

Pacific Journal of Mathematics

POLYNOMIAL CONSTRAINTS FOR FINITENESS OF SEMISIMPLE RINGS

MOHAN S. PUTCHA AND ADIL MOHAMED YAQUB

POLYNOMIAL CONSTRAINTS FOR FINITENESS OF SEMISIMPLE RINGS

MOHAN S. PUTCHA AND ADIL YAQUB

Suppose R is an associative ring with Jacobson radical J . Suppose that for each sequence x_1, \dots, x_n in R there exists a polynomial p homogeneous (of bounded degree) in each x_i and a monomial w in the x 's, in which some x_i is missing, such that $p = w$. Then R/J is finite. It is also shown that if the above polynomial p is a monomial, then R/J is finite and J is nil of bounded index.

In a recent paper, the authors proved the following theorem: Suppose R is an associative ring with Jacobson radical J . Suppose further, that, for all x_1, \dots, x_n in R , there exists a word $w(x_1, \dots, x_n)$, depending on x_1, \dots, x_n , in which at least one x_i (i varies) is missing, and such that

$$(1) \quad x_1 \cdots x_n = w(x_1, \dots, x_n).$$

Then J is a nil ring of bounded index and R/J is finite. In the present paper, we consider the structure of an associative ring R which satisfies, instead of the identity (1) above, an identity of the form

$$(2) \quad p(x_1, \dots, x_n) = w(x_1, \dots, x_n).$$

In particular, we take a closer look at the structure of R in those cases where (i) $p(x_1, \dots, x_n)$ is *any fixed* word involving each of the variables x_1, \dots, x_n at least once, or (ii) $p(x_1, \dots, x_n)$ is a variable polynomial in x_1, \dots, x_n with integer coefficients such that each x_i is of the same degree in each term of $p(x_1, \dots, x_n)$, and where these degrees are bounded. We show, for example, that if $p(x_1, \dots, x_n)$ is as in (i) above, then the Jacobson radical J of R is nil of bounded index and R/J is finite. Moreover, we show that, if $p(x_1, \dots, x_n)$ is as in (ii) above, then R/J is still finite. We conclude by giving some examples of the rings under consideration.

In establishing the results of this paper, we use the structure theory of rings, starting with the division ring case, then the primitive ring case, followed by the semisimple ring case

1. Main results. Throughout R will denote an associative ring, Z will denote the ring of integers, and n will denote a fixed positive integer >1 . We now introduce the following.

DEFINITION 1. Let $Z[x_1, \dots, x_n]$ be the ring of polynomials in n

noncommuting indeterminates x_1, \dots, x_n over Z . Let \mathcal{X}_n be the subset of $Z[x_1, \dots, x_n]$ consisting of polynomials $p(x_1, \dots, x_n)$ such that each x_i appears in every term in $p(x_1, \dots, x_n)$. By a word $w(x_1, \dots, x_n)$ we mean a product in which each factor is x_i , for some i . Let $X \subseteq \mathcal{X}_n$. An associative ring R is called an X -ring if, for all a_1, \dots, a_n in R , there exists a polynomial $p(x_1, \dots, x_n)$ in X and a word $w(x_1, \dots, x_n)$ with some x_j (j varies) missing from $w(x_1, \dots, x_n)$, such that

$$(3) \quad \begin{aligned} p(a_1, \dots, a_n) &= w(a_1, \dots, a_n), \text{ some } a_j \text{ missing from} \\ &w(a_1, \dots, a_n). \end{aligned}$$

A division ring (respectively, primitive ring, semisimple ring) which is also an X -ring is called an X -division ring (respectively, X -primitive ring, X -semisimple ring).

The following lemma is immediate from the definition of an X -ring.

LEMMA 1. (a) If $X_1 \subseteq X_2$, then any X_1 -ring is also an X_2 -ring.
 (b) Any subring and any homomorphic image of an X -ring is also an X -ring.

In preparation for the proofs of the main results, we first establish the following lemmas.

LEMMA 2. Suppose that $X \subseteq \mathcal{X}_n$ and D is an X -division ring. Then D is of prime characteristic.

Proof. Suppose that the characteristic of the X -division ring D is zero. Then D contains the rationals. Suppose that q_1, \dots, q_n are the first n primes. Then, by hypothesis,

$$(4) \quad p(q_1, \dots, q_n) = w(q_1, \dots, q_n),$$

where each term in the polynomial $p(x_1, \dots, x_n)$ involves every x_i , while some x_j is missing from the word $w(x_1, \dots, x_n)$. Thus, q_j divides the left side of (4) but q_j does not divide the right side of (4), a contradiction. This contradiction proves the lemma.

