LIE IDEALS AND DERIVATIONS IN RINGS WITH INVOLUTION

Charles Philip Lanski

LIE IDEALS AND DERIVATIONS IN RINGS
WITH INVOLUTION

CHARLES LANSKI

Let R be a prime ring with involution and L a Lie ideal of R. It is known that if the commutator of an element of R with L is in the center of R, then either the element or L is in the center, unless R is an order in a simple algebra at most four dimensional over its center. This result is shown to hold if L is replaced by its (skew-) symmetric part. More generally, if a derivation of R sends the (skew-) symmetric part of L into the center of R, then one of the three possibilities mentioned above must hold. The same conclusion follows if one assumes that the image of L under the derivation is contained in the set of (skew-) symmetric elements of R.

In the last few years, many results have beed obtained which determine the extent to which various properties of the (skew-) symmetric elements of a ring with involution affect the whole ring. In this paper we consider certain centralizing properties of the (skew-) symmetric elements of a Lie ideal in a prime ring with involution, and show that they hold for the whole ring. Specifically, if the commutator of an element and the (skew-) symmetric part of a noncentral Lie ideal lies in the center, then the element must be in the center, with certain exceptions. This result is applied to the more general setting of derivations. The theorems we obtain use the description of the Lie ideals of the skew-symmetric elements given in [2], and the corresponding results in the characteristic two case, found in [6].

Throughout the paper, R will denote a ring with involution*; $V = \{x + x^* \,|\, x \in R\}$, the set of traces of R; $S = \{x \in R \,|\, x^* = x\}$, the set of symmetric elements of R; $K = \{x \in R \,|\, x^* = -x\}$, the set of skew-symmetric elements of R; and $Z = Z(R)$, the center of R. For any additive subgroup A of R, $A_K = A \cap K$ and $A_V = \{a + a^* \in A \,|\, a \in A\}$. Note that $2x = (x + x^*) + (x - x^*) \in V + K$, so $2R \subset V + K$.

Since most of our results are about prime rings, we recall some important and well-known facts about such rings. A prime ring is said to satisfy a polynomial identity over its centroid C, if there is a nonzero element $f(x_1, x_2, \cdots, x_n) \in C\{x_1, x_2, \cdots, x_n\}$, the free algebra over C, so that every substitution, $f(r_1, r_2, \cdots, r_n) = 0$, for $r_i \in R$ [See 3]. By a result of Amitsur [1; Theorem 1, p. 63], if there is a nonzero polynomial of degree d so that all substitutions by elements

of V or K give zero, then R satisfies a polynomial identity of degree $2d$. When this conclusion holds we shall say that R satisfies S_{2d}. In this case, $Z \neq 0$ and localizing R at its center gives a simple ring [7] of dimension at most d^2 over its center [3; Theorem 6.3.1, p. 157]. As an example, if the elements of V or K commute, then R is an order in a simple algebra at most four-dimensional over its center and R satisfies S_4. Conversely, if R is an order in a d^2-dimensional simple algebra, then R satisfies S_{2d} [3; p. 154-155]. To take greater advantage of this situation, one observes that when R satisfies S_{2d}, to invert the nonzero elements of Z, it suffices to invert $Z_S - \{0\}$, since $zz^* \in Z_S$. By doing this, one keeps control over K and V because RZ_S^{-1} with the involution $(rz^{-1})^* = r^* z^{-1}$ satisfies $(RZ_S^{-1})_V = VZ_S^{-1}$ and $(RZ_S^{-1})_K = KZ_S^{-1}$. As a consequence, when R is an order in a finite dimensional simple algebra, RZ_S^{-1} is this simple algebra and its traces and skewsymmetric elements are essentially those of R. It will be clear from the conclusions we desire, that replacing R by RZ_S^{-1} results in no loss of generality, so we shall be able to assume that R is simple and finite dimensional over Z, reducing the situation to matrices.

To simplify computations, we use the notation $[x, y] = xy - yx$ for $x, y \in R$, and let $[A, B]$ denote the additive subgroup of R generated by all $[a, b]$ for $a \in A \subset R$ and $b \in B \subset R$. An additive subgroup L of R which satisfies $[L, R] \subset L$ is a *Lie ideal* of R. If $L \subset K$ and $[L, K] \subset L$, then L is called a Lie ideal of K.

We shall prove our first theorem after stating a lemma from [6] to which we must refer several times.

