HOUSTON JOURNAL OF MATHEMATICS

Volume 24, No. 1, 1998

IDEALS CONTAINED IN SUBRINGS

HOWARD E. BELL* AND ABRAHAM A. KLEIN

COMMUNICATED BY JOHNNY A. JOHNSON

ABSTRACT. Lewin has proved that if S is a ring and R a subring of finite index in S, then R contains an ideal of S which is also of finite index; and Feigelstock has recently shown that other classes of subrings must contain ideals belonging to the same class. We provide some extensions of these results, and apply them to prime rings. In the final section, we investigate finiteness of rings having only finitely many n-th powers, where $n \geq 2$ is a fixed positive integer.

1. INTRODUCTION

Let S be a ring and R a subring. By the index of R in S, we shall mean the index of $(R,+)$ in $(S,+)$; and, as usual, we shall denote it by [S:R].

A useful result of Lewin ([6], Lemma 1), recently rediscovered by Hirano ([4], Theorem 1), asserts that if R has finite index in S, then R contains an ideal I of S which also has finite index in S; and Lewin's proof gives a bound, albeit a rather large one, for $[S:I]$ in terms of $[S:R]$.

Recently Feigelstock [3] has generalized Lewin's result by replacing the notion of finite index by the property that the additive group S/R belongs to a nonempty class $\mathcal{C}$ of abelian groups satisfying the following conditions (it being understood that the statement that A is a $\mathcal{C}$-group means that $A \in \mathcal{C}$):

(F_1) For each $A \in \mathcal{C}$, the additive group of the ring of endomorphisms of A is in $\mathcal{C}$;

(F_2) $\mathcal{C}$ is closed under taking subgroups;

(F_3) $\mathcal{C}$ is closed under extensions by $\mathcal{C}$-groups;

(F_4) $\mathcal{C}$ is closed under taking epimorphic images.

*Supported by the Natural Sciences and Engineering Research Council of Canada.

Feigelstock calls such a class a *finite-like* class. We shall also use the term *finite-like* class, but with a slightly different meaning – a class $\mathcal{C}$ of abelian groups satisfying $(F_1) - (F_3)$.

Feigelstock's first result is that if $\mathcal{C}$ satisfies $(F_1) - (F_4)$ and R is a subring of S with $S/R \in \mathcal{C}$, then R contains a left ideal I_ℓ and a right ideal I_r such that $S/I_\ell \in \mathcal{C}$ and $S/I_r \in \mathcal{C}$. His second result states that if all groups in $\mathcal{C}$ are finitely-generated, then I_ℓ and I_r may be replaced by a two-sided ideal.

In our second section, we make the weaker assumption that $\mathcal{C}$ satisfies only $(F_1) - (F_3)$ and we obtain the full (two-sided ideal) extension of Lewin's result, without assuming finite generation of groups in $\mathcal{C}$. If $\mathcal{C}$ is the class of finite abelian groups, our proof yields a new proof of Lewin's result and an improved bound for $[S : I]$. In the third section, we give some applications to prime rings; and in the last section we investigate finiteness in rings with finitely many n-th powers. The first proof in this final section is, in part, an application of Lewin's original result.

2. The Extension of Lewin's Result

The ring of endomorphisms of an abelian group A will be denoted by $E(A)$, and it will be assumed that each endomorphism acts on A from the left side. As mentioned in the introduction, a nonempty class $\mathcal{C}$ of abelian groups satisfying $(F_1) - (F_3)$ will be called a finite-like class. We begin with our generalization of Lewin's result.

Theorem 2.1. *Let $\mathcal{C}$ be a finite-like class of abelian groups. If R is a subring of a ring S such that $S/R \in \mathcal{C}$, then R contains a two-sided ideal I such that $S/I \in \mathcal{C}$.*

Proof. Considering S/R as a right R-module in the natural way, we have an anti-homomorphism from R into $E(S/R)$ given by $a \mapsto a_r$, where a_r is defined by $a_r(s + R) = sa + R$. Its kernel L is the set $\{a \in R \mid Sa \subseteq R\}$, which is the largest left ideal of S contained in R. The additive group R/L is isomorphic to a subgroup of $E(S/R)$, hence $R/L \in \mathcal{C}$ by (F_1) and (F_2); and since $(S/L)/(R/L) \cong S/R$ as additive groups, it follows by (F_3) that $S/L \in \mathcal{C}$.

