DIFFERENTIAL IDENTITIES IN PRIME RINGS
WITH INVOLUTION[1]

BY

CHARLES LANSKI

ABSTRACT. Let R be a prime ring with involution. Using work of V. K. Kharchenko it is shown that any generalized identity for R involving derivations of R and the involution of R is a consequence of the generalized identities with involution which R satisfies. In obtaining this result, a generalization, to rings satisfying a GPI, of the classical theorem characterizing inner derivations of finite-dimensional simple algebras is required. Consequences of the main theorem are that in characteristic zero no outer derivation of R can act algebraically on the set of symmetric elements of R, and if the images of the set of symmetric elements under the derivations of R satisfy a polynomial relation, then R must satisfy a generalized polynomial identity.

This paper deals with differential identities of prime rings with involution, and was motivated by work of V. K. Kharchenko and of I. N. Herstein. In [5], Kharchenko shows that the differential identities of prime rings are consequences of formal identities for endomorphisms, satisfied in any ring, and of the generalized polynomial identities satisfied by the prime ring under consideration. In [4], Herstein proves that a certain identity, namely $D(s)D(t) - D(t)D(s) = 0$, where D is a derivation and both s and t are symmetric elements, cannot hold in a prime ring of characteristic different from two, unless the ring satisfies the standard identity of degree four. The extension of Kharchenko's theorem to differential identities involving involution would provide a more general context for the result of Herstein. Our goal is to provide a careful setting for the theory of differential identities (with involution) and to prove an extension of Kharchenko's theorem which shows that the differential identities of a prime ring with involution are consequences of the formal identities for endomorphisms and of the generalized polynomial identities with involution satisfied by the ring under consideration. The proof relies heavily on the result and techniques of Kharchenko, although we have attempted to make our exposition as self-contained as possible. In particular, in our Theorem 1, we adapt Kharchenko's argument [5, Lemma 2, p. 158] to our more general setting. Our main result also requires an extension to rings satisfying a generalized polynomial identity of the classical result characterizing inner derivations of finite-dimensional simple algebras. We use our main result to show, as in [5], that when the characteristic of the ring is zero, any derivation which is algebraic when restricted to the symmetric or skew-symmetric elements must be an inner derivation. We also show that a prime ring with involution, must satisfy a generalized polynomial identity if its symmetric, or skew-symmetric elements satisfy an identity of the form

---

$p(d_1(x_1), \ldots, d_k(x_k), x_{k+1}, \ldots, x_n) = 0$ where p is a polynomial in n noncommuting indeterminates and $d_1, \ldots, d_k$ are derivations of the ring. Our full result gives an affirmative answer to a generalization of a question of Kovacs [6] which asked if a prime ring must satisfy a generalized polynomial identity if it satisfies an identity of the form $p(d_1(x_1), \ldots, d_n(x_n)) = 0$, as above.

For any prime ring R, let C be its extended centroid and Q its Martindale quotient ring (see [8] for details). The elements of Q can be regarded as equivalence classes of left R-module homomorphisms from ideals of R, to R. As a consequence, one may consider $R \subset Q$ as right multiplications. Also, for any $f \in Q$, there is a nonzero ideal I_f of R so that $(I_f)f \subset R$, and if $(I_f)f = 0$ then $f = 0$. The center of Q is C, a field, and RC is a prime ring. The elements of C may be characterized as those $f \in Q$ which are R-bimodule maps of I_f into R. Equivalently, C is the centralizer of R in Q. When R has an involution, *, then RC has an involution which restricts to * on R [9, Theorem 4.1, p. 511], so in this case we may assume that * is an involution of C also.

Denote the Lie algebra of derivations of R by $\text{Der}(R)$. For any mapping h of R into Q, let r^h be the image of $r \in R$ under h. It is easy to see that any derivation of R can be extended to Q. Let $d \in \text{Der}(R)$, choose $f \in Q$ defined on I_f, set $J = (I_f)^2$ and define f^d from J to R by $yf^d = (yf)^d - (y^d)f$. This left R-module map represents an element of Q and the mapping sending f to f^d is a derivation of Q which restricts to d on RC. Henceforth, we shall consider any $d \in \text{Der}(R)$ as a derivation of Q. Now suppose that $d \in \text{Der}(R)$ becomes inner when considered in $\text{Der}(Q)$. Thus $r^d = ra - ar$ for some $a \in Q$ and each $r \in R$. It follows that $aI_a \subset (I_a)a + (I_a)^d \subset R$. Hence, we are led to consider the ring $N = \{f \in Q | fI + If \subset R \text{ for a nonzero ideal } I \text{ of } R\}$. Clearly, N contains both R and C, as well as those elements of Q which induce the derivations of R whose extensions to Q are inner. As in [5], it is straightforward to show that the extension of a derivation from R to Q restricts to a derivation of N. Throughout the paper R will denote a prime ring, and C, Q, and N will be as above. When R is a simple ring with 1, one has $R = N = Q$. We present next a somewhat less trivial example of these objects.

EXAMPLE 1. Let V be an infinite-dimensional vector space over a field C. Represent $\text{Hom}_C(V, V)$ as the set of all row finite matrices over C, with respect to a fixed well-ordered basis of V. Let R be the subring of $\text{Hom}_C(V, V)$ consisting of those matrices containing only a finite number of nonzero entries. Then $Q = \text{Hom}_C(V, V)$ and N is the subring of Q of all column finite matrices.

Our main result concerns generalized polynomial identities, for ideals of R, having coefficients in N. We need to have available certain facts in our situation which are known when evaluations and coefficients come from R. To make this paper more self-contained, and to avoid requiring the reader to find the appropriate arguments in the literature and to check carefully that those arguments can be modified for our situation, we present and prove the facts we need in the context we require. The first such result corresponds to [3, Lemma 1.3.2, p. 22].

LEMMA 1. *Let* $\{a_1, \ldots, a_n, b_1, \ldots, b_n\} \subset N - \{0\}$, *and set* $f(x) = \sum a_i x b_i$. *The following are equivalent:*

(i) $f(y) = 0$ *for all* $y \in I$ *a nonzero ideal of* R;

(ii) $\sum a_i \otimes b_i = 0$, *as an element in* $N \otimes_C N$; *and*

(iii) $f(x) = 0$ *as an element in* $Q *_C C[x]$, *the free product over* C *of* Q *and* $C[x]$.

PROOF. Clearly, it suffices to prove that (i) implies (ii). Proceed by induction on n. If $n = 1$, choose a nonzero ideal J of R satisfying $Ja + aJ \subset R$ and $J \subset I$. From (i), $aJb = 0$, so the definition of Q yields either $JaJ = 0$ or $b = 0$. Thus $JaJ = 0$ and the primeness of R gives the contradiction $a = 0$. Suppose now that $n > 1$ and that (i) implies (ii) when $k < n$. If $\{a_1, \ldots, a_n\}$ is C-dependent, pick an independent subset, and rewrite f and $\sum a_i \otimes b_i$ in terms of this subset. Should the new $\{b_j\}$ be all equal to zero, there is nothing further to prove; otherwise the lemma holds by applying the induction assumption. Therefore, we may assume that $\{a_i\}$ is C-independent. Let J be a nonzero ideal of R so that $Jb_i + b_iJ \subset R$ for each i, and $J \subset I$. Suppose that $\{x_i, y_i\} \subset J$ satisfies $\sum x_i b_1 y_i = 0$. Then for any $r \in I$, $0 = \sum_i a_1 r x_i b_1 y_i = -\sum_{j=2}^n a_j r (\sum_i x_i b_j y_i)$, using $f(rx_i) = 0$. The independence of $\{a_i\}$ and the induction assumption force $\sum_i x_i b_j y_i = 0$ for each $j \geq 2$. It follows that, for each $j \geq 2$, the map t_j defined by $(\sum x_i b_1 y_i)t_j = \sum x_i b_j y_i$ is an R bimodule map from the ideal Jb_1J to R, and so, $\sum x_i b_j y_i = \sum x_i b_1 c_j y_i$ for some $c_j \in C$. In particular, $J(b_j - b_1 c_j)J = 0$, so the primeness of R and definition of Q result in $b_j = b_1 c_j$. Using these relations, $f = (\sum a_i c_i)xb_1$, where $c_1 = 1$. The case $n = 1$ forces $\sum a_i c_i = 0$, which contradicts the independence of $\{a_i\}$ and completes the proof of the lemma.

Another result we need will enable us to conclude at the appropriate time that R must satisfy a nontrivial generalized polynomial identity (GPI). This result is similar to [8, Theorem 2, p. 578] and its proof will be an easy consequence of the following special case of an elementary but intricate lemma of Amitsur [1, Lemma 1, p. 211].

LEMMA 2. *Let T be a finite-dimensional C subspace of N, J a nonzero ideal of R so that $TJ \subset R$, and U a finite-dimensional C subspace of RC. If for each $y \in J$ there is a nonzero $t \in T$ with $ty \in U$, then R satisfies a nontrivial GPI.*

PROOF. The proof is by induction on $\dim T = n$. When $n = 1$, $T = Ct$, so $tJC \subset U$ is a right ideal of RC, and is finite dimensional over C. Since RC is a prime ring, it acts faithfully on tJC so is itself finite dimensional over C, and it follows that R satisfies a polynomial identity. When $n > 1$, pick $y_0 \in J - \{0\}$, $t_0 \in T - \{0\}$ so that $t_0 y_0 \in U$, and set $J_0 = \{y \in J | t_0 y \in U\}$. If $J \subset J_0 C$, then $t_0 JC \subset U$, and, as above, R satisfies a polynomial identity. Hence, we may assume that there is some $y_1 \in J - J_0 C$. Let $T_1 = \{t \in T | ty_1 \in U\}$ and observe that $T_1 \neq 0$ and $t_0 \notin T_1$. Clearly $T = Ct_0 \oplus S$, as vector spaces, where $\dim S = \dim T - 1$ and $T_1 \subset S$. Also, $SJ \subset R$ and $U + Ty_1$ is a finite-dimensional subspace of RC. If for each $y \in J$ there is a nonzero $s \in S$ with $sy \in U + Ty_1$, then R satisfies a GPI by induction on $\dim S$. Consequently, we may assume that, for some $y_2 \in J$, if $sy_2 \in U + Ty_1$ for $s \in S$, then $s = 0$. We know that $ty_2 \in U$ for some $t = ct_0 + s_0 \in T = Ct_0 \oplus S$, and that $c \neq 0$. Since $c^{-1}ty_2 \in U$ also, we may suppose that $(t_0 + s_0)y_2 \in U$. There is $ft_0 + s_1 \in T - \{0\}$ satisfying $(ft_0 + s_1)(y_1 + y_2) \in U$. Combining the last two facts gives $(ft_0 + s_1)(y_1 + y_2) - f(t_0 + s_0)y_2 \in U$, resulting in $(s_1 - fs_0)y_2 \in U + Ty_1$, and so, forcing $s_1 = fs_0$. Hence $ft_0 + s_1 = f(t_0 + s_0)$, so in particular, $f \neq 0$ and $f(s_0 + t_0)(y_1 + y_2) \in U$. Using $(t_0 + s_0)y_2 \in U$ and $f \neq 0$ leads to $(t_0 + s_0)y_1 \in U$, and so $t_0 + s_0 \in T_1$. Thus $t_0 \in S$ and this contradiction finishes the proof of the lemma.

