Edinburgh Research Explorer

How far can we go with Amitsur's conjecture in differential polynomial rings?

Link:
Link to publication record in Edinburgh Research Explorer

Document Version:
Peer reviewed version

Published In:
Israel journal of mathematics

HOW FAR CAN WE GO WITH AMITSUR'S THEOREM IN DIFFERENTIAL POLYNOMIAL RINGS?

AGATA SMOKTUNOWICZ

ABSTRACT. A well-known theorem by S.A. Amitsur shows that the Jacobson radical of the polynomial ring $R[x]$ equals $I[x]$ for some nil ideal I of R. In this paper, however, we show that this is not the case for differential polynomial rings, by proving that there is a ring R which is not nil and a derivation D on R such that the differential polynomial ring $R[x; D]$ is Jacobson radical. We also show that, on the other hand, the Amitsur theorem holds for a differential polynomial ring $R[x; D]$, provided that D is a locally nilpotent derivation and R is an algebra over a field of characteristic $p > 0$. The main idea of the proof introduces a new way of embedding differential polynomial rings into bigger rings, which we name platinum rings, plus a key part of the proof involves the solution of matrix theory-based problems.

1. INTRODUCTION

Let R be a noncommutative associative ring. In 1956, S.A. Amitsur proved that the Jacobson radical of the polynomial ring $R[x]$ equals $I[x]$ for some nil ideal I of R [15]. Then in 1980, S. S. Bedi and J. Ram extended Amitsur's theorem to skew polynomial rings of automorphism type [5]. The question then arises as to whether Amitsur's theorem also holds for differential polynomial rings; that is, whether the Jacobson radical of $R[x; D]$ equals $I[x; D]$ for a nil ideal I of R. In 1975, D. A. Jordan [12] showed that Amitsur's theorem holds for differential polynomial rings $R[x; D]$, provided that R is a Noetherian ring with an identity, and in 1983, M. Ferrero, K. Kishimoto and K. Motose [8] showed that in the general case the Jacobson radical of $R[x, D]$ equals $I[x, D]$ for an ideal I of R (and I is nil if R is commutative). However, it remained an open question as to whether I needs to be nil. We will answer this question in the negative, by proving the following theorem.

Theorem 1. *Let K be an arbitrary subfield of the algebraic closure of a finite field. There is an K-algebra R and a derivation D on R such that R is not nil and the algebra $R[x; D]$ is Jacobson radical.*

In particiular there is a ring R which is not nil and a derivation D on R such that the ring $R[x; D]$ is Jacobson radical.

Let F be the algebraic closure of a finite field, and let R be an F-algebra. Let K be a subfield (possibly finite) of the field F, then R is also a K-algebra. Moreover, R is nil as a K-algebra if and only if R is nil as an F-algebra; similarly $R[x; D]$ is Jacobson radical as a K-algebra if and only if $R[x; D]$ is Jacobson radical as an F-algebra. Therefore Theorem 1 also holds in the case when K is a finite field.

However, in the case when D is a locally nilpotent derivation we are able to show the following.

Theorem 2. *Let F be a field of characteristic $p > 0$, let R be an F-algebra and D be a derivation on R. If D is a locally nilpotent derivation, then the Jacobson radical of the differential polynomial ring $R[x; D]$ equals $I[x]$ for some nil ideal I of R.*

In 1987, J. Bergen, S. Montgomery and D.S. Passman showed that Amitsur's theorem also holds for differential polynomial rings in the case where R is a polynomial identity algebra, and obtained far-reaching related results for enveloping algebras of Lie algebras and crossed products [4]. Surprising applications of derivations in Lie algebras and nil algebras were found by V. M. Petrogradsky, I.P. Shestakov and E. Zelmanov [22, 23, 26]. We also note that the Jacobson radical of a ring $R[x; D]$ in the case when R has no nil ideals was investigated by P. Grzeszczuk and J. Bergen [9]. For other results on such rings, see [18, 31]. Interesting results in the case where R is a polynomial identity ring were obtained by J. Bell, B. Madill and F. Shinko in [3], and by B. Madill in [17]; for example, in [3] it was shown that, if R is a locally nilpotent ring satisfying a polynomial identity, then $R[x; D]$ is Jacobson radical. This does not hold in general for an arbitrary locally nilpotent ring R (see [30]).

It was shown by J. Krempa [14] that the Koethe conjecture is equivalent to the assertion that polynomial rings over nil rings are Jacobson radical. Notice that logically Amitsur's result works in the opposite direction to the Koethe problem. In the direction of Amitsur it was shown by P. Nielsen and M. Ziembowski [19] that $R[x; D]$ need not be prime radical provided that R is a commutative nil ring of bounded index of nilpotency. Recall also that it was shown in [8] that if $R[x; D]$

is Jacobson radical then R is Jacobson radical. Notice that if R is an algebra over a field whose cardinality exceeds the dimension of R as a vector space over F, and such that $R[x; D]$ is Jacobson radical, then $R[x; D]$ is nil and hence R is nil [2]. The following questions remain open.

Question 1. *Let R be a ring without nil ideals, and D a derivation on R; does it follow then that $R[x; D]$ is semiprimitive?*

Notice that by Theorem 2 the answer to Question 1 is affirmative when R is an algebra over a field of positive characteristic and D is locally nilpotent.

Question 2. *Let F be a field of characteristic $p > 0$, let R be an F-algebra and D be a locally nilpotent derivation on R. Suppose that $R[x; D]$ is nil. Does it follow that $R[x]$ is nil?*

Question 3. *Are there examples as in Theorem 1, over the base field of characteristic 0, or over non-algebraic extensions of finite fields?*

Question 4. *The examples constructed in Theorem 1 are not finitely generated F-algebras. Is it possible to construct finitely generated examples?*

Question 5. *Is Theorem 2 valid over fields of characteristic zero?*

Question 6. *It was proved in [28] that any primitive ideal in $R[x]$, where R is nil has the form $I[x]$. Is the analogous result valid for the differential polynomial setting?*

Let D be a derivation on a ring R. Recall that the differential polynomial ring $R[x; D]$ consists of all polynomials of the form $a_n x^n + \ldots + a_1 x + a_0$, where $a_i \in R$ for $i = 0, 1, 2 \ldots, n$. The ring $R[x; D]$ is considered with pointwise addition and multiplication given by $x^i x^j = x^{i+j}$ and $xa - ax = D(a)$, for all $a \in R$. For a given ring A we denote by A^1 the usual extension with an identity of the ring A. In a non-unital algebra we assume that the ideal generated by a given set of elements contains these elements. The main idea of the proof is contained in the following result.

Theorem 3. *Let $n > 1$ be a natural number. Let F be an infinite field, and let A' be a free (non-unital) F-algebra in generators $a_1, \ldots, a_n$ and x, and let $A^{(*)}$ be the ideal of A' generated by $a_1, \ldots, a_n$. Then $D(r) = xr - rx$ is a derivation on A'. Let P be the smallest subalgebra of A' containing elements $a_1, \ldots, a_n$ and closed under the action of D. Let I be an ideal in A' with the property that $\gamma_t(I) \subseteq I$ for*

every $t \in F$, where $\gamma_t : A' \to A'^1$ is the ring homomorphism such that $\gamma_t(a_i) = a_i$
for all $i = 1, \ldots, n$ and $\gamma_t(x) = x + t$. Then the F-algebra

$$A^{(*)}/I \cap A^{(*)}$$

is isomorphic to the differential ring $\bar{P}[y; D']$, where $\bar{P} = P/I \cap P$ and D' is the
derivation on $\bar{P}$ such that $D'(p + (I \cap P)) = xp - px + (I \cap P)$ for every $p \in P$.

Observe, on the other hand, that a differential polynomial F-algebra $R[x; D]$ can be, in a natural way, embedded into the factor ring $< R, x > /I$, where $< R, x >$ is the free product of R and the polynomial ring $F[x]$ and I is the ideal generated by relations $xr - rx - D(r)$. Notice that $\gamma_t(I) \subseteq I$ for every $t \in F$, where $\gamma_t :< R, x > \to < R, x >^1$ is the ring homomorphism such that $\gamma_t(r) = r$ for all $r \in R$ and $\gamma_t(x) = x + t$. This shows that differential polynomial rings have a presentation similar to the presentation from Theorem 39.

An outline of the proof for Theorem 1 now follows:

- Let F be a field, and let A' be a free algebra in generators a, b, x, and $A^{(*)}$ be the ideal of A' generated by a and b. We introduce ideal $I^{(*)}$ in $A^{(*)}$ which is generated by entries of powers of some matrices $X_1, X_2, \ldots$. It is then shown that $A^{(*)}/I^{(*)}$ is Jacobson radical.

- We introduce the platinum ideal $L(I^{(*)})$ of $A^{(*)}$. We define $L(I^{(*)})$ to be the smallest ideal such that $I^{(*)} \subseteq L(I^{(*)})$ and $\gamma_t(I^{(*)}) \subseteq L(I^{(*)})$ for every $t \in F$, where $\gamma_t : A' \to A'^1$ is the ring homomorphism such that $\gamma_t(a) = a$, $\gamma_t(b) = b$ and $\gamma_t(x) = x + t$.

- It is then shown that $A^{(*)}/L(I^{(*)})$ is isomorphic to some differential polynomial ring $Z[y; D]$.

- Since $A^{(*)}/I^{(*)}$ is Jacobson radical, then $A^{(*)}/L(I^{(*)})$ is Jacobson radical. It follows that $Z[y; D]$ is Jacobson radical.

- Next we introduce Assumption 1, and show that if F is a field which is the algebraic closure of a finite field then Assumption 1 holds.

- It is then shown that if Assumption 1 holds then some subrings of $A^{(*)}/L(I^{(*)})$ are not nil, which implies that Z is not nil.

- The last two sections contain matrix theory-based problems, which are an important part of the proof.

For general information on polynomial identity algebras we refer the reader to [6] and [24], and for diferential polynomial rings over associative noncommutative rings to [13, 25] and [7]. We prove Theorem 2 in Section 2. Sections $3 - 9$ and $10 - 17$ are mathematically independent of each other and hence can be considered

separately (in Sections 3-9 we prove Theorem 1 under the Assumption 1, and in Sections $10 - 17$ we prove Assumption 1 for algebras over some fields). Theorem 39 is proved in Section 4.

2. Proof of Theorem 2

Let R be a ring. Recall that an element $r \in R$ is quasi-invertible in R if there is $s \in R$ such that $r + s + rs = r + s + sr = 0$. As every ring can be embedded in a ring with an identity element, this can be written as $(1+r)(1+s) = 1$. Such an element s is called a quasi-inverse of r. We start with the following well-known fact

Lemma 4. *Let Q be a ring, and let $a \in Q$ be quasi-invertible, and let $b, c \in Q$ be quasi-inverses of a; then $b = c$.*

Proof. Q is a subring of a ring Q^1 with identity. Then $1+b = (1+b)((1+a)(1+c)) = ((1+b)(1+a))(1+c) = 1 + c$, so $b = c$. $\qquad\square$

Let F be a field of characteristic $p > 0$ and let R be an F-algebra. Let D be a locally nilpotent derivation on R. Let $a \in R$, then $D^n(a) = 0$ for some n. Observe that using rule $x \cdot D^n(a) - D^n(a) \cdot x = D^{n+1}(a)$, it can be proved by induction that $D^n(a) = \sum_{i=0}^{n} \alpha_i x^{n-i} a x^i$ where $\alpha_i = (-1)^i \binom{n}{i}$ (it can also be inferred using rule $(z - q)^n = \sum_{i=0}^{n} \alpha_i z^{j-i} q^i$, where z denotes multiplication from the left by x, and q multiplication from the right by x). Then $D^{p^m}(a) = x^{p^m} \cdot a - a \cdot x^{p^m}$. Notice that the binomial coefficients $\binom{n}{i}$ are well defined for fields of finite characteristic.

Proof of Theorem 2: Let notation be as above, and let $a \in R$. D is a locally nilpotent derivation, so there is m such that $0 = D^{p^m}(a) = x^{p^m} \cdot a - a \cdot x^{p^m}$. If $R[x; D]$ is Jacobson radical, then ax^{p^m} is quasi-invertible in $R[x, D]$. Let s be the quasi-inverse of ax^{p^m}; then $s = \sum_{i=0}^{n} a_i x^i$ for some $a_i \in R$. Let S be a subring of R generated by elements $a, a_0, a_1, \ldots, a_n$ and elements $D^i(a)$, $D^i(a_0), D^i(a_1) \ldots, D^i(a_n)$ for $i = 1, 2, \ldots$. Then D is a derivation on S and $S[x; D]$ is a subring of $R[x; D]$. Notice that element ax^{p^m} is quasi-invertible in $S[x; D]$. Recall that D is a locally nilpotent derivation, so there is $k > m$ such that $0 = D^{p^k}(a_i) = x^{p^k} a_i - a_i x^{p^k}$ for $0 \leq i \leq n$. Then x^{p^k} commutes with all elements of S, since $x^{p^k} D^j(a_i) - D^j(a_i) x^{p^k} = D^{p^k+j}(a_i) = 0$. Therefore, D is a nilpotent derivation on S, since $D^{p^k}(r) = x^{p^k} \cdot r - r \cdot x^{p^k} = 0$ for every $r \in S$. Notice that $S[x; D]$ is a subring of a ring Q, where Q is the set of all series $\sum_{i=0}^{\infty} c_i x^i$ with $c_i \in S$ with natural addition and multiplication $xc - cx = D(c)$ for $c \in S$. The multiplication on Q is well defined because D is a nilpotent derivation on S.

Recall that $x^{p^m} \cdot a - a \cdot x^{p^m} = 0$, hence $(ax^{p^m})^i = a^i \cdot x^{i \cdot p^m}$. Observe that for $c = a \cdot x^{p^m}$ we have $(1+c)(1-c+c^2-c^3+\ldots) = 1$. Therefore, $a' = \sum_{i=1}^{\infty}(-1)^i c^i = \sum_{i=1}^{\infty}(-1)^i a^i x^{i \cdot p^m}$ is a quasi-inverse of $a \cdot x^{p^m}$ in Q. By Lemma 4, we get $s = a'$, hence $a' \in S[x; D]$. It follows that $a^i x^{i \cdot p^m} = 0$ for almost all i; hence a is nilpotent.

3. Definitions and the Jacobson radical

Let F be a field. Throughout this paper we will assume that F is a countable and infinite field. Notice in particular that the algebraic closure of any finite field is countable. Let A' be a free noncommutative F- algebra generated by elements a, b and x; A' is a free algebra in the category of non-unital algebras, so it does not contain elements with non-zero constant term. We assign gradation 1 to elements a and b and we assign gradation 0 to element x. By R we denote the subalgebra of A' generated by a and b, and by A we denote a subalgebra of A' generated by ax^i, bx^i for $i \geq 0$. Notice that $A = RA' + R$, and hence A is a left ideal in A'. By $A'(n)$ we will denote the linear space spanned by all elements with gradation n in A'. In general, if T is a linear subspace of A', then we denote $T(n) = T \cap A'(n)$. In particular, $A(n)$ denotes the linear space spanned by all elements with gradation n in A. For a given ring Q we denote by Q^1 the usual extension with an identity of the ring Q. By $\langle x \rangle$ we will denote the ideal generated by x in A'.

Denote $A^{(*)} = A + xA + x^2A + \ldots = \sum_{i=0}^{\infty} x^i A$, notice that $A^{(*)}$ is the ideal of A' generated by a and b. Given an ideal I in A we denote $I^{(*)} = I + xI + x^2I + \ldots = \sum_{i=0}^{\infty} x^i I$.

The following Lemma is a reformulation of Lemma 7.2 in [29].

Lemma 5. *Let $r \in A$. Then there is a matrix X_r of some finite size with entries in $A(1)$ and such that for every $n > 0$, $r + Q_{r,n}$ is quasi-invertible in algebra $A/Q_{r,n}$ where $Q_{r,n}$ is the ideal generated by coefficients of matrix X_r^n in A. If $r \in R$, then the quasi-inverse of $r + Q_{r,n}$ equals $s + Q_{r,n}$ for some $s \in R$. If $r \in \langle x \rangle$, then there is $\alpha(X_r)$ such that X_r^i has all entries in $\langle x \rangle$ for every $i > \alpha(X_r)$.*

Proof. To every $r \in A$ we can assign matrix X_r of some finite size with entries in $A(1)$, like in Definition 7.1 in [29]. Let n be a natural number. We can apply Lemma 7.2 from [29] to $S = A(1)$ and $r = \sum_{i=1}^{\gamma} s_i$ with $s_i \in S^i = A(i)$. Recall that we used the following notation in [29], $v_0 = 1$ and v_i is the sum of all products $s_{j_1} s_{j_2} \ldots s_{j_k}$ where $j_1 + \ldots + j_k = i$ and k is arbitrary. Observe now that by Lemma 7.2 in [29] r is quasi-invertible in $A/Q(r, n)$.

Observe also that if $r \in A \cap \langle x \rangle$, then for a sufficiently large n matrix X_r^n has all entries from $A \cap \langle x \rangle$ by the Remark on page 925 in [29]. Notice also that all coefficients of X_r^n are from $A(n)$.

If $r \in R$, then the entries of matrix $Q_{r,n}$ are in R, hence by the above reasoning applied to ring R instead of A we get that $r + Q_n$ is quasi-invertible in R/Q_n, where Q_n is the ideal generated by entries of X_r^n in R. Observe that $Q_n \subseteq Q_{r,n}$. By Lemma 4, $r + Q_{r,n}$ has a quasi-inverse of the form $s + Q_{r,n}$ for some $s \in R$, as required. $\qquad\qquad\square$

The field F is countable, hence the set of elements of A is countable (since A is finitely generated). It follows that the set of all matrices X_r for $r \in A'$ is countable. We can ennumerate the matrices X_r with either $r \in A \cap A'xA'$ or $r \in R$ as $X_1, X_2, \ldots$.

