International Electronic Journal of Algebra
Volume 31 (2022) 1-12
DOI: 10.24330/ieja.1058380

ON A PROPERTY OF THE IDEALS OF THE POLYNOMIAL RING $R[x]$

Amr Ali Abdulkader Al-Maktry

Received: 3 April 2020; Revised: 2 February 2021; Accepted: 23 April 2021
Communicated by Burcu Üngör

Abstract. Let R be a commutative ring with unity $1 \neq 0$. In this paper we introduce the definition of the first derivative property on the ideals of the polynomial ring $R[x]$. In particular, when R is a finite local ring with principal maximal ideal $\mathfrak{m} \neq \{0\}$ of index of nilpotency e, where $1 < e \leq |R/\mathfrak{m}| + 1$, we show that the null ideal consisting of polynomials inducing the zero function on R satisfies this property. As an application, when R is a finite local ring with null ideal satisfying this property, we prove that the stabilizer group of R in the group of polynomial permutations on the ring $R[x]/(x^2)$, is isomorphic to a certain factor group of the null ideal.

Mathematics Subject Classification (2020): 13F20, 06B10, 13J15, 11T06, 05A05, 13B25, 20B35

Keywords: Commutative rings, polynomial ring, null ideal, null polynomial, Henselian ring, finite local ring, dual numbers, polynomial permutation, permutation polynomial, finite permutation group

1. Introduction

Let R be a commutative ring with unity $1 \neq 0$, and $R[x]$ be the polynomial ring over R of one indeterminate x. In addition to the usual operations on polynomials, $R[x]$ has a further operation, which appears in a normal way, namely the formal derivative of polynomials. Nöbauer used this operation to define the derivative of ideals with a certain property [4].

Another well known feature of $R[x]$ is that every polynomial $f(x) = \sum_{j=0}^{k} a_j x^j \in R[x]$ induces a function $F : R \longrightarrow R$, where $F(r) = \sum_{j=0}^{k} a_j r^j$ for all $r \in R$. In this case F is called a polynomial function on R. The set of all polynomial functions on R is a monoid via composition of functions. Moreover, when the function F is a bijection we say F is a polynomial permutation while f is a permutation polynomial. Obviously, the set of all polynomial permutations is a group, which

The author is supported by the Austrian Science Fund (FWF): P 30934-N35.

we denote by $\mathcal{P}(R)$. Further, $\mathcal{P}(R)$ forms the group of units of the monoid of polynomial functions.

If a polynomial $g \in R[x]$ induces the constant zero function over R, that is $g(r) = 0$ for each $r \in R$, then g is called a null polynomial over (on) R. The set of all null polynomials on R is an ideal of $R[x]$, which we denote by N_R and we call it the null ideal (on R). The null ideal N_R supplies the ring of polynomials $R[x]$ with an equivalence relation in which two polynomials $g, h \in R[x]$ are equivalent whenever $g - h \in N_R$. In other words, two polynomials are related in this relation if and only if they induce the same function on R. Moreover, every equivalence class corresponds to one polynomial function on R and vice versa.

This paper considers a property of the ideals of the ring $R[x]$ and its application to the group of polynomial permutations on finite rings. In particular, for a finite local ring R with null ideal having this property, we prove some facts about the permutation polynomials on the ring $R[x]/(x^2)$.

The property defined in the paper depends on the formal derivative of polynomials, however it is completely different from the one considered in [4].

Throughout this paper for a local ring R, let $\mathfrak{m}$ denote its maximal ideal and let $N(\mathfrak{m})$ be the set of all polynomials over R which vanish on the ideal $\mathfrak{m}$. Evidently, $N(\mathfrak{m})$ is an ideal in the polynomial ring $R[x]$ containing N_R. For $f \in R[x]$ with $f(x) = \sum_{i=0}^{n} a_i x^i$, let f' denote its formal derivative; i.e., $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.

2. The first derivative property and the null ideal

We begin this section with the definition of our property. Then we prove some supplementary results. Later, we show that the null ideal N_R has this property for a wide class of finite local rings with principal maximal ideals.

Definition 2.1. Let R be a commutative ring. An ideal I of $R[x]$ satisfies the first derivative property if $g, h \in I$ implies that $g'h' \in I$.

For shortness we use the abbreviation FDP for the first derivative property.