LEMMA 3. Let R be a \mathcal{X}_n -primitive ring. Then R is a complete matrix ring D_q over a division ring D of prime characteristic.

Proof. Let R be a \mathcal{X}_n -primitive ring. Then, by Jacobson's Density Theorem [3; p. 33], either (i) $R \cong$ a complete matrix ring D_q over a division ring D , or (ii) for every positive integer l , there

exists a subring S of R such that S maps homomorphically onto D_i for some division ring D . We now show that (ii) never holds. For, suppose (ii) is true. Then, by taking $l = n$ in (ii) and by using Lemma 1(b), we readily obtain

$$(5) \quad D_n \text{ is a } \mathcal{V}_n\text{-ring}.$$

Now, let

$$(6) \quad a_i = \begin{bmatrix} 1 & 1 & & & & & & \\ & & 1 & & & & & \\ & & & \ddots & & & & \\ & & & & 0 & & & \circ \\ & \circ & & & & 1 & & \\ & & & & & & 1 & \\ & & & & & & & \ddots \\ & & & & & & & & 1 \end{bmatrix}, (i = 1, \dots, n),$$

where a_i is a diagonal $n \times n$ matrix over D with an entry of 0 in the (i, i) position and with entries of 1 elsewhere on the main diagonal. By hypothesis, there exists a polynomial $p(x_1, \dots, x_n)$ and a word $w(x_1, \dots, x_n)$ such that

$$(7) \quad \begin{cases} p(a_1, \dots, a_n) = w(a_1, \dots, a_n); \text{ each } a_i \text{ appears in every} \\ \text{term in } p(a_1, \dots, a_n); \text{ some } a_j \text{ is missing from } w(a_1, \\ \dots, a_n). \end{cases}$$

Keeping in mind (6), and comparing the entries in the (j, j) positions of the two matrices in the equation in (7), we obtain $0 = 1$, a contradiction. This contradiction shows that (ii) above *never* holds, and hence (i) above holds always. We have thus shown that

$$(8) \quad \begin{cases} \text{The ground } \mathcal{V}_n\text{-primitive ring } R \text{ is a complete matrix} \\ \text{ring } D_q \text{ over a division ring } D. \end{cases}$$

Moreover, D , as a subring of $R(=D_q)$, is a \mathcal{V}_n -division ring (see Lemma 1(b)), and hence, by Lemma 2, D is of prime characteristic. This proves the lemma.

LEMMA 4. *The direct sum of n rings R_i each of which has a unit-element is not a \mathcal{V}_n -ring.*

Proof. Suppose that

$$(9) \quad R \cong R_1 \dot{+} \dots \dot{+} R_n; \text{ each } R_i \text{ has a unit-element}.$$

Let

$$a_i = (1, 1, \dots, 1, 0, 1, 1, \dots, 1); 0 \text{ is in the } i\text{th position}.$$

An argument similar to the one given in the proof of Lemma 3

shows that we obtain a contradiction if we assume that R is a \mathcal{V}_n -ring. This proves the lemma.

We are now in a position to prove the following

THEOREM 1. *Let $X \subseteq \mathcal{V}_n$. Then every X -semisimple ring is finite if and only if every X -division ring of prime characteristic is finite.*

Proof. The “only if” part of the theorem being obvious, we now proceed to prove the “if” part. Thus, suppose that

(10) Every X -division ring of prime characteristic is finite.

Suppose, further, that R is an X -semisimple ring which is *not* finite. We shall show that this leads to a contradiction. Since R is semi-simple, there exist ideals $I_\alpha (\alpha \in \Omega)$ of R such that [3; p. 14]

$$\bigcap_{\alpha \in \Omega} I_\alpha = (0); \text{ each } R/I_\alpha \text{ is primitive.}$$

Now, by Lemma 1 and Lemma 3, it readily follows that R/I_α is a complete matrix ring D_q over a division ring D of prime characteristic. Since D is a subring of $R/I_\alpha (= D_q)$, it follows, by Lemma 1(b), that D is an X -division ring of prime characteristic, and hence D is finite, by (10). Therefore,

(11) $R/I_\alpha (= D_q)$ is finite.

