Math. J. Okayama Univ. 40 (1998), 1-6 [2000]

NILPOTENT DERIVATIONS and COMMUTATIVITY

HOWARD E. BELL*, ABRAHAM A. KLEIN, AND JASON LUCIER

Several years ago, Lee and Lee [3] proved the following interesting result:

Theorem 0.1. *Let R be a prime ring with center Z, let I be a nonzero ideal of R, and let n be a positive integer. If d is a derivation on R such that $d^n(I) \subseteq Z$, then either $d^n = 0$ or R is commutative.*

At about the same time, Trzepizur [6], as part of a slightly more general study, proved a related theorem.

Theorem 0.2. *Let n be a nonnegative integer, let R be a prime ring with char $R = 0$ or char $R > n+1$, and let Z be the center of R. If d is a derivation on R and S a subring of R such that $d(S) \subseteq S$ and $d^n(S) \subseteq Z$, then either $d^n(S) = \{0\}$ or $S \subseteq Z$.*

It is our purpose to continue the study of derivations on prime rings satisfying the condition $d^n(S) \subseteq Z$, where d is a derivation and S a suitably-chosen subring. Our first section contains results which are essentially applications of the Lee and Lee result; the second presents a theorem extending Theorem 0.2; the final section deals with the $d^n(S) \subseteq Z$ condition in prime rings with unrestricted characteristic.

Henceforth, R will always be a prime ring unless there is a statement to the contrary, and Z will be the center. It will be important to note that the center of a prime ring R contains no nonzero elements which are zero divisors in R. Of course, for $x, y \in R$, the symbol $[x, y]$ will denote the commutator $xy - yx$; and $C_R(S)$ will be the centralizer of the subset S of R. Not surprisingly, we shall make use of Leibniz' formula for higher derivatives

$$(*) \qquad d^n(xy) = \sum_{i=0}^{n} \binom{n}{i} d^i(x) d^{n-i}(y) \text{ for all } x, y \in R.$$

We shall also use the elementary fact that a group cannot be the union of two proper subgroups, which we call Property G.

1. Some results for special subrings.

We begin with two useful results on ideals contained in subrings.

Lemma 1.1 (4). *Let R be an arbitrary ring and S a subring of finite index in R. Then S contains an ideal of R which is of finite index in R.*

*Supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. 3961.

Lemma 1.2 (2). *Let R be an arbitrary ring. If d is a derivation on R such that $d^3 \neq 0$, then the subring generated by $d(R)$ contains a nonzero ideal of R.*

We return to our blanket assumption that R is prime.

Theorem 1.3. *Let R be infinite, and let S be a subring of finite index. If d is a derivation on R and $d^n(S) \subseteq Z$ for some positive integer n, then R is commutative or $d^n = 0$.*

Proof. By Lemma 1.1, S contains an ideal I of finite index in R; and since R is infinite, $I \neq \{0\}$. Our result now follows by Theorem 0.1.

Theorem 1.4. *Let n be a positive integer. Let d be a derivation on R, let K be the subring of R generated by $d(R)$, and suppose that $d^n(K) \subseteq Z$. Suppose also that one of the following holds: (i) $n \geq 3$; (ii) $n = 1$ and char $R \neq 2$; (iii) $n = 2$, char $R \neq 2$, and $d(Z) \neq \{0\}$. Then either R is commutative or $d^n = 0$.*

Proof. (i) If $d^3 = 0$, we are finished; hence we assume $d^3 \neq 0$. By Lemma 1.2, K contains a nonzero ideal; and our conclusion follows by Theorem 0.1.
(ii) We have $d^2(R) \subseteq Z$, so by Theorem 0.1, either R is commutative or $d^2 = 0$. In the latter case, the fact that char $R \neq 2$ yields $d = 0$.
(iii) Since $d^3(R) \subseteq Z$, either R is commutative or $d^3 = 0$, by Theorem 0.1; therefore, we may assume $d^3 = 0$. Since $d^2(d(x)d(y)) \in Z$ for all $x, y \in R$, we have $2d^2(x)d^2(y) \in Z$, hence

$$d^2(x)d^2(y) \in Z \quad \text{for all } x, y \in R. \tag{1.1}$$

Similarly, the fact that $d^2(d(x)d(y)d^2(w)) \in Z$ yields

$$d^2(x)d^2(y)d^2(w) \in Z \text{ for all } x, y, w \in R.$$

It follows from (1.1) that either $d^2(R) \subseteq Z$ or $d^2(x)d^2(y) = 0$ for all $x, y \in R$. In the first case, we are finished by Theorem 0.1; hence we assume that

$$d^2(x)d^2(y) = 0 \quad \text{for all } x, y \in R. \tag{1.2}$$

Taking $y = x \in Z$ and noting that Z contains no nonzero nilpotent elements, we get $d^2(Z) = \{0\}$. But for $z \in Z$ such that $d(z) \neq 0$, we then have $d^2(z^2) = 2d(z)^2 \neq 0$; hence (1.2) cannot hold, and we are finished.

