J. Austral. Math. Soc. (*Series A*) **54** (1993), 133–141

ON CERTAIN SUBRINGS OF PRIME RINGS WITH DERIVATIONS

M. BREŠAR AND J. VUKMAN

(Received 19 May 1991; revised 13 August 1991)

Communicated by P. Schultz

Abstract

Let D be a nonzero derivation of a noncommutative prime ring R, and let U be the subring of R generated by all $[D(x), x]$, $x \in R$. A classical theorem of Posner asserts that U is not contained in the center of R. Under the additional assumption that the characteristic of R is not 2, we prove a more general result stating that U contains a nonzero left ideal of R as well as a nonzero right ideal of R.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 16 W 25, 16 N 60.
Keywords and phrases: Derivation, prime ring, ideal.

Let D be a nonzero derivation of a noncommutative prime ring R. A well-known theorem of Posner [11] states that the subset of R consisting of all $[D(x), x]$, $x \in R$, is not contained in the center of R. Roughly speaking, our intention is to show that this subset is rather large; the result we shall prove is

THEOREM. *Let R be a noncommutative prime ring of characteristic not 2, and let D be a nonzero derivation of R. Then U, the subring of R generated by all $[D(x), x]$, $x \in R$, contains a nonzero left ideal of R and a nonzero right ideal of R.*

It is easy to see that a noncommutative prime ring cannot contain a nonzero central one-sided ideal. Thus, neglecting the fact that we have to require that the characteristic of R is not 2, our result clearly generalizes

Posner's theorem (we remark that a number of authors have already generalized Posner's theorem in several ways—see, for example, some recent papers [1, 5, 12] where further references can be found).

On the other hand, our result is related to a theorem of Herstein [8] which asserts that if D is a derivation of any ring R, such that $D^3 \neq 0$, then the subring generated by all $D(x)$, $x \in R$, contains a nonzero ideal of R (see also an extension in [2]).

In order to prove the Theorem we will first prove

LEMMA 1. *Let R be a prime ring of characteristic not 2. If there exist nonzero derivations D and G of R such that $G([D(x), x]) = 0$ for all $x \in R$, then R is commutative.*

This lemma, although it may appear somewhat special, is of some independent interest. Take G to be an inner derivation, that is $G(x) = [a, x]$ for some $a \in R$; then we get

COROLLARY. *Let R be a prime ring of characteristic not 2, and let D be a nonzero derivation of R. If $a \in R$ is such that $[[D(x), x], a] = 0$ for all $x \in R$ then a lies in the center of R.*

The assumption in Posner's theorem can be written in the form

$$[[D(x), x], y] = 0 \quad \text{for all } x, y \in R.$$

Thus the assumption in the Corollary is much weaker. The Corollary can be compared with a result of the second named author [12] which states that a nonzero derivation D of a noncommutative prime ring of characteristic not 2 cannot satisfy $[[D(x), x], x] = 0$ for all $x \in R$.

Clearly, a nonzero derivation of a prime ring cannot vanish on some nonzero one-sided ideal. Therefore, Lemma 1 can be directly deduced from the Theorem. In fact, the Theorem is much more general than Lemma 1—as an illustration of this statement, note that using the Theorem it can be easily shown that Lemma 1 remains true if G is a nonzero (α, β)-derivation of R where α and β are automorphisms of R (see [9; p. 170] for the notion of (α, β)-derivations).

The assumption that the characteristic of R is not 2 cannot be removed in Lemma 1 (and, therefore, the same is true for the Theorem). Indeed, let R be any prime ring of characteristic 2 containing an element a such that $a^2 = 0$; define D by $D(x) = [a, x]$, and note that $D([D(x), x]) = 0$, $x \in R$.

Henceforth, R will represent a prime ring with center Z and extended centroid C. We list a few more or less well-known lemmas which will be needed in the sequel.

LEMMA 2. *Suppose that the elements* a_i, b_i *in the central closure of* R *satisfy* $\sum a_i y b_i = 0$ *for all* $y \in R$. *If* $b_i \neq 0$ *for some* i *then the* a_i*'s are C-dependent.*

The explanation of the notions of the extended centroid and the central closure of a prime ring, as well as the proof of Lemma 2, can be found in [7, pp. 20–23] or [10].

