Can. J. Math., Vol. XXXIV, No. 2, 1982, pp. 356–369

A THEOREM ON DERIVATIONS OF PRIME RINGS WITH INVOLUTION

I. N. HERSTEIN

In a recent note [**2**] we showed that if R is a prime ring and $d \neq 0$ a derivation of R such that $d(x)d(y) = d(y)d(x)$ for all $x, y \in R$ then, if R is not a characteristic 2, R must be commutative. (If char $R = 2$ we showed that R must be an order in a 4-dimensional simple algebra.)

In this paper we shall consider a similar problem, namely, that of a prime ring R with involution $*$ where $d(x)d(y) = d(y)d(x)$ not for all $x, y \in R$ but merely for symmetric elements $x^* = x$ and $y^* = y$. Although it is clear that some results can be obtained if R is of characteristic 2, we shall only be concerned with the case char $R \neq 2$. Even in this case one cannot hope to extend the result cited in the first paragraph, that is, to show that R is commutative. For instance, in the ring $R = F_2$ of 2×2 matrices over a field, if $*$ is the symplectic involution, all symmetric elements are central, so the property $d(x)d(y) = d(y)d(x)$ holds trivially for symmetric elements x and y. On the other hand, if $*$ on the same ring R is transpose, then if $d(x) = xe_{11} - e_{11}x$ where $e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, it is immediate that for symmetric elements x and y, $d(x)d(y) = d(y)d(x)$.

So, at best, we could merely hope to show that a prime ring with involution which has such a derivation is somehow related to 2×2 matrices or, more generally, to 4-dimensional simple algebras. What we shall prove here is that this is indeed the case, that any such prime ring is an order in a 4-dimensional simple algebra, if it is not commutative.

We begin with a simple remark in general ring theory.

LEMMA 1. *Let R be a ring having no nilpotent ideals and suppose that $L \neq 0$ is a left ideal of R such that Ra is a minimal left ideal of R for every $a \neq 0$ in L. Then L itself is a minimal left ideal of R.*

Proof. As is easy and well-known, if $a \neq 0 \in L$, since Ra is a minimal left ideal of R and R has no nilpotent ideals, $Ra = Re$ where $e^2 = e \neq 0 \in L$. If $x = xe$ for all $x \in L$ then $L = Re$ so L is indeed a minimal left ideal of R. So, suppose that for some $x \in L$, $b = x - xe \neq 0$; clearly $be = 0$. By assumption, Rb is a minimal left ideal of R, hence $Rb = Rf$ where $f^2 = f \neq 0 \in L$, and, since $be = 0$, $fe = 0$. Consider $R(e + f)$;

Received July 16, 1980 and in revised form September 28, 1981. This research was supported by the NSF grant NSG-MCS-810-2472 at the University of Chicago.

again by our assumption we have that $R(e+f) = Rg$ where $g^2 = g \in L$. Thus $(e+f)g = e+f$; if we multiply this relation from the left by f and use $fe = 0, f^2 = f$, we get $fg = f$. Therefore $(e+f)g = e+f$ also gives us $eg = e$. Thus, $Rg \supset Re$ and $Rg \supset Rf$ and since $Re \neq Rf$, Rg cannot be a minimal left ideal of R. So this second alternative, $x \neq xe$ for $x \in L$, cannot arise and we see that L is a minimal left ideal of R.

Let R be a ring with involution * and let

$$S = \{s \in R \mid s^* = s\} \quad \text{and} \quad K = \{k \in R \mid k^* = -k\}.$$

We prove a result which is well-known and can be found in a variety of places. For completeness we give a proof of it here.

LEMMA 2. *Let R have no nilpotent ideals and be 2-torsion free. If $a \in S$ is such that $aSa = 0$ then $a = 0$.*

Proof. Given $x \in R$ then $2x = s + k$ where $s = x + x^* \in S$ and $k = x - x^* \in K$. By assumption, $asa = 0$. Also, since $a \in S$, $kak \in S$ hence $a(kak)a = 0$. But this then gives us that

$$a(2x)a(2x)a = 0,$$

hence $4axaxa = 0$ and so, since R is 2-torsion free, $axaxa = 0$ for all $x \in R$. Thus aR is a right ideal of R in which the cube of every element is 0; by a result of Levitzki [3] this cannot happen in a ring with no nilpotent ideals unless $a = 0$. This proves the lemma.

In the rest of the paper R will be a prime ring, of characteristic not 2, with involution *, and S its set of symmetric elements. We shall use throughout some notions and theorems of Martindale, which can be found in [4] pages 20–31.

Let C be the extended centroid of R and let $Q = RC$ be the central closure of R. The * of R can be extended to Q; we denote this involution on Q also by *.

LEMMA 3. *If $a \neq 0$, $b \neq 0$ are in R and $aSb = 0$ then Qb is a minimal left ideal of Q, $Qb = Qe$ where $e^2 = e$, and $eQe = Ce$. Also $b^*Sb = aSa^* = 0$, $a^*a = 0$ and $bb^* = 0$.*

Proof. If $s^* = s$ where $s \in R$ then $asb = 0$. In particular, if $x \in R$ then $a(x + x^*)b = 0$, hence $axb = -ax^*b$. Thus for $x, y \in R$,

$$(1) \quad ay^*b^*xb = -ax^*byb = axbyb = -ay^*b^*x^*b,$$

so if $x^* = x$, (1) reduces to $aRb^*Sb = 0$. Since R is prime, $b^*Sb = 0$. Similarly, $aSa^* = 0$. Thus $a^*aSa^*a = 0$. From Lemma 2, we have that $a^*a = 0$.

