Canad. Math. Bull. Vol. **31** (4), 1988

SEMIDERIVATIONS AND COMMUTATIVITY IN PRIME RINGS

BY

H. E. BELL* AND W. S. MARTINDALE, III

ABSTRACT. A semiderivation of a ring R is an additive mapping $f{:}R \to R$ together with a function $g{:}R \to R$ such that $f(xy) = f(x)g(y) + xf(y) = f(x)y + g(x)f(y)$ and $f(g(x)) = g(f(x))$ for all $x, y \in R$. Motivating examples are derivations and mappings of the form $x \to x - g(x)$, g a ring endomorphism. A semiderivation f of R is centralizing on an ideal U if $[f(u), u]$ is central for all $u \in U$. For R prime of char. $\neq 2$, U a nonzero ideal of R, and $0 \neq f$ a semiderivation of R we prove: (1) if f is centralizing on U then either R is commutative or f is essentially one of the motivating examples, (2) if $[f(U), f(U)]$ is central then R is commutative.

In [2] Bergen introduced the notion of a semiderivation of a ring R:

DEFINITION. *An additive mapping $f{:}R \to R$ is a semiderivation if there exists a function $g{:}R \to R$ such that*

(i) $f(xy) = f(x)g(y) + xf(y) = f(x)y + g(x)f(y)$

(ii) $f(g(x)) = g(f(x))$

for all $x, y \in R$.

In case R is prime and $f \neq 0$ Chang ([3], Theorem 1) has shown that g must necessarily be a ring endomorphism.

For $g = 1$ a semiderivation is of course just a derivation. The other main motivating examples are of the form $f(x) = x - g(x)$ where g is any ring endomorphism of R. (On the other hand a semiderivation is a special case of what Jacobson ([5], p. 170) refers to as an (s_1, s_2)-derivation, being simultaneously a $(g, 1)$-derivation and a $(1, g)$-derivation).

If U is an ideal of R then a semiderivation f of R is said to be centralizing on U if $[f(u), u]$ lies in the center Z of R for all $u \in U$.

In [3] Chang extended a result of Posner [7] as follows.

THEOREM 9, [3]. *Let R be a prime ring of characteristic $\neq 2$, and let f be a nonzero semiderivation of R which is centralizing on R and whose associated endomorphism g is surjective. Then R is commutative.*

Received by the editors April 7, 1987.

*Supported by the Natural Sciences and Engineering Research Council of Canada, Grant No. A3961.

AMS Subject Classification (1980): 16A72, 16A70.

In the same paper Chang also generalized a result of Herstein [4]:

THEOREM 6, [4]. *Let R be a prime ring of characteristic $\neq 2$, and let f be a nonzero semiderivation of R such that $[f(R), f(R)]$ lies in the center Z of R. Then R is commutative.*

Our aim in this paper is to generalize these results of Chang in two directions. First of all we will only assume that the commutativity conditions are imposed on an ideal of R rather than on R itself. As we shall see this is not as routine a generalization as is often the case for ordinary derivations. Secondly we will treat the case of general semiderivations without the restriction that g be surjective. Specifically we establish two results in both of which we let R be a prime ring of characteristic $\neq 2$, f a nonzero semiderivation of R, and U a nonzero ideal of R.

THEOREM 1. *If f is centralizing on U then either* (a) *R is commutative or* (b) *g is not one-one, $g(U)$ is central, and there exists an element λ in the extended centroid such that $f(x) = \lambda(x - g(x))$ for all $x \in R$.*

THEOREM 2. *If $[f(U), f(U)]$ lies in the center, then R is commutative.*

We begin by citing two recent results which will prove useful in our considerations. The first is a special case of a theorem due to Lee and Lee ([6], Theorem 2):

THEOREM A. *If R is prime of characteristic $\neq 2$, $U \neq 0$ an ideal of R, and $a, b \in R$ such that $[a, [b, U]] \subset Z$, then either $a \in Z$ or $b \in Z$.*

As a well-known consequence we have

COROLLARY A. *If $[a, U] \subset Z$, then $a \in Z$.*

The second result is a special case of a theorem recently proved by us ([1], Theorem 2).

