Riv. Mat. Univ. Parma (4) **16** (1990), 161-165

JAIME GUTIÉRREZ (*)

A note on indecomposable elements in the near-rings of formal power series (**)

Introduction

Let R be a commutative ring with 1. A formal power series over R is an infinite sequence $f = (f_0, f_1, f_2, \ldots)$ of homogeneous polynomials f_n over R, each polynomial f_n being either 0 or of degree n; the smallest index n for which f_n is different from 0 is called the *order* of f, denoted by $O(f)$. Every formal power series f can be written as a power series in X, $f = \sum a_i X^i$, $a_i \in R$ (see [5]). As usual, let us denote by $R[[X]]$ be the set of all formal power series over R. It is well-known (see [4]) that $R_+[[X]]$ the set of all formal power series with positive order is an abelian near-ring with identity X, under usual addition « + » and substitution « ∘ » of formal power series, i.e.

$$\sum a_i X^i \circ \sum b_j X^j = \sum a_i (\sum b_j X^j)^i \qquad R_+[[X]] := (\{f \in R[[X]] / O(f) \geq 1\}, +, \circ).$$

The zero-symmetric part $R_0[X]$ of the near-ring of polynomials $R[X]$ is (isomorphic to) a subnear-ring of $R_+[[X]]$. We follow the notation and terminology of Pilz [4].

1 - Def. As in ring theory, we say that an element $f \in R_+[[X]]$ is *indecomposable* provided that: (i) f is a non-zero and non-unit; (ii) $f = g \circ h$ implies g or h is an unit. Otherwise we say f is *decomposable.*

(*) Indirizzo: Departamento de Matématicas Estadística y Computación, Facultad de Ciencias, Universidad de Cantabria, E-39071 Santander.

(**) Partially supported by D.G.I.C.Y.T. PA86-0471. – Ricevuto: 11-X-1989.

In the near-ring of polynomials over a field, the concept of indecomposable polynomial is connected with the degree; likewise in $R_+[[X]]$ the indecomposable series will be connected with the order, as will see.

For every $f, g \in R_+[[X]]$: $O(f \circ g) \leqslant O(f)\, O(g)$ (with equality iff R is an integral domain). Moreover, if R is an integral domain the units in the near-ring $R_+[[X]]$ are the followings: $f = \sum a_i X^i \in R_+[[X]]$ is an *unit* iff $O(f) = 1$ and a_1 is an unit in the ring R. In particular if R is a field and $f \in R_+[[X]]$ is non-zero and non-unit, we have:

(i) f is *indecomposable* iff $f = g \circ h$ implies $O(f) = O(g)$ or $O(f) = O(h)$.

(ii) There exist indecomposable elements $f_1, \ldots, f_r \in R_+[[X]]$ with $f = f_1 \circ f_2 \circ \ldots \circ f_r$. We say that $f_1, \ldots, f_r$ is a *complete decomposition* of f.

Using theorem of implicit functions over an arbitrary field K (see e.g. [5]), we have:

(i) If $f \in K_+[[X]]$ ($\mathrm{char}(K) = 0$) is non-zero and non-unit, then f is indecomposable iff $O(f)$ is a prime number.

(ii) If $f \in K_+[[X]]$, ($\mathrm{char}(K) = p \neq 0$) is non-zero and $O(f)$ non-prime and no power of p, then f is decomposable.

2 – Our criterion to determine decomposable elements in the near-ring $R_+[[X]]$ is the following

Theorem. *Let $f = \sum a_i X^i \in R_+[[X]]$ be a formal power series with $O(f) = m$ and a_m unit in the ring R. Suppose there exist a strict divisor n of m with n unit in the ring R, then f is decomposable.*

The proof is obtained by the following

Fundamental Lemma. *Let $f = \sum a_i X^i \in R_+[[X]]$ be a formal power series with $O(f) = m$ and a_m unit in the ring R. Then for every divisor n of m, with n unit in the ring R: $p(Y) = Y^n - a_m$ has a root in R iff $p^*(Y) = Y^n - f$ has one in $R[[X]]$.*

Proof. Let b be an element such that $b^n - a_m$. In order to determine $g = b_s X^s + b_{s+1} X^{s+1} + \ldots \in R_+[[X]]$ with $m = sn$ and $g^n = f$. We find the b_i's follows.

From $g^n = f$, we have $b_s^n = a_m$, we take $b_s = b$. $nb^{n-1} b_{s+1} = a_{m+1}$, we take $b_{s+1} = a_{m+1}(nb^{n-1})^{-1}$. $nb^{n-1}b_{s+2} + \binom{n}{2}b^{n-2}b_{s+1}^2 = a_{m+2}$, we take $b_{s+2} = (a_{m+2} - \binom{n}{2}b^{n-2}b_{s+1}^2)(nb^{n-1})^{-1}$. In general we obtain

$$nb^{n-1}b_{s+i} + P_n(b, b_{s+1}, \ldots, b_{s+i-1}) = a_{m+i}$$

where $P_n(b, b_{s+1}, \ldots, b_{s+i-1})$ is a polynomial in $b, b_{s+1}, \ldots, b_{s+i-1}$ with integer coefficients. So, we compute all b_i's in R.

The converse is immediate.

Proof of Theorem. $f = a_m X \circ (X^m + \sum((a_m)^{-1}a_i)X^i)$, using Fundamental Lemma, there exist $g \in R_+[[X]]$ with $f = a_m X \circ X^n \circ g = a_m X^n \circ g$.