Now, choose $\alpha_1 \in R$, and having chosen $\alpha_1, \dots, \alpha_k$ so that

$$(12) \quad \sum_{i=1}^k R/I_{\alpha_i} \cong R/\bigcap_{i=1}^k I_{\alpha_i},$$

choose $\alpha_{k+1} \in \Omega$ such that $\bigcap_{i=1}^k I_{\alpha_i} \not\subseteq I_{\alpha_{k+1}}$. That such α_{k+1} can always be so chosen is proved as follows: suppose no such α_{k+1} exists. Then $(0) = \bigcap_{\alpha \in \Omega} I_\alpha = \bigcap_{i=1}^k I_{\alpha_i}$, and hence (see (12))

$$R \cong R/\bigcap_{i=1}^k I_{\alpha_i} \cong \sum_{i=1}^k R/I_{\alpha_i}.$$

Thus, using (11), we see that R is finite, a contradiction. This contradiction shows that there exists $\alpha_{k+1} \in \Omega$ such that $\bigcap_{i=1}^k I_{\alpha_i} \not\subseteq I_{\alpha_{k+1}}$. Now, as we have seen in (11), $R/I_{\alpha_{k+1}}$ is simple. Since, moreover, $\bigcap_{i=1}^k I_{\alpha_i} \not\subseteq I_{\alpha_{k+1}}$, we have $\bigcap_{i=1}^k I_{\alpha_i} + I_{\alpha_{k+1}} = R$. Hence, by applying the second isomorphism theorem, we readily verify that

$$R/\bigcap_{i=1}^{k+1} I_{\alpha_i} \cong R/\bigcap_{i=1}^k I_{\alpha_i} + R/I_{\alpha_{k+1}} \cong \sum_{i=1}^{k+1} R/I_{\alpha_i},$$

by (12). In particular, we have

$$\sum_{i=1}^n R/I_{\alpha_i} \cong R/\bigcap_{i=1}^n R/I_{\alpha_i}.$$

Hence, using Lemma 1(b), $\sum_{i=1}^n R/I_{\alpha_i}$ is an X -ring (and thus a \mathcal{V}_n -ring) also. This, however, contradicts Lemma 4 (see (11)). This contradiction shows that R is finite, and the theorem is proved.

We call a field F *periodic* if for every x in F , we have $x^m = x^n$ for some positive integers $m, n, m \neq n$. A periodic field which is also an X -ring is called an *X -periodic field*. We now prove the following

THEOREM 2. *Let $X \subseteq \mathcal{V}_n$. Suppose that there exists a fixed integer N such that, for all polynomials $p(x_1, \dots, x_n)$ in X , the degree in x_1, \dots, x_n of every term in $p(x_1, \dots, x_n)$ is less than N . Then, every X -semisimple ring is finite if and only if every X -periodic field is finite.*

Proof. The “only if” part of the theorem being obvious, we now proceed to prove the “if” part. Thus, suppose that R is an X -semisimple ring. Now, in view of Theorem 1, it suffices to show that

$$(13) \quad \begin{cases} \text{Every } X\text{-division ring } D \text{ of prime characteristic is} \\ \text{a periodic field.} \end{cases}$$

Thus, suppose that D is an X -division ring of prime characteristic p , and suppose $a \in D$. We first show that

$$(14) \quad a \text{ is algebraic over } GF(p).$$

Clearly, we may assume that $a \neq 0$. Now, suppose that

$$(15) \quad q_1, \dots, q_n \text{ are fixed distinct primes; each } q_i > N, \text{ and}$$

$$(16) \quad h_i = (q_1 \cdots q_n)/q_i; (i = 1, \dots, n).$$

Then

$$(17) \quad q_j \text{ divides } h_i \text{ if and only if } i \neq j.$$

Let $b_i = a^{h_i}$. Then since D is an X -ring there exists a polynomial $p(x_1, \dots, x_n) \in X$, and a word $w(x_1, \dots, x_n)$ with some x_k missing such that

$$(18) \quad p(b_1, \dots, b_n) = w(b_1, \dots, b_n).$$

Since x_k is missing from $w(x_1, \dots, x_n)$ we have by (17),

$$(19) \quad w(b_1, \dots, b_n) = a^t; q_k | t.$$

Now let d_{ir} be the degree of x_i in the r th term of $p(x_1, \dots, x_n)$. Then each $d_{ir} > 0$ and

$$(20) \quad p(b_1, \dots, b_n) = \sum_r m_r a^{c_r} \text{ where } c_r = \sum_{i=1}^n d_{ir} h_i \text{ and } m_r \text{ are some integers.}$$

By hypothesis each $d_{ir} < N$ and thus, by (15), $q_k > d_{ir}$. We therefore have, by (17), that $q_k \nmid c_r$ for every r . In particular, by (19), $c_r \neq t$ for any r . We now have, by a combination of (18), (19) and (20),

$$(21) \quad \sum_r m_r a^{c_r} = a^t, c_r \neq t \text{ for all } r.$$

Hence a is algebraic over $GF(p)$ and (14) is proved.