Regarding S/L as a left S-module and proceeding as in the previous paragraph, we get a homomorphism from S into $E(S/L)$; and its restriction to L is a homomorphism from L into $E(S/L)$ with kernel $I = \{a \in L | aS \subseteq L\} = \{a \in R | Sa, aS, SaS \subseteq R\}$, which is the largest two-sided ideal of S contained in R. Since $S/L \in \mathcal{C}$ implies $E(S/L) \in \mathcal{C}$, we get $L/I \in \mathcal{C}$ and therefore $S/I \in \mathcal{C}$. $\square$

Specializing to the class $\mathcal{C}$ of finite abelian groups and combining some elementary observations on abelian groups with the proof of Theorem 2.1, we obtain a bound for [S:I].

Theorem 2.2. *Let R be a subring of S with $[S:R]=n$, and let I be the largest ideal of S contained in R. If p is the smallest prime dividing n and $\ell=[\log_p n]$, then*

$$[S:I]\leq n^{(\ell+1)^3}\ .$$

PROOF. We begin with some elementary observations on finite abelian groups. If A is an abelian group of order m and $\{a_1,a_2,\dots,a_t\}$ is a minimal set of generators for A, then it is easy to see that $t\leq\ell=[\log_p m]$, where p is the minimal prime dividing m. It is also clear that the minimal prime dividing $|E(A)|$ cannot be smaller than p. Any endomorphism θ of A is uniquely determined by the values $\theta(a_1),\theta(a_2),\dots,\theta(a_t)$; and since each $\theta(a_i)$ is one of m elements of A, we have $|E(A)|\leq m^t\leq m^\ell$.

Now let n,p, and ℓ be as in the statement of the theorem, and L and I as in the proof of Theorem 2.1. Since R/L is isomorphic to a subgroup of $E(S/R)$, and since the minimal prime dividing $|E(S/R)|$ is at least p, the minimal prime dividing $|R/L|$ is at least p.

Now consider $|S/L|$. From the equality $|S/L|=|S/R||R/L|$, we see that the minimal prime dividing $|S/L|$ is p and

$$|S/L|\leq|S/R||E(S/R)|\leq nn^\ell=n^{\ell+1}\ . \tag{2.1}$$

It follows that $|E(S/L)|\leq(n^{\ell+1})^{\ell'}$, where $\ell'=\left[\log_p|S/L|\right]\leq\left[\log_p n^{\ell+1}\right]=\left[(\ell+1)\log_p n\right]$. Now $\left[\log_p n\right]=\ell$, so $\log_p n<\ell+1$; hence $(\ell+1)\log_p n<(\ell+1)^2$ and $\ell'\leq(\ell+1)^2-1$. It follows that $|E(S/L)|\leq n^{(\ell+1)^3-(\ell+1)}$. Recalling from the proof of Theorem 2.1 that L/I is isomorphic to a subgroup of $E(S/L)$, we have

$$|L/I|\leq n^{(\ell+1)^3-(\ell+1)}\ . \tag{2.2}$$

Since $|S/I|=|S/L||L/I|$, it is immediate from 2.1 and 2.2 that $|S/I|\leq n^{(\ell+1)^3}$, which is precisely what we wished to prove. □

Remark. Theorem 2.1 may be generalized to algebras over a commutative ring K as follows. Let $\mathcal{C}$ be a nonempty class of K-modules satisfying

(F_1') For each $A\in\mathcal{C}$, the K-module $End_K(A)$ is in $\mathcal{C}$;

(F_2') $\mathcal{C}$ is closed under taking submodules;

(F_3') $\mathcal{C}$ is closed under extensions by $\mathcal{C}$-modules.

For example, if K is a principal ideal domain, the class of finitely-generated K-modules satisfies $(F_1') - (F_3')$.

For such a class $\mathcal{C}$, we obtain an analogue of Theorem 2.1 by replacing rings and ideals by K-algebras and K-algebra ideals. The proof is similar.

