ON ZERO SUBRINGS AND PERIODIC SUBRINGS

HOWARD E. BELL

(Received 23 October 2000)

ABSTRACT. We give new proofs of two theorems on rings in which every zero subring is finite; and we apply these theorems to obtain a necessary and sufficient condition for an infinite ring with periodic additive group to have an infinite periodic subring.

2000 Mathematics Subject Classification. 16N40, 16N60, 16P99.

Let $R$ be a ring and $N$ its set of nilpotent elements; and call $R$ reduced if $N = \{0\}$. Following [4], call $R$ an FZS-ring if every zero subring—that is, every subring with trivial multiplication—is finite. It was proved in [1] that every nil FZS-ring is finite—a result which in more transparent form is as follows.

**Theorem 1.** Every infinite nil ring contains an infinite zero subring.

Later, in [4], it was shown that every ring with $N$ infinite contains an infinite zero subring. The proof relies on Theorem 1 together with the following result.

**Theorem 2** (see [4]). If $R$ is any semiprime FZS-ring, then $R = B \oplus C$, where $B$ is reduced and $C$ is a direct sum of finitely many total matrix rings over finite fields.

Theorems 1 and 2 have had several applications in the study of commutativity and finiteness. Since the proofs in [1, 4] are rather complicated, it is desirable to have new and simpler proofs; and in our first major section, we present such proofs. In our final section, we apply Theorems 1 and 2 in proving a new theorem on existence of infinite periodic subrings.

1. Preliminaries. Let $\mathbb{Z}$ and $\mathbb{Z}^+$ denote, respectively the ring of integers and the set of positive integers. For the ring $R$, denote by the symbols $T$ and $P(R)$, respectively the ideal of torsion elements and the prime radical; and for each $n \in \mathbb{Z}^+$, define $R_n$ to be $\{x \in R \mid x^n = 0\}$. For $Y$ an element or subset of $R$, let $\langle Y \rangle$ be the subring generated by $Y$; let $A_l(Y)$, $A_r(Y)$, and $A(Y)$ be the left, right, and two-sided annihilators of $Y$; and let $C_R(Y)$ be the centralizer of $Y$. For $x, y \in R$, let $[x, y]$ be the commutator $xy - yx$.

The subring $S$ of $R$ is said to be of finite index in $R$ if $(S, +)$ is of finite index in $(R, +)$. An element $x \in R$ is called periodic if there exist distinct positive integers $m, n$ such that $x^m = x^n$; and the ring $R$ is called periodic if each of its elements is periodic.

We will use without explicit mention two well-known facts:

(i) the intersection of finitely many subrings of finite index in $R$ is a subring of finite index in $R$;
(ii) if \( R \) is semiprime and \( I \) is an ideal of \( R \), then \( R/A(I) \) is semiprime. We will also need several lemmas.

Lemma 1.1 is a theorem from [6]; Lemma 1.2 appears in [3], and with a different proof in [2]; Lemma 1.3, also given without proof, is all but obvious. Lemma 1.6, which appears to be new, is the key to our proofs of Theorems 1 and 2.

**Lemma 1.1.** If \( R \) is a ring and \( S \) is a subring of finite index in \( R \), then \( S \) contains an ideal of \( R \) which is of finite index in \( R \).

**Lemma 1.2.** Let \( R \) be a ring with the property that for each \( x \in R \), there exist \( m \in \mathbb{Z}^+ \) and \( p(t) \in \mathbb{Z}[t] \) such that \( x^m = x^{m+1} p(x) \). Then \( R \) is periodic.

**Lemma 1.3.** If \( R \) is any ring with \( N \subseteq T \) and \( H \) is any finite set of pairwise orthogonal elements of \( N \), then \( \langle H \rangle \) is finite.

**Lemma 1.4.** If \( R \) is any ring in which \( R_2 \) is finite, then \( R \) is of bounded index—that is, \( N = R_n \) for some \( n \in \mathbb{Z}^+ \).