Replacing x^* by x in (1) we have that

$$axbyb = ay^*b^*xb \quad \text{for all } x \in R.$$

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

Since $a \neq 0$, $b \neq 0$, by a result of Martindale [**4**], $byb = \alpha(y)b$ where $\alpha(y) \in C$, for all $y \in R$, and so, trivially, for all $y \in Q$. Hence Qb is a minimal left ideal of Q. If $Qb = Qe$, $e^2 = e$, from $bQb = Cb$ we get $eQe = Ce$.

We proceed to a general result about prime rings with involution.

LEMMA 4. *Let R be a prime ring, with involution, which is its own central closure. If $a \neq 0 \in R$ is such that aSa is finite-dimensional over C, the extended centroid of R, then R is a primitive ring with minimal right ideal.*

Proof. If $x \in R$ then $a(x + x^*)a \in V = aSa$, which is finite-dimensional over C. Thus $axa = v - ax^*a$, where $v \in V$. If $y \in R$ then

$$a(xa^*y)a = v_1 - ay^*ax^*a = v_1 - (v_2 - aya)x^*a$$
$$= v_1 - v_2ax^*a + ayax^*a,$$

where $v_1, v_2 \in V$. Fix x and let y vary over R. Thus

$$axa^*ya - ayax^*a \in V + Vax^*a,$$

which is finite-dimensional over C. If axa^* and a are linearly independent over C for some $x \in R$, then, by Lemma 1.3.3 of [**4**], R has a minimal right ideal (and so must be primitive, since it is prime). On the other hand, if $axa^* = \lambda(x)a$, where $\lambda(x) \in C$, for every $x \in R$, then by a result of Martindale [**4**] R has a minimal right ideal. Thus the lemma is proved.

We now bring a derivation $d \neq 0$ of R into play. We repeat that R will be a prime ring, with involution, of characteristic not 2.

LEMMA 5. *If $d(S) = 0$ then $S \subset Z$, the center of R, then R is commutative or is an order in a 4-dimensional simple algebra.*

Proof. If $x \in R$ then $d(x + x^*) = 0$, that is, $d(x) = -d(x^*)$. Replace x in this last relation by sx, where $s \in S$. We get, since $d(S) = 0$, that

$$sd(x) = d(sx) = -d(x^*s) = -d(x^*)s = d(x)s.$$

Thus s centralizes $d(R)$. By the main result of [**5**], $S \subset Z$ follows. By Theorem 2.1.5 of [**4**] we get that R is commutative or an order in a 4-dimensional simple algebra.

We extend the result a little in the

COROLLARY. *If $d(S) \subset Z$ then $S \subset Z$ (and so R is commutative or an order in a 4-dimensional simple algebra).*

Proof. Let $s \in S$; then $sd(s) + d(s)s = d(s^2)$ is in Z, and, since $d(s) \in Z$, we get that $2sd(s) \in Z$. If $d(s) \neq 0$, since char $R \neq 2$, we get $s \in Z$; that is, $d(s) \neq 0$ forces $s \in Z$. If $d(S) = 0$, we are done by Lemma 5. If $d(t) \neq 0$ for $t \in S$, we just saw that $t \in Z$. Suppose $d(s) = 0$; then

$d(t + s) \neq 0$, hence $t + s \in Z$. But $t \in Z$; the net result of this is that $s \in Z$. Thus we indeed have that $S \subset Z$.

We come to a result which will play an important role in all that follows. This is

THEOREM 1. *Let R be a prime ring with involution which is not commutative nor an order in a 4-dimensional simple algebra, and let $d \neq 0$ be a derivation of R. Suppose that $I = I^* \neq 0$ is an ideal of R; let*

$$L = \{x \in I | xd(S \cap I) = 0\}.$$

Then, if $L \neq 0$, given $a \in L$ we must have $a^*(S \cap I)a = 0$. In particular, if R is its own central closure, and if $L \neq 0$, then L must be a minimal left ideal of R, hence R is primitive. If $L = Re$, where $e^2 = e$, then $eRe = Ce$, where C is the extended centroid of R.

Proof. Let $S_0 = S \cap I$. By assumption, $ad(x) = -ad(x^*)$ for $x \in I$, $a \in L$. Suppose that $L \neq 0$ and that $a \neq 0 \in L$. If $s \in S_0$ and $x \in I$ then, since $ad(s) = 0$,

$$asd(x) = ad(sx) = -ad(x^*s) = -ad(x^*)s - ax^*d(s)$$
$$= ad(x)s - ax^*d(s).$$

Let $x = a^*y$ where $y \in I$; then

$$ax^*d(s) = ay^*ad(s) = 0.$$

Hence we get from the relation above,

(1) $\quad a(sd(a^*y) - d(a^*y)s) = 0 \quad$ for all $y \in I$, $s \in S_0$.

