NILPOTENT POLYNOMIALS AND NILPOTENT COEFFICIENTS

THOMAS L. DRAPER, PACE P. NIELSEN, AND JANEZ ŠTER

ABSTRACT. For any ring R, let $\mathrm{Nil}(R)$ denote the set of nilpotent elements in R, and for any subset $S \subseteq R$, let $S[x]$ denote the set of polynomials with coefficients in S. Due to a celebrated example of Smoktunowicz, there exists a ring R such that $\mathrm{Nil}(R[x])$ is a proper subset of $\mathrm{Nil}(R)[x]$. In this paper we give an example in the converse direction: there exists a ring R such that $\mathrm{Nil}(R)[x]$ is a proper subset of $\mathrm{Nil}(R[x])$. This is achieved by constructing a ring R with $\mathrm{Nil}(R)^2 = 0$ and a polynomial $f \in R[x] \setminus \mathrm{Nil}(R)[x]$ satisfying $f^2 = 0$. The smallest possible degree of such a polynomial is seven. The example we construct answers an open question of Antoine related to Armendariz rings.

1. INTRODUCTION

In this paper rings are associative, but nonunital and noncommutative in general, unless otherwise stated. If R is a commutative ring, an easy exercise shows that

$$\mathrm{Nil}(R[x]) = \mathrm{Nil}(R)[x]; \tag{1.1}$$

the nilpotent polynomials are exactly those polynomials with nilpotent coefficients. For noncommutative rings this may easily fail. For instance, let R be the 2×2 matrix ring over any nonzero unital ring, and in the polynomial ring $R[x]$ consider the two polynomials

$$f = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} x \quad \text{and} \quad g = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} x + \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix} x^2.$$

One easily checks that $f \in \mathrm{Nil}(R)[x] \backslash \mathrm{Nil}(R[x])$ and $g \in \mathrm{Nil}(R[x]) \backslash \mathrm{Nil}(R)[x]$, therefore neither of the inclusions in (1.1) holds. This raises a natural question: if one of the inclusions in (1.1) holds, does the other hold as well? In other words, does there exist a ring R satisfying $\mathrm{Nil}(R[x]) \subsetneq \mathrm{Nil}(R)[x]$ or $\mathrm{Nil}(R[x]) \supsetneq \mathrm{Nil}(R)[x]$?

The question whether the inclusion

$$\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x] \tag{1.2}$$

implies equality turns out to be equivalent to Amitsur's classical problem asking if the polynomial ring over a nil ring is nil. In fact, we show in Proposition 2.8 that if a ring R satisfies (1.2) and this inclusion is proper, then R contains a nil subring S such that $S[x]$ is not nil. While Amitsur proved in [2, Theorem 2] that any nil algebra over an *uncountable* field has a nil polynomial ring, in [20] Smoktunowicz constructed, for any countable field F, a nil F-algebra whose polynomial ring is not nil. Answering Amitsur's question in the negative, Smoktunowicz's example thus provides a ring such that the inclusion (1.2) holds and is proper.

2020 *Mathematics Subject Classification.* Primary 16N40, Secondary 16S10, 16S15, 16S36, 16U99.

Key words and phrases. Armendariz ring, nilpotent, polynomial ring, power series ring, zero-divisors.

The main goal in this paper is to give an example for the other direction, namely a ring R such that

$$\mathrm{Nil}(R[x]) \supseteq \mathrm{Nil}(R)[x] \tag{1.3}$$

and such that this inclusion is proper. The ring we construct is unital, has characteristic 2 and satisfies $\mathrm{Nil}(R)^2 = 0$, hence $\mathrm{Nil}(R)$ is a subring of R with trivial multiplication. Remarkably, we show that the inclusion (1.3) does imply equality if R is an algebra over an *infinite* field.

As further motivation, we present here some historical background related to our work. Following Rege and Chhawchharia [19], a unital ring R is called *Armendariz* when for any two polynomials $f = \sum_{i=0}^{m} a_i x^i$ and $g = \sum_{j=0}^{n} b_j x^j$ in $R[x]$, if $fg = 0$ then $a_i b_j = 0$ for all integers $i, j \geq 0$. The name is given after Armendariz who showed in [5, Lemma 1] that reduced rings (i.e., rings without nonzero nilpotents) satisfy this condition. Antoine proved in [3, Corollaries 5.2 and 3.3] that every Armendariz unital ring R satisfies (1.1) and the set of nilpotents $\mathrm{Nil}(R)$ forms a subring of R.

Rings R with $\mathrm{Nil}(R)$ a subring were studied in [11, 21] and called *NR rings* there. It was shown in [21, Theorem 2.1] that $\mathrm{Nil}(R)$ is a subring whenever it is additively closed. (It is currently unknown whether $\mathrm{Nil}(R)$ is a subring whenever it is multiplicatively closed.) An interesting connection between the condition (1.1) and the NR condition is the following equivalence (see [21, Corollary 2.5] and [9, Proposition 3.4]): *a ring R satisfies* (1.1) *if and only if $R[x]$ is a NR ring.* As a subring of a NR ring is clearly NR, this shows that every ring satisfying (1.1) is NR.

Motivated by Antoine's work in [3], Kwak and Lee in [15] studied rings R satisfying the inclusion (1.2), calling them *CN rings*. We note that Theorem 4.3 below shows that any NR ring that is an algebra over an *infinite* field satisfies (1.2). Thus, that theorem simplifies some of the computations in [15], if one is willing to work over infinite fields rather than general fields.

To give one final motivation for this study, we note the parallel situation of the Amitsur property on radicals, particularly nilradicals. There are numerous recent papers on this topic; see the references in [12] for a fairly thorough list.

The structure of the paper is as follows. In Section 2 we prove various implications between the inclusions (1.2), (1.3), and the NR property of a ring R. We show that the inclusion (1.3) implies the NR condition of a ring R (see Proposition 2.1), as does the inclusion (1.2) under an additional mild assumption that the ring R satisfies Köthe's conjecture or has characteristic 2 (see Corollaries 2.3 and 2.7). We also describe how this is related to Amitsur's problem.

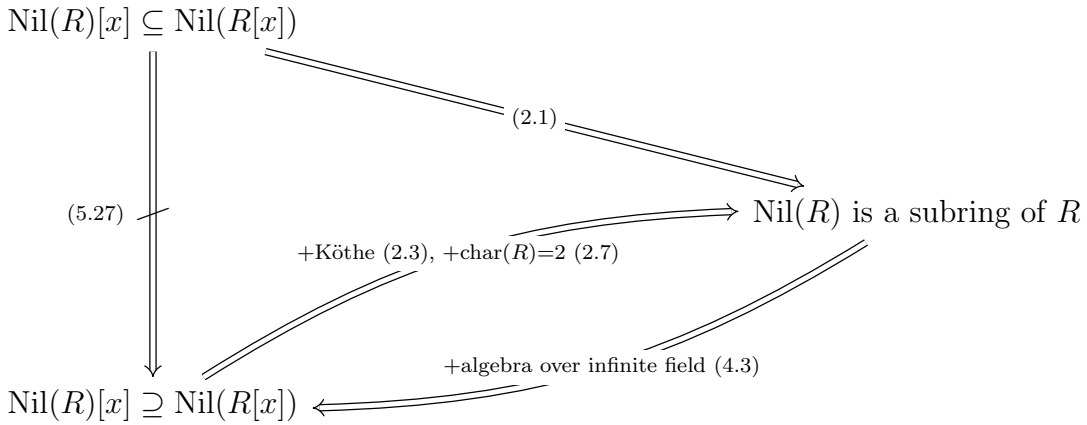
In Section 3 we consider an analogue of our problem for power series, and construct a ring R such that $\mathrm{Nil}(R)[\![x]\!]$ is a proper subset of $\mathrm{Nil}(R[\![x]\!])$. Here $R[\![x]\!]$ denotes the usual power series ring. We use the tools developed in this section again when considering polynomial rings.

In Section 4 we describe numerous conditions where nilpotent polynomials must have nilpotent coefficients under the assumption that R satisfies the NR property. This holds for algebras over infinite fields (see Theorem 4.3), as well as for polynomials of small degree. In Section 5 we construct our main example, a ring R such that the inclusion (1.3) is proper (see Theorem 5.27). As the main step in the proof, we characterize zero products in R, using

a case analysis. Our example answers a question posed in [3] and [4], asking if there exists a unital NR ring with zero upper nilradical that is not an Armendariz ring (see Remark 5.29).

In Section 6 we provide an Euler diagram that describes the various connections between the classes of rings satisfying conditions (1.2), (1.3), and other important properties studied in the paper.

Some of our main results are summarized by the following implication diagram:



In this paper $\mathbb{N}$ denotes the set of nonnegative integers. While rings considered in the paper will be nonunital in general, many of our examples will be made unital for convenience only. When we speak of a unital subring of a unital ring, we mean that the units in both rings coincide. As above, if R is a ring and $S \subseteq R$ is any subset, then $\mathrm{Nil}(S)$, $S[x]$ and $S[\![x]\!]$ denote the set of nilpotent elements in S, the set of polynomials, and the set of power series with coefficients in S. For simplicity, we treat the zero polynomial as having degree 0.

2. Preliminary Results on Inclusions Between $\mathrm{Nil}(R[x])$ and $\mathrm{Nil}(R)[x]$

Recall that any ring satisfying $\mathrm{Nil}(R[x]) = \mathrm{Nil}(R)[x]$ is a NR ring, i.e., nilpotents form a subring of R (see [21, Corollary 2.5] for a stronger statement). If we weaken the equality to the inclusion (1.3), then we still have the same conclusion.

Proposition 2.1. *If a ring R satisfies $\mathrm{Nil}(R)[x] \subseteq \mathrm{Nil}(R[x])$ then $\mathrm{Nil}(R)$ is a subring of R.*

Proof. Let $a, b \in \mathrm{Nil}(R)$. By assumption, the polynomial $a+bx$ is nilpotent. Evaluating at 1, we get that $a+b \in \mathrm{Nil}(R)$. (This argument also appears in the proof of [10, Theorem 2.11(1)]. Note that the evaluation map $R[x] \to R$, $f \mapsto f(1)$, is a well-defined homomorphism even when R is not unital.) This shows that $\mathrm{Nil}(R)$ is an additive subgroup. When $\mathrm{Nil}(R)$ is additively closed, then it a subring by [21, Theorem 2.1], a fact we will use freely. □

As for the converse inclusion, we have the following partial result:

Proposition 2.2. *If a ring R satisfies $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$ then $\mathrm{Nil}(R)$ is closed under commutators.*

Proof. Take $a, b \in \mathrm{Nil}(R)$, and embed R into a unital ring R_1. The polynomial $1 - ax$ is invertible in $R_1[x]$, with the inverse $(1-ax)^{-1} = 1 + ax + a^2x^2 + \cdots + a^{n-1}x^{n-1}$, where $a^n = 0$. Since b is a nilpotent, it follows that

$$f = (1 + ax + a^2x^2 + \cdots + a^{n-1}x^{n-1})b(1 - ax)$$

is a nilpotent polynomial in $R_1[x]$. Note that $f \in R[x]$, so $f \in \mathrm{Nil}(R[x])$, and hence by assumption $f \in \mathrm{Nil}(R)[x]$. We compute directly that the coefficient of f in degree 1 is $ab - ba$. Hence $ab - ba \in \mathrm{Nil}(R)$, as claimed. □

A ring R is said to satisfy *Köthe's conjecture* if every nil left ideal of R lies in $\mathrm{Nil}^*(R)$ (the upper nilradical of R). It is an open question if every ring satisfies Köthe's conjecture. By [21, Remark 2.2], if R satisfies Köthe's conjecture then $\mathrm{Nil}(R)$ being closed under commutators implies that $\mathrm{Nil}(R)$ is a subring of R. Thus we have:

Corollary 2.3. *Let R be a ring such that $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$ and such that R satisfies Köthe's conjecture. Then $\mathrm{Nil}(R)$ is a subring of R.* □

We were unable to prove the above statement without the additional assumption that R satisfies Köthe's conjecture. Thus we ask:

Question 2.4. If a ring R satisfies $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$, is $\mathrm{Nil}(R)$ a subring of R?

There is one further special case where we can give a positive answer to Question 2.4, which is an easy consequence of the following two lemmas.

Lemma 2.5. *If $\mathrm{Nil}(R)$ is closed under the map $(a, b) \mapsto ab + ba + b^2$, then $\mathrm{Nil}(R)$ is closed under addition.*

Proof. Given $a, b \in \mathrm{Nil}(R)$ we want to show that $a + b \in \mathrm{Nil}(R)$. We work by induction on the index of nilpotency of a. If that index is 1 then $a = 0$ and there is nothing to prove. For the inductive step, note that $(a + b)^2 = a^2 + (ab + ba + b^2)$ with $a^2, ab + ba + b^2 \in \mathrm{Nil}(R)$. Since the index of nilpotency of a^2 is smaller than that of a, we get $(a + b)^2 \in \mathrm{Nil}(R)$, hence $a + b \in \mathrm{Nil}(R)$ as needed. □

Lemma 2.6. *If $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$, then $\mathrm{Nil}(R)$ is closed under the map $(a, b) \mapsto ab - ba + b^2$.*

Proof. Let $a, b \in \mathrm{Nil}(R)$. As in the proof of Proposition 2.2, we embed R into a unital ring R_1. Considering that $(1 - ax)^{-1} = 1 + ax + \cdots + a^{n-1}x^{n-1}$ in $R_1[x]$ (where $a^n = 0$), and that $b + b^2x \in \mathrm{Nil}(R_1[x])$, we get that

$$f = (1 + ax + \cdots + a^{n-1}x^{n-1})(b + b^2x)(1 - ax)$$

is a nilpotent polynomial in $R_1[x]$. As $f \in R[x]$, it follows that $f \in \mathrm{Nil}(R[x])$ and hence $f \in \mathrm{Nil}(R)[x]$. The coefficient of f in degree 1 is exactly $ab - ba + b^2$. □

Corollary 2.7. *If R is a ring satisfying $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$ and the characteristic of R is 2, then $\mathrm{Nil}(R)$ is closed under addition and hence a subring of R.* □

With the above results at hand, we can show that the problem of finding a ring with $\mathrm{Nil}(R[x]) \subsetneq \mathrm{Nil}(R)[x]$ is equivalent to Amitsur's problem of finding a nil ring such that the polynomial ring is not nil (note that this problem was solved in [20], see also [17]). One direction is clear; if we are given a nil ring R such that $R[x]$ is not nil, then the ring R itself satisfies $\mathrm{Nil}(R[x]) \subsetneq \mathrm{Nil}(R)[x]$. To get also the converse direction, we show the following:

Proposition 2.8. *If a ring R satisfies $\mathrm{Nil}(R[x]) \subsetneq \mathrm{Nil}(R)[x]$ then R contains a nil subring S such that $S[x]$ is not nil.*

Proof. First assume that R satisfies Köthe's conjecture. Then $S = \mathrm{Nil}(R)$ is a subring of R by Corollary 2.3. We have $\mathrm{Nil}(S[x]) \subseteq \mathrm{Nil}(R[x]) \subsetneq \mathrm{Nil}(R)[x] = S[x]$, hence $S[x]$ is not nil.