**Proof.** Let \( M = \langle R_2 \rangle \) and let \( x \in N \) such that \( x^{2k} = 0 \) for \( k \geq M + 1 \); and note that \( x^k, x^{k+1}, \ldots, x^{2k-1} \) are all in \( R_2 \). Since \( k > M \), these elements cannot be distinct; hence there exist \( h, j \in \mathbb{Z}^+ \) such that \( h < j \leq 2k - 1 \) and \( x^h = x^{h+m(j-h)} \) for all \( m \in \mathbb{Z}^+ \). It follows that \( x^h = 0 \); hence \( y^{2^M} = 0 \) for all \( y \in N \).

**Lemma 1.5.** If \( R \) is any FZS-ring, then \( N \subseteq T \).

**Proof.** Let \( R \) be a ring with \( N \setminus T \neq \emptyset \), and let \( x \in N \setminus T \). Then there exists a smallest \( n \in \mathbb{Z}^+ \) such that \( x^n \in T \), and there exists \( k \in \mathbb{Z}^+ \) for which \( kx^n = 0 \). Since \( kx^{n-1} \notin T \), \( \langle kx^{n-1} \rangle \) is an infinite zero subring of \( R \).

**Lemma 1.6.** If \( R \) is any FZS-ring and \( x \) is any element of \( N \), then \( A(x) \) is of finite index in \( R \). Hence, if \( S \) is any finite subset of \( N \), \( A(S) \) is of finite index in \( R \).

**Proof.** We use induction on the degree of nilpotence. Suppose first that \( y^2 = 0 \). Define \( \Phi : R \gamma \rightarrow R \) by \( r \gamma \gamma \rightarrow [r \gamma, \gamma] = -\gamma r \gamma \); and note that \( \Phi(R \gamma) \) is a zero subring of \( R \), hence finite. Thus \( \ker \Phi = R \gamma \cap C_R(\gamma) \) is of finite index in \( R \gamma \). But it is easily seen that \( \ker \Phi \) is a zero ring, hence is finite; consequently, \( R \gamma \) is finite. Now consider \( \eta : R \rightarrow R \gamma \) defined by \( r \rightarrow r \gamma \), and note that \( \ker \eta = A_I(\gamma) \) is of finite index in \( R \). Similarly, \( A_r(\gamma) \) is of finite index and so is \( A(\gamma) = A_I(\gamma) \cap A_r(\gamma) \).

Now assume that \( A(x) \) is of finite index for all \( x \in N \) with degree of nilpotence less than \( k \), and let \( y \in N \) be such that \( y^k = 0 \). Then \( A(y^2) \) is of finite index in \( R \). Define \( \Phi : A(y^2) \gamma \rightarrow R \) by \( s \gamma \gamma \rightarrow [s \gamma, \gamma] \), \( s \in A(y^2) \); and note that both \( \Phi(A(y^2) \gamma) \) and \( \ker \Phi = A(y^2) \gamma \cap C_R(\gamma) \) are zero rings, so that \( A(y^2) \gamma \) is finite. Consider the map \( \Psi = A(y^2) \gamma \rightarrow A(y^2) \gamma \gamma \) given by \( s \gamma \rightarrow s \gamma \gamma \). Now \( \ker \Psi = A(y^2) \gamma \cap A_I(\gamma) \) must be of finite index in \( A(y^2) \gamma \); and since \( A(y^2) \gamma \) is of finite index in \( R \), \( \ker \Psi \) is of finite index in \( R \). It follows that \( A_I(\gamma) \) is of finite index in \( R \); and a similar argument shows that \( A_r(\gamma) \) is of finite index in \( R \). Therefore \( A(\gamma) \) is of finite index in \( R \).}

**Lemma 1.7.** Let \( p \) be a prime, and let \( R \) be a ring such that \( pR = \{0\} \).

(i) If \( a \in R \) and \( a^{pk} = a \), then \( a^{pk} = a \) for all \( m \in \mathbb{Z}^+ \). Hence if \( a, b \in R \) with \( a^{pk} = a \) and \( b^{p^l} = b \), there exists \( n \in \mathbb{Z}^+ \) such that \( a^{pn} = a \) and \( b^{pn} = b \).
(ii) If $a \in R$ and $a^{p^n} = a$, then for each $s \in \mathbb{Z}$, $(sa)^{p^n} = sa$.

