Canad. Math. Bull. Vol. **37** (1), 1994 pp. 124–132

DERIVATIONS WHOSE ITERATES ARE ZERO OR INVERTIBLE ON A LEFT IDEAL

BEN TILLY

ABSTRACT. Let $n \in \mathbb{Z}^+$ and R be a ring which possesses a unit element, a left ideal J, and a derivation d such that $d^n(J) \neq 0$ and $d^n(r)$ is 0 or invertible, for all $r \in J$. We prove that either R is primitive, in which case R is D_i with $1 \leq i \leq n+1$, where D_i is the ring of $i \times i$ matrices over a division ring D, or else there exist positive integers i, ℓ and p with p prime and $2 \leq ip^\ell \leq n+1$, such that R is $D_i[x_1, x_2, \ldots, x_\ell]/(x_1^p, x_2^p, \ldots, x_\ell^p)$, where D is a division ring with characteristic p, and furthermore there is a derivation f of D_i and $a_1, a_2, \ldots, a_\ell \in Z_{D_i}$, the center of D_i, such that $a \in D_i$ then

$$d(a) = f(a)x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1},$$
$$d(x_1) = 1 + a_1x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1},$$

and

$$d(x_j) = x_1^{p-1}x_2^{p-1}\cdots x_{j-1}^{p-1} + a_jx_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1}$$

for all $2 \leq j \leq \ell$.

Bergen, Herstein and Lanski [1] have related the structure of a ring R to the special behavior of one of its derivations. More precisely, they proved that if R is a ring with unit and $d \neq 0$ is a derivation of R such that for every $r \in R$, $d(r) = 0$ or $d(r)$ is invertible in R, then R must be a division ring D, the ring D_2 of 2×2 matrices over a division ring D, or else $D[x]/(x^2)$ where D has characteristic 2, $d(D) = 0$, and $d(x) = 1 + ax$ for some a in the centre of D.

For the entire paper we shall assume that $n \in \mathbb{Z}^+$, R is a ring with unit, J is a left ideal of R, and d is a derivation of R with $d^n(J) \neq 0$ such that for every $r \in J$, $d^n(r) = 0$ or $d^n(r)$ is invertible in R. The results we will obtain are similar to those of (1). In fact we shall prove the following:

THEOREM 1. *Let $n \in \mathbb{Z}^+$, R be a ring with unit, J a left ideal of R, and d a derivation of R such that $d^n(J) \neq 0$ and $d^n(r) = 0$ or $d^n(r)$ is invertible, for every $r \in J$. Then there exists a division ring D such that R is either*

1) *D_i, the ring of $i \times i$ matrices over a division ring D with $1 \leq i \leq n+1$, or*
2) *$D_i[x_1, x_2, \ldots, x_\ell]/(x_1^p, x_2^p, \ldots, x_\ell^p)$ where $i, \ell, p \in \mathbb{Z}^+$, p is prime, $2 \leq ip^\ell \leq n+1$, and* char $D = p$.

Furthermore, there exists a derivation f of D_i and $a_1, a_2, \ldots, a_\ell \in Z_{D_i}$, the center of D_i, with $d(a) = f(a)x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1}$ for all $a \in D_i$,

$$d(x_1) = 1 + a_1x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1},$$

The author wishes to acknowledge the support of Dr. C. R. Miers through NSERC Grant A-7682.
Received by the editors March 13, 1992.
AMS subject classification: Primary: 16W25; secondary: 16N60.

and

$$d(x_j) = x_1^{p-1}x_2^{p-1}\cdots x_{j-1}^{p-1} + a_j x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1} \quad \text{for } j = 2,3,\ldots,\ell.$$

Let us start with an easy generalization of a lemma from [1].

LEMMA 1. *If* $0 \neq a \in R$ *and* $d(a) = 0$ *then* a *is invertible.*

PROOF. As $d^n(J) \neq 0$ $\exists r \in J$ with $d^n(r) \neq 0$ so $d^n(r)$ is invertible. Now $d^n(ar) = \sum_{i=0}^n \binom{n}{i} d^{n-i}(a)d^i(r) = ad^n(r)$ as $0 = d(a) = d^2(a) = \cdots$. Now $ar \in J$ and $ad^n(r) \neq 0$ because $ad^n(r)\big(d^n(r)\big)^{-1} = a \neq 0$ so $ad^n(r) = d^n(ar)$ is invertible. As $d^n(R)$ is invertible, a is invertible. ■

Before our next lemma, note that R is a ring with unit so R has a maximal ideal I and R/I is primitive so we may let V be a faithful irreducible left R/I-module with commuting division ring D. By the Jacobson density theorem R/I is dense on V considered as a vector space over D. But then V is an irreducible left R-module with $\mathrm{Ann}_R(V) = I$ where $\mathrm{Ann}_R(V) = \{r \in R \mid rV = \{0\}\}$. Note also that R and D commute and R is dense on V considered as a vector space over D. From now on I, V and D will be fixed.

Let W be some finite dimensional D-subspace of V. If $a \in R$ define $W_0(a) = W$ and for $0 \leq i$, $W_{i+1}(a) = W \cap \Big(\bigcap_{j=0}^i \mathrm{Ker}\big(d^j(a)\big)\Big)$ where $d^0(a) = a$. It is not hard to show that for $r, s \in R$ and $i \in \{0,1,2,\ldots\}$, if $d^j(r)w = d^j(s)w$ $\forall 0 \leq j < i$ and $w \in W_j(r)$ then $W_i(r) = W_i(s)$.

LEMMA 2. *If* $0 \neq a \in J$ *then* $W_{n+1}(a) = 0$.