3. Applications to Prime Rings

Throughout this section, we assume that S is a prime ring and $\mathcal{C}$ is a finite-like class of abelian groups. We shall apply Theorem 2.1 for various subrings R such that $S/R \in \mathcal{C}$; and I will always denote the largest ideal of S contained in R, so that $S/I \in \mathcal{C}$. For $a \in S$, the symbols $A_\ell(a)$ and $A_r(a)$ will denote the left and right annihilators of a.

For our first theorem, we need the following lemma, the proof of which is straightforward and is omitted.

Lemma 3.1. *If R is a subring of S and R contains a nonzero ideal of S, then R is prime.*

Theorem 3.2. *If $S \notin \mathcal{C}$ and R is a subring such that $S/R \in \mathcal{C}$, then R is prime; and if S is simple, then $R = S$.*

Proof. We have $S/I \in \mathcal{C}$, and $I \neq \{0\}$ since $S \notin \mathcal{C}$; thus, R is prime by Lemma 3.1. If S is simple, then $I \neq \{0\}$ implies that $I = S$ and therefore $R = S$. □

Remarks (3a). Theorem 3.2 is an extension of Corollary 5 in [3].

(3b). One consequence of Theorem 3.2 is that if S is an infinite division ring and R is a subring of finite index, then $S = R$. This may be thought of as an analogue of the result that if S is an infinite division ring and R is a division subring whose multiplicative group has finite index in the multiplicative group of S, then $S = R$ [10, 14.2.1].

For our next theorem, which is an extension of [1, Theorem 3], we require another lemma.

Lemma 3.3. *If $S \notin \mathcal{C}$, then $aS \notin \mathcal{C}$ for any $a \in S\backslash\{0\}$.*

Proof. Assume there exists $a \in S\backslash\{0\}$ for which $aS \in \mathcal{C}$. Since $aS \cong S/A_r(a) \in \mathcal{C}$, Theorem 2.1 with $R = A_r(a)$ yields $S/I \in \mathcal{C}$ and $I \subseteq A_r(a)$. Thus $aI = \{0\}$, and since $a \neq 0$ and S is prime, we must have $I = \{0\}$. But this implies $S \in \mathcal{C}$, a contradiction. □

Theorem 3.4. *If $S \notin \mathcal{C}$, then either S is a domain or S contains a zero subring K with $K \notin \mathcal{C}$ and $S/K \notin \mathcal{C}$.*

PROOF. Suppose S is not a domain. We first prove that S contains a subring K with $K \notin \mathcal{C}$ and $K^2 = \{0\}$. A prime ring which is not a domain contains nonzero nilpotent elements, so we choose $a \in S \backslash \{0\}$ such that $a^2 = 0$. If $aSa \notin \mathcal{C}$, we can take $K = aSa$; hence we assume that $aSa \in \mathcal{C}$. In this case, take $K = aS \cap A_\ell(a)$. Since $aSa \cong aS/K \in \mathcal{C}$ and since $aS \notin \mathcal{C}$ by Lemma 3.3, (F_3) gives $K \notin \mathcal{C}$. Moreover, $K^2 \subseteq A_\ell(a)aS = \{0\}$.

It remains only to show that $S/K \notin \mathcal{C}$. Assume this is not the case. Taking $R = K$ in Theorem 2.1 gives $S/I \in \mathcal{C}$ and $I \subseteq K$. Hence $I^2 \subseteq K^2 = \{0\}$; and by primeness of S, $I = \{0\}$. But this implies $S \in \mathcal{C}$, a contradiction. □

The remainder of this section deals with derivations on prime rings.

Lemma 3.5. [2, Lemma 3]. *Let d be a derivation on S, and let I be an ideal of S. If $d(I) = \{0\}$, then $d = 0$.*

Theorem 3.6. *If $S \notin \mathcal{C}$ and d is a derivation on S with $d(S) \in \mathcal{C}$, then $d = 0$.*

PROOF. Note that $R = \ker d$ is a subring of S and $S/R \cong d(S) \in \mathcal{C}$. By Theorem 2.1 we have $S/I \in \mathcal{C}$; and $I \subseteq R$, so $d(I) = \{0\}$. Since $S \notin \mathcal{C}$, we have $I \neq \{0\}$; hence $d = 0$ by Lemma 3.5. □

Corollary 3.7. *If d is a derivation on S and $d(S)$ is finite, then either S is finite or $d = 0$.*

4. Two Finiteness Theorems

In this section, we investigate finiteness of rings having only finitely many k-th powers, where $k \geq 2$ is a fixed positive integer. We accord the $k = 2$ case special treatment because it can be handled by reasonably elementary methods, and because it provides a pretty application of Lewin's theorem.

