TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 172, October 1972

GROUP RINGS, MATRIX RINGS, AND POLYNOMIAL IDENTITIES

BY

ELIZABETH BERMAN

ABSTRACT. This paper studies the question, if R is a ring satisfying a polynomial identity, what polynomial identities are satisfied by group rings and matrix rings over R? **Theorem 2.6.** *If R is an algebra over a field with at least q elements, and R satisfies $x^q = 0$, and G is a group with an abelian subgroup of index k, then the group ring $R(G)$ satisfies $x^t = 0$, where $t = qk^2 + 2$.* **Theorem 3.2.** *If R is a ring satisfying a standard identity, and G is a finite group, then $R(G)$ satisfies a standard identity.* **Theorem 3.4.** *If R is an algebra over a field, and R satisfies a standard identity, then the k-by-k matrix ring R_k satisfies a standard identity.* Each theorem specifies the degree of the polynomial identity.

1. **Introduction.** We summarize results on matrix rings over polynomial identity rings. Let $[b]$ denote the largest integer in b. Suppose that R is a ring satisfying a homogeneous polynomial identity with coefficients in the centroid, at least one coefficient of 1, and degree d. Then for all k, R_k satisfies some power of the standard identity of degree $2k[d/2]^2$ [6, Theorem 1], [2, Theorem 8].

The *unitary polynomial* of degree q is

$$\sum_{f \in S_q} x_{f(1)} \cdots x_{f(q)},$$

where the sum is over all permutations f in S_q, the symmetric group on q letters. The *unitary identity* results from setting the polynomial equal to 0. If R is a ring satisfying the unitary identity of degree q, then R_k satisfies the unitary identity of degree $qk^2 + 1$ [2, Theorem 1].

The *docile polynomial* of degree q is

$$\sum_{f} (-1)^f x_{f(1)} \cdots x_{f(q)},$$

where the sum is over all permutations f in S_q sending even integers into even integers. If R is a ring satisfying the docile identity of degree $2q$, then R_k satisfies the standard identity of degree $2q^2k^2 + 1$ [2, Theorem 2].

The *docile product polynomial* of degree q, p is

$$\prod_{i=1}^{p} D(x_{i1}, \cdots, x_{iq})u_i,$$

Received by the editors August 5, 1971.

AMS (MOS) subject classifications (1970). Primary 16A22, 16A26, 16A38, 16A42, 20C05.

Key words and phrases. Group rings, matrix rings, polynomial identities, standard identity, bounded nil rings.

where D is the docile polynomial of degree q, and the x's and u's are noncommuting variables. If R is a ring satisfying the docile product polynomial identity of degree $2q$, p, then R_k satisfies a product of p standard identities, each of degree $2q^2k^2 + 1$ [1, Theorem 2.2].

If R is an algebra over a field with at least q elements, and R satisfies all the homogeneous components of $(\Sigma_{i=1}^{q} x_i)^q$, then R_k satisfies $x^p = 0$, with $p = qk^2 + 1$ [1, Theorem 1.2].

The next section uses these results on matrix rings to prove theorems on group rings. §3 is independent of the preceding material and contains the main results of the paper: If R is a ring satisfying the standard identity and G is a finite group, then $R(G)$ satisfies a standard identity. A similar theorem for matrix rings is a corollary.

2. **Various polynomial identities on group rings.** We know that if K is a field and G a group with an abelian subgroup of finite index k, then $K(G)$ satisfies the standard identity of degree $k^2 + 1$ [6, Theorem 4.2]. The proof below is similar.

Theorem 2.1. *Suppose that R is a ring and G a group with subgroup A of finite index k. Let E be the group ring $R(A)$, and let I be the set of all r in R such that $Rr = 0$. Then there is a homomorphism of $R(G)$ into E_k with kernel $I(G)$.*

Proof. Let $y_1, \cdots, y_k$ be a set of right coset representatives of A in G. Then $R(G)$ is a free left module over E with basis $y_1, \cdots, y_k$. Let T be the ring of linear transformations of this module. If $w \in R(G)$, let T_w be the function on the module sending y into yw. Then the map $w \to T_w$ is a homomorphism from the ring $R(G)$ into T with kernel $I(G)$. Since T is isomorphic to E_k, the theorem follows.

