PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 55 (69), 1994, 23–28

A NOTE ON SKEW POLYNOMIAL RINGS

Michael G. Voskoglou

Abstract. Let R be a ring of prime characteristic and let D be a finite set of derivations of R. We obtain results connecting the D-simplicity of R with the simplicity of the skew polynomial ring over R defined with respect to D. A similar result was quoted, without proof, by the author in an earlier paper.

1. Skew polynomial rings in finitely many variables. All the rings considered in this paper are with identities. Let R be a ring, let $H = \{f_1, \dots, f_n\}$ be a finite set of monomorphisms of R and let $D = \{d_1, \dots, d_n\}$ be a set of mappings from R to R, such that d_i is a f_i-derivation of R (cf.[**8**, section 1]), for each $i = 1, \dots, n$. Assume further that $d_i \circ d_j = d_j \circ d_i$, $f_i \circ f_j = f_j \circ f_i$ and $f_i \circ d_j = d_j \circ f_i$ for all $i, j = 1, \dots, n$ and consider the set S_n of all polynomials in n variables, say $x_1, x_2, \dots, x_n$, over R. Define in S_n addition in the usual way and define multiplication by the relations $x_i r = f_i(r)x_i + d_i(r)$, $x_i x_j = x_j x_i$, for all $r \in R$ and all $i, j = 1, \dots, n$. Then S_n becomes a ring denoted by $R[x, H, D]$ and called a skew polynomial ring over R, while S_i is a skew polynomial ring over S_{i-1}, for each $i = 1, 2, \dots, n$, with $S_0 = R$ (cf.[**8**, Theorem 2.4]). When $n = 1$, we write $S_1 = R[x_1, f_1, d_1]$.

Notice that under these conditions f_i extends to a monomorphism of S_n by $f_i(x_j) = x_j$ and d_i extends to an f_i-derivation of S_n by $d_i(x_j) = 0$, for all $i, j = 1, \dots, n$ (cf.[**8**, Theorems 2.2 and 2.3]).

We can also define the skew polynomial rings $S_n^* = R[x, D]$, when f_i is the identity map of R and $S_n' = R[x, H]$ if d_i is the zero derivation of R for each $i = 1, \dots, n$. Moreover, if H is a set of automorphisms of R, then the quotient ring of S_n' with respect to the Ore subset $A = \{x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$, with $a_1, \dots, a_n$ non-negative integers$\}$ of S_n' is denoted by $T_n = R[x, x^{-1}, H]$ and called a skew Laurent polynomial ring over R (cf.[**9**, section 2]).

In earlier papers we have obtained necessary and sufficient conditions under which the rings S_n and T_n are simple (cf.[**7**] and [**9**] respectively) and we have

AMS Subject Classification (1991): Primary 16A05

examined relations among the prime (simiprime) ideals of R and those of S_n (or T_n) in a more general context (cf.[**10**], [**11**] and [**12**]; see also [**1**], [**2**], [**3**] and their references).

2. Simple skew polynomial rings of prime characteristic. In order to simplify our notation in this section we denote by S_n the skew polynomial ring $R[x, D]$, where D is a set of n commuting derivations of R. Then an ideal I of R is called D-ideal, if $d_i(I) \subseteq I$ for all d_i in D and R is called a D-simple ring, if it has no nonzero proper D-ideals (when $n = 1$ we write d_1-ideal and d_1-simple ring respectively).

Every D-simple ring contains the field $F_0 = C(R) \cap \bigcap_{i \in D} \ker d_i$, where $C(R)$ denotes the center of R, and therefore R is either of characteristic zero, or of a prime number, say p.

In [**7**], assuming that $\mathrm{ch}\,(R) = 0$, we have connected the D-simplicity of R with the simplicity of S_n (Theorems 3.3 and 3.4) and we have also quoted, without proof, a corresponding result when $\mathrm{ch}\,(R) = p$ (Theorem 3.5). Here we are going to prove a similar result, but first we need the following two lemmas.

