

second: this result dealing with decomposability of the product FG of F and one of its K-conjugates [1] (see Theorem 2). This is an example of application of theorem 1.

In the last section of this article, by using recent results obtained in [2], we give a criterion for decomposable monic polynomials (see Proposition).

2. Our results and their proofs

Let K be a field of characteristic 0 and let L/K be a finite field extension of degree ≥ 2.

Definition 1 — *A non-constant polynomial $F \in L[\underline{x}]$ is said to be $(L - K)-$composite, if there exist two polynomials $Q(\underline{x}) \in K[\underline{x}]$ and $u(t) \in L[t]$, $\deg(u) \geq 2$ such that $F(\underline{x}) = u(Q(\underline{x}))$.*

It is clear that if $F \in L[\underline{x}]$ is $(L - K)-$composite then F is $L-$composite. However the converse is not always true. Indeed, consider $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$ and $F(x, y) = (y + x\sqrt{2})^2$. It is clear that F is $L-$composite, but by a direct calculation, F is not in the form $F = u(Q)$, with $Q \in \mathbb{Q}[x, y]$ and $u \in L[t]$ of degree ≥ 2.

[1] the conjugation in question is by an element of the Galois group $\mathrm{Gal}(\overline{K}/K)$.

Definition 2 — *Let $F \in L[\underline{x}]$ be a non-constant polynomial. An element $a \in L$ is called bad of first type if $F(\underline{x}) - a$ has a non-constant divisor in $K[\underline{x}]$.*

Following these definitions, we have:

Theorem 1 — *There exist infinitely many bad of first type $a \in L$ if and only if F is $(L-K)$-composite. Moreover if F is not $(L-K)$-composite then the number of bad of first type $a \in L$ is at most equal to* $\deg(F) - 1$.

Proof. Suppose that $F = u(Q)$, with $Q \in K[\underline{x}]$ and $u(t) \in L[t]$ of degree ≥ 2. Then by writing $F - a = \prod_{i=1}^{m}(Q - \alpha_i)$, (where $\alpha_1, \ldots, \alpha_m$ are roots of $u(t) - a$ and $m \geq 2$ is the degree of u), it suffices to take some a of the form $u(\alpha)$ with $\alpha \in K$. Thus for these a, the polynomial $u(t) - a$ has α as root in K. Then $Q - \alpha$ divides $F - a$ in $K[\underline{x}]$ for infinitely many a in L.

Conversely, suppose that there exist infinitely many bad of first type $a \in L$. In particular, $F - a$ is reducible over $\overline{L}$ for infinitely many a, and the spectrum of F is an infinite set. Then by [5; Théorème 1.1], the polynomial F is $\overline{L}-$composite. Therefore, by [1; Théorème 7], F is $L-$composite, i.e., we can write $F = u(Q)$ with $Q \in L[\underline{x}]$ and $u \in L[t]$ of degree ≥ 2.

Now the goal is to show that one can write $F = v(H)$ with $H \in K[\underline{x}]$ and $v \in L[t]$ of degree ≥ 2.

We can suppose that Q is not $L-$composite (by taking u of maximal degree). Then by our hypothesis, we have: $F - a = S_a.T$, where $S_a \in K[\underline{x}]$ and $T \in L[\underline{x}]$ for infinitely many $a \in L$. Moreover, we can suppose that S_a is irreducible in $K[\underline{x}]$ (by taking one irreducible divisor).

Since we have $F - a = u(Q) - a = \prod_{i=1}^{m}(Q - \alpha_i)$ (where $m = \deg(u) \geq 2$ and α_i are roots of $u(t) - a$), and the polynomial Q is not $L-$composite, the polynomials $Q - \alpha_i$ are irreducible, except for a finite number of a.

Hence for infinitely many $a \in L$, there exists α_i such that $Q - \alpha_i = c.S_a$, where $c \in L$, i.e., $Q = c.S_a + \alpha_i$. Then we obtain the desired conclusion by writing $F = v(S_a)$, where $v(t) = u(c.t + \alpha_i)$ for $a \in L$ and α_i chosen as above.

For the last part of our theorem: if F is not $(L-K)$-composite then F is not K-composite, and then F is not $\overline{K}$-composite (see for example [1; Théorème 7]). Thus by [5; Théorème fondamental], we get the desired estimation. ■

Now let $F \in L[\underline{x}]$ be a non-constant polynomial and $G(\underline{x})$ be a one of K-conjugates of F.

Definition 3 — *An element $b \in L$ is called bad of second type if $FG - b$ has a non-constant divisor in $K[\underline{x}]$.*

The following result is an example of application of theorem 1.

Theorem 2 — *There exist infinitely many bad of second type $b \in K$ if and only if $FG \in K[\underline{x}]$ and FG is $K-$composite. Moreover if $FG \in K[\underline{x}]$ and FG is not K-composite then the number of bad of second type $b \in K$ is at most equal to* $\deg(FG) - 1$.

Proof. For a fixed bad of second type element $b \in K$, we can write $FG - b = S_b.T$, where $S_b \in K[\underline{x}]$ and $T \in L[\underline{x}]$. Moreover for σ a $K-$automorphism of L, we have $(FG)^\sigma - b = S_b.T^\sigma$. Thus $FG - (FG)^\sigma = S_b.(T - T^\sigma)$.