Now, consider the field $(GF(p))(a)$. Since, by (14), a is algebraic over $GF(p)$, it is easily seen that $(GF(p))(a)$ is a finite field, and hence

$$a^m = a^n; m, n \text{ positive integers; } m \neq n; (a \in D).$$

Thus, by Jacobson's Theorem [3], D is a periodic field. The theorem now follows from Theorem 1.

In preparation for the proof of the next theorem, we now introduce the following notations and lemmas.

Suppose a and b are positive integers, $a > b$, which are relatively prime, and suppose

$$(22) \quad V_n = a^n - b^n, (a > b \geq 1; (a, b) = 1).$$

Let n_1, n_2, \dots, n_k be all the distinct positive divisors of n which are less than n . Then V_n is divisible by $V_{n_1}, V_{n_2}, \dots, V_{n_k}$. A divisor of V_n which is relatively prime to all of the $V_{n_i} (i = 1, \dots, k)$ is called a *primitive divisor* of V_n . For example, 5 is a primitive divisor of $2^4 - 1^4$.

The following lemma was proved by Birkhoff and Vandiver [1];

LEMMA 5. *Let n be a positive integer, $n \neq 2$, and let V_n be as in (22). Then V_n has at least one primitive divisor other than unity, with the single exception $V_n = 2^6 - 1^6$.*

Next we introduce the following

NOTATION. Z^+ will denote the set of all positive integers. Let $s \in Z^+$. Then,

$$D(s) = \{m | m \in Z^+, m \text{ divides } s\};$$

$$P(s) = \{m | m \in D(s), m \text{ is prime}\}.$$

If S is any nonempty subset of Z^+ , then

$$D(S) = \bigcup_{s \in S} D(s) \quad \text{and} \quad P(S) = \bigcup_{s \in S} P(s).$$

The following lemma is an immediate consequence of Lemma 5.

LEMMA 6. *Let $p \in Z^+$, $p > 1$, and let $\{k_i | i \in Z^+\}$ be a strictly increasing sequence of positive integers such that k_i divides k_{i+1} for each i . Let*

$$S = \{p^{k_i} - 1 | i \in Z^+\}.$$

Then $P(S)$ is infinite.

We are now in a position to prove the following

THEOREM 3 (Principal Theorem). *Let $X \subseteq \mathcal{V}_n$. Suppose that there exists a fixed integer N such that, for all polynomials $p(x_1, \dots, x_n)$ in X , the degree in x_1, \dots, x_n of every term in $p(x_1, \dots, x_n)$ is less than N . Suppose, further, that for all polynomials $p(x_1, \dots, x_n)$ in X , each x_i is of the same degree in each term in $p(x_1, \dots, x_n)$. Then every X -semisimple ring is finite.*

Proof. In view of Theorem 2, it suffices to show that every X -periodic field F is finite. Suppose not; that is, suppose that F is an infinite X -periodic field. Then F is of prime characteristic p , since F is periodic. Moreover, the subfield $\langle x \rangle$ generated by a single element x in F is finite, and hence

$$(23) \quad x^{p^k} = x \text{ for some positive integer } k = k(x).$$

Now, for each $j \in Z^+$, define

$$(24) \quad F_j = \{x | x \in F, x^{p^{j!}} = x\}.$$

Then, in view of (23) and (24), we have (since if $x \in F$ satisfies (23), then $x \in F_k$)

$$(25) \quad F_1 \subseteq F_2 \subseteq F_3 \subseteq \dots; \text{ each } F_i \text{ is a finite subfield of } F; \\ \bigcup_{i \in Z^+} F_i = F.$$

Now, since F is infinite, we can find a subsequence of (25) such that

$$(26) \quad F_{i_1} \subsetneq F_{i_2} \subsetneq F_{i_3} \subsetneq \dots, \text{ and again } \bigcup_{k \in Z^+} F_{i_k} = F.$$