Now assume that R does not satisfy Köthe's conjecture. Then there exists a nil left ideal S in R such that $S \nsubseteq \mathrm{Nil}^*(R)$. We claim that $S[x]$ is not nil. Indeed, otherwise $S[x]$ is a radical ring. By the argument given in the first paragraph of the proof of [14, Theorem 2], it follows that $S \subseteq I$ for a nil two-sided ideal I of R, a contradiction. □

Remark 2.9. Note that if R is an algebra over an uncountable field, then R must satisfy Köthe's conjecture by [1, Theorem 10]. Hence in this case we have $S = \mathrm{Nil}(R)$ in the above proof, so that S is actually a subalgebra of R. On the other hand, polynomials over a nil algebra over an uncountable field are nil by a result of Amitsur [2, Theorem 2]. This shows that the inclusion $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$ cannot be proper if R is an algebra over an uncountable field.

3. Power Series

The problems described in Section 1 retain their meaning if we replace polynomial rings with power series rings. Thus, we can ask if there exists a ring R satisfying $\mathrm{Nil}(R[\![x]\!]) \subsetneq \mathrm{Nil}(R)[\![x]\!]$, or a ring satisfying $\mathrm{Nil}(R[\![x]\!]) \supsetneq \mathrm{Nil}(R)[\![x]\!]$. One can quickly observe that Smoktunowicz's example of a nil ring with polynomials not nil answers the first of these two problems. The following answers the second problem:

Example 3.1. *There exists a ring R satisfying* $\mathrm{Nil}(R)^2 = 0$ *and* $\mathrm{Nil}(R)[\![x]\!] \subsetneq \mathrm{Nil}(R[\![x]\!])$.

Proof. We take the ring from [4, Example 1]. Let $R = \mathbb{Z}\langle a, b : a^2 = 0\rangle$, the unital $\mathbb{Z}$-algebra generated by a, b subject to the relation $a^2 = 0$. It is known that the left and right zero-divisors in R are, respectively, exactly Ra and aR; see [8, Example 9.3]. Hence $\mathrm{Nil}(R) = Ra \cap aR$ and therefore $\mathrm{Nil}(R)^2 = 0$. In particular, this implies $\mathrm{Nil}(R)[\![x]\!] \subseteq \mathrm{Nil}(R[\![x]\!])$. To find a series $f \in \mathrm{Nil}(R[\![x]\!]) \setminus \mathrm{Nil}(R)[\![x]\!]$, consider

$$\begin{aligned} f &= (1-bx)^{-1}a(1-bx) = (1 + bx + b^2x^2 + \cdots)a(1-bx) \\ &= a + (ba-ab)x + b(ba-ab)x^2 + b^2(ba-ab)x^3 + \cdots \end{aligned}$$

Since $a^2 = 0$, we have $f^2 = 0$. However, not all coefficients of f are nilpotent since $ba - ab \notin \mathrm{Nil}(R)$. □

Remark 3.2. By Antoine [4, Example 1], the ring in the above example is Armendariz, hence by [3, Corollary 5.2] it satisfies $\mathrm{Nil}(R[x]) = \mathrm{Nil}(R)[x]$.

In the following we will give an alternative, universal construction of a ring R with $\mathrm{Nil}(R)^2 = 0$ and with a square-zero power series whose coefficients are not all nilpotent (which implies $\mathrm{Nil}(R)[\![x]\!] \subsetneq \mathrm{Nil}(R[\![x]\!])$). The tools developed in the proof of this example will be needed later when considering polynomials.

Given any power series $f = \sum_{i\in\mathbb{N}} a_i x^i$, we see that $f^2 = 0$ if and only if the following relations hold among the coefficients:

$$a_k a_0 = -\sum_{i=0}^{k-1} a_i a_{k-i}, \text{ for each } k \in \mathbb{N}. \tag{3.3}$$

Let R_0 denote $\mathbb{Z}\langle a_i\,(i \in \mathbb{N})\rangle$, the unital ring freely generated by noncommuting variables indexed by $\mathbb{N}$. Let I be the ideal of R_0 generated by the relations in (3.3), and define

$$R = R_0/I.$$

Thus, R is the coefficient ring of the universal construction of a unital power series ring with a square-zero element.

We can well-order the generating variables in R_0, by the usual order on the indices, so that

$$a_0 \prec a_1 \prec a_2 \prec \dots.$$

Viewing this as giving a lexicographical order to the variables, we let $\prec$ also denote the resulting *shortlex* order (also called the "length-lexicographical" order) on the monomials of R_0. In other words, the order $\prec$ on monomials in R_0 is first determined by total degree, and monomials of the same degree are ordered lexicographically. Notice that each monomial that appears on the right side of the equality in (3.3) is smaller in this order than the monomial that appears on the left side. The shortlex order is a strict monoid well-ordering on the free monoid generated by the set $\{a_0, a_1, \dots\}$.

We view the relations in (3.3) as a reduction system, allowing us to replace the monomial on the left side of the equality with the expression on the right side. (Note that the reductions are homogeneous in the total degree of a monomial and homogeneous in the total sum of the indices of a monomial.) To show that repeatedly applying these reductions (a finite number of times until no more reductions can be made) always produces a unique reduced form for elements of R, it suffices to check that each overlap $(a_\ell a_0)a_0 = a_\ell(a_0^2)$, for $\ell \in \mathbb{N}$, "resolves" in the terminology of Bergman's Diamond Lemma [7]. The right side of the overlap reduces immediately to 0, for if $k = 0$ then (3.3) says $a_0^2 = 0$. The left side reduces to

$$-\left(\sum_{i=0}^{\ell-1} a_i a_{\ell-i}\right) a_0 = \sum_{i=0}^{\ell-1}\sum_{j=0}^{\ell-i-1} a_i a_j a_{\ell-i-j} = \sum_{i=0}^{\ell-1}\sum_{j=1}^{\ell-i-1} a_i a_j a_{\ell-i-j} - \sum_{i=0}^{\ell-1}\sum_{k=0}^{i-1} a_k a_{i-k} a_{\ell-i},$$

where the second equality comes from handling the $j = 0$ terms. Both of the final double sums are (up to relabeling the indices) equal to

$$\sum_{\substack{i,j,k\in\mathbb{N}\,:\,j,k\neq 0,\\ i+j+k=\ell}} a_i a_j a_k.$$

Thus the two double sums cancel, showing that the overlap resolves as needed.

Hereafter, abusing notation slightly, we will identify each variable a_i with its image in the factor ring R. In other words, we now assume that the variables satisfy the relations given in (3.3). Accordingly, we can write every element in R in reduced form as a $\mathbb{Z}$-linear combination of monomials of the form

$$m = a_{i_1} a_{i_2} \cdots a_{i_k}$$

where $k \in \mathbb{N}$, and $i_\ell \neq 0$ whenever $\ell \neq 1$. For every $r \in R$, let $\operatorname{supp}(r) \subseteq R$ (the *support* of r) denote the set of all monomials m of the above form which appear with nonzero coefficient in the unique reduced form for r. Note that $\operatorname{supp}(r) = \emptyset$ exactly when $r = 0$.

With the help of the next result we will be able to describe the set of nilpotents in R.

Proposition 3.4. *Let R be the unital ring generated by variables a_i (for $i \in \mathbb{N}$) subject only to the relations given in (3.3). If $r, s \in R \setminus \{0\}$ satisfy $rs = 0$, then $r \in Ra_0$ and $s \in a_0R$.*

Proof. We first prove that R can be embedded in the ring $R' = \mathbb{Z}\langle a, b \,:\, a^2 = 0\rangle$. By the proof of Example 3.1, we know that $f = a + \sum_{i=1}^{\infty} b^{i-1}(ba - ab)x^i$ is a square-zero power series over R' and hence its coefficients satisfy the relations (3.3). This allows us to define

a unital ring homomorphism $\varphi\colon R \to R'$ by setting $\varphi(a_0) = a$ and $\varphi(a_i) = b^{i-1}(ba - ab)$ for each integer $i \geq 1$.

We claim that φ is injective. Pick any $r \in R \setminus \{0\}$ and choose any monomial $m = a_{i_1}a_{i_2}\cdots a_{i_k} \in \operatorname{supp}(r)$. We have

$$\varphi(m) = \begin{cases} b^{i_1-1}(ba-ab)b^{i_2-1}(ba-ab)\cdots b^{i_k-1}(ba-ab) & \text{if } i_1 \neq 0, \\ ab^{i_2-1}(ba-ab)\cdots b^{i_k-1}(ba-ab) & \text{if } i_1 = 0. \end{cases} \tag{3.5}$$

Let $<$ denote the lexicographical order on the set of reduced monomials in R' (which is not to be confused with the shortlex order $\prec$ on R_0). For any $r' \in R'$, let $\operatorname{supp}(r')$ denote the set of all reduced monomials in R' which appear with nonzero coefficient in the reduced form for r'. (The reader should be able to tell from context whether support is being taken in R or in R'.) From (3.5) we see that the maximal element in $\operatorname{supp}(\varphi(m))$ with respect to $<$ is, in both cases,

$$\max \operatorname{supp}(\varphi(m)) = b^{i_1}ab^{i_2}a\cdots b^{i_k}a.$$

Note that this monomial uniquely determines m. Hence, picking m' to be the $<$-maximal element of $\{\max \operatorname{supp}(\varphi(m)) : m \in \operatorname{supp}(r)\}$, we conclude that m' cannot cancel with any other term in $\varphi(r)$. Hence $\varphi(r) \neq 0$, showing that φ is indeed injective.

To finish the proof, pick now any $r, s \in R \setminus \{0\}$ with $rs = 0$. By left-right symmetry in the universal property defining R, it suffices to show only that $s \in a_0R$. Since φ is injective, $\varphi(s)$ is a right zero-divisor in R' and hence $\varphi(s) \in aR'$ by [8, Example 9.3]. (One of the referees kindly pointed out that one can also use the earlier result [6, Lemma 2.16] here, as well as in Example 3.1.) On the other hand, the previous paragraph shows that if $\operatorname{supp}(s)$ contains a monomial not beginning with a_0 then $\operatorname{supp}(\varphi(s))$ contains a monomial beginning with b and hence $\varphi(s) \notin aR'$. Thus we must have $s \in a_0R$ as desired. □

The following theorem is now immediate.

Theorem 3.6. *If R is the unital ring generated by variables a_i (for $i \in \mathbb{N}$) subject only to the relations* (3.3)*, then* $\operatorname{Nil}(R) = a_0R \cap Ra_0$ *and hence* $\operatorname{Nil}(R)^2 = 0$*. In particular,* $\operatorname{Nil}(R)[\![x]\!] \subsetneq \operatorname{Nil}(R[\![x]\!])$. □

Remark 3.7. The ring R above is Armendariz since it is a subring of an Armendariz ring $\mathbb{Z}\langle a, b : a^2 = 0\rangle$. Hence it satisfies $\operatorname{Nil}(R[x]) = \operatorname{Nil}(R)[x]$.

The universal construction above is isomorphic to a factor ring of a very special type of skew differential polynomial ring. To recall the definition of skew differential polynomials, let S be a ring and let $\sigma\colon S \to S$ be a ring endomorphism. Further, let δ be a *right σ-skew derivation* on S, that is, an additive map $\delta\colon S \to S$ satisfying the multiplication rule

$$\delta(st) = s\delta(t) + \delta(s)\sigma(t), \text{ for each } s, t \in S.$$

Note that when S is unital and σ is a unital homomorphism, this rule implies $\delta(1) = 0$. Let $S[x; \sigma, \delta]$ denote the set of all formal right polynomials in the variable x (i.e., the coefficients appear on the right of the variable), which take the form

$$f = s_0 + xs_1 + \cdots + x^n s_n$$

with $s_0, s_1, \ldots, s_n \in S$ and $n \in \mathbb{N}$. We define addition on these polynomials componentwise, and multiplication is induced by the multiplication in S, along with the equality

$$sx = \delta(s) + x\sigma(s), \text{ for each } s \in S.$$

Under these operations $S[x;\sigma,\delta]$ is a ring called the *right σ-skew δ-differential polynomial ring*. (Another name for this construction is a "generalized Ore extension." For more information on this type of skew polynomial rings, and for additional references, we refer the reader to [16].)

Proposition 3.8. *Let R be a unital ring and assume that $R = S \oplus yS$ (as an Abelian group) for some unital subring S and some element $y \in R$. Further, assume that the right annihilator of y in S is zero. Let $\sigma, \delta \colon S \to S$ be the maps defined by the equality*

$$sy = \delta(s) + y\sigma(s), \quad \text{for each } s \in S. \tag{3.9}$$

Then the following hold:

1. *σ is a unital ring endomorphism and δ is a right σ-skew derivation on S,*
2. *σ is an automorphism if and only if $R = S \oplus Sy$ and the left annihilator of y in S is zero, and*
3. *if $y^2 = 0$, then $\delta^2 = \sigma \circ \delta + \delta \circ \sigma = 0$ and R is isomorphic to the factor ring $S[x;\sigma,\delta]/(x^2)$.*

Proof. (1) Using (3.9) we have

$$(s+t)y = \delta(s+t) + y\sigma(s+t),$$

but also by distributivity and two more uses of (3.9) we obtain

$$(s+t)y = sy + ty = \delta(s) + y\sigma(s) + \delta(t) + y\sigma(t) = (\delta(s) + \delta(t)) + y(\sigma(s) + \sigma(t)).$$

From the direct sum decomposition of R, we see that σ and δ are additive. Similarly, working with $(st)y$ in two ways (using (3.9), associativity in R, and the direct sum decomposition of R) we get that σ is multiplicative and δ satisfies the skew derivation axiom. Finally, computing $1y$ using (3.9) we get $\sigma(1) = 1$ (and $\delta(1) = 0$).

(2) Assume that σ is an automorphism and let $s \in S$ be arbitrary. The equality (3.9) then implies

$$ys = \sigma^{-1}(s)y - \delta(\sigma^{-1}(s)) \in S + Sy.$$

Therefore $R = S + Sy$. Moreover, if $sy \in S \cap Sy$ then $\delta(s) + y\sigma(s) \in S$, and hence $y\sigma(s) \in S$. However, $S \cap yS = \{0\}$, so $\sigma(s) = 0$, which implies $s = 0$. Therefore $S \cap Sy = \{0\}$. This computation also shows that if $sy = 0$ then $s = 0$.

Conversely, assume $R = S \oplus Sy$ and assume that the left annihilator of y in S is zero. For each $s \in S$ we can then write

$$ys = \delta'(s) + \sigma'(s)y$$

for some maps $\sigma', \delta' \colon S \to S$. We find

$$ys = \delta'(s) + \sigma'(s)y = \delta'(s) + \delta(\sigma'(s)) + y\sigma(\sigma'(s)).$$

In particular, $\sigma \circ \sigma' = \mathrm{id}_S$, and similarly $\sigma' \circ \sigma = \mathrm{id}_S$. Therefore σ is an automorphism.