PROOF. Since $d^n(a) = 0$ or is invertible it is clear from Lemma 1 that $R = Ra + Rd(a) + \cdots + Rd^n(a)$. It is trivial that $0 = d^j(a)W_{n+1}(a)$ for $j = 0,1,\ldots,n$ so we have $0 = RaW_{n+1}(a) + Rd(a)W_{n+1}(a) + \cdots + Rd^n(a)W_{n+1}(a) = RW_{n+1}(a)$ so $W_{n+1}(a) = 0$ because V is irreducible. ■

LEMMA 3. *Let* $0 \neq r \in R$, $0 \neq v \in V$, *and* $i \in \{0,1,2,\ldots\}$. *Then* $\exists a \in Rr$ *with* $a \neq 0$ *such that* $d^j(a)W_j(a) \subseteq Dv$ *for* $j = 0,1,\ldots,i$.

PROOF: INDUCTION ON i. If $i = 0$ then $W_j(a) = W_0(a) = W$. Since W is finite dimensional so is rW. If $rW = 0$ then trivially let $a = r$. If $rW \neq 0$ then, by the density of R, choose $b \in R$ such that $brW = Dv$ and set $a = br$. Then $aW_0(a) = aW \subseteq Dv$ and $a \neq 0$.

Suppose the result holds for i and choose $0 \neq s \in Rr$ such that $d^j(s)W_j(s) \subseteq Dv$ $\forall 0 \leq j \leq i$. Now if $d^{i+1}(s)W_{i+1}(s) = 0 \subseteq Dv$ then take $a = s$. Therefore without loss of generality assume that $d^{i+1}(s)W_{i+1}(s) \neq 0$. As W is finite dimensional $d^{i+1}(s)W_{i+1}(s)$ is also so by density $\exists b \in R$ such that $bd^{i+1}(s)W_{i+1}(s) = Dv$ and $bv = v$. Now for $0 \leq j \leq i+1$ and $w \in W_j(s)$ note that $d^j(bs)w = \sum_{k=0}^j \binom{j}{k} d^{j-k}(b)d^k(s)w$ but if $k < j$ then $d^k(s)w = 0$ so

$$d^j(bs)w = bd^j(s)w. \tag{1}$$

https://doi.org/10.4153/CMB-1994-018-7 Published online by Cambridge University Press

Now if $j \leq i$ then $d^j(s)w \in Dv$ so $d^j(s)w = \alpha v$ for some $\alpha \in D$. But then from (1) we get

$$(2) \qquad d^j(bs)w = bd^j(s)w = b\alpha v = \alpha bv = \alpha v = d^j(s)w.$$

From (2) and the comment before Lemma 2 we get that $W_k(s) = W_k(bs)\ \forall 0 \leq k \leq i+1$. Now let $a = bs$. Then $a \in Rs \subseteq Rr$, by (1) we get $d^{i+1}(a)W_{i+1}(a) = bd^{i+1}(s)W_{i+1}(s) = Dv \neq 0$ so $a \neq 0$ and $d^{i+1}(a)W_{i+1}(a) \subseteq Dv$, and if $0 \leq j \leq i$ then from (2), $d^j(a)W_j(a) = bd^j(s)W_j(s) = d^j(s)W_j(s) \subseteq Dv$. Therefore the result holds for $i+1$. ∎

LEMMA 4. *$R/I \cong D_i$ for some $1 \leq i \leq n+1$ where $i = \dim_D(V)$.*

PROOF. Let W be an arbitrary finite-dimensional D-subspace of V. As $d^n(J) \neq 0$, $\exists$ a nonzero $r \in J$. Also $\exists$ a nonzero $v \in V$ so take $i = n$ and a as in Lemma 3. For $0 \leq j \leq n$, $d^j(a)\colon W_j(a) \longrightarrow V$ is a D-linear map with kernel $W_{j+1}(a)$ and range contained in Dv. Hence

$$\begin{aligned}\dim_D(W) &= \dim_D\big(W_0(a)\big)\\ &= \dim_D\big(W_1(a)\big) + \dim_D\big(aW_0(a)\big) = \cdots = \dim_D\big(W_{n+1}(a)\big)\\ &\quad + \sum_{j=0}^{n} \dim_D\big(d^j(a)W_j(a)\big) \leq \dim_D\big(W_{n+1}(a)\big) + n + 1.\end{aligned}$$

By Lemma 2, $W_{n+1}(a) = 0$ so $\dim_D(W) \leq n+1$. Since W is an arbitrary finite dimensional D-subspace of V and $V \neq 0$ we have $1 \leq \dim_D(V) \leq n+1$. Now take $i = \dim_D(V)$ and by the density of R/I on V with V a faithful irreducible R/I-module we get $R/I \cong D_i$. ∎

In all that follows $i = \dim_D(V)$. If $I = 0$ there is nothing left to prove in the theorem, so we will assume from now on that $I \neq 0$. Note again that $\mathrm{Ann}_R(V) = I$. Now define $I_0 = R$ and for $0 \leq j$, $I_j = \bigcap_{k=0}^{j} d^{-k}(I)$ where $d^{-k}(I) = \{r \in R \mid d^k(r) \in I\}$. It is immediate that $d(I_j) \subseteq I_{j-1}$ and that I_j is an ideal. At this point we will develop some properties of I_j.

