JOURNAL OF ALGEBRA **186,** 781–792 (1996)
ARTICLE NO. 0394

Nil Polynomials of Prime Rings

Chi-Tsuen Yeh and Chen-Lian Chuang

Department of Mathematics, National Taiwan University, Taipei, Taiwan, Republic of China

Assume that R is a prime ring without nonzero nil one-sided ideals and that $f(x_1, \ldots, x_d)$ is a polynomial in the noncommuting variables $x_1, \ldots, x_d$ and with the coefficients in the extended centroid C of R. If for all $r_1, \ldots, r_d \in R$, there exists an integer $n = n(r_1, \ldots, r_d) \geq 1$, depending on $r_1, \ldots, r_d \in R$, such that $f(r_1, \ldots, r_d)^n = 0$, then either $f(r_1, \ldots, r_d) = 0$ for all $r_1, \ldots, r_d \in R$ or R is a finite matrix ring over a finite field.

(I) RESULT

Let R be an associative ring. An element $r \in R$ is said to be *nilpotent* if $r^n = 0$ for some integer $n \geq 1$. A subset S of R is called *nil* if all $r \in S$ are nilpotent. It is easy to see that R has no nil right ideals if and only if R has no nil left ideals. Nil right ideals or nil left ideals together are generally called nil one-sided ideals.

Assume that R is a prime ring with the extended centroid C. The ring RC is called the central closure of R. Let $f = f(x_1, \ldots, x_d)$ be a polynomial in the noncommuting variables $x_1, \ldots, x_d$ and with the coefficients in the extended centroid C. The polynomial f is called an *identity* of R, if $f(r_1, \ldots, r_d) = 0$ for all $r_1, \ldots, r_d \in R$. The polynomial f is said to be *nil* on R if for any $r_1, \ldots, r_d \in R$, $f(r_1, \ldots, r_d)$ is nilpotent, that is, $f(r_1, \ldots, r_d)^n = 0$ for some integer $n = n(r_1, \ldots, r_d) \geq 1$ depending on $r_1, \ldots, r_d$. Our aim is to investigate nil polynomials on a prime ring R without nonzero nil one-sided ideals: Polynomial identities are nil on R in a trivial way. One may thus wonder whether the converse holds. By the result of [2], this is false when R is a finite matrix ring over a finite field.

0021-8693/96 $18.00

We hence exclude these somewhat trivial exceptions. Here are some known partial results: Herstein first proved the case for $f = [x, y] \overset{\text{def.}}{=} xy - yx$ on arbitrary prime rings. The assertion for any arbitrary f on (semi)primitive rings only was proved in a joint work of Herstein, *et al.* [4]. The assertion for multilinear f on arbitrary prime rings was proved by Felzenszwalb and Giambruno [5, 6]. The special case for $f = [x, y]_k$ on any prime rings was proved in [3]. (Here $[x, y]_k$ is defined inductively by $[x, y]_1 \overset{\text{def.}}{=} [x, y]$ and $[x, y]_k \overset{\text{def.}}{=} [[x, y]_{k-1}, y]$ for $k > 1$.) This problem is solved in its full generality as follows:

THEOREM. *Assume that R is a prime ring without nonzero nil one-sided ideals. If a polynomial $f(x_1, \ldots, x_d)$, in the noncommuting variables $x_1, \ldots, x_d$ and with the coefficients in the extended centroid C of R, is nil on R, then either $f(x_1, \ldots, x_d)$ is a polynomial identity of R or R is a finite matrix ring over a finite field.*

The theorem can be used to improve results on this line by removing the multilinearity assumption. Let us mention two of them here: Let R be a prime ring without nonzero nil one-sided ideals and let $f(x_1, \ldots, x_d)$ be a polynomial satisfying the following two conditions: (A) If the characteristic of R is of the finite characteristic $p \geq 2$, then $f(x_1, \ldots, x_d)$ is *not* an identity for $p \times p$ matrices over an infinite field of the characteristic p. (B) The polynomial $f(x_1, \ldots, x_d)$ is homogeneous in some nonempty subset of its variables.

(I) Let δ be a nonzero derivation of R. If for every $r_1, \ldots, r_d \in R$, there exists an integer $n = n(r_1, \ldots, r_d) \geq 1$, depending on $r_1, \ldots, r_d$, such that

$$\delta\big(f(r_1, \ldots, r_d)^n\big) = 0,$$

then the polynomial $f(x_1, \ldots, x_d)$ is power central valued on R and the ring R satisfies the standard polynomial identity of the degree $l + 2$, where l is the degree of $f(x_1, \ldots, x_d)$.