(3) Assuming $y^2 = 0$, we have for any $s \in S$ that

$$\begin{aligned} 0 &= sy^2 = (\delta(s) + y\sigma(s))y = \delta^2(s) + y\sigma(\delta(s)) + y\delta(\sigma(s)) + y^2\sigma^2(s) \\ &= \delta^2(s) + y(\sigma(\delta(s)) + \delta(\sigma(s))). \end{aligned}$$

Hence $\delta^2 = \sigma \circ \delta + \delta \circ \sigma = 0$.

To prove the isomorphism $R \cong S[x;\sigma,\delta]/(x^2)$, we first check that $I = x^2 S[x;\sigma,\delta]$ is a two-sided ideal in $S[x;\sigma,\delta]$, so that $I = (x^2)$. For this, it suffices to see that $sx^2 \in I$ for every $s \in S$, which can be proved by computing that $sx^2 = x^2\sigma^2(s)$ (using $sx = \delta(s) + x\sigma(s)$,

and the work in the previous paragraph). Hence $I = (x^2)$ as claimed. One now verifies by another direct computation that the map

$$R \to S[x;\sigma,\delta]/I,\ s_0 + ys_1 \mapsto s_0 + xs_1 + I$$

is the needed isomorphism. □

Let R be the unital ring as described in Proposition 3.4, and let S be the unital subring generated by the a_i for $i \in \mathbb{N}_{\geq 1}$. We clearly have $R = S \oplus a_0 S$, from the reduced form for elements. Moreover, the right annihilator of a_0 in S is zero. Thus, taking $y = a_0$, the previous proposition applies in full, since $a_0^2 = 0$. Denoting the induced endomorphism σ and the right σ-skew derivation δ, we conclude that R is isomorphic to the factor ring $S[x;\sigma,\delta]/(x^2)$. By directly considering the relations (3.3), we see that σ acts on the generators of S by the action $a_i \mapsto -a_i$ (for each integer $i \geq 1$). Hence σ is an automorphism with $\sigma^2 = \mathrm{id}_S$.

The following proposition cleanly characterizes zero products in rings as described by Proposition 3.8, when the ring is subject to some additional conditions.

Proposition 3.10. *Let R be a ring as in Proposition 3.8, with $y^2 = 0$, and with σ an automorphism. If elements $u, v \in R \setminus \{0\}$ satisfy $uv = 0$, then $u \in Sy$ and $v \in yS$, as long as*

$(*)$ *for any $r, s, t \in S$, if $rs + \delta(r)t = 0$ then $r = 0$ or $s = 0$.*

Proof. Let $uv = 0$ with $u, v \in R \setminus \{0\}$, and assume that $(*)$ holds. Notice that $(*)$ implies that S is a domain (by taking $t = 0$ in its statement).

Our first goal is to show that $v \in yS$. For this purpose we may assume that $u \in yS$, since otherwise $yu \neq 0$ and we may replace u by yu. Writing $u = yr$ and $v = s + yt$ with $r, s, t \in S$, we now have

$$0 = uv = yr(s + yt) = y(rs + \delta(r)t).$$

Since $r \neq 0$, $(*)$ gives $s = 0$ and hence $v \in yS$.

In order to see that $u \in Sy$, write u as a "left polynomial" in y (using the fact that σ is an automorphism), say $u = r + sy$ for some $r, s \in S$, and $v = yt$ with $t \in S \setminus \{0\}$. We find

$$0 = uv = (r + sy)yt = ryt = \delta(r)t + y\sigma(r)t.$$

In particular, $\sigma(r)t = 0$. Since S is a domain, we have $\sigma(r) = 0$, and hence $r = 0$. Thus $u \in Sy$ as claimed. □

It is possible to now reprove Proposition 3.4 by showing that condition $(*)$ holds, when S is taken as in the paragraphs preceding Proposition 3.10. We leave that mundane task to the enthusiastic reader. However, the motivation for providing Proposition 3.10 is not merely to give an alternate way to handle Proposition 3.4, but primarily to provide some machinery that will aid us in working with our main example in Section 5.

4. Polynomials of Small Degree

In this and the next section we return to our main problem of finding a ring R such that $\mathrm{Nil}(R)[x]$ is a proper subset of $\mathrm{Nil}(R[x])$. Note that by Proposition 2.1 the inclusion $\mathrm{Nil}(R)[x] \subseteq \mathrm{Nil}(R[x])$ implies that $\mathrm{Nil}(R)$ is a subring of R. We will show that the condition that $\mathrm{Nil}(R)$ is a subring in many cases implies the *converse* inclusion $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$. For example, this will hold if R is an algebra over an infinite field. Moreover, assuming that

$\mathrm{Nil}(R)$ is a subring, we will show that polynomials $f \in \mathrm{Nil}(R[x])$ of sufficiently small degree and small index of nilpotency will satisfy $f \in \mathrm{Nil}(R)[x]$.

In this section, it will be convenient to work with algebras rather than rings. Thus, throughout the section, k will be a commutative unital ring, and R in most cases will be a (not necessarily unital) k-algebra (i.e., R is a ring, with the structure of a left k-module, such that $1_k \cdot a = a$ and $\lambda \cdot (ab) = (\lambda \cdot a)b = a(\lambda \cdot b)$, for each $\lambda \in k$ and $a, b \in R$). Note that in this case, saying that $\mathrm{Nil}(R)$ is a subring is the same as saying that it is a subalgebra. Further, this loses no generality, since every ring is a $\mathbb{Z}$-algebra.

In what follows, for any (ordered) collection $\Lambda = (\lambda_1, \lambda_2, \ldots, \lambda_n) \in k^n$ of n elements in k, we denote by

$$V_\Lambda = \prod_{1 \le i < j \le n} (\lambda_j - \lambda_i)$$

the *Vandermonde determinant* associated to $\lambda_1, \ldots, \lambda_n$, which is the determinant of the $n \times n$ Vandermonde matrix $(\lambda_i^{j-1})_{i,j}$. (As is usual, we take $\lambda^0 = 1$, for any $\lambda \in k$.)

Proposition 4.1. *Let R be a k-algebra such that $\mathrm{Nil}(R)$ is a subalgebra of R. Let Λ be a collection of $n \ge 1$ elements in k, and let $f \in R[x]$ be a polynomial with degree at most n. If $f^d \in \mathrm{Nil}(R)[x]$ for some integer $d \ge 1$, then $V_\Lambda f \in \mathrm{Nil}(R)[x]$.*

Proof. Write $\Lambda = (\lambda_1, \ldots, \lambda_n)$ and $f = \sum_{j=0}^n a_j x^j$ for some elements $\lambda_i \in k$ and $a_j \in R$. Since $f^d \in \mathrm{Nil}(R)[x]$, then for each λ_i we know that $f(\lambda_i)^d \in \mathrm{Nil}(R)$, as this is a k-linear combination of nilpotent elements. Hence $f(\lambda_i)$ is nilpotent. Moreover, a_n is nilpotent (since a_n^d is the degree nd coefficient of f^d).

Consider the system of equations

$$\begin{pmatrix} 1 & \lambda_1 & \lambda_1^2 & \cdots & \lambda_1^{n-1} & \lambda_1^n \\ 1 & \lambda_2 & \lambda_2^2 & \cdots & \lambda_2^{n-1} & \lambda_2^n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \lambda_n & \lambda_n^2 & \cdots & \lambda_n^{n-1} & \lambda_n^n \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} f(\lambda_1) \\ f(\lambda_2) \\ \vdots \\ f(\lambda_n) \\ a_n \end{pmatrix}.$$

Writing this system as $Av = b$ and multiplying both sides on the left by the adjugate matrix $\mathrm{adj}(A)$, we get

$$\det(A)v = \mathrm{adj}(A)b.$$

As $\mathrm{Nil}(R)$ is closed under linear combinations, each entry of the right side is nilpotent. Thus the same is true for the left side. In other words, $\det(A)a_j \in \mathrm{Nil}(R)$ for each j. Since the upper left $n \times n$ block of A is the Vandermonde matrix, we have $\det(A) = V_\Lambda$ and hence $V_\Lambda a_j \in \mathrm{Nil}(R)$ for each integer $0 \le j \le n$. □

Corollary 4.2. *Suppose R is an algebra over a field F and $\mathrm{Nil}(R)$ is a subalgebra. If $f \in R[x]$ has degree at most $|F|$ and $f^d \in \mathrm{Nil}(R)[x]$ for some integer $d \ge 1$, then $f \in \mathrm{Nil}(R)[x]$.*

Proof. In the previous proposition take $k = F$ and $\Lambda = (\lambda_1, \ldots, \lambda_n)$ where the λ_i are distinct elements of F. Then V_Λ is nonzero and hence a unit in F, so $V_\Lambda f \in \mathrm{Nil}(R)[x]$ implies $f \in \mathrm{Nil}(R)[x]$. □

In particular, when F is an infinite field, we get:

Theorem 4.3. *If R is an algebra over an infinite field and $\mathrm{Nil}(R)$ is a subalgebra, then any polynomial $f \in R[x]$ that has a positive power with nilpotent coefficients already has nilpotent coefficients. In particular, $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$.* □

Together with Proposition 2.1, this gives:

Theorem 4.4. *If R is an algebra over an infinite field then $\mathrm{Nil}(R)[x] \subseteq \mathrm{Nil}(R[x])$ implies $\mathrm{Nil}(R)[x] = \mathrm{Nil}(R[x])$.* □

As mentioned in the introduction, Theorem 4.3 simplifies many examples in the literature. The previous two theorems also place extremely strong restrictions on the structure of any example of the type we will construct in the next section. Some of Amitsur's results in [1], concerning nil algebras over *uncountable* fields, can also be reinterpreted in the context of Vandermonde determinants; this was part of the motivation for these results.

For the rest of the section we will repeatedly need the following easy result.

Lemma 4.5. *Let R be a k-algebra. For any $\lambda \in k$ and $a \in R$, if $\lambda^n a \in \mathrm{Nil}(R)$ for some integer $n \geq 2$, then $\lambda a \in \mathrm{Nil}(R)$.*

Proof. Suppose $(\lambda^n a)^m = 0$ for some integer $m \geq 1$. From the commutativity of λ, we see that $(\lambda a)^{mn} = (\lambda^n a)^m a^{m(n-1)} = 0$. □

We can now prove another consequence of Proposition 4.1.

Corollary 4.6. *Let R be a ring with $\mathrm{Nil}(R)$ a subring. Given any integer $n \geq 1$ and any polynomial $f \in R[x]$ of degree at most n, if $f^d \in \mathrm{Nil}(R)[x]$ for some integer $d \geq 1$, then $(n-1)!f \in \mathrm{Nil}(R)[x]$.*

Proof. Apply Proposition 4.1 with $k = \mathbb{Z}$ and $\Lambda = (1, 2, \ldots, n)$. By the definition of the Vandermonde determinant, V_Λ in this case divides a power of $(n-1)!$, say

$$(n-1)!^r = mV_\Lambda.$$

Now $V_\Lambda f \in \mathrm{Nil}(R)[x]$ implies $(n-1)!^r f = mV_\Lambda f \in \mathrm{Nil}(R)[x]$, which readily implies that $(n-1)!f \in \mathrm{Nil}(R)[x]$ by Lemma 4.5. □

Proposition 4.1 does not require that f is square-zero, or even that it is nilpotent, only that some power has nilpotent coefficients, which is a weak hypothesis. However, our conclusion is also weak; we only get that a scalar multiple of f, rather than f, has nilpotent coefficients. For example, if f is of degree 3 then Corollary 4.6 only says that $2f \in \mathrm{Nil}(R)[x]$, which is irrelevant if the characteristic of the ring is 2.

However, if we add the stronger assumption $f^2 = 0$, we are able to get stronger conclusions. To help in this derivation we will use the following standard lemma freely (see, for instance, [10, Lemma 1.5]). We include the proof for completeness.

Lemma 4.7. *Let R be a ring such that $\mathrm{Nil}(R)$ is closed under multiplication. Let $a, b, z \in R$.*

1. *If $ab, z \in \mathrm{Nil}(R)$, then $azb \in \mathrm{Nil}(R)$.*
2. *If $z, zb^2 \in \mathrm{Nil}(R)$, then $zb \in \mathrm{Nil}(R)$.*

Proof. (1) Since ab is nilpotent so is ba. One might refer to this as the "flip trick" for nilpotents. Thus, by closure under multiplication, $baz \in \mathrm{Nil}(R)$. The flip trick applied once more yields $azb \in \mathrm{Nil}(R)$.

(2) Since zb^2 is nilpotent, by part (1) taking $a = zb$ we have $(zb)z(b) \in \mathrm{Nil}(R)$. Hence $zb \in \mathrm{Nil}(R)$. □

Proposition 4.1 works because we know that $f(\lambda)$ is nilpotent, for each $\lambda \in k$. (We also used the fact that the leading coefficient, a_n, is nilpotent.) However, under the stronger assumption $f^2 = 0$ we are able to obtain more nilpotents. To give one example, write $f = \sum_{j=0}^{n} a_j x^j$ and assume $f^2 = 0$. Then

$$a_0 a_2 + a_1^2 + a_2 a_0 = 0,$$

as this is the coefficient of f^2 at degree 2. Also $a_0^2 = 0$, so multiplying the displayed equation on the left by a_0 we have

$$a_0 a_1^2 = -a_0 a_2 a_0 \in \mathrm{Nil}(R).$$

Thus, by Lemma 4.7(2), we get $a_0 a_1 \in \mathrm{Nil}(R)$. Note that $a_0 = f(0)$ and $a_1 = f'(0)$, where f' is the (usual) formal derivative of f. Thus $f(0)f'(0) \in \mathrm{Nil}(R)$. Applying the same argument for the (square-zero) polynomial $g = f(x + \lambda)$ with $\lambda \in k$, we get

$$f(\lambda) f'(\lambda) \in \mathrm{Nil}(R)$$

for each $\lambda \in k$.

By generalizing the previous computation, we will be able to go beyond the bounds obtained in Proposition 4.1. To that end, for a polynomial $f \in R[x]$ over any ring R, let us say that a set $X \subseteq R$ is *sufficient for* f if

$$\text{for each } z \in \mathrm{Nil}(R),\ zX \subseteq \mathrm{Nil}(R) \text{ implies } zf \in \mathrm{Nil}(R)[x].$$

In other words, to guarantee that zf has nilpotent coefficients, it suffices to show that zX consists of nilpotent elements. Clearly, the set of coefficients of f itself is always sufficient for f.

Lemma 4.8. *Let R be a k-algebra such that $\mathrm{Nil}(R)$ is a subalgebra. Let $\Lambda = (\lambda_1, \ldots, \lambda_n)$ be a collection of $n \geq 1$ elements in k, and let $f = \sum_{j=0}^{2n+1} a_j x^j \in R[x]$ be a polynomial of degree at most $2n+1$. Then the set*

$$X = \{f(\lambda_1), \ldots, f(\lambda_n), f'(\lambda_1), \ldots, f'(\lambda_n), a_{2n}, a_{2n+1}\}$$

is sufficient for the polynomial $V_\Lambda f$.