LEMMA 5. *If $j \in \{0,1,2,\ldots\}$, $r \in R$, and $a \in I_J \setminus I_{j+1}$ then $d^j(RaR) \cap (r+I) \neq \emptyset$.*

PROOF. Let $\varphi\colon R \longrightarrow R/I$ by $\varphi(r) = r+I$. Now $a \in I_j \setminus I_{j+1}$ so $d^j(a) \notin I$ so $\varphi\big(d^j(a)\big) \neq 0$. As I is maximal R/I is simple so $r + I \in (R/I)\,\varphi\big(d^j(a)\big)(R/I) = \varphi\big(Rd^j(a)R\big) = \varphi\big(d^j(RaR)\big)$ because $d^j(IaR) \subseteq Id^j(aR) + I \subseteq I$ with $a \in I_j$ and similarly $d^j(RaI) \subseteq I$. $\therefore d^j(RaR) \cap (r+I) \neq \emptyset$. ∎

LEMMA 6. *There is a largest m such that $I_m \cap J \neq 0$. Furthermore $1 \leq m \leq n$, $I_{m+1} = 0$ and for $0 \leq j$, $I_{j+1}d^j(I_m \cap J) = 0$.*

PROOF. If $0 \neq r \in I_{n+1} \cap J$ then $R = Rr + Rd(r) + \cdots + Rd^n(r) \subseteq I$ so since I is a proper ideal of R, $I_{n+1} \cap J = 0$. As $I_0 \cap J = J \neq 0$ we have that m exists and $0 \leq m \leq n$. Let $J_m = I_m \cap J$. Now $IJ_m \subseteq I_{m+1} \cap J = 0$ so for $j = 0$, $I_{j+1}d^j(I_m \cap J) = 0$. If $I_{j+1}d^j(I_m \cap J) = 0$ then $0 = d\big(I_{j+2}d^j(J_m)\big) = I_{j+2}d^{j+1}(J_m)$ as $d(I_{j+2})d^j(J_m) \subseteq I_{j+1}d^j(J_m)$. Thus by induction for $0 \leq j$, $I_{j+1}d^j(I_m \cap J) = 0$. Now

$$\begin{aligned}I_{n+1} &= I_{n+1}R = I_{n+1}\big(RJ_m + Rd(J_m) + \cdots + Rd^n(J_m)\big)\\ &\subseteq I_1J_m + I_2d(J_m) + \cdots + I_{n+1}d^n(J_m) = 0\end{aligned}$$

https://doi.org/10.4153/CMB-1994-018-7 Published online by Cambridge University Press

If $I_{m+1} = I_{n+1} = 0$ then m cannot be zero because $I \neq 0$ so we would be done. Now let j be the largest j such that $I_j \neq I_{j+1}$. If $j > m$ then by Lemma 5 choose $a \in I_j \setminus I_{j+1}$ such that $d^j(a) \in 1 + I$. As $a \in I_{m+1}$, $ad^m(J_m) = 0$. As for $k < j$, $d^k(a) \in I$ we have

$$0 \equiv d^j\big(ad^m(J_m)\big) \equiv d^j(a)\, d^m(J_m) \equiv d^m(J_m) \pmod I$$

and $J_m \subseteq I_m$ so $0 \neq J_m \subseteq I_{m+1} \cap J = 0$. As this is impossible, $j \leq m$. Therefore $I_{m+1} = I_{n+1}$ and we are done. ■

From now on m and J_m will be as used in Lemma 6.

LEMMA 7. *R and D have characteristic p with p prime such that* $p \setminus m + 1$. *Also* $2 \leq p \leq n + 1$.

PROOF. By Lemma 5 $\exists r \in RJ_mR \subseteq I_m$ such that $d^m(r) \in 1 + I$. By Lemma 6, $d^{m-1}(r)$ exists and $0 = d^{m-1}(r)r$. Now using the fact that $\mathrm{Ann}_R(V) = I$ we obtain $0 = d^{m+1}\big(d^{m-1}(r)r\big)V = \sum_{j=0}^{m+1} \binom{m+1}{j} d^{2m-j}(r)\, d^j(r)V = (m+1)d^m(r)d^m(r)V = (m+1)V$. But $m + 1 \in D$ so D has characteristic p such that $p \setminus m + 1$, and as D is a division ring, p is prime. But then $pV = 0$ so $p \in I$ which gives $p = 0$ in R by Lemma 1. That $2 \leq p \leq n+1$ is trivial. ■

From now on p will be the characteristic of R. Now the lemmas will begin to narrow in on the structure of R.

LEMMA 8. *If* $0 \leq j \leq m$ *then* $\exists$ *a function* $\theta: R/I \longrightarrow R$ *such that* $\theta(r + I) \in r + I$ *and* $d\big(\theta(r + I)\big) \in I_j$ *for every* $r \in R$.

PROOF: INDUCTION ON j. If $j = 0$ then take any function $\theta: R/I \longrightarrow R$ such that $\theta(r + I) \in r + I$ for every $r \in R$, then $d\big(\theta(r + I)\big) \in R = I_0$ so the result holds. Suppose the result holds for some j with $j < m$. Then $\exists \gamma: R/I \longrightarrow R$ with $\gamma(r + I) \in r + I$ and $d\big(\gamma(r + I)\big) \in I_j$ for every $r \in R$. Now $d^{m-j-1}(J_m)$ is nonempty and $d^{m-j-1}(J_m) \cap (I_{j+1} \setminus I_{j+2}) \neq \emptyset$ so for $a \in R$ $\exists b \in I_{j+1}$ such that $d^{j+1}(b) \in a + I$ by Lemma 5. $\therefore$ $\exists$ a function $\psi: R \longrightarrow I_{j+1}$ such that $d^{j+1}\big(\psi(a)\big) \in a + I$ for every $a \in R$. Now take $\theta(r + I) = \gamma(r+I) - \psi\Big(d^{j+1}\big(\gamma(r+I)\big)\Big)$. Then for $r \in R$, $\theta(r+I) \in r+I+I_{j+1} = r+I$ and $d\big(\theta(r+I)\big) = d\Big(\gamma(r+I) - \psi\Big(d^{j+1}\big(\gamma(r+I)\big)\Big)\Big) \in I_j - d(I_{j+1}) = I_j$. But $d^j\Big(d\big(\theta(r+I)\big)\Big) = d^{j+1}\big(\gamma(r+I)\big) - d^{j+1}\Big(\psi\Big(d^{j+1}\big(\gamma(r+I)\big)\Big)\Big) \in d^{j+1}\big(\gamma(r+I)\big) - \Big(d^{j+1}\big(\gamma(r+I)\big) + I\Big) = I$. $\therefore$ $d\big(\theta(r+I)\big) \in I_{j+1}$. ■

LEMMA 9. *R has a subring* R' *with* $d(R') \subseteq I_m$, $R = R' + I$, $R' \cap I = 0$, *and* $R' \cong D_i$.

