Can. J. Math. Vol. **44** (3), 1992 pp. 553–560

LIE IDEALS AND CENTRAL IDENTITIES WITH DERIVATION

CHARLES LANSKI

ABSTRACT. In this paper we consider various degree two central polynomials with derivation, holding for Lie ideals in prime rings. The results give substantial generalizations of the existing ones on central and semi-centralizing derivations, and show essentially that there are no central identities of the form $p(x,y) = c_1xy^D + c_2x^Dy + c_3yx^D + c_4y^Dx$, where D is a nonzero derivation of the prime ring R.

This paper deals with certain identities involving a derivation, which hold in a prime ring R. The results are related to those in the literature on centralizing derivations and also show that there are no degree two central polynomials with derivation. Our main result is that if $[xx^D, x^Dx] = 0$ for all x in a Lie ideal of R, then R satisfies S_4, the standard identity of degree four. While this result seems somewhat special, it is appealing in form, enables us to generalize considerably a number of existing results on centralizing derivations ([4], [6], [9], [11], [13] and [14]), demonstrates the utility of recent work of C. L. Chuang [2] on differential identities in prime rings, and both naturally arises and is important in studying certain degree two identities with derivation. It is the study of such identities which motivates the work here. We have shown [8] that a prime ring not satisfying a polynomial identity cannot satisfy a degree two multilinear polynomial differential identity $p(x^d, y^h)$, but questions remain about the existence of such identities for rings satisfying a polynomial identity, and about related identities in general. For example, can R satisfy an identity of the form $p(x,y) = c_1xy^D + c_2x^Dy + c_3yx^D + c_4y^Dx$, or more generally, can $p(x,y)$ be central? These are not polynomial differential identities as studied in [8] since the same variable occurs both with and without the derivation applied, but their consideration is important in trying to classify differential identities of minimal degree.

In investigating such an identity, it is clear that specializing $x = y$ gives an identity $axx^D + bx^Dx$, which implies the commutativity of xx^D with x^Dx, at least if not both coefficients are zero. This commutativity condition is clearly related to the notation of centralizing derivation and its generalizations. The first result of this type was Posner's theorem [14] which proved that R must be commutative if a nonzero derivation D is centralizing; that is, if $xx^D - x^Dx \in Z$, the center of R, for all $x \in R$. This result was extended to the cases when D is centralizing on an ideal of R ([4] and [13]) or on a Lie ideal of R ([9] and [11]). Assuming instead that $xx^D + x^Dx \in Z$ for all x in an ideal, will still force R to be commutative, as will the assumption that D is semi-centralizing on an ideal, which means that for all x in an ideal I, $xx^D + f(x)x^Dx \in Z$, for $f\colon I \longrightarrow \{1, -1\}$

Received by the editors April 23, 1990.

AMS subject classification: Primary: 16A72; secondary: 16A38, 16A66, 16A12.

([4] and [6]). All of these results imply that xx^D commutes with x^Dx. Thus the identity $[xx^D, x^Dx] = 0$ will be the initial focus of our study. The work of Chuang [2] is important here because it applies in the case of nonmultilinear identities, and so, enables us to avoid both more complicated calculation and the consideration of characteristic which would be necessary if one had to linearize the identity.

Throughout the paper, R will denote a prime ring with center Z, extended centroid C, and Martindale quotient ring Q [13]. A Lie ideal L of R is an additive subgroup of R so that $[x,r] = xr - rx \in L$ for all $x \in L$ and $r \in R$. A bracket of Lie ideals, such as $[L_1, L_2]$ means the additive subgroup generated by all $[x,y]$ for $x \in L_1$ and $y \in L_2$. We shall require two well known facts about Lie ideals. First, either $L \subset Z$ or L is noncommutative, meaning that $[L,L] \neq 0$, unless char $R = 2$ and R satisfies the standard polynomial S_4, and second, if L is noncommutative then $[M,M] \subset L$ for M the ideal of R generated by $[L,L]$ [10; Theorem 4, p. 118 and Theorem 13, p. 123].