Proof. Take any $z \in \mathrm{Nil}(R)$ such that $zX \subseteq \mathrm{Nil}(R)$. Consider the following system:

$$\begin{pmatrix}
1 & \lambda_1 & \lambda_1^2 & \lambda_1^3 & \cdots & \lambda_1^{2n} & \lambda_1^{2n+1} \\
0 & 1\cdot\lambda_1^0 & 2\cdot\lambda_1^1 & 3\cdot\lambda_1^2 & \cdots & 2n\cdot\lambda_1^{2n-1} & (2n+1)\cdot\lambda_1^{2n} \\
1 & \lambda_2 & \lambda_2^2 & \lambda_2^3 & \cdots & \lambda_2^{2n} & \lambda_2^{2n+1} \\
0 & 1\cdot\lambda_2^0 & 2\cdot\lambda_2^1 & 3\cdot\lambda_2^2 & \cdots & 2n\cdot\lambda_2^{2n-1} & (2n+1)\cdot\lambda_2^{2n} \\
\vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
1 & \lambda_n & \lambda_n^2 & \lambda_n^3 & \cdots & \lambda_n^{2n} & \lambda_n^{2n+1} \\
0 & 1\cdot\lambda_n^0 & 2\cdot\lambda_n^1 & 3\cdot\lambda_n^2 & \cdots & 2n\cdot\lambda_n^{2n-1} & (2n+1)\cdot\lambda_n^{2n} \\
0 & 0 & 0 & 0 & \cdots & 1 & 0 \\
0 & 0 & 0 & 0 & \cdots & 0 & 1
\end{pmatrix}
\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{2n} \\ a_{2n+1} \end{pmatrix}
=
\begin{pmatrix} f(\lambda_1) \\ f'(\lambda_1) \\ f(\lambda_2) \\ f'(\lambda_2) \\ \vdots \\ f(\lambda_n) \\ f'(\lambda_n) \\ a_{2n} \\ a_{2n+1} \end{pmatrix}.$$

Write this system as $Av = b$. Multiplying both sides on the left by $z \cdot \mathrm{adj}(A)$, where $\mathrm{adj}(A)$ is the adjugate matrix of A, we get

$$\det(A) z v = \mathrm{adj}(A) z b.$$

Since $zX \subseteq \mathrm{Nil}(R)$ and $\mathrm{Nil}(R)$ is closed under linear combinations, each entry on the right side is nilpotent. Thus the same is true for the left side. Hence $\det(A) z a_j \in \mathrm{Nil}(R)$ for each

integer j. The matrix A is known as a *confluent Vandermonde matrix* and its determinant is equal to V_Λ^4. (For a more general formula see [13, (6.1.34)], and for a proof see [18, pages 3–5].) Hence $V_\Lambda^4 z a_j \in \mathrm{Nil}(R)$, which implies $V_\Lambda z a_j \in \mathrm{Nil}(R)$ by Lemma 4.5. Hence $zV_\Lambda f = V_\Lambda z f \in \mathrm{Nil}(R)[x]$, which is what needed to be shown. □

Lemma 4.9. *Let R be a k-algebra such that $\mathrm{Nil}(R)$ is a subalgebra, let $n \in \mathbb{N}$, and let $f = \sum_{j=0}^n a_j x^j \in R[x]$ be a polynomial of degree at most n. If a set $X \subseteq R$ is sufficient for f, then it is sufficient for the following polynomials g:*

(1) $g = \sum_{j=0}^n a_j (x+\lambda)^j = f(x+\lambda)$ *for any* $\lambda \in k$,
(2) $g = \sum_{j=0}^n a_{n-j} x^j = f(x^{-1})x^n$.

Proof. In both (1) and (2), coefficients of g are k-linear combinations of coefficients of f. Now the conclusion follows immediately from the definition. □

Lemma 4.10. *Let R be a k-algebra with $\mathrm{Nil}(R)$ a subalgebra, and given an integer $n \geq 1$, let $f = \sum_{j=0}^n a_j x^j \in R[x]$ be a polynomial of degree at most n such that $f^2 \in \mathrm{Nil}(R)[x]$. If $X \subseteq R$ is sufficient for f, then so is*

(1) $X \setminus \mathrm{Nil}(R)$,
(2) $X \setminus \{f'(\lambda)\}$ *for any* $\lambda \in k$,
(3) $X \setminus \{a_{n-1}\}$.

Proof. (1) This follows from the fact that $\mathrm{Nil}(R)$ is multiplicatively closed.

(2) First let $\lambda = 0$, so that $f'(\lambda) = f'(0) = a_1$. Take $z \in \mathrm{Nil}(R)$ with $z(X \setminus \{a_1\}) \subseteq \mathrm{Nil}(R)$. Let $m \geq 0$ be the minimal nonnegative integer with the property that

$$a_0^{m-j} z a_0^j f \in \mathrm{Nil}(R)[x], \text{ for each integer } 0 \leq j \leq m.$$

Note that such an integer exists since $a_0 \in \mathrm{Nil}(R)$.

If $m = 0$ then we are done, so assume by way of contradiction $m \geq 1$. Pick any nonnegative integer $j \leq m-1$ and set $z' = a_0^{m-1-j} z a_0^j$. By the definition of m, we have $a_0 z' f, z' a_0 f \in \mathrm{Nil}(R)[x]$. In particular,

$$a_0 z' a_2, z' a_0 a_2 \in \mathrm{Nil}(R)$$

and hence (by the flip trick) also $z' a_2 a_0 \in \mathrm{Nil}(R)$. Since $f^2 \in \mathrm{Nil}(R)[x]$, we have

$$a_0 a_2 + a_1^2 + a_2 a_0 \in \mathrm{Nil}(R),$$

as this is the coefficient of f^2 at degree 2. Multiplying this element on the left by z', and considering that $\mathrm{Nil}(R)$ is a subring of R, we get $z' a_1^2 \in \mathrm{Nil}(R)$, and hence $z' a_1 \in \mathrm{Nil}(R)$ by Lemma 4.7(2).

Since $z'(X \setminus \{a_1\}) \subseteq \mathrm{Nil}(R)$ we have $z'X \subseteq \mathrm{Nil}(R)$. Since X is sufficient for f, it follows that $z'f \in \mathrm{Nil}(R)[x]$, contradicting the minimality on m. This proves the case when $\lambda = 0$.

If λ is arbitrary, we consider the polynomial $g = f(x+\lambda)$. We have $g'(0) = f'(\lambda)$, and also $g^2 \in \mathrm{Nil}(R)[x]$ as the coefficients of g^2 are linear combinations of the coefficients of f^2. Since X is sufficient for f, it is sufficient for g by Lemma 4.9(1). By what we have shown above it follows that $X \setminus \{g'(0)\}$ is sufficient for g, which in turn gives that this set is sufficient for f by Lemma 4.9(1).

(3) Consider the polynomial $g = f(x^{-1})x^n$. We have $g^2 \in \mathrm{Nil}(R)[x]$ and $g'(0) = a_{n-1}$. By Lemma 4.9(2), X is sufficient for g, hence (2) gives that $X \setminus \{g'(0)\}$ is sufficient for g. Applying Lemma 4.9(2) once again, this set is sufficient for f. □

We now have a strong extension of Proposition 4.1, if we slightly strengthen the hypothesis on f.

Theorem 4.11. *Let R be a k-algebra such that $\mathrm{Nil}(R)$ is a subalgebra of R. Let Λ be a collection of $n \geq 1$ elements in k, and let $f \in R[x]$ be a polynomial with degree at most $2n+1$. If $f^2 \in \mathrm{Nil}(R)[x]$, then $V_\Lambda f \in \mathrm{Nil}(R)[x]$.*

Proof. Fix n and $\Lambda = (\lambda_1, \ldots, \lambda_n)$. We will prove the statement by induction on $m = \deg(f)$. When $m = 0$ the conclusion is clear, so suppose that f is of degree $1 \leq m \leq 2n+1$ and that the statement holds for all polynomials of degree less than m.

Let $g = V_\Lambda f$. Writing $g = \sum_{j=0}^{2n+1} a_j x^j$, Lemma 4.8 says that the set

$$X = \{g(\lambda_1), \ldots, g(\lambda_n), g'(\lambda_1), \ldots, g'(\lambda_n), a_{2n}, a_{2n+1}\}$$

is sufficient for $V_\Lambda g$. We claim that it is then sufficient for $V_\Lambda f = g$. Taking $z \in \mathrm{Nil}(R)$ with $zX \subseteq \mathrm{Nil}(R)$, we have $V_\Lambda^2 zf = V_\Lambda zg \in \mathrm{Nil}(R)[x]$ since X is sufficient for $V_\Lambda g$, which in turn gives $V_\Lambda zf \in \mathrm{Nil}(R)[x]$. This proves the claim.

Now, since $g^2 \in \mathrm{Nil}(R)[x]$, we have $g(\lambda_i) \in \mathrm{Nil}(R)$ for all i and $a_{2n+1} \in \mathrm{Nil}(R)$, and therefore we can apply Lemma 4.10 to remove all elements of X, and the set will remain sufficient for g. Hence the empty set is sufficient for g, meaning that $zg \in \mathrm{Nil}(R)[x]$ for all $z \in \mathrm{Nil}(R)$.

Since a_m is nilpotent (being either 0 or the leading coefficient of g), we have $a_m g, g a_m \in \mathrm{Nil}(R)[x]$. Hence setting $h = g - a_m x^m$, we see that $h^2 \in \mathrm{Nil}(R)[x]$. However, $\deg(h) < m$, so by our inductive argument

$$V_\Lambda h \in \mathrm{Nil}(R)[x].$$

This shows that $V_\Lambda a_j \in \mathrm{Nil}(R)$ for $j = 0, \ldots, m-1$. Since also $a_m \in \mathrm{Nil}(R)$, it follows that $V_\Lambda g \in \mathrm{Nil}(R)[x]$. Thus $V_\Lambda^2 f \in \mathrm{Nil}(R)[x]$ and hence $V_\Lambda f \in \mathrm{Nil}(R)[x]$, which completes the proof. □

The following corollaries are analogous to Corollaries 4.2 and 4.6:

Corollary 4.12. *Let R be an algebra over a field F such that $\mathrm{Nil}(R)$ is a subalgebra. If $f \in R[x]$ has degree at most $2|F|+1$ and $f^2 \in \mathrm{Nil}(R)[x]$, then $f \in \mathrm{Nil}(R)[x]$.* □

Corollary 4.13. *Let R be a ring with $\mathrm{Nil}(R)$ a subring. Given any integer $n \geq 1$ and any $f \in R[x]$ of degree at most $2n+1$, if $f^2 \in \mathrm{Nil}(R)[x]$ then $(n-1)!f \in \mathrm{Nil}(R)[x]$.* □

In particular, taking $n = 2$ we get:

Corollary 4.14. *Let R be a ring with $\mathrm{Nil}(R)$ a subring. If $f \in R[x]$ has degree at most 5 and $f^2 \in \mathrm{Nil}(R)[x]$, then $f \in \mathrm{Nil}(R)[x]$.* □

For polynomials of degree 6, the conclusion of Corollary 4.13 (taking $n = 3$) is that $2f \in \mathrm{Nil}(R)[x]$. But we can get $f \in \mathrm{Nil}(R)[x]$ under a weak additional assumption. We were unable to determine whether an extra condition is necessary. The proof of the following proposition is quite technical, and the proposition isn't used in later sections, so readers may safely skip the proof.

Proposition 4.15. *Let R be a ring with $\mathrm{Nil}(R)$ a subring and let $f = \sum_{j=0}^{6} a_j x^j \in R[x]$ be a polynomial of degree 6. If $a_6 \,\mathrm{Nil}(R) = \mathrm{Nil}(R) a_6 = 0$ and $f^2 \in \mathrm{Nil}(R)[x]$, then $f \in \mathrm{Nil}(R)[x]$.*

Proof. We have

$$a_4a_6 + a_5^2 + a_6a_4 \in \mathrm{Nil}(R), \tag{4.16}$$

as this is the coefficient of f^2 at degree 10. Multiplying by a_6 from the left, and considering that $a_6^2 = 0$ and $a_6a_4a_6 \in \mathrm{Nil}(R)$, we have $a_6a_5^2 \in \mathrm{Nil}(R)$. Hence $a_6a_5 \in \mathrm{Nil}(R)$ by Lemma 4.7(2). Similarly, multiplying

$$a_0a_2 + a_1^2 + a_2a_0 \in \mathrm{Nil}(R)$$

(the coefficient of f^2 at degree 2) by a_6 from the left, and considering that $a_6a_0 = 0$ and $a_6a_2a_0 \in \mathrm{Nil}(R)$ (because $a_0a_6 = 0$), we have $a_6a_1^2 \in \mathrm{Nil}(R)$ and hence $a_6a_1 \in \mathrm{Nil}(R)$ by Lemma 4.7(2).

Now apply the same argument to the polynomial $g = f(x+1)$. Note that $g^2 \in \mathrm{Nil}(R)[x]$ and the leading coefficient of g is a_6, so g satisfies the same conditions as f. Thus, the above argument gives that $a_6g'(0) = a_6f'(1)$ is a nilpotent. Hence

$$a_6(a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 + 6a_6) \in \mathrm{Nil}(R). \tag{4.17}$$

By Corollary 4.13 we have $2a_i \in \mathrm{Nil}(R)$ for each i. Since also $a_6a_1, a_6a_5 \in \mathrm{Nil}(R)$, then (4.17) gives $a_6a_3 \in \mathrm{Nil}(R)$.

Now multiplying (4.16) by a_6a_3 from the left, and considering that $a_6a_3a_6 = 0$ and $a_6a_3a_4a_6 \in \mathrm{Nil}(R)$, we have $a_6a_3a_5^2 \in \mathrm{Nil}(R)$ and hence $a_6a_3a_5 \in \mathrm{Nil}(R)$ by Lemma 4.7(2). Similarly, multiplying (4.16) by a_3a_6 from the left, and considering that $a_6^2 = 0$ and $a_3a_6a_4a_6 \in \mathrm{Nil}(R)$ (because $a_6a_3a_6 = 0$), we have $a_3a_6a_5^2 \in \mathrm{Nil}(R)$ and hence $a_3a_6a_5 \in \mathrm{Nil}(R)$.