Suppose that $a^*S_0a \neq 0$; then there is an element $b^* = b \neq 0 \in a^*S_0a \subset S_0 \cap L$. Thus, using (1),

$$b(sd(by) - d(by)s) = 0.$$

Since $bd(b) = 0$, this relation above reduces to

(2) $\quad b(sd(b)y - bd(y)s + sbd(y)) = 0 \quad$ for $s \in S_0$, $y \in I$.

In particular, if $y \in S_0$, (2) further reduces to $bsd(b)y = 0$, which is to say, $bS_0d(b)S_0 = 0$. Now I cannot be commutative or an order in a 4-dimensional simple algebra, otherwise R would also be such. Thus $\bar{S}_0$, the subring generated by S_0, contains a non-zero ideal of I, hence a non-zero ideal of R by Theorem 2.1.5 of [**4**]. Since R is prime and $bS_0d(b)\bar{S}_0 = 0$, we are forced to $bS_0d(b) = 0$. If $d(b) \neq 0$, since $b \neq 0$, we get by Lemma 3 that $bSb = 0$, and so, since $b^* = b$, by Lemma 2 the contradiction $b = 0$. Hence we are forced to assume that $d(b) = 0$ for all $b \in a^*S_0a$, that is, $d(a^*S_0a) = 0$. But then (2) above becomes

$$b(sbd(y) - bd(y)s) = 0 \quad \text{for all } y \in I, s \in S_0;$$

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

therefore

(3) $bsbd(y) = b^2d(y)s$ for $s \in S_0$, $y \in I$.

In (3) let $y = zb$ where $z \in I$; since $d(b) = 0$, $d(y) = d(z)b$, hence from (3),

$$b^2d(z)sb = bsbd(z)b = bsbd(zb) = b^2d(zb)s = b^2d(z)bs,$$

that is, $b^2d(z)(bs - sb) = 0$, for $z \in I$, $s \in S_0$. Replace z by tx where $x \in R$, $t \in S_0$; since $bd(t) = 0$, we get

$$b^2td(x)(bs - sb) = 0.$$

If $d(R)(bs - sb) \neq 0$ we get by Lemma 3 that $b^2S_0b^2 = 0$, and since $b^2 = (b^2)^*$, using Lemma 2 we end up with $b^2 = 0$. But then (3) becomes $bS_0bd(I) = 0$. However $\{x \in R | xd(I) = 0\}$ is an ideal of R, and since R is prime and $d(I) \neq 0$, must be the zero ideal. Thus $bS_0b = 0$ follows, and since $b^* = b$, $b = 0$ results by Lemma 2, that is, $a^*S_0a = 0$.

If, on the other hand, $d(R)(bs - sb) = 0$ then $bs = sb$ follows, so b centralizes $\bar{S}_0$. Since we know that $\bar{S}_0$ contains an ideal of R, this fact forces $b \in Z$. But $bd(S_0) = 0$; together with $b \in Z$ and $d(S_0) \neq 0$ (Lemma 4), we end up with $b = 0$. So again we conclude that $b = 0$. In short, $a^*S_0a = 0$ for all $a \in L$, as claimed in the Theorem.

Note that if $T = \{x \in I | d(S \cap I)x = 0\}$ and if $T \neq 0$ then clearly T must be a minimal right ideal of R.

If R is its own central closure, let $I_0 = RIR$; then I_0 is centrally closed, and if $a \in L_0 = L \cap I_0$ then $a^*(S \cap I_0)a = 0$ by what we proved above. By Lemmas 1 and 3 we get that L_0 is a minimal left ideal of I_0, so $I_0L_0 = L_0$ is a minimal left ideal of R. But $L_0 \supset L \neq 0$ since $I_0 \subset I$; therefore $L = L_0$, so L is a minimal left ideal of R. The proof of Lemma 3 shows that $aRa = Ca$, from which we immediately get that if $L = Re$, $e^2 = e$, then $eRe = Ce$.

The rather long and arduous proof of Theorem 1 is now finished.

We now address ourselves to the problem mentioned in the introduction. From now on R will be a prime ring with involution, of characteristic not 2, with a derivation $d \neq 0$ such that $d(s)d(t) = d(t)d(s)$ for all $s, t \in S$. Our objective is to prove that R is either commutative or is an order in a 4-dimensional simple algebra. We suppose that this is not the case; after a series of lemmas we shall arrive at a contradiction. The first consequence of the denial of this desired proposition is that $S \not\subset Z$; hence all the lemmas we have proved so far will be valid in what follows.

We first dispose of the special case in which $d(s)d(t) = 0$ for all $s, t \in S$.

LEMMA 6. *Suppose that R is its own central closure and that $I \neq 0$ is an ideal of R. Then $d(s)d(t) \neq 0$ for some $s, t \in S \cap I$.*

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

Proof. Since R is prime, $I \cap I^* \neq 0$. We shall show that $d(s)d(t) \neq 0$ for some $s, t \in S \cap (I \cap I^*)$. Since we shall be working in $I \cap I^*$, and since $(I \cap I^*)^* = I \cap I^*$, we may assume that $I = I^*$.

Suppose that $d(s)d(t) = 0$ for all $s, t \in S \cap I$. By Lemma 5, $d(S \cap I) \neq 0$, so, if $L = \{x \in I | xd(S \cap I) = 0\}$ then $L \supset d(S \cap I)$, hence $L \neq 0$. By Theorem 1 we have that L is a minimal left ideal of R. Similarly, $T = \{x \in I | d(S \cap I)x = 0\}$ is a minimal right ideal of R.