PROOF. Apply Lemma 8 with $j = m$ to find $\theta: R/I \longrightarrow R$ such that $\theta(r+I) \in r+I$ and $d\big(\theta(r+I)\big) \in I_m$ for every $r \in R$. Now if $r \in R$ and $r_1 r_2 \in r+I$ such that $d(r_1), d(r_2) \in I_m$ then $r_1 - r_2 \in I_{m+1} = 0$ by Lemma 6 so $r_1 = r_2$. $\therefore$ $\theta(r + I)$ is the unique element $r_1 \in r+I$ with $d(r_1) \in I_m$. Now define $R' = \theta(R/I)$. Then by definition of R', $d(R') \subseteq I_m$ and as $0 \in 0 + I = I$ and $d(0) = 0 \in I_m$, we have $R' \cap I = 0$. Now if $r, s \in R$ then $\theta(r+I) + \theta(s+I) \in r+s+I$ and $d\big(\theta(r+I) + \theta(s+I)\big) \in I_m$ so $\theta(r+s+I) = \theta(r+I) + \theta(s+I)$ by the uniqueness of $t \in r + s + I$ with $d(t) \in I_m$. Similarly $\theta(rs + I) = \theta(r + I)\theta(s + I)$.

$\therefore$ θ is a ring homomorphism from $R/I \longrightarrow R'$. Now if $\theta(r+I) = 0$ then $0 \in r+I \Rightarrow r \in I$ so θ is a ring isomorphism. Using Lemma 4, $R' = \theta(R/I) \cong D_i$ so $R' \cong D_i$ and R' is a subring of R. ∎

For convenience R' will be called D_i from now on. Also Z_R will be the center of R and Z_{D_i} the center of D_i. The function θ in Lemma 8 will not be used again.

LEMMA 10. *If* $1 \leq j \leq m$ *and* $r \in R$ *then* $\exists s \in I$ *such that* $d(s) \in r + I_j$.

PROOF. Suppose that it is false and let j be the least $j \in \{1, 2, \ldots, m\}$ such that $\exists r \in R$ for which the result fails. By Lemma 6, $0 \leq m - 1$ so $d^{m-1}(J_m)$ exists and $d^{m-1}(J_m) \cap (I_1 \setminus I_2) \neq \emptyset$. Therefore Lemma 5 can be applied to show that $j \neq 1$. $\therefore$ $1 < j$ and $\exists a \in I$ such that $r - d(a) \in I_{j-1}$. As $d^{m-j}(J_m) \cap (I_j \setminus I_{j+1}) \neq \emptyset$, by Lemma 5 $\exists b \in Rd^{m-j}(J_m)R \subseteq I_j$ such that $d^j(b) \in d^{j-1}\big(r - d(a)\big) + I$. Let $s = a + b \in I$. Now $r - d(s) = \big(r - d(a)\big) - d(b) \in I_{j-1}$ and $d^{j-1}\big(r - d(s)\big) = d^{j-1}\big(r - d(a)\big) - d^j(b) \in I$ so $r - d(s) \in I_j$. $\therefore$ j does not exist by contradiction so the lemma holds. ∎

LEMMA 11. *If* $r \in Z_R$ *then* $\exists a \in I \cap Z_R$ *with* $d(a) \in r + I_m$. *If in addition* $r \in I$ *then* $r^p = 0$.

PROOF. Apply Lemma 10 to find $a \in I$ such that $r - d(a) \in I_m$. Then let $K = \{ab - ba \mid b \in R\}$. Then $K \subseteq I$ and $d(K) \subseteq K + I_m$ so it is immediate that $K \subseteq I_{m+1} = 0$ so $a \in Z_R$. If in addition $r \in I$ then $r^p \in I$ and $d(r^p) = pr^{p-1}d(r) = 0 \in I_m$ because p is the characteristic of R, so therefore $r^p \in I_{m+1} = 0$. ∎

Suppose that $\exists x_1, x_2, \ldots, x_\ell \in I \cap Z_R$ such that $d(x_1) \in 1 + I$, and $d(x_j) \in x_1^{p-1}x_2^{p-1}\cdots x_{j-1}^{p-1} + I_m$ for every $j \in \{2, 3, \ldots, \ell\}$. Recall from number theory that if $k \in \{0, 1, \ldots, p^\ell - 1\}$ then k has a unique representation as $n_\ell n_{\ell-1}\cdots n_1 = n_1 + n_2 p + \cdots + n_\ell p^{\ell-1}$ with $n_1, n_2, \ldots, n_\ell \in \{0, 1, \ldots, p-1\}$. Now define θ: $\{0, 1, \ldots, p^\ell - 1\} \longrightarrow R$ by $\theta(k) = \theta(n_\ell n_{\ell-1}\cdots n_1) = x_1^{n_1}x_2^{n_2}\cdots x_\ell^{n_\ell}$ where r^0 is defined to be 1. Note that $\theta(p^{j-1}) = x_j$. Now Lemma 12 is a technical result that is crucial in finding the structure of R.