The main result of this section is the following:

Theorem 6. *Let notation be as above, in particular let matrices $X_1, X_2, \ldots$ be as above. Let $0 < m_1 < m_2 < \ldots$ be a sequence of natural numbers such that $20m_i$ divides m_{i+1}, and $m_i > \alpha(X_i)$ (where $\alpha(X_i)$ is as in Lemma 5). Let S_i' be the linear space spanned by all entries of the matrix $X_i^{m_i}$ and let*

$$S_i = \sum_{j=1}^{\infty} A(j \cdot 20m_i - 2m_i) S_i' A(m_i) A^1.$$

Let I be the ideal of A generated by the entries of matrices $X_k^{30m_k} \cdot x^i$ for all $k > 0$ and all $i \geq 0$ (where the multiplication $X_k^{30m_k} \cdot x^i$ is component-by-component). Then I is a homogeneous ideal of A, I is contained in $\sum_{i=1}^{\infty} S_i$ and A/I is Jacobson radical. Moreover, $IA' \subseteq A'$, and if $g + h \in I$ and $g \in R$ and $h \in A \cap \langle x \rangle$ then $g, h \in I$.

Proof. By Lemma 5 all entries of matrices X_k are in $A(1)$, hence I is a homogeneous ideal of A. Let $k > 0$, observe first that the ideal I_k of A generated by entries of the matrices $X_k^{30m_k}$ is contained in the subspace S_k. It follows because entries of every matrix X_k have degree one. Namely, if $n > i + 2m_k$ then every entry of matrix X_k^n belongs to $A(i)S_k'A(m_k)A$ for every $0 \leq i$. Similarly every entry of matrix $X_k^n \cdot x^i$ belongs to $A(i)S_k'A(m_k)AA' \subseteq A(i)S_k'A(m_k)A$. Observe also that, by Lemma 5, all elements $r \in R$ and all elements $r \in A \cap \langle x \rangle$ are quasi-invertible in A/I. Notice also that $IA' \subseteq I$, as $X_k^n \cdot x^i \cdot r$ has entries in I for every $r \in A'$.

We will now show that for every $r \in A$ element $r + I$ is quasi-invertible in A/I. Let $r = u + v$, where $u \in R$ and $v \in A \cap \langle x \rangle$. Since $u \in R$ then by Lemma 5, there is $u' \in R$ such that $(1+u)(1+u') + I = 1 + I$. Notice that element $(1+r) + I$ has right

inverse if and only if element $(1+r)(1+u') + I$ has right inverse in $(A/I)^1$. We see that $(1+r)(1+u') + I = (1+u+v)(1+u') + I = 1 + v(1+u') + I$. By assumption $1 + v(1+u') + I$ has right inverse by Lemma 5, because $v(1+u') \in A \cap \langle x \rangle$ since $v \in A \cap \langle x \rangle$. It follows that $1 + r + I$ has a right inverse in $(A/I)^1$. In a similar way we show that $1 + r + I$ has a left inverse in $(A/I)^1$. Therefore $r + I$ is quasi-invertible in A/I (similarly as in Lemma 4).

The last assertion from the thesis of our theorems follws because $m_i > \alpha(X_i)$, and so the ideal generated by entries of matrix $X_i^{30m_i}$ is either contained in $\langle x \rangle$ or is generated by elements from R. $\qquad\qquad\qquad\qquad\qquad\qquad\square$

Recall that $A^{(*)} = \sum_{i=0}^{\infty} x^i A$. Notice that $A' = A^{(*)} + xF[x]$ where $F[x]$ is the polynomial ring over F (since A' does not contain elements with non-zero constant terms). Given an ideal I in A we denote $I^{(*)} = I + xI + x^2 I + \ldots = \sum_{i=0}^{\infty} x^i I$.

Lemma 7. *Let $A^{(*)}$ be as above. Let I be an ideal in A which is also a right ideal in A' (so $IA' \subseteq I$). Let $I^{(*)} = I + xI + x^2 I + \ldots = \sum_{i=0}^{\infty} x^i I$. Then $I^{(*)}$ is an ideal in $A^{(*)}$ and $I \cap R = I^{(*)} \cap R$. In addition if $r + I$ is not a nilpotent in A/I for some $r \in R$, then $r + I^{(*)}$ is not a nilpotent in $A^{(*)}/I^{(*)}$. Moreover, if A/I is Jacobson radical then $A^{(*)}/I^{(*)}$ is Jacobson radical.*

Proof. Assume that A/I is Jacobson radical. Observe that $I^{(*)}$ is a two-sided ideal in A'. From Lemma 4.1 on page 50 in [15] (by interchanging the left and the right side), we see that an element y is in the Jacobson radical of $A'/I^{(*)}$ if $yq + I^{(*)}$ is quasi-invertible in $A'/I^{(*)}$ for every $q \in A'$. Clearly, if $y \in A$ then $yq \in A$ for every $q \in A'$. By assumption, if $r = yq \in A$ then $r + I$ is quasi-invertible in A/I and hence $r + I^{(*)}$ is quasi- invertible in $A'/I^{(*)}$. Therefore every element $a + I^{(*)}$ for $a \in A$ is in the Jacobson radical of $A'/I^{(*)}$. Recall that the Jacobson radical is a two sided ideal. Therefore every element $a' + I^{(*)}$ for $a' \in A^{(*)}$ is in the Jacobson radical of $A'/I^{(*)}$. Observe that if $b + I^{(*)}$ is a quasi-inverse of $a' + I^{(*)}$, then $b = -a'b - a' \in A^{(*)} + I^{(*)} \subseteq A^{(*)}$. Therefore we can assume that $b \in A^{(*)}$. It follows that $A^{(*)}/I^{(*)}$ is Jacobson radical.

We will now show that $I \cap R = I^{(*)} \cap R$. Let $T_i = x^i(RA' + R) = x^i A$ for $i \geq 0$. Recall that A' is a free algebra, and $x \notin R$. Therefore if $0 \neq t_i \in T_i$ for $i \geq 0$ then elements $t_0, t_1, \ldots$ are linearly independent over F.

Let $i \in I$, then $i = i_0 + i_1 + \ldots + i_n$ for some $i_0 \in I, i_1 \in xI, \ldots, i_n \in x^n I$. Observe that since $I \subseteq A$ then $i_j \in T_j$ for $j = 1, 2, \ldots, n$. If $i \in R$ then $i - i_0 = i_1 + i_2 + \ldots + i_n$. Notice that $i - i_0 \in T_0$. The above observation on elements t_i

implies that elements $i-i_0, i_1, i_2, \ldots, i_n$ are all equal zero, so $i = i_0 \in I$. Therefore $I \cap R = I^{(*)} \cap R$.

Suppose now that $r + I^{(*)}$ is nilpotent in $A^{(*)}/I^{(*)}$. Then $r^n \in I^{(*)}$ for some n, so $r^n \in I$ by the above, and so $r + I$ is nilpotent in A/I. $\qquad\square$

4. Platinum ideals and platinum subspaces

In this section we introduce platinum spaces, which will be useful for constructing examples of differential polynomial rings. Let notation be as in the previous sections, in particular A' is generated by elements a, b and x, and R is generated by elements a and b.

Definition 1. Let P be the smallest subring of A' satisfying the following properties.

- $R \subseteq P$
- If $c \in P$ then $xc - cx \in P$

For a $c \in R$ define $D(c) = xc - cx$. Then D is a derivation on P. Therefore we can consider the differential polynomial ring $P[y; D]$ where $yc - cy = D(c)$ for $c \in P$.

Remark 8. Another way to define P is to first to define the inner derivation D associated with element x as $D(r) = xr - rx$ for $r \in A'$, and then define P as the intersection of all subrings of A' which contain R and are closed under the action of D. It is then clear that $P \subseteq A'$.

Recall that A' is a free algebra with free generators a, b, x. Let $q \in F$ then let $\gamma_q : A' \to A'^1$ be a ring homomorphism such that

$$\gamma_q(a) = a, \gamma_q(b) = b, \gamma_q(x) = x + q.$$

Lemma 9. *Let $q \in F$, then $\gamma_q(p) = p$ for every $p \in P$.*

Proof. We proceed by induction using the definition of P. Observe that $\gamma_q(r) = r$ for every $r \in R$. If $u, v \in P$ and $\gamma_q(u) = u$ and $\gamma_q(v) = v$ then $\gamma_q(u + v) = u + v$ and $\gamma_q(uv) = uv$ and $\gamma_q(xu - xu) = (x + q)\gamma_q(u) - \gamma_q(u)(x + q) = xu - ux$. $\qquad\square$

Lemma 10. *Let notation be as in Definition 1 and let F be an infinite field. Let $f : P[y; D] \to A'$ be a F-linear mapping such that $f(p) = p$ and $f(py^i) = px^i$ for $p \in P$, $i \geq 1$. Then f is injective and f is a homomorphism of rings.*

Proof. Observe that P embeds into A' in a natural way as a subring, hence $f(p)$ is well defined as a ring homomorphism for $p \in P$. Every element of $P[y; D]$ can be uniquely written as a linear combination of elements py^i with $p \in P$, hence f is well defined as a linear mapping. We will show that f is a ring homomorphism. Notice first that binomial coefficients $\binom{n}{i}$ are well definied in fields of finite characteristic. Observe that if $p, q \in P[y; D]$ then $py^n q = p \sum_{i=0}^{n} \binom{n}{i} D^i(q) y^{n-i}$.

Therefore $f(py^n \cdot qy^j) = f(p \sum_{i=0}^{n} \binom{n}{i} D^i(q) y^{n-i} y^j) = p \sum_{i=0}^{n} \binom{n}{i} D^i(q) x^{n-i+j}$. On the other hand, $f(py^n) f(qy^j) = px^n \cdot qx^j = p \sum_{i=0}^{n} \binom{n}{i} D^i(q) x^{n-i+j}$. Consequently, $f(py^n \cdot qy^j) = f(py^n) f(qy^j)$.

We need to show that the kernel of f is zero. Suppose that $f(\sum_{i=0}^{n} c_i y^i) = 0$ for some $c_i \in P$. Since $f(\sum_{i=0}^{n} c_i y^i) = 0$ then $\sum_{i=0}^{n} c_i x^i = 0$.

If $c = 0$ in A' then clearly $\gamma_q(c) = 0$ for every $q \in F$ (since γ_q is an homomorphism of rings). By Lemma 9 we get $0 = \gamma_q(\sum_{i=0}^{n} c_i x^i) = \sum_{i=0}^{n} c_i (x+q)^i$. We can write such equations for pairwise distinct elements $q_1, q_2, \ldots, q_{n+1} \in F$ and then write them as $(c_0, c_1, \ldots, c_n) M = 0$ where M is a matrix with i-th column equal to $(1, (x + q_i), (x + q_i)^2, \ldots, (x + q_i)^n)^T$. Observe that M is a transposition of a Vandermonde matrix, and hence the determinant of M is $det(M) = \prod_{i>j} (q_i - q_j) \in F$. Hence there is matrix N in $F[x]$ such that $MN = Id \cdot det(M)$, where Id is the identity matrix. It follows that $(c_0, c_1, \ldots, c_n) M = 0$ implies $(c_0, c_1, \ldots, c_n) det(M) = 0$, and so $c_0 = c_1 = \ldots = c_n = 0$. $\qquad\square$

Recall that $A^{(x)} = A + xA + x^2 A + \ldots$.

Lemma 11. *Every element of $A^{(*)}$ can be uniquely written in the form $P + Px + Px^2 + \ldots$, moreover since $A = RF[x] + RA^{(*)}$ every element of A can be written in the form $R[x] + RP + RPx + RPx^2 + \ldots$ (notice also that $RP \subseteq P \cap A$).*

Proof. It can be shown by induction on n that $x^n P \subseteq P + Px + Px^2 + \ldots = \sum_{i=0}^{\infty} Px^i$. Next observe that the set $P + Px + Px^2 + \ldots$ is closed under multiplication and addition, hence it is a subring of A' containing $x^i R$ and Rx^i for every i, hence it contains $A^{(*)}$.

Suppose now that some elements from $P + Px + Px^2 + \ldots$ are linearly dependent over F; then $\sum_{i=0}^{n} p_i x^i = 0$ for some $p_i \in P$. As A' is a free algebra and γ_t is a ring homomorphism for $t \in F$ then $\gamma_t(\sum_{i=0}^{n} p_i x^i) = 0$. By Lemma 9 we get $\sum_{i=0}^{n} p_i (x+t)^i = 0$. We can write such equations for different elements $t = q_1, t = q_2, \ldots, t = q_{n+1} \in F$ and then write these equations as $(p_0, p_1, \ldots, p_n) M = 0$, where M is a matrix with i-th column equal to $(1, (x+q_i), (x+q_i)^2, \ldots, (x+q_i)^n)^T$. Notice that M is a transposition of a Vandermonde matrix and the determinant

of M is $\det(M) = \prod_{i>j}(q_i - q_j) \in F$. Therefore M is invertible, with $MN = $Id for some matrix N with entries in $F[x]$ (where Id denotes the identity matrix). Hence $(p_0, \ldots, p_n)M = 0$ implies $(p_0, \ldots, p_n) = (p_o, \ldots, p_n)MN = 0$, so $p_0 = p_1 = \ldots = p_n = 0$, as required. $\qquad\square$

Definition 2. Let S be a linear subspace in A'. We will say that S is a *platinum space* if $\gamma_q(S) \subseteq S$ for every $q \in F$.

Definition 3. Let I be an ideal in A'. We will say that I is a *platinum ideal* if $\gamma_q(I) \subseteq I$ for every $q \in F$. In particular, a platinum ideal is an ideal which is a platinum subspace of A'.

We will say that A'/I is a *platinum ring* if I is a platinum ideal of A'.

Remark 12. Let I be an ideal in A' and let $\bar{I} = I \cap P$. Observe that $\bar{I}$ is an ideal in P and if $c \in \bar{I}$ then $xc - cx \in \bar{I}$ (because $xc, cx \in I$).

Let I be a platinum ideal in A'. Denote $\bar{I} = I \cap P$. For $p \in P$ we define $D(p) = xp - px$. Then $P/\bar{I}$ is a ring with the derivation $D(c + \bar{I}) = D(c) + \bar{I}$ where $D(c) = xc - cx$. By the elementary *Second Isomorphism Theorem* ring $P/\bar{I}$ can be embedded in A'/I via the mapping $h : P/\bar{I} \to A'/I$, where $h(c + \bar{I}) = c + I$ for $c \in P$ (see [12] for some related results).

Theorem 13. *Let F be an infinite field. Let I be a platinum ideal in A' then $I \subseteq A^{(*)}$. Denote $\bar{I} = I \cap P$. Let $P^* = (P/\bar{I})[y; D]$ be the differential polynomial ring with $y(c + \bar{I}) - (c + \bar{I})y = D(c + \bar{I})$ where $D(c + \bar{I}) = xc - cx + \bar{I}$, for $c \in P$. Then the mapping $f : P^* \to A'/I$ given by $f(p + \bar{I}) = p + I$ and $f((p + \bar{I})y^i) = px^i + I$ for $p \in P$, is an injective homomorphism of rings; moreover the image of P^* equals $A^{(*)}/I$. Therefore, P^* can be embedded into A'/I.*

Proof. We will first show that $I \subseteq A^{(*)}$ and hence I is an ideal in $A^{(*)}$. Observe that $A' = A^{(*)} + xF[x]$, since A' doesn't contain elements with constant terms. Let $i = u + v \in I$ where $u \in A^{(*)}$ and $v \in xF[x]$. We will show that $v = 0$; suppose on the contrary that $v \neq 0$. Notice that since F is an infinite field then $\gamma_t(v)$ contains a non-zero constant term from F for some $t \in F$. On the other hand A' doesn't contain any elements with non-zero constant terms, hence $\gamma_t(v) \notin A'$. Therefore $\gamma_t(i) = \gamma_t(u + v) \notin A'$, a contradiction since I is a platinum ideal.

We will now show that the image of P^* is $A^{(*)}/I$. Notice that $P^* = (P/\bar{I}) + (P/\bar{I})y + (P/\bar{I})y^2 \ldots = \sum_{i=0}^{\infty}(P/\bar{I})y^i$. Consequently by the definition of mapping f the image of P^* in A'/I equals $(P + I) + (Px + I) + \ldots = \sum_{i=0}^{\infty} Px^i + I$. Clearly $P + Px + \ldots \subseteq A^{(*)}$, since $A^{(*)}$ equals the ideal of A' generated by a and b. By Lemma 11 we have $A^{(*)} = \sum_{i=0}^{\infty} Px^i$, hence $A^{(*)}/I = Im(P^*)$.

We will now show that f is an injective homomorphism of rings. By Remark 12, f is well defined as a ring homomorphism on $P/\bar{I}$. Every element of P^* can be uniquely written as a linear combination of elements py^i with $p \in P$, $i \geq 0$, so f is well defined as a linear mapping on P^*. To check that f is a ring homomorphism we proceed similarly as in Lemma 43.

We need to show that the kernel of f is zero. Suppose that $f(\sum_{i=0}^{n}(c_i+\bar{I})y^i) = 0$ where $c_i + \bar{I} \in P/\bar{I}$, $c_i \in P$. By the definition of f we have $\sum_{i=0}^{n}(c_i x^i + I) = 0 + I$ in A'/I, hence $\sum_{i=0}^{n} c_i x^i \in I$. Since I is a platinum ideal we get that $\gamma_q(\sum_{i=0}^{n} c_i x^i) \in I$ for every $q \in F$. By Lemma 5, that implies $\sum_{i=0}^{n} c_i(x+q)^i \in I$. Write such equations for different elements $q_1, q_2, \ldots, q_{n+1} \in F$, and then write them as $(c_0, c_1, \ldots, c_{n+1})M = Q$ where M is a matrix with i-th column equal to $(1, (x+q_i), (x+q_i)^2, \ldots, (x+q_i)^n)^T$ and Q is a vector with all entries from I. Observe that M is a transposition of a Vandermonde matrix and hence the determinant of M is $\det(M) = \prod_{i>j}(q_i - q_j) \in F$. Therefore, M is invertible, with $MN = $Id for some matrix N with entries in $F[x]$ (where Id is the identity matrix). Hence $(c_0, c_1, \ldots, c_n)M = Q$ implies $(c_0, c_1, \ldots, c_n) = QN$. Since QN is a vector with all entries in I, then $c_0, c_1, \ldots, c_n \in I$. Since $c_i \in P$ then $c_i \in P \cap I = \bar{I}$ for $i = 0, 1, 2, \ldots, n$. Therefore $c_i + \bar{I} = 0 + \bar{I}$ for every $i \leq n+1$, and so $\sum_{i=0}^{n}(c_i + \bar{I})y^i = 0$, as required. $\square$

Proof of Theorem 3. Notice that Theorem 13 is a special case of Theorem 3 for $a_1 = a$ and $a_2 = b$. Observe that the number of generators of A doesn't influence the proof of Theorem 13, so the proof of Theorem 3 is the same as the proof of Theorem 13.