LEMMA 3. *Let $\{a_1, \ldots, a_n\} \subset N$ be C-independent. If for some $b \in N - \{0\}$ and each $r \in I$, a nonzero ideal of R, $\{bra_1, \ldots, bra_n, a_1, \ldots, a_n\}$ is C-dependent, then R satisfies a GPI.*

PROOF. Let J be a nonzero ideal of R satisfying $\sum a_i J \subset R$ and suppose that, for each $y \in J$, $\{a_i y\}$ is C-dependent. If T is the C subspace of N spanned by $\{a_i\}$ and $U = \{0\}$, then Lemma 2 may be applied to obtain the conclusion that R satisfies a GPI. Assume then that, for some $y \in J$, $\{a_i y\}$ is C-independent. Since it is clear that $\{bra_i y, a_i y\}$ is dependent for each $r \in I$ there is no loss of generality in assuming that $\{a_i\} \subset R$. Next, let J_1 be a nonzero ideal of R so that $bJ_1 \subset R$ and $J_1 \subset I$. Choose $w \in J_1$ so that $bw \neq 0$ and observe that, for all $s, t \in R$, $\{sbwta_1, \ldots, sbwta_n, sa_1, \ldots, sa_n\}$ is dependent. Now $\{(bw)x_2a_1, \ldots, (bw)x_2a_n, a_1, \ldots, a_n\}$ are distinct basis monomials in the free product $R *_Z Z\{x_1, x_2\}$, where Z is the centroid of R, and it follows that the polynomial $S_{2n}(x_1(bw)x_2a_1, \ldots, x_1(bw)x_2a_n, x_1a_1, \ldots, x_1a_n)$ is not zero for S_{2n} the standard polynomial in $2n$ variables. Thus our observation about the dependence of $\{sbwta_1, \ldots, sa_n\}$ shows that $S_{2n}(x_1bwx_2a_1, \ldots, x_1a_n)$ is a GPI for R.

The last preliminary result about N which we require is essentially [**5**, Lemma 1, p. 156]. The proof in our situation follows [**2**, Proof of Theorem 3.1, pp. 57–58].

LEMMA 4. *Let $\{a_1, \ldots, a_n\} \subset N$ be C-independent, and let J be a nonzero ideal of R so that, for each i, $Ja_i + a_i J \subset R$. There is $\{x_i, y_i\} \subset J$ so that $\sum x_i a_1 y_i \neq 0$ but $\sum x_i a_j y_i = 0$ for each $j > 1$.*

PROOF. The proof is by induction on n, the case $n = 1$ being trivial since it says that if $a_1 \neq 0$ then $Ja_1 J \neq 0$. Assume that $n > 1$ and set $A = J^0 \otimes_C J \subset N^0 \otimes_C N$ where N^0 denotes the opposite ring of N, so that if $x^0, y^0 \in N^0$ then $x^0 y^0 = (yx)^0$. For $t = \sum x_i \otimes y_i \in A$, and the action $a_j \cdot t = \sum x_i a_j y_i$, we want to find $t \in A$ satisfying $a_1 \cdot t \neq 0$ but $a_j \cdot t = 0$ if $j > 1$. Let $I = \{t \in A | a_j \cdot t = 0$ if $j > 2\}$ and set $I = A$ if $j = 2$. By induction on n, $a_2 \cdot I \neq 0$ and it is easy to see that $a_2 \cdot I$ is an ideal of R. If $t \in I$ satisfies $a_2 \cdot t = 0$ and $a_1 \cdot t \neq 0$, then the lemma is proved. Hence, we may assume that whenever $t \in I$ and $a_2 \cdot t = 0$, then $a_1 \cdot t = 0$ also. But now the mapping $(a_2 \cdot t)f = a_1 \cdot t$ is an R bimodule mapping from $a_2 \cdot I$ to R, from which it follows that $a_1 \cdot t = a_2 c \cdot t$ for some $c \in C$. Equivalently, $(a_2 c - a_1) \cdot I = 0$ and so the induction assumption shows that $\{a_2 c - a_1, a_3, \ldots, a_n\}$ is a C-dependent set. This contradiction means that there must be $t \in I$ with $a_2 \cdot t = 0$, but $a_1 \cdot t \neq 0$, proving the lemma.

Now we will explain what we mean by a generalized differential identity with involution. Roughly speaking, one has an expression in certain variables, with derivations and the involution applied to the variables, so that all substitutions from R result in zero. Note that if $d \in \text{Der}(R)$ and if its extension to Q is inner and given by $a \in N$, then the formal expression $x^d - xa + ax$ is such an identity for R. Thus we must allow such identities to have coefficients in N. We proceed to formalize these ideas, and assume now that R has an involution, $*$.

Our observations above show that $\text{Der}(R) \subset \text{Der}(N)$. Also, if $d \in \text{Der}(R)$ and $c \in C$ then $dc \in \text{Der}(N)$, where $a^{dc} = a^d c$. Thus, $\text{Der}(R)C$ is a Lie ring of derivations of N which is also a right C-module. Let V denote the subring of $\text{End}(N, +)$ generated by $\text{Der}(R)C$, and let X^V be a set of noncommuting indeterminates over C which is of the form $\{x_i\} \cup \{x_i^v | v \in V\}$, where i ranges over the positive integers.

Finally, the free product over C of N with $C\{X^V, Y^V\}$ will be denoted by F. Observe that a C-basis for F is the set of all monomials $w_0 z_1 w_1 \cdots z_n w_n$, where the $\{w_j\}$ come from a C-basis for N and $\{z_j\} \subset X^V \cup Y^V$. Any $f \in F$ involves only finitely many indeterminates, so for a suitable n, f defines a function from R^n to N by substituting r_i for x_i, r_i^* for y_i, $(r_i)^v$ for x_i^v, and $(r_i^*)^v$ for y_i^v. If J is an ideal of R and the image of J^n under f is $f(J^n)$ then f is called a *generalized *-differential identity*, or G*-DI, for J if $f(J^n) = 0$. In the case that all variables appearing in f come from $\{x_i\} \cup \{y_i\}$, we call f a generalized *-polynomial identity (G*-PI) for J if $f(J^n) = 0$. To say that $f \in F$ is multilinear and homogeneous (of degree n) means that there is some n element subset A of positive integers so that every basis monomial of F which appears in f contains exactly n indeterminates, including multiplicity, and that the set of subscripts of these is A. Of course, the exponents of the indeterminates may vary from one monomial to another. For example, $x_1 a y_2^v + b y_2^h c y_1^k + x_1 x_2 \in F$ is multilinear and homogeneous of degree 2, where $v, h, k \in V$ and $a, b, c \in N$. We call $f \in F$ multilinear if no monomial appearing in f contains two indeterminates with the same subscript. Of primary interest are the multilinear G*-DIs for J, but we note that if f is any G*-DI for J, then f can be linearized in the usual way to obtain a multilinear (and homogeneous) G*-DI for J. Note that R is GPI if $f \in R *_Z Z\{x_i\}$ is a G*-DI for R, for Z the centroid of R.

An example of a G*-DI for R can be obtained by taking a GPI for R and replacing each variable x_i appearing in it with x_i^v for some $v \in V$. Next we give an example of a linear G*-DI which is not of this type.

EXAMPLE 2. Take R as in Example 1, the matrices in $\mathrm{Hom}_C(U, U)$ having only finitely many nonzero entries, where U is now a countable dimensional vector space over the field C. Each element of R may be viewed as an element of $M_{2n}(C)$, in the upper left corner of a countable-by-countable array. The symplectic involution on $M_{2n}(C)$ extends naturally to R. Recall that for $A \in M_{2n}(C)$ regarded as $A = (A_{ij})$ for $A_{ij} \in M_2(C)$, the symplectic involution is given by $A^* = (B_{ij})$ for $B_{ij} = (A_{ji})^*$, where $\begin{pmatrix} a & b \\ c & d \end{pmatrix}^* = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. If $\{e_{ij}\}$ are the usual matrix units in R, then $e_{11} x e_{22} + e_{11} y e_{22}$ is a G*-PI for R. Hence $e_{11} x^v e_{22} + e_{11} y^v e_{22}$ is a G*-DI for R, for any $v \in V$ which restricts to an endomorphism of the symmetric elements of R. Also, if $w = \mathrm{ad}(e_{22})$, the inner derivation given by commutation with e_{22}, then $e_{11} x^w + e_{11} y^w$ is a G*-DI for R, although $e_{11} x + e_{11} y$ is not a G*-PI.

To avoid confusion later, we wish to show that if R satisfies a G*-PI with variables in $\{x_i\}$, that is, a "GPI with coefficients in N", then R satisfies a GPI.

PROPOSITION. *If R satisfies a nonzero G*-PI $f \in N *_C C\{x_i\} \subset F$, then R satisfies a nonzero GPI.*

PROOF. Clearly we may assume that f is multilinear and homogeneous. We proceed by induction on $\deg f$, and note that $\deg f > 1$ by Lemma 1. Assume first that f is not an identity for N, so that $f(t_1, \ldots, t_n) \neq 0$ for some $\{t_i\} \subset N$. In particular, $f(x, t_2, \ldots, t_n) \in F - \{0\}$, and so by using Lemma 1 again, $f(x, t_2, \ldots, t_n)$ is not an identity for R. Choose $r \in R$ with $f(r, t_2, \ldots, t_n) \neq 0$ and set $h(x_2, \ldots, x_n) = f(r, x_2, \ldots, x_n)$. Then h is a nonzero G*-PI for R with variables in $\{x_i\}$ and $\deg h < \deg f$, so by induction, R satisfies a GPI. Now suppose that f is an identity for N.

It is easy to see that N is a prime ring with extended centroid C. Briefly, if $a, b \in N$ and $aNb = 0$, then $(aI_a)R(I_b b) = 0$ shows either $a = 0$ or $b = 0$, where I_a and I_b are the appropriate ideals of R. Next, if T is an N-bimodule mapping of the ideal J of N into N, then, for any $y \in J$, T restricts to an R-bimodule map of $I_{(y)T}yR$ into R, and it follows that $T \in C$. Since f is an identity for N, it is a GPI for N, so there is $e^2 = e \in NC = N$ with eNe a division algebra, finite dimensional over C [8, Theorem 2, p. 578]. Let eNe satisfy the standard identity S_{2m}. Now $I_e e I_e \neq 0$, so there are $a \in eI_e$ and $b \in I_e e$ so that $ba \neq 0$. It follows that $bS_{2m}(ax_1 b, \dots, ax_{2m} b)ax_{2m+1}$ is a nonzero GPI for R, since $eI_e R I_e e \subset eNe \cap R$.

The example shows that a nontrivial linear G^*-PI can exist, in contrast to the situation for a linear GPI, as shown in Lemma 1. Also a G^*-DI can exist, using inner derivations, which does not arise from a G^*-PI by substitution. Our goal is to show, as in [5] for the noninvolution case, that any multilinear G^*-DI for R either arises by substitution into G^*-PIs for R, or is a consequence of identities which hold in any ring and follow from the definition of derivation or endomorphism. Examples of such identities, with $x \in \{x_i\} \cup \{y_i\}$, follow:

$x^{u+v} - x^u - x^v$ for $u, v \in V$;

$x^{vc} - x^v c$ for $v \in V$ and $c \in C$;

$x^v - x^{dh} + x^{hd}$ for $d, h \in \mathrm{Der}(R)C$ and $v = dh - hd$;

$x^d - xa + ax$ for d the inner derivation induced by $a \in N$; and

$x^v - x^{d \cdots d}$ when char $R = p > 0$, $d \in \mathrm{Der}(R)C$, $d \cdots d$ represents the product of d with itself p times, and $d \cdots d = v \in \mathrm{Der}(R)C$.

For emphasis, we note again that in our notation, if $r \in R$ and $v, u \in V$ then $r^{vu} = ((r)v)u$; and also, if V has an identity element 1, then $r^2 = 2r$, and not the product of r with itself.

More complicated identities arise by taking products of elements in $\mathrm{Der}(R)C$. For example, if $d, h, k \in \mathrm{Der}(R)C$, if d is inner and induced by $a \in N$, and if $c \in C$, then $x^{(hc)k} - x^{hk}c - x^h c^k$ is an identity for R, as is $x^{dhk} - x^{hk}a - x^h a^k - x^k a^h - xa^{hk} + a^{hk}x + a^h x^k + a^k x^h + ax^{hk}$. Identities such as these, which follow from the definition of endomorphism or derivation, are called *universal* identities, and we regard them as trivial G^*-DIs for R. For a multilinear G^*-DI for J (an ideal of R) to be nontrivial, it must not belong to the ideal of universal identities, which we define next.