LEMMA 12. *If* $x_1, x_2, \ldots, x_\ell$ *exist and* $0 \neq x_1, x_2, \ldots, x_\ell$ *then* $\forall 0 \leq k \leq p^\ell - 1$, $\theta(k) \in I_k \cap Z_R$ *and* $d^k\big(\theta(k)\big)$ *is invertible.*

PROOF: INDUCTION ON k. If $k = 0$ then $\theta(k) = x_1^0 x_2^0 \cdots x_\ell^0 = 1 \in I_0 \cap Z_R$ and is also invertible. Suppose the result holds for k and $k < p^\ell - 1$. Note that $\theta(k+1)$ is the product of elements from Z_R so $\theta(k+1) \in Z(R)$. To finish, divide into cases.

CASE I. $k + 1 = p^{j-1}$ for some $j \in \{1, 2, \ldots, \ell\}$.

Then $\theta(k+1) = x_j$. As the result holds for k, $\theta(k) \in I_k$ and $d^k\big(\theta(k)\big)$ is invertible so $0 \neq \theta(k) \in I_k \Rightarrow k \leq m$. Now $d\big(\theta(k+1)\big) = d(x_j) \in x_1^{p-1}x_2^{p-1}\cdots x_{j-1}^{p-1} + I_m = \theta\big((p-1)(1 + p + \cdots + p^{j-2})\big) + I_m = \theta(p^{j-1} - 1) + I_m = \theta(k) + I_m$ so $d\big(\theta(k+1)\big) \in I_k$. As $\theta(k+1) = x_j \in I$, $\theta(k+1) \in I_{k+1}$. As $0 \neq \theta(k+1) \in I_{k+1}$, $k + 1 \leq m$ so $d^{k+1}\big(\theta(k+1)\big) \in d^k\big(\theta(k) + I_m\big) \subseteq d^k\big(\theta(k) + I_{k+1}\big) \subseteq d^k\big(\theta(k)\big) + I$. $\therefore$ $d^{k+1}\big(\theta(k+1)\big) = d^k\big(\theta(k)\big) - a$ for some $a \in I$. As $\theta(k) \in Z_R$, $d^k\big(\theta(k)\big) \in Z_R$ and $a \in I$ so $a^{m+1} \in I_{m+1} = 0$. Since $(d^k\theta(k)) - a)$ divides $\Big(d^k\big(\theta(k)\big)\Big)^{m+1} - a^{m+1}$ and $d^k\big(\theta(k)\big)$ is invertible, so is $d^{k+1}\big(\theta(k+1)\big)$.

https://doi.org/10.4153/CMB-1994-018-7 Published online by Cambridge University Press

CASE II. $k+1 \neq p^{j-1}\ \forall 1 \leq j \leq \ell$.

Let $k+1 = n_1 + n_2 p + \cdots + n_\ell p^{\ell-1}$ with $n_1, n_2, \ldots, n_\ell \in \{0,1,\ldots,p-1\}$. Let $\{j_1, j_2, \ldots, j_N\} = \{j \in \{1,2,\ldots,\ell\} \mid n_j \neq 0\}$ with $j_1 < j_2 < \cdots < j_N$. Note that $\theta(k+1) = x_1^{n_1} x_2^{n_2} \cdots x_\ell^{n_\ell} = x_{j_1}^{n_{j_1}} x_{j_2}^{n_{j_2}} \cdots x_{j_N}^{n_{j_N}}$. Now $\theta(k+1) \in I$, $\theta(k) \in I_k$, $k \neq 0$ so n_{j_1} exists and n_{j_1} is invertible as an element of D_i (and therefore of R), and $d^k\big(\theta(k)\big)$ is invertible so the lemma would follow if $d\big(\theta(k+1)\big) = n_{j_1}\theta(k)$.

Now suppose that $2 \leq M \leq N$. Then

$$x_{j_1}^{n_1} x_{j_2}^{n_2} \cdots x_{j_{M-1}}^{n_{j_{M-1}}} d(x_{j_M}^{n_{j_M}}) x_{j_{M+1}}^{n_{j_{M+1}}} \cdots x_{j_N}^{n_{j_N}} \in x_{j_1} d(x_{j_M}) R$$

using $x_1, x_2, \ldots, x_\ell \in Z_R$. But $x_{j_1} d(x_{j_M}) R \in x_{j_1}^p R + x_{j_1} I_m = 0$ by Lemmas 6 and 11 and the fact that $j_1 < j_M$ and the definition of $d(x_{j_M})$. Therefore

$$\begin{aligned} d(k+1) &= d(x_{j_1}^{n_{j_1}} x_{j_2}^{n_{j_2}} \cdots x_{j_N}^{n_{j_N}}) \\ &= \sum_{M=1}^{N} x_{j_1}^{n_1} x_{j_1}^{n_2} \cdots x_{j_{M-1}}^{n_{M-1}} d(x_{j_M}^{n_M}) x_{j_{M+1}}^{n_{M+1}} x_{j_{M+2}}^{n_{M+2}} \cdots x_{j_N}^{n_N} \\ &= d(x_{j_1}^{n_{j_1}}) x_{j_2}^{n_{j_2}} \cdots x_{j_N}^{n_{j_N}} \in n_{j_1}(x_1^{p-1} x_2^{p-1} \cdots x_{j_1-1}^{p-1} + I_m) x_{j_1}^{n_{j_1}-1} x_{j_2}^{n_{j_2}} x_{j_3}^{n_{j_3}} \cdots x_{j_N}^{n_{j_N}}. \end{aligned}$$