(II) If for every $r_1, \ldots, r_d, s_1, \ldots, s_d \in R$, there exist two integers $n, m \geq 1$, both depending on $r_1, \ldots, r_d, s_1, \ldots, s_d$ altogether, such that

$$f(r_1, \ldots, r_d)^n f(s_1, \ldots, s_d)^m = f(s_1, \ldots, s_d)^m f(r_1, \ldots, r_d)^n,$$

then the polynomial $f(x_1, \ldots, x_d)$ is a power central valued on R and the ring R satisfies the standard polynomial identity of the degree $l + 2$, where l is the degree of $f(x_1, \ldots, x_d)$.

The result (I) for multilinear $f(x_1, \ldots, x_d)$ is proved in [9], which generalizes [5], where only inner derivation δ is considered. The result (II) for multilinear $f(x_1, \ldots, x_d)$ is proved in [1] with the restriction that the characteristic of R is not 2. The hypotheses (A) and (B) on the polynomial $f(x_1, \ldots, x_d)$ are inherited from the fundamental work [4], where the structure of power central polynomials on division rings is determined under these two hypotheses. The general method for attacking problems (I) and (II) is a reduction to nil polynomials on prime rings and to power central polynomials on division rings. Hence any progress on the knowledge of nil polynomials on prime rings and power central polynomials on division rings will automatically improve the known results in the form (I) and (II) above. Our theorem is one step toward this goal. The proofs of (I) and (II) as stated above are pretty much the same as those in [9, 1] and are omitted here for brevity.

(II) PROOF

We first recall three simple facts, whose proofs are also included here for the sake of completeness:

FACT 1. *Assume that R is a prime ring without nil-onesided ideals. Let ρ be a one-sided ideal of R and let $l(\rho) \overset{\text{def.}}{=} \{x \in R : x\rho = 0\}$ be the left annihilator of ρ. Then the quotient ring $\bar{\rho} \overset{\text{def.}}{=} \rho/\rho \cap l(\rho)$ is also a prime ring without nil one-sided ideals. Furthermore, each element of the extended centroid of R can be naturally interpreted as an element of the extended centroid of $\bar{\rho}$.*

Proof. For $t \in \rho$, let $\bar{t}$ denote the element $t + \rho \cap l(\rho)$ in the quotient ring $\bar{\rho} \overset{\text{def.}}{=} \rho/\rho \cap l(\rho)$. For a subset T of ρ, let $\overline{T} \overset{\text{def.}}{=} \{\bar{t} : t \in T\}$. For $a, b \in \rho$, if $\bar{a}\bar{\rho}\bar{b} = 0$ or, equivalently, $a\rho b\rho = 0$, then, by the primeness of R, either $a\rho = 0$ or $b\rho = 0$, that is, either $\bar{a} = 0$ or $\bar{b} = 0$. This shows the primeness of $\bar{\rho}$. Any right ideal of $\bar{\rho}$ is of the form $\overline{T}$, where T is a right ideal of ρ satisfying $T \supseteq \rho \cap l(\rho)$. Conversely, for any right ideal T of ρ satisfying $T \supseteq \rho \cap l(\rho)$, $\overline{T}$ is a right ideal of $\bar{\rho}$. Let T be a right ideal of ρ satisfying $T \supseteq \rho \cap l(\rho)$ such that $\overline{T}$ is nil. For any $t \in T$, $\bar{t}^n = 0$ for some n, that is, $t^n \in l(\rho)$ and hence $t^{n+1} = 0$. So T is nil. Since $T\rho \subseteq T$, $T\rho$ is nil. But $T\rho$ is a right ideal of R. So $T\rho = 0$ and hence $\overline{T} = 0$. This shows that $\bar{\rho}$ has no nonzero nil one-sided ideals. Finally, let α be an element of the extended centroid of R and let $0 \neq I$ be a two-sided ideal of R such that $\alpha I \subseteq R$. The map $\bar{\alpha} : \bar{t} \in \overline{\rho I} \mapsto \overline{\alpha t} \in \bar{\rho}$ for $t \in \rho I$ is well defined and gives an element of the extended centroid of $\bar{\rho}$. Hence α, when it acts on $\bar{\rho}$, is interpreted as $\bar{\alpha}$.