DEFINITION. The ideal of universal identities for R, denoted $U(R)$, is the ideal of F generated by all elements in F of the types described below, where x is used to represent any element in $\{x_i\} \cup \{y_i\}$, $c \in C$, and $u, v \in V$:

(I) x^0;

(II) $x^1 - x$, if V has an identity element 1;

(III) $x^{u+v} - x^u - x^v$;

(IV) $x^{utv} - x^{uhkv} + x^{ukhv}$ for $h, k \in \mathrm{Der}(R)C$ and $t = hk - kh$;

(V) $x^{u(hc)kv} - x^{uh(kc)v} - x^{u(hc^k)v}$ for $h, k \in \mathrm{Der}(R)C$;

(VI) $x^{vc} - x^v c$;

(VII) $x^{vd} - x^v a + ax^v$ for $d \in \mathrm{Der}(R)C$, an inner derivation of N, induced by $a \in N$;

(VIII) $x^{vtu} - x^{vd \cdots du}$ when char $R = p > 0$, $d \in \mathrm{Der}(R)C$, $d \cdots d$ is the product of d with itself p times, and $d \cdots d = t$;

(IX) any of (IV), (V), (VII), or (VIII) with either u or v replaced by the identity map on R.

The proof of our main result requires using a G^*-DI for J with very special exponents. Following the approach in [5], we describe what these are and show that if $f \in F$ is a multilinear G^*-DI for J, either $f \in U(R)$, or $f + U(R) = g + U(R)$, where g is a multilinear G^*-DI for J with exponents of the required type. To begin with, let M_0 be a basis for the C-subspace of $\mathrm{Der}(R)C$ consisting of those derivations whose extensions to Q are inner, and extend M_0 to a basis M of $\mathrm{Der}(R)C$. Note that no nontrivial linear combination of elements of $M - M_0$ can be inner on Q. Next, choose a well-ordering of M so that the elements of $M - M_0$ preceed those in M_0. Using this well-ordering, the set of all finite sequences of elements of M can be well-ordered by making longer sequences greater than shorter ones, and by ordering sequences of the same length lexicographically. Clearly, any sequence $(m_1, \ldots, m_k) \in M^k$ can be identified with the product $m_1 m_2 \cdots m_k \in V$, and we say that this product *comes from* the sequence $(m_1, \ldots, m_k)$. Of course, as an element of V, $m_1 \cdots m_k$ may have many representations as products of elements from M, and each comes from a different sequence. By identifying any product of elements from M with the sequence it comes from, we may well-order any given collection of such products, even if they all represent the same element of V. That is, we well-order the products, identified as sequences, rather than well-order the subset of V which the products represent.

The special exponents in which we are interested are those which are products of increasing elements from $M - M_0$. More specifically, let W be the set of finite sequences of elements of $M - M_0$, consisting of the empty sequence, and all $(m_1, \ldots, m_k)$ satisfying $m_1 \leq m_2 \leq \cdots \leq m_k$, and when char $R = p > 0$, having no p consecutive m_i equal. The well-ordering on the set of finite sequences of elements of M restricts to a well-ordering of W, and using this well-ordering we may consider that the collection of products of elements of $M - M_0$ which come from (the sequences in) W is also well-ordered. If 1, the identity map on R, is considered to come from the empty sequence in W, then the special exponents we want are those which come from W.

Our next lemma will show that any multilinear $f \in F$ is equivalent modulo $U(R)$ to $g \in F$ having all its exponents come from W. Let us briefly describe how one obtains g starting with $f = x^v$ for $x \in \{x_i\} \cup \{y_i\}$ and $v \in V$. First, since $v \in V$, we can write v as a sum of products of the form $d_1 d_2 \cdots d_n$ for $d_i \in \mathrm{Der}(R)C$. Of course, such an expression for v is not unique, but having picked some such expression, each d_i appearing can be written uniquely as a C-linear combination of the elements of M. Thus one can write v as a sum of terms $(m_1 c_1 + \cdots + m_k c_k) \cdots (n_1 f_1 + \cdots + n_s f_s)$ where $m_i, n_j \in M$ and $c_i, f_j \in C$. By multiplying and using the identity $(mc)n = (mn)c + mc^n$ for $m, n \in M$ and $c \in C$, one can represent v as a C-linear combination of products of elements of M, each coming from a different sequence in $\bigcup M^k$. Write $v = w_1 c_1 + \cdots + w_n c_n$ where w_i comes from the sequence $\overline{w}_i \in \bigcup M^k$. Then using elements of types (III) and (VI) in $U(R)$, one has $x^{w_1} c_1 + \cdots + x^{w_n} c_n \in x^v + U(R)$. We may also assume that the $\overline{w}_i$ are increasing sequences by using elements of type (IV). Next, the ordering on M and elements of type (VII) enable us to replace each $x^{w_i} c_i$ by a sum $\sum_j a_{ij} x^{u_i} b_{ij}$, where $a_{ij}, b_{ij} \in N$, and u_i comes from the initial segment of

the sequence $\overline{w}_i$ of elements from $M - M_0$. Since each u_i comes from W, when char $R = 0$, $g = \sum_{i,j} a_{ij} x^{u_i} b_{ij}$ is the element in $x^v + U(R)$ we want. Note that picking a different representation of v as a sum of products of elements in $\text{Der}(R)C$ could lead to a different g. The case for a general $f \in F$ is more complicated but proceeds in the manner described above. Before stating the general result, we give a useful definition.

DEFINITION. Let $f = a_1 z_1 a_2 \cdots a_n z_n a_{n+1} \in F$ be an arbitrary monomial, where each $a_i \in N$, and each z_i represents an element in $X^V \cup Y^V$. The *variable sequence* of f is the n-tuple in $(\{x_i\} \cup \{y_i\})^n$ whose jth coordinate is the indeterminate, without exponent, represented by z_j. For example, $x_3 y_2, x_3 a y_2^v$, and $a x_3^v b y_2^u$ all have variable sequence (x_3, y_2), where $a, b \in N$, and $v, u \in V$.

LEMMA 5. *Let $f \in F - U(R)$ be a monomial. Then there is a $g \in f + U(R)$ so that all exponents appearing in g come from W, and each monomial appearing in g has the same variable sequence as f.*

PROOF. Let $f = a_1 z_1 a_2 \cdots a_n z_n a_{n+1}$, where each $a_i \in N$ and each $z_i \in X^V \cup Y^V$. Since $f \notin U(R)$, no z_j has exponent 0. Also, because $U(R)$ contains all elements of type (II), namely, $x^1 - x$ if V contains 1, we may assume for convenience of notation that each z_i has exponent in $V \cup \{1\}$. That is, if x_i appears in f without exponent, we regard it as x_i^1, for 1 the identity map on R. Thus, we may now write $f = a_1 z_1^{v_1} a_2 \cdots a_n z_n^{v_n} a_{n+1}$ with each $z_i \in \{x_i\} \cup \{y_i\}$ and each $v_j \in V \cup \{1\}$. Using the procedure described above for the case $f = x^v$, for each $v_j \in V - \{1\}$, choose a way of writing v_j as a C-linear combination of products of elements of M, each of which comes from a different sequence in $\bigcup M^k$. We write this representation of v_j as $w_{j1} c_{j1} + \cdots + w_{jk(j)} c_{jk(j)}$ where w_{ji} is the product of elements of M coming from the s_i-tuple $\overline{w}_{ji} \in M^{s_i}$. Having chosen such representations for each nonidentity exponent appearing in f, we attach an integer, or weight, to f which counts the number of elements of M, including multiplicity, which are needed in the representations of its exponents. Before proceeding, note that if $v_i = v_j$ for $i \neq j$, different representations for this same exponent are allowed. For each exponent v_i in f, set $\text{Wt}(v_i) = 0$ if $v_i = 1$ and $\text{Wt}(v_i) = s_1 + \cdots + s_{k(i)}$ if $v_i \neq 1$ and has the representation described above. Set $\text{Wt}(f) = \text{Wt}(v_1) + \cdots + \text{Wt}(v_n)$. Observe that $\text{Wt}(f)$ depends on the particular choices made for the representations of the v_i as linear combinations of products of the elements of M. We proceed to prove the lemma by induction on $\text{Wt}(f)$.

If $\text{Wt}(f) = 0$, then each $v_i = 1$, so each exponent appearing in f comes from W (in fact, from the empty sequence) as required. Hence, we may assume $\text{Wt}(f) > 0$ and that the lemma holds for any monomial $f' \in F - U(R)$ satisfying $\text{Wt}(f') < \text{Wt}(f)$. Choose some exponent $v \in V$ appearing in f which has been represented as $v = w_1 c_1 + \cdots + w_k c_k$ for $\{w_i\}$ products of elements of M coming from different s_i-tuples $\overline{w}_i \in M^{s_i}$. Assume that $k > 1$ and write $f = g_1 x^v g_2$ for $x \in \{x_i\} \cup \{y_i\}$ and $g_1, g_2 \in F$. Set $u_2 = w_k c_k$ and $u_1 = v - u_2$ and observe that $q = g_1 (x^v - x^{u_1} - x^{u_2}) g_2 \in U(R)$. It follows that $f - q = g_1 x^{u_1} g_2 + g_1 x^{u_2} g_2 \in f + U(R)$, that not both $g_1 x^{u_1} g_2 \in U(R)$ and $g_1 x^{u_2} g_2 \in U(R)$, and that $\text{Wt}(g_1 x^{u_i} g_2) < \text{Wt}(f)$ for $i = 1, 2$. Therefore, we are done, by induction on $\text{Wt}(f)$, if $k > 1$. Consequently, we may assume that each nonidentity exponent appearing in f has the form wc, where w comes from some $\overline{w} \in \bigcup M^n$. As above, if we write $f = g_1 x^{wc} g_2$, then

$q = g_1(x^{wc} - x^w c)g_2 \in U(R)$, so $g_1 x^w g_2 c = f - q \in f + U(R)$, and we may assume that each nonidentity exponent appearing in f comes from some $\overline{w} \in \bigcup M^n$.

Now suppose that some nonidentity exponent $v = m_1 \cdots m_n$ appearing in f comes from $(m_1, \ldots, m_n) \in M^n$, and that $m_i > m_{i+1}$, in the well-ordering of M, for some i. For convenience of notation, let $h = m_i$, $k = m_{i+1}$, $t = hk - kh \in \mathrm{Der}(R)C$, u the product coming from $(m_i, \ldots, m_{i-1})$, and v the product coming from $(m_{i+2}, \ldots, m_n)$. Write $f = g_1 x^{uhkv} g_2$, and observe that

$$q = g_1(x^{utv} - x^{uhkv} + x^{ukhv})g_2 \in U(R),$$

so that $f + q = g_1 x^{ukhv} g_2 + g_1 x^{utv} g_2 \in f + U(R)$, and both monomials cannot be in $U(R)$. If $g_1 x^{utv} g_2 \in U(R)$, then we have, in effect, moved k to the left of h in v. If $g_1 x^{utv} g_2 \notin U(R)$, write t as a linear combination of elements of M. Using the identity $(mc)d = (md)c + mc^d$, for $m, d \in \mathrm{Der}(R)C$ and $c \in C$, one can write utv as a C-linear combination of products of elements from M each of which comes from an element in $M \cup \cdots \cup M^{n-1}$. By the arguments in the paragraph above, $g_1 x^{utv} g_2 + q_1 = \sum g_1 x^{w_j} g_2 c_j$ where $q_1 \in U(R)$ and w_j comes from some $\overline{w}_j \in M \cup \cdots \cup M^{n-1}$. Consequently, for each j, either $g_1 x^{w_j} g_2 c_j \in U(R)$ or $\mathrm{Wt}(g_1 x^{w_j} g_2 c_j) < \mathrm{Wt}(f)$. Our induction assumption allows us to conclude that, for some $q_2 \in U(R)$, $g_1 x^{utv} g_2 + q_2$ has each exponent coming from W and each monomial with the same variable sequence as f. Consequently, it suffices to prove the lemma for $g_1 x^{ukhv} g_2$, when this monomial is not in $U(R)$. By repeating this process at most $n(n-1)/2$ times we will have proved what we need about f, or we may assume that the exponent v comes from $(m_1, \ldots, m_n)$ and $m_1 \leq m_2 \leq \cdots \leq m_n$. Hence we may assume that each nonidentity exponent in f comes from an increasing sequence.