Because L is a minimal left ideal of R, $W = \{x \in R | Lx = 0\}$ is a maximal right ideal of R. But since $d(S) \subset L$, we must have that $W \subset T$, hence $W = T$. Therefore T is both a maximal and minimal right ideal of R. Thus R must be artinian, and, being prime, is a simple artinian ring. Since R has zero-divisors and T is both a minimal and maximal right ideal of R, $R = D_2$, the ring of 2×2 matrices over a division ring D. Since $L = Re$, $e^2 = e$ and $eRe = Ce$ by Theorem 1, we see that $D = C$. Thus $R = C_2$, so is 4-dimensional over C. This contradicts our running assumption that R is not an order in a 4-dimensional simple algebra. The lemma is thereby proved.

Let $\mathfrak{Z}$ be the centroid of R; the involution $*$ on R induces an involution on $\mathfrak{Z}$ and the derivation d of R induces a derivation on $\mathfrak{Z}$. We denote these induced involution and derivation by $*$ and d.

LEMMA 7. *For* $\alpha \in \mathfrak{Z}$, $d(\alpha) = 0$.

Proof. Let $\alpha^* = \alpha \in \mathfrak{Z}$; if $t, s \in S$ then $d(\alpha s) = \alpha d(s) + d(\alpha)s$ commutes with $d(t)$ since $\alpha s \in S$. Thus we get

$$d(\alpha)(sd(t) - d(t)s) = 0.$$

If $d(\alpha) \neq 0$ then $d(t)$ centralizes S, hence centralizes $\bar{S}$; since $\bar{S}$ contains an ideal of R, we get that $d(t) \in Z$, hence $d(S) \subset Z$. By the Corollary to Lemma 5 we get the contradiction $S \subset Z$. Hence $d(\alpha) = 0$ for all symmetric $\alpha \in \mathfrak{Z}$.

If $\beta \neq \beta^* \in \mathfrak{Z}$ then $\beta^2 - (\beta + \beta^*)\beta + \beta^*\beta = 0$, thus

$$d(\beta^2) - (\beta + \beta^*)d(\beta) = 0$$

since $d(\beta + \beta^*) = 0$, $d(\beta^*\beta) = 0$. But $d(\beta^2) = 2\beta d(\beta)$; therefore we obtain

$$2\beta d(\beta) - (\beta + \beta^*)d(\beta) = 0,$$

and so

$$(\beta - \beta^*)d(\beta) = 0.$$

Since $\beta \neq \beta^* \in \mathfrak{Z}$, $d(\beta) \in \mathfrak{Z}$ and $\mathfrak{Z}$ is a domain, we end up with $d(\beta) = 0$. Therefore $d(\alpha) = 0$ for all $\alpha \in \mathfrak{Z}$.

We now show that the involution $*$ must be of the first kind, that is, it must be the identity on $\mathfrak{Z}$.

LEMMA 8. *If* $\alpha \in \mathfrak{Z}$ *then* $\alpha^* = \alpha$.

Proof. Suppose that $\alpha \neq \alpha^*$ for some $\alpha \in \mathfrak{Z}$. Thus

$$(\alpha - \alpha^*)x = \alpha(x + x^*) - (\alpha x^* + \alpha^* x) = \alpha s_1 - s_2,$$

where $s_1, s_2 \in S$, for any $x \in R$. Thus

$$d((\alpha - \alpha^*)x) = (\alpha - \alpha^*)d(x) = d(\alpha s_1 - s_2) = \alpha d(s_1) - d(s_2),$$

by Lemma 7. So, if $y \in R$,

$$d((\alpha - \alpha^*)y) = (\alpha - \alpha^*)d(y) = \alpha d(s_3) - d(s_4),$$

where $s_3, s_4 \in S$. Since any two $d(s)$'s commute, we get that $(\alpha - \alpha^*)d(x)$ commutes with $(\alpha - \alpha^*)d(y)$; because $\alpha - \alpha^* \neq 0$ this implies that $d(x)d(y) = d(y)d(x)$ for all $x, y \in R$. By the main result of [**2**] we get that R must be commutative or an order in a 4-dimensional simple algebra, in contradiction to our hypothesis. Lemma 8 is thus proved.

Let K_0 be the field of quotients of $\mathfrak{Z}$ and let K be any field containing K_0. In view of Lemma 7 and 8 we can extend d and $*$ to $R \otimes_{\mathfrak{Z}} K$ by defining

$$d(r \otimes k) = d(r) \otimes k \quad \text{and} \quad (r \otimes k)^* = r^* \otimes k.$$

The condition $d(s)d(t) = d(t)d(s)$ for $s, t \in S$ carries over to $R \otimes_{\mathfrak{Z}} K$. So we may assume that $\mathfrak{Z}$ is a field, in fact an algebraically closed field; for if $R \otimes_{\mathfrak{Z}} K$ is commutative or an order in a 4-dimensional simple algebra then it, and so R, satisfies the standard identity in 4 variables. By a theorem of Posner [**4**] we then have that R is commutative or an order in a 4-dimensional simple algebra.