Definition 4. For an element $r \in A'$ we define $L(r)=\mathrm{span}_F\{\gamma_t(r) : t \in F\}$. Given a linear space $S \subseteq A'$ we define $L(S) =\mathrm{span}_F\{L(r) : r \in S\}$. Note that $L(S)$ is the linear space spanned by all elements $\gamma_t(s)$ for $t \in F$, $s \in S$.

Lemma 14. *Let S be a linear space, then $L(S)$ is the smallest platinum space containing S.*

Proof. If $S \subseteq Q$ and Q is a platinum space then $\gamma_t(S) \subseteq Q$ for every $t \in F$. Therefore $L(S) \subseteq Q$. We need to show that $L(S)$ is a platinum space. Let $s \in L(S)$, then $s = \sum_{t \in W} \gamma_t(s_t)$ where W is a finite subset of F and $s_t \in S$. Let $k \in F$, then $\gamma_k(s) = \sum_{t \in W} \gamma_k(\gamma_t(s_t)) = \sum_{t \in W} \gamma_{k+t}(s_t) \in L(S)$. $\square$

Lemma 15. *Let $S \subseteq A'$ be a platinum space, then $S \subseteq A^{(*)}$. Suppose that $sx \in S$ for every $s \in S$. Then $S = S' + S'x + S'x^2 + \ldots$ where $S' = P \cap S$.*

Proof. The proof that $S \subseteq A^{(*)}$ is the same as the proof that $I \subseteq A^{(*)}$ in Theorem 13. Observe first that $S'x^i \subseteq S$ for every i. We will show that $S \subseteq S' + S'x + S'x^2 + \ldots = \sum_{i=0}^{\infty} S'x^i$. Let $r \in S$. By Lemma 11 we have $r = \sum_{i=0}^{n} p_i x^i \in S$ for some $p_i \in P$. We will proceed by induction on n. If $n = 0$ then $r = p_0 \in P \cap S$, as required. Suppose now that $n > 0$ and the result holds for all numbers smaller than n, and we will show that it holds for n. Because A is a platinum subspace, for every $\alpha \in F$ we have $\sum_{i=0}^{n} p_i(x+\alpha)^i \in S$. Let $d = \sum_{i=0}^{n} p_i(x+\alpha)^i - r$, then $d \in S$. Observe that $d = \sum_{i=0}^{n}(p_i(x+\alpha)^i - p_i x^i) = \sum_{i=0}^{n-1} d_i x^i$ for some $d_i \in P$. By the inductive assumption $d_0 \in S$, hence $\sum_{i=1}^{n} p_i \alpha^i = d_0 \in P \cap S$. This holds for every $\alpha \in F$. By the Vandermonde matrix argument, we get $p_1, \ldots, p_n \in P \cap S$. Moreover, $p_0 = r - \sum_{i=1}^{n} p_i x^i \in S$ and since $p_0 \in P$ then $p_0 \in P \cap S$. $\square$

5. Linear mappings f and G

Let A^* be the subalgebra of A generated by elements $ax^i ax^j$ and $bx^i bx^j$ for all $i, j \geq 0$. Notice that the notation A^* is distinct from the notation $A^{(*)}$, denoting different objects.

Let $B' \subseteq A(2)$ be the linear F-space spanned by elements $ax^i bx^j$ and $bx^i ax^j$ for all $i, j \geq 0$. Let $B = \sum_{i=0}^{\infty} A(2i)B'A$. Observe that $A = A^* + B$ and $A^* \cap B = 0$.

By $F[x]$ we will denote the polynomial ring in variable x over F. Given a linear mapping f by $\ker(f)$ and Im (f) we denote the kernel and the image of f.

Lemma 16. *Let m be an even number and let $S \subseteq A^*(m)$ be a platinum space such that $sx \in S$ if $s \in S$. Then there is a linear mapping $f : A^*(m) \to A^*(m)$ such that*

1. $\ker(f) = S$,
2. $f(px^i) = f(p)x^i$ *for every* $p \in A^*(m) \cap P$,
3. $f(p) \in P$ *for every* $p \in A^*(m) \cap P$.
4. *Moreover, for every $s \in A^*(m)$ and $t \in F$,*

$$f(\gamma_t(s)) = \gamma_t(f(s)).$$

5. *There is a linear space $E \subseteq A^*(m)$ such that $f(r) = r$ for $r \in E$, and $E \oplus S = A^*(m)$. Moreover Im $(f) \oplus \ker(f) = A^*(m)$.*

Proof. By Lemma 15, $S = S' + S'x + \ldots$ where $S' = S \cap P \subseteq A^*(m)$. By Zorn's lemma, there exists a maximal linear subspace Q of $A^*(m) \cap P$ such that $S' \cap Q = 0$. Observe that then $Q + S' = A^*(m) \cap P$ and that Q is a platinum space (as every subspace of P is a platinum space, by Lemma 9). Define $f(r) = 0$ for $r \in S'$ and $f(r) = r$ for $r \in Q$. Observe that $A^*(m) = \sum_{i=0}^{\infty}(A^*(m) \cap P)x^i$ by Lemma 15.

Define $f(px^i) = px^i$ for $p \in A^*(m) \cap P$. By Lemma 11, f is a well defined linear mapping. Notice that $E = Q + Qx + Qx^2 + \ldots$ satisfies (5). Observe that $f(s) = 0$ for every $s \in S$. If $r = r_1 + r_2$ with $r_i \in S$ and $r_2 \in Q + Qx + Qx^2 + \ldots$ then $f(r) = r_2$, so the kernel of f equals S. The image of f is E, so (5) holds.

We will now show that $f(\gamma_t(s)) = \gamma_t(f(s))$. Let $s \in S$; then $s = \sum_i p_i x^i$ for some $p_i \in S'$. Then $f(s) = \sum_i f(p_i)x^i$. Since S is a platinum space then $\gamma_t(s) \in S$ for any $t \in F$. Observe that by the definition of γ_t we get

$$\gamma_t(s) = \sum_i p_i(x+t)^i,$$

since $\gamma_t(p) = p$ for $p \in P$ by Lemma 9. Therefore $f(\gamma_t(s)) = \sum_i f(p_i)(x+t)^i$.

Observe now that

$$\gamma_t(f(s)) = \gamma_t(\sum_i f(p_i)x^i) = \sum_i f(p_i)(x+t)^i$$

(by Lemma 9, since $f(p_i) \in P$). It follows that $f(\gamma_t(s)) = \gamma_t(f(s))$. $\qquad\square$

Remark 17. Notice that the fifth statement of Lemma 16 can be also formulated by saying that the short exact sequence $0 \to S \to A^*(m) \to E \to 0$ induced by $f : A^*(m) \to \mathrm{Im}(f) = E$ is split by the inclusion map section $E \to A^*(m)$.

For a matrix M, let $S(M)$ be the linear space spanned by all entries of M, and $L(M)$ be the linear space spanned by all matrices $\gamma_t(M)$ for $t \in F$ (where if M has entries $m_{i,j}$ then $\gamma_t(M)$ has respective entries $\gamma_t(m_{i,j})$). Observe that $L(S(M)) = S(L(M))$.

Definition 5. (Definition of mapping G) Let m be an even number and let $f : A^*(m) \to A^*(m)$ be a linear mapping satisfying properties (1)–(5) from Lemma 16 (for some platinum space S). Define a linear mapping $G : A^*(10m) \to A^*(10m)$ as follows:

If $v_1, \ldots, v_{10} \in A^*(m)$ are monomials (products of generators) and $v = v_1 v_2 \ldots v_{10}$, then we define

$$G(v) = G(v_1 \ldots v_{10}) = v_1 v_2 \ldots v_9 f(v_{10}).$$

We can extend the mapping G by linearity to all elements of $A^*(10m)$.

For every natural number $j > 0$ we extend the mapping G to the linear mapping $G : A^*(j \cdot 10m) \to A^*(j \cdot 10m)$ in the following way: if $w = w_1 \ldots w_j$ where w_i are monomials and $w_i \in A^*(10m)$, then we define

$$G(w) = G(w_1)G(w_2) \ldots G(w_j).$$

We can then extend the mapping G by linearity to all elements of $A^*(j \cdot 10m)$.

Moreover, we can also extend the mapping G to matrices with entries in $A^*(j \cdot 10m)$, so if M has entries $a_{i,j}$ then $G(M)$ has respectively entries $G(a_{i,j})$. In similar fashion we can extend the mappings f and γ_t to matrices.

Lemma 18. *Let m, G be as in the definition of the mapping G above. Let m_i, n be natural numbers such that n divides m, and $10m$ divides m_i. Let M_i be a matrix with entries in $A^*(n)$; then*

$$L(S(G(M_i^{\frac{m_i}{n}}))) = G(L(S(M_i^{\frac{m_i}{n}}))).$$

Proof. Recall that $S(M)$ denotes the linear space spanned by entries of matrix M, hence $S(L(M)) = L(S(M))$ and $S(G(M)) = G(S(M))$ for any matrix M with entries in C. Consequently it is sufficient to show that $L(G(M_i^{\frac{m_i}{n}})) = G(L(M_i^{\frac{m_i}{n}}))$. We will first show that $G(L(M^{10})) = L(G(M^{10}))$ for any M with entries in $A^*(m)$. Let $t \in F$, then $G(\gamma_t(M^{10})) = G(\gamma_t(M^9)\gamma_t(M)) = (\gamma_t(M))^9 f(\gamma_t(M))$. By assertion (4) from Lemma 16 we have $f(\gamma_t(M)) = \gamma_t(f(M))$. Therefore $G(\gamma_t(M^{10})) = \gamma_t(M^9)f(\gamma_t(M)) = \gamma_t(M^9)\gamma_t(f(M)) = \gamma_t(G(M^{10}))$. Consequently $G(L(M^{10})) = L(G(M^{10}))$, as required.

By the definition of G, for the same M, and for any $t \in F$, and any number k,

$$G(\gamma_t(M^{10k})) = G(\gamma_t(M^{10}))^k = \gamma_t(G(M^{10}))^k = \gamma_t(G(M^{10k})).$$

Therefore, $G(L(M^{10k}) = L(G(M^{10k}))$. The result now follows when we take $M = M_i^{\frac{m}{n}}$ and $k = \frac{m_i}{10m}$ and substitute in the above equation. $\square$

Lemma 19. *Let M be a finite matrix with entries in $A(j) \cap R$ for some j. For almost all n the dimension of the space $R \cap S(L(M^n)) = \bar{S}(M^n)$ is smaller than $\sqrt{n}$. Notice also that since the entries of M are taken from R which is γ_t invariant for all $t \in F$ then the space $S(L(M^n))$ is finite dimensional for every n.*

Proof. Since all entries of M are in R then $S(L(M^n)) = S(M^n)$. Let M be an m by m matrix, then the dimension of $\bar{S}(M^n)$ is at most m^2, which for sufficiently large n is smaller than $\sqrt{n}$. $\square$

6. Supporting lemmas

Let n, m_1 be natural numbers such that $20n$ divides m_1. Let M_1 be a matrix with entries in $A^*(n)$. Let f be a mapping satysfying properties (1)–(5) from Lemma 16 for $m = 2m_1$ and for the space $S = S(L(M_1^{\frac{m_1}{n}}))A^*(m_1)$. We can then define mapping $G : A^*(j \cdot 10 \cdot 2m_1) \to A^*(j \cdot 10 \cdot 2m_1)$ as in the previous section (for every j).

In the next three lemmas we will use the following notation. Let m be a natural number and let $V \subseteq A^*(m)$ be a linear space. Denote

$$E(V, m) = \sum_{j=1}^{\infty} A^*(j \cdot 20m - 2m) V A^*(m) A^{*1}.$$

We begin with the following lemmas:

Lemma 20. *Let j, n, m_1 be natural numbers such that $20n$ divides m_1. Let M_1 be a matrix with coefficients in $A^*(n)$. Let G be defined as at the beginning of this section. Then the kernel of $G : A^*(j \cdot 20m_1) \to A^*(j \cdot 20m_1)$ is equal to $E(V, m_1) \cap A^*(j \cdot 20m_1)$, where $V = S(L(M_1^{\frac{m_1}{n}}))$.*

Proof. By assertion (5) from Lemma 16 applied for $m = 2m_1$ and $S = V A^*(m_1)$, there is a linear space $E \subseteq A^*(2m_1)$ and such that $f(r) = r$ for $r \in E$ and $E \oplus S = A^*(2m_1)$. For $i = 1, 2, \ldots, j$, let $D = \prod_{i=1}^{j} A^*(18m_1)E$ and let

$$T_i = A^*(i \cdot 20m_1 - 2m_1) \cdot V \cdot A^*((j - i) \cdot 20m_1 + m_1).$$

Observe that $D + \sum_{i=1}^{j} T_i = A^*(j \cdot 20m_1)$. If $r \in T_i$ for some i, then $G(r) = 0$ by the definition of G. Observe that $E(V, m_1) \cap A^*(j \cdot 20m_1) = \sum_{i=1}^{j} T_i$, hence $E(V, m_1) \cap A^*(j \cdot 20m_1)$ is contained in the kernel of G.

Let r be in the kernel of f. Write $r = t + d$, where $t \in \sum_{i=1}^{j} T_i$ and $d \in D$, then by the definition of G, $G(r) = G(t + d) = G(t) + G(d) = G(d) = d$. Recall that r is in the kernel of f, so $d = 0$ and hence $r \in \sum_{i=1}^{j} T_i$. It follows that the kernel of G equals $E(V, m_1) \cap A^*(j \cdot 20m_1)$. □

Lemma 21. *Let n, k be natural numbers with n even, and let $m_1 < m_2 < \ldots < m_k$ be such that $20nm_i$ divides m_{i+1} for all $1 \leq i < k$ and $20n$ divides m_1. Let M_i be matrices with entries in $A^*(n)$ and let $G : A^*(j \cdot 20m_1) \to A^*(j \cdot 20m_1)$ be defined as at the beginning of this section, and let $j = \frac{m_k}{m_1}$. Let $u \in A^*(20m_k)$, and denote $V_i = L(S(M_i^{m_i/n}))$. Then $u \in \sum_{i=1}^{k} E(V_i, m_i)$ if and only if $G(u) \in \sum_{i=2}^{k} G(E(V_i, m_i))$.*

Proof. Suppose that $G(u) \in \sum_{i=2}^{k} G(E(V_i, m_i))$. It follows that $G(u - e) = 0$ for some $e \in \sum_{i=2}^{k} E(V_i, m_i)$. Consequently $u - e \in \ker(G)$, and since by Lemma 20 $\ker(G) \subseteq E(V_1, m_1)$, it follows that $u \in \sum_{i=1}^{k} E(V_i, m_i)$.

To see the second implication, suppose now that $u \in \sum_{i=1}^{k} E(V_i, m_i)$; then $G(u) \in \sum_{i=1}^{k} G(E(V_i, m_i))$. By Lemma 20, $E(V_1, m_1) \cap A^*(20m_k) \subseteq \ker(G)$, hence $G(L(V_1, m_1)) = 0$. It follows that $G(u) \in \sum_{i=2}^{k} G(E(V_i, m_i))$, since all the considered spaces are homogeneous. □

Lemma 22. *Let notation be as in Lemma 21. For $i = 2, 3, \ldots$ denote*

$$M_i' = G(M_i^{\frac{20m_1}{n}}), W_i = L(S(M_i'^{\frac{m_i}{20m_1}})), T_i = G(E(V_i, m_i) \cap A^*(20m_k)).$$

Then for $i \geq 2$ we have $T_i \subseteq E(W_i, m_i) \cap A^*(20m_k) \subseteq T_i + E(V_1, m_1)$.

Proof. Recall that $20m_1$ divides m_i for all $i \geq 2$; hence

$$T_i = A^*(20m_k) \cap \sum_{j=1}^{\infty} G(A^*(j20m_i - 2m_i))G(L(S(M_i^{\frac{m_i}{n}})))G(A^*(m_i))G(A^{*1}).$$

Observe that

$$M_i'^{\frac{m_i}{20m_1}} = [G(M_i^{\frac{20m_1}{n}})]^{\frac{m_i}{20m_1}} = G(M_i^{\frac{m_i}{n}})$$

by the definition of mapping G. Therefore, and by Lemma 18 applied for $m = 2m_1$,

$$L(S(M_i'^{\frac{m_i}{20m_1}})) = L(S(G(M_i^{\frac{m_i}{n}}))) = G(L(S(M_i^{\frac{m_i}{n}}))).$$

It follows that

$$T_i = A^*(20m_k) \cap \sum_{j=1}^{\infty} G(A^*(j20m_i - 2m_i))(L(S(M_i'^{\frac{m_i}{20m_1}})))G(A^*(m_i))G(A^{*1}).$$

It follows that $T_i \subseteq E(W_i, m_i) \cap A^*(20m_k)$.

We will now show that $E(W_i, m_i) \cap A^*(20m_k) \subseteq T_i + E(V_1, m_1)$. Recall that the mapping G can be defined on $A^*(j \cdot 20m_1)$ for any j, and that $20m_1$ divides m_i for each $i > 1$. Observe now that by assertion (5) from Lemma 16, $\ker(f) + \mathrm{Im}$ $(f) = A^*(m)$. Therefore, by the construction of mapping G we get that $A^*(j \cdot 20m_1) = (\mathrm{Im}\ (G) + \ker G) \cap A^*(j \cdot 20m_1)$ for every j.