Proposition 2.2. *Let I, J be ideals of $R[x]$. Then:*

(1) *I^2 satisfies FDP;*

(2) *if I and J satisfy FDP, then IJ satisfies FDP.*

Proof. We prove (2) and leave (1) to the reader. Let $f, g \in IJ$. Then there exist polynomials $f_1, \ldots, f_n; g_1, \ldots, g_m \in I$ and $h_1, \ldots, h_n; k_1, \ldots, k_m \in J$ such that $f = \sum\limits_{i=1}^{n} f_i h_i$ and $g = \sum\limits_{j=1}^{m} g_j k_j$. So $f' = \sum\limits_{i=1}^{n} f_i' h_i + \sum\limits_{i=1}^{n} f_i h_i'$ and $g' = \sum\limits_{j=1}^{m} g_j' k_j +$

$\sum_{j=1}^{m} g_j k'_j$. Obviously, $\sum_{i=1}^{n} f_i h'_i, \sum_{j=1}^{m} g_j k'_j \in I$ and $\sum_{i=1}^{n} f'_i h_i, \sum_{j=1}^{m} g'_j k_j \in J$. On the other hand, by Definition 2.1, we have $f'_i g'_j \in I$ for every $1 \leq i \leq n; 1 \leq j \leq m$. Hence $(\sum_{i=1}^{n} f'_i h_i)(\sum_{j=1}^{m} g'_j k_j) = \sum_{i,j} f'_i g'_j h_i k_j \in IJ$. Similarly, $(\sum_{i=1}^{n} f_i h'_i)(\sum_{j=1}^{m} g_j k'_j) \in IJ$. Therefore

$$f'g' = (\sum_{i=1}^{n} f'_i h_i + \sum_{i=1}^{n} f_i h'_i)(\sum_{j=1}^{m} g'_j k_j + \sum_{j=1}^{m} g_j k'_j) \in IJ.$$

□

The following result gives a criterion for FDP for finitely generated ideals over $R[x]$.

Proposition 2.3. *Let I be an ideal of $R[x]$ and suppose that $I = (f_1, \ldots, f_n)$ for some $f_1, \ldots, f_n \in R[x]$. Then I satisfies FDP if and only if $f'_i f'_j \in I$ for all $i, j \in \{1, \ldots, n\}$.*

Proof. $(\Rightarrow)$ Obvious.
$(\Leftarrow)$ Suppose that $f'_i f'_j \in I$ for any two generators $f_i, f_j \in I$. Let $g, h \in I$. Then there exist $g_1, \ldots, g_n; h_1, \ldots, h_n \in R[x]$ such that $g(x) = \sum_{i=1}^{n} g_i f_i$ and $h(x) = \sum_{i=1}^{n} h_i f_i$. We have $g' = \sum_{i=1}^{n} g'_i f_i + \sum_{i=1}^{n} g_i f'_i$ and $h' = \sum_{i=1}^{n} h'_i f_i + \sum_{i=1}^{n} h_i f'_i$. So

$$g'h' = (\sum_{i=1}^{n} g'_i f_i)h' + (\sum_{i=1}^{n} g_i f'_i)(\sum_{i=1}^{n} h'_i f_i) + (\sum_{i,j=1}^{n} g_i h_j f'_i f'_j).$$

Clearly, $g'h' \in I$, and hence I satisfies FDP. □

Remark 2.4. Let R be a local ring with maximal ideal $\mathfrak{m}$ and residue field $\mathbb{F}_q$, and let $\lambda(x) = \prod_{i=1}^{q}(x - c_i)$, where $\{c_1, \ldots, c_q\}$ is any complete systems of residue modulo $\mathfrak{m}$. It is obvious that $c_i - c_j$ is a unit in R whenever $i \neq j$; hence for every $r \in R$ such that $r \equiv c_i \mod \mathfrak{m}$, $r - c_j$ is a unit. Then the following lemma follows.

Lemma 2.5. *Let $r \in R$. Then $\lambda'(r)$ is a unit in R.*

Remark 2.6. It is a celebrated fact that every finite local commutative ring is a Henselian ring, i.e., a local ring in which Hensel's lemma holds, (see for example, [2, Theorem. XIII.4]). This allows us to use some facts about the ideals $\mathfrak{m}, N_R$, when R is a Henselian ring, from [5] to improve our related ideas on finite local rings.

Lemma 2.7. [5, Corollary 2.11] *Let R be a Henselian ring. Then $\lambda(R) = \mathfrak{m}$.*

Lemma 2.8. [5, Theorem 4.2] *Let R be a Henselian ring and $\lambda(x)$ as in Remark 2.4. If $N(\mathfrak{m}) = (F_1(x), \ldots, F_n(x))$, then $N_R = (F_1(\lambda(x)), \ldots, F_n(\lambda(x)))$.*

Recall from the introduction the definitions of the ideals $N_R, N(\mathfrak{m})$. The following result shows that, for a Henselian ring R and a finitely generated ideal $N(\mathfrak{m})$, either both $N(\mathfrak{m})$ and N_R satisfy FDP or neither satisfies FDP.