The assumption that $\mathfrak{Z}$ is an algebraically closed field will be made in the rest of this paper. We also can carry things over to the central closure of R. So we may assume that R is its own central closure and that C, the extended centroid of R, is an algebraically closed field.

LEMMA 9. *If* $s \in S$ *then* $sd(s)^2 = d(s)^2 s$.

Proof. If $s \in S$ then $d(s)d(s^2) = d(s^2)d(s)$. But $d(s^2) = sd(s) + d(s)s$. Thus

$$d(s)(sd(s) + d(s)s) = (sd(s) + d(s)s)d(s),$$

and so, $sd(s^2) = d(s)^2 s$.

We want to investigate the nature of $d(s)^2$, for $s \in S$. Our first step is

LEMMA 10. *If* $s \in S$ *and* $a = d(s)^2$ *then* $[[t, a], a] = 0$ *for all* $t \in S$.

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

Proof. By Lemma 9 $d(s)^2 s = sd(s)^2$; replace s in this by $s \pm t$ where $t \in S$. We get

(1) $d(s)^2 t + 2d(s)d(t)s = 2sd(s)d(t) + td(s)^2$.

Commute the relation in (1) with $d(s)^2$; using that $d(s)^2$ commutes with s and $d(t)$ we get the result claimed in Lemma 10.

We also note that if $d(s)^2 = 0$ for all $s \in S$ then linearizing on s gives us that $d(s)d(t) = 0$ for all $s, t \in S$. This we have seen to be impossible in Lemma 6. So we may assume that $a = d(s)^2 \neq 0$ for some $s \in S$. Define the derivation δ on R by $\delta(x) = ax - xa$ for $x \in R$. Lemma 10 tells us that $\delta^2(S) = 0$.

Let $U = S^2$; as is easily verified, S^2 is a Lie ideal of R. We prove

LEMMA 11. $\delta^2 d(U) = 0$.

Proof. If $t, v \in S$ then $d(vt) = d(v)t + vd(t)$, hence, since $\delta d(v) = ad(v) - d(v)a = 0$, and $\delta d(t) = 0$, by our basic hypothesis on R, we have that

$$\delta^2 d(vt) = d(v)\delta^2(t) + \delta^2(v)d(t) = 0$$

by Lemma 10. Thus $\delta^2 d(U) = 0$.

We sharpen the result of Lemma 11 to show that $\delta^3 = 0$.

LEMMA 12. $\delta^3 = 0$.

Proof. If $U = S^2 \subset Z$ then we easily get that $S \subset Z$, which has been ruled out. So we have that $U \not\subset Z$. Because U is a noncentral Lie ideal of R, if we could show that $\delta^3(U) = 0$, by a result of Bergen, Herstein, and Kerr (Lemma 11 of [**2**]) we would conclude that $\delta^3 = 0$. So it is enough to show that $\delta^3(U) = 0$.

If $u \in U$, $us - su$ is also in U since U is a Lie ideal of R, for that s for which $a = d(s)^2$. So $\delta^2 d(us - su) = 0$. But

$$d(us - su) = (d(u)s - sd(u)) + (ud(s) - d(s)u),$$

hence

$$0 = \delta^2 d(us - su) = \delta^2(d(u)s - sd(u)) + \delta^2(ud(s) - d(s)u).$$

However, since $\delta(s) = 0$ by Lemma 9, and $\delta^2 d(u) = 0$ we have

$$\delta^2(d(u)s - sd(u)) = 0.$$

We are thus left with $\delta^2(ud(s) - d(s)u) = 0$, that is,

$$[[[u, d(s)], d(s)^2], d(s)^2] = 0.$$

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

This gives

$$[[[u, d(s)^2], d(s)^2], d(s)^2] = 0,$$

that is, $\delta^3(u) = 0$ for all $u \in U$. As we said earlier, this forces $\delta^3 = 0$.

Because of the result of this last lemma, namely, that the cube of δ is 0, the argument now breaks naturally in two directions, the first if the characteristic of R, char R, is not 3, the second if char $R = 3$.

Recall that δ is defined by $\delta(x) = ax - xa$, where $a = d(s)^2$. We have that

$$0 = \delta^3(x) = [[[x, a], a], a].$$

If char $R = 3$ this implies that $a^3 \in Z$, that is, $d(s)^6 \in Z$. If char $R \neq 3$, a result of [7] tells us that for some $\lambda \in C$, $(a - \lambda)^2 = 0$, that is

$$(d(s)^2 - \lambda)^2 = 0.$$

Since R is centrally closed, this says that for some $\lambda \in Z$,

$$(d(s)^2 - \lambda)^2 = 0.$$

We record these as

LEMMA 13. *If $s \in S$ and $a = d(s)^2$ then:*
1. *if* char $R = 3$, $a^3 \in Z$; *and*
2. *if* char $R \neq 3$, *there exists a* $\lambda \in Z$ *such that* $(a - \lambda)^2 = 0$.

The approach to the final proof of the theorem we seek will be through a series of reductions: first we shall show that R must be a simple ring with a non-trivial center, then we shall handle the case of matrices over a field, and finally we shall reduce to the case of a simple artinian ring By exploiting the matrix result we shall be able to push the proof through to its completion. This will be the line of attack.

