Proceedings of the Edinburgh Mathematical Society (1989) 32, 73–80 ©

DISTRIBUTIVE ELEMENTS IN THE NEAR-RINGS OF POLYNOMIALS

by JAIME GUTIERREZ* and CARLOS RUIZ DE VELASCO Y BELLAS

(Received 21st May 1987)

0. Introduction

As usual in the theory of polynomial near-rings, we deal with right near-rings. If $N=(N,+,\cdot)$ is a near-ring, the set of distributive elements of N will be denoted by N_d;

$$N_d=\{d\in N\,|\,d(r+s)=dr+ds, \text{ for all } r,s\in N\}.$$

It is easy to check that, if N is an abelian near-ring (i.e., $r+s=s+r$, for all r, $s\in N$), then N_d is a subring of N.

In this paper we describe the distributive elements of the near-ring of polynomials over a commutative ring with identity, which will be denoted by R. We also prove that if R is an integral domain, the set of distributive elements contains the subrings of the near-ring of polynomials; in particular, the near-ring of polynomials has an unique maximal subring.

1. The ring of the distributive elements

The set $R[X]$, of all polynomials over R in the indeterminate X, is a near-ring under addition "+" and substitution of polynomials "$\circ$" (i.e., $f(X)\circ g(X)=f(g(X))=f\circ g$ (see [1], [4]). We shall denote by $R_0[X]$ the set of all polynomials over R whose constant term is zero.

1.1. Immediate properties

(i) *$R_0[X]$ is a subnear-ring of $(R[X],+,\circ)$ and agrees with $R[X]_0$, the zero-symmetric part of $R[X],+,\circ)$.*

(ii) *$(R[X]_d,+,\circ)$ and $(R_0[X]_d,+,\circ)$ are rings, and $R[X]_d$ is a subring of $R_0[X]_d$.*

(iii) *$(R[X]_d,+)$ and $(R_0[X]_d,+)$ are R-submodules of $R[X]$ and $R_0[X]$ (respectively).*

*Partially supported by C.A.I.C. y T 2280/83.

D

https://doi.org/10.1017/S0013091500006921 Published online by Cambridge University Press

(iv) $(R[X]_d, +, \circ)$ *and* $(R_0[X]_d, +, \circ)$ *are subrings of the ring* $(\mathrm{End}(R[X]), +, \circ)$ *and* $(\mathrm{End}(R_0[X]), +, \circ)$ *(respectively).*

Proof. (i) See [**4**, chap. 7–78].

(ii) The firsts two assertions are immediate. For the third, let $f \in R[X]_d$, let us say $f = a_n X^n + \cdots + a_1 X + a_0$; then

$$a_0 = f \circ 0 = f \circ (0+0) = f \circ 0 + f \circ 0 = a_0 + a_0 \quad \text{hence} \quad a_0 = 0.$$

(iii) They are immediate.

(iv) Consider the map $i: R[X]_d \to \mathrm{End}(R[X])$ defined by $i(f)(g) = f \circ g$ ($f \in R[X]_d$ and $g \in R[X]$); it is well defined and it is a morphism of rings.

Moreover, $\mathrm{Ker}(i) = \{0\}$. In fact, if $f \in \mathrm{Ker}(i)$, then $f = f \circ X = 0$.

1.2. Consequence. *The set* $RX = \{aX \mid a \in R\}$ *is a subring of* $R[X]_d$ *(resp.* $R_0[X]_d$*) isomorphic to* R.

Proof. As $X \in R[X]_d$ and $R[X]_d$ is a R-module, this shows that $R[X]_d \supseteq RX$. Clearly $aX \circ bX = abX$, and therefore RX is a subring of $R[X]_d$.

Our main goal in this section is to find all the elements of $R[X]_d$ and $R_0[X]_d$. The proofs of several results are similar for both, so we shall just give the proof for either $R[X]_d$ or $R_0[X]_d$. First of all we reduce the problem to the case of monomials.

Lemma 1.3. *Let a be a non-zero element of R and let $n \geqq 2$, an integer:*

(i) *If* $aX^n \notin R_0[X]_d$ ($aX^n \notin R[X]_d$), *there exists an integer* i, $1 \leqq i \leqq n-1$, *such that* $a\binom{n}{i} \neq 0$ *and for all* $t \geqq 0$, $aX^n \circ (X^t + X^{t+1}) \neq aX^n \circ X^t + aX^n \circ X^{t+1}$.