THEOREM B. *If R is prime, $U \neq 0$ an ideal of R, g an endomorphism of R which is one-one on U and centralizing on U, then R is commutative.*

Throughout this paper R will be a prime ring of characteristic $\neq 2$, Z will denote the center of R, F will denote the field of fractions of Z (if Z is nonzero), and C will denote the extended centroid of R. We shall on occasion make tacit use of the fact that R can be embedded in its central closure RC. The main appearance of the extended centroid will be in Lemma 4 where use is made of the basic fact that if $\phi: U \rightarrow R$ is an (R, R)-bimodule map of an ideal $U \neq 0$ then there exists $\lambda \in C$ such that $\lambda u = \phi(u)$ for all $u \in U$.

Furthermore we shall assume that R is endowed with a semiderivation f (with associated endomorphism g). Before imposing any commutativity conditions we begin with several lemmas of a general nature.

LEMMA 1. *If $f \neq 0$ and $U \neq 0$ is an ideal of R, then $f \neq 0$ on U.*

PROOF. Suppose $f(U) = 0$. Then for $u \in U$, $x \in R$ we have

$$0 = f(ux) = f(u)g(x) + uf(x) = uf(x),$$

forcing $f(x) = 0$ by the primeness of R.

LEMMA 2. *If $f \neq 0$, $U \neq 0$ is an ideal of R, and $a \in R$ such that $af(U) = 0$, then $a = 0$.*

PROOF. By Lemma 1 we may pick $u \in U$ such that $f(u) \neq 0$. For $v \in U$ we see that

$$0 = af(vu) = a(f(v)g(u) + vf(u)) = avf(u) = 0,$$

whence $a = 0$ by the primeness of R.

LEMMA 3. *If $f \neq 0$ and $U \neq 0$ is an ideal of R, then $f^2(U) \neq 0$.*

PROOF. Suppose $f^2(U) = 0$. Then for $u, v \in U$ we exploit the definition of f in different ways to obtain

$$\begin{aligned} (1) \qquad 0 &= f^2(uv) = f(f(u)v + g(u)f(v)) \\ &= f^2(u)v + g(f(u))f(v) + f(g(u)f(v)) \\ (2) \qquad 0 &= f^2(uv) = f(f(u)v + g(u)f(v)) \\ &= f^2(u)g(v) + f(u)f(v) + f(g(u)f(v)). \end{aligned}$$

Subtraction of (2) from (1) yields

$$(3) \qquad (g(f(u)) - f(u))f(v) = 0, \quad u, v \in U.$$

An application of Lemma 2 to (3) then says that $gf(u) = f(u)$ for all $u \in U$. Again for $u, v \in U$ we may also write

$$\begin{aligned} 0 &= f^2(uv) = f(f(u)v + g(u)f(v)) \\ &= f^2(u)g(v) + f(u)f(v) + f(g(u))g(f(v)) + g(u)f^2(v) \end{aligned}$$

whence we have

$$(4) \qquad f(u)f(v) + f(g(u))g(f(v)) = 0, \quad u, v \in U.$$

Since $f(g(u)) = g(f(u)) = f(u)$ for all $u \in U$ and characteristic $R \neq 2$ we conclude from (4) that $f(u)f(v) = 0$ for all $u, v \in U$. Another application of Lemma 2 asserts that $f(u) = 0$ for all $u \in U$, which then contradicts Lemma 1.

Some remarks are in order before we proceed to the next lemma. At first glance it may well seem that some difficulties could arise from the fact that $g(R)$ is just a subring of R and accordingly may not interact well with an ideal U

https://doi.org/10.4153/CMB-1988-072-9 Published online by Cambridge University Press

of R. Fortunately, however, it turns out that the "worst" case, namely $g(R) \cap U = 0$, actually is easily handled by use of the extended centroid C.