Our first, and key, step in this program is

LEMMA 14. *R is a simple ring. Moreover, for some $s \in S$, $d(s)$ is not nilpotent. Consequently $Z \neq 0$.*

Proof. Let $I \neq 0$, $I \neq R$ be an ideal of R; by considering $I \cap I^*$ we may assume that $I^* = I$. If $J = I^2$ then $J^* = J$ and $d(J) \subset I$; hence, if $s \in S \cap J$ then $d(s) \in I$. From the nature of the reductions we have made so far in the paper we know that if $Z \neq 0$ then Z is a field. Hence $Z \cap I = 0$.

If char $R = 3$, by Lemma 13 $d(s)^6 \in Z \cap I = 0$ for all $s \in S \cap J$. On the other hand, if char $R \neq 3$, and if $s \in S \cap J$, then $(d(s)^2 - \lambda)^2 = 0$, so $\lambda^2 \in Z \cap I = 0$; this gives $\lambda = 0$ and $d(s)^4 = 0$. Thus in any case $d(s)$ is nilpotent for $s \in S \cap J$.

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

By Lemma 10 we have that

$$(1) \quad d(s)^4t - 2d(s)^2td(s)^2 + td(s)^4 = 0$$

for $s \in S \cap J$, $t \in S$. Since $d(s)$ is nilpotent, if $d(s)^m = 0$, $d(s)^{m-1} \neq 0$, multiplying (1) from the left by $d(s)^{m-1}$ yields that

$$d(s)^{m-1}Sd(s)^4 = 0.$$

Since $d(s)^{m-1} \neq 0$, by Lemma 3, $Rd(s)^4 = 0$ or $Rd(s)^4$ is a minimal left ideal of R.

If $d(s)^4 = 0$ for all $s \in S \cap J$ then by (1),

$$d(s)^2Sd(s)^2 = 0$$

so by Lemma either $d(s)^2 = 0$ or $Rd(s)^2$ is a minimal left ideal of R. By Lemma 6 it follows easily that there is an $s \in S \cap J$ such that $d(s)^2 \neq 0$; hence $Rd(s)^2$ is a minimal left ideal of R. If $t \in S \cap J$, consider $Rd(s)^2d(t)$. Since $d(s)d(t) = d(t)d(s)$,

$$Rd(s)^2d(t) = Rd(t)d(s)^2 \subset Rd(s)^2;$$

by the minimality of $Rd(s)^2$, if $Rd(s)^2d(t) \neq 0$ then

$$Rd(s)^2d(t) = Rd(s)^2.$$

But this last relation implies that

$$0 = Rd(s)^2d(t)^4 = Rd(s)^2,$$

a contradiction. Hence $d(s)^2d(t) = 0$ for all $s, t \in SJ$.

Hence, if $L = \{x \in I \mid xd(S \cap J) = 0\}$ then $L \ni d(s)^2$ for all $s \in S \cap J$, hence $L \neq 0$. It then follows immediately from a trivial variation on Theorem 1 that L is a minimal left ideal of R. Since $d(s)^2d(t) = 0$ for all $s, t \in S \cap J$, if $d(s)^2 \neq 0$ we have $Rd(s)^2 = L$ since $Rd(s)^2 \subset L$. Thus

$$Ls = Rd(s)^2s = Rsd(s)^2 \subset Rd(s)^2 = L,$$

by Lemma 9. In other words, if $s \in S \cap J$ and $d(s)^2 \neq 0$ then $Ls \subset L$. If $t \in S \cap J$ and $d(t)^2 = 0$ then $d(s + t)^2 \neq 0$ if $d(s)^2 \neq 0$; hence $L(s + t) \subset L$. But $Ls \subset L$, therefore $Lt \subset L$. In short, $L(S \cap J) \subset L$, hence $L\overline{S \cap J} \subset L$ where $\overline{S \cap J}$ is the subring generated by $S \cap J$. Since R is not commutative, nor an order in a 4-dimensional simple algebra, the same is true for J. Thus by Theorem 2.1.5 of [**4**], $\overline{S \cap J}$ contains a non-zero ideal of J, hence a non-zero ideal, W, of R. Therefore $LW \subset L$, hence $LWd(S \cap J) = 0$. By a trivial adaptation of the argument of Lemma 5, $d(S \cap J) \neq 0$, and since $L \neq 0$ and $W \neq 0$ is an ideal of R we get the contradiction, $LWd(S \cap J) = 0$, with the primeness of R.

The proof shows that $d(s)$ cannot be nilpotent for all $s \in S$, for what we have in effect shown above is that $d(s)$ cannot even be nilpotent for all s in $S \cap I$ where I is an ideal of R. If char $R = 3$, since $d(s)^6 \in Z$,

using a non-nilpotent $d(s)$ tells us that $Z \neq 0$. If char $R \neq 3$ and $s \in S$ is such that $d(s)$ is not nilpotent, since $(d(s)^2 - \lambda)^2 = 0$ for some $\lambda \in Z$, we see that $\lambda \neq 0$. Hence $Z \neq 0$.

With this the proof of the lemma is complete.

We now proceed to the second step in the program we have outlined to effect the proof.