LEMMA 1. *Let R be prime, and let L be a Lie ideal of R. If $[x, L] \subset Z$, then either $x \in Z$ or $L \subset Z$, unless* char $R = 2$, $Z \neq 0$, *and R satisfies S_4.*

Proof. [6; Lemma 8, p. 120].

THEOREM 1. *Let R be prime with* char $R \neq 2$. *Suppose that $L^* = L$ is a Lie ideal of R and $[x, L_V] \subset Z$. Then either $x \in Z$, $L \subset Z$, or R satisfies S_4.*

Proof. If $T = \{x \in R \mid [x, L_V] \subset Z\}$, then for $t \in T$, $k \in L_K$, and $y \in L_V$, $[[t, k], y] = [[t, y], k] + [t, [k, y]] \in Z$. Since $[k, y] \in L_V$, we have that $[[T, L_K], L_V] \subset Z$, and so, $[T, L_K] \subset T$. Clearly, $[T, L_V] \subset T$. As a consequence, $[T, 2L] \subset [T, L_V + L_K] \subset T$. But $2L$ is a Lie ideal of R, so a result of Herstein [5; Theorem 5, p. 570] implies that either $[T, 2L] = 0$ or $T \supset U = [M, R] \neq 0$ for M an ideal of R. Suppose first that $[T, 2L] = 0$, and apply Lemma 1 to obtain $T \subset Z$, $L \subset Z$,

or R satisfies S_4, establishing the theorem. Hence, we may assume that $[M, R] = U \subset T$, and that R does not satisfy S_4.

Since $[U, L_V] \subset Z$ and U is a Lie ideal of R, Lemma 1 implies that $U \subset Z$ or $L_V \subset Z$. If $[M, R] = U \subset Z$, then the contradiction $[M, R] = 0$ results, using the lemma again. On the other hand, $L_V \subset Z$ allows us to conclude that $[2L, V] \subset [L_V + L_K, V] = [L_K, V] \subset L_V \subset Z$. A final application of Lemma 1 gives $L \subset Z$ or $V \subset Z$. By our discussion preceding the theorem, the second possibility means that R satisfies S_4. Therefore, one of the conclusions must hold, completing the proof of the theorem.

To see that the last possibility of the conclusion of Theorem 1 is necessary, one can consider $R = M_2(D)$, the ring of 2×2 matrices over a commutative domain. If char $D \neq 2$, use the symplectic involution on R, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Then $V = Z$, so $[x, L_V] = 0$ for any $x \in R$ and any L. If the involution on R is transpose, then the elements of K commute, so $[k, L_K] = 0$ for any $k \in K$ and any L. This shows that replacing L_V by L_K in Theorem 1 will still require the possibility that R satisfies S_4. The situation does not change when char $D = 2$, since $L = \left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \right\}$ is a noncentral commutative Lie ideal, $L \subset S$, and $L_V = 0$

Most of the results we shall quote assume that the involution fixes Z. If the involution is the identity on Z, then it is called an involution of the first kind. If $Z \not\subset S$, the involution is of the second kind. Proving the analogue of Theorem 1 for L_K instead of L_V requires different arguments for the different types of involutions.

Next we consider involutions of the second kind and observe that the result is independent of characteristic.

THEOREM 2. *Let R be prime with an involution of the second kind. If $L^* = L$ is a Lie ideal of R and $[x, L_K] \subset Z$ or $[x, L_V] \subset Z$ when* char $R = 2$, *then either $x \in Z$, $L \subset Z$, or R satisfies S_4.*

Proof. We shall assume that $[x, L_K] \subset Z$, but point out that when char $R = 2$, the same argument proves the theorem if $[x, L_V] \subset Z$. Since $Z \not\subset S$, there is $z \in Z - \{0\}$ with $z - z^* \neq 0$. Now $(z - z^*)r = (zr + z^*r^*) - z^*(r^* + r)$, so $(z - z^*)R \subset V + z^*V$. From our earlier discussion, there is no loss of generality in assuming that Z is a field, once we replace R by RZ_S^{-1} and L by LZ_S^{-1}. Thus, $R = K + z^*K$. The assumption that $[x, L_K] \subset Z$ implies that $[[x, K], L_K] \subset [[x, L_K], K] + [x, [K, L_K]] \subset [x, L_K] \subset Z$. Clearly, $[[x, z^*K], L_K] \subset Z$, so $[[x, R], L_K] \subset Z$. We have shown that $T = \{x \in R \mid [x, L_K] \subset Z\}$ is a Lie ideal of R. But $[T, L_K] \subset Z$ and Lemma 1 force R to satisfy S_4 unless $T \subset Z$

or $L_K \subset Z$. Therefore, we may assume that $L_K \subset Z$.

