Canad. Math. Bull. Vol. 29 (4), 1986

A RESULT ON DERIVATIONS WITH ALGEBRAIC VALUES

BY
ONOFRIO M. DI VINCENZO

ABSTRACT. Let R be a prime algebra over a field F and let d be a non-zero derivation in R such that for every $x \in R$, $d(x)$ is algebraic over F of bounded degree. Then R is a primitive ring with a minimal right ideal eR, where $e^2 = e$ and eRe is a finite dimensional central division algebra.

Let R be a prime ring with center Z and let d be a non-zero derivation of R. In [3] Herstein proved that if for every $x \in R$, $d(x)^n \in Z$, where $n \geq 1$ is a fixed integer, then either R is commutative or R is an order in a 4-dimensional simple algebra. In this note we will examine a more general situation in the setting of algebras over a field F. If R is such an algebra, and $d \neq 0$ a derivation in R, we suppose that for every $x \in R\, d(x)$ is algebraic over F of bounded degree, i.e., there exists a nonconstant polynomial $p_x(t) \in F[t]$ depending on x such that $p_x(d(x)) = 0$ and deg. $p_x(t) \leq n$, $n \geq 1$ a fixed integer.

We remark that in this case one cannot expect the same conclusion of Herstein's theorem to hold as the following example shows:

EXAMPLE. *Let D be a finite dimensional division algebra over F, say dim.$_F D = n$ and let V be a vector space over D with* $\dim._D V \geq \aleph_0$. *If R is a dense ring of linear transformations on V over D containing a, a non-zero transformation of finite rank k, then R is a primitive ring with minimal right ideal. Now, if d is the inner derivation induced by a then for all $x \in R$, rank $d(x) \leq 2k$ and so $d(x)$ is algebraic over F of degree $\leq 4k^2n$.*

On the other hand one cannot even expect in this case d to be an inner derivation. To see this take F to be a field with a non-zero derivation d and let $R = F_m$ be the ring of $m \times m$ matrices over F. Now d induces a derivation d' in R by setting $d'((a_{ij})) = (d(a_{ij}))$. Clearly d' is not inner.

In this note we shall prove the following result: Let R be a prime algebra over a field F and let d be a non-zero derivation in R such that for every $x \in R$, $d(x)$ is algebraic over F of bounded degree. Then R is a primitive ring with minimal right ideal eR, where $e^2 = e$ and eRe is a finite dimensional central division algebra.

Received by the editors November 8, 1984, and, in revised form, July 19, 1985.
AMS Subject Classification (1980): 16A72.

Notice that in this result d is assumed to be any non-zero derivation not necessarily F-linear.

We shall make frequent use of the following two results.

REMARK 1. If $a \in R$ is algebraic over F of degree n, then a is invertible in R or a is a nilpotent element of index $\leq n$ or there exists a polynomial $q(t) \in F[t]$ such that $q(a)$ is a non trivial idempotent in R.

REMARK 2. Let a be algebraic over F of degree n, then for some $0 \neq p_a(t) \in F[t]$ of degree n, $0 = p_a(a) = p_a(a)y$ for all $y \in R$. Writing this explicitly we get

$$0 = a^n y + \alpha_{n-1}a^{n-1}y + \ldots + \alpha_1 ay + \alpha_0 y \qquad \text{where } \alpha_i \in F.$$

Thus $a^n y, \ldots, ay, y$ are linearly dependent over F, so that $P_n(a,y) = S_{n+1}(a^n y, a^{n-1}y, \ldots, ay, y) = 0$ where $S_{n+1}(x_1, \ldots, x_{n+1})$ is the standard polynomial in $n + 1$ variables. The same argument shows that if every element of R is algebraic over F of bounded degree n then $P_n(x_1, x_2)$ is a proper polynomial identity for R.

Throughout this note R will always be a prime algebra over a field F, Z the center of R; d will be a non-zero derivation of R such that, for every $x \in R$, $d(x)$ is algebraic over F of bounded degree n.