FACT 2. *Assume that R is a prime ring satisfying a nontrivial generalized polynomial identity and that C is the extended centroid of R. Then for any* *idempotent e in the socle of RC, $R \cap eRCe$ is a prime ring and $eRCe = (R \cap eRCe)C$.*

Proof. First, we show the primeness of $R \cap eRCe$: Pick a two-sided ideal $I \neq 0$ of R such that $eI, Ie \subseteq R$. Then $eI^2e \subseteq R \cap eRCe$. For $a, b \in R \cap eRCe$, if $a(R \cap eRCe)b = 0$, then $0 = a(eI^2e)b = aI^2b$ and hence either $a = 0$ or $b = 0$. Next, we show that $eRCe$ is the Martindale quotient ring of $R \cap eRCe$: Let $a \in eRCe$ be arbitrary and let $0 \neq J$ be a two-sided ideal of R such that $eJ, Je, aJ, Ja \subseteq R$. We verify that $0 \neq eJ^3e$ is a two-sided ideal of $R \cap eRCe$: For any $x \in R \cap eRCe$, we have $xeJ^3e = exJ^3e \subseteq eRJ^3e \subseteq eJ^3e$ and similarly $eJ^3ex \subseteq eJ^3e$. Observe that $aeJ^3e = eaJ^3e \subseteq eRJ^2e \subseteq eJ^2e \subseteq R \cap eRCe$ and similarly $eJ^3ea \subseteq R \cap eRCe$. Hence $eRCe$ is "a" two-sided Martindale quotient ring of $R \cap eRCe$, as asserted. Since R satisfies a nontrivial generalized polynomial identity, $eRCe$ is a PI-ring and hence so is $R \cap eRCe$. For a prime PI-ring, its central quotient ring and its Martindale quotient ring coincide. But the center of $eRCe$ is obviously eC. So we have $eRCe \subseteq (R \cap eRCe) \cdot eC = (R \cap eRCe)C$. The other inclusion $eRCe \supseteq (R \cap eRCe)C$ is obvious. So we have the equality $eRCe = (R \cap eRCe)C$, as asserted.

An element $a \in R$ is of the nilpotency index n if $a^n = 0$ and $a^{n-1} \neq 0$. If there exists an integer $m \geq 1$ such that any nilpotent element of R has the nilpotency index $\leq m$, then the ring R is said to be of bounded nilpotency index and the least such integer m is called the nilpotency index of R. If there does *not* exist such an integer $m \geq 1$, then R is said to be of unbounded nilpotency index.

FACT 3. *If R is a ring of unbounded nilpotency index, then for any integer $n \geq 2$, there exists $a \in R$ with the nilpotency index n.*

Proof. Let $n \geq 2$ be given. Since R is of unbounded nilpotency index, there exists $b \in R$ of the nilpotency index $s > n^2$. Set

$$a \overset{\text{def.}}{=} b^{[s/n]+1},$$

where $[\cdot]$ denotes the greatest integer function. Then

$$\begin{aligned} n([s/n] + 1) > n(s/n) = s \geq n[s/n] &= (n-1)[s/n] + [s/n] \\ &> (n-1)([s/n] + 1). \end{aligned}$$

So we have $a^n = 0$ but $a^{n-1} \neq 0$. ∎

Fix arbitrarily finitely many *distinct* noncommuting variables $x, z_1, \ldots, z_d$. We will consider polynomials in these variables and with their coefficients in the extended centroid C of R. A typical monomial assumes the form

$$\mu = \mu(x, z_1, \ldots, z_d) \overset{\text{def.}}{=} \alpha x^{t_0} z_{i_1} x^{t_1} z_{i_2} x^{t_2} \cdots z_{i_n} x^{t_n}, \tag{1}$$

where $0 \neq \alpha \in C$, where $n \geq 0$, where $i_1, \ldots, i_n \in \{1, \ldots, d\}$ are *not* necessarily distinct, and where $t_0, t_1, \ldots, t_n \geq 0$ are integers. If $n = 0$, the monomial μ in (1) above is of the form $\mu \overset{\text{def.}}{=} \alpha x^{t_0}$. The *average* x-degree of the monomial μ in (1) above is defined to be $\sum_{i=0}^{n} t_i / n$ for $n > 0$ and ∞ for $n = 0$. The average x-degree of a polynomial $f = f(x, z_1, \ldots, z_d)$ in general is defined to be the *minimum* of the average x-degrees of monomials involved nontrivially in f. (Note that the average x-degree of a polynomial is, in general, either a rational ≥ 0 or ∞, *not* necessarily an integer. The average x-degree of a polynomial is ∞ if and only if it involves the variable x only.) By a *cyclic* monomial of the *initial degree* $m \geq 0$, we mean a monomial of the form