We turn our attention to the familiar case of formal power series over a field K.

Corollary. *Let* $f = \sum a_i X^i \in K_+[[X]]$ *with g.c.d.* (char(K), $O(f)$) = 1, *then f is indecomposable over K iff it is indecomposable over any extension of K.*

Examples. This corollary is also valid in the near-rings of polynomials if g.c.d. (char(K), degree(f)) = 1 ($f \in K[X]$). This assumption (see [**1**]) can not be omitted. Neither can the assumption in $K_+[[X]]$ g.c.d. (char(K), $O(f)$) = 1, the following illustrates: F_q is the finite field of q elements; f is indecomposable over K when $K = F_2$ and $f = X^4 + X^6 + X^7 + \sum a_i X^i \in K_+[[X]]$. Let α such that $\alpha^3 + \alpha + 1 = 0$, we can find the b_i's with $f = g \circ h = (X^2 + (1+\alpha^2)X^3) \circ (X^2 + \alpha X^3 + b_4 X^4 + b_5 X^5 + b_6 X^6 + \ldots)$, where $b_4^2 + (1+\alpha^2)b_4 + \alpha = a_8$ and for all $i \geq 5$ $(1+\alpha^2)b_i + p(\alpha, b_4, \ldots, b_{i-1}) = a_{i+4}$, where $p(\alpha, b_4, \ldots, b_{i-1})$ is a polynomial over K in $\alpha, b_4, \ldots, b_{i-1}$. So we compute $g, h \in F_{16}$.

As usual in the near-ring of polynomials theory when g.c.d. (char(K), degree(f)) $\neq 1$, ($f \in K[X]$) causes a lot of trouble.

In $K_+[[X]]$ when g.c.d. (char(K), $O(f)$) $\neq 1$ also is problematical. For example: let K be a field with char(K) $= p \neq 0$, then $f = \sum a_i X^i \in K_+[[X]]$ with $O(f) = m = p^r$ ($r \geq 1$) and $a_{m+1} \neq 0$ is indecomposable element.

3 – Theorem. *Let K be a field and $f \in K_+[[X]]$ with g.c.d.* (char(K), $O(f)$) = 1 *and $O(f)$ non-prime number, then:*

(i) *There exist an unique complete decomposition $f_1, \ldots, f_r$ of f satisfying:*

(1) $O(f_i)$ *is a prime number and* $O(f_1) \geqslant O(f_2) \geqslant \ldots \geqslant O(f_r)$. (2) f_i *are monics formal power series for* $i = 2, \ldots, r$. (3) f_i *are monomials for* $i = 1, \ldots, r-1$.

(ii) *If* $f_1, \ldots, f_r$ *and* $g_1, \ldots, g_s$ *are two complete decomposition of* f, *then* $r = s$ *and the sequences* $\ll O(f_i) \gg$, $\ll O(g_i) \gg$ *are permutations of each other.*

Remarks-Examples. We appoint that we can find explicitly the decomposition of f as in (i). Part (i) is not true in the near-rings of polynomials (e.g. $X^4 + X^3 + X^2 + X \in Q[X]$ is indecomposable, where Q is the rational numbers). Gutiérrez, Recio and Ruiz de Velasco in [2] present a polynomial-time algorithm to decompose a polynomial over a field.

Part (ii) is also valid in the near-rings of polynomials when g.c.d. (char(K), degree(f)) = 1. More interesting results about the «uniquess» of a complete decomposition of a polynomial are in the books Lausch and Nöbauer [3], Pilz [4] and in the paper Dorey and Whaples [1].

The assumption g.c.d. (char(K), $O(f)$) = 1 can not be omitted in (ii), for example: let $K = F_2$ and $f = X^4 + X^7 \in K_+[[X]]$, having proved that f is decomposable over K, that is, we can determine the b_i's in K such that

$$f = (X^2 + X^3 + X^4) \circ (X^2 + X^3 + X^5 + b_6 X^6 + b_7 X^7 + \ldots) = f_1 \circ f_2 .$$

Let $g = X^3 \circ f = X^3 \circ f_1 \circ f_2$. X^3, f_1, f_2 is seen to be a complete decomposition of g.

On the other hand

$$g = X^3 \circ f = (X^4 + X^7)^3 = X^{12} + X^{15} + X^{18} + X^{21} = (X^4 + X^5 + X^6 + X^7) \circ X^3$$

we see that $X^4 + X^5 + X^6 + X^7$ is an indecomposable element.

References

[1] F. DOREY and G. WHAPLES, *Prime and composite polynomials*, J. Algebra 28 (1974), 88-101.

[2] J. GUTIÉRREZ, T. RECIO and C. RUIZ DE VELASCO, *Polynomial decomposition algorithm of almost quadratic complexity*, Proc. AAECC-6. Lecture Notes Comp. Sci. 357 (1989) (Springer-Verlag), 471-476.

[3] H. LAUSCH and W. NÖBAUER, *Algebra of polynomials*, Amsterdam North-Holland Pub. Co. 1973.

[4] G. PILZ, *Near rings*, North-Holland Pub. Co. Math. Studies 23 (1983).

[5] O. ZARISKI and P. SAMUEL, *Commutative Algebra*, Volume **II**, Springer-Verlag 1960.

Abstract

In this note we investigate the indecomposable elements in the near-rings of formal power series. We indicate «coincidences» with the results on indecomposable elements in the near-rings of polynomials and we also give interesting examples of formal power series with orders divisible by the characteristic of the field having more than one decomposition.

***