LEMMA 2.1 *Let I be a nonzero ideal of S_n. Write the elements of I as polynomials in x_n with coefficients in S_{n-1} and denote by $A(I)$ the set of leading coefficients of the elements of I of minimal degree together with zero. Set $I_i = A(I_{i+1})$ for each $i = 0, 1, \dots, n-1$, where $I_n = I$. Then I_i is a $\{d_n, d_{n-1}, \dots, d_{i+1}\}$ -ideal of S_i for each $i = 0, 1, \dots, n-1$, $I_i \neq 0$.*

Proof. Notice first that $A(I) = I_{n-1}$ is a nonzero d_n-ideal of S_{n-1} and that $A(I_{n-1}) = I_{n-2}$ is a nonzero d_{n-1}-ideal of S_{n-2} (cf.[**5**, Lemma 1.3])

Next, given $0 \neq f$ in I_{n-2}, there exists $0 \neq g$ in I_{n-1} of minimal degree, say k, with respect to x_{n-1} and the leading coefficient f. Then $d_n(g) = d_n(f)X_{n-1}^k$ + terms of lower degree with respect to x_{n-1} (since $d_n(x_{n-1}) = 0$) and therefore $d_n(f)$ belongs to I_{n-2}. Thus I_{n-2} is a $\{d_n, d_{n-1}\}$-ideal of S_{n-2}. The result follows by successive applications of the same argument.

LEMMA 2.2 *Let R be aring of nonzero characteristic, say p, and let $s = vp^k$, fore some integers $v \geq 1$ and $k \geq 0$. Consider the ring S_n. Then $x_i^s r = \sum_{j=0}^{v} \binom{v}{j} d_i^{jp^k}(r) x_i^{(v-j)p^k}$, for all r in R and each $i = 1, \dots, n$ (where d_i^0 denotes the identity map of R).*

Proof. Given r in R we have that $x_i r = r x_i + d_i(r)$, for each $i = 1, \dots, n$. Furthermore an easy induction shows that $x_i^v r = \sum_{j=0}^{v} \binom{v}{j} d_i^j(r) x_i^{v-j}$, for all integers $v \geq 1$. But the subring of S_n generated by R and $x_i^{p^k}$ is isomorphic to the skew polynomial ring $S = R[z, d_i^{p^k}]$ (with z corresponding to $x_i^{p^k}$) and therefore the result follows by writting down the previous equation for the ring S.

At this point we recall that a derivation d of R is called an inner derivation of R induced by r in R, if $d(s) = rs - sr$, for all s in R. We are ready now to prove

THEOREM 2.3 *Let R be a D-simple ring of prime characteristic, say p. Assume that no derivation of the form $d = \sum_{k=0}^{m} c_k d_i^{p^k}$, with m a non-negative integer and c_k in $\bigcap_{j=k}^{n} \ker d_j$, is an inner derivation of S_{i-1} induced by an element of $\bigcap_{j=k}^{n} \ker d_j$, for all $i = 1, \ldots, n$. Then S_n is a simple ring.*

Proof. Assume that S_n is not a simple ring and let I be a nonzero proper ideal of S_n. Then, following the notation of Lemma 2.1, we have that I_0 is a D-ideal of R and therefore $I_0 = R$. Thus there exists a monic polynomial, say $f_1 = f_1(x_1)$, of minimal degree in I_1. If deg $f_1 = 0$, then $I_1 = S_1$ and therefore there exists a monic polynomial, say $f_2 = f_2(x_2)$, of minimal degree in I_2. If the f_i's keep having degree zero, then we proceed in the same way. We will finally find a monic polynomial, say $f_{n-1} = f_{n-1}(x_{n-1})$ in I_{n-1}, with deg $f_{n-1} = 0$, since otherwise we would have $I = R$, a contradiction to our hypothesis.