Finally, multiplying

$$a_2a_6 + a_3a_5 + a_4^2 + a_5a_3 + a_6a_2 \in \mathrm{Nil}(R)$$

(the coefficient of f^2 at degree 8) by a_6 from the left, and considering that $a_6a_3a_5$, $a_6a_5a_3$, and $a_6a_2a_6$ are nilpotents (and $a_6^2 = 0$), we have $a_6a_4^2 \in \mathrm{Nil}(R)$ and therefore $a_6a_4 \in \mathrm{Nil}(R)$. Since $a_6(a_0 + a_1 + a_2 + a_3 + a_4 + a_5 + a_6) = a_6f(1) = 0$ (as $f(1) \in \mathrm{Nil}(R)$), we also have $a_6a_2 \in \mathrm{Nil}(R)$. Thus $a_6a_i \in \mathrm{Nil}(R)$ for every nonnegative integer $i \leq 6$. Therefore, $h = f - a_6x^6$ is a polynomial with $\deg(h) \leq 5$ and $h^2 \in \mathrm{Nil}(R)[x]$, so that $h \in \mathrm{Nil}(R)[x]$ by Corollary 4.13. Accordingly, $f \in \mathrm{Nil}(R)[x]$, as desired. □

Corollary 4.18. *Let R be a ring with $\mathrm{Nil}(R)^2 = 0$ and let $f \in R[x]$ have degree at most 6. If $f^2 \in \mathrm{Nil}(R)[x]$ then $f \in \mathrm{Nil}(R)[x]$.* □

5. The Main Example

In this section we will construct our main example of a ring R with $\mathrm{Nil}(R)^2 = 0$ and with a square-zero polynomial $f \in R[x]$ of degree 7 whose coefficients are not all nilpotent. The polynomial f must satisfy $2f \in \mathrm{Nil}(R)[x]$, by Corollary 4.13. So the constructed ring will have characteristic 2.

Given any degree 7 polynomial $f = \sum_{i=0}^{7} a_ix^i$, the condition $f^2 = 0$ is equivalent to the following fifteen equations:

$$\sum_{i,j\,:\,i+j=k} a_ia_j = 0, \text{ for } 0 \leq k \leq 14. \tag{5.1}$$

Thus, a natural candidate for the desired ring R would be to take the free unital $\mathbb{F}_2$-algebra on the set $\{a_0, \ldots, a_7\}$ subject to these relations. However, we must also guarantee that $\mathrm{Nil}(R)^2 = 0$, and it is difficult to fully describe all the nilpotent elements in that ring. There

are three obvious nilpotents; namely, a_0, a_7 and $f(1) = \sum_{i=0}^{7} a_i$, which already have index 2. Thus, to simplify the situation further, in the hopes of more easily classifying nilpotent elements, we will force

$$a_0 = a_7 = \sum_{i=0}^{7} a_i. \tag{5.2}$$

This simplification enables us to eliminate the variables a_7 and a_6 from this system of generators and relations. After those eliminations, two equations in (5.1) can be removed; the first equation $a_0^2 = 0$ now coincides with the last equation $a_7^2 = 0$, as well as the sum of all fifteen equations $f(1)^2 = 0$. The resulting system of relations is somewhat chaotic and difficult to work with, so it will be convenient to introduce new variables

$$\begin{aligned} &b_0 = a_0,\ b_1 = a_1,\ b_2 = a_2 + a_0,\ b_3 = a_3 + a_1, \\ &b_4 = a_4 + a_2 + a_0, \text{ and } b_5 = a_5 + a_3 + a_1, \end{aligned} \tag{5.3}$$

and express the remaining thirteen equations in terms of these new variables. Note that these variables generate the same algebra; this selection of new variables was discovered through trial and error when reducing the number of monomials that appear in the relations.

In order to formally define the ring R, we will first introduce some notations. Let

$$X = \{b_0, b_1, b_2, b_3, b_4, b_5\}$$

be the given set of six symbols, and let $\langle X \rangle$ be the free monoid on X. We denote by $R_0 = \mathbb{F}_2\langle X \rangle$ the free unital $\mathbb{F}_2$-algebra on the set X. The product in R_0 will be denoted by concatenation, as usual, and elements of $\langle X \rangle$ will be called words or monomials in R_0.

Define the following reduction system in R_0:

(R1) $b_0^2 \mapsto 0$,
(R2) $b_1 b_0 \mapsto b_0 b_1$,
(R3) $b_2 b_0 \mapsto b_1^2 + b_0 b_2$,
(R4) $b_3 b_0 \mapsto b_2 b_1 + b_1 b_2 + b_0 b_3$,
(R5) $b_4 b_0 \mapsto b_0 b_4$,
(R6) $b_5 b_0 \mapsto b_0 b_5$,
(R7) $b_3 b_1 \mapsto b_2^2 + b_1 b_3$,
(R8) $b_4 b_1 \mapsto b_3 b_2 + b_2 b_3 + b_1 b_4$,
(R9) $b_5 b_1 \mapsto b_4 b_2 + b_3^2 + b_2 b_4 + b_1 b_5$,
(R10) $b_5 b_2 \mapsto b_4 b_3 + b_3 b_4 + b_2 b_5 + b_4 b_2 + b_3^2 + b_2 b_4$,
(R11) $b_5 b_3 \mapsto b_4^2 + b_3 b_5 + b_4 b_3 + b_3 b_4$,
(R12) $b_5 b_4 \mapsto b_4 b_5 + b_4^2 + b_1^2$, and
(R13) $b_5^2 \mapsto b_2 b_1 + b_1 b_2 + b_1^2$.

These reductions come from the equations (5.1) and (5.2), where variables a_i are substituted by b_i in accordance with (5.3). Let $\prec$ denote the shortlex order on $\langle X \rangle$, where we order the variables b_i via their subscripts. Then $\prec$ is a strict monoid well-ordering on $\langle X \rangle$, and the reductions (R1)–(R13) are compatible with $\prec$, in the sense that they replace each monomial by a sum of strictly $\prec$-smaller monomials.

Proposition 5.4. *All ambiguities in the reduction system* (R1)–(R13) *are resolvable, in the sense of Bergman's Diamond Lemma* [7].

Proof sketch. One needs to see that all overlaps and inclusions are resolvable. There are no inclusions, but there are twenty overlaps. Checking that they resolve is a tedious but

mechanically straightforward task. It can be done manually (computations take a page or two) or by using one of the standard algebra programs. □

Let I be the (two-sided) ideal of R_0 generated by the relations (R1)–(R13). Bergman's Diamond Lemma [7, Theorem 1.2], together with Proposition 5.4, implies that every element of R_0/I has a unique canonical form. One possible way to define the needed ring R would be by letting it equal the quotient ring R_0/I. However, for clarity of exposition, we will define our ring R in another (isomorphic) way. For this purpose denote by $\langle X\rangle_{\mathrm{irr}}$ the set of words in $\langle X\rangle$ that do not contain, as a subword, any of the thirteen monomials on the left side of the arrows in (R1)–(R13). We will call the elements of $\langle X\rangle_{\mathrm{irr}}$ the *irreducible* or *reduced* words of $\langle X\rangle$. We are now ready to define our ring R, by letting

$$R = \mathbb{F}_2\langle X\rangle_{\mathrm{irr}} \tag{5.5}$$

be the $\mathbb{F}_2$-subspace of R_0 with basis $\langle X\rangle_{\mathrm{irr}}$. This subspace becomes a $\mathbb{F}_2$-algebra with respect to multiplication

$$r \cdot s = \mathrm{red}(rs),$$

where rs denotes the usual product in R_0 and $\mathrm{red}\colon R_0 \to R$ is the map induced by the confluent reductions (R1)–(R13). According to [7, Theorem 1.2], the algebra R defined this way is isomorphic to R_0/I.

Remark 5.6. The reason why we defined R as a subspace of R_0 rather than the quotient ring R_0/I is to distinguish the product $r \cdot s$ in R from the product rs in R_0. This approach will prove convenient in our computations. For example, using this notation we have $b_1 \cdot b_0 \in b_1 \cdot R$, but on the other hand $b_1 \cdot b_0 = b_0 b_1$ from reduction (R2) and hence $b_1 \cdot b_0 \notin b_1 R$. Note that if $r, s \in R$ and $rs \in R$ then $r \cdot s = \mathrm{red}(rs) = rs$. In particular, if $r, s \in \langle X\rangle_{\mathrm{irr}}$ are reduced words and rs is reduced then $r \cdot s = rs$.

The remainder of this section is devoted to proving the key property $\mathrm{Nil}(R)^2 = 0$. This will be a consequence of the following complete characterization of zero-products in R:

Theorem 5.7. *If $r, s \in R \setminus \{0\}$ satisfy $r \cdot s = 0$, then $r \in R \cdot b_0$ and $s \in b_0 \cdot R$.*

To prove this theorem, we need some additional notation. Let P be the free monoid on the set $\{b_1, b_2, b_3, b_4, b_5\}$, so P is a submonoid of $\langle X\rangle$. Let

$$M = \langle X\rangle_{\mathrm{irr}} \cap P \subseteq P,$$

which is the set of reduced words that do not contain b_0 as a subword. Finally, take $S = \mathbb{F}_2 M$. Note that S is a unital subring of R, since the reductions (R7)–(R13) do not involve any instances of b_0. From the reduced forms of elements in R, we have $R = S \oplus (b_0 \cdot S)$, and the right annihilator of b_0 in S is zero. Taking $y = b_0$, we see that all of the conditions in Proposition 3.8 hold, where the induced map σ is the identity map on S and the (right σ-skew) derivation $\delta\colon S \to S$ satisfies $\delta(s) = b_0 \cdot s + s \cdot b_0$ for each $s \in S$. Since $b_0 \cdot b_0 = 0$ in R, Proposition 3.10 also applies. Proving Theorem 5.7 thus reduces to showing the following fundamental claim:

Lemma 5.8. *If $r, s, t \in S$ and $r, s \neq 0$, then*

$$r \cdot s \neq \delta(r) \cdot t. \tag{5.9}$$

Thus, for the remainder of this section, we will only work with the ring S. In particular, the reductions (R1)–(R6) are only relevant when dealing with $\delta(r)$, on the right side of (5.9).

Rather than working with the shortlex order $\prec$, we find it more convenient to work with the lex(icographical) order. Thus, in this section, $<$ will always denote the lex order on P, except when denoting the standard order on $\mathbb{Z}$, as context dictates. When we speak of one monomial being larger or smaller than another, we mean with respect to the lex order. (The empty monomial, 1, is the smallest monomial.) When we write $\max A$, for some finite subset $A \subseteq P$, we will mean the lex-maximal element of A, and similarly $\min A$ will be the lex-minimal element.

When we speak of the *support* of an element $s \in S$, we mean the finite set $\operatorname{supp}(s) \subseteq M$ such that

$$s = \sum_{m \in \operatorname{supp}(s)} m.$$

The support is empty only when $s = 0$.

Also, for any monomial $m \in P$, let $\deg(m)$ be the total degree of m, i.e., the total number of letters in the word m. It is an important observation that the reductions (R7)–(R13) are homogeneous—they preserve the degree of monomials. More precisely, if $p, q \in M$ and $m \in \operatorname{supp}(p \cdot q)$, then $\deg(m) = \deg(p) + \deg(q)$. This property will be used freely.

Rather than approach Lemma 5.8 directly, we will instead build up, through a sequence of lemmas, information about the ring S that we will use to identify an element in the support of the left side of (5.9) which doesn't belong to the support of the right side. The heart of the proof comes from handling the case when r is homogeneous of degree 1, and many of the lemmas below will either deal with that case, or provide means whereby we can reduce to that case.

In the following lemma we give some basic properties of the lex order on P. Since the properties are well known, the proof is omitted.

Lemma 5.10. *For every $a, b \in P$, the following hold:*

(1) *$a < b$ if and only if $ca < cb$ for every $c \in P$, and*
(2) *if $a \leq b$ then either $b \in aP$ or $ac < b$ for every $c \in P$.* □

Remark 5.11. Without some additional constraint, if $a < b$ then we do not necessarily have $ac < bc$; for instance, take $a = 1$, $b = b_1$, and $c = b_2$. Thus, the order of the products in (1) above matters. This is one of the reasons why we needed to use the shortlex order when formulating Proposition 5.4, the other being that there are infinite $<$-decreasing chains such as

$$b_2 > b_1 b_2 > b_1^2 b_2 > \dots.$$

Note that the Diamond Lemma [7, Theorem 1.2] applies only when the partial order on the monoid $\langle X \rangle$ is compatible with the multiplication and satisfies the descending chain condition.

A crucial property of the system (R7)–(R13), or even the full system (R1)–(R13), is that those reductions send monomials to sums of lex-smaller monomials. More formally:

Lemma 5.12. *For every $a, b \in M$ and $c \in \operatorname{supp}(a \cdot b)$, we have either $c = ab$ (if ab is reduced) or $c < a$. In particular, $c \leq ab$.*

Proof. Only a finite number of reductions are needed to put $a \cdot b$ into reduced form. When that number is zero, then $c = ab$. So, by recursion and Lemma 5.10, it suffices to show that

if ab is not reduced, then after a single reduction it is a sum of monomials each $<$-smaller than a. Since $a, b \in M$, the only way ab is not reduced is if $a = m_1 b_i$ and $b = b_j m_2$ for some $m_1, m_2 \in M$, and $b_i b_j$ is not reduced. Therefore

$$ab = m_1 b_i b_j m_2 \mapsto \sum_{b_k b_\ell \in \operatorname{supp}(b_i \cdot b_j)} m_1 b_k b_\ell m_2,$$

and by inspecting the reductions we see that for each integer k that occurs in the sum, we have $k < i$. Thus, each monomial in the sum on the right is smaller than a. □

The next few lemmas help codify which monomials may appear in (5.9).

Lemma 5.13. *Let $r, s \in S$ be nonzero elements, where r is homogeneous, and suppose that $u = \max \operatorname{supp}(r)$ satisfies $u \notin Mb_5$. Then $r \cdot s \neq 0$. Moreover, putting $w = \max \operatorname{supp}(r \cdot s)$ we have one of the following cases:*

1. *$w \in uM$,*
2. *$\operatorname{supp}(s) \subseteq b_1 M$, $u \in Mb_3$, and $w \in u_0 b_2^2 M$ where $u = u_0 b_3$, or*
3. *$\operatorname{supp}(s) \subseteq b_1 M$, $u \in Mb_4$, and $w \in u_0 b_3 b_2 M$ where $u = u_0 b_4$.*

Proof. If $u = 1$, then $r = 1$ and the statement is trivial. Thus suppose that $u \neq 1$.

First consider the case $u \in Mb_1 \cup Mb_2$. By inspecting (R7)–(R13), we see that $b_1 M \cup b_2 M \subseteq M$ (i.e., multiplying a reduced monomial in S by b_1 or b_2 from the left keeps it reduced). Thus, for each $q \in M$ we have $uq \in M$ and hence $u \cdot q = uq$. Therefore, multiplying $r = u + \sum_{p \in \operatorname{supp}(r) \setminus \{u\}} p$ and $s = \sum_{q \in \operatorname{supp}(s)} q$, we get

$$r \cdot s = \sum_{q \in \operatorname{supp}(s)} uq + \sum_{p \in \operatorname{supp}(r) \setminus \{u\}} p \cdot s. \tag{5.14}$$

For every $p \in \operatorname{supp}(r) \setminus \{u\}$, $q \in \operatorname{supp}(s)$, and $v \in \operatorname{supp}(p \cdot q)$, we have $v \leq pq$ by Lemma 5.12. Moreover, $pq < u$ by the homogeneity of r and Lemma 5.10(2), and therefore $v < u$. Hence, monomials in the second sum of (5.14) are strictly smaller than monomials in the first sum, and therefore the maximal monomial in (5.14) is exactly uq where $q = \max \operatorname{supp}(s)$. This gives (1).