Theorem 2.9. *Let R be a Henselian ring and $\lambda(x)$ as in Remark 2.4. If $N(\mathfrak{m}) = (F_1(x), \ldots, F_n(x))$, then N_R satisfies FDP if and only if $N(\mathfrak{m})$ satisfies FDP.*

Proof. By Lemma 2.8, $N_R = (F_1(\lambda(x)), \ldots, F_n(\lambda(x)))$.

($\Leftarrow$) Suppose that $N(\mathfrak{m})$ satisfies FDP. Then for every $i, j \in \{1, \ldots, n\}$ there exists $h_{i,j} \in N(\mathfrak{m})$ such that $F_i' F_j' = h_{i,j}$. Hence $F_i'(\lambda(x))F_j'(\lambda(x)) = h_{i,j}(\lambda(x)) \in N_R$ since $\lambda(R) = \mathfrak{m}$ by Lemma 2.7. Now

$$(F_i(\lambda(x)))'(F_j(\lambda(x)))' = (\lambda'(x))^2 F_i'(\lambda(x))F_j'(\lambda(x)) = (\lambda'(x))^2 h_{i,j}(\lambda(x)) \in N_R.$$

Thus N_R satisfies FDP by Proposition 2.3.

($\Rightarrow$) Suppose that N_R satisfies FDP. Then for every $i, j \in \{1, \ldots, n\}$ we have

$$(F_i(\lambda(x)))'(F_j(\lambda(x)))' = (\lambda'(x))^2 F_i'(\lambda(x))F_j'(\lambda(x)) \in N_R.$$

Now let $r \in R$ be arbitrary, so $(\lambda'(r))^2 F_i'(\lambda(r))F_j'(\lambda(r)) = 0$ by the definition of N_R. Hence $F_i'(\lambda(r))F_j'(\lambda(r)) = 0$ since $\lambda'(r)$ is a unit by Lemma 2.5, whence $F_i'(\lambda(x))F_j'(\lambda(x)) \in N_R$. But, $\lambda(R) = \mathfrak{m}$ by Lemma 2.7. Therefore $F_i' F_j' \in N(\mathfrak{m})$ for every $i, j \in \{1, \ldots, n\}$. Thus $N(\mathfrak{m})$ satisfies FDP by Proposition 2.3. □

Remark 2.10. Notice that we don't require R to be Noetherian. In fact there exists a Henselian ring which is non-Noetherian with a finitely generated ideal $N(\mathfrak{m})$ (see [5, Example 3.2]).

Our aim now is to show that the null ideal N_R satisfies FDP for every finite local ring with a nonzero principal maximal ideal of index of nilpotency less than or equal $q + 1$, where q is the cardinality of the residue field $\mathbb{F}_q$. To do so, we need this lemma.

Lemma 2.11. [5, Theorem 4.4] *Let R be a finite local ring with principal maximal ideal $\mathfrak{m} = (m)$ and residue filed $\mathbb{F}_q$. Suppose e is the index of nilpotency of $\mathfrak{m}$. If $e \leq q$, then $N(\mathfrak{m}) = (x, m)^e$; if $e = q + 1$, then $N(\mathfrak{m}) = (x, m)^e + (x^q - m^{q-1}x)$.*

Theorem 2.12. *Let R be a finite local ring with principal maximal ideal $\mathfrak{m} = (m)$ and residue filed $\mathbb{F}_q$. Suppose e is the index of nilpotency of $\mathfrak{m}$. If $1 < e \leq q + 1$ then N_R satisfies FDP, provided $e \geq 4$ when $e = q + 1$.*

Proof. In view of Theorem 2.9, we need only to prove that $N(\mathfrak{m})$ satisfies FDP. Now $N(\mathfrak{m})$ is finitely generated since R is finite, so it is enough to show that $g'h' \in N(\mathfrak{m})$ for every pair of generators g, h of $N(\mathfrak{m})$ by Proposition 2.3.

First assume that $1 < e < q+1$. By Lemma 2.11, $N(\mathfrak{m})$ is generated by the set $\{x^e, mx^{e-1}, \ldots, m^{e-1}x\}$. Let g, h be any generators of $N(\mathfrak{m})$. Then $g(x) = m^j x^{e-j}$ and $h(x) = m^i x^{e-i}$ for some $0 \leq i, j \leq e-1$. Therefore

$$g'(x)h'(x) = (e-i)(e-j)m^{i+j}x^{2e-i-j-2} \in N(\mathfrak{m})$$

since $e \geq 2$, and so $N(\mathfrak{m})$ satisfies FDP.

We now consider the case $e = q+1$. By Lemma 2.11, $N(\mathfrak{m})$ is generated by the following set $\{x^e, mx^{e-1}, \ldots, m^{e-1}x, x^q - m^{q-1}x\}$. Since $q \in \mathfrak{m}$ we have $q = rm$ for some $r \in R$. Let g, h any two generators of $N(\mathfrak{m})$. We distinguish three cases.