Remark. For the $n = 2$ case, the final step of the proof shows that the possibility $d^2 = 0$ cannot occur, hence R must in fact be commutative. Moreover, the hypothesis that $d(Z) \neq \{0\}$ cannot be deleted, as we see by letting R be the ring of 2×2 matrices over a field of characteristic different from 2 and letting d be the inner derivation induced by the matrix e_{12}.

We now consider the commutator subring - i.e. the subring generated by all commutators in R. We have the following lemma.

Lemma 1.5 (5, p. 344, ex. 12). *Let R be noncommutative. Then the commutator subring H contains a nonzero ideal of R.*

The final theorem of this section is immediate from Theorem 0.1 and Lemma 1.5.

Theorem 1.6. *Let H be the commutator subring of R. If d is a derivation on R and $d^n(H) \subseteq Z$ for some positive integer n, then R is commutative or $d^n = 0$.*

2. Some results for prime rings with restricted characteristic.

Theorem 2.1. *Let S be a subring of R. If there exists a derivation d on R such that $\{0\} \neq d(S) \subseteq Z$, then S is commutative. Moreover, if char $R \neq 2$, then $S \subseteq Z$.*

Proof. For all $s, t \in S$ we have $[d(st), s] = 0 = [d(s)t, s] + [sd(t), s] = d(s)[t, s]$. Thus, for fixed $s \in S$, either $d(s) = 0$ or $[t, s] = 0$ for all $t \in S$. By Property G and our hypothesis that $d(S) \neq \{0\}$, we conclude that S is commutative.

Now suppose that char $R \neq 2$. For all $s \in S$, we have $d(s^2) = 2sd(s) \in Z$, hence $2[s, x]d(s) = 0 = [s, x]d(s)$ for all $x \in R$. As before, we see that for fixed $s \in S$, either $d(s) = 0$ or $s \in Z$; and by Property G, $S \subseteq Z$.

Remark. If char $R = 2$, then $d(S) \subseteq Z$ does not imply $S \subseteq Z$. Indeed, let R be the ring of 2×2 matrices over $GF(2)$, let $S = \{0, e_{21}\}$ and let d be the inner derivation determined by e_{12}. Then $d(S) = \{0, 1\} = Z$, but clearly $S \not\subseteq Z$.

We come now to the main theorem of this section.

Theorem 2.2. *Let n be a positive integer, and let char $R = 0$ or char $R > n$. If d is a derivation on R and S is a subring of R such that $d(S) \subseteq S$ and $d^n(S) \subseteq Z$, then either S is commutative or $d^n(S) = \{0\}$. Moreover, if $d^n(S) \neq 0$ and char $R > n + 1$, then $S \subseteq Z$.*

Proof. We need only establish that either S is commutative or $d^n(S) = \{0\}$; the rest follows from Theorem 0.2.

For $n = 1$, the result is part of Theorem 2.1. Proceeding from $n - 1$ to n, we assume $d^n(S) \subseteq Z$ and $d^{n-1}(S) \not\subseteq Z$. If char $R > n + 1$, our result is included in Theorem 0.2, so we may assume that char$R = n + 1$, in which case $n + 1$ is prime and d^{n+1} is a derivation. By applying Theorem 2.1 with d^{n+1} in place of d, we see that if $d^{n+1}(S) \neq \{0\}$, then S is commutative. Therefore we may assume that

$$d^{n+1}(S) = \{0\}. \tag{2.1}$$

Of course $d^n(xy) \in Z$ for all $x, y \in S$, so by (*) we have

$$\sum_{i=0}^{n} \binom{n}{i} d^{n-i}(x) d^i(y) \in Z \text{ for all } x, y \in S.$$

Commuting with y gives

$$\sum_{i=1}^{n-1} \binom{n}{i} d^{n-i}(x)\left[d^i(y),y\right] + \sum_{i=1}^{n-1} \binom{n}{i}\left[d^{n-i}(x),y\right] d^i(y) + [x,y]d^n(y) = 0$$

for all $x, y \in S$. Substituting $d^{n-1}(y)$ for y, we now get

$$n\left[d^{n-1}(x), d^{n-1}(y)\right] d^n(y) = 0 \text{ for all } x, y \in S.$$

Thus, for each $y \in S$, either $d^n(y) = 0$ or $\left[d^{n-1}(x), d^{n-1}(y)\right] = 0$ for all $x \in S$; and by Property G, either $d^n(S) = \{0\}$ or $\left[d^{n-1}(x), d^{n-1}(y)\right] = 0$ for all $x, y \in S$.