For any $y \in L$, $y - y^* \in L_K$, so for any $r \in R$, $0 = [y - y^*, r] = [y, r] - [y^*, r]$. Consequently, $[y, r + r^*] = [y, r] + [y, r^*] = [y, r] + [y^*, r^*] = [y, r] - [y, r]^* \in L_K \subset Z$. That is, $[L, V] \subset Z$. By Lemma 1 either $V \subset Z$ or one of the conclusions of the theorem holds. But $V \subset Z$ means that R must satisfy S_4, so the theorem is proved.

Having eliminated the case of involutions of the second kind, we proceed to the skew-symmetric version of Theorem 1.

THEOREM 3. *Let R be prime with* char $R \neq 2$. *Let $L^* = L$ be a Lie ideal of R and suppose that $[x, L_K] \subset Z$. Then either $x \in Z$, $L \subset Z$, or R satisfies S_4.*

Proof. For any $t, w \in L_K$, $[x, [t, w]] = [[x, t], w] + [t, [x, w]] = 0$, and so $[x, [L_K, L_K]] = 0$. Since $[L_K, K] \subset L_K$, $[L_K, L_K]$ is a Lie ideal of K. By Theorem 2 we may assume that the involution is of the first kind, so a result of Erickson [2; Corollary, p. 533] is applicable, enabling us to conclude either that R is an order in a simple algebra at most 16-dimensional over its center, or that $[L_K, L_K] \supset [J \cap K, K]$ for $J^* = J$ a nonzero ideal of R.

If the second possibility holds, then x commutes with $A = [J \cap K, J \cap K]$, and thus, with A', the subring generated by A. As an ideal in R, J is itself a prime ring, from which it follows [2; Theorem 4, p. 528] that A' contains a nonzero ideal I of J, unless J is an order in a simple algebra at most 16-dimensional over its center. Should J be such an order, then it is wellknown that R must be also. Assume for now that $I \subset A'$. It is easy to see that JIJ is a nonzero ideal of R contained in I, and so, commutes with x. Therefore, $x \in Z$, one of the conclusions we desire. Hence, to finish the proof, we may assume that R is an order in a simple algebra, finite dimensional over its center.

In view of our earlier discussion, if we replace R by RZ_S^{-1} and L by LZ_S^{-1}, there is no loss of generality in assuming that R is a simple algebra, finite dimensional over Z. The fact that L is now a Lie ideal of a simple ring implies that $L \subset Z$ or $L \supset [R, R]$ by [4; Theorem 1.5, p. 9]. The theorem is proved unless $L \supset [R, R]$, so we may assume that $L_K \supset [K, K]$ and $[L_K, L_K] \supset U = [[K, K], [K, K]]$. U is a Lie ideal of K so either R satisfies S_4, $U \supset [K, K]$, or the square of each element of U is in Z [4; Theorem 2.9, p. 35]. If the last possibility holds, it follows [4; p. 36–39] that $[K, K] = K$, unless one of the other possibilities also holds. Therefore, we may assume that $U \supset [K, K]$. If R does not satisfy S_4, $[K, K]$ generates R [4; Theorem 2.13, p. 40]. Since x commutes with $[K, K]$, it commutes with R, so $x \in Z$ unless R satisfies S_4. We have exhausted all pos-

sibilities and completed the proof of the theorem.

To complete the sequence of results we have obtained so far, we must consider the case when char $R = 2$. The proof is much like that of Theorem 3 and uses results from [6] in place of those from [2]. Also, it is necessary to do some calculation after reducing to the simple case since the facts available when char $R = 2$ do not seem to be as complete as when char $R \neq 2$.

