TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 202, 1975

NIL AND POWER-CENTRAL POLYNOMIALS IN RINGS(1)

BY

URI LERON

ABSTRACT. A polynomial in noncommuting variables is *vanishing, nil* or *central* in a ring, R, if its value under every substitution from R is 0, nilpotent or a central element of R, respectively.

THEOREM. *If R has no nonvanishing multilinear nil polynomials then neither has the matrix ring R_n.* THEOREM. *Let R be a ring satisfying a polynomial identity modulo its nil radical N, and let f be a multilinear polynomial. If f is nil in R then f is vanishing in R/N. Applied to the polynomial $xy-yx$, this establishes the validity of a conjecture of Herstein's, in the presence of polynomial identity.* THEOREM. *Let m be a positive integer and let F be a field containing no mth roots of unity other than 1. If f is a multilinear polynomial such that for some $n > 2$ f^m is central in F_n, then f is central in F_n.*

This is related to the (non)existence of noncrossed products among p^2-dimensional central division rings.

Introduction. Let C be a fixed domain of operators which we assume to be a commutative ring with unity. All rings are unital C-algebras and all polynomials have their coefficients in C. Let R be a ring, $f(x_1, \cdots, x_k)$ a polynomial in noncommuting variables. f is said to be *vanishing, nil* or *central* in R if under any substitution from R its value is 0, nilpotent or a central element of R, respectively. f is *multilinear* if it is homogeneous and linear in every one of its variables. In §1 we prove that the $n \times n$-matrix ring R_n has no nonvanishing multilinear nil polynomials if R has none. This is the case, for example, when R has no nonzero nilpotent elements. If R satisfies a polynomial identity modulo its nil radical and $f(x_1, \cdots, x_k)$ is a multilinear polynomial which is nil in R, it is then shown (§2) that the ideal $f(R)$ generated by the elements $f(r_1, \cdots, r_k)$, $r_i \in R$, is nil. Applied to the polynomial $x_1x_2 - x_2x_1$, this establishes the validity of a conjecture of Herstein's [4, p. 30], in the presence of polynomial identity. (This corollary has been known to some people for some years, but has apparently never been published.) A polynomial is called *power-*

Received by the editors September 18, 1973.

AMS(MOS) subject classifications (1970). Primary 16A38, 15A24; Secondary 16A42, 16A70.

Key words and phrases. Polynomial identities, nil polynomials, power-central polynomials, Herstein's conjecture, crossed products.

(1) Parts of this work are contained in the author's Ph.D. Thesis, written at the Hebrew University of Jerusalem. The author wishes to express his warm thanks to his thesis advisor, S. A. Amitsur.

central in R if some power of it is central in R. The existence of noncentral power-central polynomials for matrix rings over fields has recently been closely linked [6] with the open problem whether every p^2-dimensional central division ring is a crossed product. In §3 we prove that if F is a field and $n > 2$ then, with some provisions, every multilinear power-central polynomial for F_n must be central.

1. **Nil-polynomials in matrix rings.** Let R be a ring, R_n the ring of $n \times n$-matrices over R. Let R^* be the ring obtained from R by adjoining 1, and let e_{ij} be the matrix units in R_n^* having 1 in the (i, j)th position and 0 elsewhere. (The ring R^* is introduced for notational convenience only: The matrices that occur in the sequel are all of the form ae_{ij}, with $a \in R$, and thus belong to R_n.) Recall that these units multiply according to the rules $e_{ij}e_{jk} = e_{ik}$ and $e_{ij}e_{lk} = 0$ if $j \neq l$. Also, the elements of R (thought of as scalar matrices) commute with the e_{ij}'s. Let $u = (A_1, \cdots, A_k)$ be a sequence of matrices in R_n. The *value* of u is defined to be the product $|u| = A_1 \cdot A_2 \cdots A_k$. u is *nonvanishing* if $|u| \neq 0$. For a permutation σ of $\{1, \cdots, k\}$ we write $u^\sigma = (A_{\sigma(1)}, \cdots, A_{\sigma(k)})$ and call u^σ a permutation of u. Finally, a sequence of matrices from R_n is *simple* if it has the form $u = (a_1e_{i_1j_1}, \cdots, a_ke_{i_kj_k})$, where $a_i \in R$, $i = 1, \cdots, k$. Note that the value of a simple sequence is always of the form ae_{ij} for some $a \in R$.