Corollary 2.2. *Suppose that R is a ring with unity and G is a group with an abelian subgroup A of finite index k. Then any homogeneous multilinear polynomial identity satisfied by R is also satisfied by $R(A)$, and any polynomial identity satisfied by $[R(A)]_k$ is also satisfied by $R(G)$.*

Proof. If R contains unity, $I = \{0\}$.

Remark. If R is a ring without unity, it may be imbedded in a ring with unity, as is well known. If R satisfies the docile identity, the docile product identity, or some power of the standard identity, then so does the new ring. Thus we get the following corollaries of three matrix ring theorems from the introduction:

2.3. *If R is a ring satisfying the docile identity of degree $2q$, and G is a group with abelian subgroup of index k, the $R(G)$ satisfies the standard identity of degree $2q^2k^2 + 1$.*

2.4. *If R is a ring satisfying the docile product identity of degree $2q$, p, and G is a group with an abelian subgroup of index k, then $R(G)$ satisfies a product of p standard identities, each of degree $2q^2k^2 + 1$.*

2.5. *If R is a ring satisying a homogeneous polynomial identity with coefficients in the centroid, at least one coefficient of 1, and G is a group with an abelian subgroup of index k, then $R(G)$ satisfies some power of a standard identity.*

For the unitary identity we prove the following:

Theorem 2.6. *If R is a ring satisfying the unitary identity of degree q, and G is a group with an abelian subgroup of finite index k, then $R(G)$ satisfies $x_0U(x_1, \cdots, x_p) = 0$, where U is the unitary polynomial, $p = qk^2 + 1$, and the x's are noncommuting variables.*

Proof. Let E and I be as in Theorem 2.1. There is a homomorphism from $R(G)$ into E_k with kernel $I(G)$. Now E_k satisfies $U(x_1, \cdots, x_p) = 0$. Thus if $w_1, \cdots, w_p$ are p elements of $R(G)$, then $U(w_1, \cdots, w_p) \in I(G)$. Since I is the right annihilator of R, the theorem follows.

Theorem 2.7. *If R is an algebra over a field with at least q elements, and R satisfies $x^q = 0$, and G is a group with an abelian subgroup of index k, then $R(G)$ satisfies $x^t = 0$, where $t = qk^2 + 2$.*

Proof. The polynomial $(\Sigma_{i=1}^{q} x_i)^q$ vanishes on R. Using a Vandermonde determinant, we see that every homogeneous component of this polynomial vanishes on R and hence also on $R(A)$. Thus $[R(A)]_k$ satisfies $x^p = 0$, with $p = qk^2 + 1$. Thus if $w \in R(G)$, $w^p \in I(G)$. Hence $w^{p+1} = 0$.

3. The standard identity.

Definition. Suppose that G is a semigroup and $\{g_1, \cdots, g_q\}$ is a sequence of q elements of G. To *parenthesize the sequence into j clumps* is to insert j pairs of adjacent, nonoverlapping parentheses. The subsequence within one pair of parentheses constitute a *clump*. It is *odd* or *even*, depending on whether there is an odd or even number of elements.

In the example below we parenthesize a sequence into 3 clumps:

$$\{g_1, g_2, (g_3, g_4,)(g_5,)(g_6, g_7,)g_8\}.$$

The product of the elements within a clump is the *value of the clump*. If $C_1, \cdots, C_k$ are k clumps, then the *value of* $C_1 \cdots C_k$ is the product of the values of these clumps in the stated order.