However because $k+1 \neq p^{j-1}\ \forall 1 \leq j \leq \ell$ we have trivially $2 \leq n_{j_1} + n_{j_2} + \cdots + n_{j_N}$ and $I_m \cdot I = 0$ so

$$\begin{aligned} d\big(\theta(k+1)\big) &= n_{j_1} x_1^{p-1} x_2^{p-1} \cdots x_{j_1-1}^{p-1} x_{j_1}^{n_{j_1}-1} x_{j_2}^{n_{j_2}} x_{j_3}^{n_{j_3}} \cdots x_{j_N}^{n_{j_N}} \\ &= n_{j_1}\theta\big((p-1)(1+p+\cdots+p^{j_1-2}) - p^{j_1-1} + n_{j_1}p^{j_1-1} \\ &\qquad + n_{j_2}p^{j_1-1} + \cdots + n_{j_N}p^{j_N-1}\big) \\ &= n_{j_1}\theta(-1+k+1) = n_{j_1}\theta(k). \end{aligned}$$

Therefore the lemma holds. ∎

LEMMA 13. *There exists a largest $\ell \in \mathbb{Z}^+$ such that $x_1, x_2, \ldots, x_\ell$ all exist and are nonzero. Furthermore $m = p^\ell - 1$.*

PROOF. $1 \in Z_R$ so by Lemma 11, x_1 exists. By Lemma 6, $1 \leq m$ so $d(x_1) \in 1 + I_m \subseteq 1 + I$ and $I \neq R$ so $d(x_1) \notin I \Rightarrow x_1 \neq 0$. Now if there is no last ℓ such that $x_1, x_2, \ldots, x_\ell$ all exist and are nonzero then take $\ell = m$ and then by Lemma 12, $0 \neq I_{p^\ell} \subseteq I_{m+I}$ contrary to Lemma 6 so a last such ℓ exists. But now take ℓ to be maximal and by Lemma 12, $d^{p^\ell-1}\big(\theta(p^\ell-1)\big)$ is invertible and $\theta(p^\ell-1) \in I_{p^\ell-1}$ but $d^{p^\ell-1}\big(\theta(p^\ell-1)\big) \notin I$ so $m \geq p^\ell - 1$. However by Lemma 11 $\exists x_{\ell+1} \in I \cap Z_R$ with $d(x_{\ell+1}) \in \theta(p^\ell - 1) + I_m$ but ℓ is maximal so $x_{\ell+1} = 0$ and $\theta(p^\ell - 1) \in I_m$, from which $m \leq p^\ell - 1$. Therefore $m = p^\ell - 1$. ∎

LEMMA 14. *Let $0 \leq j \leq p^\ell - 1$. Then $I_j = I_{j+1} + D_i\theta(j)$.*

PROOF. By Lemma 12, $\theta(j) \in I_j$ so as $I_{j+1} \subseteq I_j$ and I_j is an ideal, $I_{j+1} + D_i\theta(j) \subseteq I_j$. Now by Lemma 12, $d^j\big(\theta(j)\big)$ is invertible so $\theta(j) \in I_j \setminus I_{j+1}$. Therefore if $r \in I_j$ then by Lemma 5 $\exists s \in R\theta(j)R = R\theta(j)$ (because $\theta(j) \in Z_R$) such that $d^j(s) \in d^j(r) + I$. However $s = (a+b)\theta(j)$ for some $a \in D_i$ and $b \in I$ by Lemma 9. But then $d^j\big(b\theta(j)\big) \in I$ so $d^j(r) \in d^j\big(a\theta(j)\big) + I$. As $r - a\theta(j) \in I_j$ this gives $r - a\theta(j) \in I_{j+1}$. $\therefore$ $r \in a\theta(j) + I_{j+1} \subseteq D_i\theta(j) + I_{j+1}$. $\therefore$ $I_j \subseteq D_i\theta(j) + I_{j+1}$ so $I_j = D_i\theta(j) + I_{j+1}$. ∎

Now it is a matter of putting together the pieces.

LEMMA 15. *There exists a derivation f of D_i and $a_1, a_2, \ldots, a_\ell \in Z_{D_i}$ such that $\forall a \in D_i$, $d(a) = f(a)x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1}$, $d(x_1) = 1 + a_1x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1}$, and $d(x_j) = x_1^{p-1}x_2^{p-1}\cdots x_{j-1}^{p-1} + a_jx_1^{p-1}x_2^{p-1}\cdots x_j^{p-1}$ for $j = 2, 3, \ldots, \ell$.*

PROOF. Note that $x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1} = \theta(p^\ell - 1)$, and by Lemma 13, $m = p^\ell - 1$ so by Lemmas 6 and 14, $I_m = D_i\theta(p^\ell - 1)$. Now suppose that $a, b \in D_i$ and $(a-b)\theta(p^\ell - 1) = 0$. Then by Lemma 9, $0 = d^{p^\ell-1}\big((a-b)\theta(p^\ell-1)\big) \in (a-b)d^{p^\ell-1}\big(\theta(p^\ell-1)\big) + I$ so $(a-b)d^{p^\ell-1}\big(\theta(p^\ell-1)\big) \in I$ so by Lemma 12, $a - b \in I$. But then by Lemma 9, $a - b \in I \cap D_i = 0$ so $a = b$. Therefore if $a\theta(p^\ell - 1) = 0$ then $a = 0$. Thus there exists a unique function $f\colon D_i \longrightarrow D_i$ such that if $a \in D_i$ then $d(a) = f(a)\,\theta(p^\ell - 1)$. Now if $a, b \in D_i$ then $f(a+b)\,\theta(p^\ell-1) = d(a+b) = d(a) + d(b) = \big(f(a)+f(b)\big)\theta(p^\ell-1)$ so $f(a+b) = f(a)+f(b)$. Also $f(ab)\,\theta(p^\ell-1) = d(ab) = d(a)b + ad(b) = \big(f(a)b + af(b)\big)\theta(p^\ell-1)$ so $f(ab) = f(a)b + af(b)$ so f is a derivation. Now as $I_m = D_i\theta(p^\ell-1)$ by Lemma 14, from the definition of x_1 $\exists a_1 \in D_i$ with $d(x_1) = 1 + a_1\theta(p^\ell-1)$. But then by the definition of x_1, $x_1 \in Z_R$ so $1 + a_1\theta(p^\ell-1) = d(x_1) \in Z_R$ so $\forall a \in D_i$, $0 = a\big(1 + a_1\theta(p^\ell-1)\big) - \big(1 + a_1\theta(p^\ell-1)\big)a = (aa_1 - a_1a)\,\theta(p^\ell-1)$ so $aa_1 - a_1a = 0$. $\therefore$ $a_1 \in Z_{D_i}$. Similarly if $j = 2, 3, \ldots, \ell$ then $d(x_j) = x_1^{p-1}x_2^{p-1}\cdots x_{j-1}^{p-1} + a_j\theta(p^\ell-1)$ with $a_j \in Z_{D_i}$. ∎

