

DERIVATIONS IN PRIME RINGS

B. FELZENSZWALB¹

ABSTRACT. Let R be a ring and $d \neq 0$ a derivation of R such that $d(x^n) = 0$, $n = n(x) > 1$, for all $x \in R$. It is shown that if R is primitive then R is an infinite field of characteristic $p > 0$ and $p|n(x)$ if $d(x) \neq 0$. Moreover, if R is prime and the set of integers $n(x)$ is bounded, the same conclusion holds.

1. Introduction. For an element a of a ring R , the mapping $d_a: x \rightarrow ax - xa$ of R into itself is a derivation, the inner derivation determined by a .

In terms of derivations, Herstein's hypercenter theorem [1] states that if R is a ring with no nonzero nil ideals and $a \in R$ is such that $d_a(x^n) = 0$, $n = n(x) \geq 1$, for all $x \in R$, then $d_a = 0$. A natural question related to this result is the following:

If R is a ring with no nonzero nil ideals and d is an arbitrary derivation of R such that $d(x^n) = 0$, $n = n(x) \geq 1$, for all $x \in R$, can we conclude that R must be rather special or $d = 0$?

Of course, one cannot expect that d will always be 0. In fact, if K is a commutative domain of characteristic $p > 0$, and d is the usual derivation on the polynomial ring $K[X]$, then $d(f^p) = 0$ for all $f \in K[X]$, but $d \neq 0$.

In this paper we show that if R is primitive and $d \neq 0$ is a derivation of R such that $d(x^n) = 0$, $n = n(x) \geq 1$, for all $x \in R$, then R is an infinite field of characteristic $p > 0$ where $p|n(x)$ if $d(x) \neq 0$. Moreover, if R is prime and the integers $n(x)$ have a finite maximum as x ranges over R , the same conclusion holds.

2. The case R is prime with nontrivial idempotents. We begin with

LEMMA 1. *Let R be a prime ring with an idempotent $e \neq 0$, 1. If d is a derivation of R such that $d(e + ex - exe) = 0$ for all $x \in R$, then $d = 0$.*

PROOF. Set $e_1 = e$, $e_2 = 1 - e$ (formally) and $R_{ij} = e_i R e_j$. The given condition implies $d(e_1) = 0$, so $d(e_2) = 0$ and $d(R_{12}) = 0$. Hence, $d(R_{ij}) = d(e_i R_{ij} e_j) = e_i d(R_{ij}) e_j \subseteq R_{ij}$. Thus, since $d(R_{12}) = 0$, we have

$$0 = d(R_{12} R_{21} R_{12}) = R_{12} d(R_{21}) R_{12} = e_1 R d(R_{21}) R e_2$$

and the primeness of R forces $d(R_{21}) = 0$. Finally from $0 = d(R_{ii} R_{ij}) = d(R_{ii}) R_{ij} = d(R_{ii}) R e_j$ we obtain $d(R_{ii}) = 0$. Since $R = \sum R_{ij}$ and d is additive we conclude that $d = 0$.

Received by the editors May 13, 1980.

1980 *Mathematics Subject Classification.* Primary 16A12.

¹This work was supported by CNPq, Brazil.

© 1982 American Mathematical Society
0002-9939/82/0000-0004/\$02.25

As an immediate consequence we have the following:

COROLLARY. *Let R be a prime ring with nontrivial idempotents. If d is a derivation of R such that $d(x^n) = 0$, $n = n(x) \geq 1$, for all $x \in R$, then $d = 0$.*

PROOF. Let e be a nontrivial idempotent in R . If $x \in R$, then, as is quickly checked, $f = e + ex - exe$ is an idempotent. Hence, $d(f) = d(f^{n(f)}) = 0$ and the result follows.

3. The case R is primitive. In order to settle the primitive case we need the following:

LEMMA 2. *Let Δ be a division ring with a derivation $d \neq 0$ such that $d(x^n) = 0$, $n = n(x) \geq 1$, for all $x \in \Delta$. Then Δ is an infinite field of characteristic $p > 0$ where $p|n(x)$ if $d(x) \neq 0$.*

PROOF. Let A be the subring of Δ generated by all $x^{n(x)}$ where $x \in \Delta$ and $d(x^{n(x)}) = 0$. Since $d(A) = 0$ and $d \neq 0$, we have that $A \neq \Delta$. By a result of Faith [2], Δ is commutative. Hence, $nx^{n-1}d(x) = d(x^n) = 0$, $n = n(x) \geq 1$, for all $x \in \Delta$. Since $d \neq 0$, we conclude that Δ is of characteristic $p > 0$ (and $p|n(x)$ if $d(x) \neq 0$). Thus, $d(x^p) = 0$ for all $x \in \Delta$. If Δ is finite then all its elements are p th powers, forcing $d = 0$. Therefore Δ is infinite and the lemma is proved.