Therefore, without loss of generality we may assume that $f_1(x_1) = x_1^s + \sum_{i=0}^{s-1} a_i x_1^i$, with $s \neq 0$ and a_i in R for each $i = 0, 1, \ldots, s-1$. Then, for all r in R,

$$f_1 r = r x_1^s + [s d_1(r) + a_{s-1} r] x_1^{s-1} + \text{ terms of lower degree}$$

and the polynomial $f_1 r - r f_1$, wich is also in I_1, has degree less than s. Thus

$$f_1 r = r f_1. \tag{1}$$

Now, if p does not divide s, our proof is similar to that of Theorem 3.4 of [**7**]. In fact, on comparing the coefficients of x_1^{s-1} in the equation (1) we get that $s d_1(r) + a_{s-1} r = r a_{s-1}$, for all r in R. But $0 \neq s 1_R$ is in F_0 and therefore s^{-1} is in $C(R)$. Thus the previous relation gives that $d_1(r) = (-s^{-1} a_{s-1}) r - r(-s^{-1} a_{s-1})$ for all r in R and therefore d_1 is an inner derivation of R induced by $-s^{-1} a_{s-1}$. But, by Lemma 2.1, I_1 is a $\{d_2, d_3, \ldots, d_n\}$-ideal of S_1, while, since $d_j(x_1) = 0$, $d_j(f_1)$ has degree less than s and therefore $d_j(f_1) = 0$, for each $j = 2, 3, \ldots, n$. Thus,

$$d_j(a_i) = 0 \tag{2}$$

for each $i = 0, 1, \ldots, s-1$ and therefore $-s^{-1} a_{s-1}$ is in $\bigcap_{j=1}^{n} \ker d_j$, a fact which contradicts our hypothesis (set $m = 0$ and $a_0 = 1$).

Thus we may assume that

$$s = s' p^l \tag{3}$$

for some positive integer l, where p does not divide s'. In this case let $i = i(k)$ be the greatest integer less than s, such that p^k divides i, while p^{k+1} does not, for each $k = 0, 1, \ldots, l$. Therefore we can write $i = v(k) p^k$, for some positive integer $v(k)$, such that p does not divide $v(k)$. Then, because of Lemma 2.2, given r in R, $i_1(k) = i(k) - p^k = [v(k) - 1] p^k$ is the greatest integer less than i, such that $a_i x_1 i_1 r$ can have a nonzero coefficient for $x_1^{i_1}$.

Set $t = \max_k i_1(k)$; then we are going to compare the coefficients of x_1^t in equation (1). For this, observe first that $a_t x_1^t r = a_t r x_1^t$ + terms of lower degree. From the other hand it is clear that, if $i(k) = t$, then i is the unique integer of the form $v(k)p^k$, where p does not divide $v(k)$, such that $a_i x_1^i r$ can have a nonzero coefficient for x_1^t, while, if $i(k) < t$, then there is no integer with this property. Thus, in order to calculate the coefficient of x_1^t in $f_1 r$, we only need to look at the terms of the form $a_r x_1^c x$, with $s \geq c > t$. Because of the relation (3) we can write $c = qp^k$ for some integers $q \geq 1$ and k, $0 \leq k \leq l$, such that p does not divide q. Then, by Lemma 2.2, $x_1^c r = \sum_{j=0}^{q} \binom{q}{j} d_1^{jp^k}(r) x_1^{(q-j)p^k}$ and therefore $a_c x_1^c r$ can have a nonzero coefficient for x_1^t if, and only if, $t = bp^k$ for some non-negative integer b. Then, since $i(k) = v(k)p^k \geq c > t = bp^k \geq i_1(k) = [v(k) - 1]p^k$, we get that $b = v - 1$ and therefore $c = i(k)$, $0 \leq k \leq r$ and $t = i_1(k)$.

Thus, by Lemma 2.2 again,

$$a_c x_1^c r = a_{i(k)} x_1^{v(k)p^k} r = a_i(k) \sum_{j=0}^{v(k)} \binom{v(k)}{j} d_1^{jp^k}(r) x_1^{[v(k)-j]p^k}. \tag{4}$$

But $c = i(k) > t$, the fact which clearly implies that $i_1(k) = [v(k) - 1]p^k = t$, and therefore, in order to reach the coefficient of x_1^t in (4), we must take $j = 1$.