The next step is to eliminate the Q-inner derivations which may appear in the exponents of f. Since we now have the exponents in f coming from increasing sequences, the ordering on M forces the Q-inner derivations to appear to the right of the elements in $M - M_0$. Suppose that some exponent appearing in f has the form vt, where v is 1 or comes from the (increasing) sequence $(m_1, \ldots, m_{n-1})$ and $t \in M_0$ is induced on R by commutation with $a \in N$. As above, write $f = g_1 x^{vt} g_2$, observe that $q = g_1(x^{vt} - x^v a + a x^v)g_2 \in U(R)$, and then that $f - q = g_1 x^v(ag_2) - (g_1 a)x^v g_2$ has each of its monomials p satisfying $\mathrm{Wt}(p) = \mathrm{Wt}(f) - 1$. Since each monomial also has the same variable sequence as f, we would be finished by induction. Therefore, we may assume that the nonidentity exponents in f are products coming from increasing sequences of elements in $M - M_0$. Hence, if $\mathrm{char}\, R = 0$, the proof is complete.

Finally, assume $\mathrm{char}\, R = p > 0$ and that in some nonidentity exponent of f, an element in $M - M_0$ occurs p consecutive times. Let us write this exponent as $ud \cdots dv$, where $d \cdots d$ represents the occurence of $d \in M - M_0$ p times, and u and v represent products in $M - M_0$ coming from the appropriate increasing sequences. For $d \cdots d = t \in \mathrm{Der}(R)C$, write $f = g_1 x^{ud \cdots dv} g_2$, note that $q = g_1(x^{ud \cdots dv} - x^{utv})g_2 \in U(R)$, and consider $g_1 x^{utv} g_2 = f - q \in f + U(R)$. Now $f - q \notin U(R)$ and t can be written as a linear combination of elements of M. Using the argument given above to show that the exponents could be assumed to come from increasing sequences, we may conclude that $g_1 x^{utv} g_2 + q_1$, for some $q_1 \in U(R)$, satisfies the conclusion of the lemma. To review briefly, after multiplying out utv, one can represent this element as a sum of products of elements of M, replace

$g_1 x^{utv} g_2$ by a sum of monomials with the same variable sequence, but each of smaller "weight", and then apply the induction assumption to complete the proof of the lemma.

An immediate consequence of Lemma 5 is that if $f \in F - U(R)$ then there is $g \in f + U(R)$ so that all exponents appearing in g come from W. Also, each monomial in g, not in $U(R)$, must have the same variable sequence as some monomial in F. Note that the particular $g \in F$ that one obtains from f depends not only on the choices for the representations of the exponents in f as sums of products of elements in $\mathrm{Der}(R)C$, but also on the particular choice of M and on the well-ordering of M. Now if $f \in F - U(R)$ is a G^*-DI for an ideal J of R, then the $g \in f + U(R)$, as in Lemma 5, is also a G^*-DI for J, and has all of its exponents coming from W. Our goal is to show that any such multilinear g is obtained from a G^*-PI for J by substitution. As in [5], the linear case comes first and contains all of the technical difficulties. We prove first that the existence of a G^*-DI for J, which is not in $U(R)$, forces R to satisfy a GPI. The proof of this fact depends heavily on [5, Lemma 2, p. 158] changed to fit our context. Because of the importance of this result of Kharchenko, the complexity of its proof, and the consequent difficulty in following the argument of Kharchenko as it applies in our situation, we incorporate his basic argument in our proof. The place at which this occurs will be made clear. Finally, we emphasize again that to say $v \in V$ comes from some element in W means that we are viewing v as some given product of elements in $M - M_0$, rather than as an element of V. Thus, if $u = v$ are exponents coming from $\bar{u}$ and $\bar{v}$ in W, and if $\bar{u} < \bar{v}$, we regard $u < v$.

THEOREM 1. *Let R be a prime ring with involution, $*$, and let $f \in F$ have the form*
$$f = \sum_h \sum_i a_{hi} x^h b_{hi} + \sum_k \sum_j c_{kj} y^k d_{kj}$$
where all h and k come from W, $x = x_s$ and $y = y_s$ for some s, and all coefficients are in N. If $f(I) = 0$ for some nonzero ideal I of R, then either R satisfies a nonzero GPI, or for each h and each k, $\sum_i a_{hi} \otimes b_{ni} = 0$ and $\sum_j c_{kj} \otimes d_{kj} = 0$ in $N \otimes_C N$, so that $f = 0$ in F.

PROOF. Assume throughout that R does not satisfy a GPI, and note that we may assume $I^* = I$, since otherwise, replace I with II^*. Using the ordering on W, let h be the largest exponent appearing in f. We may assume that x^h appears, since $f(r^*) = 0$ shows that by interchanging x and y, one obtains another $g \in F$ with $g(I) = 0$, for which it suffices to prove the theorem.

Write $f = \sum_{i=1}^n a_{hi} x^h b_{hi} + \sum_{j=1}^m c_{hj} y^h d_{hj} + f_1$, where $f_1 \in F$ is the sum of all monomials in f having exponent smaller than h. We proceed by induction on h, and use induction on m. When $h = 1$, $f = \sum_{i=1}^n a_i x b_i + \sum_{j=1}^m c_j y d_j$. Should $m = 0$, then Lemma 1 shows that $\sum a_i \otimes b_i = 0$ and $f = 0$ in F. Suppose that $m > 0$ and $\sum a_i \otimes b_i = 0$. Once again, the conclusion follows easily from Lemma 1. Hence, we may assume that $\sum a_i \otimes b_i \neq 0$, and so, by taking a subset of $\{a_i\}$ if necessary, we may assume that $\{a_i\}$ is C-independent, and all $b_i \neq 0$. Choose a nonzero ideal J of R satisfying $c_1 J + J c_1 \subset R$. In f, replacing x with $x c_1^* r^*$ and y with $r c_1 y$, for any fixed $r \in J$ yields another G^*-DI g for I. Consider $q = g - c_1 r f$. It is clear that q is a G^*-DI for I and that $q = \sum s_i x t_i + \sum_{j=2}^m (c_j r c_1 - c_1 r c_j) y d_j$.

By induction on m, $\sum s_i \otimes t_i = 0$, and so $\{s_i\} = \{c_1 r a_i, a_i\}$ is a C-dependent set for each $r \in J$. But now Lemma 3 gives the contradiction that R satisfies a GPI. Therefore, we must have $\sum a_i \otimes b_i = 0$, completing the case when $h = 1$. Note that this case has shown that I satisfies a nonzero G*-PI if and only if R satisfies a nonzero GPI. This is a slight generalization of the linear case of [9, Theorem 4.7, p. 515].

Assume that the theorem is valid for any linear G*-DI, for some I, having exponents coming from W, and largest exponent smaller than h. Let f be as above with largest exponent h. Assume first that $m = 0$. It is this case which requires the lengthy argument of Kharchenko [5, Proof of Lemma 2, pp. 158–160] since it covers the case of his result, where no involution is assumed. Using our induction assumption, it suffices to prove that $\sum a_{hi} \otimes b_{hi} = 0$. If $\sum a_{hi} \otimes b_{hi} \neq 0$, there is no loss of generality in assuming that $\{a_{hi}\}$ is C-independent, and that no $b_{hi} = 0$. The first reduction to be made is to show that we may take $i = 1$, so suppose that $i > 1$. Choose a nonzero ideal J of R satisfying $\sum_i J a_{hi} + a_{hi} J \subset R$. By Lemma 4 there is $\{s_i, t_i\} \subset J \cap I$ so that $\sum_i s_i a_{h1} t_i \neq 0$, but $\sum_i s_i a_{hj} t_i = 0$ for $j > 1$. Consider the function $g_j : R \to N$ defined by $g_j(r) = s_j f(t_j r)$. We claim that g_j can be regarded as the evaluation of $g_j(x) \in F$ which is linear of degree one and has exponents which come from W. To see why this is so, let $w = m_1 m_2 \cdots m_k$ come from $\overline{w} = (m_1, \ldots, m_k) \in W$, let $v = m_{i_1} \cdots m_{i_j}$ come from any subsequence $\overline{v} = (m_{i_1}, \ldots, m_{i_j})$ of $\overline{w}$, and let u come from the complementary subsequence $\overline{u}$ of $\overline{w}$, obtained by deleting the elements in $\overline{v}$ from $\overline{w}$. For example, if $w = m_1 m_2 m_3 m_4$, then one choice for v and u is $v = m_2$ and $u = m_1 m_3 m_4$, and another is $v = m_1 m_4$ and $u = m_2 m_3$. For any $r, t \in R$, the definition of derivation gives $(rt)^w = \sum r^v t^u$, where the sum is taken over all possible subsequences $\overline{v}$ of $\overline{w}$, including the empty subsequence, interpreted as 1. In particular, we may write

$$(1) \qquad (rt)^w = rt^w + q r^{m_1} t^{m_2 \cdots m_k} + \cdots + r^w t$$

where q is the number of consecutive m_i equal to m_1, and the missing terms all have exponents coming from W and less than w, in the well-ordering defined by W.

Going back to $g_j(r) = s_j f(t_j r)$, letting h come from $(m_1, \ldots, m_k) \in W$, and using (1), one obtains $g_j(r) = \sum_i (s_j a_{hi} t_j) r^h b_{hi} + \overline{g}_j$, where $\overline{g}_j$ is an expression which is linear in r and having all exponents appearing on r coming from W and being less than h. Consequently, $g_j(x) = \sum_i (s_j a_{hi} t_j) x^h b_{hi} + q_j$ is a linear G*-DI for R whose exponents come from W, where all exponents appearing in q_j are less than h. From the choice of $\{s_j, t_j\}$, $g = \sum_j g_j = \sum_j (s_j a_{h1} t_j) x^h b_{h1} + \overline{g}$ is a linear G*-DI for R and the exponents appearing in $\overline{g}$ come from W and are less than h. Since g has only one monomial containing x^h, we may as well assume that $f = a x^h b + f_1$, where $f_1 \in F$ is the sum of all monomials in f having exponent smaller than h. Recall that this reduction has come about in the case $\sum a_{hi} \otimes b_{hi} \neq 0$ and $m = 0$; that is, y appears with exponents which are less than h.

As above, suppose that $h = m_1 \cdots m_n$ comes from $(m_1, \ldots, m_n) \in W$ and let v denote the product $m_2 \cdots m_n$ coming from $(m_2, \ldots, m_n) \in W$, or $v = 1$ if $n = 1$. If any exponent in f is dv, coming from $(d, m_2, \ldots, m_n)$ where $d \leq m_1$, let $m_1 > d_1 > \cdots > d_r$ be all such possible initial elements, and let the monomials in f, in which x appears with exponent $d_i v < h$, be $\sum_j a_{ij} x^{d_i v} b_{ij}$. If x also appears in f with exponent v, write the corresponding monomials as $\sum a_{0j} x^v b_{0j}$. Thus we

may write

(2) $$f = ax^h b + \sum_{ij} a_{ij} x^{d_i v} b_{ij} + \sum_j a_{0j} x^v b_{0j} + f_2,$$

where f_2 is the sum of all monomials of f containing y to some exponent smaller than h, and x to some exponent smaller than h and not any of v or $d_i v$.