It follows that $A^*(m_i) \subseteq G(A^*(m_i)) + \ker(G) \cap A^*(m_i)$. By Lemma 20, $A^*(m_i) \subseteq G(A^*(m_i)) + E(V_1, m_1) \cap A^*(m_i)$. Similarly, $A^*(j \cdot 20m_i - 2m_i) \subseteq G(A^*(j20m_i - 2m_i)) + E(V_1, n_1) \cap A^*(j \cdot 20m_i - 2m_i)$. It follows that $E(W_i, m_i) \cap A^*(20m_k) \subseteq T_i + E(V_1, m_1)$. $\square$

Theorem 23. *Let notation be as in Lemma 22. Let $u \in A^*(20m_k)$. Then*

$$u \in \sum_{i=1}^{k} E(V_i, m_i),$$

if and only if

$$G(u) \in \sum_{i=2}^{k} E(W_i, m_i).$$

Proof. We will first prove that $G(u) \in \sum_{i=2}^{k} E(W_i, m_i)$ implies $u \in \sum_{i=1}^{k} E(V_i, m_i)$. Assume on the contrary that $G(u) \in \sum_{i=2}^{k} E(W_i, m_i)$ and $u \notin \sum_{i=1}^{k} E(V_i, m_i)$. Observe that by Lemma 22, $E(W_i, m_i) \cap A^*(20m_k) \subseteq \sum_{i=2}^{k} T_i + E(V_1, m_1)$, hence

$G(u) \in \sum_{i=2}^{k} T_i + E(V_1, m_1)$. Therefore there is $g \in \sum_{i=2}^{k} T_i$ and $h \in E(V_1, m_1)$ and $G(u) = g+h$. By assertion (5) from Lemma 16 we get that Im $(G) \cap \ker(G) = 0$. Since $G(u)$ and g are in Im(G) and $h \in E(V_1, m_1)$ is in the kernel of mapping G, then $G(u) - g = h$ implies $G(u) - g = 0$. Therefore $G(u) \in \sum_{i=2}^{k} T_i$, a contradiction with Lemma 21.

We will now prove that $G(u) \notin \sum_{i=2}^{k} E(W_i, m_i)$ implies $u \notin \sum_{i=1}^{k} E(V_i, m_i)$. Suppose that $G(u) \notin \sum_{i=2}^{k} E(W_i, m_i)$. By Lemma 22, $G(u) \notin \sum_{i=2}^{k} T_i$, where $T_i = G(E(V_i, m_i) \cap A(20m_k))$. Observe that by Lemma 20, $G(E(V_1, m_1)) = 0$. Since G is a linear mapping it implies $u \notin \sum_{i=1}^{k} E(V_i, m_i)$ (as otherwise we would have $G(u) \in \sum_{i=2}^{k} T_i$.) $\square$

7. Assumptions 1 and 2

Let notation be as in Section 5. Recall that, for a matrix M, $S(M)$ denotes the linear space spanned by all entries of M, and $L(M) = \sum_{t \in F} \gamma_t(M)$. Recall that by $\langle x \rangle$ we denote the ideal generated by x in A.

The following statement will be called Assumption 1 (for F-algebra A).

Assumption 1. Let M be a matrix with entries in $A^*(j)$ for some j, and such that for almost all α matrix M^α has all entries in $\langle x \rangle$. Then there are infinitely many n, such that the dimension of the space $R \cap S(L(M^n))$ does not exceed $\sqrt{n}$.

Comment. Notice that, since A' is a graded algebra, it is necessary to assume that all elements of the matrix M have the same degree, since otherwise the entries of M^α would have many homogeneous components and $\dim_F(R \cap S(L(M^n)))$ could exceed $\sqrt{n}$. On the other hand, it would be possible to assume that M is a matrix with entries in $A(j)$ for some j; however, for our purpose it suffices to assume that M is a matrix with entries in $A^*(j)$, for some j.

Remark 24. Suppose that Assumption 1 holds, and let k be a natural number. We can apply Assumption 1 to matrix M^k to get the following implication of Assumption 1: Let m be a natural number. There are infinitely many n divisible by k such that the dimension of the space $R \cap S(L(M^n))$ is less than $\sqrt{n}$.

Definition 6. Let l, t, m, n be natural numbers and let $r_0, r_1, \ldots, r_t \in A^*$. We define

$$e(n, m)(r_0, r_1, \ldots, r_t) = \sum_{i_1 + \ldots + i_m = n} r_{i_1} r_{i_2} \ldots r_{i_m}.$$

The following lemma is similar to Lemma 7 (b) in [27].

Lemma 25. *Let m, n, t, l be natural numbers, and let $r_0, r_1, \ldots, r_l \in A^*(t)$. Denote $e(n, m) = e(n, m)(r_0, r_1, \ldots, r_l)$; then for every $0 < k < m$*

$$e(n, m) = \sum_{i=0}^{n} e(i, k) e(n - i, m - k).$$

Proof. It is easier to prove a more general result where r_i are free generators of a free algebra and we assign gradation i to element r_i. Such a result can be proved for example by induction on k. The special case when $r_i \in A^*(t)$ implies Lemma 25. □

Lemma 26. *Let l, t, m be natural numbers and let $r_0, r_1, \ldots, r_l \in A^*(t)$. Denote $r_i' = e(i, m)(r_0, r_1, \ldots, r_l)$. Then for every n and every $i \leq lmn$,*

$$e(i, n)(r_0', r_1', \ldots, r_{lm}') = e(i, mn)(r_0, r_1, \ldots, r_l).$$

Proof. We will use induction on n. If $n = 1$ then the result is clear. Suppose that $n > 1$ and that the result holds for all numbers smaller than n. By Lemma 25, $e(i, mn)(r_0, r_1, \ldots, r_l) = \sum_{j=0}^{i} e(j, m(n-1))(r_0, r_1, \ldots, r_l) \cdot e(j, m)(r_0, \ldots, r_l)$. By the inductive assumption and by Lemma 25, we get $e(i, mn)(r_0, r_1, \ldots, r_l) = \sum_{j=0}^{i} e(j, n-1)(r_0', \ldots, r_{lm}') \cdot e(j, 1)(r_0', \ldots, r_{lm}') = e(j, n)(r_0', \ldots, r_l')$. □

Recall that $\langle x \rangle$ is the ideal of A' generated by x.

Lemma 27. *Let F be a field, and suppose that Assumption 1 holds for F-algebra A. Let n, t be natural numbers and let M be a matrix with coefficients in $A^*(n)$. Assume that either all entries of M are in R or for almost all q entries of M^q are in $\langle x \rangle$. Let $t \geq 1$, $r_0, r_1, \ldots, r_t \in A^*(n) \cap R$, and denote $e(j, k) = e(j, k)(r_0, r_1, \ldots, r_t)$. Assume moreover that there are $r_i, r_{i'} \neq 0$ such that $r_{i'} \notin F \cdot r_i$ for some $0 \leq i, i' \leq t$. Then there exist m and j, j' such that $20n$ divides m and*

$$e(j, \frac{20m}{n}) \notin A^*(18m) V A^*(m)$$

and

$$e(j', \frac{20m}{n}) \notin F \cdot e(j, \frac{20m}{n}) + A^*(18m) V A^*(m),$$

where $V = L(S(M^{\frac{m}{n}})) \subseteq A^*(m)$. Moreover, if $c > 0$ is a natural number then we can assume that $20nc$ divides m.

Proof. Consider elements $e(i, \frac{20m}{n})$ for all m divisible by n. Observe that, for almost all such m, the linear space spanned by $e(i, \frac{20m}{n})$ for $i = 0, 1, 2, \ldots$ has dimension larger than $\sqrt{\frac{20m}{n}} + 2$. By Assumption 1 and Lemma 19, $\dim_F V \leq \sqrt{\frac{20m}{n}}$ for infinitely many m (moreover by Remark 24 we can assume that infinitely

many m are divisible by $20nc$). Consequently there is m divisible by n and j, j' such that $e(j, \frac{m}{n}) \notin V$ and $e(j', \frac{m}{n}) \notin V + F \cdot e(j', \frac{m}{n})$. Moreover, we can assume that $20nc$ divides m, by the Remark 24.

Let j be minimal such that $e(j, \frac{m}{n}) \notin V$ and j' minimal such that $e(j', m) \notin V + F \cdot e(j, \frac{m}{n})$. We claim that $e(j, \frac{20m}{n}) \notin A^*(18m)VA(m)$ and $e(j', \frac{20m}{n}) \notin A^*(18m)VA(m) + F \cdot e(j, \frac{20m}{n})$.

Notice that $e(0, \frac{m}{n}) = r_0 \frac{m}{n}$. Recall that A^* is a graded algebra, and therefore $e(j, \frac{m}{n})e(0, \frac{m}{n}) \notin VA^*(m_1)$; this can be seen by comparing the elements from $A^*(m)$ at the end of each side. By Lemma 25, $e(j, \frac{2m}{n}) = e(j, \frac{m}{n})e(0, \frac{m}{n}) + \sum_{i<j} e(i, \frac{m}{n})e(j-i, \frac{m}{n})$. By the minimality of j, we get $e(j, \frac{2m}{n}) \notin VA^*(m)$. Notice also that, by a similar argument j is minimal such that $e(j, \frac{2m}{n}) \notin VA^*(m)$. Observe now that $e(0, \frac{18m}{n})e(j, \frac{2m}{n}) \notin A^*(18m)VA^*(m)$; this can be seen by comparing the elements from $A^*(18m)$ at the beginning of each side. By Lemma 25, $e(j, \frac{20m}{n}) = e(0, \frac{18m}{n})e(j, \frac{2m}{n}) + \sum_{i<j} e(j-i, \frac{18m}{n})e(i, \frac{2m}{n})$. Recall that j was minimal such that $e(j, \frac{2m}{n}) \notin VA^*(m)$, therefore $e(j, \frac{20m}{n}) \notin A^*(18m)VA(m)$.

Observe now that, since $e(j', \frac{m}{n}) \notin V + F \cdot e(j, \frac{m}{n})$, then by the same reasoning as above applied to the set $T' = V + F \cdot e(j, \frac{m}{n})$ instead of the set V, we get

$$ e(j', \frac{20m}{n}) \notin A^*(18m)T'A^*(m). $$

By the definition of T' we have $e(j, \frac{m}{n}) \in T'$ and by the minimality of j, $e(i, \frac{m}{n}) \in V$ for $i < j$. By Lemma 25,

$$ e(j, \frac{20m}{n}) \in A^*(18m) \sum_{i=0}^{j} e(i, \frac{m}{n})A^*(m) \subseteq A^*(18m)T'A^*(m). $$

Therefore $A^*(18m)VA(m) + F \cdot e(j, 20m) \subseteq A^*(18m)T'A^*(m)$. Hence $e(j', \frac{20m}{n}) \notin A^*(18m)VA^*(m) + F \cdot e(j, 20m)$, as required. $\qquad\square$

We will now introduce Assumption 2. We introduce this Assumption to shorten the statements of several theorems, where we will simply write *let Assumption 2 hold* instead of writing the sentences from below. The Assumption 2 simply says that numbers m_i and matrices M_i satisfy some conditions, these conditions are now described.

Assumption 2. Let n, k be natural numbers with n even, and let $m_1 < m_2 < \ldots < m_k$ be such that $20nm_i$ divides m_{i+1} for all $1 \leq i < k$ and $20n$ divides m_1. Let M_i for $i = 1, 2, \ldots, k+1$ be matrices with entries in $A^*(n)$ and assume that either M_i^q has entries in $\langle x \rangle$ for almost all q, or M_i has entries in R.

We will use the following notation. The mapping $G : A^*(t \cdot 20m_1) \to A^*(t \cdot 20m_1)$ is defined as in Lemma 20 for $t = \frac{m_k}{m_1}$.

For $i = 2, 3, \ldots$ denote $V_i = L(S(M_i^{m_i/n}))$, $M_i' = G(M_i^{\frac{20m_1}{n}})$, $W_i = L(S(M_i'^{\frac{m_i}{20m_1}}))$ and $T_i = G(E(V_i, m_i) \cap A^*(20m_k))$.

Lemma 28. *Suppose that Assumption 1 holds for F-algebra A. Suppose that Assumption 2 holds. Let $k \geq 0$ be a natural number. Then the following conditions hold.*

1. *If $k = 0$, let $r_0, r_1, \ldots, r_l \in A^*(n)$. Suppose that there are j, j' such that*

$$\alpha \cdot r_j + \beta \cdot r_{j'} \neq 0,$$

   provided that $\alpha, \beta \in F$ are not both zero. Denote $e(j, k) = e(j, k)(r_0, r_1, \ldots, r_t)$. Then there exists m_1 such that $20n$ divides m_1 and

$$\alpha \cdot e(l, \frac{20m_1}{n}) + \beta \cdot e(l', \frac{20m_1}{n}) \notin E(V_1, m_1).$$

2. *If $k > 0$, let $r_0, r_1, \ldots, r_l \in R \cap A^*(20m_k)$ for some $l \geq 1$. Suppose that there are j, j' such that*

$$\alpha \cdot r_j + \beta \cdot r_{j'} \notin W,$$

   provided that $\alpha, \beta \in F$ are not both zero, where $W = \sum_{i=1}^{k} E(V_i, m_i)$. Denote $e(j, k) = e(j, k)(r_0, r_1, \ldots, r_t)$.
   Then there exist m_{k+1} such that for some l, l',

$$\alpha \cdot e(l, \frac{m_{k+1}}{m_k}) + \beta \cdot e(l', \frac{m_{k+1}}{m_k}) \notin W',$$

   provided that $\alpha, \beta \in F$ are not both zero, where $W' = \sum_{i=1}^{k+1} E(V_i, m_i)$ and $V_{k+1} = L(S(M_{k+1}^{\frac{m_{k+1}}{n}}))$. Moreover, $20nm_k$ divides m_{k+1}.

Proof. We will proceed by induction on k. If $k = 0$ then the result follows from Lemma 27 applied for $m = m_1$ and matrix $M = M_1$. Let $k \geq 1$ and assume that the thesis is true for all numbers smaller than k; we will prove it for k.

Suppose that $k = 1$. By the assumption there are j, j' such that $\alpha \cdot r_j + \beta \cdot r_{j'} \notin E(V_1, m_1)$ provided that α, β are not both zero. Let f, G be as in Theorems 20 and 23; then by Theorem 23

$$\alpha \cdot G(r_j) + \beta \cdot G(r_{j'}) \notin \sum_{i=2}^{k} E(W_i, m_i) = 0,$$

since $k = 1$. Next we apply Lemma 27 for matrix $M = G(M_1^{\frac{20m_1}{n}})$, for elements $G(r_i)$ instead of elements r_i, and for $n = 20m_1$, and we find m such that if $\alpha, \beta \in F$ are not both zero then

$$\alpha \bar{e}(j', \frac{20m}{20m_1}) + \beta \bar{e}(j, \frac{20m}{20m_1}) \notin A^*(18m)W_1A^*(m),$$

where $\bar{e}(i, \frac{20m}{20m_1}) = e((i, \frac{20m}{20m_1})(G(r_1), \ldots, G(r_l))$ and $W_1 = S(L(G(M^{\frac{m}{20m_1}}))) = S(L(G(M_1^{\frac{m}{n}})))$.

Observe that $\bar{e}(i, \frac{m}{m_1}) = G(e(i, \frac{m}{m_1}))$. Let $m_2 = m$ then

$$\alpha G(e(j', \frac{m_2}{m_1})) + \beta G(e(j, \frac{m_2}{m_1})) \notin A^*(18m_2)W_1A^*(m_2),$$

By Theorem 23,

$$\alpha e(j', \frac{m_2}{m_1}) + \beta e(j, \frac{m_2}{m_1}) \notin W',$$

hence Lemma 28 holds.

Suppose that $k > 1$ and assume that the result holds for all numbers smaller than k. By the assumption there are j, j' such that $\alpha \cdot r_j + \beta \cdot r_{j'} \notin W$ provided that α, β are not both zero. Let f, G be as in Theorems 20 and 23; then by Theorem 23

$$\alpha \cdot G(r_j) + \beta \cdot G(r_{j'}) \notin \sum_{i=2}^{k} E(W_i, m_i),$$

provided that $\alpha, \beta \in F$ are not both zero.

Recall that $M_i' = G(M_i)^{\frac{20m_1}{n}}$ and $W_i = L(S(M_i'^{\frac{m_i}{20m_1}}))$ for $i = 2, 3, \ldots, k$. Observe that the number of matrices M_i' is $k-1$, hence we can apply the inductive assumption to matrices $M_2', M_3', \ldots, M_k'$. Namely we enumerate $M_i'' = M_{i+1}'$, $m_i' = m_{i+1}$ for every i and we apply the inductive assumption to matrices M_i'' for $i \leq k-1$ and to numbers m_i' and to elements $\bar{r}_i = G(r_i)$ and to $n = 20m_1$. We obtain that there is $m = m_{k+1}$ and j, j' such that if $\alpha, \beta \in F$ are not both zero then

$$\alpha \cdot G(e(j, \frac{m_{k+1}}{m_k})) + \beta \cdot G(e(j', \frac{m_{k+1}}{m_k})) \notin \sum_{i=2}^{k} E(W_i, m_i),$$

since $G(e(j, \frac{m_{k+1}}{m_k})) = e(j, \frac{m_{k+1}}{m_k})(G(r_0), G(r_1), \ldots, G(r_l))$. By Theorem 23, we get $\alpha \cdot e(j, \frac{m_{k+1}}{m_k}) + \beta \cdot e(j', \frac{m_{k+1}}{m_k})) \notin W'$, unless $\alpha = \beta = 0$.   □

Let $X_1, X_2, \ldots$ be matrices as in Theorem 6. Let $Y_1, Y_2, \ldots$ be matrices such that Y_i has entries in $A^*(2)$ and $X_i^2 = Y_i + M(B')$, where $M(B)$ is the set of matrices with entries in $M(B')$. Recall that Let $B' \subseteq A(2)$ is the linear F- space spanned by elements ax^ibx^j and bx^iax^j for all $i, j \geq 0$.

Recall that $e(i, n)(a^2, b^2)$ is the sum of all products of n elements, such that i of them are equal to b^2 and $n - i$ of them are equal to a^2.