Now we choose another bad of second type element $c \in K,\ c \neq b$ such that the polynomials S_b and S_c have no common non-constant divisor $h \in K[\underline{x}] \setminus K$ (otherwise a such h divides $FG - b - (FG - c) = c - b$ then $\deg(h) = 0$ and $h \in K$). The existence of infinitely many bad of second type $b \in K$ implies the existence of infinitely many S_b that divide $FG-(FG)^\sigma$. Then $FG-(FG)^\sigma = 0$, this means that $FG = (FG)^\sigma$ and $FG \in K[\underline{x}]$.

Moreover, our assumption implies that the polynomial $FG - b$ is reducible in $L[\underline{x}]$ for infinitely many $b \in K$. Thus FG is L-composite (by [5; Théorème 1.1]), and then it is K-composite (by [1;Théorème 7]).

Conversely, if $FG \in K[\underline{x}]$ and FG is $K-$composite then we have $FG = u(Q)$, with $Q \in K[\underline{x}]$ and $u(t) \in K[t]$ of degree ≥ 2. Then as in the beginning of the proof of theorem 1, it suffices to take some $b = u(c),\ c \in K$. Thus for these b, the polynomial $Q - c$ divides $FG - b$ in $K[\underline{x}]$. Therefore, $FG - b$ has a non-constant divisor in $K[\underline{x}]$ for infinitely many b in K.

The estimation is a direct application of [5; Théorème fondamental]. ■

Remark. Our Theorem 2 remain valid for a general polynomial $f \in L[\underline{x}]$ (instead of FG), more precisely, we have equivalence between: **(i)** $f \in K[\underline{x}]$ *and f is $K-$composite* and **(ii)** *there exist infinitely many $b \in K$ such that $f - b$ has a non-constant divisor in $K[\underline{x}]$*, (and the assertion **(ii)** corresponds to say that there exist infinitely many bad of first type $b \in K$). Therefore, one can see the equivalence between: **(i)** and **(ii)** as the particular case "$L = K$" of theorem 1.

3. Other criterion of decomposability

In this section, we will use some results obtained by Bodin in [2] in order to give a criterion for decomposable monic polynomials (see Proposition below).

Let $F \in L[\underline{x}]$ be a non-constant polynomial of degree $\deg(F)$ and let $d \geq 2$ be a divisor of $\deg(F)$.

Definition 4 — *The polynomial F is said to be $L - (d)-$composite, if there exist two polynomials $Q(\underline{x}) \in L[\underline{x}]$ and $u(t) \in L[t]$ with* $\deg(u) = d$ *such that*

$F(\underline{x}) = u(Q(\underline{x}))$. *(Again F is said to be $(L-K)-(d)-$composite if $Q \in K[\underline{x}]$).*

Since $\deg(u)$ is a divisor of $\deg(F)$, we have this fact:

fact. The polynomial F is $(L-K)-$composite *if and only if* there exists $d \geq 2$ such that F is $(L-K)-(d)-$ composite.

Let us state this result.

Proposition — *We suppose that F is monic* [2]. *The polynomial F is $(L-K)-(d)-$composite if and only if F is $L-$ composite and the $\dfrac{\deg(F)}{d}$ first coefficients of F are in K.*

This proposition is due to a private communication with Arnaud Bodin (September 2010).

Proof.

Here we will use notations and definitions of [2; Section 2].

If F is $(L-K)-(d)-$composite then $F = u(Q)$ where $Q \in K[\underline{x}]$ and $u \in L[t]$ with $\deg(u) = d$. Thus F is $L-$ composite (see fact above), and the $\dfrac{\deg(F)}{d}$ first coefficients of F (who are the coefficients of Q by using the system **(S)** of [2; Section 2]) are in K.

Conversely, if the $\dfrac{\deg(F)}{d}$ first coefficients of F are in K, then $Q \in K[\underline{x}]$ for the *d-decomposition* $F = u(Q) + R$, where $u(t) \in L[t]$ with $\deg(u) = d$, and $R \in L[\underline{x}]$ with $\deg(R) < \deg(F) - \dfrac{\deg(F)}{d}$. Then one places here with $R = 0$ (because F is $L-$ composite) which is equivalent to $F = u(Q)$ and then F is $(L-K)-(d)-$composite. ■

Acknowledgments. The author wishes to thank A. Bodin, P. Dèbes and Y. Bilu for interesting discussions about these results.

References

[1] M. Ayad, *Sur les polynômes $f(X,Y)$ tels que $K[f]$ est intégralement fermé dans $K[X,Y]$,* Acta Arith. 105 (2002), 9–28.

[2] A. Bodin, *Decomposition of polynomials and approximate roots,* Proc. Amer. Math. Soc. 138(6) (2010), 1989–1994.

[3] A. Bodin, P. Dèbes, S. Najib, *Indecomposable polynomials and their spectrum,* Acta Arith. 139 (2009), 79–100.

[4] S. Najib, *Une généralisation de l'inégalité de Stein-Lorenzini,* J. Algebra 292(2) (2005), 566–573.

[5] S. Najib, *Autour d'un théorème de Stein,* Extracta Math. 23(2) (2008), 173–180.

[2] means that the gcd of its coefficients is equal to 1.

[6] A. Schinzel, *Polynomials with special regards to reducibility,* Cambridge Univ. Press (2000).
[7] Y. Stein, *The total reducibility order of a polynomial in two variables,* Isr. J. Math. 68 (1989), 109–122.

Received: September, 2010