Lemma 3.1. *Suppose that G is a group with unity e. Let j and n be positive integers, with $p = \Sigma_{i=0}^{n-1} j^i$. Let $S = \{g_1, \cdots, g_p\}$ be a sequence of p*

elements of G. Then S may be parenthesized into clumps such that at least one of the following conditions holds:

1. *There are n consecutive clumps $C_1, \cdots, C_n$ such that C_1 begins with g_1, and the values of $C_1, C_1C_2, \cdots, C_1C_2 \cdots C_n$ are all distinct.*

2. *There are j consecutive clumps each of value e.*

Proof. Induct on n. If $n = 1$, then $p = 1$. If S is a sequence composed of a solitary element g_1, then we form one clump consisting of g_1, and condition 1 holds.

Assume that the lemma is true for n. Let $p = \Sigma_{i=0}^{n-1} j^i$, and let $q = \Sigma_{i=0}^{n} j^i = jp + 1$.

Suppose that $\{g_1, \cdots, g_q\}$ is a sequence of q elements of G. Let $S' = \{g_2, \cdots, g_{p+1}\}$. If S' has j consecutive clumps of value e, then we are done. If not, then by induction hypothesis we can form n consecutive clumps $C_2, \cdots, C_{n+1}$ in S' such that C_2 begins with g_2, and the values of $C_2, \cdots, C_2 \cdots C_{n+1}$ are all distinct. Form a new clump C_1 consisting of g_1.

Case 1. The values of $C_1, C_1C_2, \cdots, C_1 \cdots C_{n+1}$ are all distinct. Then conclusion 1 holds.

Case 2. These values are not all distinct. Then there exist positive integers k and r such that $k + r \leq n + 1$ and $C_1 \cdots C_k = C_1 \cdots C_{k+r}$. If $k > 1$, then we cancel the value of C_1 and obtain $C_2 \cdots C_k = C_2 \cdots C_{k+r}$. But this is impossible. Hence $k = 1$, and

$$C_1 = C_1 \cdots C_{1+r}.$$

Thus $e = C_2 \cdots C_{1+r}$.

Combine the clumps $C_2, \cdots, C_{1+r}$ to form a new clump D_1 of value e. Let g_m be the entry in the sequence following D_1. Continue the argument as before with the next p entries, starting with g_m. If we do not finish then, we get a second clump D_2 of value e. Since there are jp elements after g_1, we will get j clumps $D_1, \cdots, D_j$, each of value e, if we do not finish earlier.

Theorem 3.1. *Suppose that n and j are positive integers, G is a group of order $n > 1$, and $q = (j^n - 1)/(j - 1)$. Then any sequence of q elements of G can be parenthesized into j clumps, each of value e.*

Proof. By the formula for the sum of a geometric progression $q = \Sigma_{i=0}^{n} j^i$. If the theorem is false, then G has at least $n + 1$ elements.

Lemma 3.2. *If $\{g_1, \cdots, g_q\}$ is a sequence of elements of a set, and one parenthesizes them into j odd clumps, and permutes the clumps with some permutation f in S_j, then the resulting permutation of the original q elements has the same parity as f* [2, *Corollary to Lemma* 4].

Lemma 3.3. *Suppose that n and k are positive integers, and A and B are sets, A containing at least $n(k-1)+1$ elements, B containing exactly n elements. Let h be a function from A into B. Then at least k elements of A have the same image in B* [2, *Lemma* 1].

Lemma 3.4. *Suppose that A and B are finite nonempty sets, $|A| = m$, and $|B| = n$. Let h be a function from A into B. Let $[j]$ be the largest integer in j, and let $k = [(m+n-1)/n]$. Then at least k elements of A have the same image in B.*

Proof. Since $k \leq (m+n-1)/n$, we have $nk \leq m+n-1$, and $n(k-1)+1 \leq m$. The previous lemma now applies.

