Can. J. Math. Vol. 45 (1), 1993 pp. 22–32

HOMOGENEOUS POLYNOMIALS, CENTRALIZERS AND DERIVATIONS IN RINGS

ONOFRIO MARIO DI VINCENZO AND ROSA SAGONA

ABSTRACT Let d be a non-zero derivation on a primitive ring R and $f(x_1, \ldots, x_n)$ a homogeneous polynomial of degree m We prove that the condition $d\big(f(r_1, \ldots, r_n)^t\big) = 0$, for all $r_1, \ldots, r_n \in R$, with t depending on $r_1, \ldots, r_n$, forces R to be a finite dimensional central simple algebra and f power-central valued on R We also obtain bounds on $[R : Z(R)]$ in terms of m

Let C be a fixed commutative ring with 1 and let $C\{X\}$ be the free algebra over C generated by a countable set X of noncommutative variables. If R is a C-algebra then given a polynomial $f = f(x_1, \ldots, x_n)$ in $C\{X\}$ in n variables, f induces a map $R^n \longrightarrow R$ which is said to be *algebraic valued.*

The study of such functions includes as a special case the theory of algebras with polynomial identities or with central polynomials (see [10]).

Many results have been proved concerning the relationship between a ring R and the valuations in R of some nonzero polynomial in $C\{X\}$ (see [1], [4], [5] and [9]).

We recall that the polynomial $f(x_1, \ldots, x_n)$ is said to be *power-central valued* in R if for all $r_1, \ldots, r_n$ in R there exists an integer $t = t(r_1, \ldots, r_n) \geq 1$ such that $f(r_1, \ldots, r_n)^t$ is in $Z(R)$, the center of R.

The main result of this paper is the following:

THEOREM 2. *Let R be a primitive ring, $f(x_1, \ldots, x_n)$ a homogeneous polynomial of degree m. Suppose that d is a non-zero derivation on R such that, for all $r_1, \ldots, r_n \in R$, there exists $t \in \mathbb{N}$, $t = t(r_1, \ldots, r_n)$, such that $d\big(f(r_1, \ldots, r_n)^t\big) = 0$. If* char $R = p > 0$ *we assume that f is not an identity for $p \times p$ matrices in characteristic p. Then $f(x_1, \ldots, x_n)$ is power-central valued and R is a finite dimensional central simple algebra. Moreover, if f is not a polynomial identity on R then either d is an inner derivation on R or $Z(R)$ is infinite of characteristic $p \neq 0$.*

We also obtain bounds on $[R : Z(R)]$ in terms of m.

The hypothesis that f is not an identity for $p \times p$ matrices in characteristic $p \neq 0$ is required in the result of [9], that if D is a division ring and f power-central valued on D then D is finite dimensional over its center. Since that result is fundamental in what we do, we assume this hypothesis throughout this paper.

The first author's work was done within the activity of G N S A G A of C N R with the support of M U R S T (Italy)

Received by the editors January 30, 1991, revised May 29, 1991

AMS subject classification 16A38, 16A72

As a consequence of our result we also obtain a characterization of the subring $T(R)$ of R of those elements which commute with some power of the valuations of $f(x_1,\ldots,x_n)$. More precisely as in [3] let

$$T(R) = \{a \in R \mid af(r_1,\ldots,r_n)^t = f(r_1,\ldots,r_n)^t a; r_1,\ldots,r_n \in R, t = t(a,r_1,\ldots,r_n) \geq 1\}.$$

Then either $T(R) = Z(R)$ or R is a finite dimensional central simple algebra and f is power-central valued.

Notice that in the special case when f is multilinear it was proved in [2] and [3] that if R is a prime ring with no non-zero nil right ideals then f must be power-central valued and R satisfies the standard identity of degree $n+2$.

In all that follows $f = f(x_1,\ldots,x_n)$ will denote a homogeneous polynomial of degree m, we assume also that d is a non-zero derivation on R which is C-linear (*i.e.* for all $c \in C$, $r \in R$ $d(cr) = cd(r)$) and satisfies the following condition:

$$d\big(f(r_1,\ldots,r_n)^t\big) = 0$$

for all $r_1,\ldots,r_n \in R$, $t = t(r_1,\ldots,r_n) \geq 1$. Moreover, if $\operatorname{char} R = p$ we assume that f is not a polynomial identity for $p \times p$ matrices in characteristic p. Finally, since throughout R will be a prime ring, we may assume that C is a domain and R is torsion free over C.

We begin with the case when f is power-central valued. We set as in [9]

$$\phi(m) = \left[\frac{\log(m[m/2]+1)}{\log 2}\right]([m/2]+1)$$

where $[x]$ is the integral part of the real number x.

We have the following theorem.