A special case of Lemma 2, but very important one, is

LEMMA 3. *The elements* a, b *in the central closure of* R *are C-dependent if and only if* $ayb = bya$ *holds for all* $y \in R$.

Using Lemma 2 (or even directly) one easily obtains

LEMMA 4. *Suppose that the elements* a, b, c *in the central closure of* R *satisfy* $ayb = cya$ *for all* $y \in R$. *If* $a \neq 0$ *then* $b = c$.

PROOF OF LEMMA 1. For the proof we need several steps.

STEP 1. For all $x, y \in R$,

$$[D(x), x]G(x) + G(x)[D(x), x] = 0, \tag{1}$$

$$\begin{aligned}(D(x)x - 2xD(x))yG(x) + G(x)y(2D(x)x - xD(x)) \\ + D(x)yxG(x) - G(x)xyD(x) = 0.\end{aligned} \tag{2}$$

PROOF. We define a mapping $B: R \times R \to R$ by

$$B(x, y) = [D(x), y] + [D(y), x].$$

Linearizing $G([D(x), x]) = 0$ we see that $G(B(x, y)) = 0$, $x, y \in R$.

Note that

$$B(xy, x) = B(x, x)y + xB(x, y) + D(x)[y, x].$$

Since $G(B(xy, x)) = 0$, $G(B(x, x)) = 0$, and $G(B(x, y)) = 0$, it follows from this identity that

$$B(x, x)G(y) + G(x)B(x, y) + (GD)(x)[y, x] + D(x)G([y, x]) = 0. \tag{3}$$

In particular, if $y = x$, we have $B(x, x)G(x) + G(x)B(x, x) = 0$. Since the characteristic of R is not 2 this proves (1).

Replacing y by yx in (3), and noting that

$$B(x, yx) = B(x, y)x + yB(x, x) + [y, x]D(x),$$

https://doi.org/10.1017/S1446788700037046 Published online by Cambridge University Press

one obtains

$$B(x, x)G(y)x + B(x, x)yG(x) + G(x)B(x, y)x + G(x)yB(x, x) + G(x)[y, x]D(x) + (GD)(x)[y, x]x + D(x)G([y, x])x + D(x)[y, x]G(x) = 0.$$

According to (3) this relation reduces to

$$B(x, x)yG(x) + G(x)yB(x, x) + G(x)[y, x]D(x) + D(x)[y, x]G(x) = 0.$$

Transposing and collecting terms, we obtain (2).

We set $M = \{x \in R | D(x)$ and $G(x)$ are C-dependent$\}$.

STEP 2. (i) If $\operatorname{char} R \neq 3$ then R is the union of its subsets M and $N = \{x \in R | D(x)$ and $[D(x), x]$ are C-dependent$\}$.

(ii) If $\operatorname{char} R = 3$ then R is the union of its subsets M and $\{x \in R | [G(x), x] = 0\}$.

PROOF. Take $x \notin M$. We set

$$a_1 = D(x)x - 2xD(x), \quad a_4 = -G(x)x,$$
$$a_2 = 2D(x)x - xD(x), \quad b = G(x),$$
$$a_3 = xG(x), \quad c = D(x).$$

We have assumed that b and c are C-independent. By (2) we have

$$a_1yb + bya_2 + cya_3 + a_4yc = 0, \quad y \in R. \tag{4}$$

Substituting ycz for y in (4) we get

$$a_1yczb + bycza_2 + cycza_3 + a_4yczc = 0.$$

But on the other hand we see from (4) that

$$(a_4yc)zc = -a_1ybzc - bya_2zc - cya_3zc.$$

Comparing the last two relations, we arrive at

$$a_1y(czb - bzc) + by(cza_2 - a_2zc) + cy(cza_3 - a_3zc) = 0, \quad y, z \in R. \tag{5}$$

By Lemma 2 there exists $z \in R$ such that $czb - bzc \neq 0$. Therefore it follows from (5) and Lemma 2 that the elements a_1, b and c are C-dependent. Since b and c are C-independent we have

$$a_1 = \lambda b + \mu c \tag{6}$$

for some $\lambda, \mu \in C$. Applying (6) in (5) we get

$$by(cz(\lambda b + a_2) - (\lambda b + a_2)zc) + cy(cz(\mu b + a_3) - (\mu b + a_3)zc) = 0, \quad y, z \in R.$$

https://doi.org/10.1017/S1446788700037046 Published online by Cambridge University Press