Let D be a nonzero derivation of R. It is easy to check that D extends uniquely to a derivation of Q, so restricts to a derivation of the central closure $RC + C$ of R (see [2] or [7]). We say that D is *inner* if its extention to Q is the inner derivation $\mathrm{ad}(A)(x) = xA - Ax$. As discussed above, we are interested in showing that R is commutative if $[xx^D, x^Dx] = 0$ for all $x \in L$, a noncommutative Lie ideal of R. Now this conclusion cannot always hold, since if $R = M_2(F)$ for F a field, and if $L = [R,R]$, then it is easy to see that $x^2 \in Z$ for all $x \in L$. Apply D to $x^2 \in Z$ to obtain $xx^D + x^Dx \in Z$, which forces $[xx^D, x^Dx] = 0$. Thus, instead of showing that R is commutative, we must try to prove that R satisfies S_4, or equivalently, that R embeds in $M_2(F)$ for F a field [5; Theorem 2, p. 57].

Our approach uses the work of C. L. Chuang [2] to show that D is an inner derivation and that R satisfies a generalized polynomial identity, and then to argue that R must satisfy S_4. We can now state our first result.

THEOREM 1. *Let R be a prime ring, L a noncommutative Lie ideal of R, and D a nonzero derivation of R. If for all $x \in L$, $[xx^D, x^Dx] = 0$, then R satisfies S_4.*

PROOF. Let M be the nonzero ideal of R generated by $[L,L]$. Since $[M,M] \subset L$ [9; Lemma 2, p. 280], replacing x with $[x,y]$, for $x, y \in M$ shows that

$$\left[[x,y]([x^D,y] + [x,y^D]), ([x^D,y] + [x,y^D])[x,y]\right] = 0 \tag{1}$$

holds for all $x, y \in M$. This is a differential identity satisfied on M, so by the main result of Chuang [2; Main Theorem, p. 255 and Remark 1, p. 278], if D is an outer derivation on Q, then in (1) we may replace x^D and y^D with new variables to obtain a new identity for R. Denote this new identity by $g(x,y,z,t) = \left[[x,y][z,y] + [x,y][x,t], [z,y][x,y] + [x,t][x,y]\right] = 0$, and set $t = 0$ to yield the identity $f(x,y,z) = \left[[x,y][z,y], [z,y][x,y]\right] = 0$. Thus R satisfies a polynomial identity of degree 8, and it follows that $f(x,y,z)$ is an identity for $RC = RZ^{-1}$ [5; Theorem 2, p. 57]. If C is finite, then $RC \cong M_n(C)$, and $n \leq 4$ [3; p. 41]. If C is infinite then $RC \otimes F \cong M_n(F)$ satisfies $f(x,y,z)$ for F a splitting field of RC [5; Lemma 1, p. 89], and again $n \leq 4$. Since we want $n = 2$, assume that $R = M_n(F)$ for $n \geq 3$ and let $\{e_{ij}\}$ be the usual matrix units. A simple computation shows that

$f(e_{21}-e_{12},e_{11},e_{31}-e_{13}) \neq 0$, so we must conclude that $n=2$, and R satisfies S_4, or else D is an inner derivation.

Assuming now that $D = \mathrm{ad}(A) \neq 0$, we have that $p(x) = \big[x[x,A],[x,A]x\big]$ is an identity on L. As above, replacing x with $[x,y]$ for $x,y \in M$ shows that $p([x,y])$ is a generalized polynomial identity (GPI) on M and is not trivial since $A \notin C$. Consequently, $f([x,y])$ is a GPI for R [2; Proposition 4, p. 267]. It follows that R satisfies a GPI with coefficients in R [1; Theorem 3, p. 725], so by Martindale's theorem [12; Theorem 3, p. 579] RC is a primitive ring with $H = \mathrm{Soc}(RC) \neq 0$ and $eRCe$ is finite dimensional over C for any primitive idempotent e in RC. We want to show next that $p(x)$ holds on $[H,H]$, which would be easy to see if $p(x)$ were multilinear.

