

***DERIVATIONS WHOSE ITERATES ARE
ZERO OR INVERTIBLE ON A
LEFT IDEAL***

by

BEN TILLY

DMS-619-IR

September 1992

DERIVATIONS WHOSE ITERATES ARE ZERO OR INVERTIBLE
ON A LEFT IDEAL¹

by

Ben Tilly²

Department of Mathematics and Statistics
University of Victoria³
Victoria, B.C., V8W 3P4
CANADA

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 $D_i[x_1, x_2, \dots, x_\ell]/(x_1^p, x_2^p, \dots, x_\ell^p)$, where D is a division ring with characteristic p , and furthermore there is a derivation f of D_i and $a_1, a_2, \dots, a_\ell \in Z_{D_i}$, the center of D_i , such that if $a \in D_i$ then

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

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

and

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

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

¹AMS *Subject Classification*: Primary 16W25; Secondary 16N60.

²The author wishes to acknowledge the support of Dr. C.R. Miers through NSERC Grant A-7682.

³The author is presently at Dartmouth College, Department of Mathematics and Computer Science, Hanover, NH 03755.

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

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

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

and

$$d(x_j) = x_1^{p-1}x_2^{p-1}\dots x_{j-1}^{p-1} + a_jx_1^{p-1}x_2^{p-1}\dots x_\ell^{p-1} \quad \text{for } j = 2, 3, \dots, \ell.$$

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 $0 = d(a) = d^2(a) = \dots$. Now $ar \in J$ and $ad^n(r) \neq 0$ because $ad^n(r)(d^n(r))^{-1} = a \neq 0$ 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 $\text{Ann}_R(V) = I$ where $\text{Ann}_R(V) = \{r \in R \mid rV = \{0\}\}$. 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 and let W be some finite dimensional D -subspace of V . If $a \in S$ define $W_0(a) = W$ and for $0 \leq i$, $W_{i+1}(a) = W \cap \left[\bigcap_{j=1}^i \text{Ker}(d^j(a)) \right]$ where $d^0(a) = a$. It is not hard to show that for $r, s \in R$ and $i \in \{0, 1, 2, \dots\}$, 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 $R = Ra + Rd(a) + \dots + Rd^n(a)$. It is trivial that $0 = d^j(a)W_{n+1}(a)$ for $j = 0, 1, \dots, n$ so we have $0 = RaW_{n+1}(a) + Rd(a)W_{n+1}(a) + \dots + Rd^n(a)W_{n+1}(a) = RW_{n+1}(a)$ so $W_{n+1}(a) = 0$ because V is irreducible. ■

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

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

$$(1) \quad d^j(bs)w = bd^j(s)w.$$

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

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

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 $i + 1$. \blacksquare

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 $0 \leq j \leq n$, $d^j(a) : W_j(a) \rightarrow V$ is a D -linear map with kernel $W_{j+1}(a)$ and range contained in Dv . Hence

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

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 so we will assume from now on that $I \neq 0$. Note again that $\text{Ann}_R(V) = I$. 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 $j \in \{0,1,2,\dots\}$, $r \in R$, and $a \in I_j \setminus I_{j+1}$ then $d^j(RaR) \cap (r+I) \neq \emptyset$.

Proof. Let $\varphi : R \rightarrow R/I$ by $\varphi(r) = r + I$. Now $a \in I_j \setminus I_{j+1}$ so $d^j(a) \notin I$ so $\varphi(d^j(a)) \neq 0$. As I is maximal R/I is simple so $r + I \in (R/I)\varphi(d^j(a))(R/I)$

$= \varphi(\text{Rd}^j(a)R) = \varphi(d^j(RaR))$ because $d^j(IaR) \subseteq \text{Id}^j(aR) + I \subseteq I$ 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 $R = Rr + \text{Rd}(r) + \dots + \text{Rd}^n(r) \subseteq I$ 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 $0 = d(I_{j+2}d^j(J_m)) = I_{j+2}d^{j+1}(J_m)$ 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

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

If $I_{m+1} = I_{n+1} = 0$ then m cannot be zero because $I \neq 0$ so we would finish. 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 $a \in I_{m+1}$, $\text{ad}^m(J_m) = 0$. As for $k < j$, $d^k(a) \in I$ we have

$$0 \equiv d^j(\text{ad}^m(J_m)) \equiv d^j(a)d^m(J_m) \equiv d^m(J_m) \pmod{I}$$

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 $p/m+1$.

Also $2 \leq p \leq n + 1$.