THEOREM 1. *Let R be a primitive ring, $f(x_1,\ldots,x_n)$ a homogeneous polynomial of degree m. If $\operatorname{char} R = p$ we also assume that f is not a polynomial identity for $p \times p$ matrices in characteristic p. If f is power-central valued in R then R is a finite dimensional central simple algebra. Let $N^2 = [R : Z(R)]$, then*

1) *either f is a polynomial identity for $(N-1) \times (N-1)$ matrices over $Z(R)$ and $N \leq \frac{1}{2}(m+2)$ or*
2) *$Z(R)$ is a finite field with $|Z(R)| \leq \phi(m)m$ and $N \leq \phi(m)+1$.*

PROOF. Since R is primitive, R is a dense ring of linear transformations on a vector space V over a division ring D.

Suppose that V is infinite dimensional over D; then, for every integer k, f is power-central valued on D_k, the ring of $k \times k$ matrices over D. We can regard D_{k-1} as the subring of D_k consisting of all $k \times k$ matrices with zero in the last row and last column. Thus $f(x_1,\ldots,x_n)$ is nil-valued on D_{k-1}. By [9] (Theorem 1.7, Corollary 1.8) either f is an identity of D_{k-1} or D_{k-1} is a finite ring and $f(x_1,\ldots,x_n)^{\phi(m)}$ is a polynomial identity on D_{k-1}. In any case we must have $2k \leq \phi(m)m+2$ for all k, and this is a contradiction.

Therefore $\dim_D V = t$ and so $R \simeq D_t$

If $t = 1$ then $R \simeq D$ is a division ring and by Theorem 3 2 of [9] R is finite dimensional over its center $Z(R)$ Also if $N^2 = [R \ \ Z(R)]$, f is an identity for $(N-1)\times(N-1)$ matrices over $Z(R)$, $f(x_1, \ \ , x_n)^N$ is a central polynomial on R and $N \leq \frac{1}{2}(m+2)$

Suppose now $t > 1$ The previous argument shows that f is nil-valued in $D_{t \ \ 1}$, hence f is an identity on D Thus $[D \ \ Z(D)] = r^2$ and $R \simeq D_t$ is a central simple algebra and $N^2 = (rt)^2 = [R \ \ Z(R)]$ Since f is power-central valued on R and the center of R is a field, f also has multinomial degree one on R (see Definition 0 2 of [9])

If $Z(R)$ is not algebraic over a finite field, then by Theorem 3 8 of [9] we can conclude that $N \leq \frac{1}{2}(m+2)$, f is an identity on $(N-1)\times(N-1)$ matrices over $Z(R)$, and $f(x_1, \ \ , x_n)^N$ is central on R

Finally suppose that $Z(R) = Z(D)$ is algebraic over a finite field P As $[D \ \ Z(D)] = r^2$ one has that every element a of D is algebraic over P Hence $P(a)$ is a finite field and so there exists an integer $s = s(a)$ greater than 1 such that $a^s = a$ By a result of Jacobson, this suffices to conclude that D is commutative ([6] Theorem 3 1 2) Therefore, in this case, $r = 1$, $N = t$ and $R \simeq Z_N$ As we said above f is nil-valued on $Z_{N \ \ 1}$ and so Theorem 1 7 of [9] again implies that either f is a polynomial identity on Z_{N-1} or Z is a finite field of order $|Z| \leq \phi(m)m$ and $N-1 \leq \phi(m)$

In any case N is bounded by an explicit function of the degree m of $f(x_1, \ \ , x_n)$ This completes the proof

REMARK 1 Let F be a finite field of order q and $R = F_N$ Assume $f(x_1, \ \ , x_n)$ is power-central valued on R and let $a = f(r_1, \ \ , r_n)$ for $r_1, \ \ , r_n \in R$ If $a^{s(a)} \in F$ then we have

1) either a is nilpotent, hence $s(a) \leq N$, or

2) a is invertible, and by Lagrange's Theorem $a^{|\mathrm{GL}(N \ F)|} = I$

As a result $f(x_1, \ \ , x_n)^M$ is a central polynomial on F_N, where

$$M = N|\,\mathrm{GL}(N,F)| = N \quad q^{\frac{1}{2}N(N-1)} \quad \prod_{i=1}^{N}(q^i - 1)$$

Moreover, either $f(x_1, \ \ , x_n)$ is a polynomial identity on F_{N-1} and so $N \leq \frac{1}{2}(m+2)$ or $N \leq \phi(m) + 1$ and $q \leq \phi(m)m$ with $m =$ degree of f

Notice that if d is the inner derivation induced by an element a of R then the condition $d\big(f(r_1, \ \ , r_n)^t\big) = 0$ for all $r_1, \ \ , r_n \in R$, $t = t(r_1, \ \ , r_n) \geq 1$ implies that a is in $T(R)$ which is $T(R) = \{a \in R \mid af(r_1, \ \ , r_n)^t = f(r_1, \ \ , r_n)^t a, t = t(a, r_1, \ \ , r_n)\}$ As quoted in [3], $T(R)$ is a subring of R containing $Z(R)$, invariant under all automorphisms of R, moreover we notice that the proof of Lemma 1 in [3] holds also for homogeneous polynomials, hence we have the following