THEOREM 4. *Let R be a prime ring with* char $R = 2$. *Let $L^* = L$ be a Lie ideal if R and suppose that $[x, L_V] \subset Z$. Then either $x \in Z, L \subset Z$, or R satisfies S_4.*

Proof. Just as in the proof of Theorem 3, we obtain that $[x, [L_V, L_V]] = 0$, and that $[L_V, L_V]$ is a Lie ideal of V. In view of Theorem 2, we may assume that the involution on R is of the first kind. Hence, Theorem 31 of [6] can be applied, enabling us to conclude that either $[L_V, L_V] \subset Z, R$ is an order in a simple algebra at most 36-dimensional over its center, or $[L_V, L_V] \supset [J_V, J_V]$ for $J = J^*$, a nonzero ideal of R. Consider the last of these possibilities. We have that x must commute with A, the subring generated by $[J_V, J_V]$, and A contains a nonzero ideal I of J, unless J is an order in a simple algebra at most 36-dimensional over its center [6; Theorem 25, p. 129]. As in the proof of Theorem 3, if the ideal J of R is such an order, so is R. If this is not the case, then x commutes with the nonzero ideal JIJ of R, forcing $x \in Z$. Therefore, to prove the theorem, it suffices to assume that either $[L_V, L_V] \subset Z$, or that R is an order as described above.

Assume that $[L_V, L_V] \subset Z$, and note that $[L_V, V] \subset L_V$. Use Theorem 31 of [6] applied to L_V, to obtain that either $L_V \subset Z, L_V \supset [J_V, J_V]$, or R is an order in a simple algebra of dimension at most 36 over its center. Should the second possibility hold, then by [6; Corollary 32, p. 132], we are again in the situation where R is an order, or the subring A generated by $[L_V, L_V]$ must contain a nonzero ideal of R. But the assumption that $[L_V, L_V] \subset Z$, combined with A containing an ideal, would force R to be commutative, completing the proof.

Now suppose that $L_V \subset Z$. Then for $t \in L$ and $r \in R$,

$$0 = [t+t^*, r] = [t, r] + [t^*, r] .$$

Consequently, $[t, r + r^*] = [t, r] + [t, r^*] = [t, r] + [t^*, r^*] = [t, r] + [t, r]^*$, which means that $[L, V] \subset L_V \subset Z$. By Lemma 1 and the discussion preceding it, either $L \subset Z$ or R satisfies S_4.

The theorem has now been proved except when R is an order in a simple algebra at most 36-dimensional over its center. We make this assmption for the remainder of the proof, and further assume that $L \not\subset Z$ and R does not satisfy S_4. We must show that $x \in Z$. As we have seen before, there is no loss of generality in assuming that Z is a field and that R is itself simple of dimension at most 36 over Z. Using [4; Theorem 1.5, p. 9] again implies that $L \supset [R, R] \supset [V, V]$. Since x commutes with $[L_V, L_V]$, x must commute with $U = [[V, V], [V, V]]$. Clearly, to show $x \in Z$, it suffices to prove that U generates R as an algebra over Z. To do this, we reduce to matrices.

Let F be an algebraic closure of Z, and set $R_F = R \otimes_Z F$. Give R_F the involution induced by $(r \otimes a)^* = r^* \otimes a$, for $r \in R$ and $a \in F$. It is easy to see that $V(R_F) = V \otimes F$, $[V(R_F), V(R_F)] = [V, V] \otimes F$, and $(L \otimes F)_V = L_V \otimes F$. Hence, none of our assumptions is changed by assuming that Z is algebraically closed, and so, $R = M_n(Z)$, the complete $n \times n$ matrix ring over Z for $n \leq 6$. The advantage of this representation of R is that the form of the involution is well-known to be of one of two types: transpose or symplectic.

If the involution is of transpose type then for $A = (a_{ij}) \in R$, $A^* = (b_{ij})$ where $b_{ij} = z_i^{-1} z_j a_{ji}$ for $z_i \in Z - \{0\}$. Since $R = M_n(Z)$ and R does not satisfy S_4, it follows that $n \geq 3$. If $\{e_{ij}\}$ are the usual matrix units, let $y_{ij} = z_i e_{ij} + z_j e_{ji}$. A simple computation shows that $y_{ij} \in V$ when $i \neq j$, and that $[y_{ij}, y_{kj}] = z_i y_{ik} \in [V, V]$ for i, j, k distinct. Consequently, ZU contains all y_{ij}, so the subalgebra generate by U contains $y_{ij} y_{jk} = z_i z_j e_{ik}$. Therefore, this subalgebra contains all e_{ij} for $i \neq j$, and the fact that these generate R implies that U does also.