Moreover, the order of $F_{i_\sigma} = p^{k_\sigma}(\sigma \in Z^+)$. Next, let

$$S = \{p^{k_\sigma} - 1 | \sigma \in Z^+\}.$$

Then, as is well known, $k_\sigma | k_{\sigma+1}$ for each $\sigma \in Z^+$, and $k_\sigma < k_{\sigma+1}$, by (26). Hence by Lemma 6, $P(S)$ is infinite, and there, therefore, exist n distinct primes q_1, \dots, q_n in $P(S)$, such that

$$(27) \quad q_i > N + p, \quad (i = 1, \dots, n).$$

Thus, there exists $m_j \in Z^+$ such that

$$q_j \in P(p^{k_{m_j}} - 1), \quad (j = 1, \dots, n).$$

Now, since the nonzero elements of the field $F_{i_{m_j}}$ form a multiplicative group of order $p^{k_{m_j}} - 1$, and since the prime $q_j | p^{k_{m_j}} - 1$, it follows, by Cauchy's theorem, that there exists $a_j \in F_{i_{m_j}} (\subseteq F)$ such that

$$(28) \quad \text{order of } a_j = q_j; a_j \neq 0 \quad (j = 1, \dots, n).$$

Now, since F is an X -ring, there exists a polynomial $p(x_1, \dots, x_n)$ in X and a word $w(x_1, \dots, x_n)$ such that

$$(29) \quad \begin{cases} p(a_1, \dots, a_n) = w(a_1, \dots, a_n); \text{ each } x_i \text{ appears in every} \\ \text{term in } p(x_1, \dots, x_n); \text{ some } x_j \text{ is missing from } w(x_1, \dots, x_n); \\ \text{all coefficients in } p(x_1, \dots, x_n) \text{ are integers.} \end{cases}$$

Moreover, recalling that F is commutative, and using the hypothesis regarding the degrees of the x_i 's in the various terms of $p(x_1, \dots, x_n)$, we see that

$$(30) \quad \begin{cases} p(a_1, \dots, a_n) = m w_1(a_1, \dots, a_n); m \text{ an integer;} \\ w_1(a_1, \dots, a_n) \text{ a word involving every } a_i. \end{cases}$$

Furthermore, $m \neq 0$, since $w(a_1, \dots, a_n) \neq 0$ (see (29), (30) and recall that each $a_i \neq 0$). Hence, by Fermat's Little Theorem (recall that F is of prime characteristic p), we have

$$(31) \quad m^{p-1} = 1.$$

Now, let c_j be the degree of x_j in the word $w_1(x_1, \dots, x_n)$. Then, by hypothesis,

$$(32) \quad c_j < N; \quad (j = 1, \dots, n).$$

Let

$$(33) \quad M = \frac{q_1 \cdots q_n}{q_j} \cdot (p - 1).$$

Then, by (29), (30),

$$(34) \quad (m w_1(a_1, \dots, a_n))^M = (w(a_1, \dots, a_n))^M.$$

Hence by (31), (28), (33), and the fact that a_j is missing from the

word $w(a_1, \dots, a_n)$, the above equality reduces to

$$(a_j^{c_j})^M = 1.$$

Therefore (see (28)), q_j divides $c_j M$. This is absurd, however, since q_j does *not* divide c_j (recall that $q_j > N > c_j$; see (27), (32)), and q_j does *not* divide M (recall that $q_j > p$, by (27); also see (33)). This contradiction proves the theorem.

Next, we prove the following

THEOREM 4. *Let X be a collection of words in \mathcal{V}_n each of which is of degree $< N$ in x_1, \dots, x_n . If R is an X -ring with Jacobson radical J , then J is a nil ring of bounded index, and R/J is finite.*

Proof. Clearly, X satisfies the hypotheses of Theorem 3, and hence the X -semisimple ring R/J is finite. Now, to prove that J is nil, let $a \in J$, and suppose that

$$(35) \quad q_1, \dots, q_n \text{ are distinct primes, each } q_i > N.$$

Let

$$(36) \quad h_i = \frac{q_1 \cdots q_n}{q_i}; \quad (i = 1, \dots, n),$$

and let

$$(37) \quad b_i = a^{h_i}; \quad (i = 1, \dots, n).$$

Then, since R is an X -ring, there exist words $w_1(x_1, \dots, x_n)$ and $w(x_1, \dots, x_n)$ such that

$$(38) \quad \begin{cases} w_1(b_1, \dots, b_n) = w(b_1, \dots, b_n); w_1(x_1, \dots, x_n) \in X; \\ \text{some } x_j \text{ is missing from } w(x_1, \dots, x_n). \end{cases}$$