Proof. By lemma 5 $\exists r \in R \setminus J_m R \subseteq I_m$ 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 $\text{Ann}_R(V) = I$ we obtain $0 = d^{m+1}(d^{m-1}(r)r)V = \sum_{j=0}^{m+1} \binom{m+1}{j} d^{2m-j}(r)d^j(r)V = (m+1)d^m(r)d^m(r)V = (m+1)V$. But $m + 1 \in D$ so D has characteristic p such that $p/m+1$, and as D is a division ring, p is prime. But then $pV = 0$ so $p \in I$ which gives $p = 0$ 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 $\theta : R/I \rightarrow R$ such that $\theta(r+I) \in r + I$ and $d(\theta(r+I)) \in I_j$ for every $r \in R$.

Proof. Induction on j . If $j = 0$ then take any function $\theta : R/I \rightarrow R$ such that $\theta(r+I) \in r + I$ for every $r \in R$, then $d(\theta(r+I)) \in R = I_0$ so the result holds. Suppose the result holds for some j with $j < m$. Then $\exists \gamma : R/I \rightarrow R$ with $\gamma(r+I) \in r + I$ and $d(\gamma(r+I)) \in I_j$ 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 $\psi : R \rightarrow I_{j+1}$ such that $d^{j+1}(\psi(a)) \in a + I$ for every $a \in R$. Now take $\theta(r+I) = \gamma(r+I) - \psi(d^{j+1}(\gamma(r+I)))$. Then for $r \in R$, $\theta(r+I) \in r + I + I_{j+1} = r + I$ and $d(\theta(r+I)) = d(\gamma(r+I) - \psi(d^{j+1}(\gamma(r+I)))) \in I_j - d(I_{j+1}) = I_j$. But $d^j(d(\theta(r+I))) = d^{j+1}(\gamma(r+I)) - d^{j+1}(\psi(d^{j+1}(\gamma(r+I)))) \in d^{j+1}(\gamma(r+I)) - (d^{j+1}(\gamma(r+I)) + I) = I$.

$\therefore d(\theta(r+I)) \in I_{j+1}$. ■

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 $\theta : R/I \rightarrow R$ such that $\theta(r+I) \in r + I$ and $d(\theta(r+I)) \in I_m$ 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 the 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 $d(\theta(r+I) + \theta(s+I)) \in I_m$ 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 $\theta(rs+I) = \theta(r+I)\theta(s+I)$. $\therefore \theta$ is a ring homomorphism from $R/I \rightarrow R'$. 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 $j \in \{1, 2, \dots, m\}$ 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 $\exists b \in R d^{m-j}(J_m) R \subseteq I_j$ such that

$d^j(b) \in d^{j-1}(r-d(a)) + I$. Let $s = a + b \in I$. Now $r - d(s) = (r-d(a)) - d(b) \in I_{j-1}$ and $d^{j-1}(r-d(s)) = d^{j-1}(r-d(a)) - d^j(b) \in I$ 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 $r^p \in I$ and $d(r^p) = pr^{p-1}d(r) = 0 \in I_m$ because p is the characteristic of R so $r^p \in I_{m+1} = 0$. ■

Suppose that $\exists x_1, x_2, \dots, x_\ell \in I \cap Z_R$ such that $d(x_1) \in 1 + I$, and $d(x_j) \in x_1^{p-1}x_2^{p-1} \dots x_{j-1}^{p-1} + I_m$ for every $j \in \{2, 3, \dots, \ell\}$. Recall from number theory that if $k \in \{0, 1, \dots, p^\ell - 1\}$ then k has a unique representation as $n_\ell n_{\ell-1} \dots n_1 = n_1 + n_2 p + \dots + n_\ell p^{\ell-1}$ with $n_1, n_2, \dots, n_\ell \in \{0, 1, \dots, p-1\}$. Now define $\theta: \{0, 1, \dots, p^\ell - 1\} \rightarrow R$ by $\theta(k) = \theta(n_\ell n_{\ell-1} \dots n_1) = x_1^{n_1} x_2^{n_2} \dots x_\ell^{n_\ell}$ 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, \dots, x_ℓ exist and $0 \neq x_1, x_2, \dots, x_\ell$ then $\forall 0 \leq k \leq p^\ell - 1$, $\theta(k) \in I_k \cap Z_R$ and $d^k(\theta(k))$ is invertible.*

Proof. Induction on k . If $k = 0$ then $\theta(k) = x_1^0 x_2^0 \dots x_\ell^0 = 1 \in I_0 \cap Z_R$ 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 $j \in \{1, 2, \dots, \ell\}$.

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

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

Let $k + 1 = n_1 + n_2 p + \dots + n_\ell p^{\ell-1}$ with $n_1, n_2, \dots, n_\ell \in \{0, 1, \dots, p-1\}$.