LEMMA 4. *If there exists a nonzero ideal U of R for which $U \cap g(R) = 0$, then there exists $\lambda \in C$ such that $f(x) = \lambda(x - g(x))$ for all $x \in R$.*

PROOF. We let W be the ideal $\sum_{x \in R} U(x - g(x))U$ and note that $W \neq 0$ (otherwise g would be the identity mapping in contradiction to $U \cap g(R) = 0$). We define a mapping $\phi: W \to R$ according to the rule:

$$\sum u_i(x_i - g(x_i))v_i \to \sum u_i f(x_i)v_i$$

where $u_i, v_i \in U$ and $x_i \in R$. Of course our main problem is to prove that ϕ is well-defined, since once we have done this it is immediate that ϕ is an (R, R)-bimodule map of W into R. To this end we suppose that

$$\sum u_i(x_i - g(x_i))v_i = 0 \tag{5}$$

and attempt to show that $\sum u_i f(x_i)v_i = 0$. Applying f to (5) we see that

$$\begin{aligned}
0 &= f \sum (u_i x_i v_i - u_i g(x_i)v_i) \\
&= \sum [u_i f(x_i v_i) + f(u_i)g(x_i v_i) - f(u_i g(x_i))g(v_i) - u_i g(x_i)f(v_i)] \\
&= \sum [u_i f(x_i)v_i + u_i g(x_i)f(v_i) + f(u_i)g(x_i)g(v_i) \\
&\quad - f(u_i)g(x_i)g(v_i) - g(u_i)f(g(x_i))g(v_i) - u_i g(x_i)f(v_i)] \\
&= \sum u_i f(x_i)v_i - \sum g(u_i)g(f(x_i))g(v_i) \\
&= \sum u_i f(x_i)v_i - g(\sum u_i f(x_i)v_i).
\end{aligned}$$

Therefore

$$\sum u_i f(x_i)v_i = g(\sum u_i f(x_i)v_i) \in U \cap g(R) = 0,$$

whence $\sum u_i f(x_i)v_i = 0$ and ϕ is well-defined. By the nature of the extended centroid C it follows that there exists $\lambda \in C$ such that $\lambda w = \phi(w)$ for all $w \in W$. Now, regarding R as a subring of the central closure RC, we have for all $u, v \in U$ and $x \in R$

$$u\lambda(x - g(x))v = \lambda(u(x - g(x))v) = \phi(u(x - g(x))v) = uf(x)v.$$

From the primeness of R we thus see that $f(x) = \lambda(x - g(x))$ for all $x \in R$.

Another situation in which f is close to being of the form $x - g(x)$ is given by

LEMMA 5. *If g is not one-one and $V \neq 0$ is an ideal of R contained in* ker g *then*

(a) *$f(V)$ is a nonzero ideal of R,*

(b) *there exists $\lambda \in C$ such that $f(x) = \lambda(x - g(x))$ for all $x \in R$.*

PROOF. For $v \in V$ and $r \in R$ we see immediately from

$$f(vr) = f(v)r + g(v)f(r) = f(v)r$$

and

$$f(rv) = rf(v) + f(r)g(v) = rf(v)$$

that $f(V)$ is an ideal of R. Furthermore $f(V) \neq 0$ in view of Lemma 1 and so (a) is proved. The argument establishing (a) also shows that f is an (R, R)-bimodule map of V into R. As we know this gives rise to an element $\lambda \in C$ such that $f(v) = \lambda v$ for all $v \in V$. For $v \in V$ and $r \in R$ we then see that

$$\lambda vr = f(vr) = vf(r) + f(v)g(r) = vf(r) + \lambda vg(r),$$

in other words, $v(f(r) + g(r) - \lambda r) = 0$. The primeness of R then forces $f(r) = \lambda(r - g(r))$ for all $r \in R$.

Before coming to our main theorems we treat one case in which an especially strong commutativity condition is imposed.