Now, let

$$(39) \quad \text{degree of } x_i \text{ in } w_1(x_1, \dots, x_n) = c_i; \quad (i = 1, \dots, n).$$

Then, by (38), (37), (39), we obtain

$$(40) \quad a^{c_1 h_1 + \cdots + c_n h_n} = a^t.$$

Moreover, since x_j is *missing* from the word $w(x_1, \dots, x_n)$, it is easily seen (see (36)) that

$$(41) \quad q_j \text{ divides } t.$$

On the other hand, since $q_j > N$, by (35), and $c_j < N$ (since $w_1(x_1, \dots, x_n) \in X$), q_j does *not* divide c_j . Also, by (36), q_j does *not* divide

h_j , and hence the prime q_j does not divide $c_j h_j$. However, by (36), q_j divides h_i for each $i \neq j$. Therefore,

$$(42) \quad q_j \text{ does not divide } c_1 h_1 + \cdots + c_n h_n .$$

Comparing (41), (42), we see that

$$(43) \quad c_1 h_1 + \cdots + c_n h_n \neq t .$$

Now, let $c_1 h_1 + \cdots + c_n h_n = l$, and let

$$(44) \quad M = N h_1 + \cdots + N h_n; (M > l, \text{ since each } c_i < N) .$$

Then, by (40), (43), (44), it is easily seen that

$$(45) \quad a^M = a^s, \text{ for some positive integer } s; s \neq M .$$

Now, if in (45), $s < M$, by iterating in (45), we can eventually make $s > M$. We have thus shown that

$$(46) \quad a^M = a^s; s > M > 0; M \text{ fixed} .$$

Equation (46) readily implies that a suitable power of a is an idempotent element in J (recall that a is in J), and hence by (46), $a^M = 0$, (M fixed). Thus J is nil of bounded index, and the theorem is proved.

In view of Theorem 4, it follows that J is locally nilpotent [2; p. 28].

The following corollary is an immediate consequence of Theorem 4 as well as Theorem 3.

COROLLARY 1. *Let X consist of a single fixed word involving each of the variables x_1, \dots, x_n . Then every X -semisimple ring is finite.*

If, further, we let X consist of the single fixed word $x_1 \cdots x_n$, we obtain, as a further corollary of Theorem 4, the following result which has already been proved by the authors [5]:

COROLLARY 2. *Let R be an associative ring with Jacobson radical J and with the property that, for all x_1, \dots, x_n in R , there exists a word $w(x_1, \dots, x_n)$ depending on x_1, \dots, x_n , in which at least one x_i (i varies) is missing, and such that $x_1 \cdots x_n = w(x_1, \dots, x_n)$. Then J is a nil ring of bounded index and R/J is finite.*

2. Examples and remarks. In the following examples, we show that the class of X -rings subsumes all finite rings and all nilpotent rings. We also give an example of an X -ring which is neither finite

nor nilpotent.

EXAMPLE 1. Let R be any finite ring with exactly m elements. Let x_1, \dots, x_{m+1} be any elements of R . Then $x_i = x_j$ for some $i > j$, and hence

$$\begin{aligned} x_1 \cdots x_{m+1} &= x_1 \cdots x_j \cdots x_{i-1} x_j x_{i+1} \cdots x_{m+1} \\ &= w(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_{m+1}). \end{aligned}$$

Thus R is an X -ring, where $X = \{x_1 \cdots x_{m+1}\}$.

EXAMPLE 2. Let R be any nilpotent ring, say $R^m = (0)$. Then, for all elements x_1, \dots, x_{m+1} of R , we have

$$x_1 \cdots x_{m+1} = 0 = x_1 \cdots x_m.$$

Thus R is an X -ring, where $X = \{x_1 \cdots x_{m+1}\}$.

EXAMPLE 3. Let R_0 be an infinite field of characteristic 2, and let

$$R = \left\{ \begin{pmatrix} a & u \\ 0 & 0 \end{pmatrix} \mid a \in GF(2), u \in R_0 \right\}.$$

Let x_1, x_2, x_3 be any elements of R . Then, as is readily verified,

$$\begin{aligned} x_1 x_2 x_3 &= x_2 x_3 \quad \text{if} \quad x_1 = \begin{pmatrix} 1 & u \\ 0 & 0 \end{pmatrix}; \\ x_1 x_2 x_3 &= x_1 x_2 \quad \text{if} \quad x_1 = \begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix}. \end{aligned}$$

Hence R is an X -ring, where $X = \{x_1 x_2 x_3\}$. Observe that R is neither finite nor nilpotent. In fact, R is not isomorphic to any finite direct sum of finite or nilpotent rings.