We start with

LEMMA 1. *If R has no nontrivial idempotents then R is a division ring.*

PROOF. By remark 1 for $x \in R$, $d(x)$ is either invertible or nilpotent of bounded index. Then by theorem 1.2 of [2] $R = D$, a division ring, or $R = D_2$, the 2×2 matrices over a division ring. Since D_2 has nontrivial idempotents R must be a division ring.

LEMMA 2. *If R is commutative then R is a field whose elements are algebraic over F of bounded degree.*

PROOF. As R is commutative, R is a domain. Then R has no idempotents elements $\neq 0, 1$ and by lemma 1 R is a field. Now let x be a transcendental element such that $d(x) \neq 0$; we have

$$0 = d(1) = d(xx^{-1}) = d(x)x^{-1} + xd(x^{-1}); \qquad \text{thus } x^2 = -d(x)d(x^{-1})^{-1}$$

is algebraic over F.

Therefore $d(x) = 0$ for all transcendental elements of R; since $d \neq 0$, there exists $y \in R$ such that $d(y) \neq 0$ and y is algebraic. Let m be its degree; since, for all $x \in R$, $d(xy) = d(x)y + xd(y)$ is algebraic of degree n then $x = (d(xy) - d(x)y)d(y)^{-1}$ is algebraic over F of degree $\leq n^2(1 + m)$.

We are now in a position to prove the main result in the case of a division ring. In the next theorem we will use the techniques given in [3].

THEOREM 1. *If R is a division ring then R is a finite dimensional over its center Z and all elements of Z are algebraic over F of bounded degree.*

https://doi.org/10.4153/CMB-1986-068-5 Published online by Cambridge University Press

PROOF. We split the proof into two different cases according as $d(Z) \neq 0$ or $d(Z) = 0$.

CASE 1. *Since* $0 \neq d(Z) \subset Z$, *Z is an infinite field and by lemma 2 all of its elements are algebraic over F of bounded degree. If* char. $Z = 0$ *and* $d(a) \neq 0$ *for some a in Z, then* $(d(a+m))/(a+m) = (d(a))/(a+m)$ *takes on an infinite set of distinct values in Z, as m runs over the integers.*

If char. $Z = p \neq 0$ then, for $a \in Z\, d(a^p) = pad(a^{p-1}) = 0$, so $a^p \in Z_0$, where $Z_0 = \{b \in Z : d(b) = 0\}$. If $a \notin Z_0$ then a is purely inseparable over Z_0 and so Z_0 is infinite. Hence $(d(a+b))/(a+b) = (d(a))/(a+b)$ takes on an infinite set of distinct values in Z as b runs over Z_0.

So we have that $(d(c))/c$ takes on an infinite set of distinct values as c runs over Z.

If $x \in R$, $0 \neq a \in Z$ then $d(ax) = d(a)x + ad(x)$ is algebraic over F of degree n; since $a^{-1} \in Z$ is algebraic of bounded degree we have that, for all $x \in R$, $d(x) + bx$ is algebraic over F of bounded degree, and $b = (d(a))/a$ takes an infinite set of distinct values in Z.

By remark 2, for all x, $y \in R$, $P_m(\mathrm{d}(x) + bx, y) = 0$ where m is an integer independent of x, y and b. As $b \in Z$ we may arrange $P_m(d(x) + bx, y)$ with respect to decreasing powers of b. Thus we obtain a polynomial in b, which is zero for infinitely many distinct values of b. By a Van der Monde determinant argument we have that all of its coefficients are zero. In particular $P_m(x, y)$ which is the coefficient of the term of highest degree is zero.

Thus $P_m(\mathrm{x}_1, x_2)$ is a proper polynomial identity for R, and R is finite dimensional over Z.