LEMMA 1. *Let u be a nonvanishing simple sequence from R_n and u^σ a nonvanishing permutation of u.*

(a) *If $|u| = ae_{ii}$ for some $a \in R$ and $1 \leqslant i \leqslant n$ then $|u^\sigma| = be_{jj}$ for some $b \in R$ and $1 \leqslant j \leqslant n$.*

(b) *If $u = ae_{ij}$ for some $a \in R$ and $i \neq j$ then $|u^\sigma| = be_{ij}$ for some $b \in R$ and the same i, j.*

PROOF. For any simple sequence $w = (c_1e_{i_1j_1}, \cdots, c_ke_{i_kj_k})$ write $\lambda(w, p)$ (respectively $\rho(w, p)$) for the number of occurrences of the number p as a left (respectively right) index of one of the unit matrices occurring in w. Since u^σ is a permutation of u, it is clear that for every $1 \leqslant p \leqslant n$, $\lambda(u, p) = \lambda(u^\sigma, p)$ and $\rho(u, p) = \rho(u^\sigma, p)$. Suppose now $|u| = ae_{ij} \neq 0$ for any i and j (not necessarily distinct). Then u must have the form

$$(*) \qquad u = (a_1e_{ii_1}, a_2e_{i_1i_2}, a_3e_{i_2i_3}, \cdots, a_ke_{i_{k-1}j}).$$

Hence it is seen that $i = j$ if and only if $\lambda(u, p) = \rho(u, p)$ for every p. To prove (a), assume $|u| = ae_{ii}$. Then $\lambda(u, p) = \rho(u, p)$ for every p and so $\lambda(u^\sigma, p) = \rho(u^\sigma, p)$ for every p, hence $|u^\sigma| = be_{jj}$ for some $b \in R$ and some j. To prove (b), assume $|u| = ae_{ij}$ and $i \neq j$. Then, by $(*)$, $\lambda(u, p) = \rho(u, p)$ for every $p \neq i, j$, while $\lambda(u, i) = \rho(u, i) + 1$ and $\lambda(u, j) = \rho(u, j) - 1$. The same relations must therefore hold also for u^σ, and this can only happen if $|u^\sigma| = be_{ij}$. Thus the proof is completed.

DEFINITION. Let u be a simple sequence. Then u is called *even* if for some σ, $|u^\sigma| = be_{ii} \neq 0$, and *odd* if for some σ, $|u^\sigma| = be_{ij} \neq 0$ where $i \neq j$.

These terms are well defined by Lemma 1, and are explained by the observation that if $i = j$ (respectively $i \neq j$) then i and j have an even (respectively odd) number of occurrences in the indices of the unit matrices of u. Note that if $|u^\sigma| = 0$ for all σ, then u is neither odd nor even.

LEMMA 2 (REGEV). *Let R be a ring, $f(x_1, \cdots, x_k)$ a multilinear polynomial. Let $u = (A_1, \cdots, A_k)$ be a simple sequence of matrices from R_n.*

(a) *If u is even then the matrix $f(u)$, obtained by substituting u in f, is diagonal.*

(b) *If u is odd then $f(u) = ae_{ij}$ for some $a \in R$ and $i \neq j$.*

PROOF. Since f is multilinear, it has the form $f(x_1, \cdots, x_k) = \Sigma_{\sigma \in S_k} c_\sigma x_{\sigma(1)}, \cdots, x_{\sigma(k)}$, where S_k is the symmetric group on $\{1, \cdots, k\}$ and $c_\sigma \in C$. Thus $f(u) = \Sigma_{\sigma \in S_k} c_\sigma |u^\sigma|$. Let $T = \{\sigma \in S_k \mid |u^\sigma| \neq 0\}$, and note that in the sum for $f(u)$ it suffices to let σ range over T.

(a) If u is even then, for some $\sigma \in T$, $|u^\sigma|$ is of the form ae_{ii}, whence, by Lemma 1, $|u^\sigma| = a_\sigma e_{i_\sigma i_\sigma}$ for *every* $\sigma \in T$. Thus

$$f(u) = \sum_{\sigma \in T} c_\sigma |u^\sigma| = \sum_{\sigma \in T} c_\sigma a_\sigma e_{i_\sigma i_\sigma},$$

that is, a diagonal matrix.

(b) If u is odd then for some $\sigma \in T$ $|u^\sigma|$ is of the form ae_{ij} with $i \neq j$; hence, by Lemma 1, $|u^\sigma| = a_\sigma e_{ij}$ for every $\sigma \in T$. Thus

$$\begin{aligned} f(u) &= \sum_{\sigma \in T} c_\sigma |u^\sigma| = \sum_{\sigma \in T} c_\sigma a_\sigma e_{ij} \\ &= \left(\sum_{\sigma \in T} c_\sigma a_\sigma \right) e_{ij} = ae_{ij}, \text{ where } a = \sum_{\sigma \in T} c_\sigma a_\sigma, \end{aligned}$$

and Lemma 2 is proved.