LEMMA 15. *If F is a field of characteristic not 2, and F_n, $n > 1$, is the ring of $n \times n$ matrices over F, suppose that d defined by $d(x) = ax - xa$ for $x \in F_n$ satisfies $d(s)d(t) = d(t)d(s)$ for all $s, t \in S$, for some involution on F_n. Then, if $a \notin F$, $n = 2$.*

Proof. If $n > 2$, all the results we have proved so far will hold in F_n. In particular, $\alpha^* = \alpha$ for $\alpha \in F$ and some $d(s)$, for $s \in S$, cannot be nilpotent. By extending F to its algebraic closure we may assume that F is algebraically closed. Thus the involution on F_n is either the transpose or, if n is even, the symplectic involution.

Every element in F_n is a sum of elements of rank 1, hence every element in S is a sum of elements of rank at most 2. If $s \in S$ is of rank at most 2, then $d(s) = as - sa$ is of rank at most 4, so, if $n > 4$, $d(s)$ cannot be invertible, so must be nilpotent by Lemma 13. If $t \in S$ then $t = s_1 + \ldots + s_k$ where the s_i are of rank at most 2, so $d(t) = d(s_1) + \ldots + d(s_k)$ and the $d(s_i)$ are nilpotent and commute among themselves. So $d(t)$ is nilpotent. Hence $n \leqq 4$.

For the transpose case, if $n > 2$, using the e_{ii} and that $d(e_{ii}) = ae_{ii} - e_{ii}a$ is of rank at most 2 leads to $d(s)$ nilpotent if s is a diagonal matrix. From this, using diagonal matrices with distinct entries, one can show (using $d(s)^2 s = sd(s)^2$) that a is diagonal. Finally, computing $ae_{ij} - e_{ij}a$ and using Lemma 13, leads to $a \in F$.

For the symplectic case, using symmetric matrices

$$\begin{pmatrix} u & 0 \\ 0 & u \end{pmatrix}, \begin{pmatrix} 0 & j \\ 0 & 0 \end{pmatrix}, \text{ and } \begin{pmatrix} 0 & 0 \\ j & 0 \end{pmatrix},$$

where $u \in F_2$ is arbitrary, 1 denotes transpose, and $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, quickly leads on a computation of $as - sa$ to $a \in F$.

Thus we can conclude that if $a \notin F$ then $n = 2$.

We are now able to prove the theorem we set out to prove, namely,

THEOREM 2. *Let R be a prime ring of characteristic not 2, with an involution $*$. Suppose that $d \neq 0$ is a derivation of R such that $d(s)d(t) = d(t)d(s)$ for all $s, t \in S$. Then either R is commutative or is an order in a 4-dimensional simple algebra.*

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

Proof. Suppose that R is not commutative nor an order in a 4-dimensional simple algebra. As we have seen, we may assume that R is a simple ring with a non-trivial center $Z \neq 0$. Also d is linear with respect to Z and $\alpha^* = \alpha$ for $\alpha \in Z$. By Lemma 14 there is an $s \in S$ such that $d(s)$ is not nilpotent.

We divide the argument according as char $R = 3$ or char $R \neq 3$.

Suppose that char $R \neq 3$; let $s \in S$ such that $d(s)$ is not nilpotent, hence certainly $d(s)^2 \neq 0$. By Lemma 13, there exists a $\lambda \neq 0 \in Z$ such that $(d(s)^2 - \lambda)^2 = 0$. Let $b = d(s)^2 - \lambda$. By Lemma 10, if $a = d(s)^2$, $[[t, a], a] = 0$ for $t \in S$; hence for $b = a - \lambda$, $[[t, b], b] = 0$. Since $b^2 = 0$, we get from this $bSb = 0$. So, by Lemma 3, if $b \neq 0$ then Rb is a minimal left ideal of R. Our first objective in the proof is to show that R is simple artinian. If $b \neq 0$ then R is a simple ring, with unit (since $Z \neq 0$) and with a minimal right ideal $Rb \neq 0$. Then R must be simple artinian.

So, if R is not artinian we must have $b = 0$, that is, $d(s)^2 = \lambda$. This gives us that $d(t)^2 \in Z$ for all $t \in S$, so, if $d(s)^2 \neq 0$, we have from $d(s + t)^2 \in Z$ that $d(t) = \sigma d(s)$ where $\sigma \in Z$. Similarly, $d(st + ts) = \alpha d(s)$; but

$$\begin{aligned} d(st + ts) &= d(s)t + td(s) + sd(t) + d(t)s \\ &= d(s)t + td(s) + \sigma(d(s)s + sd(s)) = d(s)t + td(s) + \sigma d(s^2). \end{aligned}$$

Since $d(s^2) = \mu d(s)$ we get

$$d(s)t + td(s) = \beta d(s),$$

and so

$$\left(t - \frac{\beta}{2}\right)d(s) + d(s)\left(t - \frac{\beta}{2}\right) = 0;$$

thus $(t - \beta/2)^2$ commutes with $d(s)$. Since $(t - \beta/2)^2 \in S$, by the above,

$$2\left(t - \frac{\beta}{2}\right)^2 d(s) = \left(t - \frac{\beta}{2}\right)^2 d(s) + d(s)\left(t - \frac{\beta}{2}\right)^2 = \gamma d(s).$$

Therefore, since $d(s)$ is invertible, $2(t - \beta/2)^2 = \gamma$. Since S is quadratic over Z it satisfies a polynomial identity hence by [**4**], R satisfies a polynomial identity. Then certainly from Kaplansky's theorem R is artinian (finite-dimensional over Z). So, if char $R \neq 3$, R must be simple artinian.