LEMMA 1 *If D is a division ring then either $T(D) = Z(D)$ or $[D \ \ Z(D)] = N^2$, $f(x_1, \ \ , x_n)^N$ is central in D and $N \leq \frac{1}{2}(m+2)$*

REMARK 2 If $T(R) = R$ and R is an algebra finite dimensional over its center Z, then for $r_1, \ \ , r_n \in R$ there exists $t \geq 1$ such that $f(r_1, \ \ , r_n)^t$ centralizes a fixed basis of R over Z

Hence $f(r_1,\ldots,r_n)^t \in Z$, that is f is power-central valued.

We continue with:

LEMMA 2. *Let $R = \mathrm{GF}(2)_2$ be the ring of 2×2 matrices over* GF(2). *Then either $T(R) = Z(R)$ or $f(x_1,\ldots,x_n)^6$ is central in R.*

PROOF. We consider the following set-partition of R:

$$Z = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I \right\} \text{ the center of } R,$$

$$\mathcal{E} = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} \right\}$$

the set of non-central idempotents,

$$\mathcal{N} = \left\{ \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} \right\} \text{ the set of nilpotent elements and}$$

$$L = \left\{ a = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, b = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, c = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, u = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, v = \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \right\}$$

the set of non-central invertible elements of R.

We remark that the 6-th power of all elements of L lies in the center of R; in fact $a^2 = b^2 = c^2 = I$ and also $u^3 = v^3 = I$.

Hence, if $f(x_1,\ldots,x_n)$ is not power-central valued then there exist $s_1,\ldots,s_n \in R$ such that $f(s_1,\ldots,s_n) = e \in \mathcal{E}$.

If $a \in T(R)$, then a commutes with $f(s_1,\ldots,s_n)^l = e$ and for any automorphism β of R we also have $af(s_1^\beta,\ldots,s_n^\beta)^t = f(s_1^\beta,\ldots,s_n^\beta)^t a$, where t depends on $a, s_1,\ldots,s_n$ and β.

Since any two distinct elements of $\mathcal{E}$ are conjugate in R this implies that a centralizes all of $\mathcal{E}$. Let $\hat{\mathcal{E}}$ be the subring of R generated by $\mathcal{E}$; then the previous argument shows that either $f(x_1,\ldots,x_n)^6$ is a central polynomial in R or $T(R) \subseteq C(\mathcal{E}) = C(\hat{\mathcal{E}}) = Z(R)$ and this proves the lemma.

Now, we extend the previous result to primitive rings with a nontrivial idempotent. More precisely we have:

LEMMA 3. *Let R be a primitive ring with a nontrivial idempotent, $f(x_1,\ldots,x_n)$ a homogeneous polynomial of degree m. Then either $T(R) = Z(R)$ or $f(x_1,\ldots,x_n)$ is power-central valued in R (and the conclusion of Theorem 1 holds).*

PROOF. $T(R)$ is a subring of R invariant under all automorphisms of R; also, by Lemma 2, we may assume that $R \neq \mathrm{GF}(2)_2$. Hence, since R is a prime ring with a non-trivial idempotent, by [8, Theorem] either $T(R) = Z(R)$ or $T(R) \supset I$, a non-zero two-sided ideal of R.

Suppose then $T(R) \neq Z(R)$.

Since R is primitive, R is a dense ring of linear transformations on a vector space V over a division ring D; also I, as an ideal of R, is dense on V over D. Moreover $T(R) \supset I$ implies $T(I) = I$.

If V is finite dimensional over D, then $R \cong D_k$ and so $R = I$ and $T(R) = R$. Hence $T(D) = D$ and, by Lemma 1, D is finite dimensional over its center. It follows that R is finite dimensional central simple algebra and by Remark 2, f is power-central valued, as required

Suppose now that V is not finite dimensional over D If ϕ is the function described before Theorem 1, define an integer M as follows

$$M = \begin{cases} \frac{1}{2}(m+2)+1 & \text{if } Z(D) \text{ is an infinite field} \\ \phi(m)+2 & \text{otherwise} \end{cases}$$

Now, by [6, Theorem 2 1 4] D_M is a homomorphic image of a subring S of I Clearly $T(S) = S$ and so, $T(D_M) = D_M$ As above this implies that f is power-central valued in D_M and this, by Theorem 1, contradicts the choice of M

Next we are going to examine the general case concerning an arbitrary derivation d The first result is the following lemma, (see [2], [3] and Lemma 1)

LEMMA 4 *If R is a division ring then $f(x_1, \quad, x_n)$ is power-central valued and R is finite dimensional over its center*