Lemmas 1 and 2 will now be applied to discuss polynomial identities and nil polynomials in matrix rings.

LEMMA 3. *Let R be a ring and $f(x_1, \cdots, x_k)$ a multilinear polynomial. If f vanishes under every even substitution from R_n then f vanishes in R_n.*

PROOF. Since f is multilinear and the matrices of the form ae_{ij}, $a \in R$, generate R_n additively, it will suffice to show that f vanishes under every simple substitution $u = (A_1, \cdots, A_k)$ from R_n. This vanishing is given for even substitutions, so assume u is odd. By Lemma 2, $f(u) = ae_{ij}$ for some $a \in R$ and $i \neq j$, and we wish to show $a = 0$. Consider the invertible matrix $A = 1 + e_{ji}$ (its inverse is $A^{-1} = 1 - e_{ji}$) and the inner automorphism φ: $x \mapsto AxA^{-1}$ it induces in R_n. Writing u^φ for the image of the sequence u under φ, we have

$$f(u^{\varphi}) = f(u)^{\varphi} = ae_{ij}^{\varphi} = a(e_{jj} - e_{ii} + e_{ij} - e_{ji}),$$

since φ leaves a fixed. Now u^{φ} may not be a simple sequence, but we can write $f(u^{\varphi}) = \Sigma_{r=1}^{m} f(u^{(r)})$, where the $u^{(r)}$ are simple. We claim that the entries on the main diagonal of the matrix $f(u^{(r)})$ are all 0 for $r = 1, \cdots, m$. Indeed, this is given for even $u^{(r)}$ and follows from Lemma 2 for odd $u^{(r)}$. Thus the main diagonal also vanishes in the matrix $f(u^{\varphi}) = a(e_{jj} - e_{ii} + e_{ij} - e_{ji})$ and, given $i \neq j$, this forces $a = 0$. Hence $f(u) = ae_{ij} = 0$, and the proof is completed.

REMARK. Lemma 3 asserts that a multilinear polynomial which vanishes under even substitutions from R_n must also vanish under odd ones. The converse of this statement is false for every n. For if R is, for example, a field of characteristic zero, then by [3] there exists a multilinear polynomial f, which is central and nonvanishing in R_n; and, by Lemma 2, f vanishes under every odd substitution from R_n.

The main theorem of this section follows.

THEOREM 4. *If in a ring R every multilinear nil polynomial vanishes, then the same holds for R_n.*

PROOF. Suppose $f(x_1, \cdots, x_k)$ is a multilinear polynomial which is nil in R_n. Then we shall show that f vanishes in R_n. By Lemma 3 we need only show that $f(u) = 0$ whenever

$$u = (a_1 e_{i_1 j_1}, \cdots, a_k e_{i_k j_k})$$

is even. To this end, consider the matrices $x_\nu e_{i_\nu j_\nu}$, $\nu = 1, \cdots, k$, with polynomial entries. Substitute these matrices in f and write

$$f(x_1 e_{i_1 j_1}, \cdots, x_k e_{i_k j_k}) = \begin{pmatrix} f_1(x_1, \cdots, x_k) & & 0 \\ & \ddots & \\ 0 & & f_n(x_1, \cdots, x_k) \end{pmatrix},$$

where the f_i are multilinear polynomials over C in the variables $x_1, \cdots, x_k$. The off-diagonal entries are guaranteed by Lemma 2 to be 0, since the original sequence u was even. If we now make any substitution $x_i = b_i \in R$ in the above relation, then the left-hand member becomes a nilpotent matrix since f is nil in R_n. Therefore, the diagonal matrix on the right also becomes nilpotent and it follows that each polynomial f_i is nil in R, hence vanishes in R. In particular, by substituting $x_i = a_i$, we obtain $f(u) = 0$. As mentioned above this completes the proof of the theorem.

The following special case of Theorem 4 is of particular interest.

COROLLARY 5. *Let R be a ring with no nonzero nilpotent elements and let f be a multilinear polynomial. If f is nil in R_n then f vanishes in R_n.*

Examples of rings R as in Corollary 5 are fields, division rings and direct products thereof.

