PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 39, Number 1, June 1973

RINGS SATISFYING MONOMIAL CONSTRAINTS

MOHAN S. PUTCHA[1] AND ADIL YAQUB

ABSTRACT. The following theorem is proved: Suppose R is an associative ring and suppose J is the Jacobson radical of R. Suppose that for all $x_1, \cdots, x_n$ in R, there exists a word $w_{x_1,\cdots,x_n}(x_1, \cdots, x_n)$, depending on $x_1, \cdots, x_n$, in which at least one x_i (i varies) is missing, and such that $x_1 \cdots x_n = w_{x_1,\cdots,x_n}(x_1, \cdots, x_n)$. Then J is a nil ring of bounded index and R/J is finite. It is further proved that a commutative nil semigroup satisfies the above identity if and only if it is nilpotent.

In this paper, we investigate the structure of an associative ring R with the property that, for all $x_1, \cdots, x_n$ in R, $x_1 \cdots x_n = w_{x_1,\cdots x_n}(x_1, \cdots, x_n)$, where w is a word, depending on $x_1, \cdots, x_n$, and where some x_i (i varies) is missing in w. For such a ring R, we prove the Jacobson radical J is a nil ring of bounded index. We also show that R/J is finite. Finally, we show that a commutative nil semigroup satisfies the above identity if and only if it is nilpotent.

In preparation for the proofs of the main results, we first introduce

DEFINITION 1. Let n be a positive integer, and let S be a semigroup. We say that S is a β_n-semigroup if, for all $x_1, \cdots, x_n$ in S, there exists a word $w_{x_1,\cdots,x_n}(x_1, \cdots, x_n)$ consisting of a product of the x_i's with some x_j (j varies) missing, such that $x_1 \cdots x_n = w_{x_1,\cdots,x_n}(x_1, \cdots, x_n)$. A ring R is called a β_n-ring if its multiplicative semigroup is a β_n-semigroup.

LEMMA 1. *Let S be a finite semigroup or a nilpotent semigroup. Then S is a β_n-semigroup, for some n.*

PROOF. First, suppose S is finite, of order n, and suppose $x_1, \cdots, x_{n+1}$ are any elements of S. Then $x_i = x_j$ for some $i > j$, and hence

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

Thus S is a β_{n+1}-semigroup. Next, suppose S is nilpotent, say, $S^m = (0)$.

Presented to the Society, January 18, 1972; received by the editors August 10, 1971 and, in revised form, October 6, 1971.

AMS (MOS) subject classifications (1970). Primary 16A38, 16A48; Secondary 20M10.

[1] The author was supported by a National Science Foundation Graduate Fellowship.

Then, for all elements $x_1, \cdots, x_{m+1}$ of S, we have

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

Thus S is a β_{m+1}-semigroup, and the lemma is proved.

We now pause to give an example of a β_n-ring which is not of the type described in Lemma 1. To this end, let R_0 be an infinite field of characteristic 2, and let

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

It is readily verified that R is a β_3-ring. Indeed, $x_1x_2x_3 = x_2x_3$ if

$$x_1 = \begin{pmatrix} 1 & u \\ 0 & 0 \end{pmatrix},$$

while $x_1x_2x_3 = x_1x_2$ if

$$x_1 = \begin{pmatrix} 0 & u \\ 0 & 0 \end{pmatrix}.$$

Moreover, R is neither finite nor nilpotent and, in fact, R is not isomorphic to any finite direct sum of finite or nilpotent rings. (An example of an *infinite* β_n-group is given in Remark 1 below.)

LEMMA 2. *Let S be a β_n-semigroup. Then any subsemigroup of S and any homomorphic image of S are also β_n-semigroups.*

This follows at once from the definition.