Returning to our Principal Theorem (Theorem 3), we have the following

REMARK. In the proof of Theorem 3, we showed that every X -periodic field is finite. We claim that the group-theoretic analogue of this result is false. To see this, consider the group $Z(p^\infty)$, which consists of the set of all p^n th roots of unity, where p is a fixed prime and $n = 0, 1, 2, \dots$ [4, p. 4]. Suppose that $x_1, x_2 \in Z(p^\infty)$. Then, for some integer n , $x_1, x_2 \in Z(p^n)$, where $Z(p^n)$ is the group of all p^n th roots of unity. Let σ be a generator of $Z(p^n)$. Then

$$x_1 = \sigma^r, x_2 = \sigma^s; 1 \leq r \leq p^n, 1 \leq s \leq p^n.$$

Now let

$$r = r_0 p^i, s = s_0 p^j; (r_0, p) = 1, (s_0, p) = 1,$$

and suppose, without loss of generality, that $i \leq j$. Since $(r/p^i, p) = 1$, there exists a solution x to

$$(r/p^i)x \equiv s/p^j \pmod{p^n},$$

and hence $rxp^{j-i} \equiv s \pmod{p^n}$. Thus, $r + s \equiv r(1 + xp^{j-i}) \pmod{p^n}$, and hence

$$\sigma^{r+s} = (\sigma^r)^{1+xp^{j-i}},$$

since $\sigma^{p^n} = 1$. Therefore $x_1 x_2 = (x_1)^{1+xp^{j-i}}$. Note that $Z(p^\infty)$ is an infinite group.

We leave as an open question whether or not Corollary 1 is true when X consists of a single fixed polynomial in which each term involves every variable x_1, \dots, x_n . In view of Theorem 2, this question reduces to whether or not an X -periodic field is finite in this case.

REFERENCES

1. G. D. Birkhoff and H. S. Vandiver, *On the integral divisors of $a^n - b^n$* , Annals of Math., **5** (1903), 173-180.
2. I. N. Herstein, *Theory of rings*, Math. Lecture Notes, University of Chicago, Chicago, Ill. 1961.
3. N. Jacobson, *Structure of rings*, rev. ed., Amer. Math. Soc. Colloq. Publ., vol. **37**, Amer. Math. Soc., Providence, R. I. 1964.
4. I. Kaplansky, *Infinite abelian groups*, Univ. of Michigan Press, Ann Arbor, Mich., 1954.
5. M. S. Putcha and A. Yaqub, *Rings satisfying monomial constraints*, Proc. Amer. Math. Soc., **39** (1) (1973), 10-18.

Received October 18, 1974.

UNIVERSITY OF CALIFORNIA, BERKELEY

AND

UNIVERSITY OF CALIFORNIA, SANTA BARBARA

PACIFIC JOURNAL OF MATHEMATICS

EDITORS

RICHARD ARENS (Managing Editor)

University of California
Los Angeles, California 90024

J. DUGUNDJI

Department of Mathematics
University of Southern California
Los Angeles, California 90007

R. A. BEAUMONT

University of Washington
Seattle, Washington 98105

D. GILBARG AND J. MILGRAM

Stanford University
Stanford, California 94305

ASSOCIATE EDITORS

E. F. BECKENBACH

B. H. NEUMANN

F. WOLF

K. YOSHIDA

SUPPORTING INSTITUTIONS

UNIVERSITY OF BRITISH COLUMBIA
CALIFORNIA INSTITUTE OF TECHNOLOGY
UNIVERSITY OF CALIFORNIA
MONTANA STATE UNIVERSITY
UNIVERSITY OF NEVADA
NEW MEXICO STATE UNIVERSITY
OREGON STATE UNIVERSITY
UNIVERSITY OF OREGON
OSAKA UNIVERSITY

UNIVERSITY OF SOUTHERN CALIFORNIA
STANFORD UNIVERSITY
UNIVERSITY OF TOKYO
UNIVERSITY OF UTAH
WASHINGTON STATE UNIVERSITY
UNIVERSITY OF WASHINGTON
* * *
AMERICAN MATHEMATICAL SOCIETY

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

The Pacific Journal of Mathematics expects the author's institution to pay page charges, and reserves the right to delay publication for nonpayment of charges in case of financial emergency.