Now consider the case $u \in Mb_3 \cup Mb_4$ and $\operatorname{supp}(s) \not\subseteq b_1 M$. In this case, decompose $s = s_1 + s_2$ where $s_1, s_2 \in S$ with $\operatorname{supp}(s_1) \cap b_1 M = \emptyset$, $\operatorname{supp}(s_2) \subseteq b_1 M$, and $s_1 \neq 0$. Notice that $uq \in M$ and hence $u \cdot q = uq$ for each $q \in \operatorname{supp}(s_1)$. Hence, similarly as above we get

$$r \cdot s = \sum_{q \in \operatorname{supp}(s_1)} uq + \sum_{q \in \operatorname{supp}(s_2)} u \cdot q + \sum_{p \in \operatorname{supp}(r) \setminus \{u\}} p \cdot s.$$

Monomials in the third sum are smaller than u by the same argument as above. Moreover, monomials in the second sum are smaller than u by Lemma 5.12. Since monomials in the first sum are all greater than or equal to u, we conclude that $\max \operatorname{supp}(r \cdot s) = uq$ where $q = \max \operatorname{supp}(s_1)$, which gives (1).

We now only need to consider when $\operatorname{supp}(s) \subseteq b_1 M$, and $u \in Mb_3$ or $u \in Mb_4$. We first consider the case $u \in Mb_3$. Write $u = u_0 b_3$ with $u_0 \in M$, and note that $u_0 \notin Mb_5$, otherwise $u_0 b_3 \notin M$ by (R11). We first prove that

$$\max \operatorname{supp}(r \cdot b_1) = u_0 b_2^2.$$

From (R7) we get $u \cdot b_1 = u_0 b_3 \cdot b_1 = u_0 b_2^2 + u_0 \cdot b_1 b_3$. (Note that $u_0 b_2^2$ is reduced since $u_0 \notin M b_5$.) Thus, multiplying $r = u + \sum_{p \in \operatorname{supp}(r) \setminus \{u\}} p$ and b_1 gives

$$r \cdot b_1 = u_0 b_2^2 + u_0 \cdot b_1 b_3 + \sum_{p \in \operatorname{supp}(r) \setminus \{u\}} p \cdot b_1. \tag{5.15}$$

By Lemma 5.12, monomials in the second term are smaller than or equal to $u_0 b_1 b_3$ and hence smaller than $u_0 b_2^2$. We argue that monomials in the last term are also smaller than $u_0 b_2^2$. Taking any $p \in \operatorname{supp}(r) \setminus \{u\}$, by Lemma 5.12 it suffices to prove that $p b_1 < u_0 b_2^2$. Since $p < u_0 b_3$ and r is homogeneous, we have $p \leq u_0 b_2$. Hence Lemma 5.10(2) gives either $u_0 b_2 \in pM$ (which forces $p = u_0 b_2$ by homogeneity) or $p b_1 < u_0 b_2$. In both cases we get $p b_1 < u_0 b_2^2$ as claimed. This shows that the maximal monomial in (5.15) is $u_0 b_2^2$.

Now, to complete this case, write $s = b_1 s_1$ with $s_1 \in S$. Since $\max \operatorname{supp}(r \cdot b_1) = u_0 b_2^2 \in M b_2$, the case in the second paragraph of this proof then gives

$$\max \operatorname{supp}(r \cdot s) = \max \operatorname{supp}((r \cdot b_1) \cdot s_1) \in u_0 b_2^2 M.$$

Thus (2) holds.

A similar argument in the case when $u \in M b_4$ yields (3); the details are left to the reader. □

The next lemma shows that the left side of (5.9) is nonzero when r is homogeneous of degree 1, and it gives bounds on the lex-maximal element as well.

Lemma 5.16. *Let $r, s \in S \setminus \{0\}$, where r is homogeneous of degree 1. Then $r \cdot s \neq 0$. Moreover, if $r \neq b_1$ then $\max \operatorname{supp}(r \cdot s) \geq b_2$, and if $b_3 \in \operatorname{supp}(r)$ then $\max \operatorname{supp}(r \cdot s) \geq b_2^2$.*

Proof. For any $q \in M$, we see that $b_1 \cdot q = b_1 q$, as a quick look at the reductions reveals. In particular, if $r = b_1$, then $r \cdot s \neq 0$.

Assume now that $r \neq b_1$. Our main goal is to prove that there is some monomial in $\operatorname{supp}(r \cdot s)$ not beginning with b_1, and in particular $r \cdot s \neq 0$. Note that since every element of $\operatorname{supp}(b_1 \cdot s)$ begins with b_1, the monomials of $\operatorname{supp}(r \cdot s)$ not beginning with b_1 are exactly the same as those of $\operatorname{supp}((r - b_1) \cdot s)$. Thus, without loss of generality, for the remainder of the proof we assume $b_1 \notin \operatorname{supp}(r)$.

Next we consider the case $b_5 \notin \operatorname{supp}(r)$. In this case, $r \cdot s \neq 0$ follows directly from Lemma 5.13. Moreover, denoting $w = \max \operatorname{supp}(r \cdot s)$, Lemma 5.13 yields the following cases:

$$\begin{array}{ll} w \in b_2 M, & \text{if } \max \operatorname{supp}(r) = b_2, \\ w \in b_3 M \cup b_2^2 M, & \text{if } \max \operatorname{supp}(r) = b_3, \\ w \in b_4 M \cup b_3 b_2 M, & \text{if } \max \operatorname{supp}(r) = b_4. \end{array}$$

Hence $w \geq b_2$ holds under all three cases, with $w \geq b_2^2$ as soon as $r \neq b_2$ (i.e., $\max \operatorname{supp}(r) > b_2$). This proves the claim for this case.

We assume for the rest of the proof that $b_5 \in \operatorname{supp}(r)$. Write $r = b_5 + r'$ with $\operatorname{supp}(r') \subseteq \{b_2, b_3, b_4\}$. We will consider each of the eight possibilities for r'; these cases are organized to take advantage of arguments that pass from one case to another.

Let T denote the subring of S generated by reduced monomials without b_5 as a subword—this is a subring since (R7)–(R8) do not involve b_5 in any way. We have

$$t \cdot b_5 + b_5 \cdot t \in T \text{ for every } t \in T, \tag{5.17}$$

which is established using the reductions (R9)–(R12) and induction on degrees of monomials in T. Hence we can write every element in S as $v + b_5 \cdot w$ for some $v, w \in T$. Moreover, since

$b_5 \in \operatorname{supp}(r)$, we can also write such an element as $v + r \cdot w$ for some $v, w \in T$. Using this idea, we can therefore decompose s as

$$s = s_1 + r \cdot s_2$$

with $s_1, s_2 \in T$. Multiplying this equation on the left by r we get

$$r \cdot s = r \cdot s_1 + r \cdot r \cdot s_2. \tag{5.18}$$

We have $r \cdot r = (b_5 + r') \cdot (b_5 + r') \in T$; this is a simple consequence of (5.17) and the fact that $b_5 \cdot b_5 \in T$ by (R13). Hence $r \cdot r \cdot s_2 \in T$. Moreover, $r \cdot s_1 + b_5 \cdot s_1 = r' \cdot s_1 \in T$ and hence, by (5.17) once again, $r \cdot s_1 + s_1 \cdot b_5 \in T$. Thus (5.18) gives $r \cdot s = s_1 \cdot b_5 + s'$ where $s' \in T$. In particular,

$$pb_5 \in \operatorname{supp}(r \cdot s) \text{ for every } p \in \operatorname{supp}(s_1). \tag{5.19}$$

We reduce to the case $\operatorname{supp}(s_1) \subseteq b_1 M \cup b_2 b_1 M$. In fact, if this condition is not satisfied then we can find $p \in \operatorname{supp}(s_1)$ such that either $p = 1$ or $p = b_2$ or $p \geq b_2^2$. In all three cases we have $pb_5 \geq b_2^2$, and since also $pb_5 \in \operatorname{supp}(r \cdot s)$ by (5.19), we conclude that $r \cdot s \neq 0$ and $\max \operatorname{supp}(r \cdot s) \geq b_2^2$, which finishes the proof.

Case 1: $b_3 \notin \operatorname{supp}(r)$.

In this case, we only need to show that $\max \operatorname{supp}(r \cdot s) \geq b_2$, rather than $\geq b_2^2$. The argument of the previous paragraph lets us reduce to $\operatorname{supp}(s_1) \subseteq b_1 M$. Writing $s_1 = b_1 s_1'$ with $s_1' \in T$, then (5.18) gives

$$r \cdot s = r_1 \cdot s_1' + r_2 \cdot s_2 \tag{5.20}$$

where $r_1 = r \cdot b_1$ and $r_2 = r \cdot r$ are homogeneous polynomials of degree 2.

Case 1.1: $r' = 0$ or $r' = b_4$. We compute directly (using (R8), (R9), (R12) and (R13)) that $\max \operatorname{supp}(r_1) = b_4 b_2$ and $\max \operatorname{supp}(r_2) = b_2 b_1$. By Lemma 5.13, it follows that either

$$s_1' = 0 \text{ or } \max \operatorname{supp}(r_1 \cdot s_1') \in b_4 b_2 M,$$

and that either

$$s_2 = 0 \text{ or } \max \operatorname{supp}(r_2 \cdot s_2) \in b_2 b_1 M.$$

Hence, if $s_1' \neq 0$ then $\max \operatorname{supp}(r \cdot s) = \max \operatorname{supp}(r_1 \cdot s_1') \geq b_4 b_2 \geq b_2$. Otherwise $s_2 \neq 0$ (because $s \neq 0$) and $\max \operatorname{supp}(r \cdot s) = \max \operatorname{supp}(r_2 \cdot s_2) \geq b_2 b_1 \geq b_2$.

Case 1.2: $r' = b_2$ or $r' = b_4 + b_2$. In this case we compute $\max \operatorname{supp}(r_1) = b_4 b_2$ and $\max \operatorname{supp}(r_2) = b_4 b_3$. By Lemma 5.13 we have

$$s_1' = 0 \text{ or } \max \operatorname{supp}(r_1 \cdot s_1') \in b_4 b_2 M,$$

and similarly

$$\operatorname{supp}(s_2) \subseteq b_1 M \text{ or } \max \operatorname{supp}(r_2 \cdot s_2) \in b_4 b_3 M.$$

Thus, if $\operatorname{supp}(s_2) \not\subseteq b_1 M$ then $\max \operatorname{supp}(r \cdot s) = \max \operatorname{supp}(r_2 \cdot s_2) \geq b_4 b_3 \geq b_2$. Hence we may assume that $s_2 = b_1 s_2'$ for some $s_2' \in T$.

If $r' = b_2$, then we take $s_1'' = s_1' + (b_1 + b_2) \cdot s_2'$. We can rewrite (5.20) as

$$r \cdot s = r_1 \cdot s_1' + r_2 \cdot b_1 s_2' = r_1 \cdot (s_1'' + (b_1 + b_2) \cdot s_2') + r_2 \cdot b_1 s_2' = r_1 \cdot s_1'' + r_2' \cdot s_2'$$

where $r_2' = r_1 \cdot (b_1 + b_2) + r_2 \cdot b_1$. Note that r_2' is a homogeneous polynomial of degree 3, and we can check directly that $\max \operatorname{supp}(r_2') = b_2 b_4 b_2$. Thus by Lemma 5.13 we have either

$$s_2' = 0 \text{ or } \max \operatorname{supp}(r_2' \cdot s_2') \in b_2 b_4 b_2 M,$$

and also either

$$s_1'' = 0 \text{ or } \max\operatorname{supp}(r_1 \cdot s_1'') \in b_4b_2M.$$

Hence, if $s_1'' \neq 0$ then $\max\operatorname{supp}(r \cdot s) \geq b_4b_2 \geq b_2$. Otherwise $s_2' \neq 0$ (since $s \neq 0$) and $\max\operatorname{supp}(r \cdot s) \geq b_2b_4b_2 \geq b_2$ as desired.

If $r' = b_4 + b_2$ then we use the same argument, except that in this case we take $s_1'' = s_1' + b_2 \cdot s_2'$. Then (5.20) gives

$$r \cdot s = r_1 \cdot s_1' + r_2 \cdot b_1s_2' = r_1 \cdot (s_1'' + b_2 \cdot s_2') + r_2 \cdot b_1s_2' = r_1 \cdot s_1'' + r_2' \cdot s_2'$$

where $r_2' = r_1 \cdot b_2 + r_2 \cdot b_1$. We check that $\max\operatorname{supp}(r_2') = b_2b_4b_2$, so that the conclusion is the same as above.

Case 2: $b_3 \in \operatorname{supp}(r)$.

Recall that we are assuming that $\operatorname{supp}(s_1) \subseteq b_1M \cup b_2b_1M$. Write $s_1 = b_1s_1' + b_2b_1s_1''$ with $s_1', s_1'' \in T$. Then (5.18) becomes

$$r \cdot s = r \cdot (b_1s_1' + b_2b_1s_1'') + r \cdot r \cdot s_2 = r_1 \cdot s_1' + r_2 \cdot s_1'' + r_3 \cdot s_2 \tag{5.21}$$

where $r_1 = r \cdot b_1$, $r_2 = r \cdot b_2b_1$ and $r_3 = r \cdot r$. Note that r_1, r_3 are homogeneous of degree 2 and r_2 is homogeneous of degree 3. We can check that, for each of the four cases for r', we always get $\max\operatorname{supp}(r_1) = b_4b_2$, $\max\operatorname{supp}(r_2) = b_4b_2^2$ and $\max\operatorname{supp}(r_3) = b_4^2$. Thus, if $s_2 \neq 0$ then Lemma 5.13 gives

$$\max\operatorname{supp}(r \cdot s) = \max\operatorname{supp}(r_3 \cdot s_2) \in b_4^2M \cup b_4b_3b_2M$$

and thus $\max\operatorname{supp}(r \cdot s) \geq b_2^2$. Hence we may assume that $s_2 = 0$.

Case 2.1: $r' = b_4 + b_3$ or $r' = b_4 + b_3 + b_2$. We set $s_1''' = s_1' + b_2 \cdot s_1''$. Rewriting (5.21) we get

$$r \cdot s = r_1 \cdot (s_1''' + b_2 \cdot s_1'') + r_2 \cdot s_1'' = r_1 \cdot s_1''' + r_2' \cdot s_1''$$

where $r_2' = r_1 \cdot b_2 + r_2$. We compute $\max\operatorname{supp}(r_2') = b_3b_2b_1$. Hence, if $s_1''' \neq 0$ then Lemma 5.13 gives

$$\max\operatorname{supp}(r \cdot s) = \max\operatorname{supp}(r_1 \cdot s_1''') \in b_4b_2M.$$

Otherwise $s_1'' \neq 0$ and hence Lemma 5.13 gives

$$\max\operatorname{supp}(r \cdot s) = \max\operatorname{supp}(r_2' \cdot s_1'') \in b_3b_2b_1M.$$

Thus we have $\max\operatorname{supp}(r \cdot s) \geq b_2^2$ in any case.