LEMMA 3. *Let S be a β_n-semigroup. Then there exists a fixed positive integer k with the property that, for any a in S, there is an integer $l > k$ such that $a^k = a^l$.*

PROOF. Let $q_1, \cdots, q_n$ be the first n positive primes, and let

$$m_i = (q_1 \cdots q_n)/q_i \qquad (i = 1, \cdots, n). \tag{1}$$

Let $k = m_1 + \cdots + m_n$. Now, since S is a β_n-semigroup, there exists a word $w(a^{m_1}, \cdots, a^{m_n})$, *with some a^{m_j} missing in the word w*, such that

$$a^k = (a^{m_1}) \cdots (a^{m_n}) = w(a^{m_1}, \cdots, a^{m_n}) \equiv a^l. \tag{2}$$

Since a^{m_j} is missing from w, it follows, by (1), that q_j divides l. But, by (1) again, q_j does not divide k, and hence $l \neq k$. Now, if in (2), $l < k$, then by iterating in (2), we can make $l > k$. This proves the lemma.

Notation 1. Let Z^+ denote the set of all positive integers, and let

$$D(s) = \{m \mid m \in Z^+, m \text{ divides } s\}; \qquad P(s) = \{m \mid m \in D(s), m \text{ is prime}\}.$$

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

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

LEMMA 4. *Let S be any infinite set of positive integers and let $P(S)$ be finite. Then there exists $q \in P(S)$ such that $q^i \in D(S)$ for all $i \in Z^+$.*

PROOF. If the lemma were false, then $D(S)$ would be finite, since $P(S)$ is finite. But $D(S)$ is infinite, since $D(S) \supseteq S$.

In preparation for the proof of the next lemma, we first state the following two well-known results. The proof of Lemma A appears in [**4**, p. 164], while the proof of Lemma B appears in [**6**, p. 2].

LEMMA A. *Let a be an integer and n an integer >1. Let $\Phi_n(x)$ denote the cyclotomic polynomial of order n* [**5**, p. 60]. *If a prime number p divides $\Phi_n(a)$, then either $p|n$ or $n|p-1$.*

LEMMA B. *Let l be a prime number and a an integer >1. Then $\Phi_{l^\nu}(a)$ is a multiple of l if and only if $a\equiv 1 \bmod l$. If $a \equiv 1 \bmod l$, then the l-order of $\Phi_{l^\nu}(a)$ is equal to 1 except in the case where $l=2$, $\nu=1$, and $a\equiv 3 \bmod 4$. For any ν, $\mu>0$, $\nu\neq\mu$, G.C.D.$(\Phi_{l^\mu}(a), \Phi_{l^\nu}(a))=1$ or l.*

COROLLARY. *Let l be a prime number, a an integer >1, and suppose $a\equiv 1 \bmod l$. Then there exist infinitely many prime numbers dividing $\Phi_{l^{\nu_1}}(a), \Phi_{l^{\nu_2}}(a), \cdots$ for any increasing sequence $\nu_1, \nu_2, \cdots \to \infty$.*

We are now in a position to prove

LEMMA 5. *Let a be an integer >1 and let*

$$T = \{k_i \mid i \in Z^+\} \tag{3}$$

be a strictly increasing sequence of positive integers such that k_i divides k_{i+1} for each i. Let

$$S = \{a^{k_i} - 1 \mid i \in Z^+\}. \tag{4}$$

Then $P(S)$ is infinite.

PROOF. We distinguish two cases.

Case 1. $P(T)$ is infinite. Let $E_1=\{p_1, \cdots, p_l\}$ be a finite set of prime numbers, and $k_1', k_2', \cdots$ be the series of integers such that

$$k_n = p_1^{c_{1,n}} \cdots p_l^{c_{l,n}} k_n' \qquad (k_n', p_1 \cdots p_l) = 1.$$

Then, since $P(T)$ is infinite, $\lim_{n\to\infty} k_n' = \infty$. Hence, for any n with $k_n' \geqq \max(p_1, \cdots, p_l)$, we conclude, using Lemma A, that $p_1, \cdots, p_l$ do not divide $\Phi_{k_n'}(a)$. Moreover, since k_n' divides k_n, $\Phi_{k_n'}(a)$ divides $a^{k_n}-1$. Thus, if p is any prime divisor of $\Phi_{k_n'}(a)$, then p divides $a^{k_n}-1$ and, clearly, $p\neq p_i$ $(i=1, \cdots, l)$. Hence $P(S)$ is infinite.