100 reprints are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is issued monthly as of January 1966. Regular subscription rate: \$72.00 a year (6 Vols., 12 issues). Special rate: \$36.00 a year to individual members of supporting institutions.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley, California, 94708.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), 270, 3-chome Totsuka-cho, Shinjuku-ku, Tokyo 160, Japan.

Copyright © 1975 by Pacific Journal of Mathematics
Manufactured and first issued in Japan

Norman Larrabee Alling, <i>On Cauchy's theorem for real algebraic curves with boundary</i>	315
Daniel D. Anderson, <i>A remark on the lattice of ideals of a Prüfer domain</i>	323
Dennis Neal Barr and Peter D. Miletta, <i>A necessary and sufficient condition for uniqueness of solutions to two point boundary value problems</i>	325
Ladislav Beran, <i>On solvability of generalized orthomodular lattices</i>	331
L. Carlitz, <i>A three-term relation for some sums related to Dedekind sums</i>	339
Arthur Herbert Copeland, Jr. and Albert Oscar Shar, <i>Images and pre-images of localization maps</i>	349
G. G. Dandapat, John L. Hunsucker and Carl Pomerance, <i>Some new results on odd perfect numbers</i>	359
M. Edelstein and L. Keener, <i>Characterizations of infinite-dimensional and nonreflexive spaces</i>	365
Francis James Flanigan, <i>On Levi factors of derivation algebras and the radical embedding problem</i>	371
Harvey Friedman, <i>Provable equality in primitive recursive arithmetic with and without induction</i>	379
Joseph Braucher Fugate and Lee K. Mohler, <i>The fixed point property for tree-like continua with finitely many arc components</i>	393
John Norman Ginsburg and Victor Harold Saks, <i>Some applications of ultrafilters in topology</i>	403
Arjun K. Gupta, <i>Generalisation of a "square" functional equation</i>	419
Thomas Lee Hayden and Frank Jones Massey, <i>Nonlinear holomorphic semigroups</i>	423
V. Kannan and Thekkedath Thiruvikraman, <i>Lattices of Hausdorff compactifications of a locally compact space</i>	441
J. E. Kerlin and Wilfred Dennis Pepe, <i>Norm decreasing homomorphisms between group algebras</i>	445
Young K. Kwon, <i>Behavior of Φ-bounded harmonic functions at the Wiener boundary</i>	453
Richard Arthur Levaro, <i>Projective quasi-coherent sheaves of modules</i>	457
Chung Lin, <i>Rearranging Fourier transforms on groups</i>	463
David Lowell Lovelady, <i>An asymptotic analysis of an odd order linear differential equation</i> ...	475
Jerry Malzan, <i>On groups with a single involution</i>	481
J. F. McClendon, <i>Metric families</i>	491
Carl Pomerance, <i>On multiply perfect numbers with a special property</i>	511
Mohan S. Putcha and Adil Mohamed Yaqub, <i>Polynomial constraints for finiteness of semisimple rings</i>	519
Calvin R. Putnam, <i>Hyponormal contractions and strong power convergence</i>	531
Douglas Conner Ravenel, <i>Multiplicative operations in BP*BP</i>	539
Judith Roitman, <i>Attaining the spread at cardinals which are not strong limits</i>	545
Kazuyuki Saitô, <i>Groups of *-automorphisms and invariant maps of von Neumann algebras</i>	553
Brian Kirkwood Schmidt, <i>Homotopy invariance of contravariant functors acting on smooth manifolds</i>	559
Kenneth Barry Stolarsky, <i>The sum of the distances to N points on a sphere</i>	563
Mark Lawrence Teply, <i>Semiprime rings with the singular splitting property</i>	575
J. Pelham Thomas, <i>Maximal connected Hausdorff spaces</i>	581
Charles Thomas Tucker, II, <i>Concerning σ-homomorphisms of Riesz spaces</i>	585
Rangachari Venkataraman, <i>Compactness in abelian topological groups</i>	591
William Charles Waterhouse, <i>Basically bounded functors and flat sheaves</i>	597
David Westreich, <i>Bifurcation of operator equations with unbounded linearized part</i>	611
William Robin Zame, <i>Extendibility, boundedness and sequential convergence in spaces of holomorphic functions</i>	619