Should the involution on R be of symplectic type, then since R does not satisfy S_4, $R = M_n(Z)$ for $n = 4$ or $n = 6$. If $A = (A_{ij}) \in R$ for $A_{ij} \in M_2(Z)$, then the involution acting on A gives (B_{ij}) where $B_{ij} = A_{ij}^*$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} d & b \\ c & a \end{pmatrix}$. Letting E_{ij} be the 2×2 identity matrix in the "$i - j$" position, it is easy to see that a typical element of V has the form $\Sigma z_i E_{ii} + \Sigma(A_{ij} E_{ij} + A_{ij}^* E_{ji})$. Note that each element of V has trace equal to zero, and so, since $n > 2$, $V \subset [R, R]$. Therefore, in the case we are considering, $L \supset V$ and it follows that $[L_V, L_V] \supset [V, V]$. Thus, to prove $x \in Z$, it is enough to show that $[V, V]$ generates R as an algebra over Z. But V contains E_{ii}, as well as $AE_{ij} + A^* E_{ji}$ for $A \in M_2(Z)$, so an easy calculation shows that $[V, V]$ contains $[AE_{ij} + A^* E_{ji}, E_{ii}] = AE_{ij} + A^* E_{ji}$. Therefore, the subalgebra T generated by $[V, V]$ contains

$$(AE_{ij} + A^* E_{ji})(E_{ij} + E_{ji}) = AE_{ii} + A^* E_{jj} .$$

Multiply two such elements to get $ABE_{ii} + A^*B^*E_{jj}$ and add $BAE_{ii} + (BA)^*E_{jj}$ to obtain $[A, B]E_{ii}$. Since $[M_2(Z), M_2(Z)]$ generates $M_2(Z)$ as an algebra, T contains AE_{ii} for any i. Multiplying AE_{ii} by $E_{ij} + E_{ji}$ yields $AE_{ij} \in T$ for $i \neq j$. Combining these results gives $T = R$, which proves that $x \in Z$, and finally completes the proof of the theorem.

Thus far we have assumed and used the fact $L^* = L$. If $L^* \neq L$, then the same results we have obtained hold for the Lie ideal $[L, L^*] \subset L \cap L^*$, which is invariant under the action of the involution.

COROLLARY 1. *Let R be prime and L a Lie ideal of R. If $[x, [L, L^*]_V] \subset Z$ or if $[x, [L, L^*]_K] \subset Z$, then either $x \in Z, L \subset Z$, or R satisfies S_4.*

Proof. Under either hypothesis, the conclusions of the appropriate one of our previous theorems prove the Corollary, unless $[L, L^*] \subset Z$. But in this case, Lemma 1 forces $L \subset Z$ except if R satisfies S_4.

That the various results we have proved cannot hold for semi-prime rings follows by taking suitable direct sums of prime rings. Our next theorem shows that a semi-prime ring in which $[x, L_V] \subset Z$ or $[x, L_K] \subset Z$ must "decompose" into a direct sum of three rings so that one of the usual conditions holds in each.

THEOREM 5. *Let R be semi-prime and $L^* = L$ a Lie ideal of R. If $[x, L_V] \subset Z$ or $[x, L_K] \subset Z$, then R is a subdirect sum of semi-prime *-homomorphic images R_1, R_2 and R_3 so that R_1 satisfies S_4, the image of x in R_2 is in the center, and the image of L in R_3 is in the center.*

Proof. We shall prove the theorem assuming that $[x, L_K] \subset Z$, since the argument is virtually identical for L_V. Since the intersection of all the prime ideals of R is zero, it will suffice to show that for any prime ideal P, R/P either satisfies S_4, $x + P \in Z(R/P)$, or $L + P \subset Z(R/P)$. Now P^* is also a prime ideal of R and satisfies the first and third of these possibilities exactly when P does. Consequently, if $x + P^* \notin Z(R/P^*)$, then R/P satisfies S_4 or $L + P \subset Z(R/P)$, which implies that one of the conditions holds for $R/(P \cap P^*)$. Considering $P \cap P^*$, for each prime P, as falling into one of three classes, depending on which condition $R/(P \cap P^*)$ satisfies, and taking the quotients of R by the intersection of all members of a given class

produces each of the R_i described in the theorem.

First consider the case when P is a prime ideal of R and $P^* = P$. Then R/P inherits an involution from R by setting $(r + P)^* = r^* + P$, and $L + P$ is a Lie ideal of R/P, invariant under the induced involution. If $\ell + P \in (L + P)_K$ and char $(R/P) \neq 2$, then $2\ell + P = (\ell - \ell^*) + P \in L_K + P$. Should char $(R/P) = 2$, then $L_K + P \supset (L + P)_V$, since $(\ell + P) + (\ell + P)^* = (\ell + \ell^*) + P = (\ell - \ell^*) + P$. Hence, depending on char (R/P), either

$$[x + P, (L + P)_K] \subset Z(R/P)$$

or $[x + P, (L + P)_V] \subset Z(R/P)$. Applying the appropriate one of our previous results to R/P gives that either R/P satisfies S_4, $x + P \in Z(R/P)$, or $L + P \subset Z(R/P)$.