Case 2. $P(T)$ is finite. In this case, we argue by contradiction. Thus suppose $P(S)$ is finite. Since $P(T)$ is finite, it follows by Lemma 4 that there exists $l \in P(T)$ such that

$$l^j \in D(T) \quad \text{for all } j \in Z^+. \tag{5}$$

Now, let

$$S' = \{a^{l^j} - 1 \mid j \in Z^+\}. \tag{6}$$

Then, by (5) and (3), $l^j | k_i$ for some k_i, and hence $a^{l^j} - 1 | a^{k_i} - 1$. Therefore $P(S') \subseteq P(S)$, and hence $P(S')$ is finite. Thus, there exists $k \in Z^+$ such that

$$P(a^{l^k} - 1) = P(a^{l^{k+1}} - 1). \tag{7}$$

Moreover, observe that $a^{l^{k+1}} - 1 = (a^{l^k} - 1)w$, where

$$w = (a^{l^k})^{l-1} + \cdots + (a^{l^k}) + 1. \tag{8}$$

Now, let $t \in P(w)$. Then $t \in P(a^{l^{k+1}} - 1) = P(a^{l^k} - 1)$, and hence $a^{l^k} \equiv 1 \bmod t$. Combining this with (8), we get $0 \equiv w \equiv l \bmod t$, and hence $t | l$. Therefore $t = l$. Moreover, by Fermat's Little Theorem, $a^l \equiv a \bmod l$ and hence $a^{l^k} \equiv a \bmod l$. Combining this with $a^{l^k} \equiv 1 \bmod t \ (=l)$, we obtain $a \equiv 1 \bmod l$. Hence, by the corollary to Lemma B, there exists infinitely many prime numbers dividing $\Phi_{l^{\nu_1}}(a)$, $\Phi_{l^{\nu_2}}(a), \cdots$ for any increasing sequence $\nu_1, \nu_2, \cdots \to \infty$. Moreover, since $\Phi_{l^{\nu_1}}(a)$ divides $a^{l^{\nu_1}} - 1$, and recalling (6), we conclude that $P(S')$ is infinite. But, as we have shown above, $P(S')$ is finite. This contradiction proves the lemma.

We call a field F *periodic* if, for every x in F, we have $x^m = x^n$ for some positive integers m, n, $m \neq n$.

THEOREM 1. *Suppose that F is a β_n-field. Then F is finite.*

PROOF. Suppose F is infinite. Since, by Lemma 3, F is periodic, F has a prime characteristic p. Moreover, the subfield $\langle x \rangle$ generated by a single element x in F is finite, and hence

$$x^{p^k} = x \quad \text{for some positive integer } k = k(x). \tag{9}$$

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

$$F_j = \{x \mid x \in F, x^{p^{j!}} = x\}. \tag{10}$$

Then, in view of (9) and (10), we have (since if $x \in F$ satisfies (9), then $x \in F_k$)

$$F_1 \subseteq F_2 \subseteq F_3 \subseteq \cdots; \text{ each } F_i \text{ is a subfield of } F; \bigcup_{i \in Z^+} F_i = F. \tag{11}$$

Now, since F is infinite, we can find a subsequence of (11) such that

(12) $$F_{i_1} \subsetneqq F_{i_2} \subsetneqq F_{i_3} \subsetneqq \cdots, \text{ and again } \bigcup_{k \in Z^+} F_{i_k} = F.$$

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

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

Then, as is well known, $k_\sigma | k_{\sigma+1}$ for each $\sigma \in Z^+$, and $k_\sigma < k_{\sigma+1}$, by (12). Hence, by Lemma 5, $P(S)$ is infinite, and there, therefore, exist n distinct primes $q_1, \cdots, q_n$ in $P(S)$. Thus, there exists $m_j \in Z^+$ such that

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

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 $x_j \in F_{i_{m_j}}$ ($\subseteq F$) such that

(14) $$\text{order of } x_j = q_j \qquad (j = 1, \cdots, n).$$

Moreover, since F is a β_n-field, there exists a word $w(x_1, \cdots, x_n)$, *with some* x_j *missing*, such that

(15) $$x_1 \cdots x_n = w(x_1, \cdots, x_n).$$

But, by (14), the order of $x_1 \cdots x_n = q_1 \cdots q_n$, while the order of $w(x_1, \cdots, x_n) \leqq (q_1 \cdots q_n)/q_j$ (since x_j does *not* appear in w), a contradiction. This contradiction proves the theorem.