Theorem 29. *Let F be a countable field, and suppose that Assumption 1 holds for F-algebra A. For every i, n denote $e(i, n) = e(i, n)(a^2, b^2)$. Let $Y_1, Y_2, \ldots$ be as above, then there are natural numbers $m_1 < m_2 < \ldots$ such that $20nm_i$ divides m_{i+1} for all i and 40 divides m_1. Moreover, for every n there are j, j' such that $\alpha e(j, n) + \beta e(j', n) \notin T$, provided that $\alpha, \beta \in F$ are not both zero, where $T = \sum_{i=1}^{\infty} E(V_i, m_i)$ and $V_i = L(S(Y_i^{\frac{m_i}{2}}))$.*

Proof. Notice that $e(j, n) \subseteq A^*(2n)$ for every n. Observe first that if $u(j, n) \in T$ for some n and all $j \leq n$, then by Lemma 25 for every $n' > n$ we have $e(j, n') \in T$, for all $j \leq 2n'$. Therefore, it is sufficient to prove that there are $m_1 < m_2 < \ldots$ and $j_1, j_2, \ldots$ and $j_1', j_2', \ldots$ such that for every k,

$$\alpha \cdot e(j_k, 10m_k) + \beta \cdot e(j_k', 10m_k) \notin T,$$

provided that $\alpha, \beta \in F$ are not both zero. Notice that

$$T \cap A^*(20m_k) = \sum_{i=1}^{k} E(V_i, m_i),$$

since all spaces $E(V_i, m_i)$ are homogeneous.

We will construct numbers $m_1, m_2, \ldots$ inductively using Lemma 28. By Lemma 28, applied for $n = 2$ and matrices $M_i = Y_i$, there is m_1 and j, j' such that $\alpha \cdot e(j, 10m_1) + \beta \cdot e(j', 10m_1) \notin T$, provided that $\alpha, \beta \in F$ are not both zero, moreover 40 divides m_1.

Suppose now that for some $k \geq 1$ we constructed elements $m_1, \ldots, m_k$ such that if $\alpha, \beta \in F$ are not both zero then

$$\alpha \cdot e(j_k, 10m_k) + \beta \cdot e(j_k', 10m_k) \notin T.$$

By Lemma 28 there are l, l' such that

$$\alpha \cdot e(l, \frac{m_{k+1}}{m_k})(r_0, \ldots, r_{10m_k}) + \beta \cdot e(l', \frac{m_{k+1}}{m_k})(r_0, \ldots, r_{10m_k}) \notin T,$$

where $r_i = e(i, 10m_k)$. By Lemma 26, we get $e(i, 10m_{k+1}) = e(i, \frac{m_{k+1}}{m_k})(r_0, \ldots, r_{10m_k})$. Consequently, $\alpha \cdot e(l, 10m_{k+1}) + \beta \cdot e(l', 10m_{k+1}) \notin T$, therefore we constructed m_{k+1} satisfying the thesis of our theorem. Continuing in this way we construct all elements m_i. $\square$

8. NILITY

Let A^* be a subalgebra of A generated by elements $ax^i ax^j$ and $bx^i bx^j$ for all $i, j \geq 0$.

Let $B' \subseteq A(2)$ be a linear F- space spanned by elements $ax^i bx^j$ and $bx^i ax^j$ for all $i, j \geq 0$. Let $B = \sum_{i=0}^{\infty} A(2i)B'A$. Observe that $A = A^* + B$ and $A^* \cap B = 0$.

In this chapter we denote $e(i, n) = e(i, n)(a^2, b^2)$ to be the sum of all products of n elements, such that i of them are equal to b^2 and $n - i$ of them are equal to a^2, so $e(k, n) \in A^*(2n)$. Recall that an ideal in A is homogeneous if it is homogeneous with respect to the gradation given by assigning gradation 1 to elements a and b and gradation 0 to element x.

Lemma 30. *Suppose that J is a homogeneous ideal in A such that $R/R \cap J$ is a nil algebra. Then there is $m > 0$ such that $e(k, m) \in J + B$, for every $0 \leq k \leq m$.*

Proof. By assumption, there is a number m such that for every $n \geq m$ we have $(a + b^2)^n \in J$. Let $v(k, n)$ be the sum of all products of k elements b^2 and $n - 2k$ elements a; then $v(k, n) \in A(n)$. Observe that

$$(a + b^2)^n = \sum_{0 \leq k \leq \frac{n}{2}} v(k, n + k) \in J,$$

and since J is homogeneous and $v(k, n + k) \in A(n + k)$ it follows that

$$v(k, n + k) \in J$$

for every natural $k \leq \frac{n}{2}$, and every $n \geq m$.

Therefore $v(k, 2m) = v(k, (2m - k) + k) \in J$ for every $0 \leq k \leq m$, since $2m - k \geq m$. Observe that $e(k, m) - v(k, 2m) \in B$, so $e(k, m) \in B + J$. $\qquad\square$

Theorem 31. *Let notation be as in Theorem 6, and denote $Q = \sum_{i=1}^{\infty} S_i$. Then there is a homogeneous ideal J in A which is a platinum ideal, A/J is Jacobson radical and J is contained in $L(Q)$. Moreover, $JA' \subseteq J$ so J is a right ideal in A'.*

Proof. By Theorem 6, there is an ideal I in A such that $I \subseteq Q$. Denote $J = L(I)$; then $L(I) = \sum_{t \in F} \gamma_t(I)$. Observe that $I \subseteq Q$ implies $L(I) \subseteq L(Q)$. We claim that $L(I)$ is an ideal in A, and a right ideal in A'. We need to show that if $\alpha \in L(Q)$ then $r\alpha, \alpha r' \in L(I)$, for every $r \in A$ and $r' \in A'$. Since $\alpha \in L(Q)$ then $\alpha = \sum_{t \in W} \gamma_t(s_t)$ for some finite subset W of F, and where $s_t \in I$. Observe that $r\gamma_t(s) = \gamma_t(\gamma_{-t}(r)s_t) \in \gamma_{-t}(I) \subseteq L(I)$ and $\gamma_t(s)r' = \gamma_t(s\gamma_{-t}(r')) \subseteq \gamma_t(I) \subseteq L(I)$, since by Theorem 6, I is a right ideal in A'. By Lemma 14, $L(I)$ is a platinum ideal in A. Since A/I is a Jacobson radical then $A/L(I)$ is a Jacobson radical, so we can set $J = L(I)$. $\qquad\square$

9. ASSUMPTION 1 IMPLIES THEOREM 1

The aim of this section is to prove the following.

Theorem 32. *Let F be a field, and suppose that Assumption* 1 *holds for F-algebra A. Then there is an F-algebra Z and a derivation D on Z such that the differential polynomial ring $Z[y; D]$ is Jacobson radical but Z is not nil.*

Proof. Let $m_1, m_2, \ldots$ be as in Theorem 29 and denote $T = \sum_{i=1}^{\infty} E(V_i, m_i)$ and $V_i = L(S(Y_i^{\frac{m_i}{2}}))$. By Theorem 29 for every n there are j, j' such that $\alpha \cdot e(j, n) + \beta \cdot e(j', n) \notin T$, provided that $\alpha, \beta \in F$ are not both zero. Observe that since $e(j, n) \in A^*$ and $T \subseteq A^*$ and $A^* \cap B = 0$, it follows that for every n there are $j, j' \leq n$ such that

$$\alpha \cdot e(j, n) + \beta \cdot e(j', n) \notin T + B,$$

provided that $\alpha, \beta \in F$ are not both zero.

By Theorem 31 applied for such $m_1, m_2, \ldots$ we get that there is a homogeneous ideal J in A which is a platinum ideal, A/J is Jacobson radical and J is contained in $L(Q)$, where $Q = \sum_{i=1}^{\infty} S_i$ as in Theorem 6. Moreover, $JA' \subseteq J$ so J is a right ideal in A'. Denote $J^{(*)} = J + xJ + x^2 J + \ldots = \sum_{i=0}^{\infty} x^i J$, then $J^{(*)}$ is a platinum ideal in A'. Let $A^{(*)} = A + xA + x^2 A + \ldots$; then $A^{(*)}$ is an F-algebra and $J^{(*)}$ is an ideal in $A^{(*)}$. By Lemma 7, $A^{(*)}/J^{(*)}$ is Jacobson radical. In addition, if $r + J$ is not a nilpotent in A/J for some $r \in R$, then $r + J^{(*)}$ is not a nilpotent in $A^{(*)}/J^{(*)}$.

We will now show that $R/R \cap J$ is not a nil algebra. Observe now that $L(S_i) \subseteq \sum_{j=1}^{\infty} A(j \cdot 20m_i - 2m_i) L(S_i') A(m_i) A^1$, where $S_i' = S(X_i^{m_i})$ (since $L(A(j)) \subseteq A(j)$ for any j), and that $X_i^2 = Y_i + B_i$, where B_i are matrices with entries in B. Moreover $A(j) \subseteq A^*(j) + B$ for every even j, by the definition of B. It follows that $L(S_i A^1) \subseteq E(V_i, m_i) + B$ for every i. By the first part of this proof we get that for every n there are $j, j' \leq n$ such that $\alpha \cdot e(j, n) + \beta \cdot e(j', n) \notin T + B$. On the other hand $J \subseteq L(Q) = \sum_{i=1}^{\infty} L(S_i) \subseteq T + B$. It follows that

$$\alpha \cdot e(j, n) + \beta \cdot e(j', n) \notin J$$

provided that $\alpha, \beta \in F$ are not both zero. By Lemma 30 we get that $R/R \cap J$ is not a nil algebra. So there is $r \in R$ such that $r + J$ is not nilpotent in A/J. By Lemma 7, $r + J^{(*)}$ is not nilpotent in $A^{(*)}/J^{(*)}$.

Let P be as in Theorem 13; so if $a \in P$ then $ax - xa \in P$, $R \subseteq P$ and P is the smallest subring of A' with this property. We can apply Theorem 13 to $I = J^{(*)}$ and let $Z = P/\bar{J}$ where $\bar{J} = P \cap J^{(*)}$. Then $Z[y; D]$ is a differential polynomial

ring with $y(r + \bar{J}) - (r + \bar{J})y = D(r) + \bar{J}$, where $D(r + \bar{J}) = xr - rx + \bar{J}$. By Theorem 13, $Z[y; D]$ can be embedded in $A'/J^{(*)}$ and the image of $Z[y; D]$ equals $A^{(*)}/J^{(*)}$ where $A^{(*)} = A + xA + x^2A + \ldots$, hence the image of $Z[y; D]$ is Jacobson radical, and so $Z[y; D]$ is Jacobson radical.

It remains to show that Z is not a nil ring. By Lemma 30 we get that $R/R \cap J$ is not a nil algebra. So there is $r \in R$ such that $r + J$ is not nilpotent in A/J. By Lemma 7 we get that $r^n \notin J^{(*)}$, and therefore $r^n \notin \bar{J} = J^{(*)} \cap P$ for $n \geq 1$. Therefore $r + \bar{J}$ is not nilpotent in $P/\bar{J}$, so $P/\bar{J}$ is not nil.   □

10. ASSUMPTION 3

Let C be a matrix with entries $a_{i,j} \in F$ and let $r \in A$ then Ca will denote the matrix with entries $a_{i,j} \cdot r$.

Let $M = \sum_{i=1}^{\xi} A_i a_i$, where for each i, A_i is a matrix with coefficients in F, and $a_1, a_2, \ldots, a_\xi \in A$. By H we will denote the F-algebra generated by matrices A_i, and by W we will denote the Wedderburn radical of H, which is the sum of all nilpotent ideals in H. Notice that W is the largest nilpotent ideal in H, since H is finite dimensional. By s we will denote the smallest natural number such that $W^s = 0$.

We will say that a matrix M satisfies **Assumption 3** if the following holds:

1. $M = \sum_{i=1}^{\xi} A_i a_i$, where for each i, A_i is a matrix with coefficients in F, and $a_1, a_2, \ldots, a_\xi$ are elements from A which are linearly independent over F and have the same degree – say α. Moreover, $a_i \in A(\alpha) \cap \langle x \rangle$ for each $i \leq \xi$ (where $\langle x \rangle$ is the ideal generated by x in A').

2. $A_1 = e$, where e is a matrix such that $e^2 = e$, $r - er \in W$, $r - re \in W$. where W is as at the beginning of this section.

Let $A'^1[y]$ be the polynomial ring in variable y over ring A'^1.

Definition 7. For a variable y (commuting with all elements from A') let $\gamma_y : A' \to A'^1[y]$ be a homomorphism of algebras such that $\gamma_y(a) = a, \gamma_y(b) = b$ and $\gamma_y(x) = x + y$.

For a variable y (commuting with all elements from A') we can write

$$\gamma_y(M) = \sum_{i=0}^{t} y^i M_i,$$

where all entries of M_i are homogeneous elements of A of degree α, similarly to the entries of matrix M.

Let matrix $M = \sum_{i=1}^{\xi} A_i a_i$ satisfy Assumption 3. Let $\gamma_y(M) = \sum_{i=0}^{t} y^i M_i$. Denote

$$w(n,m) = \sum_{i_1+i_2+\ldots+i_m=n} M_{i_1} M_{i_2} \ldots M_{i_m}.$$

The following lemma is known, and is another variant of Lemma 7 in [27].

Lemma 33. *Let notation be as above. Let m, n be natural numbers; then for every $k < m$*

$$w(n,m) = \sum_{i=0}^{n} w(i,k) w(n-i, m-k).$$

Lemma 34. *Let F be an infinite field. Let matrix $M = \sum_{i=1}^{\xi} A_i a_i$ satisfy Assumption 3 and $\gamma_y(M) = \sum_{i=0}^{t} y^i M_i$. Then for each j,*

$$M_j \subseteq \sum_{i=1}^{\xi} A_i A.$$

Moreover, for every $n, m, w(m,n) \subseteq HA$ where H is the algebra generated by matices $A_1, \ldots, A_\xi$.

Proof. Recall that $\gamma_y(M) = \sum_{i=0}^{t} y^i M_i$; therefore by substituting $y = \alpha_i$ for $\alpha \in F$, we get $\gamma_\alpha(M) = \sum_{i=0}^{t} \alpha^i M_i$. By applying this for $\alpha = t_1, \ldots, \alpha = t_\xi$ for various $t_1, \ldots, t_\xi \in F$, and using the fact that a Vandermonde matrix is invertible that each M_i is a linear combination of matrices $\gamma_\alpha(M)$ for various $\alpha \in F$. Recall that $M = \sum_{i=1}^{\xi} A_i a_i$, hence $\gamma_\alpha(M) = \sum_{i=1}^{\xi} A_i \gamma_\alpha(a_i)$. Therefore each M_j is a linear combination of matrices $A_i \gamma_\alpha(a_i) \subseteq A_i A$. By the definition of elements $w(n,m)$ (Definition 7) we get $w(n,m) \in HA$. $\square$

Lemma 35. *Let F be an infinite field and let n be a natural number. Let Q be the linear subspace of A spanned by all entries of matrices $w(n,m)$ for $n = 0, 1, \ldots$; then all entries of the matrix M^m belong to Q. Moreover $Q = S(L(M^m))$.*

Proof. By assumption $\gamma_y(M^m) = (\sum_{i=0}^{t} y^i M_i)^m$, hence for any $\alpha \in F$, when substituting $y = \alpha$ we get

$$\gamma_\alpha(M^m) = (\sum_{i=0}^{t} \alpha^i M_i)^m = \sum_{i=0}^{m \cdot t} \alpha^i w(i,m).$$

Therefore every entry of a matrix $\gamma_\alpha(M^m)$ is in the subspace generated by entries of matrices $w(i,n)$ for various i; hence $S(L(M^m) \subseteq Q$.

On the other hand, let $\alpha_1, \alpha_2, \ldots, \alpha_{tm}$ be non-zero distinct elements of F, then we can substitute $\alpha = \alpha_j$ into the equation

$$\sum_{i=0}^{t \cdot m} \alpha^i \cdot w(i, m) = \gamma_\alpha(M^m).$$

We can then use the Vandermonde matrix argument to show that each $w(i, m)$ is a linear combination of elements $\gamma_{\alpha_i}(M^m)$ for $1 \le i \le tm$. Therefore $Q \subseteq S(L(M^m))$. $\qquad\square$

11. EMBEDDING PLATINUM SUBSPACES IN BIGGER SUBSPACES

Let notation be as in the previous section. Let M be a matrix satisfying Assumption 3. Let H, W, e be as in Assumption 3.

Definition 8. Recall that H can be considered as a subalgebra of some matrix algebra over F. Let H' denote algebra $H + FI$, where I is the identity matrix.

Recall that

$$w(n, m) = \sum_{i_1 + i_2 + \ldots + i_m = n} M_{i_1} M_{i_2} M_{i_3} \ldots M_{i_m}.$$

Let s be such that $W^s = 0$.

Let $f_1, f_2, \ldots$ be elements from H'. We define element $(f_1, f_2, \ldots) * w(m, n)$ for $j = 1, 2, \ldots$ in the following way:

$$(f_1, f_2, \ldots) * w(n, m) = \sum_{i_1 + i_2 + \ldots + i_m = n} f_1 M_{i_1} f_2 M_{i_2} f_3 M_{i_3} \ldots f_m M_{i_m}.$$

Lemma 36. *Let notation be as above and let m be a natural number larger than s (where $W^s = 0$). Let $u = (f_1, f_2, \ldots)$ be such that $f_1, f_2, \ldots, f_s \in W \cup \{I - e\}$; then $u * w(n, m) = 0$, for every n.*

Proof. Observe that for every k, $f_k M_{i_k}$ is a matrix with entries in W; hence $u * w(n, m)$ has entries in $W^s = 0$. $\qquad\square$

Definition 9. For $n \ge 1$ define $t_n = (f_1, f_2, \ldots)$, where $f_1 = f_2 = \ldots = f_{n-1} = I - e$, $f_n = e$ and $I = f_{n+1} = f_{n+2} = \ldots$. For $n \ge 0$ define $t'_n = (f_1, f_2, \ldots)$, where $f_1 = f_2 = \ldots = f_n = I - e$ and $I = f_{n+1} = f_{n+2} = \ldots$.

Lemma 37. *Let notation be as above. Then for every m, n,*

$$w(n, m) = \sum_{i=0}^{s} t_i * w(n, m).$$

Proof. Observe first that $w(n,m) = (I, I, \ldots) * w(n,m) = t_1 * w(n,m) + t_1' * w(n,m)$; then $t_1' * w(n,m) = t_2 * w(n,m) + t_2' * w(n,m)$, and for every i, $t_i' * w(n,m) = t_{i+1} * w(n,m) + t_{i+1}' * w(n,m)$. By summing all these equations for $i = 1, 2, \ldots, s$, and the equation $w(n,m) = t_1 * w(n,m) + t_1' * w(n,m)$, we get $w(n,m) + \sum_{i=1}^{s} t_i' * w(n,m) = \sum_{i=1}^{s+1} t_i * w(n,m) + t_i' * w(n,m)$. By Lemma 36, $t_{s+1} = t_{s+1}' = t_s = 0$. It follows that $w(n,m) = \sum_{i=0}^{s} t_i * w(n,m)$. $\qquad\square$

Definition 10. (Definition of set $D(M)$)

Let matrix M satisfy Assumption 3, and let H, W, e be as in Assumption 3.