(ii) *If* $aX^n \in R[X]_d$ ($aX^n \in R_0[X]_d$), *then the order of a (denoted by* $0(a)$*) is finite.*

Proof. (i) If $aX^n \notin R_0[X]_d$, there exists $f, g \in R_0[X]$ such that: $aX^n \circ (f+g) \neq af^n + ag^n$, hence for some i, $1 \leqq i \leqq n-1$, we have $a\binom{n}{i} \neq 0$. Let $j = \max\{i/1 \leqq i \leqq n-1,\ a\binom{n}{i} \neq 0\}$, then $aX^n \circ (X^t + X^{t+1}) = a(X^t(1+X))^n = aX^{tn}(1+X)^n = aX^{tn} + anX^{tn+1} + \cdots + a\binom{n}{j}X^{tn+j} + aX^{tn}X^n$, and $a\binom{n}{j}X^{tn+j} \neq 0$.

(ii) If $0(a)$ is infinite, we have

$$aX^n \circ (X + X^2) = aX^n + anX^{n+1} + \cdots + anX^{2n-1} + aX^{2n} \neq aX^n \circ X + aX^n \circ X^2$$

$$= aX^n + aX^{2n};$$

by hypothesis $anX^{2n-1} \neq 0$, which leads to a contradiction.

https://doi.org/10.1017/S0013091500006921 Published online by Cambridge University Press

Proposition 1.4. *Let $f=a_nX^n+\cdots+a_1X\in R[X]$; then $f\in R[X]_d$ (resp. $R_0[X]_d$) if and only if $a_iX^i\in R[X]_d$ (resp. $R_0[X]_d$) for all $i=1,\ldots,n$.*

Proof. Suppose $f\in R[X]_d$ and $a_nX^n\notin R[X]_d$, and we consider, $j=\max\{i/1\leqq i\leqq n-1, a_n\binom{n}{i}\neq 0\}$ (see Lemma 1.3) and t an integer $\geqq 1$; then we get $f(X)\circ(X^t+X^{t+1})=f(X^t)+f(X^{t+1})=a_nX^{tn}+\cdots+a_1X^t+a_nX^{(t+1)n}+\cdots+a_1X^{t+1}\equiv(*)$. On the other hand $f(X)\circ(X^t+X^{t+1})=a_n(X^t+X^{t+1})^n+\cdots+a_1(X^t+X^{t+1})\equiv(**)$. Moreover, the first summand of $(**)$ is: $a_n(X^t+X^{t+1})^n=a_nX^{tn}+\cdots+a_n\binom{n}{j}X^{tn+j}+a_nX^{(t+1)n}$, (with $a_n\binom{n}{j}X^{tn+j}\neq 0$ which is the highest degree monomial (different from $a_nX^{(t+1)n}$) occurring in the development of $a_n(X^t+X^{t+1})^n$. We now prove that for a large enough integer t, $a_n\binom{n}{j}X^{tn+j}\neq 0$ is the highest degree monomial (different from $a_nX^{(t+1)n}$) occurring in the development of the polynomial $f(X)\circ(X^t+X^{t+1})$. In fact, the monomials of $f(X)\circ(X^t+X^{t+1})$ are all of the form $a_m\binom{m}{k}X^{tm+k}$ with $0\leqq k\leqq m<n$ except for the monomials given by a_nX^n (a case already studied above). Now, we can choose an integer t large enough such that $tn+j>tm+k$; since $(*)=(**)$, contradiction.

Theorem 1.5. *If all the non-zero elements of R have infinite order (torsion free), then: $R[X]_d=R_0[X]_d=RX$.*

Proof. It is an immediate consequence of 1.1(ii), 1.3(ii) and 1.4.

We now prove some preliminary lemmas for the explicit description of $R[X]_d$ and $R_0[X]_d$ in the remaining cases.

Lemma 1.6. *Let n, p be two integers such that $n\geqq 1$ and p is a prime number. Suppose $n=p^ar$, where a is a non-negative integer and r is a positive integer such that p does not divide r. Then, if $t\leqq a$, the integer $\binom{n}{p^t}$ is divisible by p^{a-t} but it is not divisible by p^{a-t+1}.*

From this last result it is easy to prove the following lemma, of which we have not found any references in the literature.