PROOF Let $S = \{r \in R \mid d(r) = 0\}$, then for $x \in S$ we have

$$0 = d(1) = d(xx^{\ 1}) = d(x)x^{\ 1} + xd(x^{\ 1}) = xd(x^{\ 1})$$

which implies $d(x^{-1}) = 0$, that is $x^{\ 1} \in S$, so that S is a proper subdivision ring of R, moreover for all $r_1, \quad, r_n \in R$ there exists $t = t(r_1, \quad, r_n) \geq 1$ such that $f(r_1, \quad, r_n)^t \in S$

Let $r = f(r_1, \quad, r_n)$, if $x \in R - S$ we can choose $t \geq 1$ such that $r^t \in S$, $(xrx^{-1})^t = \left(xf(r_1, \quad, r_n)x^{-1}\right)^t = f(xr_1x^{-1}, \quad, xr_nx^{\ 1})^t \in S$ and $\left((1+x)r(1+x)^{\ 1}\right)^t \in S$

Thus, using a Brauer-Cartan-Hua type argument, for some $a, b \in S$ we have

$$\text{(I)} \qquad xr^t = ax$$
$$(1+x)r^t = b(1+x)$$

Subtracting we get $r^t = b + (b-a)x$, hence $(b-a)x \in S$ Since S is a subdivision ring of R and $x \notin S$ then $a = b$

From (I) we deduce $xr^t = r^t x$

Let now $y \in S$ By the first part of the proof we have $(x+y)r^{t'} = r^t(x+y)$ for a suitable t' Since $xr^{tt'} = r^{tt'}x$ we get $yr^{tt} = r^{tt'}y$ Therefore $T(R) = R$ and by Lemma 1 f is power-central valued and $[R \quad Z(R)] \leq \frac{1}{2}(m+2)$

We continue with

LEMMA 5 *Let R be a prime ring and suppose that $T(R) = Z(R)$ If $t \in R$ is such that $t^2 = 0$ then $d(t) = 0$*

PROOF Let $0 \neq t \in R$ be such that $t^2 = 0$, then the map $\eta_t \ R \longrightarrow R$ defined by $\eta_t(r) = r + tr - rt + trt$ is an automorphism of R Even if R does not have a unit element we write $\eta_t(r) = (1+t)r(1-t)$ and also $(1+t)r = r + tr$ or $r(1+t) = r + rt$

Let $x = f(r_1, \ldots, r_n)$; there exists $s \geq 1$ such that $d(x^s) = 0$ and $d\Big((1+t)x^s(1-t)\Big) = d\Big(\big((1+t)x(1-t)\big)^s\Big) = 0$. Thus $d\Big((1+t)x^s(1-t)(1+t)\Big) = d\Big((1+t)x^s\Big) = d(t)x^s$ and $d\Big((1+t)x^s(1-t)(1+t)\Big) = (1+t)x^s(1-t)d(t)$. Therefore $(1-t)d(t)x^s = x^s(1-t)d(t)$, that is $(1-t)d(t) = z$ for some $z \in T(R) = Z(R)$, and so $d(t) = z(1+t)$.

It follows that $0 = d(t^2) = td(t) + d(t)t = 2zt$. If $\operatorname{char} R \neq 2$ then $zt = 0$. Moreover since $z \in Z(R)$ either $z = 0$ or z is not a zero divisor in R; in any case $d(t) = 0$.

Now we suppose that $\operatorname{char} R = 2$ and we split the proof into two different cases: $Z(R) \neq \mathrm{GF}(2)$ or $Z(R) = \mathrm{GF}(2)$.

CASE 1: $Z(R) \neq \mathrm{GF}(2)$. Let $\gamma \in Z(R) - \{0, 1\}$. Then $d(\gamma^2 t) = z'(1 + \gamma^2 t)$ for some $z' \in Z(R)$. Since $d(\gamma^2) = \gamma d(\gamma) + d(\gamma)\gamma = 2\gamma d(\gamma) = 0$ we also have $d(\gamma^2 t) = \gamma^2 d(t) = \gamma^2 z(1+t)$. So we get $z'(1+\gamma^2 t) = \gamma^2 z(1+t)$. Hence $\gamma^2(z'-z)t \in Z(R)$. As t is not a central element of the prime ring R, this implies $z = z'$. Thus $z = \gamma^2 z$ and so $(\gamma^2+1)z = 0$. Since $\gamma^2 + 1 \neq 0$ we get $z = 0$ and, once again, $d(t) = 0$.

CASE 2: $Z(R) = \mathrm{GF}(2)$. Suppose that $d(t) \neq 0$ for some $t \in R$ with $t^2 = 0$. By the first part of the proof, $d(t) = 1 + t$. If $r \in R$ then $(trt)^2 = 0$. Hence $d(trt) = 0$ or $d(trt) = 1 + trt$ again. But $d(trt) = d(tr)t + trd(t) = d(tr)t + tr(1+t)$; hence $d(trt)t = trt$. However, as we mentioned above, $d(trt) = 0$ or $d(trt) = 1 + trt$. Hence $trt = d(trt)t = 0$ or $trt = t$.