Fix $E_1, E_2, \ldots, E_\beta$ - a basis of W for some β (recall that W is the Wedderburn radical of H).

Let $E = \{I - e, E_1, E_2, \ldots, E_\beta\}$.

Let $P_1, P_2, \ldots, P_{\beta'}$ be such that $E_1, \ldots, E_\beta, P_1, \ldots, P_{\beta'}$ span algebra H. We can assume that for every i

$$P_i e = P_i.$$

It follows because $H = He + H(I - e) \subseteq He + W$. Moreover $e = he$ for $h = e$.

Recall that $W^s = 0$.

Let $0 \le q < s$. We say that element $(f_1, f_2, \ldots)$ is good and has distance $q + 1$ if $f_1, \ldots, f_q \in E$, $f_{q+1} \in \{e, P_1, P_2, \ldots, P_{\beta'}\}$ and $I = f_{q+2} = f_{q+3} = \ldots$.

The set of all good elements will be denoted $D(M)$.

Lemma 38. *Let M be a matrix satisfying Assumption 3. The set $D(M)$ is finite.*

Proof. It follows because every element in $D(M)$ has distance at most s. $\qquad\square$

Lemma 39. *Let M be a matrix satisfying Assumption 3. Then, for every m, n, $w(n,m)$ is a linear combination of elements $u * w(n,m)$ with $u \in D(M)$.*

Proof. It follows from Lemma 37, since every $t_i \in D(M)$. $\qquad\square$

Fix m. Let $u \in D(M)$. Recall that $u * w(n,m)$ is a matrix with coefficients in A. By $u * w(n,m)_{k,l}$ we denote the element of A which is at the k, l entry of matrix $u * w(n,m)$. By $[u * w(n,m)]_{k,l}$ we will mean the quintuple (u, n, m, k, l).

Recall that by I we denote the identity element in H' (which can be also seen as the identity matrix when we embed H into a matrix ring.)

Definition 11. (Definition of ordering)

We first denote an ordering on elements of E : $E_1 < E_2 < \ldots < E_\beta$. We then define $E_\beta < I - e < e < P_1$ and $P_1 < P_2 < \ldots < P_{\beta'}$. We can now define a lexicographical ordering on the good set $D(M)$.

In particular, if the distance of v is larger than the distance of u then $v < u$; for example $(I - e, e, I, \ldots) < (P_1, I, I, \ldots)$.

Let M be a matrix satisfying Assumption 3. Fix m, and define the following ordering on quintuples $[u * w(n, m)]_{k,l}$ with $u \in D(M)$, and $k, l \leq d$ where M is a d by d matrix:

1. If the distance of v is larger than the distance of u then $[v * w(n, m)]_{k,l} < [u * w(n', m)]_{k',l'}$, for every $n, n', k, k', l, l' \leq d$.

2. If the distance of v is the same as the distance of u and $n < n'$ then $[v * w(n, m)]_{k,l} < [u * w(n', m)]_{k',l'}$, for every $k, k', l, l' \leq d$.

3. If the distance of u is the same as the distance of v and v is smaller than u then $[v * w(n, m)]_{k,l} < [u * w(n, m)]_{k',l'}$, for every $k, k', l, l' \leq d$.

4. If $(k, l) < (k', l')$ with respect of lexicographical ordering then $[u * w(n, m)]_{k,l} < [u * w(n, m)]_{k',l'}$, for every u, n.

Fix m. Notice that this is an ordering on the set of quintuples $[u * w(n, m)]_{k,l}$ with $u \in D(M)$ and $k, l \leq d$, where M is a d by d matrix.

12. SETS $B_m(M)$ AND $Z_m(M)$

We now define sets $B_m(M)$ and $Z_m(M)$.

Definition 12. (Definition of set $B_m(M)$) Let M be a matrix satisfying Assumption 3, and m, n be natural numbers.

We will say that quintuple $[u * w(n, m)]_{k,l}$ is in the set $B_m(M)$ if $u * w(n, m)_{k,l}$ is a linear combination over F of elements $v * w(n', m)_{k',l'}$ such that $[v * w(n', m)]_{k',l'} < [u * w(n, m)]_{k,l}$.

Definition 13. (Definition of set $Z_m(M)$) Let M be a matrix satisfying Assumption 3, and m, n be natural numbers.

Recall that R is the algebra generated by elements a and b.

We will say that quintuple $[u * w(n, m)]_{k,l}$ is in the set $Z_m(M)$ if there is element $r \in R$ such that:

1. This element r is a linear combination of elements $v * w(n', m)_{k',l'}$ such that $[v * w(n', m)]_{k',l'} \leq [u * w(n, m)]_{k,l}$.

2. r is not a linear combination of elements $v * w(n', m)_{k',l'}$ with $[v * w(n', m)]_{k',l'} < [u * w(n, m)]_{k,l}$.

Notice that for a given quintuple $[u * w(n, m)]_{k,l} = (u, n, m, k, l) \in Z_m(M)$, there may be many elements r satisfying Properties [1] and [2] above. However, we fix one such element r and call it $r(u, n, m, k, l)$.

Lemma 40. *Fix m. Let M be a matrix satisfying Assumption 3. The sets $Z_m(M)$ and $B_m(M)$ are disjoint, that is $Z_m(M) \cap B_m(M) = 0$.*

Proof. Suppose on the contrary, that there is some element in $[u * w(n, m)]_{k,l} \in Z_m(M) \cap B_m(M)$, then there is $r \in R$ which is a linear combination of some elements $v * w(n', m)_{k',l'}$ such that $[v * w(n', m)]_{k',l'} \leq [u * w(n, m)]_{k,l}$. Because $[u * w(n, m)]_{k,l} \in B_m(M)$ then $u * w(n, m)_{k,l}$ is a linear combination of $v * w(n', m)_{k',l'}$ such that $[v * w(n', m)]_{k',l'} < [u * w(n, m)]_{k,l}$. Therefore r is also a linear combination of $[v * w(n', m)]_{k',l'}$ such that $[v * w(n', m)]_{k',l'} < [u * w(n, m)]_{k,l}$, a contradiction with the definition of set $Z_m(M)$. $\qquad\square$

Lemma 41. *Let notation be as above. Let m be a natural number and let $R_m(M)$ be the linear space spanned by all elements from R which are a linear combination of elements $u * w(n, m)_{k,l}$ for some $u \in D(M)$ and some n, k, l with $k, l \leq d$ (where M is a d by d matrix). Then the dimension of the space $R_m(M)$ is the same as the cardinality of set $Z_m(M)$.*

Proof. Let $r(u, n, m, k, l) \in R$ be as in Definition 13. Let $Q_m(M)$ be the linear space spanned by elements $r(u, n, m, k, l) \in R$ for $(u, n, m, k, l) \in Z_m(M)$. We will show that $R_m(M) = Q_m(M)$. Observe first that if $s \in R_m(M)$ then

$$s = \sum_{(v,n',m,k',l') \leq (u,n,m,k,l)} \alpha_{(v,n',m,k',l')} \cdot v * w(n', m)_{k',l'},$$

for some $(u, n, m, k, l) = [u * w(n, m)]_{k,l}$ and some $\alpha_{(v,n',m,k',l')} \in F$. If we take a presentation of s with $[u * w(n, m)]_{k,l}$ minimal possible, we in addition get $\alpha_{(u,n,m,k,l)} \neq 0$ and $[u * w(n, m)]_{k,l} \in Z_m(M)$.

Note that if $s = r(u, n, m, k, l)$, then $s \in Z_m(M)$. Suppose that $s \neq r(u, n, m, k, l)$; then by Definition 13 there is $\alpha \in F$ such that

$$s - \alpha \cdot r(u, n, m, k, l) = \sum_{(v,n',m,k',l') < (u,n,m,k,l)} \beta_{(v,n',m,k',l')} \cdot v * w(n', m)_{k',l'}$$

for some $\beta_{(v,n',m,k',l')} \in F$. Therefore $s - r(u, n, m, k, l) \in R_m(M)$.

We will now show that $s \in Q_m(M)$ by induction with respect to the ordering of the quintuples $(u, n, m, k, l) \in Z_m(M)$.

Let $[u_0 * w(i, m)]_{t,t'}$ be the minimal quintuple in $Z_m(M)$ such that there is $s \in R_m(M)$ with $s \notin Q_m(M)$. Notice that $r(u_0, i, m, t, t') \in R_m(M)$. Let $s \in R_m(M)$ have a presentation as above with $(u, n, m, k, l) = (u_0, i, m, t, t')$. By the definition of $Z_m(M)$ we get that for some α the element $s - \alpha \cdot r(u_0, i, m, t, t')$ is a sum of elements associated to quintuples smaller than (u_0, i, m, t, t'). Notice that $s - \alpha \cdot r(u_0, i, m, t, t') \in R_m(M)$, and by the minimality of s we get that

$s - \alpha \cdot r(u_0, i, m, t, t') \in Q_m(M)$. Since $r(u_0, i, m, t, t') \in Q_m(M)$, it follows that $s \in Q_m(M)$. $\qquad\square$

13. Main supporting lemma

Let M be a matrix which satisfies Assumption 3, and let notation be as in the previous section.

Lemma 42. *Let M be a matrix satisfying Assumption 3. Let m be a natural number and let $u = (f_1, f_2, \ldots) \in D(M)$. For every $k \leq m$,*

$$u*w(n,m) = \sum_{j=0}^{n}((f_1, f_2, \ldots, f_k, I, I, \ldots)*w(j,k)) \cdot ((f_{k+1}, f_{k+2}, \ldots)*w(n-j, m-k)).$$

Proof. This follows from Lemma 33 and from the definition of operation $*$. $\qquad\square$

Lemma 43. *Let notation be as in Lemma 42. Suppose that u has distance $k+1$. Then*

$$u * w(n,m) = \sum_{j=0}^{n}((f_1, f_2, \ldots, f_k) * w(j,k)) \cdot f_{k+1} \cdot w(n-j, m-k).$$

Moreover, for every $t \leq m - k$,

$$w(n-j, m-k) = w(0,t)w(n-j, m-k-t) + \sum_{i=1}^{n-j} w(i,t)w(n-j-i, m-k-t).]$$

Proof. Since u has distance $k+1$ then $u = (f_1, f_2, \ldots, f_k, f_{k+1}, I, I, \ldots, I)$, where $f_{k+1} \in \{e, P_1, \ldots, P_{\beta'}\}$ and by assumptions on P_i's we have $f_{k+1}e = f_{k+1}$. The first equation follows from Lemma 42. The second equation follows when we apply Lemma 33 to $w(n-j, m-k)$. $\qquad\square$

Let M be a matrix satisfying Assumption 3, and let notation be as in Assumption 3. In particular, H' is an algebra generated by matrices from H and an identity matrix, W is the Wedderburn radical of H and $W^s = 0$. Recall that I denotes the identity element in H'.

Lemma 44. *Let notation be as above. Let $f_1, f_2, \ldots, f_k \in W \cup \{I - e\}$ and let $f_{k+1} \in H'$. Let $u = (f_1, f_2, \ldots, f_{k+1}, I, I, \ldots)$, and let $m, n > 0$, $m > k+1$, $m > s$. Then $u * w(n,m)$ is a linear combination of matrices of the form $u' * w(n,m)$ and $u'' * w(n,m)$, where $u' \in D(M)$ and u' has distance $k+1$, and where u'' is of the form $(g_1, \ldots, g_{k+1}, I, I, \ldots)$ where $g_1, g_2, \ldots, g_{k+1} \in E$.*

Proof. Observe that f_{k+1} is a linear combination of elements α_i and β_i, where $\alpha_1 \in E = \{E_1, \ldots, E_\beta, I - e\}$ and $\beta_i \in \{e, P_1, \ldots, P_{\beta'}\}$ (where notation is as in the definition of the ordering of $D(M)$). Therefore $u * w(n, m)$ is a linear combination of elements $u(i) * w(n, m)$ and elements $u(i) * w(n, m)$, where $u(i) = (f_1, \ldots, f_k, \alpha_i, I, I, \ldots)$ and elements $u'(i) = (f_1, \ldots, f_k, \beta_i, I, I, \ldots)$, for some i. Observe that $u'(i)$ are in the set $D(M)$ and have distance $k + 1$. On the other hand, elements $u(i)$ are of the form $(g_1, \ldots, g_{k+1}, I, I, \ldots)$, where $g_1, g_2, \ldots, g_{k+1} \in W \cup \{I - e\}$ and $g_{k+2} = I$, as required. $\square$

14. INTRODUCING SETS $U_{k,t}$ AND $V_{k,t}$

Let $M = \sum_{i=1}^{\xi} A_i a_i$ be a matrix satisfying Assumption 3. Let notation be as in Assumption 3 and in the previous sections. Let $a_{\xi+1}, a_{\xi+2}, \ldots$ be such that $a_1, a_2, \ldots, a_\xi, a_{\xi+1}, \ldots$ is a basis of $A(\alpha)$ (such elements exist by Zorn's lemma). Recall that $a_1, \ldots, a_\xi \in \langle x \rangle$; hence we can assume that every a_i is either in $\langle x \rangle$ or in R. Recall that $\langle x \rangle$ is the ideal of A' generated by x.

Denote $Q_t = \sum_{(i_1, i_2, \ldots, i_t) \neq (1,1,\ldots,1)} a_{i_1} a_{i_2} \ldots a_{i_t} A$. Let k, t be natural numbers, and define:

$$V = A(k)a_1^t A, U = A(k)Q_t.$$

Recall that M is a d by d matrix. By $T(U)$ we will denote the set of all d by d matrices with all entries in U, and by $T(V)$ we will denote the set of all d by d matrices whose entries are in V. Recall that s is such that $W^s = 0$.

Remark 45. Let $r \in R \cap A(m)$ for some $m > t + k$. Then $r \in U$.

Proof. Denote $Q = A(k)(R \cap A(t))A(m-t-k)$, $Q' = A(k)(\langle x \rangle \cap A(t))A(m-t-k)$. Notice that $Q \cap Q' = 0$, since A is the free algebra generated by ax^i, bx^i for $i \geq 0$. Let $U_1 = U \cap Q$ and $U_2 = U \cap Q'$. Observe that $U \cap A(m) = U_1 \oplus U_2$, because every element among $a_1, a_2, \ldots$ is either in R or in $\langle x \rangle$.

Notice that if $a \in A(m)$ then $a \in U_1 + U_2 + V$. Recall that $U_2, V \subseteq \langle x \rangle$, since $a_1 \in \langle x \rangle$. Let $r = r_1 + r_2 + r_3$, where $r_1 \in U_1, r_2 \in U_2, r_3 \in V$. Observe that $r - r_1 \in Q$ and $r_2 + r_3 \in Q'$; it follows that $r = r' \in U_1 \subseteq U$. $\square$

Let $\mathcal{G} : A(m) \cap V \to A(m - t)$ be the linear mapping defined for monomials and then extended by linearity to all elements from $A(m) \cap V$ as follows:

$\mathcal{G}(wa_1^t w') = ww'$, where w is a monomial from $A(k)$ and w' is a monomial from $A(m - k - t)$. We can then extend mapping $\mathcal{G}$ to matrices: if M is a matrix with entries $a_{i,j}$ then $\mathcal{G}(M)$ is the matrix with entries $\mathcal{G}(a_{i,j})$.

Lemma 46. *Let n, m, k, t be natural numbers with $m > k + t, m > t + s, t \geq 1$. Let $\mathcal{G}$ be defined as before this theorem. Let $u = (f_1, f_2, \ldots) \in D(M)$ have distance $k + 1$, so $f_1, \ldots, f_k \in E$ and $f_{k+1} = he$ for some $h \notin W$. Then $u * w(n, m) = \bar{v} + \bar{u}$ for some $\bar{v} \in T(V)$, $\bar{u} \in T(U)$. Moreover, $\mathcal{G}(\bar{v}) = u * w(n, m - t) + s$, where s is a linear combination of elements of the form $u' * w(n - i, m - t)$ for $i > 0$ and where $u' \in D(M)$ has either the same distance as u or larger distance than u.*

Proof. Observe that $w(n, m) = \sum_{i=0}^{n} F_i'$ by Lemma 43, where

$$F_i' = \sum_{j=0}^{n-i} w(j, k) w(i, t) w(n - i - j, m - k - t).$$

By the definition of operation $*$ we get $u * w(n, m) = \sum_{i=0} F_i$ where

$$F_i = \sum_{j=0}^{n-i} [u' * w(j, k)] \cdot f_{k+1} \cdot w(i, t) \cdot w(n - i - j, m - k - t),$$

where $u' = (f_1, f_2, \ldots, f_k, I, I \ldots)$. Recall also that $f_{k+1} = he$ for some $h \notin W$.