LEMMA 6. *If $f \neq 0$, g is one-one, and there exists a nonzero ideal U such that $f(U) \subset Z$, then R is commutative.*

PROOF. For $u \in U$ and $r \in R$ we first remark from $f([u, r]) = [f(u), r] + [g(u), f(r)]$ that $[g(u), f(r)] \in Z$ (here $[x, y]$ denotes the Lie bracket $xy - yx$). Replacing r by $g(r)$ and making use of $f(g(r)) = g(f(r))$ we then see that $g([u, f(r)]) = [g(u), g(f(r))] \in Z$ and in particular $g([u, f(r)])$ lies in the center of $g(R)$. Since g is one-one it follows that $[U, f(R)] \subset Z$, whence $f(R) \subset Z$ by Corollary A. If $f(Z) = 0$ then $f^2(U) \subset f(Z) = 0$ which contradicts Lemma 3. Therefore we may choose $z \in Z$ such that $f(z) \neq 0$. Now from $f(zr) = f(z)g(r) + zf(r)$ we conclude that $f(z)g(R) \subset Z$. Since $0 \neq f(z) \in Z$ it follows that $g(R) \subset Z$ and consequently that R is commutative in view of g being one-one.

We are now ready to impose the condition that f is centralizing on an ideal U (i.e., $[u, f(u)] \in Z$ for all $u \in U$) and to prove our first main result.

THEOREM 1. *Let R be a prime ring of characteristic $\neq 2$, let f be a nonzero semi-derivation of R (with associated endomorphism g), and let U be a nonzero ideal of R such that f is centralizing on U. Then the following hold*:

(a) *If R is commutative, then either f is a derivation of R or there exists an element λ in the field of fractions F of R such that $f(x) = \lambda(x - g(x))$ for all $x \in R$.*

(b) *If R is not commutative, then* $\ker g \neq 0$, *$g(U) \subset Z$ and there exists $\lambda \in C$ such that $f(x) = \lambda(x - g(x))$ for all $x \in R$. Moreover, if $f(g(U)) \neq 0$, then $g(R) \subset Z$, and $\lambda \in F$.*

PROOF. To prove (a) we may suppose that $g \neq 1$, since $g = 1$ simply means that f is a derivation. Accordingly we may choose $a \in R$ such that $a - g(a) \neq 0$ and set $\lambda = f(a)(a - g(a))^{-1} \in F$. From

$$f(xa) = f(x)a + g(x)f(a) = f(x)g(a) + xf(a)$$

it follows that $f(x)(a - g(a)) = f(a)(x - g(x))$, i.e., $f(x) = \lambda(x - g(x))$ for all $x \in R$ and we are done.

To prove (b) we start with the given condition

$$(6) \qquad [u, f(u)] \in Z, \quad u \in U.$$

Linearization of (6) produces

$$(7) \qquad [a, f(u)] + [u, f(a)] \in Z, \quad a, u \in U$$

and replacement of u by $[a, u]$ in (7) yields

$$(8) \qquad [a, f([a, u])] + [[a, u], f(a)] \in Z, \quad a, u \in U.$$

Expanding $f([a, u])$ in (8) we then have

$$(9) \qquad [a, [f(a), u]] + [a, [g(a), f(u)]] + [[a, u], f(a)] \in Z,$$

and applying the Jacobi identity to the first summand in (9) gives us

$$(10) \qquad [[a, f(a)], u] + [f(a), [a, u]] + [a, [g(a), f(u)]] + [[a, u], f(a)] \in Z.$$

The first summand in (10) is 0 by our hypothesis, the second and fourth summands cancel, and so we are left with

$$(11) \qquad [a, [g(a), f(u)]] \in Z, \quad a, u \in U.$$

From $0 = f([a, a]) = [f(a), a] + [g(a), f(a)]$ we see that

$$(12) \qquad [g(a), f(a)] \in Z, \quad a \in U,$$

and we can linearize (12) to obtain

$$(13) \qquad [g(a), f(u)] + [g(u), f(a)] \in Z, \quad u, a \in U.$$

In view of (13) we can now rewrite (11) as

$$(14) \qquad [a, [g(u), f(a)]] \in Z, \quad a, u \in U.$$

At this point we examine the case where g is one-one. We set $V = g^{-1}(U) = \{v \in R \mid g(v) \in U\}$ and note that V is an ideal of R. We first assume that $V \neq 0$. In (14) we set $a = g(v)$, $v \in V$ thereby achieving

$$\begin{aligned} g([v, [u, f(v)]]) &= [g(v), [g(u), g(f(u))]] \\ &= [g(v), [g(u), f(g(v))]] \in Z \end{aligned}$$