Case 1. $g(x) = h(x) = x^q - m^{q-1}x$. Then

$$g'(x)h'(x) = (qx^{q-1} - m^{q-1})^2 = q^2x^{2q-2} - 2qm^{q-1}x^{q-1} + m^{2q-2},$$

whence

$$g'(x)h'(x) = r^2m^2x^{2e-4} - 2rm^{e-1}x^{e-2} + m^{2e-4}.$$

Evidently, $r^2m^2x^{2e-4} - 2rm^{e-1}x^{e-2} \in N(\mathfrak{m})$ since $e = q+1 \geq 3$. Thus $g'h' \in N(\mathfrak{m})$ if and only if $m^{2e-4} \in N(\mathfrak{m})$ if and only if $m^{2e-4} = 0$, provided $e \geq 4$.

Case 2. $g(x) = x^q - m^{q-1}x$ and $h(x) = m^i x^{e-i}$ for some $0 \leq i \leq e-1$.
Then
$g'(x)h'(x) = (e-i)m^i x^{e-i-1}(qx^{q-1} - m^{q-1}) = (e-i)m^i x^{e-i-1}(rmx^{e-2} - m^{e-2}) =$
$= (e-i)m^{i+1}x^{e-i-1}(rx^{e-2} - m^{e-3}) \in N(\mathfrak{m})$ since $m^{i+1}x^{e-i-1} \in N(\mathfrak{m})$ and $e \geq 4 > 3$.

Case 3. $g(x) = m^j x^{e-j}$ and $h(x) = m^i x^{e-i}$ for some $0 \leq i, j \leq e-1$. Then

$$g'(x)h'(x) = (e-i)(e-j)m^{i+j}x^{2e-i-j-2} \in N(\mathfrak{m})$$

since $e \geq 4$.

Therefore $N(\mathfrak{m})$ satisfies FDP. □

Remark 2.13. (1) If $e = 1$, then $R = \mathbb{F}_q$. In this case $N_{\mathbb{F}_q} = (x^q - x)\mathbb{F}_q[x]$. But, $N_{\mathbb{F}_q}$ does not satisfy FDP. Because, if we take $g(x) = x^q - x$, then $(g'(x))^2 = (qx^{q-1} - 1)^2 = 1 \notin N_{\mathbb{F}_q}$.

(2) Consider $g(x) = (x^2 - x)^2 - 2(x^2 - x) \in \mathbb{Z}_8[x]$, by Fermat's Theorem, one can show easily that $g(a) \equiv 0 \pmod 8$ for every $a \in \mathbb{Z}_8$, that is, $g \in N_{\mathbb{Z}_8}$. However, $N_{\mathbb{Z}_8}$ does not satisfy FDP since $(g')^2 \notin N_{\mathbb{Z}_8}$. Indeed, $(g'(1))^2 = 4 \not\equiv 0 \pmod 8$. Note that $e = q + 1 = 3 < 4$.

Corollary 2.14. *Let n be a positive integer and p a prime number.*

(1) *If $p > 2$, then $N_{\mathbb{Z}_{p^n}}$ satisfies FDP for every $1 < n \leq p + 1$.*
(2) *If $p = 2$, then $N_{\mathbb{Z}_4}$ satisfies FDP.*

Although we defined null ideals for finite rings, the definition is still true for infinite rings. We consider this fact in the following example.

Example 2.15. Let R be a boolean ring (not necessary finite). By definition, $f = x^2 - x \in N_R$. But, $(f')^2 = (-1)^2 = 1 \notin N_R$.

Right now we have achieved our first main goal, that is, showing the existence of a wide class of finite local rings with null ideals having FDP. In the next section we employ FDP to infer some facts about a group of polynomial permutations over the ring $R[x]/(x^2)$.

3. Applications to polynomial permutations of the ring $R[x]/(x^2)$

In this section, for a finite local commutative ring R with the null ideal N_R satisfying the first derivative property, we prove some facts about some kind of permutation polynomials on the ring $R[x]/(x^2)$.

Throughout this section all rings are finite.

Recall that $R[x]/(x^2)$ is isomorphic to the ring $R[\alpha] = \{a + b\alpha : a, b \in R\}$, where $\alpha \notin R$ and $\alpha^2 = 0$. Here are some easily verifiable facts about polynomials over $R[\alpha]$.

Fact 3.1. *Let $h \in R[x]$. Then $h(a + b\alpha) = h(a) + bh'(a)\alpha$ for each $a, b \in R$.*

Fact 3.2. *Let $g \in R[\alpha][x]$. Then $g = g_1 + g_2\alpha$ for some $g_1, g_2 \in R[x]$.*

Recall from the introduction that $\mathcal{P}(R[\alpha])$ denotes the group of polynomial permutations on the ring $R[\alpha]$.