Lemma 1.7. *Let $n>1$ be an integer. The greatest common divisor (gcd) of $\{\binom{n}{i}\mid i=1,2,\ldots,n-1\}$ is p if n is a power of a prime number p, and 1 otherwise.*

Proof. Let d be the gcd of $\{\binom{n}{i}\mid i=1,2,\ldots,n-1\}$. If n is a power of the prime p, say $n=p^a$, then d divides $\binom{n}{p^{a-1}}$, and by Lemma 1.6 we get $d=p$. Now, if $n=p_1^{a_1}\ldots p_t^{a_t}$, with $t\geqq 2$, then $d=p_1^{\alpha_1}\ldots p_t^{\alpha_t}$ with $0\leqq\alpha_i\leqq a_i$; as d divides $\binom{n}{p_i^{a_i}}$ for all i, $i=1,\ldots,t$, using again the lemma, we conclude $\alpha_i=0$, $i=1,\ldots,t$.

Proposition 1.8. *Let $a\neq 0$ be an element of R and let $n\geqq 2$ be an integer. Then $aX^n\in R[X]_d$ (resp. $R_0[X]_d$) if and only if the order of a divides $\binom{n}{i}$ for all $i=1,\ldots,n-1$.*

Proof. Let us suppose $aX^n\in R[X]_d$, we have $aX^n(1+X)^n=a(X(1+X))^n=a(X+$

$X^2)^n = aX^n \circ (X+X^2) = aX^n + aX^{2n}$. By expanding the first member, we notice $a\binom{n}{i}X^{n+i} = 0$ for all $i = 1, 2, \ldots, n-1$; hence $a\binom{n}{i} = 0$.

Theorem 1.9. *Let $a \neq 0$ be an element of R, and let $n \geqq 2$ be an integer; then $aX^n \in R[X]_d$ (resp. $R_0[X]_d$) if and only if there exists a prime p and a positive integer α such that $n = p^\alpha$ and $0(a) = p$.*

Proof. Let us assume $aX^n \in R[X]_d$, by Proposition 1.8 $0(a)$ divides $gcd\{\binom{n}{i} \mid i = 1, \ldots, n-1\}$; as $0(a) > 1$, using Lemma 1.7, we have $n = p^\alpha$ for some prime p and an integer $\alpha > 0$. Now the converse is obvious.

As a consequence of 1.4 and 1.9 we obtain the following:

Theorem 1.10. $R[X]_d = R_0[X]_d$.

In order to get an explicit description of the ring $R[X]_d$, we introduce the following notation: given a prime p

$$\mathbf{I}_p := \{a \in R \mid 0(a) = p\} \cup \{0\},$$

$$\mathbf{I}_p[X] := \{a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \cdots + a_1 X^{p^1} / a_i \in \mathbf{I}_p, n \geqq 1\}.$$

Lemma 1.11. (i) *For every prime p, $\mathbf{I}_p$ is an ideal of R.*

(ii) *If p, q are different primes, the set $\mathbf{I}_p\mathbf{I}_q := \{ab \mid a \in \mathbf{I}_p,\ b \in \mathbf{I}_q\} = \{0\}$.*

(iii) *For every prime p, $\mathbf{I}_p[X]$ is an ideal of $R[X]_d$.*

Proof. It is straightforward; for (iii) it is enough to consider monomials and use (i) and (ii).

Theorem 1.12. *We have*

$$R[X]_d = \left(\bigoplus_{p \in \mathbf{P}} \mathbf{I}_p[X] \right) \oplus RX$$

where **P** *denotes the set of all prime numbers.*

Proof. It is an immediate consequence of 1.9 and 1.11.