Case 2.2: $r' = b_3$ or $r' = b_3 + b_2$. We use the same argument, except that in this case we set $s_1''' = s_1' + (b_1 + b_2) \cdot s_1''$. Then (5.21) gives

$$r \cdot s = r_1 \cdot (s_1''' + (b_1 + b_2) \cdot s_1'') + r_2 \cdot s_1'' = r_1 \cdot s_1''' + r_2' \cdot s_1''$$

where $r_2' = r_1 \cdot (b_1 + b_2) + r_2$. We have $\max\operatorname{supp}(r_2') = b_3b_2b_1$, so the conclusion is the same as above. □

Our next step is to investigate the right side of (5.9). Particularly, we are interested in the possible monomials belonging to the support of $\delta(r)$. Recall that we defined $\delta(r) = b_0 \cdot r + r \cdot b_0$. The following lemma captures the information we will need.

Lemma 5.22. *For every $u \in M$, $t \in S$, and $v \in \operatorname{supp}(\delta(u) \cdot t)$, then $v < u$. Moreover, if $u = pb_i$ for some $p \in M$ and $1 \leq i \leq 5$, then*

(1) *$v < p$ for $i \in \{1, 4, 5\}$,*
(2) *$v < pb_2$ for $i = 2$, and*

(3) $v < pb_2^2$ *for* $i = 3$.

Proof. We use induction on $\deg(u)$. If $u = 1$ then $\delta(u) = 0$ and all the inequalities hold vacuously. Assuming $\deg(u) \geq 1$, write $u = pb_i$ for some $p \in M$ and $1 \leq i \leq 5$, with $\deg(p) < \deg(u)$. Then $\delta(u) = \delta(p) \cdot b_i + p \cdot \delta(b_i)$, hence $v \in \operatorname{supp}(\delta(u) \cdot t)$ yields either $v \in \operatorname{supp}(\delta(p) \cdot b_i \cdot t)$ or $v \in \operatorname{supp}(p \cdot \delta(b_i) \cdot t)$.

In the first case, the inductive hypothesis gives $v < p$, and hence also $v < pb_i = u$, as desired. In the second case, the only nontrivial possibilities are $i = 2$ and $i = 3$, since otherwise $\delta(b_i) = 0$. If $i = 2$ then $\delta(b_i) = b_1^2$, hence $v \in \operatorname{supp}(p \cdot b_1^2 \cdot t)$. By Lemma 5.12 it follows $v < pb_2 = u$. If $i = 3$ then $\delta(b_i) = b_2b_1 + b_1b_2$, hence $v \in \operatorname{supp}(p \cdot b_1b_2 \cdot t)$ or $v \in \operatorname{supp}(p \cdot b_2b_1 \cdot t)$. As before, we apply Lemma 5.12 to conclude that

$$v < pb_2^2 < pb_3 = u.$$

This completes the inductive step. □

Let $r, s, t \in S$ be as in Lemma 5.8. There is one immediate simplification we can make when checking the nonequality (5.9). If $r \neq 0$ then $b_1 \cdot r = b_1 r \neq 0$. Also $\delta(b_1 \cdot r) = b_1 \cdot \delta(r) + \delta(b_1) \cdot r = b_1 \cdot \delta(r)$. Therefore, after replacing r by $b_1 \cdot r$ if necessary, we now assume $1 \notin \operatorname{supp}(r)$.

Before finally proving the nonequality (5.9), we need some more notation. For each $p \in M$ let $I_p = \{i \in \{1, 2, 3, 4, 5\} \,:\, pb_i \in \operatorname{supp}(r)\}$. (Note that I_p relies implicitly on r. We did not include r in the notation for simplicity, and we will continue to follow this notational choice.) Further, let $A = \{p \in M \,:\, I_p \neq \emptyset\}$. We can thus decompose r in the form

$$r = \sum_{p \in A} \left(\sum_{i \in I_p} pb_i \right). \tag{5.23}$$

We think of each $p \in A$ as a "left prefix" of the homogeneous element $\sum_{i \in I_p} b_i$, which has degree 1 and is thus amenable to the work in our previous lemmas.

Let $p_{\max} = \max A$. The monomial $p_{\max}$ is an important element of A, but there is another monomial that plays an even more critical role. The definition of this monomial is somewhat complicated. First, define

$$\begin{aligned} A_1 &= \{p \in A \,:\, p_{\max} \in pb_1M \text{ and } I_p \neq \{1\}\} \text{ and} \\ A_2 &= \{p \in A \,:\, p_{\max} \in pb_2M,\ 3 \in I_p, \text{ and } pb_2b_iM \cap \operatorname{supp}(r) = \emptyset \text{ for each } i \geq 2\}. \end{aligned}$$

One may think of the conditions defining the sets A_1 and A_2 as collecting those $p \in A$ which can extend to the right only in certain ways. We then put

$$p_0 = \begin{cases} \min A_1 \cup A_2 & \text{if } A_1 \cup A_2 \neq \emptyset, \\ p_{\max} & \text{otherwise.} \end{cases} \tag{5.24}$$

From the first defining condition in both A_1 and A_2, we see that in every case

$$p_{\max} \in p_0M. \tag{5.25}$$

We define one further auxiliary monomial

$$q_0 = \begin{cases} p_0 & \text{if } I_{p_0} = \{1\}, \\ p_0b_2 & \text{if } 3 \notin I_{p_0} \text{ and } I_{p_0} \neq \{1\}, \\ p_0b_2^2 & \text{if } 3 \in I_{p_0}. \end{cases}$$

The monomial q_0 is related to some of the bounds we found in the previous lemmas, and helps simplify the statement of the following lemma.

Lemma 5.26. *If $p \in A$, then one of the following three conditions holds:*

(1) *$pm < q_0$ for each $m \in M$,*
(2) *$p_0 \in pM$, or*
(3) *$p = p_0 b_2$, $I_p = \{1\}$, and $3 \in I_{p_0}$.*

Proof. Consider the case when $\deg(p) \leq \deg(p_0)$. If $p > p_0$, then $p > p_{\max}$ by (5.25) and Lemma 5.10(2), which is impossible. Thus $p \leq p_0$ and hence either $p_0 \in pM$ or $pm < p_0 \leq q_0$, for each $m \in M$, by Lemma 5.10.

Now assume $\deg(p) > \deg(p_0)$. If $p < p_0$, then Lemma 5.10(2) tells us that condition (1) holds. So we may assume $p \geq p_0$. By Lemma 5.10(2) we get either $p > p_0 m$ for each $m \in M$ or $p \in p_0 M$. The first case contradicts (5.25), so that $p \in p_0 M$. There are now three cases to consider, according to how p_0 was defined.

First, if $p_0 \in A_1$ then $p \leq p_{\max} \in p_0 b_1 M$. As $\deg(p) > \deg(p_0)$, we must have $p \in p_0 b_1 M$. Therefore, $pm < p_0 b_2 \leq q_0$ for each $m \in M$.

Second, if $p_0 \in A_2$ then $p \leq p_{\max} \in p_0 b_2 M$. As $\deg(p) > \deg(p_0)$, either $p \in p_0 b_1 M$ or $p \in p_0 b_2 M$. When $p \in p_0 b_1 M$, the same analysis as in the previous paragraph still works; we may thus assume $p \in p_0 b_2 M$. The last defining condition for A_2 then tells us that either condition (3) of this lemma holds, or $p \in p_0 b_2 b_1 M$. In the latter case, $pm < p_0 b_2^2 = q_0$ for each $m \in M$.

Third, and finally, if $A_1 \cup A_2 = \emptyset$, then this contradicts the fact that $\deg(p) > \deg(p_0)$ and $p \geq p_0 = p_{\max}$. □

We are now prepared to prove Lemma 5.8.

Proof of Lemma 5.8. Let $r, s, t \in S$ with $r, s \neq 0$, and $1 \notin \operatorname{supp}(r)$. Let $p_{\max}$, p_0, and q_0 be as defined above. Also let s' be the homogeneous component of s of largest degree. Our analysis relies heavily on the decomposition (5.23).

By Lemma 5.16, we know that $\left(\sum_{i \in I_{p_0}} b_i\right) \cdot s' \neq 0$. Let u be the maximal monomial in the support of this product. By the additional information in Lemma 5.16, we know that $u \geq b_2^2$ when $3 \in I_{p_0}$, and also that $u \geq b_2$ when $I_{p_0} \neq \{1\}$. Notice that $p_0 \notin M b_5$ since $I_{p_0} \neq \emptyset$. Further $p_0 \notin M b_3 \cup M b_4$ if $1 \in I_{p_0}$. Therefore $q = p_0 u$ is a reduced monomial. Further, this must be the maximal monomial in the support of $p_0 \cdot \left(\sum_{i \in I_{p_0}} b_i \cdot s'\right)$ by Lemma 5.10(1) and Lemma 5.12. Clearly, $q = p_0 u \geq q_0$.

Now, just from degree considerations, we see that

$$q \in \operatorname{supp}\left(\sum_{i \in I_{p_0}} p_0 b_i \cdot s\right).$$

We will show, for each $p \in A \setminus \{p_0\}$ and each

$$w \in \operatorname{supp}\left(\sum_{i \in I_p} p b_i \cdot s\right),$$

that $w \neq q$, thus showing that q belongs to the support of the left side of (5.9). We do this by analyzing the three cases that arise in Lemma 5.26, separately. If condition (1) of Lemma

5.26 holds, then Lemma 5.12 immediately gives $w \leq pm < q_0 \leq q$ (for some $m \in M$). If condition (2) holds, with $p \neq p_0$, then $\deg(p) < \deg(p_0)$ and hence $\deg(w) < \deg(q)$. Finally, if condition (3) holds, then $\sum_{i \in I_p} pb_i = pb_1 = p_0 b_2 b_1$, and then Lemma 5.12 gives us the first inequality in the chain

$$w \leq p_0 b_2 b_1 m < p_0 b_2^2 = q_0 \leq q,$$

for some $m \in M$, with the last equality coming from the fact that $3 \in I_{p_0}$ (again from condition (3) of Lemma 5.26).

All that remains is to show that q does not belong to the support of the right side of (5.9). It suffices to show, for each $p \in A$, each $i \in I_p$, and each

$$v \in \operatorname{supp}(\delta(pb_i) \cdot t),$$

that $v < q_0$. We again do this by cases. If condition (1) of Lemma 5.26 holds, then the inequality in the first sentence of Lemma 5.22 gives us $v < pb_i < q_0$. If condition (3) of Lemma 5.26 holds, then $pb_i = p_0 b_2 b_1$ and the inequality in the first sentence of Lemma 5.22 yields $v < p_0 b_2 b_1 < p_0 b_2^2 = q_0$. Thus, only condition (2) of Lemma 5.26 remains.

Write $p_0 = pm$ for some $m \in M$. For $i \in \{1, 4, 5\}$, then Lemma 5.22(1) gives us $v < p \leq p_0 \leq q_0$.

For $i = 2$, then Lemma 5.22(2) gives us $v < pb_2$. When $m = 1$ we have $pb_2 = p_0 b_2 \leq q_0$, which suffices. Assuming $m \neq 1$, suppose by way of contradiction that $m \in b_1 M$. By (5.25) we find

$$p_{\max} \in p_0 M = pmM \subseteq pb_1 M.$$

But also $I_p \neq \{1\}$ (since $2 \in I_p$), and hence $p \in A_1$, contradicting the minimality of $p_0 = pm > p$. Therefore $m \notin b_1 M$, and hence $v < pb_2 \leq pm = p_0 \leq q_0$.

For $i = 3$, then Lemma 5.22(2) gives us $v < pb_2^2$. When $m = 1$ we have $pb_2^2 = p_0 b_2^2 = q_0$, so assume $m \neq 1$. Then $p < p_0$ and so $p \notin A_1 \cup A_2$ (by the minimality assumption on p_0). Just as in the previous paragraph, from knowing $p \notin A_1$ we have $m \notin b_1 M$. If $m \geq b_2^2$ then $v < pb_2^2 \leq pm = p_0 \leq q_0$. Thus either $m \in b_2 b_1 M$ or $m = b_2$.

First consider the possibility that $m \in b_2 b_1 M$. As $p_{\max} \in p_0 M \subseteq pb_2 b_1 M$ and $3 \in I_p$, we see that $p \notin A_2$ implies that $pb_2 b_j m' \in \operatorname{supp}(r)$ for some $m' \in M$ and $j \geq 2$. If $m' \neq 1$, this would contradict the maximality of $p_{\max} \in pb_2 b_1 M$. Thus $m' = 1$, entailing $pb_2 \in A_1$ (since then $j \in I_{pb_2}$ and $p_{\max} \in pb_2 b_1 M$), contradicting the fact that $pb_2 < p_0$.

Finally, suppose that $m = b_2$, so that $p_0 = pb_2$. If $I_{p_0} \neq \{1\}$, then

$$v < pb_2^2 = p_0 b_2 \leq q_0.$$

Thus, we may assume $I_{p_0} = \{1\}$, which implies $p_0 \notin A_1 \cup A_2$, hence $p_0 = p_{\max}$. From the maximality of $p_{\max}$, and the fact that $I_{p_{\max}} = \{1\}$, we have

$$pb_2 M \cap \operatorname{supp}(r) = p_{\max} M \cap \operatorname{supp}(r) \subseteq \{p_{\max}, p_{\max} b_1\}.$$

Thus p satisfies all the conditions to belong to A_2, showing that this case cannot happen. □

Having proved Lemma 5.8, the proof of Theorem 5.7 is now complete. Hence, we are ready to state:

Theorem 5.27. *There exists a ring R such that $\operatorname{Nil}(R)^2 = 0$ and $\operatorname{Nil}(R)[x] \subsetneq \operatorname{Nil}(R[x])$.*

Proof. By Theorem 5.7, the ring R defined in (5.5) satisfies $\operatorname{Nil}(R) \subseteq b_0 \cdot R \cap R \cdot b_0$. As $b_0^2 = 0$, it follows that $\operatorname{Nil}(R)^2 = 0$. Clearly, this also implies that $\operatorname{Nil}(R)[x] \subseteq \operatorname{Nil}(R[x])$.