Definition 3.3. Let $St_\alpha(R) = \{F \in \mathcal{P}(R[\alpha]) : F(r) = r \text{ for each } r \in R\}$.

Obviously, $St_\alpha(R)$ is a nonempty finite subset of $\mathcal{P}(R[\alpha])$. Further, it is closed under the composition of functions. Therefore $St_\alpha(R)$ is a subgroup of $\mathcal{P}(R[\alpha])$. The group $St_\alpha(R)$ by definition stabilizes every element of R; for this we call it the stabilizer group of R in the group of polynomial permutations of $R[\alpha]$ or more shortly the stabilizer group.

Lemma 3.4. *Let A be a ring and $g, h \in A[x]$. If g and h induce the same function over A, then there exists $f \in N_A$ such that $g = h + f$.*

Proof. Take $f = g - h$. Then $f \in N_A$. □

We need some facts from [1]. However, we prove these facts as the proofs do not depend on extra materials.

Lemma 3.5. [1, Lemma 3.4] *Let $h \in N_R$. Then $h\alpha$ induces the zero function over $R[\alpha]$.*

Proof. By Fact 3.1, $h(a+b\alpha)\alpha = (h(a) + bh'(a)\alpha)\alpha = h(a)\alpha + 0 = 0\alpha = 0$ for all $a, b \in R$. □

Proposition 3.6. [1, Proposition 4.6] *Let R be a ring. Then*

$$St_\alpha(R) = \{F \in \mathcal{P}(R[\alpha]) : F \text{ is induced by } x + f(x) \text{ for some } f \in N_R\}.$$

Proof. It is obvious that

$$St_\alpha(R) \supseteq \{F \in \mathcal{P}(R[\alpha]) : F \text{ is induced by } x + f(x) \text{ for some } f \in N_R\}.$$

Now let $F \in \mathcal{P}(R[\alpha])$ such that $F(r) = r$ for each $r \in R$. Since F is a polynomial permutation over $R[\alpha]$, F is induced by a polynomial $g \in R[\alpha][x]$. By Fact 3.2, $g = g_0 + g_1\,\alpha$, where $g_0, g_1 \in R[x]$. Now $r = F(r) = g(r) = g_0(r) + g_1(r)\,\alpha$ for each $r \in R$. Then $g_1(r)\,\alpha = 0$, and so $g_1(r) = 0$ for each $r \in R$, i.e., $g_1 \in N_R$. Hence, $g_1\alpha$ is a null polynomial over $R[\alpha]$ by Lemma 3.5. Thus g_0 and $g_0 + g_1\alpha$ both induce F on $R[\alpha]$, i.e., F is induced by g_0. Further, $g_0 \equiv x \mod N_R$, i.e., g_0 induces the identity on R, and therefore $g_0(x) = x + h(x)$ for some $h \in N_R$ by Lemma 3.4. This shows the other inclusion. □

Lemma 3.7. *Let $F \in St_\alpha(R)$. Suppose that $x + f(x)$ induces F, where $f \in N_R$. Then the following statements are equivalent*

(1) $(f')^2 \in N_R$;
(2) $x - f(x)$ *induces* F^{-1};
(3) $F^k = \underbrace{F \circ F \circ \cdots \circ F}_{k \text{ times}}$ *is induced by* $x + kf(x)$ *for every* $k \in \mathbb{N}$.

Proof. (1) ⇒ (2) Let G be the function induced by $x - f(x)$. Then for every $r, s \in R$ we have

$$\begin{aligned} G \circ F(r + s\,\alpha) &= G(r + s\,\alpha + f(r + s\,\alpha)) \\ &= G(r + s\,\alpha + f(r) + sf'(r)\,\alpha) \text{ (by Fact 3.1)} \\ &= G(r + s\,\alpha + sf'(r)\,\alpha) \quad \text{(since } f \text{ is null)} \\ &= (r + s\,\alpha + sf'(r)\,\alpha) - f(r + (s + sf'(r))\,\alpha) \\ &= (r + s\,\alpha + sf'(r)\,\alpha) - \big(f(r) + (s + sf'(r))f'(r)\,\alpha\big) \text{ (by Fact 3.1)} \\ &= r + s\,\alpha + sf'(r)\,\alpha - sf'(r)\,\alpha \quad \text{(since } (f')^2 \in N_R) \\ &= r + s\,\alpha\,. \end{aligned}$$

Thus $F^{-1} = G$, whence $x - f(x)$ induces F^{-1}.

(2) ⇒ (1) Let $x - f(x)$ induces F^{-1}. Then one can use the previous calculations to get that for every $r, s \in R$, $r + s\alpha = F^{-1} \circ F(r + s\,\alpha) = r + s\,\alpha - s(f'(r))^2\alpha$.