(iii) If $R$ is reduced and $a$ is a periodic element of $R$, then there exists $n \in \mathbb{Z}^+$ such that $a^{p^n} = a$.

**Proof.** (i) is almost obvious, and (ii) follows from the fact that $s^p \equiv s \pmod{p}$ for all $s \in \mathbb{Z}$. To obtain (iii), note that if $R$ is reduced and $a$ is periodic, then $\langle a \rangle$ is finite, hence a direct sum of finite fields, necessarily of characteristic $p$. Since $\text{GF}(p^\alpha)$ satisfies the identity $x^{p\alpha} = x$, the conclusion of (iii) follows by (i).

### 2. Proofs of Theorems 1 and 2

**Proof of Theorem 1.** Suppose $R$ is a counterexample. Note that $R$ is an FZS-ring, so $R = T$ by Lemma 1.5. It is easy to see that $R$ contains a maximal finite zero subring $S$. By Lemma 1.6, $A(S)$ is infinite; and maximality of $S$ forces $A(S)_2 = S$. Thus, by replacing $R$ by $A(S)$, we may assume that $R_2$ is finite.

By Lemma 1.6, we can construct infinite sequences of pairwise orthogonal elements; and by Lemma 1.4 there is a smallest $M \in \mathbb{Z}^+$ for which $R_M$ contains such sequences. Let $u_1, u_2, \ldots$ be an infinite sequence of pairwise orthogonal elements of $R_M$. Using Lemma 1.3, we can refine this sequence to obtain an infinite subsequence $v_1, v_2, \ldots$ such that for each $j \geq 2$, $v_j \notin \langle v_1, v_2, \ldots, v_{j-1} \rangle$. Defining $V_0$ to be $\{v_j^2 \mid j \in \mathbb{Z}^+\}$, we see that $V_0 \subseteq R_{M-1}$ and hence $V_0$ is finite, so we may assume without loss of generality that there exists a single $s \in R$ such that $v_j^2 = s$ for all $j \in \mathbb{Z}^+$. Take $m \in \mathbb{Z}^+$ such that $ms = 0$; and for each $j \in \mathbb{Z}^+$, define $w_j = \sum_{i=1}^{m-1} v_i$. Then the $w_j$ form an infinite subset of $R_2$, contrary to the fact that $R_2$ is finite. The proof is now complete.

**Proof of Theorem 2.** As before, since $R$ is an FZS-ring, there is a maximal finite zero subring $S$; and by Lemma 1.6 $A(S)$ is of finite index in $R$. By Lemma 1.1, $A(S)$ contains an ideal $I$ of $R$ which is also of finite index in $R$. Let $C = A(I)$ and let $B = A(C)$. Then $B \supseteq I$, so $B$ is of finite index in $R$.

Next we show that $B$ is reduced. Let $x \in B$ such that $x^2 = 0$. Then $x \in A(C)$, and since $S \subseteq C$, the maximality of $S$ forces $x \in B \cap C = \{0\}$. Therefore, $B$ is reduced.

The rest of the proof is as in [4]. Since $R/B$ is finite and semiprime, we can write it as $M_1 \oplus \cdots \oplus M_k$, where the $M_i$ are total matrix rings over finite fields. Let $C' = (B + C)/B$ and note that $C'$ is an ideal of $R/B$ and $C' \cong C$. Now $C'$ must be a direct sum of some of the $M_i$, so $R/B = C' \oplus D'$ where $D'$ is the annihilator of $C'$. Taking $D$ to be an ideal of $R$ containing $B$ for which $D/B = D'$, and noting that $C'D' = \{0\}$, we have $CD \subseteq B$. But $CD \subseteq C$ as well, so $CD \subseteq B \cap C = \{0\}$ and $D \subseteq A(C) = B$; therefore $D' = \{0\}$ and $C' = R/B$. It follows that $R = B + C$ and hence $R = B \oplus C$; and since $C \subseteq C'$, $C$ is a direct sum of total matrix rings as required.