Observe that

$$w(j, t) = q_j a_1{}^t + u_j',$$

for some $u_j' \in T(U)$ and some matrix q_j with entries in F. Recall that $w(0, t) = M_0{}^t = M^t = (\sum_{i=1}^{\xi} A_i a_i)^t$ and that $A_1 = e$. Therefore $q_0 = A_1{}^t = e$, so $w(0, t) = e a_1{}^t + u_0'$. It follows that $F_0 = v_0 + u_0$, where $u_0 \in T(U)$ and

$$v_0 = \sum_{j=0}^{n} [u' * w(j, k)] \cdot f_{k+1} e a_1{}^t \cdot w(n - j, m - k - t) \in T(V).$$

Recall that $f_{k+1} e = f_{k+1}$, by assumption on P_i's. By Lemma 33,

$$\mathcal{G}(v_0) = \sum_{j=0}^{n} [u' * w(j, k)] \cdot f_{k+1} e \cdot w(n - j, m - k - t) = u * w(n, m - t).$$

Observe now that $F_i = v_i + u_i$, where $u_i \in T(U)$ and

$$v_i = \sum_{j=0}^{n-i} [u' * w(k, j)] \cdot f_{k+1} \cdot q_i a_1{}^t \cdot w(m - k - t, n - i - j) \in T(V).$$

By Lemma 25,

$$\mathcal{G}(v_i) = u(i) * w(, n - i, m - t)$$

where $u(i) = (f_1, f_2, \ldots, f_k, f_{k+1} q_i, I, I, \ldots)$. By applying Lemma 44 several times we get that $u(i) * w(n - i, m - t)$ is a linear combination of elements of the form $u' * w(n - i, m - t)$ for $i > 0$ and where u' is in $D(M)$ and has distance at least $k + 1$, or $u' = (g_1, \ldots g_l, I, I, \ldots)$ for some $l > s$ and all $g_1, \ldots, g_l \in E$. In the latter case $u' * w(n - i, m - t) = 0$ by Lemma 36, hence the latter case

can be omitted. Observe now that $\bar{v} = \sum_{i=0}^{n} v_i$, so $\mathcal{G}(\bar{v}) = \mathcal{G}(v_0) + \sum_i \mathcal{G}(v_i) = u * w(n, m-t) + \sum_{i=1}^{n} u(i) * w(n-i, m-t)$ and the result follows (since u has distance $k+1$). $\qquad\square$

Lemma 47. *Let m, k, t, n be natural numbers with $m > k + t$, $m > t + s$ and $t \geq s$, $t \geq 1$ (where $W^s = 0$). Let $u = (f_1, f_2, \ldots) \in D(M)$ have distance larger than $k+1$, so $f_1, \ldots, f_{k+1} \in E$. Then $u * w(n, m) = \bar{v} + \bar{u}$ for some $\bar{v} \in T(V)$, $\bar{u} \in T(U)$.*

Let $\mathcal{G} : A(m) \cap V \to A(m-t)$ be as defined and extended to matrices as in Lemma 46. Then $\mathcal{G}(\bar{v})$ is a linear combination of elements of the form $u' * w(n', m-t)$ for $n' \geq 0$ and where $u' \in D(M)$ has distance larger than $k+1$.

Proof. Observe that $w(n, m) = \sum_{i=0}^{n} F_i'$ by Lemma 43, where

$$F_i' = \sum_{j=0}^{n-i} w(j, k) w(i, t) w(n-i-j, m-k-t).$$

By the definition of operation $*$ we get $u * w(n, m) = \sum_{i=0} F_i$ where

$$F_i = \sum_{j=0}^{n-i} [u' * w(j, k)] \cdot u'' * \cdot w(i, t) \cdot w(n-i-j, m-k-t),$$

where $u' = (f_1, f_2, \ldots, f_k, I, I \ldots)$ and $u'' = (f_{k+1}, f_{k+2}, \ldots, f_s, I, I, \ldots)$ (as elements of $D(M)$ have distance at most s).

Observe that

$$u'' * w(j, t) = q_j a_1{}^t + u_j'$$

for some $u_j' \in T(U)$ and some matrix q_j with entries in F. Notice also that $q_j = f_{k+1} h$ for some matrix h since f_{k+1} is the first entry of u''. It follows that $q_j \in W$ since $f_{k+1} \in W \cup \{I - e\}$.

Observe now that $F_i = v_i + u_i$, where

$$v_i = \sum_{j=0}^{n-i} [u' * w(j, k)] \cdot q_i a_1{}^t \cdot w(n-i-j, m-k-t), \in T(V)$$

and $u_i \in T(U)$. By Lemma 33,

$$\mathcal{G}(v_i) = u(i) * w(n-i, m-t)$$

where $u(i) = (f_1, f_2, \ldots, f_k, q_i, I, I, \ldots)$. Recall that $q_i \in W$. Because $f_1, \ldots, f_{k+1} \in W$, then by Lemma 44 applied several times we get that $u(i) * w(n-i, m-t)$ is a linear combination of elements of the form $u' * w(n-i, m-t)$ for $i > 0$ and where either u' is in $D(M)$ and has the distance larger than $k+1$, or $u' = (g_1, \ldots g_l, I, I, \ldots)$ for some $l > s$ and all $g_1, \ldots, g_l \in E$. In the latter case $u' * w(m, n) = 0$ by

Lemma 36, hence this case can be omitted. Observe now that $\bar{v} = \sum_{i=0}^{n} v_i$, so $\mathcal{G}(\bar{v}) = \sum_{i=0}^{n} \mathcal{G}(v_i) = \sum_{i=0}^{n} u(i) * w(n-i, m-t)$; the result follows (since each $u(i)$ has distance larger than $k+1$). $\qquad\square$

Recall that s is such that $W^s = 0$.

Theorem 48. *Let M be a matrix satisfying Assumption 3. Let $t > s$, and $k, l > 0, m > k+t, m > t+s, n \geq 0$ be natural numbers. Let $u \in D(M)$. If element $[u * w(n, m)]_{j,l} \in Z_m(D)$ then $[u * w(n, m-t)]_{j,l} \in B_{m-t}(M)$.*

Proof. Since $u \in D(M)$ then u has distance $k+1$ for some $k \geq 0$. By the definition of set $Z_m(M)$ there is $r \in R$ such that

$$r = \sum_{(v, n', m, j', l') \leq (u, n, m, j, l)} \alpha_{(v, n', m, j', l')} v * w(n', m)_{j', l'}$$

where $\alpha_{(v, n', m, j', l')} \in F$ and $\alpha_{(u, n, m, j, l)} \neq 0$. Observe that for every $v \in D(M)$ and every n' we can write

$$v * w(n', m) = q(v, n', m) + z(v, n', m)$$

where $q(v, n', m) \in T(V)$ and $z(v, n', m) \in T(U)$, where $T(U), T(V)$ are as in Lemmas 46 and 47. By $q(v, n', m)_{j,l}$ we will denote the k, l-entry of matrix $q(v, n', m)$ (similarly for $z(v, n', m)$). It follows that

$$r = \sum_{(v, n', m, j', l') \leq (u, n, m, j, l)} \alpha_{(v, n', m, j', l')} (q(v, n', m)_{j', l'} + z(v, n', m)_{j', l'}).$$

By Remark 45 $r \in U$, hence $\sum_{(v, n', m, j', l') \leq (u, n, m, j, l)} \alpha_{(v, n', m, j', l')} q(v, n', m)_{j', l'} \in U$. Since $U \cap V = 0$ it follows that

$$\sum_{(v, n', m, j', l') \leq (u, n, m, j, l)} \alpha_{(v, n', m, j', l')} q(v, n', m)_{j', l'} = 0.$$

We can apply mapping $\mathcal{G}$ to this equation. We then get

$$\mathcal{G}(q(v, n, m)_{j,l}) = \sum_{(v, n', m, j', l') < (u, n, m, j, l)} \beta_{(v, n', m, j', l')} \mathcal{G}(q(v, n', m)_{j', l'}),$$

for some $\beta_{(v, n', m, j', l')} \in F$. Let W be the linear space spanned by all elements $v * w(n', m-t)_{j', l'}$ with $[v * w(n', m-t)]_{j', l'} < [u * w(n, m-t)]_{j, l}$. By Lemma 46, $\mathcal{G}(q(u, n, m)_{j,l}) - u * w(n, m-t)_{j, l} \in W$. By Lemmas 47 and 46, $\mathcal{G}(q(v, n', m)_{j', l'}) \in W$, provided that $[v * w(n', m)]_{k', l'} < [u * w(n, m)]_{j', l'}$ (if v has the same distance as u then we use Lemma 46; if v has distance larger than u we use Lemma 47). Therefore, $u * w(n, m-t)_{j, l} \in W$. This means that $[u * w(n, m-t)]_{j, l} \in B_{m-t}(M)$. $\qquad\square$

15. Main result

Let N be a matrix. Recall that by $S(N)$ we denote the linear space spanned by all entries of matrix N; similarly if $N_1, N_2, \ldots, N_k$ are matrices with entries in A then by $S(N_1, N_2, \ldots, N_k)$ we will denote the linear space spanned by all entries of matrices $N_1, N_2, \ldots, N_k$.

Theorem 49. *Let M be a matrix satisfying Assumption 3. For arbitrary c, there is $m > c$ such that $R \cap S(w(0, m), w(1, m), w(2, m), w(3, m), \ldots)$ is a linear space over F of dimension less than $\sqrt{n}$.*

Proof. Recall that, by Lemma 39, $w(0, m), w(1, m), \ldots \in \sum_{u \in D(M), i=0,1,\ldots} Fu * w(i, m)$ for $i = 1, 2, \ldots k$ and $u \in D(M)$ with distance at most s, where $W^s = 0$. It is sufficient to show that for infinitely many m the dimension of the set $R_m(M) = R \cap \sum_{u \in D_m(M), i=0,1,\ldots} S(u * w(i, m))$ is less than $\sqrt{m}$. By Lemma 41 it is equivalent to show that the cardinality of set $Z_m(M)$ is smaller than $\sqrt{m}$ for infinitely many m.

We will provide a proof by contradiction. Suppose, on the contrary, that there is c such that for every $m > c$, set Z_m has more than $\sqrt{m}$ elements.

By Theorem 48, if $[u' * w(i, m)]_{k,l} \in Z_m(M)$ and $[u * w(i', m')]_{k',l'} \in Z_{m'}(M)$ and $m > m' + s$, $m' > 2s$ then $(u, i, k, l) \neq (u', i', k', l')$. It follows because by Theorem 48 $[u * w(i, m')]_{k,l} \in B_{m'}(M)$ and $B_{m'}(M) \cap Z_{m'}(M) = 0$ by Theorem 40, so $(u, i, k, l) \neq (u', i', k', l')$.

Let m be a natural number. Recall that M is a d by d matrix with entries in $A(\alpha) \cap \langle x \rangle$. Recall that $\gamma_y(M) = \sum_{i=0}^{t} M_i y^i$, so $w(i, m) = 0$ if $i > tm$.

Let $C_m(M)$ be the set of all tuplets (u, i, m, k, l), where $0 \leq i \leq m(s + 2)t$, $k, l \leq d$, $u \in D(M)$. Recall that set $D(M)$ is finite. Therefore there is a constant z such that for every m the cardinality of the set $C_m(M)$ is smaller than zm.

We can now choose $m > z^2$ and $m > c + 3s$.

For $q = 1, 2, \ldots, m$ let F_q be the set of elements (u, i, m, k, l) such that $(u, i, m + q(s + 1), k, l) \in Z_{m+q(s+1)}(M)$ where $u \in D(M)$.

Let $(u, i, m + q(s + 1), k, l) \in Z_{m+q(s+1)}(M)$. Notice that $i \leq t(m + q(s + 1)) \leq m \cdot t \cdot (s + 2)$, as otherwise $w(i, m + q(s + 1)) = 0$ (since $w(i, j)$ is zero if $i > t \cdot j$ by the construction of $w(i, j)$). Therefore $F_q \subseteq C_m(M)$, for $q = 1, 2, \ldots, m$.

Notice that the cardinality of F_q is the same as the cardinality of $Z_{m+q(s+1)}(M)$, and hence larger than $\sqrt{m}$. By Theorem 48, $F_i \cap F_j = \emptyset$ for any $1 \leq i, j \leq m$. Therefore the cardinality of $\bigcup_{i=1}^{s} F_i$ is larger than $m\sqrt{m}$.

Recall that $F_i \subseteq C_m(M)$ for $i = 1, 2, \ldots, m$. Therefore, the cardinality of $C_m(M)$ has to be at least $m\sqrt{m}$. This gives us a contradiction, since we showed that the cardinality of $C_m(M)$ is smaller than zm, yet we assumed that $m > z^2$. $\qquad\square$

We will now prove that Assumption 1 holds for algebras over a field F, where F is the algebraic closure of a finite field.

Theorem 50. *Let F be a field. Let M be a matrix satisfying Assumption 3. For arbitrary c, there is $m > c$ such that $R \cap S(L(M^m))$ is a linear space over F of dimension less than $\sqrt{n}$.*

Proof. We can now apply Theorem 49 to the matrix M to get that

$$R \cap S(w(0, m), w(1, m), w(2, m), \ldots)$$

is a linear space over F of dimension less than $\sqrt{n}$. By Lemma 35, we have

$$S(L(M^m)) = S(w(0, m), w(1, m), w(2, m), \ldots).$$

$\qquad\square$

16. Matrices

In this section F denotes the algebraic closure of a finite field. The aim of the next two sections is to show that, if N is an arbitrary matrix with entries in $A(j) \cap \langle x \rangle$ for some j, then some power of N satisfies Assumption 3. Here the notation A and R is not related to the similar notation appearing in previous chapters; instead, R denotes a general ring.

Definition 14. Let R be a finite dimensional F-algebra generated by elements $r_1, r_2, \ldots, r_n \in R$. Let M be the multiplicative monoid generated by elements $r_1, \ldots, r_n$. Let Z^+ be the set of all positive integers. Let $\alpha : M \to Z^+$ be the function such that

- $\alpha(r_i) = 1$ for $i = 1, \ldots, n$.
- If $u, v \in M$ then $\alpha(u \cdot v) = \alpha(u) + \alpha(v)$.

The number $\alpha(r)$ will be caled the weight of element $r \in M$. Notice that one element may have many weights.

We say that α is the weight function on R related to elements $r_1, \ldots, r_n$.

Definition 15. Let notation be as in Definition 14. We will say that an element $r \in R$ is pseudo-homogeneous if it can be expressed as a linear combination of

elements with the same weight, say β. The weight of r is β. The weight of r will be denoted $\deg_w(r)$.

By the linear space of pseudo-homogeneous elements of weight n we will mean the linear space over F spanned by all pseudo-homogeneous elements of weight n; this linear space will be denoted $R(n)$.

By R^1, we will denote the algebra which is the usual extension of R by an identity element, and by $R(0)$ we will denote the space $F \cdot 1$ in R^1.

The following Lemma closely resembles Lemma 1 from [21]. However, our ring need not be graded, so we provide a detailed proof using similar methods as in [21].

Lemma 51. *Let R be a simple F-algebra with an identity element and let notation be as in Definition 14. Assume that*

$$1 = \sum_{i=k}^{k'} b_i,$$

where b_i is a pseudo-homogeneous element of weight i for each i. Let $h \in R$ be a pseudo-homogeneous element in R. Denote $H_i = \sum_{j=0}^{i-\deg_w h} R(j)hR(i-j-\deg_w h)$ for $n \geq \deg_w h$. Then there exist $c_i \in H(i)$ such that

$$1 = \sum_{i=t}^{t'} c_i$$

for some $t > k'$ and $t' - t < k'$.

Proof. Let I be the ideal generated by h in R then $I = \sum_{i=\deg_w h}^{\infty} H_i$. Notice that $R = I$ since R is a simple algebra, therefore there are $c_i \in H(i)$ such that $1 = \sum_{i=t}^{t'} c_i$; $t' - t$ will be called the length of expression $1 = \sum_{i=t}^{t'} c_i$. We can assume that $t > k$ and that $t' - t$ is minimal possible. If $t' - t < k'$ then the result follws; suppose that $t' - t \geq k'$. Recall that $\sum_{i=k}^{k'} b_i = 1$ therefore

$$1 = c_t(\sum_{i=k}^{k'} b_i) + \sum_{i=t+1}^{t'} c_i.$$

Notice that the weight of element $c_t b_{k'}$ is $t + k' \leq t'$. Therefore, $1 = \sum_{i=t+1}^{t'} e_i$ where $e_i = c_t b_{i-t} + c_i$ for $i \geq t + 1$. We have obtained a contradiction since the expression $1 = \sum_{i=t+1}^{t'} e_i$ has smaller length than the expression $1 = \sum_{i=t}^{t'} c_i$. $\square$

The following lemma resembles Proposition 1 from [21]. However, our ring is ungraded, so we need to repeat the argument.

Lemma 52. *Let R be a simple F-algebra with an identity element and let notation be as in Definition 14. Let*

$$1 = \sum_{i=k}^{k'} b_i$$

with each b_i pseudo-homogeneous of weight i for some k, k', with $k' - k$ the minimal possible. Then all b_i are in the center of R.

Proof. The proof is similar to the proof of Proposition 1 in [21]. We will show first that all b_i belong to the center of R. Suppose the contrary, and let z be minimal such that $c' = rb_z - b_z r \neq 0$ for some pseudo-homogeneous r (we can assume that r is pseudo-homogeneous, since every element in R is a linear combination of pseudo-homogeneous elements). Since R is simple, then R equals the ideal generated by c'. Notice that c' is a pseudo-homogeneous element. Let c be a pseudo-homogeneous element which is a product of the generators $r_1, \ldots, r_n$ of R and the element c', with the element c' appearing at least $2k'$ times. Such a non-zero element c exists, since a simple ring is prime.

By the previous lemma,

$$1 = \sum_{j=t}^{t'} c_i$$

where c_i are pseudo-homogeneous and $c_i \in \sum_{j=0}^{i - \deg_w c} R(j) c R(i - j - \deg_w c) \subseteq R_i$. Moreover, $t' - t < k'$. Recall that $c' = -\sum_{i=z+1}^{k'} d_i$, with $d_i = rb_i - b_i r$.

Notice that c_t is pseudo-homogeneous of weight t. Observe that c' is pseudo-homogeneous of weight $z + \deg_w r$ and each d_i is pseudo-homogeneous of weight $i + \deg_w r$. Recall that each c_i is a linear combination of products of elements a_i and element c'; we can substitute at some place in each of these products $c' = -\sum_{i=z+1}^{k'} d_i$. Therefore,

$$c_t = \sum_{i=t+1}^{k'-z+t} f_j$$

where each f_j is a linear combination of products of some generators $r_1, \ldots, r_n$ of R and element c', with element c' appearing at least $2k' - 1$ times and each product is pseudo-homogeneous of weight j (so each f_j is pseudo-homogeneous of weight j). Now if $k' - z + t \leq t'$ we can substitute in this way for element c_t in $1 = \sum_{j=t}^{t'} c_i$ and obtain

$$1 = \sum_{j=t+1}^{t'} c_i'$$

where each c_i' is pseudo-homogeneous of weight i and is a linear combination of products of the generators $r_1, \ldots, r_n$ of R and the element c', with the element c' appearing at least $2l - 1$ times.