Hence $s(f'(r))^2\alpha = 0$, whence $(f'(r))^2 s = 0$ for every $r, s \in R$. So if $s = 1$, we have $(f'(r))^2 = 0$ for every $r \in R$. Therefore $(f')^2 \in N_R$.

(1) ⇒ (3) By induction on k.

(3) ⇒ (1) Let $k = 2$. Then F^2 is induced by $x + 2f(x)$, and so that

$$F^2(r + s\,\alpha) = r + s\,\alpha + 2f'(r)s\,\alpha\,.$$

While, by successive calculations,

$$F^2(r+s\,\alpha) = F \circ F(r+s\,\alpha) = F(r+s\,\alpha+sf'(r)\,\alpha) = r+s\,\alpha+s(2f'(r)+(f'(r))^2)\alpha.$$

Then from the two expression of $F^2(r + s\,\alpha)$ follows that $s(f'(r))^2 = 0$ for every $r, s \in R$. Thus $(f'(r))^2 = 0$ for every $r \in R$, and hence $(f')^2 \in N_R$. □

In the following proposition we show that how FDP is useful in describing the behavior of the elements of the stabilizer group $St_\alpha(R)$ in connection with their polynomial expressions.

Proposition 3.8. *Let $F \in St_\alpha(R)$. Suppose that $x + f(x)$ induces F, where $f \in N_R$. If N_R satisfies FDP, then the following statements hold:*

(1) *$x - f(x)$ induces F^{-1};*

(2) *$F^k = \underbrace{F \circ F \circ \cdots \circ F}_{k\ times}$ is induced by $x + kf(x)$ for every $k \in \mathbb{N}$;*

(3) *if $G \in St_\alpha(R)$ is induced by $x + g(x)$, where $g \in N_R$, then $x + f(x) + g(x)$ induces $F \circ G$.*

Proof. Since N_R satisfies FDP, we have $(f')^2 \in N_R$, and hence (1) and (2) hold by Lemma 3.7.
(3) Let $G \in St_\alpha(R)$ be induced by $x + g(x)$, where $g \in N_R$. Then by FDP, $f'g' \in N_R$. Now we have for every $r, s \in R$, by Fact 3.1 and since $f, g \in N_R$,

$$\begin{aligned} G \circ F(r + s\,\alpha) &= G(r + s\,\alpha + sf'(r)\,\alpha) \\ &= (r + s\,\alpha + sf'(r)\,\alpha) + g(r + s\,\alpha + sf'(r)\,\alpha) \\ &= (r + s\,\alpha + sf'(r)\,\alpha) + (s + sf'(r))g'(r)\,\alpha \\ &= r + s\,\alpha + sf'(r)\,\alpha + sg'(r)\,\alpha \ \text{ by FDP.} \end{aligned}$$

Therefore $G \circ F$ is induced by the polynomial $x + f(x) + g(x)$. □

We prove now a special case of [1, Theorem 4.1].

Lemma 3.9. *Let $g \in R[x]$. Then g is a permutation polynomial on $R[\alpha]$ if and only if g is a permutation polynomial on R and $g'(r)$ is a unit for every $r \in R$.*

Proof. ($\Rightarrow$) Let $c \in R$. Then $c \in R[\alpha]$. Since g is a permutation polynomial over $R[\alpha]$, there exist $a, b \in R$ such that $g(a + b\alpha) = c$. Thus $g(a) + bg'(a)\alpha = c$ by Fact 3.1. So $g(a) = c$, whence g is surjective on the ring R. Hence g is a permutation polynomial on R.

Let $a \in R$ and suppose that $g'(a)$ is a non-unit in R. Then $g'(a)$ is a zero divisor of R. Let $b \in R$, $b \neq 0$, such that $bg'(a) = 0$. Then $g(a+b\alpha) = g(a)+bg'(a)\alpha = g(a)$, so g is not injective, which contradicts to the fact being bijective over $R[\alpha]$.
($\Leftarrow$) We need only to prove that g is injective. For this let $a, b, c, d \in R$ such that $g(a + b\alpha) = g(c + d\alpha)$. Then $g(a) + bg'(a)\alpha = g(c) + dg'(c)\alpha$ by Fact 3.1. Thus we have $g(a) = g(c)$ and $bg'(a) = dg'(c)$. Hence $a = c$ since g is a permutation polynomial on R. So, since $g'(a)$ is a unit in R, $b = d$ follows. □

We recall the following well-known result.

Lemma 3.10. [3, Theorem 3] *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$, and $g \in R[x]$. Then g is a permutation polynomial on R if and only if the following conditions hold:*

(1) *g is a permutation polynomial on $R/\mathfrak{m}$;*
(2) $g'(r) \not\equiv 0 \mod \mathfrak{m}$, *for all $r \in R$.*

Lemma 3.11. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$, and $g \in R[x]$. Then g is a permutation polynomial on $R[\alpha]$ if and only if g is a permutation polynomial on R.*

Proof. ($\Rightarrow$) Follows by Lemma 3.9.