Given any $s_k, t_k \in R$, consider, as above, the function $g_k : I \to N$ defined by $g_k(r) = s_k f(t_k r)$. Using (1), the comments following it, and the last expression for f in (2), one obtains the linear G*-DI for I

(3) $$g_k(x) = (s_k a t_k) x^h b + q s_k a (t_k)^{m_1} x^v b$$
$$+ \sum_{i,j} s_k a_{ij} (t_k)^{d_i} x^v b_{ij} + \sum_j (s_k a_{ij} t_k) x^v b_{ij} + \bar{g}_k$$

where q is the number of m_i equal to m_1, all exponents appearing in $\bar{g}_k$ come from W, and no exponent in $\bar{g}_k$ appearing on x can be $v = m_2 \cdots m_n$. Now $a \in N$, so there is a nonzero ideal J of R with $Ja + aJ \subset R$, and there is $\{s_k, t_k\} \subset J - \{0\}$ satisfying $\sum_k s_k a t_k = 0$. For example, if $s, t, u \in J^2$, then $(asat)au - (as)a(tau) = 0$. Given such elements $\{s_k, t_k\}$, and the corresponding $g_k(x)$ as given in (3), we get

(4) $$g(x) = \sum g_k(x) = q \sum_k s_k a (t_k)^{m_1} x^v b + \sum_{i,j,k} s_k a_{ij} (t_k)^{d_i} x^v b_{ij}$$
$$+ \sum_{j,k} (s_k a_{0j} t_k) x^v b_{0j} + \bar{g}.$$

Now g is a linear G*-DI for I whose exponents come from W, and $\bar{g}$ is the sum of all monomials in g in which x appears with exponents less than h and different from v, and y appears with exponents less than h. Applying our induction assumption on h to $g \in F$ enables us to conclude that the tensor product of the coefficients of the monomials containing x^v must be zero. Specifically, we obtain

(5) $$\left(q \sum_k s_k a (t_k)^{m_1} \right) \otimes b + \sum_{i,j} \left(\sum_k s_k a_{ij} (t_k)^{d_i} \right) \otimes b_{ij}$$
$$+ \sum_j \left(\sum_k s_k a_{0j} t_k \right) \otimes b_{0j} = 0.$$

If one chooses a C-independent subset of the right factors $\{b, b_{ij}, b_{0j}\}$, if the other right factors are written as C-linear combinations of these, and if (5) is rewritten using the independent subset only, then the new left factors must be zero. In particular, $q \sum_k s_k a (t_k)^{m_1}$ is a C-linear combination of $\{(\sum_k s_k a_{ij} (t_k)^{d_i}), \sum_k s_k a_{0j} t_k\}$, and since the elements of C used in this linear combination are those arising from the dependence relations among the $\{b, b_{ij}, b_{0j}\}$, these elements of C do not depend on $\{s_k, t_k\} \subset J$. The definition of W shows that $q \neq 0$ in R, so we may write

(6) $$\sum_k s_k a (t_k)^{m_1} + \sum_{i,j,k} s_k (c_{ij} a_{ij}) (t_k)^{d_i} + \sum_{j,k} s_k (c_j a_{0j}) t_k = 0$$

for $\{c_i, c_{ij}\} \subset C$ and independent of $\{s_k, t_k\} \subset J$ satisfying $\sum s_k at_k = 0$. In (6), set $a_i = \sum_j c_{ij} a_j$ and $a_0 = \sum_j c_j a_{0j}$ to obtain

$$(7) \qquad \sum_k s_k a(t_k)^{m_1} + \sum_{i,k} s_k a_i(t_k)^{d_i} + \sum_k s_k a_0 t_k = 0$$

for $\{a_0, a_i\} \subset N$ and, independent of the choice of $\{s_k, t_k\} \subset J$, satisfying $\sum s_k at_k = 0$.

Define $T \colon JaJ \to N$ by

$$\left(\sum p_j a q_j\right) T = \sum_j p_j a(q_j)^{m_1} + \sum_{i,j} p_j a_i(q_j)^{d_i} + \sum_j p_j a_0 q_j,$$

and note that T is a function because of (7). It is clear that T is a left R module homomorphism as well. Now $\{m_1, d_i\} \subset \mathrm{Der}(R)C$, so this subset of M can be written using a finite subset of $\mathrm{Der}(R)$ and a finite subset of C, say $\{c_k\}$. There is a nonzero ideal B of R, so that $B \subset J$, $c_k B \subset R$ for all $c_k \in \{c_k\}$, and so that $aB + Ba + a_0 B + Ba_0 + \sum_i (Ba_i + a_i B) \subset R$. It follows that $(BaB^2)T \subset R$, which means that T is a left R module homomorphism from the ideal BaB^2 of R, into R. Hence, T is given by right multiplication by some $t \in Q$, so

$$(8) \qquad \left(\sum p_j a q_j\right) t = \sum_j p_j a(q_j)^{m_1} + \sum_{i,j} p_j a(q_j)^{d_i} + \sum_j p_j a_0 q_j.$$

Now for any $r \in R$, by using (8) we have

$$\left(\sum p_j a q_j\right)(rt) = \left(\sum p_j a(q_j r)\right) t$$
$$= \sum_j (p_j a q_j) r^{m_1} + \sum_j p_j a(q_j)^{m_1} r + \sum_{i,j} (p_j a_{ij} q_j) r^{d_i}$$
$$+ \sum_{i,j} p_j a_i(q_j)^{d_i} r + \sum p_j a_0 q_j r,$$

and substracting from this equation (8) multiplied by r on the right yields

$$(9) \quad \left(\sum p_j a q_j\right)(rt - tr) = \sum_j (p_j a q_j) r^{m_1} + \sum_{i,j} (p_j a_i q_j) r^{d_i} \quad \text{for any } \{p_j, q_j\} \subset B^2.$$

Let $a, e_2, \dots, e_m$ be a C-basis for the C subspace of N spanned by $\{a, a_i\}$, and use Lemma 4 to find $\{p_j, q_j\} \subset B^2$ with $\sum p_j a q_j \neq 0$ but $\sum p_j e_i q_j = 0$ for $i \geq 2$. Set $L = \{\sum p_j a q_j \in B^2 a B^2 \mid \sum_j p_j e_i q_j = 0 \text{ for each } i\}$. Clearly, L is a nonzero ideal of R, and if $\sum p_j a q_j \in L$, then, since $a_i = c_i a + \sum c_{ij} e_j$, one has $\sum p_j a_i q_j = c_i \sum p_j a q_j$. Consequently, if $s \in L$ then (9) reduces to $s(rt - tr) = sr^{m_1} + \sum_i c_i sr^{d_i}$. Therefore $Lr^d = 0$ where $d = \mathrm{ad}(t) - m_1 - \sum d_i c_i \in \mathrm{Der}(Q)$. The definition of Q gives $R^d = 0$, so $d = 0$ results from $(I_q q)^d = 0$ for any $q \in Q$. This means that $\mathrm{ad}(t) = m_1 + \sum d_i c_i$ is a derivation in $\mathrm{Der}(R)C$ which becomes inner on Q. But $\{m_1, d_i\} \subset M - M_0$, and no linear combination of these basis elements can be inner on Q, by the choice of M. This contradiction establishes what we wanted: in the case under consideration, when y appears in f with exponents less than h, one must have $\sum_i a_{hi} \otimes b_{hi} = 0$.

Finally, we return to the general case, when f has the form $\sum_{i=1}^n a_{hi} x^h b_{hi} + \sum_{j=1}^m c_{hj} y^h d_{hj} + f_1$, where all exponents appearing in f_1 are smaller than h. Now,

when $m > 0$, repeat the argument for the case $h = 1$. Specifically, if $\sum_i a_{hi} \otimes b_{hi} \neq 0$, let $r \in J$, where J is chosen so that $Jc_{h1} + c_{h1}J \subset R$, replace x with $xc_{h1}^* r^*$ and y with $rc_{h1}y$, and use (1) to obtain a G^*-DI for I, say $g = \sum_i a_{hi}x^h c_{h1}^* r^* b_{hi} + \sum_j c_{hj}rc_{h1}y^h d_{hj} + g_1$, where all exponents appearing in g_1 are less than h. Again, set $q = g - c_{h1}rf = \sum s_i x^h t_i + \sum_{j=2}^m u_j y^h v_j + q_1$ and use induction on m and Lemma 3 to conclude that $\sum a_{hi} \otimes b_{hi} = 0$. Interchanging x and y, as explained in the first paragraph of the proof, and the case $m = 0$ give $\sum c_{hj} \otimes d_{hj} = 0$. But now, by Lemma 1(iii) and induction on h, the proof of the theorem is complete.

As we stated above, we shall improve upon Theorem 1 by showing that, for each exponent h appearing in f, $\sum_i a_{hi}xb_{hi} + \sum_j c_{hj}yd_{hj}$ is a G^*-PI for R. To do this we must characterize inner derivations and determine the relation between identities satisfied by R and identities satisfied by ideals of R. Our next theorem extends, although requires, the classical result that a derivation of a finite-dimensional simple algebra is inner exactly when it annihilates the center. First we prove a lemma which clarifies some details involving the slightly more general situation which we must consider in Theorem 2.

LEMMA 6. *Let $d \in \mathrm{Der}(RC)$ so that $I^d \subset R$ for some nonzero ideal I of R. Then d extends to a derivation of Q. Furthermore, if $r^d = rf - fr$ for some $f \in Q$ and each $r \in R$, then $f \in N$ and $\mathrm{ad}(f)$ is the extension of d to Q.*

PROOF. To see that d extends to Q, use the same procedure as described earlier for $d \in \mathrm{Der}(R)$. In particular, for $g \in Q$ defined on I_g, set $J = (I \cap I_g)^2$ and define g^d from J to R by $(x)g^d = (xg)^d - (x^d)g$. Now suppose that $r^d = rf - fr$. By using the ideal $I \cap I_f$, one gets $f \in N$. Finally, for any $g \in Q$ and $J = (I \cap I_g)^2$, we have for $x \in J$ that $xg^d = (xg)^d - (x^d)g = xgf - fxg - (xf - fx)g = xgf - xfg$. It follows that $J(g^d - (gf - fg)) = 0$, and the defining properties of Q yield $d = \mathrm{ad}(f)$.

THEOREM 2. *Let R be a prime ring which satisfies a GPI. Suppose that $d \in \mathrm{Der}(RC)$ with $I^d \subset R$ for some nonzero ideal I of R. If $C^d = 0$, then the extension of d to Q is $\mathrm{ad}(a)$ for some $a \in N$.*

PROOF. By [8, Theorem 2, p. 578] RC is a primitive ring with minimal right ideal eRC, and $eRCe$ is a division ring finite dimensional over its center, eC. Now $e^d = (e^2)^d = ee^d + e^d e$, and it follows that $ee^d e = 0$. Thus, one can (formally) write $e^d = ee^d(1-e) + (1-e)e^d e$, or equivalently, $e^d = s + t$ with $es = s$, $se = 0$ $et = 0$, and $te = t$. For any $y \in RC$, $(eye)^d = e^d ye + ey^d e + eye^d = (s+t)ye + ey^d e + ey(s+t)$. If $h = \mathrm{ad}(s-t)$, the inner derivation of RC determined by $s-t$, then $(eye)^h = eys + tye$. Hence $(eye)^{d-h} = sye + ey^d e + eyt \in eRCe$, and for $y = ec$, with $c \in C$, $(ece)^{d-h} = e(ec)^d e = ee^d ec = 0$ since $C^d = 0$. Therefore, the restriction of $d - h$ to $eRCe$ is a derivation of $eRCe$ annihilating eC; so is $\mathrm{ad}(v)$ for some $v \in eRCe$. Equivalently, $w = d - h - \mathrm{ad}(v)$ is a derivation of RC satisfying $(eRCe)^w = e(RC)^w e = 0$. Note also that w satisfies the assumption on d that $J^w \subset R$ for an ideal of R, namely $J = I \cap I_s \cap I_t \cap I_v$. In addition, we may as well assume that $Je + eJ \subset R$.

For $x, y \in J$, $0 = e(xy)^w e = ex^w ye + exy^w e$. If $\{a_i, b_i\} \subset J$ with $\sum a_i eb_i = 0$, then $0 = \sum a_i eb_i y^w e = -\sum a_i eb_i^w ye$, which forces $\sum a_i eb_i^w = 0$. Thus, we can define $f \in \mathrm{Hom}(_R JeJ, R)$ via $(\sum a_i eb_i)f = \sum a_i eb_i^w$, and so, consider $f \in Q$. In this last equation, replacing each b_i by $b_i r$ for $r \in R$ yields $(\sum a_i eb_i r)f = \sum a_i eb_i^w r + \sum a_i eb_i r^w$. Subtract from this, the result of multiplying the previous

equation by r on the right to obtain $(JeJ)(rf - fr - r^w) = 0$. The properties of Q force $r^w = rf - fr$ for each $r \in R$. By Lemma 6, $f \in N$, and so $r^d = ra - ar$ with $a = s - t + v + f \in N$. Applying Lemma 6, again, yields $d = \mathrm{ad}(a)$, considered in $\mathrm{Der}(Q)$.