LEMMA 16. $R \cong D_i[y_1, y_2, \ldots, y_\ell]/(y_1^p, y_2^p, \ldots, y_\ell^p)$.

PROOF. By Lemma 11, $0 = x_1^p = x_2^p = \cdots = x_\ell^p$ so there is a unique ring homomorphism $\psi\colon D_i[y_1, y_2, \ldots, y_\ell]/(y_1^p, y_2^p, \ldots, y_\ell^p) \longrightarrow R$ with $\psi(a) = a\ \forall a \in D_i$ and $\psi(y_j) = x_j$ for $j = 1, 2, \ldots, \ell$. Now ψ is an epimorphism because by Lemmas 14 and 13,

$$\begin{aligned} R = I_0 &= D_i + I_1 \\ &= D_i + D_i\theta(1) + I_2 = \cdots = D_i + D_i\theta(1) + D_i\theta(2) + \cdots + D_i\theta(p^\ell - 1) \\ &\subseteq \psi\big(D_i[y_1, y_2, \ldots, y_\ell]/(y_1, y_2, \ldots, y_\ell)\big). \end{aligned}$$

Now to finish it suffices to show that ψ is one-to-one. Now suppose that $a \in D_i[y_1, y_2, \ldots, y_\ell]/(y_1^p, y_2^p, \ldots, y_\ell^p)$ and that $\psi(a) = 0$. Formally, $\psi(a) = a_0 + a_1\theta(1) + \cdots + a_{p^\ell-1}\theta(p^\ell - 1)$ with $a_0, a_1, \ldots, a_{p^\ell-1} \in D_i$. If some $a_j \neq 0$ then let j be the least j such that $a_j \neq 0$ and note that $d^j\big(\psi(a)\big) \notin I$ contrary to $\psi(a) = 0$. Clearly if $a_0, a_1, \ldots, a_{p^\ell-1}$ are all 0 then $a = 0$ so ψ is one-to-one. ∎

Let us review what part of Theorem 1 we now know. For the case where $I = 0$, Lemma 4 does the job. If $I \neq 0$ then Lemmas 15 and 16 give us most of Theorem 1 and together with Lemma 7 all that we do not know is $2 \leq ip^\ell \leq n + 1$. However we have $1 \leq i \leq n+1$ from Lemma 4, $2 \leq p \leq n + 1$ from Lemma 7 and $1 \leq \ell$ from Lemmas 6 and 13. Thus we know that $2 \leq ip^\ell$. The rest of the paper will show that $ip^\ell \leq n + 1$.

From Lemmas 6 and 14 $\exists b \in D_i$ such that $0 \neq b\theta(m) \in I_m \cap J$. By similar reasoning to Lemma 3, $\exists 0 \neq a \in D_ib$ such that $\dim_D\Big(f^j(a)\Big(\bigcap_{k=0}^{j-1}\operatorname{Ker}\big(f^k(a)\big)\Big)\Big) = 0$ or 1 for $j = 1, 2, \ldots, n$ and $\dim_D(aV) = 0$ or 1 also. Now define $L_0 = 0$ and for $j \in \mathbb{Z}^+$, $L_j = D_ia + D_if(a) + \cdots + D_if^{j-1}(a)$. Therefore $L_0 \subseteq L_1 \subseteq \cdots$ and $f(L_0) \subseteq L_1, f(L_1) \subseteq L_2,$

https://doi.org/10.4153/CMB-1994-018-7 Published online by Cambridge University Press

$f(L_2) \subseteq L_3, \ldots$. Now if $N = jp^\ell + k$ with $j \in \{0,1,2,\ldots,\}$ and $k \in \{0,1,\ldots,p^\ell - 1\}$ then define $\mathcal{L}[N] = \mathcal{L}(j,k) = RL_j + I_{p^\ell-k-1}L_{j+1}$. Note that $0 \neq a \in J$ and Lemma 1 imply that $R = Ra + Rd(a) + \cdots + Rd^n(a)$.

THEOREM 1. *Let $n \in \mathbb{Z}^+$, R be a ring with unit, J a left ideal of R, and d a derivation of R such that $d^n(J) \neq 0$ and $d^n(r) = 0$ or $d^n(r)$ is invertible, for every $r \in J$. Then there exists a division ring D such that R is either:*

1) D_i, the ring of $i \times i$ matrices over a division ring D with $1 \le i \le n+1$, or

2) $D_i[x_1, x_2, \ldots, x_\ell]/(x_1^p, x_2^p, \ldots, x_\ell^p)$ where $i, \ell, p \in \mathbb{Z}^+$, p is prime, $2 \le ip^\ell \le n+1$, and char $D = p$.