If C is finite, then the definition of Q shows that there is a nonzero ideal I of R with $I \subset M$ and $IC \subset M$, from which it follows that $[IC,IC] \subset [M,M] \subset L$. Hence $p(x)=0$ holds for $x \in [IC,IC]$, and so for $x \in [H,H]$ since H is the minimal ideal of RC. Note that $eHe = eF$ for any primitive idempotent $e \in H$, where F is a finite extension of C. Fairly standard arguments give the same conclusion when C is infinite. The only problem is that we cannot evaluate $p(x)$ at arbitrary C-linear combinations of elements of L. Briefly, consider the formal expression $p(z_1x_1+\cdots+z_4x_4)$, where the z_j are indeterminates commuting with the $\{z_j,x_j\}$, and expand in $\{m\}$ of monomials of degree four in the $\{z_j\}$ to obtain $\sum mf_m$. Now fix a set of at least seven elements $\{z_j\} \subset C$ and an ideal I of R with $I \subset M$ and $z_jI \subset M$. For $x_i \in [I,I]$, $z_jx_i \in [M,I] \subset [M,M] \subset L$, and so, given a fixed choice of $x_1,\ldots,x_4$ with various choices of the z_j as coefficients, by using a Vandermonde determinant argument one can conclude that each $f_m(x_1,\ldots,x_4)=0$. Since $p(x)$ is of degree four, it follows that $p(x)=0$ for $x \in C[I,I] = [CI,CI] \supset [H,H]$. Indeed, the argument shows that $p(x)$ is an identity for $x \in [IC,IC]\otimes F$, for any extension field of C, and so for $x \in [H\otimes F,H\otimes F] \cong [\mathrm{Soc}(RC\otimes F),\mathrm{Soc}(RC\otimes F)]$. The upshot of these computations is that regardless of the cardinality of C we may essentially reduce to H. That is, since $H^D \subset H$ [7; p. 766 and Lemma 7, p. 779], $D=\mathrm{ad}(A)$ is a nonzero derivation on H (and on $H\otimes F$), $p(x)=0$ for $x \in [H,H]$, and for each primitive idempotent $e \in H$, $eHe = eF$ for F a field. Note also that $A \in Q \subset Q(RC\otimes F) \cong Q(H\otimes F)$.

If H fails to contain three orthogonal idempotents, then we are finished since it is either commutative or is $M_2(F)$. But R is not commutative, so H cannot be, and R satisfies S_4 if H does. Therefore, we may assume that e,f, and g are orthogonal rank one idempotents in H, and that, for example, $eHe = eF$. Our goal is to obtain the contradiction that $D=0$. Observe that for any $h \in H$, $ehf = [eh,f] \in [H,H]$, and that $1+ehf = v$ acts formally as an automorphism of H; specifically, for $r \in H$, $r^v = vrv^{-1} = r + ehfr - rehf - ehfrehf$. Assume that $eAg \neq 0$ and set $u = 1-ghf$ for $h \in H$. Now $[H,H]^u = [H,H]$, so for any $x \in [H,H]$, $up(u^{-1}xu)u^{-1} = 0$, and it follows that in $p(x)$, A may be replaced with $A^u = A - ghfA + Aghf - ghfAghf$. In particular, $eA^ug = eAg \neq 0$, and $eA^uf = eAf + eAghf$. Since e,f, and g are rank one, there is a choice of h, possibly $h=0$, so that $eA^uf = 0$. To contradict the existence of $\{e,f,g\}$, we may without loss of generality replace A with A^u, and so assume that $eAg \neq 0$ and $eAf = 0$.

For $x \in [H,H]$ with $x^3 = 0$, it is straightforward to see that $p(x) = x^2AxAx - x^2A^2x^2 + xAxAx^2 = 0$, and so, $xp(x) = x^2AxAx^2 = 0$. Choose $x = grf + fte$ with $r,t \in H$

and satisfying $x^2 = grfte \neq 0$. Using $x^2AxAx^2 = 0$ together with $eAf = 0$ yields $grfteAgrfAgrfte = 0$. Since none of grf, fte, or eAg is zero, and all the idempotents have rank one, we are forced to conclude that $fAg = 0$. Now set $x = fre + gte + gwf$ with $r, t, w \in H$ and satisfying $x^2 = gwfre \neq 0$, and compute $fp(x) = freAxAgwfre = 0$. But $eAf = 0 = fAg$, so $freAgteAgwfre = 0$ and this contradicts $eAg \neq 0$ since e, f, and g are all rank one. Therefore, we must have $eAg = 0$ for e and g distinct idempotents in any set of three or more rank one orthogonal idempotents.