As a consequence $tRt = \mathrm{GF}(2)t$.

If $0 \neq a \in tR$ then $0 \neq aRt \subseteq tRt = \mathrm{GF}(2)t$ and so $t \in aRt$. Hence $aR = tR$ for all $0 \neq a \in tR$ and this says that tR is a minimal right ideal of R. Thus R is a primitive ring with minimal right ideal tR. Moreover its commuting ring is GF(2) as $tRt = \mathrm{GF}(2)t$. If $I \neq 0$ is an ideal of R then $tIt \neq 0$. Hence $tit \neq 0$ for some $i \in I$; thus $tit = t$ and so $t \in I$. Since I^2 is a nonzero ideal of R, $t \in I^2$. Hence $1 + t = d(t) \in d(I^2) \subseteq d(I)I + Id(I) \subseteq I$. Together with $t \in I$ this implies that $1 \in I$ and so $I = R$. In other words R is simple. Since R is simple with 1 and has a minimal right ideal, R is simple artinian and since the commuting ring of R is GF(2), by Wedderburn's theorem we conclude that $R \simeq \mathrm{GF}(2)_k$ for some $k \in \mathbb{N}$ [7]. But in this case, as proved by Jacobson, any derivation is an inner derivation (see p. 100 of [6]) and by Lemma 3 we obtain $d = 0$ which is a contradiction.

We now settle the case when R contains a nontrivial idempotent.

LEMMA 6. *Let R be a primitive ring with a nontrivial idempotent. Then $f(x_1, \ldots, x_n)$ is power-central valued.*

PROOF. Suppose that $R = \mathrm{GF}(2)_2$. Then, as we quoted above, d is the inner derivation induced by a certain element a of R. As $d \neq 0$, $a \notin Z(R)$. Hence $T(R) \neq Z(R)$ and by Lemma 2 $f(x_1, \ldots, x_n)^6$ is a central polynomial on R.

Assume now that $R \neq \mathrm{GF}(2)_2$ and let A be the subring generated by all square zero elements of R. A is invariant under all automorphisms of R. Since R is a prime ring with a nontrivial idempotent, by [8, Theorem], A contains a nonzero ideal I of R. On the other hand, by Lemma 3 either $T(R) = Z(R)$ or f is power-central valued.

https://doi.org/10.4153/CJM-1993-003-4 Published online by Cambridge University Press

In the first case by Lemma 5 $d(x) = 0$ for all $x \in A$ and so $d(I) = 0$. Now, since $0 = d(I) \supseteq d(IR) = Id(R)$, by the primeness of R we obtain $d(R) = 0$ which is a contradiction. Hence in any case f is power-central valued on R and R is a finite dimensional central simple algebra.

Finally we have:

THEOREM 2. *Let R be a primitive ring, $f(x_1, \ldots, x_n)$ a homogeneous polynomial of degree m. Suppose that d is a nonzero derivation on R such that for all $r_1, \ldots, r_n \in R$ there exists $t \in \mathbb{N}$, $t = t(r_1, \ldots, r_n)$, with $d\big(f(r_1, \ldots, r_n)^t\big) = 0$. If* char $R = p > 0$ *we assume that f is not an identity for $p \times p$ matrices in characteristic p. Then $f(x_1, \ldots, x_n)$ is power-central valued and R is a finite dimensional central simple algebra. Let $N^2 = [R : Z(R)]$; then*

1) *either f is a polynomial identity for $(N-1) \times (N-1)$ matrices over $Z(R)$ and $N \leq \frac{1}{2}(m+2)$ or*
2) *$Z(R)$ is a finite field with $|Z(R)| \leq \phi(m)m$ and $N \leq \phi(m) + 1$.*

Moreover, if $f(x_1, \ldots, x_n)$ is not a polynomial identity on R then either d is an inner derivation or $Z(R)$ is infinite of characteristic $p \neq 0$.

PROOF. Let V be a faithful irreducible right R-module with endomorphism ring D a division ring. First we assume that V is infinite dimensional over D and R does not contain a nontrivial idempotent. This says that R does not have nonzero linear transformations of finite rank.

We will prove that these assumptions lead to a contradiction.

Let $vr = 0$ for some $v \in R$ and $r \in R$, and suppose that $vd(r) \neq 0$. Since r has infinite rank, there exist $w_1, \ldots, w_n \in \operatorname{Im} r$ such that $vd(r), w_1, \ldots, w_n$ are linearly independent and let $v_1, \ldots, v_n \in V$ such that $w_i = v_i r$, $i = 1, \ldots, n$.