We note that RX is a subring of $R[X]_d$, but it is not an ideal. In the following corollary we express $R[X]_d$ as a direct sum of ideals in some particular cases. For every prime p we define

$$\mathbf{I}_p^*[X] := \{a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \cdots + a_1 X^{p^1} + a_0 X^{p^0} / a_i \in \mathbf{I}_p, n \geqq 0\}$$

Lemma 1.13. *For every prime p, $\mathbf{I}_p^*[X]$ is an ideal of $R[X]_d$.*

Corollary 1.14. *Let R be a unitary commutative ring with the following property (P): "there are some prime numbers $p_1, \ldots, p_s$ and elements a_1 in $\mathbf{I}_{p1}, \ldots, a_s$ in $\mathbf{I}_{p_s}$ such that $1 = a_1 + \cdots + a_s$", then:*

$$R[X]_d = \bigoplus_{p \in P} \mathbf{I}_p^*[X]$$

The property required in Corollary 1.14 is not always verified as we can see in the following:

Examples 1.15. (i) Let R be a ring of characteristic an integer $n > 1$ such that $n = p_1 p_2 \ldots p_r$, $r > 1$ and $p_1, p_2, \ldots, p_r$ distinct primes; we have here $p_1 \ldots p_{i-1} \hat{p}_i p_{i+1} \ldots p_r \in \mathbf{I}_{pi}$, for all $i = 1, 2, \ldots, r$; where $\hat{}$ denotes omission of the p_i. As

$$gcd(p_2 \ldots p_r \ldots p_1 \ldots p_{i-1} p_{i+1} \ldots p_r \ldots p_1 p_2 \ldots p_{r-1}) = 1$$

we get $1 = a_1 + \cdots + a_r$ with $a_i \in \mathbf{I}_{p_i}$, so this kind (or class) of rings verifies the above property (P).

(ii) Let $R = Z_{12}$, the integers modulo 12, then $\mathbf{I}_2 = \{0, 6\}$, $\mathbf{I}_3 = \{0, 4, 8\}$ and $\mathbf{I}_p = \{0\}$ otherwise. In this case 1 cannot be expressed as a sum of elements of the $\mathbf{I}_p$'s, hence this ring does not verify the property.

Corollary 1.16. *If the characteristic of R is a prime number p, then*

$$R[X]_d = \{a_n X^{p^n} + a_{n-1} X^{p^{n-1}} + \cdots + a_1 X^{p^1} + a_0 X^{p^0} / a_i \in R, n \geqq 0\}.$$

The elements of $R[X]_d$ are, in this case, the so called p-polynomials. They were introduced and studied by Ore when R is a finite field, but in another context, they have interesting properties (see [3]). See also [2] pages 108 onwards and references there mentioned.

2. Rings in near-rings of polynomials

In this section, we investigate rings which are contained in $R[X]$. Since all rings are zero-symmetric near-rings, we only need to search for them in $R_0[X]$.

We prove our main result:

Theorem 2.1. *Let S be a subring of $R[X]$ (not necessarily unitary). If R is an integral domain then S is contained in $R[X]_d$.*

The proof requires a series of lemmas as well as a number of results from Section 1.

Lemma 2.2. *Let R be an integral domain and let S be a subring of $R[X]$ (not necessarily unitary) then: $f\circ(X+f)=f+f\circ f$, for all $f\in S$.*

Proof. Let $f\neq 0$ then f, $f\circ f\neq 0\in S$, we have $f\circ(f+f\circ f)=f\circ f+f\circ f\circ f=(f+f\circ f)\circ f$, but on the other hand $f\circ(f+f\circ f)=f\circ(X+f)\circ f$, since R is an integral domain hence f is right cancellable (see [1]).

The characteristic of an integral domain is either 0 or a prime number p. We treat those cases separately and start with:

Proposition 2.3. *Let R be an integral domain of characteristic 0 and let S be a subring of $R[X]$ (not necessarily unitary) then: S is contained in $R[X]_d$.*

Proof. Let $f=a_nX^n+\cdots a_1X\in S$, by the last lemma; $f\circ(X+f)=f+f\circ f$, then $a_n(X+f)^n+\cdots+a_1(X+f)=a_nX^n+\cdots+a_1X+a_nf^n+\cdots+a_1f$, we get $n=1$ or $a_n=0$, and we end the proof using Proposition 1.5.

Corollary 2.4. *Let R be an integral domain of characteristic 0 then the subrings of $R[X]$ are (isomorphic to) subrings of the ring R.*

Proof. It is immediate using 1.2, 1.5 and 2.3.

Hence we have proved our Theorem 2.1 in the case when the characteristic of R is 0. Now we consider the case of characteristic a prime number p.