COROLLARY 1. *Any β_n-division ring D is finite.*

PROOF. By Lemma 3, D is periodic, and hence, for any $x \in D$, we have $x^m = x^k$, for some $m, k, m \neq k$. Therefore, $x^{r(x)} = x$ for some $r(x) > 1$, and hence by Jacobson's Theorem [**2**, p. 217], D is a field. The corollary now follows at once from Theorem 1.

COROLLARY 2. *Any β_n-primitive ring R is finite.*

PROOF. By Jacobson's Density Theorem [**2**, p. 33], either $R \cong D_m$, where D_m is a complete matrix ring over a division ring D, in which case we are done by Corollary 1 and Lemma 2, or D_{n+1} is a homomorphic image of some subring R_0 of R. Now, by Lemma 2, D_{n+1} is a β_n-ring also. Let $x_i \in D_{n+1}$ be the matrix with 1 in the $(i, i+1)$ position and zero elsewhere:

(16) $$x_i = E_{i,i+1} \qquad (i = 1, \cdots, n).$$

It is readily verified that

(17) $$x_1 \cdots x_n = E_{1,n+1} \neq 0, \text{ and } x_i x_j \neq 0 \text{ if and only if } j = i + 1.$$

Since D_{n+1} is a β_n-ring, we have

(18) $$x_1 \cdots x_n = w(x_1, \cdots, x_n); \quad \text{some } x_j \text{ missing in } w.$$

In view of (17) and (18), we obtain $w(x_1, \cdots, x_n) \neq 0$ and thus (see (17))

(19) $w(x_1, \cdots, x_n) = x_\sigma x_{\sigma+1} x_{\sigma+2} \cdots x_{\sigma+\tau}$; $\sigma \neq 1$ or $\sigma + \tau \neq n$.

Hence, by (16)–(19), we obtain $E_{1,n+1} = E_{\sigma,\sigma+\tau+1}$, and thus $\sigma = 1$ and $\sigma + \tau = n$, which contradicts (19). This proves the corollary.

Next, we prove the following:

LEMMA 6. *Let $R_1, \cdots, R_n$ be associative rings with identities. Then the direct sum $R_1 \dotplus \cdots \dotplus R_n$ is not a β_n-ring.*

PROOF. Suppose that $R_1 \dotplus \cdots \dotplus R_n$ is a β_n-ring, and define

(20) $x_i = (1, 1, \cdots, 1, 0, 1, 1, \cdots, 1)$,
0 is in the ith position $(i = 1, \cdots, n)$.

Since $R_1 \dotplus \cdots \dotplus R_n$ is a β_n-ring, there exists a word $w(x_1, \cdots, x_n)$ such that

(21) $x_1 \cdots x_n = w(x_1, \cdots, x_n)$; some x_j missing in w.

Comparing the jth coordinates of both sides of (21), we obtain $0 = 1$ (since x_j is missing in w), a contradiction. This proves the lemma.

LEMMA 7. *Let R be an associative ring, and let I_1, I_2 be ideals of R with $I_1 \nsubseteq I_2$ and R/I_2 simple. Then $R/I_1 \cap I_2 \cong R/I_1 \dotplus R/I_2$.*

PROOF. Since R/I_2 is simple and $I_1 \nsubseteq I_2$, $I_1 + I_2 = R$, and hence, by the second isomorphism theorem,

$$R/I_1 \cap I_2 \cong I_1/I_1 \cap I_2 \dotplus I_2/I_1 \cap I_2 \cong R/I_2 \dotplus R/I_1.$$

We are now in a position to prove the following fundamental

THEOREM 2. *Let R be a semisimple ring. Then R is a β_n-ring, for some n, if and only if R is finite.*

PROOF. Suppose that R is a β_n-ring and suppose R is infinite. We shall show that this leads to a contradiction. Since R is semisimple, there exist ideals I_α $(\alpha \in \Omega)$ of R such that [**2**, p. 14] $\bigcap_{\alpha\in\Omega} I_\alpha = (0)$, and each R/I_α is primitive.