To finish the proof we show that $D = 0$. Let $\{e_i\}$ be any set of at least three rank one orthogonal idempotents. As we have seen, for $i \neq j$ and $u = 1 - e_ire_j$, both $e_iAe_j = 0$ and $e_iA^ue_j = 0$. These observations yield $0 = e_iA^ue_j = -e_ire_jAe_j + e_iAe_ire_j$. Now $HA + AH \subset H$ [7; p. 766 and Lemma 7, p. 779], so $e_iAe_i \in e_iHe_i$, $e_iAe_i = c_ie_i$ for some $c_i \in F$, and it follows from the last computation that $(c_i - c_j)e_ire_j = 0$. Thus $e_iAe_i = ce_i$ for all i. Given any $h \in H$, by Litoff's theorem [8; p. 235], there is an idempotent e so that $h, hA, Ah \in eHe$. Therefore, there is a set of $\{e_i\}$ as above so that $h = \sum he_i = \sum e_ih$, $Ah = \sum e_jAh$, and $hA = \sum hAe_j$. Thus, $Ah = \sum e_jAh = \sum e_jA(\sum e_ih) = c\sum e_ih = ch$ and $hA = \sum hAe_i = \sum(\sum he_j)Ae_i = \sum he_ic = ch$, which result in $[h, A] = 0$. Since this holds for each $h \in H$, we must have $H^D = 0$. This contradiction shows that H cannot have three orthogonal idempotents and finishes the proof of the theorem.

We shall see shortly that Theorem 1 is important in the consideration of degree two identities involving a derivation, and gives a genuine extension to Lie ideals of the various results on centralizing or semi-centralizing derivations. One would naturally like to obtain the existing results from ours, and the only real difference is that they start with an ideal of R, rather than a Lie ideal, and conclude that R must be commutative. Our next theorem uses Theorem 1 to get the stronger conclusion that R is commutative when one starts with an ideal.

THEOREM 2. *Let R be a prime ring, I a nonzero ideal of R, and D a nonzero derivation of R. If $p(x) = [xx^D, x^Dx] = 0$ for all $x \in I$, then R is commutative.*

PROOF. Assume that R is not commutative, so that I is not commutative [3; Corollary, p. 7]. Since I is clearly a Lie ideal of R, we may apply Theorem 1 to conclude that R satisfies S_4. Suppose first that $D = \mathrm{ad}(A)$ is an inner derivation and that $R = M_2(F)$ for F a field. Of course, now $I = R$. Since for any unit $v \in R$, $vp(x)v^{-1} = 0$, we can replace A by any conjugate and so assume that A is in rational canonical form. With this assumption, the computation $p(e_{11}) = 0$ forces A to be singular, and this condition must still hold if A is replaced with $A + fI_2$ for any scalar. Hence, $C = \mathrm{GF}(2)$ and A is similar to e_{11}. But now $p(e_{11} + e_{12} + e_{21}) \neq 0$, and this contradiction forces R to be commutative. Thus, assuming that R is not commutative, it suffices to show that R can be replaced with $M_2(F)$, and that D is inner.

Since R satisfies S_4, $RZ^{-1} = RC$ is a simple algebra four dimensional over C, the quotient field of Z [5; Theorem 2, p. 57 and Theorem, p. 17]. If C is finite, then $R \cong M_2(C)$, D must be inner, and we are done. When C is infinite, but D is outer, proceed as in Theorem 1 and apply the results in [2] to the identity $[xx^D, x^Dx]$ to conclude that

$[xy, yx]$ is an identity for RC, and so by standard arguments, for $M_2(F) \cong RC \otimes F$, for F a splitting field for RC. The contradiction obtained by setting $x = e_{12} + e_{21}$ and $y = e_{22}$ forces D to be inner. Once again, since $p(x)$ is now a GPI holding for I, it holds for RC [2; Proposition 4, p. 267], and since C is infinite, for $M_2(F)$ as above, completing the proof of the theorem.