Let m be the maximal k such that $i_1(k) = t$; then, if $k > m$, is $i_1(k) < t$ and therefore we must take $c = i(k)$, $0 \leq k \leq m$. Thus, using the relation (4) and comparing the coefficients of x_1^t in the equation (1), we get that

$$r a_t = a_t r + \sum_{k=0}^{m} c_k d_1^{p^k}(r) \tag{5}$$

with $c_k = v(k) a_{i(k)}$ if $i(k) > t$ and $c_k = 0$, if $i(k) \leq t$ ($c_m \neq 0$, since $t = i_1(m) < i(m)$).

Furthermore $x_1 f_1 - f_1 x_1 = \sum_{i=0}^{s-1} d_1(a_i) x_1^i$ is in I_1 and has degree less than s; therefore $d_1(a_i) = 0$, for each $i = 0, 1, \ldots, s-1$. But we have already seen that $d_j(a_i) = 0$ for each $j = 2, 3, \ldots, n$ (see the relation (2)) and therefore $a_{i(k)}$ and a_t are in $\bigcap_{j=1}^{n} \ker d_j$. Therefore the equation (5) contradicts our hypothesis and this completes the proof.

The previous theorem has the following converse.

THEOREM 2.4 *If S_n is a simple ring of prime characteristic, say p, then R is a D-simple ring and there is no inner derivation of R of the form $d = \sum_{j=0}^{m} a_j d_i^{p^j}$, with $m \geq 0$ and a_j in F_0 for each j, induced by a nonzero element r of $\bigcap_{d_i \in D} \ker d_i$, for all $i = 1, \ldots, n$.*

Proof. Since S_n is a simple ring, R is a D-simple ring and no element of D can be an inner derivation of R induced by some $0 \neq r$ in $\bigcap_{d_i \in D} \ker d_i$ (cf.[**7**, Theorem 3.3]).

Assume now that there exists an inner derivation of R the form $d = \sum_{j=0}^{m} a_j d_i^{p^j}$ with $m > 0$ and a_j in F_0 for each j, induced by a nonzero element r of $\bigcap_{d_i \in D} \ker d_i$. Consider the polynomial $f(x_i) = \sum_{j=0}^{m} a_j x_i p^j - r$ and let s be in R. Then, since a_j is in the center of R for each j, applying Lemma 2.2 for $v = 1$, we get

$$f(x_i)s = \sum_{j=0}^{m} \left[a_j s x_i^{p^j} + a_j d_i^{p^j}(s)\right] - rs = s\left(\sum_{j=0}^{m} a_j x_i^{p^j}\right) + d(s) - rs = sf(x_i).$$

Furthermore

$$\begin{aligned} x_k f(x_i) &= \sum_{j=0}^{m} x_k a_j x_i^{p^j} - x_k r = \sum_{j=0}^{m} [a_j x_k + d_k(a_j)] x_i^{p^j} - [r x_k + d_k(r)] \\ &= \sum_{j=0}^{m} (a_j x_i P^j) x_k - r x_k = f(x_i) x_k \qquad \text{for all } k = 1, \dots, n \end{aligned}$$

(since r is in $\bigcap_{d_i \in D} \ker d_i$ and a_j is in F_0). Thus $f(x_i)$ is in the center of S_n. But a_m, being in the field F_0, is a regular element of R and therefore $f(x_i)$ is not a unit of S_n, because otherwise, by Lemma 3.2 of [**7**], we would have that $m = 0$. Thus $f(x_i)S_n$ is a nonzero proper ideal of S_n, a contradiction to our hypothesis.

Remarks (i) The following example illustrates the construction of t and of the derivation d in the proof of Theorem 2.3. Assume that $\operatorname{ch}(R) = 3$ and let $s = 54 = 2 \cdot 3^3$. Then $i(0) = 53$, $i(1) = 51$, $i(2) = 45$ and $i(3) = 27$; therefore $i_1(0) = 52$, $i_1(1) = 48$, $i_1(2) = 36$ and $i_1(3) = 0$. Thus $t = 52$, $m = 0$ and therefore $d = c_0 d_1 = v(0) a_{i(0)} d_1 = a_{53} d_1$.