https://doi.org/10.4153/CMB-1988-072-9 Published online by Cambridge University Press

for all $v \in V$ and $u \in U$. This puts $g([v, [u, f(v)]])$ in the center of $g(R)$ and hence $[v, [u, f(v)]] \subset Z$ since g is one-one. By Theorem A either $v \in Z$ or $f(v) \in Z$. Setting $A = \{x \in V | x \in Z\}$ and $B = \{x \in V | f(x) \in Z\}$ we know that $V = A \cup B$ whence by a familiar group theory argument either $V = A$ or $V = B$, i.e., either $V \subset Z$ or $f(V) \subset Z$. In the former case it is well-known that R is commutative and in the latter case we may conclude that R is commutative by Lemma 6. This completes the argument in case $V \neq 0$. The situation where $V = g^{-1}(U) = 0$ means that $g(R) \cap U = 0$. Here Lemma 4 says that there exists $\lambda \in C$ such that $f(x) = \lambda(x - g(x))$ for all $x \in R$. But now, since f is centralizing on U, we see that g must also be centralizing on U, i.e., $[g(u), u] \in Z$ for all $u \in U$. As g is one-one an application of Theorem B then forces R to be commutative. All told the situation in which g is one-one always leads to R being commutative, contradictory to the hypothesis in part (b).

To complete the proof of (b) we now assume that $\ker g \neq 0$ and set $W = U \cap \ker g$. By Lemma 5 $f(W)$ is a nonzero ideal of R and there exists $\lambda \in C$ such that $f(x) = \lambda(x - g(x))$ for all $x \in R$. For $u \in U$ and $w \in W$ relation (13) tells us that $[g(u), f(w)] \in Z$, i.e., $[g(U), f(W)] \subset Z$. By Corollary A it follows that $g(U) \subset Z$ and the first part of (b) has been established. Finally, if $f(g(U)) \neq 0$, we may choose $a \in U$ such that $f(g(a)) \neq 0$. In particular $0 \neq g(a) \in Z$, and from $g(ra) = g(r)g(a) \in Z$, $r \in R$, we observe that $g(R) \subset Z$. As a result we may write $0 \neq f(g(a)) = \lambda(g(a) - g^2(a))$, which shows simultaneously that $0 \neq g(a) - g^2(a) \in Z$ and $f(g(a)) \in Z$. Therefore $\lambda = f(g(a))(g(a) - g^2(a))^{-1} \in F$ and the proof of Theorem 1 is complete.

As an example of a highly noncommutative prime ring possessing a nonzero centralizing semiderivation we cite the free algebra $R = \phi\langle x_1, x_2, \ldots\rangle$. Here we let g be the endomorphism which maps every element onto its constant term and set $f(x) = x - g(x)$. Since $g(R)$ is central it follows that f is centralizing.

We come now to our second main result.

THEOREM 2. *Let R be a prime ring of characteristic $\neq 2$, and let f be a nonzero semiderivation of R. If there exists a nonzero ideal U for which $[f(U), f(U)] \subset Z$, then R is commutative.*

PROOF. Without loss of generality we may assume that g (the endomorphism associated with f) is one-one. Indeed, if $\ker g \neq 0$ and $W = U \cap \ker g$ then by Lemma 5(a) $f(W)$ is a nonzero ideal of R. Accordingly $[f(W), f(W)] \subset Z$ forces commutativity of R in view of Corollary A.

With g one-one we first treat the case where $g(R) \cap U = 0$. By Lemma 4 there exists $\lambda \neq 0 \in C$ such that $f(x) = \lambda(x - g(x))$ for all $x \in R$, so that our hypothesis now yields

(15) $$[[u - g(u), v - g(v)], g(r)] = 0, \quad u, v \in U, r \in R.$$

But when expanded (15) reads

$$[g([u, v]), g(r)] = [[u, g(v)] + [g(u), v] - [u, v], g(r)]$$
$$\in g(R) \cap U = 0$$

that is, $g([[u, v], r]) = 0$. Since g is one-one we then have $[[u, v], r] = 0$ for $u, v \in U, r \in R$, and this forces commutativity of R.