However, b and c are C-independent, therefore it follows by Lemma 2 that $cz(\lambda b + a_2) = (\lambda b + a_2)zc$ for all $z \in R$. Since $c \neq 0$, we then have $\lambda b + a_2 = \nu c$ for some $\nu \in C$. Hence we see from (6) that $a_1 + a_2 = (\mu + \nu)c$; that is, $3[D(x), x] = (\mu + \nu)D(x)$. Thus, if $\operatorname{char} R \neq 3$ this means that $x \in N$.

Now suppose that $\operatorname{char} R = 3$. Note that in this case $a_2 = -a_1$. Therefore (4) and (6) yield $cy(\mu b + a_3) = (\mu b - a_4)yc$, $y \in R$. Hence $a_3 = -a_4$ by Lemma 4. That is, $G(x)x = xG(x)$.

STEP 3. (i) If $x \in M$ then either $G(x) = 0$ or $[D(x), x] = 0$.

(ii) If $x \in M$ then either $D(x) = 0$ or $[G(x), x] = 0$.

PROOF. Take $u \in M$ such that $G(u) \neq 0$. We want to show that $[D(u), u] = 0$. Of course we may assume that $D(u) \neq 0$. Thus $G(u) = \alpha D(u)$ for some $\alpha \neq 0$ in C. Observe that (2) then implies

$$-2\alpha u D(u) y D(u) + 2\alpha D(u) y D(u) u = 0, \quad y \in R.$$

Since $\alpha \neq 0$ and the characteristic of R is not 2, it follows that $D(u)yD(u)u = uD(u)yD(u)$, $y \in R$. Consequently $D(u)u = uD(u)$ by Lemma 4. Thus (i) is proved. Analogously one proves (ii).

STEP 4. If $\operatorname{char} R = 3$ then R is commutative.

PROOF. From (ii) in Step 2 and (ii) in Step 3 we see that given $x \in R$, we have either $D(x) = 0$ or $[G(x), x] = 0$. We claim that $[G(x), x] = 0$ for all $x \in R$. Suppose this does not hold for some $x \in R$. Then, of course, $D(x) = 0$. Since $D \neq 0$ we have $D(y) \neq 0$ for some $y \in R$. Thus $[G(y), y] = 0$. Now, consider the elements $x+y$ and $x-y$. We have $D(x+y) \neq 0$, $D(x-y) \neq 0$, so that $[G(x+y), x+y] = 0$, $[G(x-y), x-y] = 0$; note that these two relations contradict the assumption that $[G(x), x] \neq 0$.

Thus $[G(x), x] = 0$ holds for all $x \in R$. By Posner's theorem, R is commutative.

We assume henceforth that $\operatorname{char} R \neq 3$.

STEP 5. If $x \in N$ then either $[D(x), x] = 0$ or $D(x)G(x) + G(x)D(x) = 0$.

PROOF. Take $x \in N$. Since $D(x) = 0$ implies $[D(x), x] = 0$ we may assume that $D(x) \neq 0$ and it follows that $[D(x), x] = \beta D(x)$ for some $\beta \in C$. By (1) we then see that $\beta(D(x)G(x) + G(x)D(x)) = 0$. Thus either $\beta = 0$, i.e., $[D(x), x] = 0$, or $D(x)G(x) + G(x)D(x) = 0$.

STEP 6. R is the union of its subsets $P = \{x \in R | [D(x), x] = 0\}$ and $Q = \{x \in R | D(x)G(x) + G(x)D(x) = 0\}$.

PROOF. Combine (i) in Step 2, (i) in Step 3, and Step 5.

STEP 7. Either $P = R$ or $Q = R$.

PROOF. We define biadditive mappings $A_1 : R \times R \to R$ and $A_2 : R \times R \to R$ by

$$A_1(x, y) = [D(x), y],$$
$$A_2(x, y) = D(x)G(y) + G(x)D(y).$$

By Step 6 we see that for any $x \in R$, either $A_1(x, x) = 0$ (that is, $x \in P$) or $A_2(x, x) = 0$ (that is, $x \in Q$). Suppose that $P \neq R$ and $Q \neq R$. Thus there exist $x, y \in R$ such that $A_1(x, x) \neq 0$ and $A_2(y, y) \neq 0$. In this case we have $A_1(y, y) = 0$ and $A_2(x, x) = 0$.