(ii) In the statement of Theorem 3.5 in [**7**] we have assumed that the c_k's of the derivation $d = \sum_{k=0}^{m} c_k d_i^{p^k}$ (cf.Theorem 2.3 above) are in

$$F_{k-1} = C(S_{k-1}) \cap \Big(\bigcap_{j=k}^{n} \ker d_j\Big).$$

For the derivation d constructed in the proof of Theorem 2.3 we have shown that the c_k's are in $\bigcap_{j=k}^{n} \ker d_j$, but it remains to show that c_k is in $C(R)$. To show this, since $c_k = v(k) a_{i(k)}$ when $i(k) > t$, it suffices to show that $a_{i(k)}$ is in $C(R)$ (F_{k-1} is a subring of S_{k-1}. At the first glance we thought that this turns out on comparing the coefficients of $x_1^{i(k)}$ in the equation (1), but this does not look quite obvious to us now. For instance, reconsider example (i) and compare the coefficients of x_1^{51} in $f_1 r = r f_1$. Since $x_1^c r = r x_1^c$ + terms of lower degree, you must look to $x_1^c r$ for $c = 52, 53, 54$. Thus $r a_{51} = a_{51} r + 52 a_{52} d(r) + \binom{53}{2} a_{53} d^2(r) (\binom{54}{3} d^3(r) = 0$, since 3 divides $\binom{54}{3}$) fact which shows that a_{51} is not in the center of R (this is not a counter example since $51 < t$).

(iii) Theorems 2.3 and 2.4 above for $n = 1$ give a result due to Jordan (cf.[**5**] or [**7**, Corollary 3.6 (ii)]).

(iv) After quoting Theorem 3.5 in [**7**], Malm gave a proof different from ours above, considering the case $n = 1$ and applying induction on n (cf.[**6**, Theorem 4]). He also proved in a different way Theorems 3.3 and 3.4 of [**7**] (cf.[**6**, Theorem 2]), i.e. the case where R is of characteristic zero.

REFERENCES

[1] A. W. Goldie and G. Michler, *Ore extensions and polycyclic group rings*, J. London Math. Soc. (2) **9** (1974), 337–345.

[2] R. S. Irving, *Prime ideals of Ore extensions over commutative rings*, J. Algebra **56** (1979) 315–342.

[3] R. S. Irving, *Prime ideals of Ore extensions over commutative rings II*, J. Algebra **58** (1979) 399–423.

[4] D. Jordan, *Ore extensions and Jacobson rings*, Ph. D. Thesis, Leeds, 1975.

[5] D. Jordan *Noetherian Ore extensions and Jacobson rings*, J. London Math. Soc. (2) **10** (1975) 281–291.

[6] D. R. Malm, *Simplicity of partial and Schmidt differential operator rings*, Pacific J. Math **132** (1988), 85–112.

[7] M. G. Voskoglou, *Simple skew polynomial rings*, Publ. Inst. Math. (Beograd) **37(51)** (1985), 37–41.

[8] M. G. Voskoglou, *Extending derivations and endomorphisms to skew polynomial rings*, Publ. Inst. Marh. (Beograd) **39(53)** (1986), 79–82.

[9] M. G. Voskoglou, *Simple skew Laurent polynomial rings*, Boll. U.M.I. (Italy), (7), 1 - A, 1987, 255–260.

[10] M. G. Voskoglou, *Prime ideals of skew polynomial rings*, Riv. Mat. Univ. Parma (4) **15** (1989), 17–25

[11] M. G. Voskoglou, *Semiprime ideals of skew polynomial rings*, Publ. Inst. Math. (Beograd) **47(61)** (1990), 33–38.

[12] M. G. Voskoglou, *Prime and semiprime ideals of skew Laurent polynomial rings*, Riv. Mat. Univ. Parma (4) **17** (1991), 211–215.

Technological & Educational
Institute (T. E. I.)
New Buildings - 30200 Mesolongi
Greece

(Received 23 03 1993)