We now settle the primitive case.

THEOREM 1. *Let R be a primitive ring with a derivation $d \neq 0$ such that $d(x^n) = 0$, $n = n(x) \geq 1$, for all $x \in R$. Then R is an infinite field of characteristic $p > 0$ where $p|n(x)$ if $d(x) \neq 0$.*

PROOF. Since R is primitive, it is a dense ring of linear transformations on a vector space V over a division ring Δ . If for some $x \neq 0$, in R , $\dim_{\Delta} Vx = 1$ (i.e., x is of rank one), then R has a minimal right ideal. So, either R has nontrivial idempotents or R is a division ring. By the corollary to Lemma 1, the first possibility leads to $d = 0$, contrary to our assumptions. Thus, R is a division ring and, by Lemma 2, the result follows. In other words, we may assume that $\dim_{\Delta} Vx > 1$ for all $x \in R$.

Let $x \neq 0$ be in R and suppose that, for some $v \in V$, $vd(x)$ and vx are linearly independent over Δ . By the density of the action of R on V , there exists $y \in R$ with $vd(x)y = 0$ and $vxy = v$. Let $n, m \geq 1$ be such that $d((yx)^n) = d((xy)^m) = 0$. Then, if $k = nm$, $d((yx)^k) = d((xy)^k) = 0$ and consequently

$$d(x)(yx)^k = d(x(yx)^k) = d((xy)^k x) = (xy)^k d(x).$$

So, $0 = vd(x)(yx)^k = v(xy)^k d(x) = vd(x)$, a contradiction. Thus, given $v \in V$, $vd(x) = \lambda(v)vx$ where $\lambda(v) \in \Delta$.

Let $v, w \in V$ be such that vx and wx are linearly independent over Δ . Since $vd(x) = \lambda(v)vx$, $wd(x) = \lambda(w)wx$ and $(v + w)d(x) = \lambda(v + w)(v + w)x$, we obtain

$$(\lambda(v) - \lambda(v + w))vx + (\lambda(w) - \lambda(v + w))wx = 0.$$

By the independence of vx and wx over Δ we conclude that $\lambda(v) = \lambda(v + w) = \lambda(w)$. Since λ is constant on these independent elements, and since $\dim_{\Delta} Vx > 1$, we get $\lambda(v) = \lambda$, λ independent of v , for all $v \in V$.

Thus, $v(d(x)x) = (vd(x))x = (\lambda vx)x$ and $v(xd(x)) = (vx)d(x) = (\lambda vx)x$; so, $v(d(x)x - xd(x)) = 0$ for all $v \in V$. Since R acts faithfully on V , we have $d(x)x = xd(x)$ for all $x \in R$.

Let $x, y \in R$ and let $n \geq 1$ be such that $d(y^n) = 0$. By the above,

$$d(x + y^n)(x + y^n) = (x + y^n)d(x + y^n) \quad \text{and} \quad d(x)x = xd(x).$$

These yield $d(x)y^n = y^n d(x)$. By the hypercenter theorem, $d(R) \subseteq Z$, the center of R .

Now, since $d \neq 0$, there exists an $x \in R$ such that $d(x) \neq 0$. By hypothesis, $d(xy^n) = d(x)y^n$, $n = n(y) \geq 1$, for all $y \in R$. Since R is prime, $d(R) \subseteq Z$ and $d(x) \neq 0$, we conclude that $y^{n(y)} \in Z$ for all $y \in R$. By the hypercenter theorem, R is commutative. By Lemma 2 the result follows.