Suppose that $x+y \in P$; that is, $A_1(x+y, x+y) = 0$. Since $A_1(y, y) = 0$ this relation can be written in the form

$$A_1(x, x) + A_1(x, y) + A_1(y, x) = 0. \tag{7}$$

If also $x-y$ lies in P, then it follows that $A_1(x, x) - A_1(x, y) - A_1(y, x) = 0$. But then (7) yields $A_1(x, x) = 0$, contrary to the assumption. Thus $x - y \in Q$. That is, $A_2(x - y, x - y) = 0$, and therefore

$$-A_2(x, y) - A_2(y, x) + A_2(y, y) = 0 \tag{8}$$

since $A_2(x, x) = 0$. Consider the element $x + 2y$. If this element lies in P then we have $A_1(x, x) + 2A_1(x, y) + 2A_1(y, x) = 0$—but then it follows from (7) that $A_1(x, x) = 0$. Thus $x + 2y \in Q$. Consequently $2A_2(x, y) + 2A_2(y, x) + 4A_2(y, y) = 0$. According to (8) we then have $6A_2(y, y) = 0$, which leads to $A_2(y, y) = 0$ since we have assumed that the characteristic of R is different from 2 and 3. But this also contradicts the assumption.

Thus we have proved that $x + y \notin P$, and so $x + y \in Q$. In a similar fashion as above one shows that this is impossible if $x \notin P$ and $y \notin Q$.

STEP 8. R is commutative.

PROOF. Suppose that $Q = R$, that is, $D(x)G(x) + G(x)D(x) = 0$, $x \in R$. We claim that this relation contradicts the assumption that D and G are nonzero (this assertion is also presented in our paper [4]; however, we include the proof since it is rather short).

Note that any derivations D and G satisfy

$$(DG)(x^2) = (DG)(x)x + D(x)G(x) + G(x)D(x) + x(DG)(x).$$

If $D(x)G(x) + G(x)D(x) = 0$, $x \in R$, we then have $(DG)(x^2) = (DG)(x)x + x(DG)(x)$, $x \in R$. That is, DG is a Jordan derivation. A theorem of Herstein then tells us that DG is a derivation (see [6; Theorem 3.3] or [3] where

a brief proof is presented). But the composition of two nonzero derivations of a prime ring of characteristic not 2 cannot be a derivation [11; Theorem 1].

Thus $Q \neq R$. By Step 7 we then have $P = R$, that is, $[D(x), x] = 0$, $x \in R$. But then Posner's theorem tells us that R is commutative.

PROOF OF THE THEOREM. We assume that the Theorem is not true. By left-right symmetry we may assume that U does not contain nonzero left ideals.

STEP 1. For all $u \in U$, $[D(u), u] = 0$.

PROOF. As above, by $B(x, y)$ we denote $[D(x), y] + [D(y), x]$. Since $B(x, y) = [D(x+y), x+y] - [D(x), x] - [D(y), y]$ we see that $B(x, y) \in U$, $x, y \in R$. Expanding $B(x^2, x)$ we then get $B(x, x)x + xB(x, x) \in U$. Replacing x by $x + u$ we arrive at

$$B(x, x)u + uB(x, x) + 2B(x, u)u + 2uB(x, u) + 2B(x, u)x + 2xB(x, u) + B(u, u)x + xB(u, u) \in U.$$

If $u \in U$ then the first four summands lie in U, so it follows that

$$2B(x, u)x + 2xB(x, u) + B(u, u)x + xB(u, u) \in U$$

for $u \in U$, $x \in R$. A substitution $-x$ for x clearly yields

$$2B(u, u)x + 2xB(u, u) \in U, \quad u \in U, \quad x \in R. \tag{9}$$

Hence, given $u, v \in U$, $x \in R$, we have that

$$x[v, 2B(u, u)] = \{2B(u, u)xv + 2xvB(u, u)\} - (2B(u, u)x + 2xB(u, u))v$$

lies in U. That is, U contains a left ideal $R[v, 2B(u, u)]$ where u and v are arbitrary elements in U. By assumption it follows that $[v, 2B(u, u)] = 0$, $u, v \in U$. In particular, $2B(u, u)$ commutes with all elements of the form $[D(x), x]$, $x \in R$. Therefore $2B(u, u) \in Z$ by the Corollary. But then (9) gives $R(4B(u, u)) \in U$. By assumption, $4B(u, u) = 0$ and so $B(u, u) = 0$; that is, $2[D(u), u] = 0$.