**Remark 2.1.** In [5], Lanski established the conclusion of Theorem 2 under the apparently stronger hypothesis that $N$ is finite; and his proof uses induction on $|N|$. As we noted in the introduction, it follows from Theorems 1 and 2 that $R$ is an FZS-ring if and only if $N$ is finite.

### 3. A theorem on periodic subrings

We have noted that if $N$ is infinite, $R$ contains an infinite nil subring. Since periodic elements extend the notion of nilpotent element,
it is natural to ask whether there is a periodic analogue—that is, to ask whether a ring with infinitely many periodic elements must have an infinite periodic subring. The answer in general is no, even in the case of commutative rings. The complex field $\mathbb{C}$ is a counterexample, for the set of nonzero periodic elements is the set $U$ of roots of unity, and $u \in U$ implies $2u \notin U$. Moreover, if $S$ is any finite ring, $\mathbb{C} \oplus S$ is also a counterexample; therefore, we restrict our attention to rings $R$ for which $R = T$.

**Theorem 3.1.** Let $R$ be a ring with $R = T$. Then a necessary and sufficient condition for $R$ to have an infinite periodic subring is that $R$ contains an infinite set of pairwise-commuting periodic elements.

**Proof.** It is known that in any infinite periodic ring $R$, either $N$ is infinite or the center $Z$ is infinite [4, Theorem 7]. Therefore our condition is necessary.

For sufficiency, suppose that $R$ has infinitely many pairwise-commuting periodic elements. Now $R$ is the direct sum of its $p$-primary components $R^{(p)}$; and if there exist infinitely many primes $p_1, p_2, p_3, \ldots$ such that $R^{(p_i)}$ contains a nonzero periodic element $a_{p_i}$, then the direct sum of the rings $\langle a_{p_i} \rangle$ is an infinite periodic subring. Thus, we may assume that only finitely many $R^{(p)}$ contain nonzero periodic elements, so we need only consider the case that $R = R^{(p)}$ for some prime $p$. Of course we may assume that $R$ is an FZS-ring.

Consider the factor ring $\bar{R} = R/P(R)$. Since $R$ is an FZS-ring, it follows from Theorem 1 that $P(R)$ is finite, in which case $\bar{R}$ inherits our hypothesis on pairwise-commuting periodic elements. If $\bar{R}$ has an infinite periodic subring $\bar{S}$ and $S$ is its preimage in $R$, then for all $x \in S$, there exist distinct $m, n \in \mathbb{Z}^+$ such that $x^n - x^m \in P(R) \subseteq N$; hence $S$ is periodic by Lemma 1.2. Thus, we may assume that $R = R^{(p)}$ and that $R$ is a semiprime FZS-ring.

By Theorem 2, write $R = B \oplus C$, where $B$ is reduced and $C$ is finite; and note that $B$ must have an infinite subset $H$ of pairwise-commuting periodic elements. Note also that $pB = \{0\}$, since $B$ is reduced. Let $a, b \in H$, and by Lemma 1.7(i) and (iii) obtain $n \in \mathbb{Z}^+$ such that $a^{p^n} = a$ and $b^{p^n} = b$. It follows at once that $(a - b)^{p^n} = a^{p^n} - b^{p^n} = a - b$ and $(ab)^{p^n} = a^{p^n}b^{p^n} = ab$; and these facts, together with Lemma 1.7(ii) imply that $\langle H \rangle$ is an infinite periodic subring of $R$.

**Acknowledgement.** This research was supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. 3961.

**References**


Howard E. Bell: Department of Mathematics, Brock University, St. Catharines, Ontario, Canada L2S 3A1
E-mail address: hbell@spartan.ac.brocku.ca