$$\mu = \mu(x, z_1, \ldots, z_d) \overset{\text{def.}}{=} \alpha x^m z_{i_1} x^l z_{i_2} x^l \cdots z_{i_n} x^{l-m}, \tag{2}$$

where $0 \neq \alpha \in C$, where $n \geq 1$, where $i_1, \ldots, i_n \in \{1, \ldots, d\}$ are not necessarily distinct, and where l, m are integers such that $l \geq m \geq 0$. The average x-degree of the cyclic monomial μ displayed in (2) above is obviously l. For convenience, the monomial of the form $\mu \overset{\text{def.}}{=} \alpha x^t$ is also said to be cyclic of the initial degree t. A cyclic monomial involved nontrivially in a given polynomial $f = f(x, z_1, \ldots, z_d)$ is said to be *leading* if its average x-degree is equal to the average x-degree of f, that is, if it is of the lowest possible average x-degree. For a given polynomial $f = f(x, z_1, \ldots, z_d)$, we define, for each integer $m \geq 0$, $f^{(m)} = f^{(m)}(x, z_1, \ldots, z_d)$ to be the sum of leading cyclic monomials of f with the initial degree m. (Hence if m is $>$ the average x-degree of f, then $f^{(m)} = 0$ by the definition.)

The following contains the main computation of our argument:

LEMMA 1. *If $f(x, z_1, \ldots, z_d)$ is a polynomial of the average x-degree l, where l is an integer, then the equality*

$$a^{l-m}\big(f(a, z_1, \ldots, z_d)\big)^s a^m = \big(f^{(m)}(1, a^l z_1, \ldots, a^l z_d)\big)^s a^l$$

holds for any integers $m, s \geq 0$ with $m \leq l$ and for any $a \in R$ of the nilpotency index $l + 1$.

Proof. Let $f_0 = f_0(x) = f_0(x, z_1, \ldots, z_d)$ be the sum of the monomials of f which involve only the variable x. If a term $\mu(x, z_1, \ldots, z_d)$ of $f(x, z_1, \ldots, z_d)$ in the form (1) is such that $t_n > l - m$ or such that $t_i > l$

for some $i = 1, \ldots, n-1$, then $\mu(a, z_1, \ldots, z_d)a^m = 0$. We hence let S be the set of all terms μ of f, in the form (1), with $t_n \le l - m$ and $t_i \le l$ for all $i = 1, \ldots, n-1$. Then we have

$$f(a, z_1, \ldots, z_d)a^m = \left(\sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) + f_0(a) \right) a^m.$$

But for a typical term $\mu \in S$ of the form (1), since the average x-degree of μ is $\ge l$, we have $t_0 + t_n \ge l$ and hence also $t_0 \ge m$. We may thus write

$$\sum_{\mu \in S} \mu(x, z_1, \ldots, z_d) = x^m g(x, z_1, \ldots, z_d),$$

where $g(x, z_1, \ldots, z_d)$ is a polynomial of $x, z_1, \ldots, z_d$. We hence have

$$\begin{aligned} f(a, z_1, \ldots, z_d)a^m &= \left(\sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) + f_0(a) \right) a^m \\ &= (a^m g(a, z_1, \ldots, z_d) + f_0(a))a^m \\ &= a^m (g(a, z_1, \ldots, z_d)a^m + f_0(a)). \end{aligned}$$

Using this equality, we have for any integer $s > 0$,

$$\begin{aligned} f(a, z_1, \ldots, z_d)^s a^m &= f(a, z_1, \ldots, z_d)^{s-1} f(a, z_1, \ldots, z_d)a^m \\ &= f(a, z_1, \ldots, z_d)^{s-1} a^m (g(a, z_1, \ldots, z_d)a^m + f_0(a)) \\ &= f(a, z_1, \ldots, z_d)^{s-2} a^m (g(a, z_1, \ldots, z_d)a^m + f_0(a))^2 \\ &= \cdots \\ &= a^m (g(a, z_1, \ldots, z_d)a^m + f_0(a))^s \\ &= (a^m g(a, z_1, \ldots, z_d) + f_0(a)) \\ &\quad \times a^m (g(a, z_1, \ldots, z_d)a^m + f_0(a))^{s-1} \\ &= (a^m g(a, z_1, \ldots, z_d) + f_0(a))^2 \\ &\quad \times a^m (g(a, z_1, \ldots, z_d)a^m + f_0(a))^{s-2} \\ &= \cdots \\ &= (a^m g(a, z_1, \ldots, z_d) + f_0(a))^s a^m \\ &= \left(\sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) + f_0(a) \right)^s a^m. \end{aligned}$$