STEP 2. For all $u \in U$, $x \in R$, $[x, u]D(u) \in U$ and $D(u)[x, u] \in U$.

PROOF. Noting that $B(ux, u) = B(u, u)x + uB(x, u) + D(u)[x, u]$ and using Step 1 it follows that $D(u)[x, u] \in U$. Expanding $B(xu, u)$ one obtains that $[x, u]D(u) \in U$.

STEP 3. For every $u \in U$ there exists $\lambda(u) \in C$ so that $D(u)u = \lambda(u)D(u)$.

PROOF. Take $u \in U$. For simplicity we denote $D(u)$ by a, and by δ we denote the inner derivation $\delta(x) = [x, u]$. By Step 1 we have $\delta(a) = 0$, and

https://doi.org/10.1017/S1446788700037046 Published online by Cambridge University Press

by Step 2 we have $\delta(x)a \in U$, $x \in R$. Taking $xa\delta(y)$ for x we then get $(\delta(x)a)(\delta(y)a)+xa\delta^2(y)a \in U$. The first term is in U, so it follows that for any $y \in R$, U contains the left ideal $Ra\delta^2(y)a$. Consequently $a\delta^2(y)a = 0$, $y \in R$. Therefore, observing that $\delta^2(yaz) = \delta^2(y)az+2\delta(y)a\delta(z)+ya\delta^2(z)$ and using $a\delta^2(yaz)a = 0$, $a\delta^2(y)a = 0$ and $a\delta^2(z)a = 0$, one obtains that $a\delta(y)a\delta(z)a = 0$, $y, z \in R$. Replacing y by zay and expanding the relation so obtained, it follows at once that $a\delta(z)ayaa\delta(z)a = 0$, $y, z \in R$. But then $a\delta(z)a = 0$ by the primeness of R. By definitions of a and δ, this means that $D(u)uzD(u) = D(u)zuD(u)$ where $u \in U$ and $z \in R$ are arbitrary. Since $D(u)$ commutes with u (Step 1), this relation can be rewritten as $D(u)uzD(u) = D(u)zD(u)u$; now apply Lemma 3.

STEP 4. (i) For $u, v \in U$, either $D(u)(v-\lambda(v)) = 0$ or $D(v)(u-\lambda(u)) = 0$.

(ii) For $u, v \in U$, either $(v-\lambda(v))D(u) = 0$ or $(u-\lambda(u))D(v) = 0$.

PROOF. A linearization of $[D(u), u] = 0$, $u \in U$, gives $[D(u), v] + [D(v), u] = 0$, $u, v \in U$. Replacing v by uv we get

$$\begin{aligned} 0 &= [D(u), uv] + [uD(v) + D(u)v, u] \\ &= [D(u), u]v + u\{[D(u), v] + [D(v), u]\} \\ &\quad + D(u)[v, u] + [D(u), u]v. \end{aligned}$$

Note that in the last sum, every summand except possibly $D(u)[v, u]$ is 0; but then $D(u)[v, u] = 0$ as well. That is, $D(u)v(u-\lambda(u)) = 0$, $u, v \in U$. By Steps 1, 2 and 3, U contains elements of the form $(v-\lambda(v))xD(v)$, $v \in U$, $x \in R$. Therefore the last relation yields $D(u)(v-\lambda(v))xD(v)(u-\lambda(u)) = 0$ for all $u, v \in U$, $x \in R$. Since R is prime, this proves (i). In a similar fashion (first showing that $[v, u]D(u) = 0$, and then applying Step 2) one proves (ii).

STEP 5. Either $D(U) = 0$ or $U \subseteq Z$.