By Corollary 2 and Lemma 2, each R/I_α is finite, and hence [**2**, p. 33] each of the primitive rings R/I_α is a complete matrix ring over a finite field. Thus each R/I_α is a simple ring with identity. Next, choose $\alpha_1 \in R$, and having chosen $\alpha_1, \cdots, \alpha_k$ so that $\dot{\sum}_{i=1}^k R/I_{\alpha_i} \cong R/\bigcap_{i=1}^k I_{\alpha_i}$, choose $\alpha_{k+1} \in \Omega$ such that $\bigcap_{i=1}^k I_{\alpha_i} \nsubseteq I_{\alpha_{k+1}}$. 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

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

Thus R is finite, a contradiction. This contradiction shows that there exists $\alpha_{k+1} \in \Omega$ such that $\bigcap_{i=1}^{k} I_{\alpha_i} \nsubseteq I_{\alpha_{k+1}}$. Hence, by Lemma 7,

$$R\Big/\bigcap_{i=1}^{k+1} I_{\alpha_i} \cong R\Big/\bigcap_{i=1}^{k} I_{\alpha_i} \dotplus R/I_{\alpha_{k+1}} \cong \sum_{i=1}^{k+1}{}^{\bullet} R/I_{\alpha_i}.$$

In particular, we obtain

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

Now, by Lemma 2, $R/\bigcap_{i=1}^{n} R/I_{\alpha_i}$ is a β_n-ring, and hence $\sum_{i=1}^{\bullet n} R/I_{\alpha_i}$ is a β_n-ring also, which contradicts Lemma 6. This contradiction shows that R is finite. The converse part follows at once from Lemma 1.

Combined with Lemma 3, we easily obtain

COROLLARY 3. *Let R be an associative β_n-ring with Jacobson radical J. Then J is a nil ring of bounded index, and R/J is finite.*

In the above corollary, it follows [**1**, p. 28] that the Jacobson radical is locally nilpotent. It is not known to the authors whether the Jacobson radical must be nilpotent. However we have

THEOREM 3. *Let S be a commutative nil semigroup. Then S is a β_n-semigroup, for some n, if and only if S is nilpotent.*

PROOF. Let S be a β_n-semigroup. By Lemma 3, $x^k=0$ for *all* $x \in S$. So there exists a least positive integer q for which a positive integer m exists such that, for all $a_1, \cdots, a_m \in S$,

$$a_1^q \cdots a_m^q = 0 \qquad (q \text{ minimal}). \tag{22}$$

We now assume that $q>1$ and obtain a contradiction. Let $a_1, \cdots, a_{mn} \in S$, and for each i, $0 \leqq i \leqq n-1$, define $x_{i+1}=a_{im+1}^{q-1} \cdots a_{im+m}^{q-1}$. Then, since S is commutative and $q \geqq 2$, we have by (22), $x_{i+1}^2=0$ for each i. Since S is a β_n-semigroup,

$$x_1 \cdots x_n = w(x_1, \cdots, x_n) = w, \quad \text{some } x_j \text{ missing in } w. \tag{23}$$

Now, if some x_i appears twice in the word w, then by (23), $x_1 \cdots x_n=0$. Otherwise, since S is commutative and x_j does not appear in w, we can write $x_1 \cdots x_n \equiv wv$, where v is a product of at least one x_i. Hence, by (23), we have $wv=w$. Therefore, $w=wv=wv^k=0$, and hence once again $x_1 \cdots x_n=0$. Hence, $a_1^{q-1} \cdots a_{mn}^{q-1}=0$. This contradicts the minimality of q, and hence $q=1$. Therefore, by (22), $a_1 \cdots a_m=0$, and thus S is nilpotent. The converse follows at once from Lemma 1.

Combined with Corollary 3, we easily obtain

COROLLARY 4. *Let R be a commutative associative β_n-ring with Jacobson radical J. Then J is nilpotent and R/J is finite.*

We conclude with the following two remarks.