REMARK. If R is a ring with no nonzero nilpotent elements, it is an open question whether nonvanishing nil polynomials (necessarily nonmultilinear) for R_n exist. In case R is an infinite field the answer is negative, as follows from [1, Theorem 4], by noting that if f is nil in R_n then f^n must vanish in R_n.

2. **A generalized Herstein's conjecture.** One of the principal problems concerning nil polynomials is the following open problem, which was formulated by Herstein [4, p. 30] for the case of the polynomial $x_1x_2-x_2x_1$: If $f(x_1, \cdots, x_k)$ is nil in R, is the ideal generated in R by the elements $f(r_1, \cdots, r_k)$ nil? The answer is known to be "yes" in case $f(x_1, x_2) = x_1x_2 - x_2x_1$ and the indices of nilpotency are bounded [ibid.]. In this case the ring satisfies the identity $(x_1x_2 - x_2x_1)^m$ for some m. We shall now show that the answer is still positive if R satisfies any polynomial identity modulo its nil radical and f is any multilinear polynomial. We start with a generalization to nil polynomials, of Kaplansky's classical theorem on primitive rings satisfying a polynomial identity.

THEOREM 6. *Let R be a (Jacobson) semisimple ring and let $f(x_1, \cdots, x_k)$ be a multilinear polynomial of degree k which is nil in R. Then f vanishes in R. If, in particular, R is primitive, then it is a central simple algebra of dimension $\leqslant [k/2]^2$ over its center.*

PROOF. If $R = D_n$ is a matrix ring over a division ring, then f vanishes in R by Corollary 5. Suppose next that R is primitive. Then there exists a division ring D such that either $R \cong D_n$ for some n, or D_n is a homomorphic image of a subring of R for every n. But the latter is impossible for it leads to the absurd conclusion that f is nil (hence vanishes) in D_n for every n. Thus $R \cong D_n$ for some n and f vanishes in R. Finally, if R is semisimple then it is a subdirect product of primitive rings R_i and f is nil in each R_i. Thus f vanishes in each R_i, hence also in R.

THEOREM 7. *Let R be a ring, N its maximal nil ideal, and suppose R/N satisfies a polynomial identity. Let $f(x_1, \cdots, x_k)$ be a multilinear polynomial which is nil in R. Then the ideal $f(R)$, generated in R by all the elements $f(r_1, \cdots, r_k)$, $r_i \in R$, is nil.*

PROOF. Suppose first that R is an algebra over a field. By considering R/N instead of R, we may suppose that R satisfies a polynomial identity and has no nonzero nil ideals. We then wish to show that $f(R) = \{0\}$, i.e. f vanishes in R. Consider any element a of $f(R)$. a can be written as a finite sum of terms of the form $xf(r_1, \cdots, r_k)y$, where $x, y, r_1, \cdots, r_k \in R$. If R_0 is the subalgebra of

R generated by all the elements appearing in such an expression for a, then clearly $a \in f(R_0)$. Let J_0 be the (Jacobson) radical of R_0. Then f is nil in the semisimple algebra R_0/J_0 and, by Theorem 6, f vanishes in R_0/J_0. Thus $f(R_0) \subseteq J_0$ and in particular $a \in J_0$. But J_0, being the radical of a finitely generated polynomial identity algebra over a field, is nil [2] and so a is nilpotent. Since a was an arbitrary element of $f(R)$, $f(R)$ is seen to be a nil ideal, hence $f(R) = \{0\}$. This establishes the theorem for algebras over fields. The transition to general rings is standard and will be omitted (see e.g. [5, p. 416]).

Applying Theorem 7 to the polynomial $f(x_1, x_2) = x_1x_2 - x_2x_1$, one obtains a proof of Herstein's conjecture, in the presence of polynomial identity.

COROLLARY 8. *Let R be a ring, N its maximal nil ideal, and suppose R/N satisfies a polynomial identity. If all the commutators in R are nilpotent, then the ideal $C(R)$ generated by them is nil. (Equivalently, the collection of nilpotent elements of R is an ideal.)*

REMARKS. (a) Theorem 7 asserts that the condition that R/N satisfies a polynomial identity is sufficient for the validity of the "generalized Herstein's conjecture". It is interesting to note that this condition is also necessary. For if R is any ring and the ideal $f(R)$ is nil, then f vanishes in R/N.

(b) Theorem 7 and Corollary 8 still hold if, instead of assuming that R/N satisfies a polynomial identity, we assume that R is an algebra over an uncountable field.