CASE 2. *Suppose first that* $d^2 = 0$; *then, for* $x, y \in R$, $d(x)d(y) = d(xd(y)) - xd^2(y) = d(xd(y)) \in d(R)$; *hence $d(R)$ is a subring of R and by hypothesis all of its elements are algebraic over F of bounded degree. Thus $d(R)$ is a division ring and by remark 2 $d(R)$ satisfies a proper polynomial identity; so $d(R)$ is finite dimensional over its center K.*

If $r \in R$ and $d(r) \neq 0$ then $d(rd(r)^{-1}) = 1 + rd(d(r)^{-1}) = 1 - rd(r)^{-1}d^2(r)d(r)^{-1} = 1$; this says that there exists $u \in R$ such that $d(u) = 1$. Hence if $a \in Z$, $a = a1 = ad(u) = d(au) - d(a)u = d(au)$ is in $Z \cap d(R) \subset K$, and so Z is contained in K.

On the other hand if $a \in K$ and a is not in Z then by the result of [4] we have that char. $R = 2, a^2 \in Z$ and $d(x) = \lambda_a(ax - xa)$ for some $\lambda_a \neq 0$ in Z.

If $b \neq a$ is in $K - Z$ we also have $d(x) = \lambda_b(bx - xb)$ for some $\lambda_b \neq 0$ in Z. Thus for all $x \in R$ we obtain $\lambda_a(ax - xa) = d(x) = \lambda_b(bx - xb)$ and so $(\lambda_a a + \lambda_b b)x = x(\lambda_a a + \lambda_b b)$; that is $\lambda_a a + \lambda_b b \in Z$.

This implies that b is in $Z(a)$, hence $K = Z(a)$ where $a^2 \in Z$. We have proved that $d(R)$ is a vector space finite dimensional over Z and by a result of [1] R is finite dimensional over Z. This fact can be also proved by the following argument:

If $d(c) = 0$, then if $d(r) \neq 0$, $d(crd(r)^{-1}) = \ldots = c$, so $c \in d(R)$. If $n = \dim._Z d(R)$, then given $x_1, \ldots, x_{n+1} \in R$, there exist

$$z_1, \ldots, z_{n+1} \in Z \qquad \text{with } 0 = \sum_i z_i d(x_i) = d\Big(\sum_i z_i x_i\Big).$$

Thus the Z vector space $R/d(R)$ has dimension $\leqslant n$, which implies R is finite dimensional over Z.

Now suppose $d^2 \neq 0$ and let $r \in R$ be such that $d^2(r) \neq 0$.

If $\bar{Z}$ is the algebraic closure of Z then d can be extended to a $\bar{Z}$-linear derivation d on $R' = R \otimes_Z \bar{Z}$. Such derivation does not satisfy the hypothesis of the theorem, however R' satisfies again the relation

$$\sum_{\sigma \in S_n} \alpha_\sigma d(x_{\sigma(1)}) \ldots d(x_{\sigma(n)}) = 0.$$

which is obtained in R by linearizing the identity $P_n(d(x), d(y)) = 0$.

R' is a simple ring with 1 and if $\alpha \in \bar{Z}$ is a root of a polynomial of $F[t]$ satisfied by $d(r)$ then $u = d(r) - \alpha \neq 0$ is a zero divisor in R'. Let $L = \{x \in R' : xu = 0\}$; since u is a zero divisor $L \neq 0$, since $d(u) = d^2(r) \neq 0$ is invertible $Ld(u) \neq 0$.

Let $x_1, \ldots, x_n$ be in L; thus $x_i u = 0$ and so $0 = d(x_i u) = d(x_i)u + x_i d(u)$. Now

$$\sum_\sigma \alpha_\sigma d(ux_{\sigma(1)}) \ldots d(ux_{\sigma(n)}) = 0,$$

therefore

$$\sum_\sigma \alpha_\sigma d(ux_{\sigma(1)}) \ldots d(ux_{\sigma(n)})u = 0.$$

But

$$\begin{aligned} d(ux_{\sigma(1)}) \ldots d(ux_{\sigma(n)})u &= d(ux_{\sigma(1)}) \ldots d(ux_{\sigma(n-1)})(d(u)x_{\sigma(n)} + ud(x_{\sigma(n)}))u \\ &= d(ux_{\sigma(1)}) \ldots d(ux_{\sigma(n-1)})ud(x_{\sigma(n)}))u = \ldots = ud(x_{\sigma(1)})ud(x_{\sigma(2)})u \ldots ud(x_{\sigma(n)})u. \end{aligned}$$