Lemma 3.5. *Suppose that G is a group of order $n \geq 2$, and p is a positive integer. Let $t = n(p-1)+2$. Let $q = (t^n-1)/(t-1)$. Then any sequence of q elements in G can be parenthesized into $2p$ odd clumps whose values commute with each other.*

Proof. By Theorem 3.1, the sequence can be parenthesized into t clumps, each of value e. Let E be the number of even clumps, and let D be the number of odd clumps. Let $k = [(E+n-1)/n]$.

Let A be the set of even clumps. If A is nonempty, define a function from A into G, letting the image of each even clump be its initial element. By Lemma 3.4, since $|G| = n$, at least k even clumps have the same initial element g. Choose the first k such clumps; call them $\{C_1, \cdots, C_k\} = C$.

If A is empty, $k = 0$. Let C be the empty set.

Let J be the union of C with all the odd clumps. Create new clumps as follows: Let E_1 be the first clump in J. If E_1 is odd, form the new clump F_1 by combining E_1 with all even clumps to the right, if any, up to the next clump from J. Then F_1 is odd, of value e.

If E_1 is even, form two new clumps F_1 and F_2: let F_1 consist of the single element g that begins E_1. Obviously, F_1 is odd, of value g. Let F_2 consist of all subsequent elements, up to the next clump from J. Now E_1, with g deleted, is odd, of value g^{-1}. All following clumps not in J are even, of value e. Thus F_2 is odd, of value g^{-1}.

Continuing in this manner, we form $2k+D$ new clumps, adjacent, odd, and of value either g, g^{-1}, or e. We next show that $2k+D \geq 2p$.

Case 1. Suppose that $D = 0$ or 1. Now $E = t - D = n(p-1)+2-D$. Thus

$$k = \left[\frac{E+n-1}{n}\right] = \left[\frac{np+1-D}{n}\right] \geq \frac{np+1-1}{n} = p.$$

Hence $2k+D \geq 2p$.

Case 2. Suppose that $D \geq 2$. Then

$$2k + D = 2\left[\frac{np + 1 - D}{n}\right] + D > 2\left(\frac{np + 1 - D}{n} - 1\right) + D$$

$$= 2\frac{np + 1}{n} - 2 + D\left(1 - \frac{2}{n}\right) \geq 2\frac{np + 1}{n} - 2 + 2\left(1 - \frac{2}{n}\right)$$

$$= 2p - \frac{2}{n} \geq 2p - 1.$$

Since $2k + D$ is an integer, $2k + D \geq 2p$.

Note. The next theorem hypothesizes that R satisfies a standard identity of even degree. Leron and Vapne mention that a ring with unity satisfying a standard identity of degree $2p + 1$ also satisfies the standard identity of degree $2p$ [4, p. 130].

Theorem 3.2. *If R is a ring satisfying the standard identity of degree $2p$, and G is a group of order $n > 1$, and q is the integer defined in Lemma 3.4, then $R(G)$ satisfies the standard identity of degree q.*

Proof. Let $P(x_1, \cdots, x_q) = 0$ be the standard identity of degree q. It suffices to prove that P vanishes on elements of $R(G)$ of form rg, where $r \in R$, and $g \in G$. Let $r_1g_1, \cdots, r_qg_q$ be q such elements, and let f be any permutation in S_q. Let S be the sequence in G $\{g_{f(1)}, \cdots, g_{f(q)}\}$. Then S can be parenthesized into $2p$ odd clumps whose values commute with each other. Consider f as a sequence: $\{f(1), \cdots, f(q)\}$, and parenthesize f in the same manner as S. We can partition S_q into disjoint subsets, such that if f and f' are in the same subset, they satisfy the following relations:

1. The integers before the first clump are the same integers in the same order.
2. The integers after the last clump are the same integers in the same order.
3. The $2p$ odd clumps are the same, but in any order. Now

$$P(r_1g_1, \cdots, r_qg_q) = \sum_{f \in S_q} (-1)^f r_{f(1)}g_{f(1)} \cdots r_{f(q)}g_{f(q)}.$$