If the first of these conditions holds, we are finished; hence, we assume the second holds. Two applications of the following lemma will complete the proof.

Lemma 2.3. *If R satisfies the hypotheses of Theorem 2.2 and $d^n(S) \neq \{0\}$, then*

$$C_R(d^{n-1}(S)) \subseteq C_R(S).$$

Proof. Let $y \in C_R\left(d^{n-1}(S)\right)$. Then $\left[d^{n-1}(xw), y\right] = 0$ for all $x, w \in S$; and applying (*) to $d^{n-1}(xw)$ and performing standard commutator calculations, we get

$$\sum_{i=0}^{n-1} \binom{n-1}{i} d^{n-1-i}(x)\left[d^i(w),y\right] + \sum_{i=0}^{n-1} \binom{n-1}{i}\left[d^{n-1-i}(x),y\right] d^i(w) = 0$$
$$\text{for all } x, w \in S.$$

In this equation, we replace x by $d^{n-1}(x), d^{n-2}(x), ..., d(x)$ in turn and use (2.1), thereby obtaining $n-1$ equations, the j-th of which has the form

$$\binom{n-1}{j} d^n(x)\left[d^{n-1-j}(w),y\right] + f_j = 0,$$

where $f_j = f_j(x,w,y,d)$ is a sum of products each having a factor $\left[d^t(u),y\right]$ with $t > n-1-j$. Since R is $\binom{n-1}{j}$-torsion-free and since $d^n(S) \neq \{0\}$, a backward induction shows at once that $[w,y] = 0$ for all $w \in S$; hence $y \in C_R(S)$.

3. Some results for prime rings of arbitrary characteristic.

If R is a prime ring with center $Z \neq \{0\}$, localizing at $Z \setminus \{0\}$ yields a prime ring $\overline{R}$ with center $\overline{Z}$ equal to the quotient field of Z. Clearly $\overline{R}$ may be regarded as a vector space over $\overline{Z}$. We call R small (resp. big) if $\overline{R}$ is finite (resp. infinite) dimensional over $\overline{Z}$.

If S is a (not necessarily prime) subring of R with $ZS \subseteq S$, we give $\overline{S}$ the obvious meaning and define S to be a small or big subring of R according as $\overline{S}$ is a finite-dimensional or infinite-dimensional subspace of $\overline{R}$. In a big ring, big subrings are not hard to find, as the next theorem shows.

Theorem 3.1. *A nonzero left ideal of a big ring R is big.*

Proof. Let L be a nonzero left ideal of the big ring R. Let $\overline{R}, \overline{Z}$, and $\overline{L}$ be as usual. Suppose $\overline{L}$ is a finite-dimensional subspace of $\overline{R}$ with basis $\{v_1, v_2, ..., v_n\}$. Then for any $\overline{x} \in \overline{R}$, $\overline{x}v_j \in \overline{L}$, hence $\overline{x}v_j = \sum_{i=1}^{n} a_{ij}v_i$. Thus we have a representation $\overline{R} \to M_n(\overline{Z})$ given by $\overline{x} \longmapsto [a_{ij}]$. Since R is big, the kernel $\overline{K}$ of the representation is a nonzero ideal of $\overline{R}$ with $\overline{K}\,\overline{L} = \{0\}$, contradicting the fact that $\overline{R}$ is prime. Therefore $\overline{L}$ is infinite-dimensional and L is big.

We come now to our major result on big subrings.

Theorem 3.2. *Let R be a big ring with center $Z \neq \{0\}$, and let S be a big subring of R. If there exists a derivation d on R such that $d(S) \subseteq S$ and $d^n(S) \subseteq Z$ for some positive integer n, then either $d^n(S) = \{0\}$ or S is commutative.*

Proof. Again we use induction on n. If $n = 1$, the result is included in Theorem 2.1; hence we proceed on the assumption that $d^n(S) \subseteq Z$ and $d^{n-1}(S) \not\subseteq Z$. Following the argument used in the first four paragraphs of the proof of Theorem 1 of [3], with R replaced by S whenever necessary, we obtain $d(Z) = \{0\}$.