COROLLARY 1. *Let R be a prime ring which satisfies a GPI. Then $d \in \mathrm{Der}(R)$ is inner when extended to Q if and only if $C^d = 0$.*

We require another easy corollary of Theorem 2 when R has an involution, $*$. Recall that $*$ extends to C, and let $C_S = \{c \in C | c^* = c\}$.

COROLLARY 2. *Let R be a prime ring with involution, $*$, and satisfying a GPI. Suppose that $d \in \mathrm{Der}(RC)$ so that $I^d \subset R$ for a nonzero ideal I of R. If $(C_S)^d = 0$ then the extension of d to Q is $\mathrm{ad}(a)$ for $a \in N$.*

PROOF. For any $c \in C$, apply d to the formal identity $c^2 - (c + c^*)c + c^*c = 0$. Using $(C_S)^d = 0$ yields $2cc^d - (c + c^*)c^d = 0$, and so, $(c - c^*)c^d = 0$. Consequently, if $c \notin C_S$, $c^d = 0$, forcing $C^d = 0$. The corollary now follows from Theorem 2.

If f is a linear G*-DI for I with its exponents coming from W, as in Theorem 1, then as a consequence of Theorems 1 and 2, none of the derivations involved in f can annihilate C_S. It is by using this fact that we shall show that, for each h coming from W and appearing in f, $\sum_i a_{hi}xb_{hi} + \sum_j c_{hj}yd_{hj}$ is a G*-PI for some ideal of R. Certainly, we want to conclude that this expression is also a G*-PI for R. Our next few results show this to be the case.

LEMMA 7. *Let R be a prime ring satisfying a GPI. If $H = \mathrm{Soc}(RC)$ and $f \in N$, then $Hf + fH \subset H$.*

PROOF. From our earlier discussion, $If + fI \subset R$ for some nonzero ideal of R. Now H is the unique minimal ideal of RC, so $H \subset IC$, and it follows that $Hf + fH = H^2f + fH^2 \subset H(RC) + (RC)H \subset H$.

LEMMA 8. *Let R be a prime ring with involution, $*$, satisfying a GPI. If $C = C_S$ and $h_1, \ldots, h_n \in H = \mathrm{Soc}(RC)$, then there is $e^* = e = e^2 \in H$ so that $eh_i = h_i e = h_i$ for all i.*

PROOF. This result is just [7, Theorem 4, p. 89], observing that RC is a primitive ring with $H \neq 0$ by [8, Theorem 3, p. 579].

Using the last two lemmas we can show that any G*-PI for any ideal of R is satisfied by R as well.

THEOREM 3. *Let R be a prime ring with involution, $*$. Choose $f \in F$ of the form $f = \sum_i a_i xb_i + \sum_j c_j yd_j$. If $f(I) = 0$ for some nonzero ideal I of R, then $f(R) = 0$.*

PROOF. Note that by Theorem 1, either $f = 0$ in F, or R satisfies a nonzero GPI. We proceed with the second possibility, and so $\mathrm{Soc}(RC) \neq 0$. Assume first that $C \neq C_S$ and choose $z \in C - C_S$. There is a nonzero ideal J of R so that $J \subset I$, $J = J^*$, and $zJ \subset I$. Since for all $t \in J$, $f(zt) = 0 = zf(t) = z^*f(t)$, one obtains $\sum a_i tb_i = \sum c_j t^* d_i = 0$. It follows from Lemma 1 that $f(R) = 0$. Thus, we may now assume that $C = C_S$, and so $f(IC) = 0$. For any $s, t \in H = \mathrm{Soc}(RC)$, IC, and so H satisfies $sf(x)t = \sum sa_i xb_i t + \sum sc_j yd_j t$. Now $\{sa_i, d_j t\} \subset H$ by Lemma

7, so Lemma 8 provides an idempotent $g = g^* \in H$ which acts like an identity on all sa_i and $d_j t$. Since $gR \subset H$, for any $r \in R$ we have

$$0 = \sum sa_i grb_i t + \sum sc_j r^* g d_j t$$
$$= \sum sa_i rb_i t + \sum sc_j r^* d_j t = sf(r)t.$$

Hence $Hf(R)H = 0$ and the primeness of RC forces $f(R) = 0$.

COROLLARY. *Let R be a prime ring with involution,* *. *If*

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n) \in F$$

is multilinear and homogeneous and if $f(I^n) = 0$ for a nonzero ideal I of R, then $f(R^n) = 0$.

PROOF. Write $f = \sum p_i x_n q_i + \sum u_j y_n w_j$. Substituting elements of I for $x_1, \ldots, x_{n-1}$ results in the linear identity $\sum a_i x_n b_i + \sum c_j y_n d_j$ for I. By the theorem, this identity holds for R. Therefore, substituting $r \in R$ for x_n in f gives an identity for I of degree $n-1$, so by induction on n, $f(R^n) = 0$.

Putting together the results which have been obtained so far, we can now prove our main theorem for linear identities, which corresponds to [5, Theorem 1, p. 158].The notation is the same as that which was used in Theorem 1.

THEOREM 4. *Let R be a prime ring with involution,* *, *and let $f \in F$ be linear and have all its exponents coming from W, so that $f = \sum_h \sum_i a_{hi} x^h b_{hi} + \sum_k \sum_j c_{kj} y^k d_{kj}$ with all h and k coming from W and all coefficients in N. If for some nonzero ideal I of R, $f(I) = 0$, then for each exponent w appearing in f, $f_w(x) = \sum_i a_{wi} x b_{wi} + \sum_j c_{wj} y d_{wj}$ is a G^*-PI for R.*

PROOF. Since there is nothing further to prove if $f = 0$ in F, assume $f \neq 0$, so that R satisfies a GPI by Theorem 1. As in Theorem 1, we proceed by induction on the largest exponent appearing in f. Let h be the largest such, and suppose that $h = 1$. Then $f = f_h$, so f is a G^*-PI for R by Theorem 3. Before considering the general case, observe that if w comes from $(m_1, \ldots, m_k) \in W$ and if v comes from $(m_2, \ldots, m_k)$, then using (1) with $c \in C_S$ and $r \in I_c$ gives $(cr)^w = cr^w + qc^{m_1} r^v + \cdots + c^w r$, where the exponents of r in the unrepresented terms are smaller than w, in fact smaller than v, and q is the number of consecutive m_j equal to m_1. Note that p does not divide q when char $R = p$, by definition of W.

Given any $c \in C_S$, the ideal $J = II_c$ of R satisfies $J \subset I$ and $cJ \subset I$. Hence, for substitutions of elements of J for x, the observation above shows that $g(x) = f(cx) - cf(x)$ is a linear G^*-DI for J and each exponent appearing in g comes from an element of W smaller than h. Therefore, we can apply our inductive assumption to g. Now if h comes from $(m_1, d_2, \ldots, d_n) \in W$ and v comes from $(d_2, \ldots, d_n)$, then v appears as a coefficient in g, so by induction, taking the sum of monomials in g appearing with exponent v and replacing v with 1, gives a G^*-PI for R. To determine what this G^*-PI for R is, let $h = m_1 v$, $w_2 = m_2 v, \ldots, w_t = m_t v$ be the list of all exponents in f coming from elements $(m_i, d_2, \ldots, d_n) \in W$, arranged so $m_1 > m_2 > \cdots > m_t$. Then (1) and the definition of g show that the G^*-PI arising by induction from the exponent v is $qc^{m_1} f_h(x) + c^{m_2} f_{w_2}(x) + \cdots + c^{m_t} f_{w_t}(x)$.

Clearly, to finish to proof, suffices to show that $f_h(x)$ is a G*-PI for R, and this follows if there exist $c_1, \ldots, c_t \in C_S$ so that the matrix $((c_i)^{m_j})$ is invertible.

If $((c_i)^{m_j})$ is singular for all choices of c_i, choose k minimal so that $d_1, \ldots, d_k \in M - M_0$ has this same property. For any $c = c_1 \in C_S$ and fixed $c_2, \ldots, c_k \in C_S$, the cofactor expansion of the determinant of $((c_i)^{d_j})$ along the first row gives $c^{d_1} z_1 + \cdots + c^{d_k} z_k = 0$ where some $z_i \neq 0$ for a suitable choice of $c_2, \ldots, c_k \in C_S$ because of the minimality of k. Thus $d = \sum d_i z_i \in \mathrm{Der}(RC)$, $(C_S)^d = 0$, and $(J^3)^d \subset R$ where J is the intersection of all I_{z_i} and I_{t_j} for $t_j \in C$ which are needed to write $d_i \in \mathrm{Der}(R)C$. By Corollary 2 of Theorem 2, the extension of d to Q is an inner derivation, contradicting the choice of $d_i \in M - M_0$. Thus $((c_i)^{m_j})$ must be invertible for some choice of $c_1, \ldots, c_t \in C_S$, completing the proof of the theorem.

In [5], Kharchenko uses his result on linear differential identities to obtain results about algebraic derivations. Using Theorem 4 we can obtain similar results about derivations which are algebraic when restricted to the symmetric or skew-symmetric elements in an ideal of R. First we mention a consequence of our results which has nothing to do with involutions, but uses our generalization of Kharchenko's work to ideals. In our work so far, the assumption of an involution has been necessary only to evaluate elements of F containing indeterminates from Y^V. If one considers only $f \in N *_C C\{X^V\} \subset F$ which are G*-DIs for I, then all of our results hold for R without involution, so in particular, Theorem 4 does give a generalization to ideals of [5, Lemma 2, p. 158]. This observation enables us to generalize [5, Corollary 2, p. 160 and Corollary 3, p. 161] to ideals.

THEOREM 5. *Let R be a prime ring and I a nonzero ideal of R. Suppose that $d \in \mathrm{Der}(R)$ and $f(x) = x^n + x^{n-1} c_{n-1} + \cdots + x c_1 \in C[x]$ so that $I^{f(d)} = 0$. Then d is algebraic over C and*

(i) *if char $R = 0$, the extension of d to Q is inner and given by $\mathrm{ad}(a)$ for $a \in N$ and algebraic over C; and*

(ii) *if char $R = p > 0$, then $\sum_{i=0}^m d^{p^i} z_i = \mathrm{ad}(a)$, where $z_i \in C$ and $a \in N - C$ and algebraic over C.*

PROOF. Assume first that char $R = 0$ and that the extension of d to Q is not inner. There is a basis M of $\mathrm{Der}(R)C$, as described before Lemma 5, so that $d \in M - M_0$. Since $I^{f(d)} = 0$, $x^{f(d)}$ is a linear G*-DI for I, and as in the proof of Lemma 5, by using elements of types (III) and (VI) in $U(R)$, we may conclude that $x^{d^n} + \cdots + x^d c_1 \in x^{f(d)} + U(R)$ is a linear G*-DI for I, all of whose exponents come from W. Applying Theorem 4 shows that x is a G*-PI for R. But $R \neq 0$, so this contradiction forces the extension of d to Q to be $\mathrm{ad}(a)$ for $a \in N$ when char $R = 0$. Thus, if $t \in I$, $t^d = ta - at$, and it follows that $0 = t^{f(d)} = \sum_{i=0}^n a^i t p_i(a)$, where $p_i(a) \in C[a]$. Hence, Lemma 1 yields the facts that a is algebraic over C, and that $R^{f(d)} = 0$, or equivalently, that d is algebraic over C.