Let T be one of the partition subsets defined above. Let $f' \in T$, and let $g = g_{f'(1)} \cdots g_{f'(q)}$. Then

$$\sum_{f \in T} (-1)^f r_{f(1)}g_{f(1)} \cdots r_{f(q)}g_{f(q)} = \left[\sum_{f \in T} (-1)^f r_{f(1)} \cdots r_{f(q)}\right] g.$$

For each $f \in T$, we parenthesize the sequence $\{r_{f(1)}, \cdots, r_{f(q)}\}$ in the same manner as S, forming $2p$ odd clumps. The expression within brackets above is the product of the following factors

1. The product of all the r's before the first clump.
2. Polynomial P, evaluated on the $2p$ odd clumps.
3. The product of all r's after the last clump.

Since the second factor is 0, the theorem follows.

Theorem 3.3. *Suppose that R is a ring satisfying the standard identity of degree $2p$. Let k be a positive integer, and let $n = 2^k k!$. Let q be as in Lemma 3.4. Suppose that 2^q does not annihilate R. Then R_k satisfies $2^q P(x_1, \cdots, x_q) = 0$, where P is the standard polynomial.*

Proof. As is well known, R_k is isomorphic to $R \otimes Z_k$, where Z is the ring of integers. Let B be the subset of Z_k of nonsingular matrices in which each row consists entirely of zeroes, except for a single entry of either 1 or -1. Under matrix multiplication, G is a group of order $2^k k!$.

If $r \in R$, and $g \in G$, let $f(rg) = r \otimes g \in R \otimes Z_k$. Then f can be extended to get a ring homomorphism of $R(G)$ into $R \otimes Z_k$. Suppose that e_{ij} is the matrix unit in Z_k with 1 in row i, column j. Let w and z be elements of G such that every entry in w is the negative of the corresponding entry in z, except that each has 1 in row i, column j. Then $2e_{ij} = w + z$. Thus if $r \in R$, and u is a matrix unit in Z_k, then $r \otimes 2u$ lies in the image of the homomorphism.

If $r_1, \cdots, r_q \in R$, and $u_1, \cdots, u_q$ are matrix units, then

$$2^q P(r_1 \otimes u_1, \cdots, r_q \otimes u_q) = P(r_1 \otimes 2u_1, \cdots, r_q \otimes 2u_q) = 0.$$

Hence $2^q P$ vanishes on R_k.

Theorem 3.4. *Hypothesis: Let R be an algebra over a field F. Suppose that R satisfies the standard identity of degree $2p$. Let k be a positive integer, and let q be as in Lemma 3.4.*

Conclusion: If F has characteristic 2, then R_k satisfies the standard identity of degree $2pk^2 + 1$. If F has another characteristic, then R_k satisfies the standard identity of degree q.

Proof. The first statement is the Corollary to Theorem 1 from [2]. The second is a corollary of Theorem 3.3.

REFERENCES

1. Elizabeth Berman, *Matrix rings over polynomial identity rings*, Trans. Amer. Math. Soc. 172 (1972), 231–239.

2. ———, *Tensor products of polynomial identity algebras*, Trans. Amer. Math. Soc. 156 (1971), 259–271. MR 43 #278.

3. Nathan Jacobson, *Structure of rings*, rev. ed., Amer. Math Soc. Colloq. Publ., vol. 37, Amer. Math. Soc., Providence, R. I., 1964. MR 36 #5158.

4. Uri Leron and Amitai Vapne, *Polynomial identities of related rings*, Israel J. Math. 8 (1970), 127–137. MR 42 #4589.

5. D. S. Passman, *Linear identities in group rings*, Pacific J. Math. 36 (1971), 457–483.

6. C. Procesi and L. Small, *Endomorphism rings of modules over* PI-*algebras*, Math. Z. 106 (1968), 178–180. MR 38 #2167.

DEPARTMENT OF MATHEMATICS, ROCKHURST COLLEGE, KANSAS CITY, MISSOURI 64110