We now consider the product

$$a^{l-m}f(a, z_1, \ldots, z_d)^s a^m = a^{l-m}\left(\sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) + f_0(a)\right)^s a^m.$$

If $\mu(x, z_1, \ldots, z_d) \in S$, in the form (1), satisfies $t_0 > m$, then $a^{l-m}\mu(a, z_1, \ldots, z_d) = 0$. We hence let T be the set consisting of all terms $\mu \in S$, in the form (1), with $t_0 \leq m$. Then we have

$$a^{l-m} \sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) = a^{l-m} \sum_{\mu \in T} \mu(a, z_1, \ldots, z_d).$$

A typical term $\mu \in T$ in the form (1) satisfies $t_0 \leq m$, $t_n \leq l - m$, and $t_i \leq l$ for all $i = 1, \ldots, n-1$. Since the average x-degree of $\mu \in T$ is $\geq l$, we must have $t_0 = m$, $t_n = l - m$, and $t_i = l$ for all $i = 1, \ldots, n-1$. That is, each $\mu \in T$ must be a leading cyclic monomial with the initial degree m. Conversely, T obviously consists of all such leading cyclic monomials with the initial degree m. Hence,

$$f^{(m)}(x, z_1, \ldots, z_d) = \sum_{\mu \in T} \mu(x, z_1, \ldots, z_d).$$

Since each leading cyclic monomial of the initial degree m starts with x^m and ends with x^{l-m}, we may write

$$f^{(m)}(x, z_1, \ldots, z_d) = x^m h(x, z_1, \ldots, z_d) x^{l-m},$$

where $h(x, z_1, \ldots, z_d)$ is polynomial in $x, z_1, \ldots, z_d$. We hence have

$$\begin{aligned} a^{l-m} \sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) &= a^{l-m} \sum_{\mu \in T} \mu(a, z_1, \ldots, z_d) \\ &= a^{l-m} f^{(m)}(a, z_1, \ldots, z_d) \\ &= a^l h(a, z_1, \ldots, z_d) a^{l-m}. \end{aligned}$$

With this equality, we compute:

$$\begin{aligned} &a^{l-m}f(a, z_1, \ldots, z_d)^s a^m \\ &\quad = a^{l-m}\left(\sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) + f_0(a)\right) \\ &\qquad \times \left(\sum_{\mu \in S} \mu(a, z_1, \ldots, z_d) + f_0(a)\right)^{s-1} a^m \\ &\quad = \left(a^l h(a, z_1, \ldots, z_d) + f_0(a)\right) \end{aligned}$$

$$\times a^{l-m}\Bigg(\sum_{\mu\in S}\mu(a,z_1,\dots,z_d)+f_0(a)\Bigg)^{s-1}a^m$$

$$= \big(a^l h(a,z_1,\dots,z_d)+f_0(a)\big)^2$$

$$\times a^{l-m}\Bigg(\sum_{\mu\in S}\mu(a,z_1,\dots,z_d)+f_0(a)\Bigg)^{s-2}a^m$$

$$= \cdots$$

$$= \big(a^l h(a,z_1,\dots,z_d)+f_0(a)\big)^s a^l.$$

Since $a^{l+1}=0$ and since $f_0(a)$ is a C-linear combination of positive powers of a, we have $f_0(a)a^l=0$. Using this, we continue our computation:

$$\begin{aligned}
&\big(a^l h(a,z_1,\dots,z_d)+f_0(a)\big)^s a^l\\
&\quad= \big(a^l h(a,z_1,\dots,z_d)+f_0(a)\big)^{s-1}\big(a^l h(a,z_1,\dots,z_d)+f_0(a)\big)a^l\\
&\quad= \big(a^l h(a,z_1,\dots,z_d)+f_0(a)\big)^{s-1}a^l h(a,z_1,\dots,z_d)a^l\\
&\quad= \big(a^l h(a,z_1,\dots,z_d)+f_0(a)\big)^{s-2}a^l\big(h(a,z_1,\dots,z_d)a^l\big)^2\\
&\quad= \cdots\\
&\quad= a^l\big(h(a,z_1,\dots,z_d)a^l\big)^s\\
&\quad= \big(a^l h(a,z_1,\dots,z_d)\big)^s a^l.
\end{aligned}$$

Finally, by the definition of the polynomial $h(x,z_1,\dots,z_d)$, we observe

$$a^l h(a,z_1,\dots,z_d)=f^{(m)}\big(1,a^l z_1,\dots,a^l z_d\big).$$

Combining all these computations, we have

$$a^{l-m}\big(f(a,z_1,\dots,z_d)\big)^s a^m=\big(f^{(m)}\big(1,a^l z_1,\dots,a^l z_d\big)\big)^s a^l,$$

as asserted.