PROOF. Take $v \in U$ and assume that $D(v) \neq 0$. Suppose that $D(u)(v-\lambda(v)) \neq 0$ for some $u \in U$. Then $D(v)(u-\lambda(u)) = 0$ by Step 4. Now, consider the pair of elements v and $u+v$. Since $D(u+v)(v-\lambda(v)) \neq 0$ (namely, $D(u)(v-\lambda(v)) \neq 0$ and $D(v)(v-\lambda(v)) = 0$), it follows that $D(v)(u+v-\lambda(u+v)) = 0$. We have $D(v)u = \lambda(u)D(v)$, $D(v)v = \lambda(v)D(v)$, so it follows that $D(v)(\lambda(u)+\lambda(v)-\lambda(u+v)) = 0$. By assumption, $D(v) \neq 0$, hence $\lambda(u+v) = \lambda(u)+\lambda(v)$. Consequently

$$\begin{aligned} 0 &= D(u+v)((u+v)-\lambda(u+v)) \\ &= (D(u)+D(v))((u-\lambda(u))+(v-\lambda(v))). \end{aligned}$$

Since $D(u)(u-\lambda(u)) = 0$, $D(v)(u-\lambda(u)) = 0$ and $D(v)(v-\lambda(v)) = 0$, it follows that $D(u)(v-\lambda(v)) = 0$, contrary to the assumption. Thus we

have showed that if $D(v) \neq 0$ then $D(u)(v - \lambda(v)) = 0$ for all $u \in U$. Similarly one shows that in this case we also have $(v - \lambda(v))D(u) = 0$, $u \in U$. Combining both statements we see that v commutes with all $D(u)$, $u \in U$. This means that U is the union of its additive subgroups $G = \{v \in U | D(v) = 0\}$ and $H = \{v \in U | [D(u), v] = 0 \text{ for all } u \in U\}$. However, a group cannot be the union of two proper subgroups, hence either $G = U$, that is, $D(U) = 0$, or $H = U$, that is, $D(U) \subseteq Z$ by the Corollary. In any case $D(U) \subseteq Z$. But then $D(u)(u - \lambda(u)) = 0$ implies $D(u)R(u - \lambda(u)) = 0$, and so for any $u \in U$ we have either $D(u) = 0$ or $u \in C \cap R = Z$. Again using the fact that a group cannot be the union of two proper subgroups it follows that $D(U) = 0$ or $U \subseteq Z$.

None of the assertions in Step 5 can hold—by Lemma 1, D cannot vanish on U, and by Posner's theorem, U cannot be contained in Z. The proof of the Theorem is thereby completed.

We conclude with an open question: is it possible to generalize the Theorem by proving that U contains a nonzero two-sided ideal?

References

[1] H. E. Bell and W. S. Martindale, 'Semiderivations and commutativity in prime rings', *Canad. Math. Bull.* **31** (1988), 500–508.
[2] J. Bergen, I. N. Herstein, and J. W. Kerr, 'Lie ideals and derivations in prime rings', *J. Algebra* **71** (1981), 259–267.
[3] M. Brešar and J. Vukman, 'Jordan derivations on prime rings', *Bull. Austral. Math. Soc.* **37** (1988), 321–322.
[4] ——, 'Orthogonal derivations and an extension of a theorem of Posner', *Rad. Mat.* **5** (1989), 237–246.
[5] ——, 'On left derivations and related mappings', *Proc. Amer. Math. Soc.* **110** (1990), 7–16.
[6] I. N. Herstein, *Topics in ring theory* (Univ. of Chicago Press, Chicago, 1969).
[7] ——, *Rings with involution* (Univ. of Chicago Press, Chicago, 1976).
[8] ——, 'A note on derivations', *Canad. Math. Bull.* **21** (1978), 369–370.
[9] N. Jacobson, *Structure of rings*, Colloq. Publ. 37 (Amer. Math. Soc., Providence, RI, 1956).
[10] W. S. Martindale, 'Prime rings satisfying a generalized polynomial identity', *J. Algebra* **12** (1969), 576–584.
[11] E. C. Posner, 'Derivations in prime rings', *Proc. Amer. Math. Soc.* **8** (1957), 1093–1100.
[12] J. Vukman, 'Commuting and centralizing mappings in prime rings', *Proc. Amer. Math. Soc.* **109** (1990), 47–52.

University of Maribor
PF, Koroška
160, 62000 Maribor
Slovenia