Combining the last two results with our introductory remarks leads immediately to the following corollaries. The first generalizes results on semi-centralizing derivations, not only to Lie ideals, but allows variable coefficients as well.

COROLLARY 1. *Let R be a prime ring, L a noncommutative Lie ideal of R, and D a nonzero derivation of R. If $f(x)xx^D + g(x)x^Dx \in C$ for each $x \in L$ and some $f, g\colon L \longrightarrow C$ satisfying $\big(f(x), g(x)\big) \neq (0,0)$ for each $x \in L$, then R satisfies S_4. If in addition, L is an ideal of R, then R must be commutative.*

The next corollary explicitly gives [4; Theorem 1(2), p. 125], [6; Theorem 1, p. 11], and [13; Theorem 1, p. 124], and their extensions to Lie ideals.

COROLLARY 2. *Let R be a prime ring, L a noncommutative Lie ideal of R, and D a nonzero derivation of R. If for all $x \in L$, $xx^D + f(x)x^Dx \in Z$, for $f\colon L \longrightarrow \{-1, 1\}$, then R satisfies S_4. If L is an ideal of R, then R must be commutative.*

In order to completely characterize degree two central polynomials with derivation, we need a more precise version of Corollary 1 for fixed coefficients which will show that the only exception when R satisfies S_4 must arise from the fact that squares of elements in $[R, R]$ are central. First a short lemma isolates a special case of the result we need.

LEMMA. *Let R be a prime ring satisfying S_4, L a noncommutative Lie ideal of R, and D a nonzero outer derivation of R. If $xx^D \in Z$, or if $x^Dx \in Z$, for all $x \in L$, then R is commutative.*

PROOF. Assume that R is not commutative, and that $xx^D \in Z$. Linearize this relation to obtain $p(x, y) = xy^D + yx^D \in Z$ for all $x, y \in L$. Since D is outer, there is $w \in Z$ so that $w^D \neq 0$ [7; Theorem 2, p. 778]. If M is the ideal of R satisfying $[M, M] \subset L$, then $wx \in L$ for $x \in [M, M]$, and so, $p(wx, y) = wp(x, y) + w^Dyx \in Z$. By choice of w, it follows that $yx \in Z$, for $x, y \in [M, M]$. As in the proof of Theorem 2, $RC = RZ^{-1}$ and $H = M_2(F) \cong RC \otimes F$, for F a splitting field of RC. Now $MC \cong RC$, so $[M, M]C \otimes F \cong [H, H]$, and we may conclude that $yx \in F$ for $x, y \in [H, H]$. But $H = [H, H]^2$ gives the contradiction that R is commutative. A similar argument proves the Lemma if $x^Dx \in Z$ for all $x \in L$.

COROLLARY 3. *Let R be a prime ring, L a noncommutative Lie ideal of R, and D a nonzero derivation of R. If for all $x \in L$, $p(x) = cxx^D + zx^Dx \in C$ for $c, z \in C$, then either $c = z = 0$, R is commutative, or $c = z$ and R satisfies S_4. If L is an ideal of R, then $c = z = 0$ or R is commutative.*

PROOF. Assume that not both c and z are zero. Applying Corollary 1 gives the second statement, and shows that R must satisfy S_4. It is easy to see that $y^2 \in Z$ for $y \in [R, R]$, so if $x \in [M,M] \subset L$ it follows that $xx^D + x^Dx \in Z$. Combining this with $p(x)$ shows that $(c - z)xx^D \in C$. By the Lemma, if D is an outer derivation, then $c = z$ or R is commutative, and we are finished. Assuming $D = \mathrm{ad}(A)$, we may now take $R = M_2(F)$ and $L = [R,R]$, as in the last paragraph of the proof of Theorem 2. Also, by conjugating $p(x)$ we may assume that A is in rational canonical form. But now $p(e_{12}) = (z-c)e_{12} \in F$, forcing $c = z$, and completing the proof of the corollary.