Then we have

$$(*)\ 0 = \sum_\sigma \alpha_\sigma d(ux_{\sigma(1)}) \ldots d(ux_{\sigma(n)})u = \sum_\sigma \alpha_\sigma ud(x_{\sigma(1)})u \ldots ud(x_{\sigma(n)})u.$$

But $d(x_{\sigma(i)})u = -x_{\sigma(i)}d(u)$ since $x_{\sigma(i)}u = 0$. So $(*)$ implies that:

$$u \sum_\sigma \alpha_\sigma x_{\sigma(1)} d(u) x_{\sigma(2)} d(u) \ldots x_{\sigma(n)} d(u) = 0 \quad \text{for } x_1, \ldots, x_n \in L.$$

In conclusion, for $y_1, \ldots, y_n \in Ld(u)$ we have

$$0 = u\Big(\sum_\sigma \alpha_\sigma y_{\sigma(1)} y_{\sigma(2)} \ldots y_{\sigma(n)}\Big).$$

https://doi.org/10.4153/CMB-1986-068-5 Published online by Cambridge University Press

By lemma 1 of [3] the left ideal $Ld(u) \neq 0$ of R' satisfies a polynomial identity over Z. By a result of Martindale [6, Th. 1.3.2], R' has a minimal left ideal $R'e$. Since R' is simple with 1 and has a minimal left ideal we get that R' is Artinian and $R' \approx \bar{Z}_q$ for some q.

Since $R' = R \otimes_Z \bar{Z} \approx \bar{Z}_q$ is finite dimensional over $\bar{Z}$, R is finite dimensional over Z.

Finally for $a \in Z$ and $x \in R$ with $d(x) \neq 0$ we have $d(ax) = ad(x)$ and $d(x)^{-1}$ commutes with $d(ax)$; hence $a = d(ax)d(x)^{-1}$ is algebraic over F of bounded degree.

LEMMA 3. *If R has idempotent elements $\neq 0, 1$, then R has a one sided ideal which is algebraic over F of bounded degree.*

PROOF. Let $a \in R$ and let $T(a) = \{y \in R : ay = 0\}$ be the right annihilator of a in R. If $x \in T(a)$, let $p_{xa}(t) = \Sigma_0^n \alpha_i t^i \in F[t]$ be such that $p_{xa}(d(xa)) = 0$; hence $\Sigma_0^n \alpha_i d(xa)^i = 0$ and we have:

$$0 = \left(\sum_0^n \alpha_i d(xa)^i\right)x = \sum_0^n \alpha_i d(xa)^i x.$$

But

$$d(xa)^i x = d(xa)^{i-1}(d(x)a + xd(a))x = d(xa)^{i-1}xd(a)x = \ldots = x(d(a))x)^i;$$

hence

$$0 = \sum_0^n \alpha_i d(xa)^i x = \sum_0^n \alpha_i x(d(a)x)^i = \sum_0^n \alpha_i d(a)x(d(a)x)^i = \sum_0^n \alpha_i (d(a)x)^{i+1}.$$

Therefore all the elements of $d(a)T(a)$ are algebraic over F of bounded degree. If R has no algebraic right ideals of bounded degree then $d(a)T(a) = 0$. Since for $x \in T(a) 0 = d(ax) = d(a)x + ad(x) = ad(x)$ then $d(T(a)) \subset T(a)$.

An analogous argument shows that if $L(a) = \{y \in R : ya = 0\}$ is the left annihilator of a in R, then $d(L(a)) \subset L(a)$.

If $r \in R$ and e is an idempotent then $e(r - er) = 0$. Hence $d(e)(r - er) = 0$, and so $(d(e) - d(e)e)R = 0$. But R is a prime ring forcing $d(e) = d(e)e$.