Continuing in this way we can substiture $c' = -\sum_{i=z+1}^{k'} d_i$ several times to obtain (because $t' - t \leq l$) that

$$1 = \sum_{j=t'-(k'-z)+1}^{t'} c_i''$$

where c_i'' are pseudo-homogeneous of weight i. Observe that $t' - (t' - (k' - z) + 1) = k' - z - 1 < k' - k$. This is a shorter presentation than

$$1 = \sum_{i=k}^{k'} b_i.$$

Hence we obtain a contradiction. $\qquad\square$

Lemma 53. *Let R be a finite dimensional simple F-algebra and let notation be as in Definition 14. Then 1 is a pseudo-homogeneous element of R.*

Proof. Since $a_1, \ldots, a_n$ generate R, then there are pseudo-homogeneous elements b_i such that

$$1 = \sum_{i=k}^{k'} b_i.$$

We can assume that $k' - k$ is the minimal possible. By the previous lemma, each b_i is central. By the Wedderburn-Artin theorem, R is isomorphic to a matrix ring with coefficients from F. Hence, every central element is of the form $\alpha \cdot I$, where I is the identity matrix and α is from F. Then $p_i = \alpha_i \cdot I$, and since $1 = \sum_{i=k}^{k'} b_i$, then some $\alpha_i \neq 0$. Then $\frac{1}{\alpha_i} b_i = I$ is pseudo-homogeneous. $\qquad\square$

Remark 54. Since F is the algebraic closure of a finite field, then for every matrix m there is a natural number $\gamma(M) > 0$ such that $(M^{\gamma(M)})^2 = M^{\gamma(M)}$ is a diagonalizable matrix. Moreover, if all eigenvalues of M are nonzero, then there is a natural number $\beta(M) > 0$ such that $M^{\beta(M)} = I$, the identity matrix.

To prove this, we need to restrict ourselves to diagonal matrices, where this result holds, and to the Jordan blocks. Let $\alpha I + N$ be a Jordan block with α on diagonal; then N is a stricly uppertriangular matrix, and hence nilpotent. Let p be a characteristic of the field F. Then $(\alpha I + N)^{p^n} = \alpha^{p^n} I + N^{p^n}$; therefore $(\alpha I + N)^{p^n} = \alpha^n I = I$ for sufficiently large n, as required. For some related results see [1].

If $R_1, R_2, \ldots R_t$ are algebras, then elements of algebra $R = \oplus_{i=1}^{t} R_i$ will be written as $(q_1, q_2, \ldots, q_t)$, with $q_i \in R_i$.

Theorem 55. *Let R be a finite dimensional F-algebra and let notation be as in Definition 14. Suppose that $R = R_1 \oplus R_2 \oplus \cdots \oplus R_t$ for some simple finite dimensional F-algebras $R_1, R_2, \ldots, R_t$. Then 1 is a pseudo-homogeneous element of R.*

Proof. We proceed by induction on t. If $t = 1$ then the result follows from the previous Lemma. Assume that $t > 1$ and that the result holds for numbers $1, 2, \ldots, t - 1$. Recall that $r_1, \ldots, r_n$ are generators of R (see Definition 14). Each element r_i can be written as $r_i = (r_i', e_i)$ with $r_i' \in R'$ where $R' = R_1 \oplus R_2 \oplus \cdots \oplus R_{t-1}$ and $e_i \in R_t$. We can apply the inductive assumption to the algebra $R' = R_1 \oplus R_2 \oplus \cdots \oplus R_{t-1}$ with generators a_i' for $i = 1, \ldots, n$. Then the identity element of R' is pseudo-homogeneous in R'. It follows that element $(1, e)$ is a pseudo-homogeneous element of R for some $e \in R_t$.

Similarly, by the previous Lemma applied to the ring R_n we obtain that $(f, 1)$ is a pseudo-homogeneous element of R, for some $f \in R'$.

Observe that, since a power of a pseudo-homogeneous element is a pseudo-homogeneous element, then $(1, e)^\gamma$ and $(f, 1)^\beta$ are pseudo-homogeneous elements of the same weight for some $\gamma, \beta > 0$. Let $\alpha_1, \ldots, \alpha_s$ be the eigenvalues of matrix f^β; then for any scalar c the matrix $cI + f^\beta$ has the eigenvalues $c + \alpha_1, \ldots, c + \alpha_s$. The field F is infinite, therefore there are $c, c' \in F'$ such that all the eigenvalues of matrix $M = c(1, e)^\gamma + c'(f, 1)^\beta$ are nonzero. By Remark 54, some power of the matrix M is the identity matrix. As M is a pseudo-homogeneous element of R it proves the result. $\square$

We will now prove the following result for rings which are not necessarily semisimple.

Theorem 56. *Let R be a finite dimensional F-algebra which is not nilpotent and let notation be as in Definition 14. Then there is a pseudo-homogeneous element $e \in R$ such that $e^2 - e \in W$, and for every $r \in R$ we have $r - er \in W$ and $r - re \in W$, where W is the Wedderburn radical of R (the largest nilpotent ideal in R).*

Proof. Consider the algebra $R' = R/W$. Then $r_1' = r_1 + W, r_2' = r_2 + W, \ldots, r_n' = r_n + W$ are generators of R'. We can consider Definition 14 for the algebra R' and its generators $r_1', \ldots, r_n'$ (in place of R and $r_1, \ldots, r_n$). The algebra R' is

semisimple, so by Theorem 55 it has a pseudo-homogeneous identity element $e + W = 1$ for some pseudo-homogeneous $e \in R$. Observe that for every $r \in R$ we have $r + W = 1 \cdot (r + W) = (r + W) \cdot 1$, hence $r - er \in W$ and $r - re \in W$ for every $r \in R$. In particular $e^2 - e \in W$. $\qquad\square$

Theorem 57. *Let R be a finite dimensional F-algebra which is not nilpotent and let notation be as in Definition 14. Then there is $f \in R$ such that $f^2 = f$ and for every $r \in R$ we have $r - fr \in W$ and $r - rf \in W$, where W is the Wedderburn radical of R.*

Notice then that for every $r \in R$ we have $f(fr) = fr$, because $f^2 = f$.

Proof. Let e be as in the previous theorem. Then $e^2 - e \in W$, and by the remark before Lemma 55 there is $m > 0$ such that $f = e^m$ satisfies $f^2 = f$. Notice also that for every $r \in R$ we have $r - re^m \in W$. Indeed, the latter follows because $r - e^m r = (r - er) + (er - e^2 r) + \ldots + (e^{m-1} r - e^m r) \in W$, since $r' - er' \in W$ where $r' = e^i r$, by assumption. Similarly $r - e^m r \in W$. $\qquad\square$

17. Matrices and noncommutative algebras

In this section F denotes the algebraic closure of a finite field. Let N be a matrix whose coefficients are elements of A of the same degree. Assume that for almost all i entries of N^i are in $\langle x \rangle$. We will first show that for some natural number q either $N^q = 0$ or $M = N^q$ satisfies Assumption 3.

Lemma 58. *Let $N = \sum_{i=1}^{\xi'} A_i' a_i'$ where for each i, A_i' is a matrix with coefficients in F and $a_1', a_2', \ldots a_{\xi'}'$ are elements from A which are linearly independent over F and have the same degree. Let H' be the F-algebra generated by matrices A_i'. Let β be a natural number. Then, for some ξ, $N^\beta = \sum_{i=1}^{\xi} A_i a_i$ where each a_i is a product of exactly β elements from the set $\{a_0', a_1', \ldots, a_\xi'\}$. Moreover, $a_0, a_1, \ldots, a_\xi$ are linearly independent over F and $\{A_1, A_2, \ldots, A_\xi\}$ equals the set of matrices which are products of exactly β matrices from the set $\{A_1', \ldots, A_{\xi'}'\}$*

Proof. Observe that distinct products $a_{i_1}' a_{i_2}' \cdots a_{i_\beta}'$ are linearly independent over F, because each of them has the same degree and each of them is a product of elements starting with a or b—the generators of R. Therefore their products are linearly independent over F. Alternatively, it can be proved by induction on β. $\qquad\square$

Lemma 59. *Let notation be as in Lemma 58, and let H be an algebra generated by matrices $A_1, A_2, \ldots, A_\xi$. Let W be the Wedderburn radical of H, and W' the Wedderburn radical of H'. If $r \in H \cap W'$ then $r \in W$.*

Proof. Observe first that the ideal generated by r in H' is nilpotent, as $r \in W'$. Therefore the ideal generated by r in H is nilpotent, and since W is the sum of all nilpotent ideals in H it follows that $r \in W$. $\qquad\square$

Theorem 60. *Let notation be as in Lemmas 58 and 59. Assume that for almost all i entries of N^i are in $\langle x \rangle$. Then for infinitely many β the matrix $M = N^\beta$ satisfies the following: either $M = 0$ or $M = \sum_{i=1}^{\xi} A_i a_i$, where for each i, A_i is a matrix with entries in F and $a_1, a_2, \ldots, a_\xi$ are elements from $A \cap \langle x \rangle$ which are linearly independent over F and have the same degree. Moreover, there is an element $e \in H$ which is a linear combination of matrices $A_1, \ldots, A_\xi$ and such that $e^2 = e$ and $r - er \in W$ and $r - re \in W$ for all $r \in H$, where W is the Wedderburn radical of H.*

Proof. Recall that $N = \sum_{i=1}^{\xi'} A_i' a_i'$. If the algebra H' generated by $A_1', A_2', \ldots, A_{\xi'}'$ is nilpotent then $N^\beta = 0$ for almost all β. It remains to consider the case when N is not a nilpotent matrix.

We will first show that all the assertions of our theorem except the assertion that $a_1, a_2, \ldots, a_\xi$ are elements from $A \cap \langle x \rangle$ hold for some number β. Recall that $A_1', A_2', \ldots A_{\xi'}'$ are generators of algebra H'. We can consider Definition 14 for algebra $R = H'$ and for generators $r_i = A_i'$ for $i = 1, \ldots, n$ where $n = \xi'$. We can then apply Theorem 57 to algebra H' to get that there is $f \in H'$ such that $f^2 = f$ and $f - fr = 0$ and $r - rf = 0$, and f is a pseudo-homogeneous element of weight β, for an appropriate β. By Lemma 58 the set $\{A_1, A_2, \ldots, A_\xi\}$ equals the set of elements which are products of exactly β elements from the set $\{A_1', \ldots, A_{\xi'}'\}$. Therefore matrices $A_1, \ldots, A_\xi$ span the linear space of pseudo-homogeneous elements of weight β in H', hence f is a linear combination of $A_1, \ldots, A_\xi$; hence $f \in H$. Let W' be the Wedderburn radical of H'. By Lemma 59, $W' \cap H \subseteq W$, therefore $r - rf \in W$ and $r - fr \in W$ for all $r \in H$. Therefore our result holds for $e = f$ and $M = N^\beta$ (by Lemma 58). We have shown that our result holds for some β.

To show that there are infinitely many elements β with this property, observe that for any natural number $k > 0$ we can apply the same reasoning to $\beta_k = k \cdot \beta$ and $e_k = e^k$ instead of β and e. In this way we will obtain infinitely many $\beta \in \{\beta_1, \beta_2, \beta_3, \ldots\}$ satisfying the thesis.

Notice that $a_1, a_2, \ldots, a_\xi$ are elements from $A \cap \langle x \rangle$ for sufficiently large β, this finishes the proof. $\qquad\square$

Corollary 61. *Let notation be as in Theorem 60. Then we can assume that $A_1 = e$ (by using linear combinations of elements a_i instead of elements a_i).*

Corollary 62. *Let A, A', R be as in Theorem 6, and $\langle x \rangle$ denote the ideal generated by x in A'. Let N be a matrix whose coefficients are elements of A of the same degree. Assume that for almost all i entries of N^i are in $\langle x \rangle$, then for some natural number q either $N^q = 0$ or $M = N^q$ satisfies Assumption 3.*

Proof. It follows from Theorem 60 and from Corollary 61. $\qquad\square$

Theorem 63. *Assumption 1 holds for F-algebra A.*

Proof. Let N be a matrix with entries in $A^*(j)$ for some j, and such that for almost all i matrix N^i has all entries in $\langle x \rangle$. By Corollary 62 either N is a nilpotent matrix or for some q matrix $M = N^q$ satisfies Assumption 3. By Theorem 50 applied to $M = N^q$, there are infinitely many n such that the dimension of the space $R \cap S(L(M^n))$ doesn't exceed $\sqrt{n}$. Observe that $S(L(M^n)) = S(L(N^{q \cdot n}))$ (because operations S and L depend only upon the matrix, not on the way it is presented). Therefore $R \cap S(L(N^{q \cdot n}))$ has dimension $\leq \sqrt{n} \leq \sqrt{qn}$. This holds for infinitely many n.

$\qquad\square$

Proof of Theorem 1. Recall that F is the algebraic closure of a finite field, and hence F is countable and infinite. By Theorem 63, Assumption 1 holds for F-algebra A. Then, by Theorem 32 there is an F-algebra Z and a derivation D on Z such that the differential polynomial ring $Z[y; D]$ is Jacobson radical but Z is not nil.

Assume now that K is a subfield of F. If R is an F-algebra then R is also a K-algebra. Therefore, Theorem 1 also holds for an arbitrary subfield of the algebraic closure of any finite field.

References

[1] Marek Aleksiejczyk, Alicja Smoktunowicz, *On properties of quadratic matrices*, Mathematica Pannonica (11) 2 (2000), 239-248.

[2] S. A. Amitsur, *Radicals of polynomial rings*, Canad. J. Math. 8 (1956), 355–361.

[3] Jason Bell, Blake Madill, and Forte Shinko, *Differential polynomial rings over rings satisfying a polynomial identity*, J. Algebra, Vol 423, 2015, 28–36.

[4] Jefrey Bergen, S. Montgomery, and D. S. Passman, *Radicals of crossed products of enveloping algebras*, Israel J. Math. 59 (1987), no. 2, 167–184.

[5] S. S. Bedi and J. Ram, *Jacobson radical of skew polynomial rings and skew group rings*, Israel J. Math., 35 (1980), 327-338.

[6] Vesselin Drensky and Edward Formanek, Polynomial identity rings, Advanced Courses in Mathematics. CRM Barcelona, Birkhauser Verlag, Basel, 2004.

[7] Carl Faith, Rings and Things and a fine array of Twentieth Century Associative Algebras, second edition, AMS Mathematical Surveys and Monographs, 2004.

[8] Miguel Ferrero, Kazuo Kishimoto, and Kaoru Motose, *On radicals of skew polynomial rings of derivation type*, J. London Math. Soc. (2) 28 (1983), no. 1, 8–16.

[9] J. Bergen and P. Grzeszczuk, *Jacobson radical of ring extensions*, Journal of Pure and Applied Algebra, 216 (2012) 2601–2607.

[10] C.Y. Hong, N.K. Kim, Y. Lee, and P. Nielsen, *Amitsur's property for skew polynomials of derivation type*, preprint.

[11] C. R. Jordan, Jordan, D. A. Jordan, *A note on semiprimitivity of Ore extensions*, Comm. Algebra 4(7), 647–656.

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

[13] V. K. Kharchenko, Automorphisms and derivations of associative rings, Kluwer Academic Publisher, 1991.

[14] J. Krempa, *Logical connections between some open problems concerning nil rings*, Fundamenta Mathematicae 76 (1972), no. 2, 121–130.

[15] T. Y. Lam, A First Course in Noncommutative Rings, Graduate Texts in Mathematics, Springer-Verlag, 2001.

[16] Andre Leroy, Jerzy Matczuk, *The extended centroid and X-inner automorphisms of Ore extensions*, Journal of Algebra, Volume 145, Issue 1, January 1992, Pages 143–177.

[17] Blake Madill, *On the Jacobson radical of skew extensions of rings satisfying a polynomial identity*, to appear in Comm. Algebra.

[18] Alireza Nasr-Isfahani, *Jacobson Radicals of Skew Polynomial Rings of Derivation Type*, Canad. Math. Bull. 57 (2014), no. 3, 609–613.

[19] Pace P. Nielsen and Micha Ziembowski, *Derivations and bounded nilpotence index*, Int. J. Algebra Comput. 25, 433 (2015).

[20] Jan Okniński, Semigroups of Matrices, World Scientific Publishing Co Pte Ltd ,1 Sept. 1998.

[21] E.R. Puczyłowski, A.Smoktunowicz, *On maximal ideals and the Brown McCoy radical of polynomial rings*, Communications in Algebra, 26 (8), 2473–2482.

[22] V. M. Petrogradsky, *Examples of self iterating Lie algebras*, J. Algebra 302 (2006), no. 2, 881–886.

[23] V. M. Petrogradsky,I.P. Shestakov, E. Zelmanov, *Nil graded self similar algebras*, Groups Geom. Dyn. 4 (2010), no. 4, 873–900.

[24] Louis Halle Rowen, Polynomial identities in ring theory, Pure and Applied Mathematics, vol. 84, Academic Press, Inc., Harcourt Brace Jovanovich, Publishers, New York-London, 1980.

[25] Louis Halle Rowen, Ring Theory, Student Edition, 1991 Academic Press Inc.

[26] I. P. Shestakov, E. Zelmanov, *Some examples of Lie algebras*, J. Eur. Math. Soc. (JEMS), **10** (2008), no. 2, 391–398.

[27] Agata Smoktunowicz, *Polynomial rings over nil rings need not be nil*, Journal of Algebra 233, 2000, 427–436.

[28] Agata Smoktunowicz, *On primitive ideals in polynomial rings over nil rings*, Algebras and Representation Theory (2005) 8, 69–73.

[29] Agata Smoktunowicz, *The Jacobson radical of rings with nilpotent homogeneous elements*, Bull. London Math. Soc. 40 (2008), 917–928.

[30] Agata Smoktunowicz, Michal Ziembowski, *Differential polynomial rings over locally nilpotent rings need not be Jacobson radical*, Journal of Algebra 412 (2014), 207–217.

[31] Yuan-Tsung Tsai, Tsu-Yang Wu, and Chen-Lian Chuang, *Jacobson radicals of Ore extensions of derivation type*, Comm. Algebra 35 (2007), no. 3, 975–982.

Maxwell Institute for Mathematical Sciences, School of Mathematics,
University of Edinburgh,
JCM Building, Kings Buildings, Mayfield Road Edinburgh EH9 3JZ, Scotland, UK,
E-mail: A.Smoktunowicz@ed.ac.uk