Our last result uses Corollary 3 to show that a Lie ideal of R cannot satisfy a degree two multilinear identity with one derivation applied, with two exceptions. For $R = M_2(F)$, any element of trace zero has its square central, so for $A, B \in [R,R] = L$, $AB + BA$ is central. Since $B^D \in [R,R]$ for any derivation D, one has $AB^D + B^DA \in F$. In addition, when $\mathrm{char}\, R = 2$, then $L = [R,R]$ satisfies $[L,L] \subset F$, so if $D = \mathrm{ad}(A)$ for $A \in L$, then $[x,y]^D \in F$ for any $x, y \in R$. Expanding this gives the central differential polynomial $xy^D + x^Dy + yx^D + y^Dx \in F$ satisfied on R.

THEOREM 3. *Let R be a prime ring, L a noncommutative Lie ideal of R, and D a nonzero derivation of R. If for all $x, y \in L$, $p(x,y) = c_1xy^D + c_2x^Dy + c_3yx^D + c_4y^Dx \in C$ for $\{c_i\} \subset C$, then one of the following holds;*

i) all $c_i = 0$;

ii) R is commutative; or,

iii) R satisfies S_4, $c_1 = c_4$, $c_2 = c_3$, and

a) if $L \subset [RC, RC]$, then L satisfies $xy^D + y^Dx \in Z$, or

b) if $L \not\subset [RC, RC]$, then $\mathrm{char}\, R = 2$, all $c_i = c \neq 0$, and $D = \mathrm{ad}(A)$ is an inner derivation on RC, with $A \in [RC, RC]$.

If L is an ideal of R, then all the $c_i = 0$, R is commutative, or $\mathrm{char}\, R = 2$, all $c_i = c \neq 0$, and $D = \mathrm{ad}(A)$ is an inner derivation on RC, with $A \in [RC, RC]$.

PROOF. Set $x = y$ to obtain the relation $(c_1 + c_3)xx^D + (c_2 + c_4)x^Dx \in C$, and apply Corollary 3. The theorem is proved if R is commutative, so assume henceforth that this is not the case, and proceed with the assumption that R satisfies S_4 and that $c_1 + c_3 = c_2 + c_4$. Our argument will also handle the case when L is an ideal and R satisfies S_4. We begin with some observations which hold because R satisfies S_4. As we have seen before, $RZ^{-1} = RC$ and $H = M_2(F) \cong RC \otimes F$, for F a splitting field of RC, where either $F = C$ or F is a separable quadratic extension of C. Consequently, the action of D on C extends uniquely to F [15; Corollary 2, p. 124], and so D extends to H by setting $(a \otimes f)^D = (a^D \otimes f) + (a \otimes f^D)$. Set $U = LC \otimes F$ and observe that U is a Lie ideal and F-subspace of H, so that either $U = [H,H]$ or $U = H$. Also, if M is the ideal in R satisfying $[M,M] \subset L$, then $[M,M]C \otimes F = [H,H]$. Now $[H,H]^D \subset [H,H]$, so for $x, y \in [H,H]$, $y^D \in [H,H]$ as well and $xy^D + y^Dx \in F$ follows from our comments preceeding the theorem.

For any $x, y \in [M,M] \subset [H,H]$, $g(x,y) = (c_1 - c_4)xy^D + (c_2 - c_3)x^Dy = p(x,y) - c_4(xy^D + y^Dx) - c_3(x^Dy + yx^D) \in C$. Since $c_1 + c_3 = c_2 + c_4$, we have $c_1 - c_4 = c_2 - c_3 = c$, and if $c \neq 0$, then $(xy)^D \in Z$ results. Should D be an inner derivation, then it is easy to see that $(xy)^D \in F$ holds for $x, y \in [H,H]$. But $[H,H]^2 = H$, so we must conclude that $H^D \subset F$, which implies that $[H,H]^D = 0$. Hence, the contradiction $D = 0$ follows from the fact that $[H,H]$ generates H. Thus, we may assume that D is an outer derivation, and as in the Lemma, there is $w \in Z$ with $w^D \neq 0$. Observing that $wx \in [M,M]$ for $x \in [M,M]$, we have $\big((wx)y\big)^D = w^D xy + w(xy)^D \in Z$. This implies that $xy \in Z$ for $x, y \in [M,M]$, and again as in the Lemma, this gives the contradiction that R is commutative. Consequently, we must have $c = 0$, so $c_1 = c_4$ and $c_2 = c_3$, and we may write $p(x,y) = c(xy^D + y^D x) + z(x^D y + yx^D)$. If $U = [H,H]$, then for all $x, y \in L$, $x, y^D \in U$, and so $xy^D + y^D x \in Z$, proving the theorem.