Recall that a ring R is called periodic if for each $x \in R$ there exist distinct positive integers m and n for which $x^m = x^n$. We shall need to use the fact that if R is periodic, each element has an idempotent power and hence the Jacobson radical $J(R)$ is nil.

For the remainder of the paper, Z will denote the center of R; and for each $x \in R$, $C(x)$ and $A(x)$ will be respectively the centralizer and two-sided annihilator of x in R. The symbol $H_k(R)$ will denote the set $\{x^k \mid x \in R\}$.

Theorem 4.1. *Let R be a ring with no nonzero nil ideals. If $H_2(R)$ is finite, then R is finite.*

PROOF. Note that if R is any ring with $H_2(R)$ finite and if $|H_2(R)| = k$, then for any $x \in R$ the elements $x^2, x^4, \ldots, x^{2k+2}$ cannot be distinct; hence R is periodic. Note also that R contains only finitely many idempotents.

Assume the theorem is false, and let R be a counterexample with a minimum number of nonzero idempotents (necessarily at least 1). Observe that R can contain no nonzero central idempotent f which is a zero divisor; otherwise, we would have $R = Rf \oplus A(f)$, where each summand satisfies our original hypotheses and has fewer nonzero idempotents than R, hence is finite. It follows that if R has nonzero central idempotents, then R has 1 and 1 is the only nonzero central idempotent.

Now R has only finitely many elements of the form $xy + yx = (x+y)^2 - x^2 - y^2$. Thus, for fixed $x \in R$, the map $y \mapsto xy + yx$ has finite image and its kernel K_x has finite index. Of course K_x need not be a subring of R; however, K_x is contained in the subring $C(x^2)$, which also has finite index. Since $H_2(R)$ is finite, the subring $\bigcap_{x \in R} C(x^2)$ has finite index, and by Lewin's result contains an ideal I of finite index. Since R is infinite, $I \neq \{0\}$; and since R has no nonzero nil ideals, I must contain a nonzero idempotent e. Now any idempotent in I centralizes x^2 for all $x \in R$, hence centralizes all idempotents in R, hence is in Z. Thus, $e = 1$, $I = R$, and all idempotents of R are central; hence, 1 is the only nonzero idempotent in R.

We have noted that some power of each element of R is idempotent, hence each element of R is either nilpotent or invertible. It is known that this property implies that the nilpotent elements form an ideal [7], which in our context must be trivial; therefore R is a division ring. But periodic division rings are commutative by Jacobson's "$a^n = a$ theorem". In a field $u^2 = v^2$ if and only if $u = \pm v$; hence our R cannot be a counterexample, and no counterexamples exist. □

This theorem invites the question of whether $H_2(R)$ can be replaced by $H_n(R)$ for $n > 2$. The answer is yes; but the proof, unlike that of Theorem 4.1, is not elementary.

Theorem 4.2. *Let R be a ring with no nonzero nil ideals and let k be an integer greater than 1. If $H_k(R)$ is finite, then R is finite.*

Lemma 4.3. [8, Theorem 1]. *Let R be a semiprimitive PI-ring with center Z. If I is any nonzero ideal of R, then $I \cap Z \neq \{0\}$.*

Lemma 4.4. *Let $x_1, x_2, \ldots, x_k$ be a finite number of elements of a ring R such that for each i, there exist positive integers m_i and n_i for which $x_i^{m_i} = x_i^{n_i}$ and $n_i - m_i > 0$. Then there exist distinct positive integers m and n such that $x_i^m = x_i^n$ for $i = 1, 2, \ldots, k$.*

PROOF. Let $m = \max\{m_1, m_2, \ldots, m_k\}$ and $n = m + \Pi(n_i - m_i)$. Then $x_i^n = x_i^m$ for each i. □

PROOF OF THEOREM 4.2. As in the proof of Theorem 4.1, we see that any R with $H_k(R)$ finite is periodic; and by Lemma 4.4, we conclude that R satisfies a polynomial identity of the form $x^n = x^m$. Since the Jacobson radical of a periodic ring is nil and R has no nonzero nil ideals, R is semiprimitive.