Suppose then that char $R = 3$. By Lemma 13 there is a non-nilpotent $d(s)$, and since $d(s)^6 \in Z$ we have $d(s)^6 = \alpha \neq 0 \in Z$. If $t \in S$ then $d(s + t)^6 \in Z$ gives us that $d(s)^3 d(t)^3 \in Z$, and so $d(t)^3 = \sigma d(s)^3$ where $\sigma \in Z$. Since we saw that we may assume that Z is algebraically closed, $\sigma = \mu^3$ for $\mu \in Z$, hence $d(t)^3 = \mu^3 d(s)^3$, which gives us

$$(d(t - \mu s))^3 = 0.$$

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

Let $t_0 = t - \mu s$; then $d(t_0)^3 = 0$. Since

$$d(t_0)^4 w - 2d(t_0)^2 w d(t_0)^2 + w d(t_0)^4 = 0,$$

for $w \in S$, we get $d(t_0)^2 S d(t_0)^2 = 0$. If $d(t_0)^2 \neq 0$ then by Lemma 3, $Rd(t_0)^2$ is a minimal left ideal of R, hence, as above, R is simple artinian. So we get that if $t \in S$ and $d(t)$ is nilpotent then $d(t)^2 = 0$, if R is not artinian. Let

$$S_0 = \{t \in S | d(t)^2 = 0\};$$

by the above, if $t \in S$, $t - \mu s \in S_0$, hence S_0 is of co-dimension 1 in S.

If $t, w \in S_0$ then $d(t + w) = d(t) + d(w)$ is nilpotent, hence $d(t + w)^2 = 0$, which yields $d(t)d(w) = 0$. Also $t \in S_0$ implies $t^2 \in S_0$; for we have

$$d(t)^2 s + 2d(s)d(t)t = 2td(s)d(t) + sd(t)^2$$

that is, $d(s)d(t)t = td(s)d(t)$. Therefore

$$0 = d(s)d(t)^2 t = d(t)td(t)d(s),$$

whence $d(t)td(t) = 0$. Thus

$$d(t)d(t^2) = d(t)(td(t) + d(t)t) = 0;$$

if $d(t) \neq 0$ then $d(t^2)$ is a zero divisor so is nilpotent; if $d(t) = 0$ then $d(t^2) = 0$. So $t^2 \in S_0$. If $w \in S_0$, $(t + w)^2 \in S_0$ so $tw + wt \in S_0$; thus

$$d(t)d(tw + wt) = 0,$$

which gives us

$$d(t)wd(t) + d(t)td(w) = 0.$$

Because $d(t^2)d(w) = 0$ we get $d(t)td(w) = 0$. All this boils down to $d(t)S_0d(t) = 0$. So, if $d(t) \neq 0$ then

$$d(t)d(S)d(t) = d(t)d(S_0)d(t) + Zd(t)sd(t) = Zd(t)sd(t)$$

is 1-dimensional over Z. By Lemma 4 R has a minimal left ideal, so as before, is artinian. So, if R is not artinian, $d(t) = 0$ for $t \in S_0$. But then $d(w) = \sigma d(s)$, $\sigma \in Z$, for all $w \in S$. The proof given after this point for char $R \neq 3$ shows that R is artinian. Hence R is a simple artinian ring, whence $R = D_n$, the $n \times n$ matrices over a division ring D.

Let K be a maximal subfield of D and consider $R \otimes_Z K$; the argument just given for R works for $R \otimes_Z K$ and since d is linear with respect to K, d must be an inner automorphism on K_n. So $d(x) = ax - xa$ for $x \in K_n$, and since $d(s)d(t) = d(t)d(s)$ for any two symmetric elements of $R \otimes_Z K = K_m$, by Lemma 15, we get then $m = 2$. So $R \otimes_Z K$ is 4-dimensional over Z. With this contradiction the theorem is proved.

One should point out here that we cannot obtain an analogous result for polynomial identities of higher degree. As Lin [**6**] has pointed out, for

https://doi.org/10.4153/CJM-1982-023-x Published online by Cambridge University Press

any $n \geqq 3$ there exists a derivation $d \neq 0$ on F_n, the ring of $n \times n$ matrices over a field F, and on involution on F_n such that

$$d(s_1)d(s_2)d(s_3) = 0$$

for any three symmetric elements s_1, s_2, s_3 in F_n.

References

1. J. Bergen, I. N. Herstein and J. W. Kerr, *Lie ideals and derivations of prime rings*, (to appear).
2. I. N. Herstein, *A note on derivations*, Canadian Math. Bull. *21* (1978), 369–370.
3. ——— *Topics in ring theory* (Univ. of Chicago Press, Chicago, 1969).
4. ——— *Rings with involution* (Univ. of Chicago Press, Chicago, 1976).
5. ——— *A note on derivations II*, Canadian Math. Bull. *22* (1979), 509–511.
6. J. S. Lin, *On derivations of prime rings with involution*, Ph.D. thesis, Univ. of Chicago (1981).
7. R. Miers and W. Martindale, *On the iterates of derivations of prime rings*, (to appear).

University of Chicago,
Chicago, Illinois