Since the average x-degree of a cyclic monomial must be an integer, only those polynomials with integral average x-degrees can possibly possess leading cyclic monomials. Obviously, *not* every polynomial $f(x,z_1,\dots,z_d)$ with the integral average x-degree involves nontrivially leading cyclic monomials. However, for any given polynomial, there does exist a proper substitution that results in a polynomial involving nontrivially leading cyclic monomials. For notational simplicity, we restrict ourselves to polynomials in *two* distinct variables only: A typical monomial in the two variables x, y assumes the form:

$$\mu = \mu(x, y) \stackrel{\text{def.}}{=} \alpha x^{t_0} y x^{t_1} y x^{t_2} \cdots y x^{t_n}, \tag{3}$$

where $0 \neq \alpha \in C$, where $n \geq 0$ and where $t_0, t_1, \dots, t_n \geq 0$ are integers. Let $z_1, \dots, z_n$ be a set of distinct new variables. We consider the substitution of x by x^b and y by $\sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i}$, where $b, \rho, \rho_i \geq 0$ are integers with $\rho \geq \rho_i$. Assume that the average x-degree of $\mu(x, y)$, given in (3), is l, that is, $l \stackrel{\text{def.}}{=} \sum_{i=0}^{n} t_n / n$. Then the average x-degree of $\mu(x^b, y)$ is obviously equal to bl. It is also obvious that *all* terms in the expansion of $\mu(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i})$ have the average x-degree $bl + \rho$. Hence, if $\mu(x, y)$ is a term of a polynomial $f(x, y)$ with the lowest possible average x-degree, then all terms in the expansion of $\mu(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i})$ still possess the lowest possible average x-degree in $f(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i})$.

LEMMA 2. *Let $f = f(x, y)$ be a polynomial in the two distinct variables x, y. Assume that the monomial $\mu = \mu(x, y)$, in the form of* (3), *is a term of f with the lowest possible average x-degree. Then there exist integers $b, \rho, \rho_i \geq 0$, with $\rho \geq \rho_i$, such that, in the expansion of $\mu(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i})$, the polynomial expression.*

$$\tilde{\mu} = \tilde{\mu}(x, z_1, \dots, z_n) \stackrel{\text{def.}}{=} \alpha x^{bt_0} (x^{\rho_1} z_1 x^{\rho - \rho_1}) x^{bt_1} (x^{\rho_2} z_2 x^{\rho - \rho_2}) x^{bt_2} \cdots (x^{\rho_n} z_n x^{\rho - \rho_n}) x^{bt_n} \tag{4}$$

is a leading cyclic monomial of the polynomial $f(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i})$.

Proof. Assume that the average x-degree of $f(x, y)$ is $l \geq 0$ and that the monomial $\mu(x, y)$, given in the form of (3), is a term of $f(x, y)$ also with the average x-degree l. We first choose $b \geq 1$ so that bl is an integer. Then both $f(x^b, y)$ and $\mu(x^b, y)$ are of the average x-degree bl. Also, the expression (4), being a term of the expansion of $\mu(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i})$, is of the average x-degree $bl + \rho$. In order to make the expression (4) cyclic, the following conditions must be satisfied:

$$\begin{aligned}
(\rho - \rho_1) + bt_1 + \rho_2 &= bl + \rho, \\
(\rho - \rho_2) + bt_2 + \rho_3 &= bl + \rho, \\
&\cdots, \\
(\rho - \rho_{n-1}) + bt_{n-1} + \rho_n &= bl + \rho, \\
(\rho - \rho_n) + b(t_n + t_0) + \rho_1 &= bl + \rho.
\end{aligned}$$

These are equivalent to the following:

$$\begin{aligned} \rho_2 - \rho_1 &= bl - bt_1, \\ \rho_3 - \rho_2 &= bl - bt_2, \\ &\cdots, \\ \rho_n - \rho_{n-1} &= bl - bt_{n-1}, \\ \rho_1 - \rho_n &= bl - b(t_n + t_0). \end{aligned}$$