4. The case R is prime. In this section we prove the result for prime rings stated in the introduction. To this end we need the following:

LEMMA 3. *Let R be a prime ring and $d \neq 0$ a derivation of R . Suppose that $d(x^n) = 0$ for all $x \in R$, where $n > 1$ is a fixed integer. Then R satisfies a generalized polynomial identity.*

PROOF. Suppose first that, for all $x \in R$, x and $d(x)$ are C -dependent where C is the extended centroid of R . Then $xd(x) = d(x)x$, and replacing x by $x + y^n$ we get $y^n d(x) = d(x)y^n$ for all $x, y \in R$. If, for some $a \in R$, $d(a)$ is not central then $f(X) = X^n d(a) - d(a)X^n$ is a nontrivial GPI. Thus we may assume $d(R) \subseteq Z$, the center of R . Let $x, y \in R$. If $d(x) \neq 0$ commute x with $d(xy) = d(x)y + xd(y)$ to get $d(x)(xy - yx) = 0$; since R is prime this forces $xy - yx = 0$, i.e., $x \in Z$. If $d(x) = 0$ then $d(xy) = xd(y) \in Z$ and choosing y with $d(y) \neq 0$ we again have, by the primeness of R , that $x \in Z$. Therefore R is commutative and we are done.

Suppose now that a and $d(a)$ are C -independent for some $a \in R$. Let $x \in R$; then by hypothesis, $d(a)(xa)^n = d(a(xa)^n) = d((ax)^n a) = (ax)^n d(a)$. By a standard linearization process, we obtain

$$\sum_{\sigma \in S_n} d(a)x_{\sigma(1)}ax_{\sigma(2)}a \cdots ax_{\sigma(n)}a = \sum_{\sigma \in S_n} ax_{\sigma(1)}ax_{\sigma(2)}a \cdots ax_{\sigma(n)}d(a)$$

where $x_1, \dots, x_n \in R$ and S_n is the symmetric group of degree n . Let X_1, \dots, X_n be noncommuting indeterminates. Set

$$f(X_1, \dots, X_n) = \sum_{\sigma \in S_n} d(a)X_{\sigma(1)}aX_{\sigma(2)} \cdots aX_{\sigma(n)}a - aX_{\sigma(1)}aX_{\sigma(2)} \cdots aX_{\sigma(n)}d(a).$$

Then f is a generalized identity satisfied by R . If it is trivial, we get $d(a)X_1aX_2a \cdots aX_n a - aX_1aX_2a \cdots aX_n d(a) = 0$ for these are the only monomials in f containing the X 's in this order. Fixing values for X_2, \dots, X_n in R , and using a result of Smith [5, Lemma 3] we have that a and $d(a)$ are C -dependent, a contradiction. Therefore f is nontrivial, and the lemma is proved.

Before proceeding we show that one can extend a derivation from a prime ring to its central closure. This is

LEMMA 4. *Let R be a prime ring with a derivation d , and let $S = RC$ be the central closure of R . Then we can extend d in a unique way to a derivation on S .*

PROOF. Let $s \in S$; then $s = [U, f]$, where $U \neq 0$ is an ideal of R and $f: U \rightarrow R$ is a right R -module map. Set $d(s) = [U^2, d(f)]$ where

$$(*) \quad d(f) = d(f(x)) - f(d(x)), \quad x \in U^2$$

(note that $d(U^2) \subseteq U$). It is easy to check that $d(f)$ is a right R -module map of U^2 into R . If $s = 0$, then $f = 0$ on some ideal $W \neq 0$ of R where $W \subseteq U$; hence, $d(f) = 0$ on W^2 and consequently $d(s) = 0$. Now, if f is a bimodule map of U into R , then $d(f)$ is also a bimodule map of U^2 into R ; thus $d(C) \subseteq C$ follows. Moreover, $d(rc) = d(r)c + rd(c)$ for $r \in R, c \in C$. Therefore

$$d(\sum r_i c_i) = \sum d(r_i) c_i + \sum r_i d(c_i), \quad r_i \in R, c_i \in C,$$

defines a derivation on S extending that of R . The uniqueness follows immediately from (*).

We are now in a position to prove

THEOREM 2. *Let R be a prime ring with a derivation $d \neq 0$ such that $d(x^n) = 0$ for all $x \in R$, where $n > 1$ is a fixed integer. Then R is an infinite commutative domain of characteristic $p > 0$ where $p|n$.*

PROOF. Let $S = RC$ be the central closure of R . By Lemma 3, R satisfies a generalized homogeneous multilinear identity. Therefore S satisfies this same generalized identity. By Martindale's theorem [4], S is a primitive ring containing a minimal right ideal $eS, e^2 = e$, and $\Delta = eSe$ is a division algebra finite dimensional over C . Moreover, by Lemma 4, we can extend d to a derivation on S , which we shall also denote by d .