Now assume that char $R = p > 0$ and that no polynomial $\sum d^{p^i} z_i$ is an inner derivation of Q. As in the case above, one can choose a basis of $\mathrm{Der}(R)C$ so that $v_0 = d$ and all $v_i = d^{p^i}$ are distinct elements in $M - M_0$; and one can arrange the ordering on M so $v_i < v_j$ if $i < j$. For any positive integer j, one may use the representation of j as a sum of powers of p to write $d^j = v_0^{a_0} v_1^{a_1} \cdots v_k^{a_k}$, where the tuple of integers $(a_0, \ldots, a_k)$ is unique with respect to the conditions $0 \leq a_i < p$, $v_i^0 = 1$, and $a_k \neq 0$. These representations allow us to assume that

the powers of d come from distinct elements of W. Arguing exactly as in the case char $R = 0$, it follows from the assumption that $I^{f(d)} = 0$ that $R = 0$. This contradiction forces the conclusion that for suitable i and z_i, $\sum d^{p^i} z_i = \text{ad}(a)$, with $a \in N - C$. To see that a and d must be algebraic over C, consider the subring L of $\text{End}(N, +)$ generated by d and all right multiplications by elements of C, denoted C_R. Although L is not a commutative ring, by using $c_R d = d c_R + (c^d)_R$, for all $c_R \in C_R$, one recognizes that L consists of (right) polynomials in d over $C_R \cong C$. The assumption $I^{f(d)} = 0$ means that the restriction of L to I is a finite-dimensional right C_R-module. In particular, $\text{ad}(a)$ restricted to I is algebraic over C. But now, the argument at the end of the char $R = 0$ case, using Lemma 1, shows that a and d are algebraic over C.

We turn now to the *-version of Kharchenko's results on algebraic derivations. For any ideal I of R, let $T(I) = \{r + r^* | r \in I\}$ and $K(I) = \{r - r^* | r \in I\}$. Clearly, $T(I)$ and $K(I)$ are sets of symmetric and skew-symmetric elements of R, respectively, and when char $R = 2$, $T = K$. It is easy to see that if $K(I) = 0$ then * is the identity map on R and R is commutative; and if char $R \neq 2$ then $T \neq 0$.

THEOREM 6. *Let R be a prime ring with involution* *, so that* * *is not the identity map on R, let I be a nonzero ideal of R, and let $d \in \text{Der}(R)$ and $f(x) = x^n + x^{n-1} c_{n-1} + \cdots + x c_1 \in C[x]$ so that either $T(I)^{f(d)} = 0$ or $K(I)^{f(d)} = 0$. Then if char $R = 0$, the extension of d to Q is inner; and, if char $R = p > 0$, then $\sum_{i=0}^m d^{p^i} z_i = \text{ad}(a)$, where $z_i \in C$, $a \in N - C$, a is algebraic over C, and d is algebraic over C.*

PROOF. The proof is essentially the same as the proof of Theorem 5. As in that proof, when char $R = 0$, assuming that the extension of d to Q is not inner allows us to take $d \in M - M_0$. If $T(I)^{f(d)} = 0$, then $x^{f(d)} + y^{f(d)}$ is a linear G*-DI for I, and as in Lemma 5, $x^{d^n} + \cdots + x^d c_1 + y^{d^n} + \cdots + y^d c_1 \in x^{f(d)} + y^{f(d)} + U(R)$ is a linear G*-DI for I with exponents coming from W. Thus, Theorem 4 implies that $x + y$ is a G*-PI for R. Similarly, assuming that $K(I)^{f(d)} = 0$ leads to the conclusion that $x - y$ is a G*-PI for R. Since neither $T(R) = 0$, nor $K(R) = 0$, this contradiction shows that the extension of d to Q must be inner.

When char $R = p > 0$, by assuming that no $\sum d^{p^i} z_i$ is inner on Q, one gets that each d^j can be represented as a product coming from W, as in the proof of Theorem 5. Proceeding as in the paragraph above, one obtains the contradiction $T(I) = 0$, or $K(I) = 0$. Consequently, some $\sum d^{p^i} z_i = \text{ad}(a) \neq 0$, when acting on either $T(I)$ or $K(I)$. Again as in Theorem 5, the subring L of $\text{End}(N, +)$ generated by d and C_R, the right multiplications by elements in C when restricted to $T(I)$ or to $K(I)$, is a finite-dimensional right C_R module. In particular, if $h = \text{ad}(a)$, then $\{h, h^p, \ldots, h^{p^i}, \ldots\}$ is right C_R-dependent when acting on $T(I)$, or $K(I)$. For specificity say $T(I)^{g(h)} = 0$, or $K(I)^{g(h)} = 0$, for $g(h) = \sum h^{p^j} z_j \neq 0$. Since char $R = p$, $g(h) \in \text{Der}(N)$, so $T(I)^{g(h)} = 0$ forces $(\overline{T}(I))^{g(h)} = 0$ where $\overline{T}(I)$ is the subring of R generated by $T(I)$, and similarly, $K(I)^{g(h)} = 0$ forces $(\overline{K}(I))^{g(h)} = 0$. It is well known that $\overline{T}(II^*)$ contains a nonzero ideal of II^*, and so, a nonzero ideal of R, unless RC is at most four dimensional over C. The same conclusion is well known for $\overline{K}(II^*)$. Thus both $\overline{T}(I)$ and $\overline{K}(I)$ contain a nonzero ideal J of R, unless RC is finite dimensional over C. But if $J^{g(h)} = 0$, then a and h are algebraic over C, as in the proof of Theorem 5, and it is immediate that d is algebraic over

C. On the other hand, if RC is finite dimensional over C, then $RC = Q$, so a is certainly algebraic over C. Again, it follows that h, and so d, is algebraic over C.

Note that in the case char $R = 0$ in Theorem 6, we did not conclude that a derivation which is inner on Q and algebraic over C when acting on $T(I)$, or $K(I)$, is an algebraic derivation. It seems likely that this must be true but we cannot prove it at this time.

Next we obtain a multilinear version of Theorem 4. Let $f \in F$ be multilinear and homogeneous of degree n, with exponents coming from W, and for simplicity assume that each variable appearing in f has subscript in the set $\{1, 2, \ldots, n\}$. Any monomial in f contains exactly one of x_i or y_i to some exponent, say w_i, and so gives rise to an n-tuple $(w_1, \ldots, w_n)$. We recall once again that exponents are regarded as different if they come from different elements of W. Let $W(f)$ denote the set of all such distinct n-tuples. Of course, many monomials in f may give rise to the same $\overline{w} \in W(f)$. For example, when $n = 2$, $x_1^m y_2 + y_1^m x_2 - y_1^m y_2 + x_2 x_1^m - y_2 x_1^m = g$ satisfies $W(g) = \{(m, 1)\}$ where $m \in M - M_0$.

THEOREM 7. *Let R be a prime ring with involution, $*$, and $f \in F$ be multilinear and homogeneous of degree n with all exponents coming from W and all subscripts of variables in $\{1, 2, \ldots, n\}$. For*

$$\overline{w} = (w_1, \ldots, w_n) \in W(f),$$

let $f_{\overline{w}}(x_1^{w_1}, \ldots, x_n^{w_n}, y_1^{w_1}, \ldots, y_n^{w_n})$ denote the sum of all monomials in f in which x_i, or y_i, appears with exponent w_i. If f is a G^*-DI for I, a nonzero ideal of R, then each $f_{\overline{w}}(x_1, \ldots, x_n, y_1, \ldots, y_n)$ is a G^*-PI for R, and R satisfies a GPI, unless $f = 0$ in F.

PROOF. Assume throughout that $f \neq 0$ in F. The proof proceeds by induction on the number of variables which appear with nonidentity exponent. If this number is zero, then $W(f) = \{(1, \ldots, 1)\}$, so $f = f_{\overline{w}}$ is a G^*-PI for I. By the corollary to Theorem 3, f is a G^*-PI for R. Represent f as $\sum_i p_i x_n q_i + \sum_j u_j y_n v_j$ and substitute arbitrary elements from I for $x_1, \ldots, x_{n-1}$ to obtain the linear G^*-PI $\sum a_i x_n b_i + \sum c_j y_n d_j$. By Theorem 1, either R satisfies a GPI or both $\sum a_i x_n b_i$ and $\sum c_j y_n d_j$ are zero in F. In the latter case, it follows that both $\sum p_i x_n q_i$ and $\sum u_j y_n v_j$ give zero when $x_1, \ldots, x_{n-1}$ are chosen from I and $x_n \in R$. If R does not satisfy a GPI, then repeating the argument for the other variables in turn shows that the sum of all monomials of f containing a fixed choice of x_i or y_i, for each i, is a G^*-PI for R. Therefore, R must satisfy a GPI by the Proposition.

The general case is a repetition of the argument given above. Let x_i or y_i appear in f with nonidentity exponent w_i, write $f = \sum_h \sum_j p_{hj} x_i^h q_{hj} + \sum_k \sum_t u_{kt} y_i^k v_{kt}$, and substitute elements of I for the variables with subscripts other than i to obtain the linear G^*-DI $\sum_{h,j} a_{hj} x_i^h b_{hj} + \sum_{k,t} c_{kt} y_i^k d_{kt}$. As above, one can conclude that R satisfies a GPI by using Theorem 1 and induction on the number of variables appearing with nonempty exponent. Also, for $h = w_i$, Theorem 4 shows that $\sum_j p_{hj} x_i q_{hj} + \sum_t u_{ht} y_i v_{ht}$ is a G^*-DI for I. But now applying our induction assumption gives the proof of the theorem.

Our next result gives an affirmative answer to a question of Kovacs [6], extended to rings with involution. We want to consider elements $f \in F$ having all coefficients in C, or equivalently, those f in the subring $C\{X^V, Y^V\}$ of F.

Any $f \in C\{X^V, Y^V\}$ having all exponents in $(\mathrm{Der}(R) - \{0\}) \cup \{1\}$, of the form $f = f(x_1^{d_1}, \ldots, x_n^{d_n}, y_1^{h_1}, \ldots, y_n^{h_n})$, and satisfying $f(I^n) = 0$ for a nonzero ideal I of R, will be called a polynomial *-differential identity (P*-DI) for I. Thus, every occurrence of x_i or y_i in f carries a fixed exponent in $\mathrm{Der}(R) \cup \{1\}$. Clearly, any nonzero P*-DI for I can be linearized to obtain a nonzero multilinear and homogeneous P*-DI for I, so we may restrict our attention to this case.

THEOREM 8. *Let R be a prime ring with involution, $*$. If p is a nonzero multilinear and homogeneous P*-DI for I, a nonzero ideal of R, then $p \notin U(R)$ and R satisfies a nonzero GPI.*

PROOF. The conclusion follows from Lemma 5 and Theorem 7 if $p \notin U(R)$. If $p = p(x_1^{h_1}, \ldots, x_n^{h_n}, y_1^{k_1}, \ldots, y_n^{k_n})$, there is no loss of generality in assuming that p contains a monomial $\overline{p} = t_1^{d_1} \cdots t_n^{d_n}$, where t_i is either x_i or y_i, and d_i is the corresponding h_i or k_i. As defined earlier, $(t_1, \ldots, t_n)$ is called the variable sequence of $\overline{p}$. Note that p cannot contain two monomials having the same variable sequence, by definition of a P*-DI. Let us say that $f \in F$ has a variable sequence if each of its monomials has the same variable sequence. Then it is clear from the definition of $U(R)$ that $U(R)$ has a C-basis consisting of elements each of which has a variable sequence. The span of all basis elements having the same variable sequence is a C-subspace of $U(R)$, and these subspaces give a direct sum decomposition for $U(R)$. It follows that if $f \in U(R)$, then the sum of all monomials in f having any fixed variable sequence is also in $U(R)$. In particular, if $p \in U(R)$, then $\overline{p} \in U(R)$, and so $\overline{p}$ is a G*-DI for R. Now $\overline{p}$ has exactly one occurance of x_i or y_i, so $R^{d_1} R^{d_2} \cdots R^{d_n} = 0$ results. The primeness of R implies that R^{d_i} has no left or right annihilator in R, and the definition of P*-DI requires $d_i \neq 0$, so we are forced to conclude that $p \in U(R)$ is impossible. Therefore, $p \notin U(R)$, completing the proof of the theorem.