These n-equations are dependent: The last equation is the sum of the first $n - 1$ equations since l, the average x-degree of $\mu(x, y)$, is defined to be $\sum_{i=0}^{n} t_i/n$. We can solve $\rho_2, \dots, \rho_n$ in terms of ρ_1:

$$\begin{aligned} \rho_2 &= \rho_1 + bl - bt_1, \\ \rho_3 &= \rho_2 + bl - bt_2 = \rho_1 + 2bl - b(t_1 + t_2), \\ &\cdots, \\ \rho_n &= \rho_{n-1} + bl - bt_{n-1} = \rho_1 + (n-1)bl - b(t_1 + \cdots + t_{n-1}). \end{aligned}$$

We can thus choose the positive integer ρ_1 so large that all $\rho_2, \dots, \rho_n \geq 0$, and then we let ρ be the maximum of ρ_i, $i = 1, \dots, n$, to insure that each $\rho - \rho_i \geq 0$. Finally, we observe that among all terms of $f(x, y)$, only the monomial $\mu(x, y)$ can give rise to the expression (4). Hence the expression (4) does occur nontrivially in $f(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i})$, as asserted.

As we consider only polynomials in the two variables x, y, we need a substitution which converts polynomials in variables other than x, y to polynomials in x, y only:

LEMMA 3. *If $f = f(x, y, z_1, \dots, z_d)$ is a nontrivial polynomial in the distinct variables $x, y, z_1, \dots, z_d$, then there exist integers $m_1, \dots, m_n \geq 1$ such that the polynomial*

$$f(x, y, x^{m_1} y, \dots, x^{m_d} y),$$

in the two variables x, y only, is nontrivial.

Proof. If m_1 is an integer strictly larger than the x-degree of f, then the polynomial $f(x, y, x^{m_1} y, z_2, \dots, z_d)$ remains nontrivial. (For, by changing all occurrence of $x^{m_1} y$ in $f(x, y, x^{m_1} y, z_2, \dots, z_d)$ back to z_1, we can get back $f(x, y, z_1, \dots, z_d)$.) By repeating this process for $z_2, \dots, z_d$ consecutively, the claim is proved.

With these lemmas in hand, we are now ready to give:

Proof of Theorem. We first show that if R satisfies a nontrivial generalized polynomial identity, then the assertion of the theorem holds: By the result of [8], RC is then a primitive ring with nonzero socle. First, assume that the extended centroid C is finite. We can then pick a nonzero two-sided ideal I of R such that $\alpha I \subseteq R$ for *each* $\alpha \in C$. But IC is a nonzero two-sided ideal of RC and hence must contain the socle. Since I is so chosen that $IC \subseteq R$, the ring R itself must also contain the socle and hence must be also primitive. The assertion now follows from Theorem 1.7 of [4]. Second, assume that C is infinite. Let $e \in RC$ be an idempotent of the finite rank k. Then f^k is a polynomial identity of $R \cap eRCe$. But the ring $R \cap eRCe$ and its central quotient ring $eRCe$ (by Fact 2) satisfy the same polynomial identities by Theorem 2 on page 52 of [7]. So f^k is also an identity of $eRCe$. By Theorem 2 on page 90 of [7], the polynomial f itself also vanishes identically on $eRCe$. Since any finitely many elements of the socle of RC must fall in some $eRCe$ for a suitable idempotent $e \in RC$ of the large enough finite rank, f vanishes on the socle of RC. Since the socle of RC is a dense subring of RC, the identity f vanishes on RC and hence on R as asserted.

It thus suffices to show that R satisfies a nontrivial generalized polynomial identity. By Lemma 3, R also possesses a nil polynomial in x, y only, say $g(x, y)$. We proceed by the induction on the y-degree of $g(x, y)$ to show that R satisfies a nontrivial generalized polynomial identity: As the induction basis, we first assume that the y-degree of $g(x, y)$ is 0. That is, $g(x, y)$ is a polynomial in x only, say,

$$g(x, y) = g(x) \overset{\text{def.}}{=} x^m(1 + \alpha_1 x + \cdots + \alpha_n x^n),$$

where $\alpha_1, \ldots, \alpha_n \in C$ and where $m \geq 1$, $n \geq 0$ are integers. If the Jacobson radical $\mathscr{J}(R)$ of R is trivial, the assertion follows from Corollary 1.8 of [4]. We may thus assume that $\mathscr{J}(R) \neq 0$. Let I be a nonzero two-sided ideal of R such that $\alpha_i I \subseteq \mathscr{J}(R)$ for $i = 1, \ldots, n$. For any arbitrary $a \in I$, there exists an integer $s = s(a) \geq 1$ such that