Let $M = M(x_1, \ldots, x_n)$ be a nonzero monomial of $f(x_1, \ldots, x_n)$ and let $\deg_{x_i} M(x_1, \ldots, x_n) = m_i \geq 1$, hence $m_1 + \cdots + m_n = m = \deg f$.

By considering the order of the x_i's in $M(x_1, \ldots, x_n)$ we construct a partition of $\mathcal{A} = \{1, \ldots, m\}$ in n disjoint subsets, one for each x_i. More precisely we define, for $i = 1, \ldots, n$, the subset $\mathcal{A}_i$ of $\mathcal{A}$ in the following way:

$$j \in \mathcal{A}_i \Leftrightarrow M = M_j x_i M'_j$$

where $M_j = M_j(x_1, \ldots, x_n)$ has degree $j-1$ and $M'_j = M'_j(x_1, \ldots, x_n)$ has degree $m-j$. In other words, in the ordered monomial M, $\mathcal{A}_i$ is the set of positions in which x_i occurs.

We can assume that $1 \in \mathcal{A}_1$, that is $M = \alpha x_1 M'_1$, where $M_1 = \alpha \in C$, and we let for convenience $v_{n+1} = v_1$. By the Jacobson density theorem there exist $a_1, \ldots, a_n \in R$ such that, for $i = 1, \ldots, n$

$$w_j a_i = \begin{cases} v_{j+1} & \text{if } j \in \mathcal{A}_i \\ 0 & \text{otherwise} \end{cases}$$

and moreover, since $vd(r), w_1, \ldots, w_n$ are linearly independent, we can set $vd(r)a_1 = v_2$ and $vd(r)a_i = 0$ for $i = 2, \ldots, n$.

We remark that if $j \in \mathcal{A}_t$ then

$$M_{j+1}(x_1,\ldots,x_n) = M_j(x_1,\ldots,x_n)x_t \text{ and}$$
$$M'_{j-1}(x_1,\ldots,x_n) = x_t M'_j(x_1,\ldots,x_n).$$

Hence $v_j M'_{j-1}(ra_1,\ldots,ra_n) = v_j r a_t M'_j(ra_1,\ldots,ra_n) = w_j a_t M'_j(ra_1,\ldots,ra_n) = v_{j+1}M'_j(ra_1,\ldots,ra_n)$. Therefore we have

$$\begin{aligned} v_1 M(ra_1,\ldots,ra_n) &= \alpha v_1 r a_1 M'_1(ra_1,\ldots,ra_n) \\ &= \alpha v_2 M'_1(ra_1,\ldots,ra_n) \\ &= \alpha v_3 M'_2(ra_1,\ldots,ra_n) \\ &\;\vdots \\ &= \alpha v_n M'_{n-1}(ra_1,\ldots,ra_n) \\ &= \alpha v_n r a_s \\ &= \alpha v_1. \end{aligned}$$

In a similar way we can prove that

$$v_1 M_j(ra_1,\ldots,ra_n) = \alpha v_j \text{ for } j = 1,\ldots,n.$$

On the other hand if $N(x_1,\ldots,x_n)$ is a monomial of f different from M then $v_1 N(ra_1,\ldots,ra_n) = 0$. In fact, let $1 \le j \le m$ be the smallest integer such that $N = M_j x_t N'$ and $M = M_j x_i M'_j$ with $t \neq i$. Since $j \in \mathcal{A}_i$ and $\mathcal{A}_i \cap \mathcal{A}_t = \emptyset$ we have $j \notin \mathcal{A}_t$ and so $w_j a_t = 0$. Hence

$$\begin{aligned} v_1 N(ra_1,\ldots,ra_n) &= v_1 M_j(ra_1,\ldots,ra_n) r a_t N'(ra_1,\ldots,ra_n) \\ &= \alpha v_j r a_t N'(ra_1,\ldots,ra_n) = \alpha w_j a_t N'(ra_1,\ldots,ra_n) = 0 \end{aligned}$$

Therefore $v_1 f(ra_1,\ldots,ra_n) = \alpha v_1$.

Now we will calculate $vd\big(f(ra_1,\ldots,ra_n)\big)$. As above, since $1 \in \mathcal{A}_1$,

$$\begin{aligned} vd\big(M(ra_1,\ldots,ra_n)\big) &= \alpha vd\big(ra_1 M'_1(ra_1,\ldots,ra_n)\big) \\ &= \alpha vd(r) a_1 M'_1(ra_1,\ldots,ra_n) + \alpha v r d\big(a_1 M'_1(ra_1,\ldots,ra_n)\big) \\ &= \alpha vd(r) a_1 M'_1(ra_1,\ldots,ra_n) \\ &= \alpha v_2 M'_1(ra_1,\ldots,ra_n) \\ &\;\vdots \\ &= \alpha v_1. \end{aligned}$$

Let $N(x_1,\ldots,x_n)$ be another monomial of f and let $1 \le j \le m$ be the smallest integer such that $N = M_j x_t N'$ and $M = M_j x_i M'_j$ with $t \neq j$.