Lemma 2.5. (a) *The set $R'[X]_0:=\{f\in R_0[x]/f'=\text{constant}$, where f' is the formal derivative of $f\}$ is a subnear-ring of $R[X]$ containing $R[X]_d$ and moreover $R'[X]_0=R[X]_d$ if and only if R is torsion free.*

(b) *If R is an integral domain of characteristic a prime number p. Let $a\neq 0$ be an element of R and let $n\geqq 2$ be an integer then: $aX^n\in R'[X]_0$ if and only if p divides n.*

Proof. (a) The first assertion is straightforward. It suffices to observe that $f=a_nX^n+\cdots+a_1X\in R'[X]_0$ if and only if $a_iX^i\in R'[X]_0$, for all $i=1$ to n, now use 1.9. For the second assertion; let $a\neq 0$ be an element of R and let $n\geqq 2$ be an integer such that $na=0$ and $n=p_1^{r_1}\dots p_t^{r_t}$. We distinguish two cases: if $t\geqq 2$, then $aX^n\in R'[X]_0$ but $aX^n\notin R[X]_d$. If $t=1$, let q be a prime number with $q\neq p_1$, then $aX^{p_1^{r_1}q}\in R'[X]_0$ but $aX^{p_1^{r_1}q}\notin R[X]_d$. The converse is immediate.

(b) is immediate.

Lemma 2.6. *Let R be an integral domain of characteristic a prime number p and let S be a subring of $R[X]$ (not necessarily unitary) then: S is contained in $R'[X]_0$.*

Proof. Let $f=a_nX^n+\cdots+a_1X\in S$. If $n=1$ then S is contained in $R'[X]_0$. Suppose $n\geqq 2$. First we show that p divides n. Suppose $gcd(n,p)=1$ by Lemma 2.2 $f\circ(X+f)=f+f\circ f$, we have $(a_nX^n+\cdots+a_1X)\circ(X+f)=a_n(X+f)^n+\cdots+a_1(X+f)$, the first summand $a_n(X+f)^n=a_nX^n+\cdots+na_nf^{n-1}X+a_nf^n$; we see $na_nf^{n-1}X=na_n^nX^{n(n-1)+1}+\ldots$, with $na_n^nX^{n(n-1)+1}\neq 0$, so $f\circ(X+f)-(f+f\circ f)=na_n^nX^{n(n-1)+1}+\ldots\neq 0$, contradiction. Hence p divides n.

We take $r=\max\{i/i=1,2,\ldots,n, a_i\neq 0 \text{ and } gcd(i,p)=1\}$. Two cases occur:

(i) If $r=1$ by 2.5 $f\in R'[X]_0$, then S is contained in $R'[X]_0$.

(ii) If $r\geqq 2$, we have $f=a_nX^n+\cdots+a_rX^r+\cdots+a_1X$ with $a_r\neq 0$, $r<n$, $gcd(r,p)=1$ again by 2.2 $f\circ(X+f)=f+f\circ f$ and by the properties of the derivative we get: $(f'\circ(X+f))(1+f')=f'+(f'\circ f)f'$ on the right hand side we have $(f'\circ(X+f))(1+f')=((ra_rX^{r-1}+\cdots+a_1)\circ(X+f))(1+f')=(ra_r(X+f)^{r-1}+\cdots+a_1)+(ra_r(X+f)^{r-1}+\cdots+a_1)f'$. Let $g=(ra_r(X+f)^{r-1}+\cdots+a_1)-f'$, then $g\neq 0$ and the degree of g is $n(r-1)$. Let $h=(ra_r(X+f)^{r-1}+\cdots+a_1)f'-(f'\circ f)f'$, then the degree of h, t is $t<n(r-1)$. So $(f'\circ(X+f))(1+f')-f'+(f'\circ f)f'=g(X)+h(X)\neq 0$, a contradiction. Therefore $r=1$ and $f\in R'[X]_0$.

Proposition 2.7. *Let R be an integral domain of characteristic a prime number p and let S be a subring of $R[X]$ (not neccessarily unitary) then: S is contained in $R[X]_d$.*

Proof. Let $f=a_nX^n+\cdots+a_1X\in S$. There exist $h,g\in R[X]$ such that $f=h+g$, with $g\in R[X]_d$ and $h=b_mX^m+\cdots+b_tX^t$, with $b_iX^i\notin R[X]_d$ for all $i=1,\ldots,m$ and $t>1$. If $h=0$, then $f\in R[X]_d$ and S is contained in $R[X]_d$.