Finally we analyze the situation in which $g^{-1}(U) \neq 0$. We first set $w = U \cap g^{-1}(U)$. For $u, v, \in U$ we see from

$$[f(u), f([f(u), v])] = [f(u), [f^2(u), g(v)]] + [f(u), [f(u), f(v)]]$$

that $[f(u), [f^2(u), g(v)]] \in Z$ for all $u, v \in U$. In particular, for $w \in W$, we have

$$[f(g(w)), [f^2(g(w)), g(v)]] \in Z$$

that is, $g([f(w), [f^2(w), v]]) \in Z$. Since g is one-one we know that this forces $[f(w), [f^2(w), v]] \in Z$ for all $w \in W, v \in U$. By Theorem A it follows that for any $w \in W$ either $f(w) \in Z$ or $f^2(w) \in Z$. The same group theory argument used in the proof of Theorem 1 can then be invoked at this point to conclude that either $f(W) \subset Z$ or $f^2(W) \subset Z$. In the former case we know by Lemma 6 that R is commutative. Therefore we may assume that $f^2(W) \subset Z$. From Lemma 3 we also know that $f^2(W) \neq 0$, and so we may choose $w \in W$ such that $\alpha = f^2(w) \neq 0 \in Z$. Starting with $[f(f(w)u), f(v)] \in Z$, $u, v \in U$, we obtain

$$[f^2(w)g(u), f(v)] + [f(w)f(u), f(v)] \in Z$$

which when further expanded yields

(16) $$f^2(w)[g(u), f(v)] + [f(w), f(v)]f(u) + f(w)[f(u), f(v)] \in Z.$$

Commuting (16) with $f(y)$, $y \in U$, then results in

$$f^2(w)[[g(u), f(v)], f(y)] + [f(w), f(v)][f(u), f(y)]$$
$$+ [f(w), f(y)][f(u), f(v)] = 0$$

from which in turn we conclude that

(17) $$f^2(w)[[g(u), f(v)], f(y)] \in Z, \quad u, v, y \in U.$$

Since $f^2(w) \neq 0$ (17) implies

(18) $$[[g(u), f(v)], f(y)] \in Z, \quad u, v, y \in U.$$

Replacement in (18) of v by $g(r)$ and y by $g(r)$, $r \in W$, results in

https://doi.org/10.4153/CMB-1988-072-9 Published online by Cambridge University Press

$$[\,[g(u), f(g(r))\,], f(g(r))\,] \in Z$$

or in other words

$$g(\,[\,[u, f(r)\,], f(r)\,]\,) \in Z. \tag{19}$$

As we know, since g is one-one, (19) imples that $[\,[u, f(r)\,], f(r)\,] = 0$ for all $u \in U$ and $r \in W$. By Theorem A we then conclude that $f(W) \subset Z$, whence R is commutative by Lemma 6.

References

1. H. E. Bell and W. S. Martindale, III, *Centralizing mappings of semiprime rings*, Canad. Math. Bull. **30** (1987), pp. 92-101.
2. J. Bergen, *Derivations in prime rings*, Canad. Math. Bull. **26** (1983), pp. 267-270.
3. J.-C. Chang, *On semiderivations of prime rings*, Chinese J. Math. **12** (1984), pp. 255-262.
4. I. N. Herstein, *A note on derivations II*, Canad. Math. Bull. **22** (1979), pp. 509-511.
5. N. Jacobson, *Structure of rings*, Colloq. Publ. 37, Amer. Math. Soc. (1956).
6. P. H. Lee and T. K. Lee, *Lie ideals of prime rings with derivations*, Bull. Institute of Math. Academia Sinica **11** (1983), pp. 75-79.
7. E. C. Posner, *Derivations in prime rings*, Proc. Amer. Math. Soc. **8** (1957), pp. 1093-1100.

DEPARTMENT OF MATHEMATICS
BROCK UNIVERSITY
ST. CATHARINES, ONTARIO
CANADA L2S 3A1

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF MASSACHUSETTS
AMHERST, MASSACHUSETTS 01003

https://doi.org/10.4153/CMB-1988-072-9 Published online by Cambridge University Press