Next assume that $P^* \neq P$. In this case, $P^* + P$ is a nonzero ideal in R/P, and if $y \in P^*$, then $y + P = y - y^* + P$. Consequently $(L \cap P^*) + P \subset L_K + P$, and so, $[x + P, (L \cap P^*) + P] \subset Z(R/P)$. Since $[L, P^*] + P$ is a Lie ideal contained in $(L \cap P^*) + P$, it follows from Lemma 1 applied to R/P that either R/P satisfies S_4, $x + P \in Z(R/P)$, or $[L, P^*] + P \subset Z(R/P)$. Using Lemma 1 again, should the last possibility hold, gives $L + P \subset Z(R/P)$ or $P^* + P \subset Z(R/P)$. But $P^* + P \subset Z(R/P)$ forces R/P to be commutative, completing the proof of the theorem.

A result, analogous to Corollary 1, holds for semi-prime rings. As in Corollary 1, if we assume that $[x, [L, L^*]_K] \subset Z$, for example, then Theorem 5 will imply that a certain subdirect decomposition for R exists, and in one of the summands, the image of $[L, L^*]$ will be in the center. By looking at the prime images of this summand and applying Lemma 1, one can show that a further decomposition occurs. Specifically, the summand in question is a subdirect sum of two semi-prime rings with the image of L in the center of one and the image of L^* in the center of the other. We state this result as

COROLLARY 2. *Let R be semi-prime and L a Lie ideal of R. If either $[x, [L, L^*]_K] \subset Z$ or $[x, [L, L^*]_V] \subset Z$, then R is a subdirect sum of semi-prime images R_j for $1 \leq j \leq 4$, and the R_j satisfy:*
  (i) *R_1 and R_2 inherit the involution from R,*
  (ii) *R_1 satisfies S_4,*
  (iii) *the image of x is in the center of R_2,*
  (iv) *the image of L is in the center of R_3,*
  (v) *the image of L^* is in the center of R_4.*

Observe that R_3 and R_4 in Corollary 2 need not have an induced involution. For example, if A is any semi-prime ring and L any

Lie ideal of A, let $R = A \oplus B$ where B is the opposite ring of A, and where the involution on R is obtained by interchanging coordinates. Then the image of $(L, 0)$ in B is central, and the image of $(L, 0)^* = (0, L)$ in A is central, but L need not be central in A.

Our theorems can be interpreted as statements about derivations. Recall that a derivation D of R is an additive homomorphism of R and satisfies $D(xy) = xD(y) + D(x)y$. It follows that the mapping $D_r(x) = [r, x]$ is a derivation of R for any $r \in R$, and is called an inner derivation of R. Using our results for inner derivations, we shall prove the corresponding theorems for abstract derivations. First we make some elementary observations. Is D is a derivation of R, then $D(Z) \subset Z$. This follows from the computation $0 = D[z, r] = [D(z), r] + [z, D(r)] = [D(z), r]$ for $z \in Z$ and $r \in R$. Also, if R is a prime ring and L is a Lie ideal of R with $D(L) = 0$, then either $L \subset Z$, $D(R) = 0$, or R satisfies S_4. To prove this, note that $D(L) = 0$ implies that $D(L') = 0$, where L' is the subring generated by L. It is well-known that either $L \subset Z$, R satisfies S_4, or $L' \supset I \neq 0$, for I an ideal of R [4; Lemma 2.3, p. 4 and 6; Theorem 4, p. 118]. But $D(I) = 0$ implies, for $r \in R$, that $ID(r) = 0$, forcing $D(r) = 0$, since R is prime. We shall use these facts freely in what follows.