Now we localize R at $Z\backslash\{0\}$, obtaining $\overline{R}$, $\overline{Z}$ and $\overline{S}$ as above. Since $d(Z) = \{0\}$, we can define a derivation $\overline{d}$ on $\overline{R}$ by $\overline{d}\left(\frac{x}{z}\right) = \frac{d(x)}{z}$ for all $x \in R$ and $z \in Z\backslash\{0\}$; and we have $\overline{d}(\overline{S}) \subseteq \overline{S}$ and $\overline{d}^n(\overline{S}) \subseteq \overline{Z}$. Therefore, $\overline{d}^n(\overline{S})$ has dimension at most 1 over $\overline{Z}$.

Proceeding as in the sixth paragraph of the proof of Theorem 1 of [3], we show that if $\overline{d}^k(S)$ is finite-dimensional over $\overline{Z}$, then either $\overline{d}^{k-1}(\bar{S})$ is finite-dimensional or $\overline{d}^n(\overline{S}) = \{0\}$. Hence either $\overline{S}$ is finite-dimensional or $\overline{d}^n(\overline{S}) = \{0\}$. But the first of these alternatives is ruled out by our hypothesis that S is big, hence $\overline{d}^n(\overline{S}) = \{0\}$; and it follows that $d^n(S) = \{0\}$.

If char $R \neq 2$, then by Theorem 2.1 the $n = 1$ case yields the stronger conclusion that $S \subseteq Z$ or $d(S) = \{0\}$; and the assumption that S is big rules out the possibility that $S \subseteq Z$. Thus the same inductive argument that we have just used gives

Corollary 3.3. *Let R be a big ring with char $R \neq 2$ and center $Z \neq \{0\}$, and let S be a big subring of R. If there exists a derivation d on R such that $d(S) \subseteq S$ and $d^n(S) \subseteq Z$ for some positive integer n, then $d^n(S) = \{0\}$.*

Of course, Theorem 3.1 yields an interesting application of Theorem 3.2. However, this result is a special case of our final theorem.

Theorem 3.4. *Let R be an arbitrary prime ring. Let L be a left ideal of R. If d is a derivation on R such that $d^n(L) \subseteq Z$ for some positive integer n, then either R is commutative or $d^n(L) = \{0\}$.*

Proof. We may assume that $Z \neq \{0\}$ and $L \neq \{0\}$. Moreover, by replacing L by $L + d(L) + d^2(L) + ...$ if necessary, we may assume $d(L) \subseteq L$. Repeating the first two paragraphs of the proof of Theorem 3.2 with L in place of S, we obtain $\overline{d}^n(\overline{L}) \subseteq \overline{Z}$; and since $\overline{d}^n(\overline{L}) \subseteq \overline{L}$, we have $\overline{d}^n(\overline{L}) \subseteq \overline{L} \cap \overline{Z}$. Now $\overline{Z}$ is a field, hence $\overline{L} \cap \overline{Z} = \{0\}$ or $\overline{L} = \overline{R}$; therefore either $\overline{d}^n(\overline{L}) = \{0\}$ or $\overline{d}^n(\overline{R}) \subseteq \overline{Z}$, and our result follows from Theorem 0.1.

Corollary 3.5. *Let R be an arbitrary prime ring, and let L be a nonzero left ideal of R. If d is a derivation on R such that $d^n(L) \subseteq Z$ for some positive integer n, then either R is commutative or $d^{2n-1} = 0$.*

Proof. In [1], Chung and Luh proved that if $d^n(L) = \{0\}$, then $d^{2n-1} = 0$.

References

[1] L. O. Chung and J. Luh, Nilpotency of derivatives on an ideal, Proc. Amer. Math. Soc. 90 (1984), 211-214.
[2] I. N. Herstein, A note on derivations, Canad. Math. Bull. 21 (1978), 369-370.
[3] P. H. Lee and T. K. Lee, Note on nilpotent derivations, Proc. Amer. Math. Soc. 98 (1986), 31-32.
[4] J. Lewin, Subrings of finite index in finitely-generated rings, J. Algebra 5 (1967), 84-88.
[5] L. H. Rowen, Ring Theory I, Academic Press, 1988.
[6] A. Trzepizur, Differential rings with central derivatives of higher order, Math. J. Okayama Univ. 27 (1985), 7-9.

Howard E. Bell
Department of Mathematics
Brock University
St. Catharines, Ontario
Canada L2S 3A1

Abraham A. Klein
School of Mathematical Sciences
Tel Aviv University,Ramat Aviv
69978 Tel-Aviv, Israel

Jason Lucier
Department of Mathematics
University of Waterloo
Waterloo, Ontario
Canada N2L 3G1

(*Received September 9, 1998*)