($\Leftarrow$) Suppose that g is a permutation polynomial on R. Then for all $a \in R$, $g'(a) \not\equiv 0 \mod \mathfrak{m}$ by Lemma 3.10. Thus for all $a \in R$, $g'(a)$ is a unit in R since R is a local ring. Hence g is a permutation polynomial on $R[\alpha]$ by Lemma 3.9. □

Corollary 3.12. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$ and let $f \in N_R$. If F is the function induced by $x + f(x)$, then $F \in St_\alpha(R)$.*

In the rest of the paper let $N'_R = \{f \in N_R : f' \in N_R\}$. It is evident that N'_R is an ideal of $R[x]$ contained in N_R.

Lemma 3.13. *Let $g \in R[x]$. Then g is a null polynomial on $R[\alpha]$ if and only if $g \in N'_R$.*

Proof. By Fact 3.1, $g(a + b\alpha) = g(a) + bg'(a)\alpha$ for every $a, b \in R$.

($\Leftarrow$) Immediately.

($\Rightarrow$) Since g is null on $R[\alpha]$ we have that $g(a) + bg'(a)\alpha = 0$ for every $a, b \in R$. This is equivalent to $g(a) = bg'(a) = 0$ for every $a, b \in R$. Thus if $b = 1$, we have $g(a) = g'(a) = 0$ for very $a \in R$. Hence $g \in N'_R$. □

We are now ready to prove our main result for this section.

Proposition 3.14. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$. If N_R satisfies FDP, then*

$$St_\alpha(R) \cong {}^{N_R}\!/\!_{N'_R}.$$

Proof. Let $f \in N_R$, then obviously $[x + f(x)] \in St_\alpha(R)$ by Corollary 3.12, where $[x + f(x)]$ denotes the function induced by $x + f(x)$ on $R[\alpha]$.

Now define a function $\psi : N_R \longrightarrow St_\alpha(R)$ by $\psi(f) = [x + f(x)]$. By Proposition 3.6, ψ is surjective. Let $g \in N_R$. Then set $F_1 = [x + f(x)], F_2 = [x + g(x)]$ and $F_3 = [x + f(x) + g(x)]$. By Proposition 3.8, $F_1 \circ F_2 = F_3$. Therefore $\psi(f + g) = \psi(f) \circ \psi(g)$, whence ψ is a homomorphism. Hence ${}^{N_R}\!/\!_{\ker\psi} \cong St_\alpha(R)$ by the first isomorphism theorem.

Now, $\ker\psi = \{f \in N_R : [x + f(x)]$ is the identity permutation on $R[\alpha]\}$. By Lemma 3.13, $N'_R \subseteq \ker\psi$. On the other, if $f \in \ker\psi$, then $x + f(x)$ induces the identity on $R[\alpha]$. Hence $x + f(x) = x + h(x)$ for some null polynomial (on $R[\alpha]$) $h \in R[\alpha][x]$ by Lemma 3.4. Thus $f = h$ and f is a null polynomial on $R[\alpha]$. Since $f \in R[x]$ we have $f \in N'_R$ by Lemma 3.13. Therefore $\ker\psi \subseteq N'_R$. □

Remark 3.15. In [1], for the case $R = \mathbb{Z}_{p^n}$ the ring of integers modulo p^n, it was only proved that $|St_\alpha(\mathbb{Z}_{p^n})| = [N_{\mathbb{Z}_{p^n}} : N'_{\mathbb{Z}_{p^n}}]$, for every $n > 1$, and it was unclear whether $St_\alpha(\mathbb{Z}_{p^n})$and $N_{\mathbb{Z}_{p^n}}/N'_{\mathbb{Z}_{p^n}}$ are isomorphic or not. But, now Proposition 3.14 tells us they are isomorphic via a map induced by the function ψ defined in the above proof, when N_R satisfies FDP.

Corollary 3.16. *Let R be a local ring with nonzero maximal ideal $\mathfrak{m}$. The function $\psi : N_R \longrightarrow St_\alpha(R)$, defined by $\psi(f) = [x + f(x)]$ for every $f \in N_R$, is a homomorphism if and only if N_R satisfies FDP.*