Similarly we obtain $d(e) = ed(e)$ and it follows that $d(e) = d(e^2) = d(e)e + ed(e) = d(e) + d(e)$. Consequently $d(e) = 0$ for every idempotent in R; this says that $d(E) = 0$ where E is the subring generated by all the idempotents. Since E is invariant with respect to all the automorphisms of R, by the result of [5], either R is the ring of 2×2 matrices over $GF(2)$ or E contains a two-sided ideal $I \neq 0$ of R.

In the first case R is a finite ring, so R is algebraic over F of bounded degree and we are done.

In the second case $d(I) \subset d(E) = 0$ implying $d = 0$, a contradiction.

We now prove the main result of this note.

THEOREM 2. *Let R be a prime algebra over a field F and let d be a non-zero derivation in R such that, for every $x \in R$, $d(x)$ is algebraic over F of bounded degree. Then R is an algebra with minimal right ideal eR and eRe is a division ring finite dimensional over its center. Moreover if $d(Z(R)) \neq 0$ then R is a finite dimensional central simple algebra.*

PROOF. If R has no idempotent elements $\neq 0, 1$ then by lemma 1 and theorem 1 R is a division ring finite dimensional over its center.

Hence, without loss of generality, we may assume that R has nontrivial idempotents; by lemma 3 R contains a right ideal $\rho \neq 0$ which is algebraic over F of bounded degree. If $\rho = R$, by remark 2 R satisfies a proper polynomial identity. By Posner's theorem ([6]) $Z(R)$, the center of R, is different from zero and R is a order in $A = \{xz^{-1}: x \in R, z \in Z(R)\}$ which is also a P. I. algebra. Since $Z(R)$ is a domain and all of its elements are algebraic over the field F we have that $Z(R)$ is a field; and so $R = A$ is a finite dimensional central simple algebra.

Suppose now $\rho \neq R$; by remark 1 if ρ has not non-trivial idempotents then all of its elements are nilpotent of bounded index. By a theorem of Levitzki ([6]) then R contains a nilpotent right ideal $\rho' \neq 0$; but R is a prime ring and so ρ must have an idempotent $e_0 \neq 0, 1$.

Of course $S = e_0Re_0 \subset \rho$ is a prime algebra whose elements are algebraic over F of bounded degree, and the above argument shows that S is a central simple algebra finite dimensional over its center.

Then S has a minimal right ideal eS, $e^2 = e \in S$ and eSe is a division ring. Since e_0 is the unit element of S, $eSe = ee_0Re_0e = eRe$ is a division ring and so eR is a minimal right ideal of R.

Therefore R is a primitive algebra, eR is a minimal right ideal and eRe is a division ring finite dimensional over its center.

Moreover if $d(Z(R)) \neq 0$ then the restriction of d to $Z(R)$ is a derivation $d \neq 0$ such that for every $z \in Z(R), d(z)$ is algebraic over F of bounded degree.

By using the same argument of theorem 1, (case 1), we obtain that R satisfies a proper polynomial identity, so that R is a finite dimensional central simple algebra.

REFERENCES

1. J. Bergen, Ph.D. dissertation, U. of Chicago (1981).

2. J. Bergen, *Lie ideals with regular and nilpotent elements and a result on derivations*, Rend. Circ. Mat. Palermo (2), **33** (1984), pp. 99–108.

3. I. N. Herstein, *Derivations of prime rings having power central values*, Algebraists' Homage, Contemporary Math. Vol. 13, AMS (1982), pp. 163–171.

4. I. N. Herstein, *A note on derivations II*, Can. Math. Bull., **22** (1979), pp. 509–511.

5. I. N. Herstein, *A theorem on invariant subrings*, J. Algebra, **83** (1983), pp. 26–32.

6. I. N. Herstein, *Rings with involution*, U. of Chicago Press (1976).

ISTITUTO DI MATEMATICA
UNIVERSITÀ DI PALERMO
VIA ARCHIRAFI 34
90123 PALERMO, ITALY