THEOREM 6.   *Let R be prime with char $R \neq 2$. Let D be a derivation of R and L a Lie ideal of R with $L^* = L$ and $D(L_V) \subset Z$. Then either $L \subset Z, D(R) = 0$, or R satisfies S_4.*

Proof. As we have seen before, $[L_V, L_K] \subset L_V$, so $D([L_V, L_K]) \subset Z$. Thus $[L_V, D(L_K)] \subset Z$, and the conclusion follows from Theorem 1, unless $D(L_K) \subset Z$. But then $D(2L) \subset D(L_V + L_K) \subset Z$, or equivalently, $D(L) \subset Z$. Therefore, $D([L, L]) = 0$, and the fact that $[L, L]$ is a Lie ideal of R gives one of the three desired conclusions, by our discussion above, proving the theorem.

The situation for L_K is slightly more involved.

THEOREM 7.   *Let R be prime with char $R \neq 2$. Let D be a derivation of R and L a Lie ideal of R with $L^* = L$ and $D(L_K) \subset Z$. Then either $L \subset Z, D(R) = 0$, or R satisfies S_4.*

Proof. The hypothesis implies that $D([L_K, K]) \subset Z$, from which it follows that $[L_K, D(K)] \subset Z$. Using Theorem 3, we may conclude that either $L \subset Z$, R satisfies S_4, or $D(K) \subset Z$. Since the first and second possibilities prove the theorem, assume that $D(K) \subset Z$ and that R does not satisfy S_4. It is easy to see that $D(K) \subset Z$ implies

$D([K, K]) = 0$. For $k \in K$ and $t \in [K, K]$, $ktk \in K$, and so, $D(ktk) \in Z$. Expand by using the definition of derivation and use $D(t) = 0$ to obtain $(kt + tk)D(k) \in Z$. If $D(k) \neq 0$, then $kt + tk \in Z$. Applying D gives $D(kt + tk) = 2D(k)t \in Z$, and since we are assuming that $D(k) \neq 0$, we have $t \in Z$. Thus, $[K, K] \subset Z$. On the other hand, if $D(K) = 0$, then $D(K^2) = 0$. It is well known and easy that K^2 is a Lie ideal of R $(k_1 k_2 r - r k_1 k_2 = k_1 (k_2 r + r^* k_2) - (k_1 r^* + r k_1) k_2)$ so unless $D(R) = 0$, we must have $K^2 \subset Z$. But $[K, K] \subset K^2$, so we may assume that $[K, K] \subset Z$. Applying Theorem 3 with L there replaced by R yields that R must satisfy S_4, which establishes the theorem.

In the same spirit as the last two theorems, the final result on derivations uses Theorem 4 to handle the case when char $R = 2$.

THEOREM 8. *Let R be prime with* char $R = 2$. *Let D be a derivation of R and L a Lie ideal of R with $L^* = L$ and $D(L_V) \subset Z$. Then either $L \subset Z$, $D(R) = 0$, or R satisfies S_4.*

Proof. Beginning as in Theorem 7, with K there replaced by V, and applying Theorem 4, gives one of the desired conclusions or that $D(V) \subset Z$. Assuming the latter situation and using $sts = sts^* \in V$ for $s, t \in V$, yields $D(sts) \in Z$. Expanding this produces $s^2 D(t) + D(s)(ts + st) \in Z$. In particular, when $s = t$, $s^2 D(s) \in Z$ results. If $D(s) \neq 0$, then $s^2 \in Z$. If $D(s) = 0$ but $D(t) \neq 0$ for some $t \in V$, then $s^2 D(t) \in Z$, by the above, so $s^2 \in Z$. Hence, either $D(V) = 0$ or $s^2 \in V$ for all $s \in V$.

Assume first that $D(V) = 0$. Then using $D(V^2) = 0$, together with the fact that V^2 is a Lie ideal of $R(v_1 v_2 r + r v_1 v_2 = v_1(v_2 r + r^* v_2) + (v_1 r^* + r v_1)v_2)$, forces us to conclude that $V^2 \subset Z$, $D(R) = 0$, or R satisfies S_4. The first possibility implies that $s^2 \in Z$ for all $s \in V$. Hence, it suffices to consider this situation in order to prove the theorem. Linearize by setting $s = t + w$ to obtain $[V, V] \subset Z$. Using Theorem 4, with L there equal to R, shows that R must satisfy S_4, completing the proof of the theorem.

Of course, the same modification as before holds now. That is, if one replaces L in any of the last three theorems by $[L, L^*]$, then the same conclusions are valid, since $[L, L^*] \subset Z$ implies that $L \subset Z$ by Lemma 1. For the sake of completeness, we state it formally.