Proof. ($\Leftarrow$) Follows by the same argument given in the proof of the previous proposition.
($\Rightarrow$) Assume that ψ is a homomorphism. Let $f, g \in N_R$. Put $F_1 = [x + f(x)], F_2 = [x + g(x)]$ and $F_3 = [x + f(x) + g(x)]$. Then $F_1, F_2, F_3 \in St_\alpha(R)$ by Corollary 3.12. We now consider $\psi(f+g) = [x+f(x)+g(x)] = F_3$. But, since ψ is a homomorphism by assumption, we have that $\psi(f + g) = \psi(f) \circ \psi(g) = F_1 \circ F_2$. Thus $F_1 \circ F_2 = F_3$. Now, for every $a, b \in R$, we have

$$F_1 \circ F_2(a + b\alpha) = a + b\alpha + b(g'(a) + f'(a) + f'(a)g'(a))\alpha,$$

and $F_3(a + b\alpha) = a + b\alpha + b(f'(a) + g'(a))\alpha$.
Hence $bf'(a)g'(a)\alpha = 0$ for every $a, b \in R$, which implies that $f'(a)g'(a) = 0$ for every $a \in R$. Thus $f'g' \in N_R$, and so N_R satisfies FDP. □

Remark 3.17. The function ψ defined in Corollary 3.16 seems natural in the sense that it sends every polynomial $g \in N_R$ to the function induced by $x + g(x)$ over $R[\alpha]$, however, we notice the following.

(1) When $R = \mathbb{F}_q$, the function ψ is not defined. For instance, take $f(x) = x^q - x \in N_{\mathbb{F}_q}$, but $F = [f(x) + x] = [x^q] \notin St_\alpha(\mathbb{F}_q)$ since F is not a permutation as $F(0) = F(\alpha) = 0$ (compare this with Remark 2.13-(1)).
(2) If $R = \mathbb{Z}_8$, the function ψ can be defined by Corollary 3.12. But, by Remark 2.13-(2), $N_{\mathbb{Z}_8}$ does not satisfy FDP. So ψ is not a homomorphism by Corollary 3.16.

Applying Proposition 3.14 to Corollary 2.14 gives the following result.

Corollary 3.18. *Let p be a prime number and n a positive integer.*

(1) *If $p > 2$, then $St_\alpha(\mathbb{Z}_{p^n}) \cong {N_{\mathbb{Z}_{p^n}}}/{N'_{\mathbb{Z}_{p^n}}}$ for every $1 < n \leq p + 1$.*
(2) *If $p = 2$, then $St_\alpha(\mathbb{Z}_4) \cong {N_{\mathbb{Z}_4}}/{N'_{\mathbb{Z}_4}}$.*

We conclude the paper by showing that the null ideal on dual numbers satisfies FDP. For this we recall the following fact from [1].

Lemma 3.19. [1, Theorem 3.5] *Let R be a commutative ring and let $A = R[\alpha]$ be the ring of dual numbers over R. Let $f = f_1 + f_2\,\alpha$, where $f_1, f_2 \in R[x]$. Then $f \in N_A$ if and only if $f_1 \in N'_R$ and $f_2 \in N_R$.*

Proposition 3.20. *Let R be a commutative ring and let $A = R[\alpha]$ be the ring of dual numbers over R. Then N_A satisfies FDP.*

Proof. Let $f, g \in N_A$. Then $f = f_1 + f_2\,\alpha$ and $g = g_1 + g_2\,\alpha$ for some $f_1, f_2, g_1, g_2 \in R[x]$ such that $f_1, g_1 \in N'_R$ and $f_2, g_2 \in N_R$ by Fact 3.2 and Lemma 3.19, respectively. But then $f'_1 g'_1 \in N'_R$ and $f'_1 g'_2 + f'_2 g'_1 \in N_R$. Thus, by Lemma 3.19,

$$f'g' = f'_1 g'_1 + (f'_1 g'_2 + f'_2 g'_1)\,\alpha \in N_A. \qquad \square$$

Acknowledgement. I would like to thank the reviewers for their suggestions and helpful comments. I am also very grateful to Chimere Anabanti for his useful comments on an earlier version of the manuscript.

References

[1] H. Al-Ezeh, A. A. Al-Maktry and S. Frisch, *Polynomial functions on rings of dual numbers over residue class rings of the integers*, Math. Slovaca, 71(5) (2021), 1063-1088.

[2] B. R. McDonald, Finite rings with identity, Pure and Applied Mathematics, Vol. 28, Marcel Dekker, Inc., New York, 1974.

[3] A. A. Necaev, *Polynomial transformations of finite commutative local rings of principal ideals*, Math. Notes, 27(5-6) (1980), 425-432, translate from Mat. Zametki, 27(6) (1980), 885-897.

[4] W. Nöbauer, *Über die Ableitungen der Vollideale*, Math. Z., 75 (1961), 14-21.

[5] M. W. Rogers and C. Wickham, *Polynomials inducing the zero function on local rings*, Int. Electron. J. Algebra, 22 (2017), 170-186.

Amr Ali Al-Maktry
Institute of Analysis and Number Theory (5010)
Technische Universität Graz
kopernikusgasse 24/II
8010 Graz, Austria
e-mail: almaktry@math.tugraz.at