If $j=1$, then

$$\begin{aligned} vd\big(N(ra_1,\ldots,ra_n)\big) &= vd\big(\alpha ra_t N'(ra_1,\ldots,ra_n)\big) \\ &= \alpha vd(r)a_t N'(ra_1,\ldots,ra_n) + \alpha vrd\big(a_t N'(ra_1,\ldots,ra_n)\big) \\ &= 0, \end{aligned}$$

as $vr=0$ and $t\neq 1$. If $j>1$, then we can write

$$M_j(x_1,\ldots,x_n) = x_1 M_j''(x_1,\ldots,x_n)$$

with $\deg M_j''(x_1,\ldots,x_n) = j-2$; hence

$$\begin{aligned} vd\big(N(ra_1,\ldots,ra_n)\big) &= vd\big(\alpha ra_1 M_j''(ra_1,\ldots,ra_n) ra_t N'(ra_1,\ldots,ra_n)\big) \\ &= \alpha vd(r)a_1 M_j''(ra_1,\ldots,ra_n) ra_t N'(ra_1,\ldots,ra_n) \\ &\quad + \alpha vrd\big(a_1 M_j''(ra_1,\ldots,ra_n) ra_t N'(ra_1,\ldots,ra_n)\big) \\ &= \alpha v_2 M_j''(ra_1,\ldots,ra_n) ra_t N'(ra_1,\ldots,ra_n) \\ &= \alpha v_j ra_t N'(ra_1,\ldots,ra_n) \\ &= \alpha w_j a_t N'(ra_1,\ldots,ra_n) \\ &= 0, \end{aligned}$$

as $w_j a_t = 0$.

This proves that $vd\big(f(ra_1,\ldots,ra_n)\big) = \alpha v_1$. Now, let $s\geq 1$ be such that $d\big(f(ra_1,\ldots,ra_n)^s\big)=0$. Hence we have

$$\begin{aligned} 0 &= vd\big(f(ra_1,\ldots,ra_n)^s\big) \\ &= \sum_{p+q=s-1} vf(ra_1,\ldots,ra_n)^p d\big(f(ra_1,\ldots,ra_n)\big) f(ra_1,\ldots,ra_n)^q \\ &= vd\big(f(ra_1,\ldots,ra_n)\big) f(ra_1,\ldots,ra_n)^{s-1} \\ &= \alpha v_1 f(ra_1,\ldots,ra_n)^{s-1} \\ &\;\vdots \\ &= \alpha^s v_1, \end{aligned}$$

a contradiction.

Thus if $vr=0$, $vd(r)=0$.

Let $0\neq v\in V$ and suppose that vr and $vd(r)$ are linearly dependent for all $r\in R$. Let $x,y\in R$ be such that vx and vy are linearly independent. Then $vd(x)=\lambda_x vx$, $vd(y)=\lambda_y vy$ and $vd(x+y)=\lambda_{x+y}v(x+y)$, where λ_x, λ_y, λ_{x+y} are in D. Therefore $\lambda_{x+y}vx+\lambda_{x+y}vy = \lambda_x vx+\lambda_y vy$, and thus $\lambda_x=\lambda_y$. As a result there exists $\lambda\in D$ such that $vd(x)=\lambda vx$ for all $x\in R$, with $vx\neq 0$. On the other hand, as we proved above, if $vr=0$ then $vd(r)=0$. Hence $vd(x)=\lambda vx$ for all $x\in R$.

https://doi.org/10.4153/CJM-1993-003-4 Published online by Cambridge University Press

Since V is infinite dimensional over D, there exist $v_2, \dots v_n \in V$ such that $v, v_2, \dots, v_n$ are linearly independent, and we let for convenience $v = v_1 = v_{n+1}$. By the Jacobson density theorem again, there exist $b_1, \dots, b_n \in R$ such that, for $i = 1, \dots, n$

$$v_j b_i = \begin{cases} v_{j+1} & \text{if } j \in \mathcal{A}_i \\ 0 & \text{otherwise} \end{cases}$$

where the $\mathcal{A}_i$'s are the sets defined above. As above we can easily prove that $vf(b_1, \dots, b_n) = \alpha v$ and so $vf(b_1, \dots, b_n)^s = \alpha^s v$ for all $s \in \mathbb{N}$.

Now, for some $s \in \mathbb{N}, f(b_1, \dots, b_n)^s \in S = \{x \in R \mid d(x) = 0\}$. Hence there is $x \in S$ such that $vx \neq 0$ and we obtain $0 = vd(x) = \lambda vx$ and so $\lambda = 0$.

Thus if vr and $vd(r)$ are linearly dependent for all $v \in V$ and $r \in R$, then $Vd(R) = 0$ and so $d = 0$.