Suppose $h\neq 0$, by Lemma 2.6 $f\in R'[X]_0$ so $h\in R'[X]_0$. By Lemma 2.5 we get $h=b_mX^{p^{r_m}k_m}+\cdots+b_tX^{p^{r_t}k_t}$ with $r_i\geqq 1, b_i\neq 0$, $k_i>1$, $gcd(p,k_i)=1$ for all $i=t,\ldots,m$, and $p^{r_j}k_j>p^{r_i}k_i$ for all $j>i$.

Let $r_h=\min\{r_i/i=t,\ldots,m\}$. To simplify notation, we shall write $k_h=k$ and $r_h=r$; then $h=(b_mX^{p^{s_m}k_m}+\cdots+b_hX^k+\cdots+b_tX^{p^{s_t}k_t})\circ X^{p^r}$. Let F be the quotient field of R and let $\bar{F}$ be the algebraic closure of F. There exist $c_i\in\bar{F}$, with $c_i\neq 0$ and $h=X^{p^r}\circ(c_mX^{p^{s_m}k_m}+\cdots+c_hX^k+\cdots+c_tX^{p^{s_t}k_t})$. We can write $h(X)=X^{p^r}\circ c$, where $c=c_mX^{p^{s_m}k_m}+\cdots+c_hX^k+\cdots+c_tX^{p^{s_t}k_t}$. By Lemma 2.2 $f\circ(X+f)=f+f\circ f$, since $g\in R[X]_d$, $h\circ(X+f)=h+h\circ f$; so $(X^{p^r}\circ c)\circ(X+f)=X^{p^r}\circ c+X^{p^r}\circ c\circ f$, as $X^{p^r}\in F[X]_d$ we have $X^{p^r}\circ(c\circ(X+f))=X^{p^r}\circ(c+c\circ f)$, since $r>1$ and since R is an integral domain then $c\circ(X+f)=c+c\circ f$. Using the properties of the derivative we have $(c'\circ(X+f))(1+f')=c'+(c'\circ f)f'$ and we arrive at a contradiction. The proof is similar to the one in Lemma 2.6 and is therefore omitted.

This completes the proof of Theorem 2.1.

Remark 2.8. If R is not an integral domain, then Theorem 2.1 does not hold: we take $R=Z_4$, the ring of integers modulo 4. Let B be the group generated by $\langle X, 2X^{3^i}$ for all $i \geqq 0\rangle$ then $B = \langle X, 2X^{3^i}$ for all $i \geqq 0\rangle$ is an infinite unitary ring, but B is not contained in $R[X]_d$. We also see that B is not contained in $R'[X]_0$.

Corollary 2.9. *Let R be an integral domain of characteristic a prime number p, then:*

(i) *$R[X]$ has an unique maximal subring.*

(ii) *$R[X]$ has a subring S isomorphic to the polynomial ring $(Z_p[X], +, \cdot)$, where Z_p is the field of integers modulo p. In particular, the subrings of $Z_p[X]$ are (isomorphic to) subrings of the polynomial ring $(Z_p[X], +, \cdot)$.*

Proof. (ii) The map ϕ from $(Z_p[X]_d, +, \circ)$ to $(Z_p[X], +, \cdot)$, defined as follows: $\phi(aX^{p^n}) = aX^n$ is a ring isomorphism. The proof is now immediate using 1.16 and 2.7.

Acknowledgement. We would like to thank Professor Günter Pilz for his generous help.

REFERENCES

1. H. Lausch and W. Nöbauer, *Algebra of polynomials,* (North-Holland, Amsterdam-New York, 1973).

2. R. Lidl and H. Neiderreiter, *Finite fields* (Addison-Wesley, Reading, Massachusetts, 1983).

3. O. Ore, On a special class of polynomials, *Trans. Amer. Math. Soc.* **35** (1933), 539–584.

4. G. Pilz, *Near-rings* (North-Holland, Amsterdam, 1983).

Departmento de Matematicas
Facultad de Ciencias
Universidad de Cantabria
39005-Santander, Spain.