Again we assume a counterexample R with a minimum number of nonzero idempotents. Since ideals of semiprimitive rings are semiprimitive rings, we conclude as in the proof of Theorem 4.1 that R contains no nonzero central idempotents which are zero divisors in R, and hence that R can have no central idempotents except possibly 1.

By Lemma 4.3, $Z \neq \{0\}$; and since R is semiprime, Z has no nonzero nilpotent elements, hence must contain a nonzero idempotent, necessarily 1. Since 1 is the only nonzero central idempotent in R, Z must therefore be a field; and since Z satisfies a polynomial identity $x^n = x^m$, Z must be finite.

Let I be any nonzero ideal of R. By Lemma 4.3 $I \cap Z \neq \{0\}$, so I contains 1 and hence $I = R$. Therefore, R is simple with 1, hence primitive; and by a well-known theorem of Kaplansky [9, Th. 6.1.25], R is finite-dimensional over Z, hence finite. This demolishes the assumption that R is a counterexample.

Corollary 4.5. *If R is a semiprime ring and there exists $k > 1$ such that $H_k(R)$ is finite, then R is finite.*

PROOF. Since R satisfies an identity $x^n = x^m$, nilpotent elements have bounded index of nilpotency. Since Levitzki's theorem [9, Prop. 2.6, 26] precludes nil ideals of bounded index in semiprime rings, R has no nonzero nil ideals and is therefore finite by Theorem 4.2. □

Corollary 4.6. *Let R be a ring with only a finite number of nilpotent elements. If there exists $k > 1$ for which $H_k(R)$ is finite, then R is finite.*

PROOF. The prime radical $P(R)$ is finite; and $R/P(R)$ is finite by Corollary 4.5. Therefore R is finite. □

Remark. In general, a ring R with $H_k(R)$ finite need not be finite; an obvious counterexample is an infinite zero ring. It is perhaps interesting that by Corollary

4.6, every counterexample contains an infinite zero subring, for it has recently been proved that every ring with infinitely many nilpotent elements contains an infinite zero subring [5, Theorem 6].

References

[1] H.E. Bell and A.A. Klein, On finiteness, commutativity, and periodicity in rings, Math. J. Okayama Univ. 35(1993), 181-188.

[2] H.E. Bell and W.S. Martindale, Centralizing mappings of semiprime rings, Canad. Math. Bull. 30(1987), 92-101.

[3] S. Feigelstock, Subrings containing ideals, Math. J. Okayama Univ. 34(1992), 149-151.

[4] Y. Hirano, On extensions of rings with finite additive index, Math. J. Okayama Univ. 32(1990), 93-95.

[5] A.A. Klein and H.E. Bell, Rings with finitely many nilpotent elements, Comm. Algebra 22(1994), 349-354.

[6] J. Lewin, Subrings of finite index in finitely-generated rings, J. Algebra 5(1967), 84-88.

[7] D.L. Outcalt and A. Yaqub, A commutativity theorem for rings, Bull. Austral. Math. Soc. 2(1970), 95-99.

[8] L.H. Rowen, Some results on the center of a ring with polynomial identity, Bull. Amer. Math. Soc. 79(1973), 219-223.

[9] L.H. Rowen, Ring Theory I and II, Academic Press, 1988.

[10] W.R. Scott, Group Theory, Prentice-Hall 1964.

Received September 1, 1995

Revised version received January 22, 1996

(Bell) Department of Mathematics, Brock University, St. Catharines, Ontario, Canada L2S 3A1

E-mail address: hbell@spartan.ac.brocku.ca

(Klein) School of Mathematical Sciences, Sackler Faculty of Exact Sciences, Tel Aviv University, Tel Aviv, Israel 69978

E-mail address: aaklein@math.tau.ac.il