Furthermore, there exists a derivation f of D_i and $a_1, a_2, \ldots, a_\ell \in Z_{D_i}$, the center of D_i, with $d(a) = f(a)x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1}$ for all $a \in D_i$, $d(x_1) = 1 + a_1x_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1}$, and

$$d(x_j) = x_1^{p-1}x_2^{p-1}\cdots x_{j-1}^{p-1} + a_jx_1^{p-1}x_2^{p-1}\cdots x_\ell^{p-1}$$

for $j = 2, 3, \ldots, \ell$.

PROOF. As has been noted, all that is left is to show that $ip^\ell \le n+1$. This will be proved under the assumption $d(\mathcal{L}[N]) \subseteq \mathcal{L}[N+1]\ \forall N \ge 0$, and then that assumption will be proved.

PART 1. Assume $d(\mathcal{L}[N]) \subseteq \mathcal{L}[N+1]\ \forall N \ge 0$.

Note that $\mathcal{L}[0] \subseteq \mathcal{L}[1] \subseteq \cdots \subseteq \mathcal{L}[n]$ and for $N \in \{0,1,2,\ldots\}$, $d^N(\mathcal{L}[0]) \subseteq \mathcal{L}[N]$. Now choose j, k with $0 \le k \le p^\ell - 1$ with $n+1 = jp^\ell + k$. It is easy to verify that $\mathcal{L}[n] \subseteq L_j + I$. But $a\theta(p^\ell - 1) \in \mathcal{L}[0]$ so $R \subseteq R\mathcal{L}[0] + R\mathcal{L}[1] + \cdots + R\mathcal{L}[n] = R\mathcal{L}[n] \subseteq (D_i+I)(L_j+I) \subseteq L_j + I \subseteq R$ so $R = L_j + I$. Note that if $c_1 \in D_i$ then $c_1 \in L_j + I$ so $\exists c_2 \in L_j$ with $c_1 - c_2 \in D_i \cap I = 0$ by Lemma 9 and $L_j \subseteq D_i$ so $D_i = L_j = D_ia + D_if(a) + \cdots + f^{j-1}(a)$ so by the same reasoning as in Lemmas 2 and 4, $j \ge \dim_D(V) = i$ but $n+1 = jp^\ell + k$ and $0 \le k$ so $j \le \frac{n+1}{p^\ell}$ so $ip^\ell \le n+1$.

PART 2. Prove that $d(\mathcal{L}[N]) \subseteq \mathcal{L}[N+1]\ \forall N \ge 0$.

INDUCTION ON N. If $N = 0$ then $\mathcal{L}[N] = \mathcal{L}(0,0) = RL_0 + I_{p^\ell-1}L_1 = I_{p^\ell-1}L_1$ so $d(\mathcal{L}[N]) \subseteq I_{p^\ell-2}L_1 + Id(L_1) = RL_0 + I_{p^\ell-1-1}L_1 = \mathcal{L}[1]$ using the fact that $d(L_1) \subseteq I_m$. Now suppose that $d(\mathcal{L}[N]) \subseteq \mathcal{L}[N+1]$ and divide into cases.

CASE I. $N+1 = jp^\ell + k$ with $1 \le k < p^\ell - 1$.

Then by Lemma 14, $\mathcal{L}[N+1] = \mathcal{L}(j,k) = RL_j + I_{p^\ell-k-1}L_{j+1} = RL_j + I_{p^\ell-k}L_{j+1} + D_i\theta(p^\ell - k - 1)L_{j+1} \subseteq \mathcal{L}[N] + I_{p^\ell-k-1}L_{j+1}$. $\therefore$ $d(\mathcal{L}[N+1]) \subseteq d(\mathcal{L}[N]) + d(I_{p^\ell-k-1})L_{j+1} + I_{p^\ell-k-1}d(L_{j+1}) \subseteq \mathcal{L}[N+1] + I_{p^\ell-k-2}L_{j+1} \subseteq RL_j + I_{p^\ell-k-2}L_{j+1} = \mathcal{L}(j,k+1) = \mathcal{L}[N+2]$.

CASE II. $N+1 = jp^\ell + k$ with $k = p^\ell - 1$.

Then $\mathcal{L}(N+1) = RL_j + I_0L_{j+1} = RL_{j+1}$ because $I_0 = R$. $\therefore$ $d(\mathcal{L}[N+1]) \subseteq d(R)L_{j+1} + R\theta(p^\ell - 1)f(L_{j+1}) \subseteq RL_{j+1} + I_{p^\ell-1}L_{j+2} = \mathcal{L}(j+1,0) = \mathcal{L}[N+2]$.

CASE III. $N+1 = jp^\ell + k$ with $j \in \mathbb{Z}^+$ and $k = 0$.

Then $\mathcal{L}[N+1] = RL_j + I_{p^\ell-1}L_{j+1} = RL_{j-1} + I_0L_j + I_{p^\ell-1}L_{j+1} = \mathcal{L}[N] + I_{p^\ell-1}L_{j+1}$. Therefore $d(\mathcal{L}[N+1]) \subseteq \mathcal{L}[N+1] + I_{p^\ell-2}L_{j+1} = RL_j + I_{p^\ell-2}L_{j+1} = \mathcal{L}(j,1) = \mathcal{L}[N+2]$. ∎

https://doi.org/10.4153/CMB-1994-018-7 Published online by Cambridge University Press

References

1. J. Bergen, I. N. Herstein and C. Lanski, *Derivations with invertible values*, Can. J. Math. **35**(1983), 300–310.

Department of Mathematics and Statistics
University of Victoria
Victoria, British Columbia
V8W 3P4

Present address:
6188 Bradley Hall
Dartmouth College
Department of Mathematics and Computer Science
Hanover, New Hampshire 03755
U.S.A.

https://doi.org/10.4153/CMB-1994-018-7 Published online by Cambridge University Press