We may now assume that $U = H$, which includes the situation when L is an ideal of R. If D is an outer derivation, and $w \in Z$ with $w^D \neq 0$, then for $x \in [M,M]$ and $y \in L$, $p(wx,y) = wp(x,y) + zw^D(xy + yx) \in Z$. It follows that $xy + yx \in Z$ as long as $z \neq 0$. When $z = 0$, then using $p(y,wx) \in Z$ will give $xy + yx \in Z$, unless $c = 0$, which would mean that all $c_i = 0$. Therefore, $xy + yx \in Z$ for all $x \in [M,M]$ and $y \in L$. Since $xy + yx$ is multilinear, we can extend to H and obtain $xy + yx \in F$ for $x \in [H,H]$ and $y \in U = H$. A contradiction arises by taking $x = e_{12}$ and $y = e_{22}$. Consequently, $D = \mathrm{ad}(A)$ must be an inner derivation.

Now that D is inner, $p(x,y)$ is multilinear so our hypothesis extends to H; that is, $p(x,y) \in F$ for $x, y \in U = H$. For $e \in H$ an idempotent, $p(e,e) = (z + c)(ee^D + e^D e) = (z + c)e^D \in F$. If $z + c \neq 0$, then $e^D \in F$ for all idempotents, and since H is spanned over F by its idempotents, it follows that $H^D \subset F$. As above, this forces $D = 0$. Hence $z + c = 0$, and we are clearly done if $c = 0$. We may harmlessly replace $p(x,y)$ with $c^{-1}p(x,y) = xy^D + y^D x - x^D y - yx^D$. For $x \in F$, $p(x,y) = 2xy^D \in F$, and this yields $H^D \subset F$ when $\mathrm{char}\, H \neq 2$. We have already seen that this condition gives the contradiction $D = 0$, so we must have $\mathrm{char}\, H = 2$. Therefore, all the c_i must have been equal, and since $\mathrm{char}\, R = 2$, $p(x,y) = c[x,y]^D$. That D is the inner derivation $\mathrm{ad}(A)$ for $A \in [H,H]$ follows from $[e_{12}, A] \in F$, so the theorem holds when R satisfies S_4.

Assuming now that R does not satisfy S_4, and applying Corollary 3 as in the beginning of the proof, we may assume that the theorem is proved or $c_1 + c_3 = c_2 + c_4 = 0$, and in this case we may rewrite $p(x,y) = c(xy^D - yx^D) + z(x^D y - y^D x)$, where not both c and z are zero. Should $c = z$, then $c^{-1}p(x,y) = (xy)^D - (yx)^D = [x,y]^D \in C$. This means that $[L,L]^D \subset C$, which forces R to satisfy S_4 since $D \neq 0$ and L is not commutative [9; Lemma 2, p. 280]. This contradiction means that $c \neq z$.

We show now that D is an inner derivation. By assumption, we have $g(x,y,t) = [c(xy^D - yx^D) + z(x^D y - y^D x), t] = 0$ for $x, y \in L$ and $t \in R$. If D is an outer derivation and L is an ideal, then by [7; Theorem 7, p. 783] the terms containing x, y^D, and t give the identity $[cxy - zyx, t] = 0$ for R. But R is a prime ring satisfying a polynomial identity of degree three, so R must be commutative [5; Lemma 2, p. 55]. When L is a Lie ideal, proceed as in Theorem 1 by replacing x with $[x_1, x_2]$ and y with $[y_1, y_2]$ in $g(x,y,t)$. Now $g(x_1, \ldots, y_2, t)$ is an identity for the ideal M satisfying $[M,M] \subset L$, and applying [7; Theorem 7, p. 783] for the exponents $(1, 1, D, 1, 1)$ gives the identity $\big[c[x_1,x_2][y_1,y_2] - z[y_1,y_2][x_1,x_2], t\big] = 0$ for R. Again, since R is prime and satisfies an identity of degree five, R must satisfy S_4 [5; Lemma 2, p. 55]. Therefore, we may assume that $D = \mathrm{ad}(A)$ is an inner derivation of Q.