We claim that $d(e) = 0$.

In fact, let $U \neq 0$ be an ideal of R such that $eU \subseteq R$. Let $u \in U$; since $e^2 = e$, by our hypothesis on $d, d(e)(eu)^n = d(e(eu)^n) = d((eu)^n) = 0$. If $d(e)e \neq 0$, then, by the density of the action of S on Se , there exists an $s \in S$ with $sd(e)e = e$. So,

$$0 = sd(e)(eu)^n = sd(e)e(ue)^{n-1}u = e(ue)^{n-1}u = (eu)^n.$$

That is, eU is a nil right ideal of R of bounded index of nilpotence. By a result of Levitzki [3, Lemma 2.1.1], this is not possible in a prime ring unless $eU = 0$, in which case $e = 0$. Therefore $d(e)e = 0$. Thus, since $d(e) = d(e^2) = d(e)e + ed(e)$, we have $d(e) = ed(e) \in eS$.

Suppose $d(e) \neq 0$. Then $d(e)$ and e are linearly independent over Δ (for otherwise, $d(e) = \lambda e, \lambda \in \Delta$; so, $0 = d(e)e = \lambda e^2 = \lambda e$ and consequently $d(e) = 0$). Hence, by the density of the action of S on eS , there exists an $s \in S$ with $d(e)s = e$ and $es = 0$. Let $U \neq 0$ be an ideal of R such that $sd(e)U \subseteq R$ and let $u \in U$. Since $es = 0, d(e)s = e$ and $ed(e) = d(e)$, we have

$$\begin{aligned} 0 &= d(e)(sd(e)u)^n = d(e)s(d(e)us)^{n-1}d(e)u \\ &= e(d(e)us)^{n-1}d(e)u = (d(e)us)^{n-1}d(e)u; \end{aligned}$$

thus, $(sd(e)u)^n = 0$. That is, $sd(e)U$ is a nil right ideal of R of bounded index of nilpotence. As before, this forces $sd(e) = 0$. Therefore $d(e) = ed(e) = (d(e)s)d(e) = 0$, and the claim is established.

Now, let $x \in S$. Then $f = e + ex - exe$ is an idempotent; moreover, $f \neq 0$ for otherwise $e = fe = 0$. By the minimality of eS , we have $fS = eS$ and so, by the argument used above, $d(f) = 0$. Since $d \neq 0$, by Lemma 1 we conclude that $e = 1$. Hence S is a division ring finite dimensional over C and every element in S is of the form az^{-1} where $a \in R$, $z \neq 0$ is in the center of R [3, Theorem 1.4.3]. Thus the condition $d(x^n) = 0$ holds in S and, by Lemma 2, the result follows.

Finally, let R be a prime ring with a derivation $d \neq 0$ such that $d(x^n) = 0$, $n = n(x) > 1$, for all $x \in R$. Suppose further that the integers $n(x)$ have a finite maximum, N , as x ranges over R . Then, from the derivation properties, $d(x^{N!}) = 0$ for all $x \in R$ and the conclusion of the above theorem holds.

Note. As the referee pointed out to us, the process of extending derivations to the central closure (and even larger rings of quotients) has been done previously by others, e.g. Kharchenko (*Differential identities of prime rings*, Algebra i Logika (2) (1978), 220–238) and Kovacs (*Idempotent derivations of prime rings*, Technion preprint series no. MT-447, Haifa, Israel, 1979).

ACKNOWLEDGEMENT. The author wishes to thank C. Polcino Milies for helpful conversations while writing this manuscript.

REFERENCES

1. I. N. Herstein, *On the hypercenter of a ring*, J. Algebra **36** (1975), 151–157.
2. _____, *On a result of Faith*, Canad. Math. Bull. **18** (1975), 609.
3. _____, *Rings with involution*, Univ. of Chicago Press, Chicago, Ill., 1976.
4. W. Martindale, *Prime rings satisfying a generalized polynomial identity*, J. Algebra **12** (1969), 576–584.
5. M. Smith, *Rings with an integral element whose centralizer satisfies a polynomial identity*, Duke Math. J. **42** (1975), 137–149.

INSTITUTO DE MATEMATICA, UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, CAIXA POSTAL 68530, 21910-RIO DE JANEIRO, RJ, BRAZIL