Theorem 8 shows that a nonzero P*-DI p cannot be a trivial identity. If the exponents of p were independent outer derivations of Q, then Theorem 7 would show that p is the sum of P*-DIs, each of which is obtained from G*-PI by substitutions of the form x^d. We would like the same conclusion for any allowable exponents, and this is the content of our last theorem. Recall that M is a C-basis of $\mathrm{Der}(R)C$ so that $M_0 \subset M$ spans the space of derivations which are inner on Q.

THEOREM 9. *Let R be a prime ring with involution, $*$, and*
$$p = p(x_1^{h_1}, \ldots, x_n^{h_n}, y_1^{k_1}, \ldots, y_n^{k_n}),$$
a nonzero multilinear and homogeneous P-DI for a nonzero ideal I of R. Assume that for each i, if one of h_i or k_i is inner on Q, then the other is either inner on Q also, or is in $\mathrm{Span}(M - M_0)$. Then R satisfies the nonzero G*-PI obtained from p by the following: replacing $x_i^{h_i}$ with $x_i a_i - a_i x_i$ if $h_i = \mathrm{ad}(a_i)$ on Q; replacing $y_j^{k_j}$ with $y_j b_j - b_j y_j$ if $k_j = \mathrm{ad}(b_j)$ on Q; and replacing every other $x_i^{h_i}$ with x_i and $y_j^{k_j}$ with y_j.*

PROOF. Suppose that for some i, $h_i = \mathrm{ad}(a_i)$ on Q. By using $x_i^{h_i} - x_i a_i + a_i x_i \in U(R)$, the substitution of $x_i a_i - a_i x_i$ for $x_i^{h_i}$ in p gives a nonzero G*-DI for I which is congruent modulo $U(R)$ to p, and in which x_i appears without exponent. Make a similar substitution for each h_i and k_j which is inner on Q to obtain a G*-DI

f for I which is congruent modulo $U(R)$ to p and having no exponent which is inner on Q. If f has no variable appearing with exponent in $\mathrm{Der}(R)C$, then f is the G^*-PI described in the theorem. Otherwise, we may write the remaining exponents as linear combinations of the elements of M, and in each case one must use elements from $M - M_0$. Specifically, if h_i appears in f, let $h_i = \sum m_{ij1}c_{ij1}$, and if k_i appears in f, let $k_i = \sum m_{ij2}c_{ij2}$. It is clear that by using elements of types (III) and (VI) in $U(R)$, replacing $x_i^{h_i}$ with $\sum x_i^{m_{ij1}}c_{ij1}$ in f gives a G^*-DI for I which is congruent modulo $U(R)$, to f, and so, to p. Making similar substitutions for the other exponents appearing in f gives a G^*-DI for I, congruent modulo U to p and having all exponents in $\{m_{ij1}, m_{ij2}\}$. Finally, as in the beginning of the proof, we may replace each $x_i^{m_{ij1}}$ and $y_i^{m_{ij2}}$ with a suitable $x_i a - a x_i$ or $y_i b - b y_i$ if its exponent is in M_0. Thus we obtain a G^*-DI for I, say g, congruent modulo $U(R)$ to p and having all exponents in $B = \{m_{ij1}, m_{ij2}\} \cap (M - M_0)$. In particular, the exponents of g come from W and $g \notin U(R)$, so we may apply Theorem 7: for any n-tuple $\overline{w} = (d_1, \ldots, d_n) \in (B \cup \{1\})^n$, $g_{\overline{w}}(x_1, \ldots, x_n, y_1, \ldots, y_n)$ is a G^*-PI for R. To complete the proof, we must find a suitable subset $\{\overline{w}_k\} \subset (B \cup \{1\})^n$ so that $\sum g_{\overline{w}_k}$ is the G^*-PI described in the theorem.

Let us go back to those h_i and k_j which are not inner on Q, and so are the exponents of f. Fix i, and suppose first that h_i appears in f but k_i does not. By assumption, $\{m_{ij1}\} \subset M - M_0$ and set $v_i = m_{ij1}$ for any of the m_{ij1}. If k_i appears in f but h_i does not, let $v_i = m_{ij2}$ for any of the $\{m_{ij2}\} \subset M - M_0$. Next suppose that both h_i and k_i appear in f. Set $v_i = m_{ij1} \in \{m_{ij1}\} \cap \{m_{ij2}\}$ if such a choice is possible. If for i, $\{m_{ij1}\}$ and $\{m_{ij2}\}$ are disjoint, let $v_{i1} \in \{m_{ij1}\} \subset (M - M_0)$ and $v_{i2} \in \{m_{ij2}\} \subset (M - M_0)$. Now we can describe the $\{\overline{w}_k\} \subset (B \cup \{1\})^n$ that we require. Consider all $\overline{w} = (d_1, \ldots, d_n) \in (B \cup \{1\})^n$ satisfying the following: for each i, d_i must be 1 if neither h_i nor k_i appear in f; d_i must be v_i if both h_i and k_i appear in f and $v_i \in \{m_{ij1}\} \cap \{m_{ij2}\}$; d_i is either v_{i1} or v_{i2} if both h_i and k_i appear in f but $\{m_{ij1}\}$ and $\{m_{ij2}\}$ are disjoint; and d_i is either v_i or 1 if exactly one of h_i or k_i appears in f. If the set of all such n-tuples is $\{\overline{w}_k\}$, then the choices of the v_i, or v_{i1} and v_{i2}, insure that each monomial in the G^*-PI described in the theorem appears in exactly one of the $g_{\overline{w}_k}(x_1, \ldots, y_n)$. In this regard, it is important to note that if $d_i = 1$ in $\overline{w}_k$, then either both h_i and k_i are inner on Q and x_i and y_i occur in $g_{\overline{w}_k}$ if both occurred in p, or exactly one is inner on Q, say k_i, in which case x_i cannot occur in $g_{\overline{w}_k}$ by our assumption on the pair h_i and k_i. Similarly, if d_i is a v_* then $g_{\overline{w}_k}$ contains the occurances of both x_i and y_i, or just one of these and not the other. It follows that $\sum g_{\overline{w}_k}(x_1, \ldots, y_n)$ is the G^*-PI obtained from p by the substitutions described in the statement of the theorem.

A case of Theorem 9 of particular interest is when $h_i = k_i$ for each i. The hypothesis of Theorem 9 is certainly satisfied, and the proof of Theorem 9 is very much simplified because the resulting G^*-PI is just $g_{\overline{w}}(x_1, \ldots, y_n)$ where $\overline{w} = (d_1, \ldots, d_n)$ is defined by $d_i = 1$ if h_i is inner on Q, and $d_i = v_i$ otherwise. We state this result as

COROLLARY 1. *Let R and p be as in Theorem 9 and*

$$p = p(x_1^{d_1}, \ldots, x_n^{d_n}, y_1^{d_1}, \ldots, y_n^{d_n}).$$

Then R satisfies the nonzero G^*-PI obtained from p by replacing $x_i^{d_i}$ with $x_i a_i - a_i x_i$ and $y_i^{d_i}$ with $y_i a_i - a_i y_i$ when $d_i = \mathrm{ad}(a_i)$ on Q, and for all other j, replacing $x_j^{d_j}$ with x_j and $y_j^{d_j}$ with y_j.

By considering $p \in C\{X^V\}$ in Theorem 9 and using the comments before Theorem 5, one obtains an affirmative answer to the question of Kovacs [**6**]. Indeed, the corollary shows that if R satisfies such an identity, then R must satisfy a polynomial identity unless some d_i is inner on Q.

Our next corollary relates more closely what we have done so far to Herstein's result [**4**] mentioned above. Recall that $T(I) = \{r+r^*|r \in I\}$ and $K(I) = \{r-r^*|r \in I\}$ for I an ideal of R.

COROLLARY 2. *Let R be a prime ring with involution, $*$, I a nonzero ideal of R, and $p(x_1,\ldots,x_n)$ a nonzero multilinear polynomial over C in noncommuting indeterminates $\{x_i\}$. Choose $\{d_1,\ldots,d_n\} \in \mathrm{Der}(R) \cup \{1\}$ and suppose that $p(h_1^{d_1},\ldots,h_n^{d_n}) = 0$ for all choices of $h_i \in H$, where H is either $T(I)$ or $K(I)$ and $H \neq 0$. Then R satisfies a GPI and also satisfies the G^*-PI obtained from p by replacing x_j with $(x_j \pm y_j)a - a(x_j \pm y_j)$ if $d_j = \mathrm{ad}(a)$ on Q, and replacing all the other x_i with $x_i \pm y_i$ where the sign depends on whether H is $T(I)$ or $K(I)$.*

PROOF. In p, replace all x_i with $x_i^{d_i} + y_i^{d_i}$ if $H = T(I)$ and with $x_i^{d_i} - y_i^{d_i}$ if $H = K(I)$. The resulting expression is a nonzero P*-DI for I, so the corollary is an immediate consequence of Corollary 1 and Theorem 8.

Consider the special case of the last corollary when all $d_i = d \in \mathrm{Der}(R)$. Then R satisfies a GPI and if d does not extend to an inner derivation of Q, then $p(h_1,\ldots,h_n) = 0$. It follows from a theorem of Amitsur [**3**, Lemma 5.1.5, p. 195] that R satisfies the standard identity S_{2n}. When d is inner on Q, it seems difficult to obtain additional information by direct calculation, even when $p = x_1 x_2 - x_2 x_1$. Of course, for this polynomial Herstein's result shows that R must satisfy S_4. A question which arises is whether, for any n and p, R must satisfy S_{2n}. Our final example shows this is not the case, even for $n = 2$.

EXAMPLE 3. Let R be as in Example 2; that is, the subring of countable-by-countable matrices over C having only finitely many nonzero entries, with the extended symplectic involution. Assume $\mathrm{char}\, C \neq 2$, let $\{e_{ij}\}$ denote the usual matrix units, and set $E_i = e_{ii}$. Since $\mathrm{char}\, R \neq 2$, $T = S = \{r \in R|r^* = r\}$, and it is easy to verify that $E_1 s E_2 = E_2 s E_1 = 0$ for $s \in S$. If $d = \mathrm{ad}(e_{12})$, then using $(e_{12})^2 = 0$ and the fact that $st + ts \in S$ if $s,t \in S$, give both $s^d t^d + t^d s^d = 0$ and $s^d t^d v^d = 0$ for $s,t,v \in S$. Thus R may satisfy no polynomial identity although T^d satisfies either $x_1 x_2 + x_2 x_1$ or $x_1 x_2 x_3 \cdots x_n$ for $n > 2$. These same identities hold if R is replaced with N, in this case the subring of matrices which are row finite and column finite, and if e_{12} is replaced by $a = \sum e_{2n-1\, 2n}$, the sum taken over all $n \geq 1$. In this case, once again $a^2 = 0$, and for $s \in S$, $E_{2n} s E_{2k-1} + E_{2k} s E_{2n-1} = 0$ so that $asa = 0$.

REFERENCES

1. S. A. Amitsur, *Generalized polynomial identities and pivotal monomials*, Trans. Amer. Math. Soc. **114** (1965), 210–226.
2. T. S. Erickson, W. S. Martindale III and J. M. Osborn, *Prime nonassociative algebras*, Pacific J. Math. **60** (1975), 49–63.

3. I. N. Herstein, *Rings with involution*, Univ. of Chicago Press, Chicago, 1976.

4. ____ , *A theorem on derivations of prime rings with involution*, Canad. J. Math. **34** (1982), 356–369.

5. V. K. Kharchenko, *Differential identities of prime rings*, Algebra and Logic **17** (1978), 155–168.

6. A. Kovacs, *On derivations in prime rings and a question of Herstein*, Canad. Math. Bull. **22** (1979), 339–344.

7. C. Lanski, *Invariant submodules in semi-prime rings with involution*, Comm. Algebra **6** (1978), 75–96.

8. W. S. Martindale III, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12** (1969), 574–584.

9. ____ , *Prime rings with involution and generalized polynomial identities*, J. Algebra **22** (1972), 502–516.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SOUTHERN CALIFORNIA, LOS ANGELES, CALIFORNIA 90089-1113