3. **Power-central polynomials.**

LEMMA 9. *Let R be a ring, $f(x_1, \cdots, x_k)$ a multilinear polynomial and $n > 2$ an integer. If $f(u) \in$ Center (R_n) for every even substitution u from R_n then f is central in R_n. The conclusion still holds if $n = 2$ and $2a \neq 0$ for all $a \neq 0$ in R.*

The proof is similar to that of Lemma 3, but we repeat it for completeness.

PROOF. It is enough to show that f vanishes under every odd substitution from R_n. Let u be odd and let $f(u) = ae_{ij}$ for some $a \in R$ and $i \neq j$. Applying the same transformation φ as in the proof of Lemma 3, we have $f(u^\varphi) = a(e_{jj} - e_{ii} + e_{ij} - e_{ji})$. Write $f(u^\varphi) = \Sigma_{r=1}^m f(u^{(r)})$ where $u^{(r)}$ are all simple. Then, by Lemma 2, the sum over all the even $u^{(r)}$'s must equal $a(e_{jj} - e_{ii})$. But by the assumption of the lemma, this sum is in the center of R_n. Thus $a(e_{jj} - e_{ii}) \in$ Center (R_n). Since we are assuming $n > 2$ or $a \neq -a$, this forces $a = 0$. Hence $f(u) = ae_{ij} = 0$ and f is central.

Note that the restriction in Lemma 9 is essential, for if F is a field of characteristic 2, then the commutator $[x_1, x_2] = x_1x_2 - x_2x_1$ is a multilinear polynomial and is central under even substitutions from F_2, but $[e_{11}, e_{12}] = e_{12} \notin$ Center (F_2).

THEOREM 10. *Let f be a multilinear polynomial, m and $n > 2$ positive integers, and F a field containing no mth roots of unity other than 1. If f^m is central in F_n, then so must be f. The conclusion holds also for $n = 2$, provided* char $(F) \neq 2$.

PROOF. Assume that f^m is central in F_n and let u be an even substitution from F_n. By Lemma 9, we need only show that $f(u) \in$ Center (F_n). Since u is even, $f(u)$ is a diagonal matrix, $f(u) = \Sigma_{i=1}^n a_i e_{ii}$, $a_i \in F$. We may assume $f(u) \neq 0$, say $a_1 \neq 0$. Since $f^m(u) = \Sigma_{i=1}^m a_i^m e_{ii}$ is in the center of F_n, we have $a_1^m = a_2^m = \cdots = a_n^m$. Thus, for any $1 < i \leqslant n$, $(a_i/a_1)^m = 1$; so $a_i/a_1 = 1$ and $a_i = a_1$, that is, $f(u) = \Sigma_{i=1}^n a_i e_{ii} \in$ Center (F_n).

Let Q denote the field of rational numbers, and for a prime q let $Z_q(t)$ denote the field of rational functions in t over the field of q elements. Let F denote either Q or $Z_q(t)$ and $q = \text{char } F$. In [6] Schacher and Small proved the equivalence of the following statements for an odd prime p:

(a) Every p^2-dimensional division ring of characteristic q (0 or a prime) is a crossed product.

(b) There exists for F_p a noncentral polynomial f such that f^p is central.

Whether these statements are true or false is still an open problem (for $p \geqslant 5$). However, we have the following.

COROLLARY 11. *Let q and $p > 2$ be primes such that $q \leqslant p$, and let F be Q or $Z_q(t)$. Then F_p has no noncentral multilinear polynomial f such that f^p is central.*

PROOF. Note that F has no pth roots of unity other than 1, then apply Theorem 10.

REFERENCES

1. S. A. Amitsur, *The T-ideals of the free ring,* J. London Math. Soc. 30 (1955), 470–475. MR 17, 122.

2. ———, *A generalization of Hilbert's Nullstellensatz,* Proc. Amer. Math. Soc. 8 (1957), 649–656. MR 19, 384.

3. E. Formanek, *Central polynomials for matrix rings,* J. Algebra 23 (1972), 129–132. MR 46 #1833.

4. I. N. Herstein, *Theory of rings,* University of Chicago Lectures Notes, 1961.

5. T. P. Kezlan, *Rings in which certain subsets satisfy polynomial identities,* Trans. Amer. Math. Soc. 125 (1966), 414–421. MR 36 #211.

6. M. Schacher and L. Small, *Central polynomials which are pth powers,* Comm. Algebra (to appear).

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, LOS ANGELES, CALIFORNIA 90024

Current address: Department of Mathematics, Technion-Israel Institute of Technology, Haifa, Israel