REMARK 1. The group-theoretic analogue of Theorem 1 is false. Indeed, the group $Z(p^\infty)$, which consists of the set of all p^nth roots of unity, where p is a fixed prime and $n=0, 1, 2, \cdots$ [3, p. 4], is a β_2-semigroup. To prove this, 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^nth roots of unity. Let σ be a generator of $Z(p^n)$. Then

$$x_1 = \sigma^r, \quad x_2 = \sigma^s; \qquad 1 \leqq r \leqq p^n,\ 1 \leqq s \leqq p^n. \tag{24}$$

Now, let

$$r = r_0 p^i, \quad s = s_0 p^j; \qquad (r_0, p) = 1,\ (s_0, p) = 1, \tag{25}$$

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

$$(r/p^i)x \equiv s/p^j \bmod p^n,$$

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

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

since $\sigma^{p^n}=1$. Therefore $x_1x_2 = (x_1)^{1+xp^{j-i}}$ and thus $Z(p^\infty)$ is a β_2-semigroup.

REMARK 2. The converse of Corollary 4 is false. To see this, let F be an infinite field of characteristic 2, and let

$$R = \left\{ \begin{pmatrix} a & x \\ 0 & a \end{pmatrix} \,\middle|\, a \in GF(2),\ x \in F \right\}. \tag{26}$$

It is readily verified that the Jacobson radical J of R satisfies $J^2=(0)$, and, moreover, $R/J \cong GF(2)$. However, R is *not* a β_n-ring for *any* n. We prove this by contradiction. Thus, suppose that R is a β_n-ring for some integer n, and define

$$T = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \,\middle|\, x \in F \right\}. \tag{27}$$

By Lemma 2, T is a β_n-semigroup. Moreover, the mapping

$$\sigma : x \to \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \qquad (x \in F) \tag{28}$$

is easily seen to yield an isomorphism of $F(+)$ onto $T(\times)$. But [3, p. 17]

$$F(+) \cong \text{a direct sum of an infinite number of nontrivial finite cyclic groups } G_i \ (i \in \Gamma). \tag{29}$$

Now, let $a_i \in G_i$; $a_i \neq 0$; $i=1, \cdots, n$, and let the elements x_i of F be defined by (see (29))

$$x_i = (0, 0, \cdots, 0, a_i, 0, 0, \cdots) \qquad i = 1, \cdots, n, \tag{30}$$

where a_i appears in the ith position. Let x_i' be the element of T defined by

$$x_i' = \begin{pmatrix} 1 & x_i \\ 0 & 1 \end{pmatrix} (= \sigma(x_i)), \qquad i = 1, \cdots, n. \tag{31}$$

Since T is a β_n-semigroup, there exists a word $w = w_{x_1', \cdots, x_n'}(x_1', \cdots, x_n')$, *with some* x_j' *missing in* w, such that

$$x_1' \cdots x_n' = w_{x_1', \cdots, x_n'}(x_1', \cdots, x_n'). \tag{32}$$

Now, in view of the isomorphism σ, this equation reflects in $F(+)$ as (see (28) and (31))

$$x_1 + \cdots + x_n = w^*(x_1, \cdots, x_n), \tag{33}$$

where $w^* = w^*(x_1, \cdots, x_n)$ is the (additive) word obtained by replacing "$\times$" by "$+$" throughout the word w, and by replacing each x_i' by x_i. Moreover, since x_j' is missing in w, x_j is missing in the word w^*. Now, equating the jth coordinates of both sides of (33) (see (30)), we get $a_j = 0$ (since $w^*(x_1, \cdots, x_n)$ *does not involve* x_j), which contradicts the choice of a_j. This contradiction proves that R is not a β_n-ring.

In conclusion, we wish to express our indebtedness and gratitude to the referee for his valuable suggestions.

References

1. I. N. Herstein, *Theory of rings*, Lecture Notes, University of Chicago, Chicago, Ill., 1961.

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

3. I. Kaplansky, *Infinite abelian groups*, Univ. of Michigan Press, Ann Arbor, Mich., 1954. MR **16**, 444.

4. T. Nagell, *Introduction to number theory*, 2nd ed., Chelsea, New York, 1964. MR **30** #4714.

5. H. Rademacher, *Lectures on elementary number theory*, Blaisdell, Waltham, Mass., 1964. MR **30** #1079.

6. B. L. van der Waerden, *Elementarer Beweis eines zahlentheoretischen Existenztheorems*, J. Reine Angew. Math. **171** (1934), 1–3.

Department of Mathematics, University of California, Santa Barbara, California 93106