Since $g(x,y,t)$ is a nonzero multilinear GPI for L, we may conclude from [9; Theorem 1, p. 280] that R satisfies a GPI and that $p(x,y) = c(xy^D - yx^D) + z(x^D y - y^D x)$ is central for all $x, y \in [H,H]$, where $H = \mathrm{Soc}(RC \otimes F)$ for F an algebraic closure of C. Recall as in Theorem 1 that $HA + AH \subset H$ [7; Lemma 7, p. 779]. As in Theorem 1, to prove that R satisfies S_4 it suffices to show that H does not contain three orthogonal idempotents. Assume that $e, f, g \in H$ are rank one orthogonal idempotents and note that $eHe = eF$. For suitable $s, t \in H$, $e - f = [esf, fte] \in [H,H]$, and so, $(z-c)fAg = fp(e-f, e-g)g = 0$. Since $c \neq z$, we must conclude that $fAg = 0$. It is clear that A may be replaced in $p(x,y)$ by its conjugate $B = (1-erf)A(1+erf)$, and doing so yields $-erfAf + eAerf = eBf = 0$. This forces $eAe = ve$ and $fAf = vf$ for $v \in F$ [12; Theorem 1, p. 577]. As in the proof of Theorem 1, it follows that $D = 0$. Thus H cannot contain three orthogonal idempotents and R must satisfy S_4. This contradiction proves the theorem.

REFERENCES

1. C. L. Chuang, GPI*'s having coefficients in Utumi quotient rings*, Proc. Amer. Math. Soc. **103**(1988), 723–728.

2. ———, **-Differential identities of prime rings with involution*, Trans. Amer. Math. Soc. **316**(1989), 251–279.

3. I. N. Herstein, *Rings with Involution*, The University of Chicago Press, Chicago, 1976.

4. Y. Hirano, A. Kaya and H. Tominaga, *On a theorem of Mayne*, Math. J. Okayama Univ. **25**(1983), 125–132.

5. N. Jacobson, PI-*Algebras*, Lecture Notes in Math. **441**, Springer-Verlag, New York, 1975.

6. A. Kaya, *A theorem on semi-centralizing derivations of prime rings*, Math. J. Okayama Univ. **27**(1985), 11–12.

7. C. Lanski, *Differential identities in prime rings with involution*, Trans. Amer. Math. Soc. **291**(1985), 765–787; Correction to: *Differential identities in prime rings with involution*, Trans. Amer. Math. Soc. **309**(1988), 857–859.

8. ———, *Minimal differential identities in prime rings*, Israel J. Math. **56**(1986), 231–246.

9. ———, *Differential identities, Lie ideals, and Posner's theorems*, Pacific J. Math. **134**(1988), 275–297.

10. C. Lanski and S. Montgomery, *Lie structure of prime rings of characteristic* 2, Pacific J. Math. **42**(1972), 117–136.

11. P. H. Lee and T. K. Lee, *Lie ideals of prime rings with derivations*, Bull. Inst. Math. Acad. Sinica. **11**(1983), 75–80.

12. W. S. Martindale III, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12**(1969), 576–584.

13. J. Mayne, *Centralizing mappings of prime rings*, Canad. Math. Bull. **27**(1984), 122–126.

14. E. C. Posner, *Derivations in prime rings*, Proc. Amer. Math. Soc. **8**(1957), 1093–1100.

15. O. Zariski and P. Samuel, *Commutative Algebra*, **I**, D. Van Nostrand Co., Inc., New York, 1958.

Department of Mathematics
University of Southern California
Los Angeles, California 90089-1113