Let $f \in R[x]$ be defined as

$$f = b_0 + b_1x + (b_0 + b_2)x^2 + (b_1 + b_3)x^3 + (b_2 + b_4)x^4 + (b_3 + b_5)x^5 + (b_4 + b_5)x^6 + b_0x^7.$$

Note that this is exactly the polynomial from the beginning of this section, where we used (5.2) and substitutions (5.3). One can check using (R1)–(R13) that f squares to zero as a polynomial over R. Moreover, $b_1 \notin \mathrm{Nil}(R)$ since $b_1^n \in \langle X \rangle_{\mathrm{irr}}$ for each integer $n \geq 1$, and hence $f \notin \mathrm{Nil}(R)[x]$. □

We conclude this section by explaining the role of our example in the theory of Armendariz rings. In [3], Antoine introduced a generalization of Armendariz rings called *nil-Armendariz* rings. These are unital rings R with the property that for any two polynomials $f = \sum_{i=0}^{m} a_i x^i$ and $g = \sum_{j=0}^{n} b_j x^j$ in $R[x]$, if $fg \in \mathrm{Nil}(R)[x]$ then $a_i b_j \in \mathrm{Nil}(R)$ for all integers $i, j \geq 0$. Antoine derived many properties of nil-Armendariz rings, such as the fact that Armendariz rings are nil-Armendariz. If R is nil-Armendariz then it satisfies the inclusion $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$, and $\mathrm{Nil}(R)$ forms a subring of R.

Antoine in [3, Question 2] (see also the diagram on page 4133 of [4]) raised the question whether every unital ring R such that $\mathrm{Nil}(R)$ is a subring (i.e., R is a NR ring) is nil-Armendariz. With our example at hand, we can now answer this question:

Corollary 5.28. *There exists a unital, NR ring that is not nil-Armendariz.*

Proof. The ring R constructed above satisfies $\mathrm{Nil}(R)^2 = 0$, hence it is a NR ring. By the contrapositive of [3, Lemma 5.1], the ring R is not nil-Armendariz. □

Remark 5.29. As shown by Antoine, nil-Armendariz rings are exactly those rings that are Armendariz modulo the upper nilradical, see [3, Theorem 3.5]. Also note that a ring R is NR if and only if $R/\mathrm{Nil}^*(R)$ is NR; here $\mathrm{Nil}^*(R)$ is the upper nilradical, as usual. Hence, Antoine's question is actually equivalent to the question whether every unital NR ring R with $\mathrm{Nil}^*(R) = 0$ is Armendariz.

It may be interesting to notice that the ring R we have constructed satisfies $\mathrm{Nil}^*(R) = 0$. To prove this, take any $r \in \mathrm{Nil}^*(R)$. Since $\mathrm{Nil}(R) = b_0 \cdot R \cap R \cdot b_0 \subseteq b_0 S$, we may write $r = b_0 s$ for some $s \in S$. Now,

$$b_2 \cdot r = b_2 \cdot b_0 s = (b_0 b_2 + b_1^2) \cdot s = b_0 b_2 s + b_1^2 s.$$

Since $b_2 \cdot r \in \mathrm{Nil}(R) \subseteq b_0 S$, it follows that $b_1^2 s = 0$ and therefore $s = 0$. Hence $r = 0$ as desired.

Remark 5.30. Note that $\mathbb{F}_2\langle b_1, b_2 \rangle \subseteq R$ is free in the variables b_1 and b_2. As pointed out by one of the referees, this may be of interest as Smoktunowicz has constructed a nil algebra whose iterated polynomial extension contains a free subalgebra. As far as we know it is an open question how many iterations of the polynomial extension are needed, but our construction may shed light on that question.

6. Final Remarks

In this section we study the connections between the different properties studied in this paper. In Section 2 we have shown that each of the inclusions between the sets $\mathrm{Nil}(R)[x]$ and $\mathrm{Nil}(R[x])$ is related to the NR property for the ring R. The following proposition describes some more natural situations where we can get information on the sets $\mathrm{Nil}(R[x])$ and $\mathrm{Nil}(R)[x]$. For convenience, below when we write $S \subseteq R$, $S \leq R$, or $S \trianglelefteq R$, we mean, respectively, that S is a subset, subring, or (two-sided) ideal of R.

Proposition 6.1. *For any ring R the following hold:*

(1) $\mathrm{Nil}(R) \leq R$ *if and only if* $\mathrm{Nil}(R)[x] \leq R[x]$.
(2) $\mathrm{Nil}(R) \trianglelefteq R$ *if and only if* $\mathrm{Nil}(R)[x] \trianglelefteq R[x]$.
(3) $\mathrm{Nil}(R[x]) \leq R[x]$ *if and only if* $\mathrm{Nil}(R)[x] = \mathrm{Nil}(R[x])$.
(4) *If* $\mathrm{Nil}(R) \trianglelefteq R$ *then* $\mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$.
(5) $\mathrm{Nil}(R[x]) \trianglelefteq R[x]$ *if and only if both* $\mathrm{Nil}(R)[x] \subseteq \mathrm{Nil}(R[x])$ *and* $\mathrm{Nil}(R) \trianglelefteq R$.

Proof. (1) and (2) are straightforward verifications, and (3) is [21, Corollary 2.5]. To prove (4), assume that $\mathrm{Nil}(R)$ is an ideal. Then the factor ring $\overline{R} = R/\mathrm{Nil}(R)$ is defined and has no nonzero nilpotent elements. Thus $\mathrm{Nil}(\overline{R}[x]) = 0$, as any leading term of a nilpotent polynomial must have been zero. Under the natural map $\varphi\colon R[x] \to \overline{R}[x]$, the set $\mathrm{Nil}(R[x])$ maps into $\mathrm{Nil}(\overline{R}[x]) = 0$. Hence $\mathrm{Nil}(R[x]) \subseteq \ker(\varphi) = \mathrm{Nil}(R)[x]$.

(5): Assuming $\mathrm{Nil}(R[x]) \trianglelefteq R[x]$, we trivially have $\mathrm{Nil}(R) \trianglelefteq R$, and also $\mathrm{Nil}(R)[x] = \mathrm{Nil}(R[x])$ by (3). Conversely, assume $\mathrm{Nil}(R)[x] \subseteq \mathrm{Nil}(R[x])$ and $\mathrm{Nil}(R) \trianglelefteq R$. By (4) we have $\mathrm{Nil}(R)[x] = \mathrm{Nil}(R[x])$, and hence $\mathrm{Nil}(R[x]) = \mathrm{Nil}(R)[x] \trianglelefteq R[x]$ by (2). □

With all the work we have done we will now prove that Figure 6.2, below, is an Euler diagram for the classes of rings R satisfying the stated properties, except that the region marked with **?** might be empty (see Question 2.4).

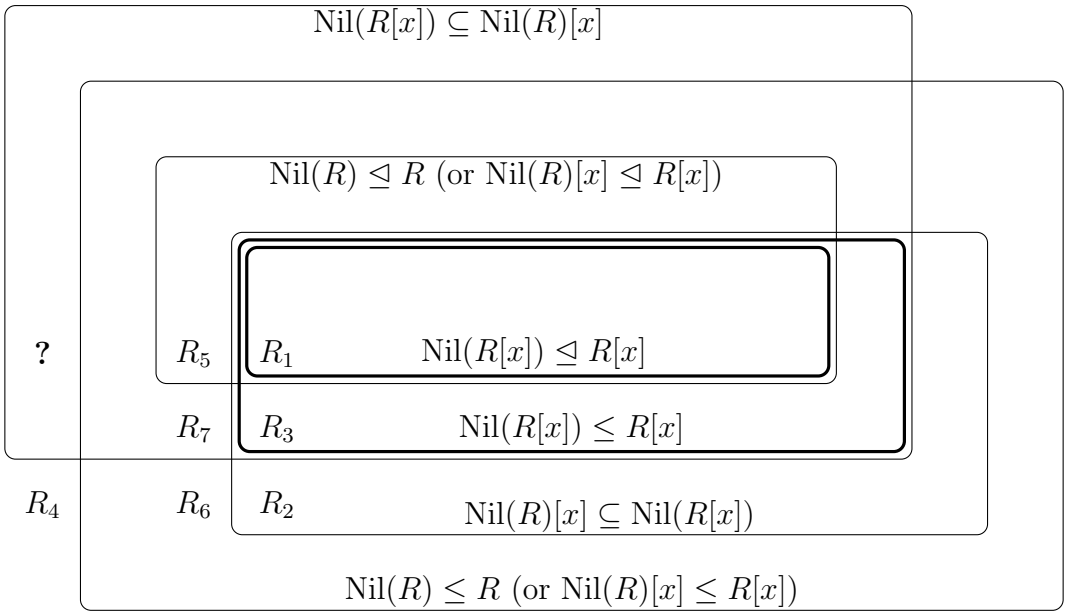


FIGURE 6.2. Inclusions among some classes of rings.

The two implications

$$\mathrm{Nil}(R)[x] \subseteq \mathrm{Nil}(R[x]) \Rightarrow \mathrm{Nil}(R) \leq R$$

and

$$\mathrm{Nil}(R) \trianglelefteq R \Rightarrow \mathrm{Nil}(R[x]) \subseteq \mathrm{Nil}(R)[x]$$

are consequences of Propositions 2.1 and 6.1(4), respectively. Further, both of the parenthetical equivalences written in the diagram are consequences of Proposition 6.1, parts

(1) and (2). Moreover, the two intersections (marked with thick lines) are consequences of Proposition 6.1, parts (3) and (5).

It now suffices to show that each region, except the one marked with **?**, is nonempty. First, any commutative ring R_1 belongs to all four boxes. Second, in the previous section we constructed a ring R for which $\mathrm{Nil}(R)[x] \subseteq \mathrm{Nil}(R[x])$ holds but the reverse inclusion fails; call any such ring R_2.

Third, the ring $R_3 = \mathbb{Z}\langle a, b \,:\, a^2 = 0\rangle$ is Armendariz and hence it satisfies $\mathrm{Nil}(R_3)[x] = \mathrm{Nil}(R_3[x])$, but $\mathrm{Nil}(R_3)$ is not an ideal of R_3. Fourth, the ring R_4 of 2×2 matrices over a field does not satisfy any of the four properties.

Fifth, let R_5 be a nil ring such that $R_5[x]$ is not nil (as in [20]). Then $\mathrm{Nil}(R_5) = R_5$ is an ideal of R_5, but $\mathrm{Nil}(R_5)[x] \not\subseteq \mathrm{Nil}(R_5[x])$.

Finally, it is straightforward to check that:

- $R_6 = R_2 \times R_5$ has $\mathrm{Nil}(R_6)$ as a subring but there are no inclusions between $\mathrm{Nil}(R_6)[x]$ and $\mathrm{Nil}(R_6[x])$, and
- $R_7 = R_3 \times R_5$ has $\mathrm{Nil}(R_7)$ as a subring but not an ideal, and $\mathrm{Nil}(R_7[x]) \subseteq \mathrm{Nil}(R_7)[x]$ holds but not the reverse inclusion.

Acknowledgements

We thank George Bergman for comments on an earlier draft of the paper. We also thank the two referees for extensive comments that helped improve the quality of the paper, and for the suggestion to include an implication diagram in the introduction. The work of the third author was supported by the Slovenian Research Agency (grant number P1—0222).

References

[1] A. S. Amitsur, *Algebras over infinite fields*, Proc. Amer. Math. Soc. **7** (1956), no. 1, 35–48. MR 75933
[2] S. A. Amitsur, *Radicals of polynomial rings*, Canadian J. Math. **8** (1956), 355–361. MR 78345
[3] Ramon Antoine, *Nilpotent elements and Armendariz rings*, J. Algebra **319** (2008), no. 8, 3128–3140. MR 2408310
[4] Ramon Antoine, *Examples of Armendariz rings*, Comm. Algebra **38** (2010), no. 11, 4130–4143. MR 2764855
[5] Efraim P. Armendariz, *A note on extensions of Baer and P.P.-rings*, J. Austral. Math. Soc. **18** (1974), no. 4, 470–473. MR 366979
[6] George M. Bergman, *Modules over coproducts of rings*, Trans. Amer. Math. Soc. **200** (1974), 1–32. MR 357502
[7] George M. Bergman, *The diamond lemma for ring theory*, Adv. in Math. **29** (1978), no. 2, 178–218. MR 506890
[8] Victor Camillo and Pace P. Nielsen, *McCoy rings and zero-divisors*, J. Pure Appl. Algebra **212** (2008), no. 3, 599–615. MR 2365335
[9] Weixing Chen, *On linearly weak Armendariz rings*, J. Pure Appl. Algebra **219** (2015), no. 4, 1122–1130. MR 3282130
[10] Kwang Jin Choi, Tai Keun Kwak, and Yang Lee, *Rings whose nilpotents form a multiplicative set*, Comm. Algebra **46** (2018), no. 8, 3229–3240. MR 3788991
[11] Young Chun, Young Cheol Jeon, Sungkyung Kang, Key Nyoung Lee, and Yang Lee, *A concept unifying the Armendariz and NI conditions*, Bull. Korean Math. Soc. **48** (2011), no. 1, 115–127. MR 2778501
[12] Chan Yong Hong, Nam Kyun Kim, Yang Lee, and Pace P. Nielsen, *Amitsur's property for skew polynomials of derivation type*, Rocky Mountain J. Math. **47** (2017), no. 7, 2197–2218. MR 3748228
[13] Roger A. Horn and Charles R. Johnson, *Topics in matrix analysis*, Cambridge University Press, Cambridge, 1991. MR 1091716

[14] Jan Krempa, *Logical connections between some open problems concerning nil rings*, Fund. Math. **76** (1972), no. 2, 121–130. MR 306251
[15] Tai Keun Kwak and Yang Lee, *Rings over which coefficients of nilpotent polynomials are nilpotent*, Internat. J. Algebra Comput. **21** (2011), no. 5, 745–762. MR 2827201
[16] T.Y. Lam, A. Leroy, and J. Matczuk, *Primeness, semiprimeness and prime radical of Ore extensions*, Comm. Algebra **25** (1997), no. 8, 2459–2506. MR 1459571
[17] Pace P. Nielsen, *Simplifying Smoktunowicz's extraordinary example*, Comm. Algebra **41** (2013), no. 11, 4339–4350. MR 3169522
[18] Vassilis G. Papanicolaou, *Generalized (or confluent) Vandermonde determinants*, Online notes accessed at `http://www.math.ntua.gr/~papanico/` (2019), 1–6.
[19] M. B. Rege and Sima Chhawchharia, *Armendariz rings*, Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), no. 1, 14–17. MR 1442245
[20] Agata Smoktunowicz, *Polynomial rings over nil rings need not be nil*, J. Algebra **233** (2000), no. 2, 427–436. MR 1793911
[21] Janez Šter, *Rings in which nilpotents form a subring*, Carpathian J. Math. **32** (2016), no. 2, 251–258. MR 3587893

Department of Mathematics, Brigham Young University, Provo, UT 84602, USA
Email address: `shaletome@gmail.com`

Department of Mathematics, Brigham Young University, Provo, UT 84602, USA
Email address: `pace@math.byu.edu`

Faculty of Mathematics and Physics, University of Ljubljana, Jadranska 21, 1000 Ljubljana, Slovenia
Email address: `janez.ster@fmf.uni-lj.si`