$$0 = g(a)^s = a^{ms}(1 + \alpha_1 a + \cdots + \alpha_n a^n)^s.$$

Since $\alpha_1 a, \ldots, \alpha_n a^n \in \mathscr{J}(R)$, the element $1 + \alpha_1 a + \cdots + \alpha_n a^n$ is invertible and hence $a^{ms} = 0$. This shows that I is a nonzero nil two-sided ideal of R, a contradiction to our assumption. So we assume that the y-degree of $g(x, y)$ is > 0. Fix an arbitrary term of $g(x, y)$ in the lowest possible average x-degree and let n be the y-degree of this term. (Hence n must be $\leq$ the y-degree of $g(x, y)$.) By Lemma 2, there exist integers $b, \rho, \rho_i \geq 0$

with $\rho \geq \rho_i$ such that the polynomial

$$h(x, z_1, \dots, z_n) \stackrel{\text{def.}}{=} g\left(x^b, \sum_{i=1}^{n} x^{\rho_i} z_i x^{\rho - \rho_i}\right)$$

possesses nonzero leading cyclic monomials, say, of the initial degree $m \geq 0$. Let l be the average x-degree of $h(x, z_1, \dots, z_n)$. If R is of the bounded nilpotency index, say, q, then $g(x, y)^q$ is already a polynomial identity of R and we are done in this case. We may thus assume that R is of the *un*bounded nilpotency index. By Fact 3, we may pick $a \in R$ of the nilpotency index $l + 1$. By Lemma 1, the polynomial $h^{(m)}(1, z_1, \dots, z_n)$ is nil on the right ideal $\rho \stackrel{\text{def.}}{=} a^l R$ and hence also on $\bar{\rho} \stackrel{\text{def.}}{=} \rho / \rho \cap l(\rho)$. By Lemma 3, there exist integers $m_3, \dots, m_n \geq 1$ such that the polynomial

$$g'(x, y) \stackrel{\text{def.}}{=} h^{(m)}(1, x, y, x^{m_3} y, \dots, x^{m_n} y)$$

is nontrivial. The y-degree of $g'(x, y)$ is obviously $<$ the y-degree of $g(x, y)$. By Fact 1, $\bar{\rho} \stackrel{\text{def.}}{=} \rho / \rho \cap l(\rho)$ is a prime ring without nonzero nil one-sided ideals. By the induction hypothesis applied to the polynomial $g'(x, y)$ nil on $\bar{\rho}$, $\bar{\rho}$ satisfies nontrivial generalized polynomial identities. By the result of the previous paragraph, $\bar{\rho}$ is a PI-ring. Say, $p(x_1, \dots, x_s)$ is a polynomial identity of $\bar{\rho}$. Then $p(a^l x_1, \dots, a^l x_s) a^l$ is a nontrivial generalized polynomial identity of R, as asserted.

REFERENCES

1. J. Bergen, Multilinear polynomials with power commuting values, *Houston J. Math.* **11** (1985), 283–292.
2. C.-L. Chuang, On ranges of polynomials in finite matrix rings, *Proc. Amer. Math. Soc.* **110** (1990), 293–302.
3. C.-L. Chuang and J.-S. Lin, Rings with nil and power central k-th commutators, *Rend. Circ. Mat. Palermo* **41** (1992), 62–68.
4. I. N. Herstein, C. Procesi, and M. Schacher, Algebraic valued functions on noncommutative rings, *J. Algebra* **36** (1975), 128–150.
5. B. Felzenszwalb and A. Giambruno, Centralizers and multilinear polynomials in noncommutative rings, *J. London Math. Soc.* **19** (1979), 417–428.
6. B. Felzenszwalb and A. Giambruno, Periodic and nil polynomials in rings, *Canad. Math. Bull.* **23** (1980), 473–476.
7. N. Jacobson, "PI-Algebra, An Introduction," *Lecture Notes in Mathematics*, Vol. 441 Springer-Verlag, New York/Berlin, (1967).
8. W. S. Martindale III, Prime rings satisfying a generalized polynomial identity, *J. Algebra* **12** (1969), 576–584.
9. Di Vincenzo, Derivations and multilinear polynomials, *Rend. Sem. Mat. Univ. Padova* **81** (1989), 209–219.