COROLLARY 3. *Let R be prime, D a derivation of R, and L a Lie ideal of R. If $D([L, L^*]_V) \subset Z$ or if $D([L, L^*]_K) \subset Z$, then either $L \subset Z$, $D(R) = 0$, or R satisfies S_4.*

Our final results concern a slightly different situation. We have seen that if $D(L) = 0$, then one of the conclusions of Corollary 3 must hold. Assuming that $D(L) \subset K$ or $D(L) \subset V$, must the same be true? The answer is yes, and we divide the proof into two cases, each of which is easy.

THEOREM 9. *Let R be prime with* char $R \neq 2$. *Let D be a derivation of R and L a Lie ideal of R with $L^* = L$ and $D(L) \subset K$ or $D(L) \subset S$. Then either $L \subset Z$, $D(R) = 0$, or R satisfies S_4.*

Proof. Assume first that $D(L) \subset K$. Since $[L, K] \subset L$, apply D to get $D([L, K]) \subset K$. This implies that $[L, D(K)] \subset K$, using $[K, K] \subset K$. In particular, $[L_V, D(L_K)] \subset K$. But $[L_V, D(L_K)] \subset [V, K] \subset S$, so $[L_V, D(L_K)] = 0$. By Theorem 1, either $L \subset Z$, $D(L_K) \subset Z$, or R satisfies S_4. Should $D(L_K) \subset Z$, then an application of Theorem 7 completes the proof. In the case that $D(L) \subset S$, the same argument holds.

We end the paper with the companion result for char $R = 2$ case, and the usual corollary.

THEOREM 10. *Let R be prime with* char $R = 2$. *Let D be a be derivation of R and L a Lie ideal of R such that $L^* = L$ and $D(L) \subset S$. Then either $L \subset Z$, $D(R) = 0$, or R satisfies S_4.*

Proof. Since $D([L, S]) \subset D(L) \subset S$, it follows that $[L, D(S)] \subset S$, using $[S, S] \subset S$. For $y \in L$ and $t \in D(L_V)$, $[y, t]^* = [y, t]$, which implies that $[y, t] = [y^*, t]$, or $[y + y^*, t] = 0$. Thus $[L_V, D(L_V)] = 0$ and as a consequence, Theorem 4 implies that either $L \subset Z$, $D(L_V) \subset Z$, or R satisfies S_4. If $D(L_V) \subset Z$, then an application of Theorem 8 completes the proof.

COROLLARY 4. *Let R be prime, D a derivation of R, and L a Lie ideal of R. If $D([L, L^*]) \subset K$ or if $D([L, L^*]) \subset S$, then either $L \subset Z$, $D(R) = 0$, or R satisfies S_4.*

REFERENCES

1. S. A. Amitsur, *Identities in rings with involution*, Israel J. Math., **7** (1969), 63–68.
2. T. S. Erickson, *The Lie structure in prime rings with involution*, J. of Algebra, **21** (1972), 523–534.
3. I. N. Herstein, *Non Commutative Rings*, The Carus Mathematical Monographs, the Mathematical Assn. of America, Washington D. C., 1968.
4. ———, *Topics in Ring Theory*, The University of Chicago Press, Chicago, 1969.
5. ———, *On the Lie structure of an associative ring*, J. of Algebra, **14** (1970), 561–571.

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

7. L. Rowen, *Some results on the center of a ring with polynomial identity*, Bull. Amer. Math. Soc., **79** (1974), 219–223.

UNIVERSITY OF SOUTHERN CALIFORNIA
LOS ANGELES, CA 90007

PACIFIC JOURNAL OF MATHEMATICS

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be in typed form or offset-reproduced, (not dittoed), double spaced with large margins. Please do not use built up fractions in the text of your manuscript. You may however, use them in the displayed equations. Underline Greek letters in red, German in green, and script in blue. The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. Items of the bibliography should not be cited there unless absolutely necessary, in which case they must be identified by author and Journal, rather than by item number. Manuscripts, in triplicate, may be sent to any one of the editors. Please classify according to the scheme of Math. Reviews, Index to Vol. **39**. All other communications should be addressed to the managing editor, or Elaine Barth, University of California, Los Angeles, California, 90024.

The Pacific Journal of Mathematics expects the author's institution to pay page charges, and reserves the right to delay publication for nonpayment of charges in case of financial emergency

100 reprints are provided free for each article, only if page charges have been substantially paid. Additional copies may be obtained at cost in multiples of 50.

Pacific Journal of Mathematics
Vol. 69, No. 2   June, 1977