Therefore we may assume that there exist $v \in V$, $r \in R$ such that vr and $vd(r)$ are linearly independent. Let $a \in R$ such that $(vr)a = 0$ and $\big(vd(r)\big)a \neq 0$. By the above $0 = (vr)a = v(ra)$ implies $(vr)d(a) = 0$ and also $vd(ra) = 0$; hence $0 = vd(ra) = vd(r)a + vrd(a) = vd(r)a \neq 0$, a contradiction. Thus either V is finite dimensional over D and $R \simeq D_k$ or R contains a nontrivial idempotent.

This, together with Lemma 4 and Lemma 6, suffices to prove that $f(x_1, \dots, x_n)$ is power-central valued on R and R is a finite dimensional central simple algebra. Moreover $[R : Z(R)]$ is bounded as in Theorem 1 by an explicit function of the degree of $f(x_1, \dots, x_n)$.

Finally, by a result of Jacobson [6, p. 100], either d is an inner derivation or $d\big(Z(R)\big) \neq 0$. In this case, for all $r_1, \dots, r_n \in R$ and z in $Z(R)$, we can choose $t \geq 1$ such that $d\big(f(zr_1, \dots, zr_n)^t\big) = 0$ and $d\big(f(r_1, \dots, r_n)^t\big) = 0$. Thus

$$\begin{aligned} 0 &= d\big(f(zr_1, \dots, zr_n)^t\big) \\ &= d\big(z^{mt} f(r_1, \dots, r_n)^t\big) \\ &= d(z^{mt}) f(r_1, \dots, r_n)^t + z^{mt} d\big(f(r_1, \dots, r_n)^t\big) \\ &= d(z^{mt}) f(r_1, \dots, r_n)^t. \end{aligned}$$

Since R is primitive this implies that either $f(x_1, \dots, x_n)$ is nil-valued on R or $d(z^{mt}) = 0$ for all $z \in Z(R)$ with $t = t(z)$.

If $f(x_1, \dots, x_n)$ is not a polynomial identity on R, by Theorem 1.7 of [9], we must have that $Z(R)$ is a finite field and so $d\big(Z(R)\big) = 0$.

Therefore we obtain that $d(z^s) = 0$ for all $z \in Z(R)$, and $s = s(z)$ depends on z. Of course this implies that $Z(R)$ is infinite of characteristic $p \neq 0$; and this completes the proof.

As quoted above we can interpret the case of the inner derivations in terms of elements of $T(R)$. Hence we obtain the following result which is of some independent interest:

COROLLARY. *Let R be a primitive ring, $f(x_1, \dots, x_n)$ a homogeneous polynomial of degree m. If* char $R = p > 0$ *we assume that f is not an identity for $p \times p$ matrices in* *characteristic p. Then either $T(R) = Z(R)$ or $f(x_1, \ldots, x_n)$ is power-central valued and R is a finite dimensional central simple algebra. In the last case let $N^2 = [R : Z(R)]$, then*

1) either f is a polynomial identity for $(N-1) \times (N-1)$ matrices over $Z(R)$ and $N \leq \frac{1}{2}(m+2)$ or

2) $Z(R)$ is a finite field with $|Z(R)| \leq \phi(m)m$ and $N \leq \phi(m) + 1$.

REFERENCES

1. J Bergen and A Giambruno, *f-radical extensions of rings*, Rend Sem Mat Univ Padova **77**(1987), 125–133

2. O M Di Vincenzo, *Derivations and multilinear polynomials*, Rend Sem Mat Univ Padova **81**(1989), 209–219

3. B Felzenszwalb and A Giambruno, *Centralizers and multilinear polynomials in non-commutative rings*, J London Math Soc (2) **19**(1979), 417–428

4. ———, *Periodic and nil polynomials in rings*, Canad Math Bull (4) **23**(1980), 473–476

5. A Giambruno, *Rings f-radical over P I subrings*, Rend Mat Roma (1) (VI) **13**(1980), 105–113

6. I N Herstein, *Noncommutative rings*, Carus Mathematical Monographs, Math Assoc Amer 1968

7. ———, *Rings with involution*, Univ Chicago Press, Chicago, 1976

8. ———, *A Theorem on invariant subrings*, J Algebra **83**(1983), 26–32

9. I N Herstein, C Procesi and M Shacher, *Algebraic valued functions on noncommutative rings*, J Algebra **36**(1975), 128–150

10. L H Rowen, *Polynomial identities in ring theory*, Academic Press, New York, 1973

Dipartimento di Matematica
Università della Basilicata
via N Sauro 85
85100 Potenza
Italy

Dipartimento di Matematica
Università di Palermo
via Archirafi 34
90123 Palermo
Italy

https://doi.org/10.4153/CJM-1993-003-4 Published online by Cambridge University Press