Let $\{j_1, j_2, \dots, j_N\} = \{j \in \{1, 2, \dots, \ell\} \mid n_j \neq 0\}$ with $j_1 < j_2 < \dots < j_N$. Note that $\theta(k+1) = x_1^{n_1} x_2^{n_2} \dots x_\ell^{n_\ell} = x_{j_1}^{n_{j_1}} x_{j_2}^{n_{j_2}} \dots x_{j_N}^{n_{j_N}}$. 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_{j_1} (and therefore of R), and $d^k(\theta(k))$ is invertible so the lemma would follow if $d(\theta(k+1)) = n_{j_1} \theta(k)$.

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

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

using that $x_1, x_2, \dots, x_\ell \in Z_R$. 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

$d(k+1))$

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

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

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

Therefore the lemma holds. \blacksquare

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

Proof. $1 \in \mathbb{Z}_R$ 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 was no

last ℓ such that x_1, x_2, \dots, x_ℓ all exist and are nonzero then take $\ell = m$ and then by lemma 12, $0 \neq I_p^\ell \subseteq I_{m+1}$ contrary to lemma 6 so a last such ℓ exists.

But now take ℓ to be maximal and by lemma 12, $d^{p^{\ell-1}}(\theta(p^{\ell-1}))$ is invertible and $\theta(p^{\ell-1}) \in I_{p^{\ell-1}}$ but $d^{p^{\ell-1}}(\theta(p^{\ell-1})) \notin I$ 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, $d^j(\theta(j))$ 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 $d^j(b\theta(j)) \in I$ so $d^j(r) \in d^j(a\theta(j)) + I$. 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 $a_1, a_2, \dots, a_\ell \in Z_{D_i}$ such that $\forall a \in D_i$, $d(a) = f(a)x_1^{p-1}x_2^{p-1} \dots x_\ell^{p-1}$, $d(x_1) = 1 + a_1x_1^{p-1}x_2^{p-1} \dots x_\ell^{p-1}$, and $d(x_j) = x_1^{p-1}x_2^{p-1} \dots x_{j-1}^{p-1} + a_jx_1^{p-1}x_2^{p-1} \dots x_j^{p-1}$ for $j = 2, 3, \dots, \ell$.*

Proof. Note that $x_1^{p-1}x_2^{p-1} \dots x_\ell^{p-1} = \theta(p^{\ell-1})$, 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, $0 = d^{p^{\ell-1}}((a-b)\theta(p^{\ell-1})) \in (a-b)d^{p^{\ell-1}}(\theta(p^{\ell-1})) + I$ so $(a-b)d^{p^{\ell-1}}(\theta(p^{\ell-1})) \in I$ 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 $f : D_i \rightarrow D_i$ such that if $a \in D_i$ then $d(a) = f(a)\theta(p^{\ell-1})$. Now if $a, b \in D_i$ then $f(a+b)\theta(p^{\ell-1}) = d(a+b) = d(a) + d(b) = (f(a) + f(b))\theta(p^{\ell-1})$ so $f(a+b) = f(a) + f(b)$. Also $f(ab)\theta(p^{\ell-1}) = d(ab) = d(a)b + ad(b) = (f(a)b + af(b))\theta(p^{\ell-1})$ 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 $\forall a \in D_i$, $0 = a(1+a_1\theta(p^{\ell-1})) - (1+a_1\theta(p^{\ell-1}))a = (aa_1 - a_1a)\theta(p^{\ell-1})$ so $aa_1 - a_1a = 0$. $\therefore a_1 \in Z_{D_i}$. Similarly if $j = 2, 3, \dots, \ell$ then $d(x_j) = x_1^{p-1}x_2^{p-1} \dots x_{j-1}^{p-1} + a_j\theta(p^{\ell-1})$ with $a_j \in Z_{D_i}$. ■

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

Proof. By lemma 11, $0 = x_1^p = x_2^p = \dots = x_\ell^p$ so there is a unique ring homomorphism $\psi : D_i[y_1, y_2, \dots, y_\ell] / (y_1^p, y_2^p, \dots, y_\ell^p) \rightarrow R$ with $\psi(a) = a \quad \forall a \in D_i$ and $\psi(y_j) = x_j$ for $j = 1, 2, \dots, \ell$. Now ψ is an epimorphism because by lemmas 14 and 13,

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

Now to finish it suffices to show that ψ is one-to-one. Now suppose that $a \in D_i[y_1, y_2, \dots, y_\ell] / (y_1^p, y_2^p, \dots, y_\ell^p)$ and that $\psi(a) = 0$. Formally, $\psi(a) =$

$a_0 + a_1 \theta(1) + \dots + a_{p^{\ell-1}} \theta(p^{\ell-1})$ with $a_0, a_1, \dots, a_{p^{\ell-1}} \in D_i$. If some $a_j \neq 0$ then let j be the least j such that $a_j \neq 0$ and note that $d^j(\psi(a)) \notin I$ contrary to $\psi(a) = 0$. Clearly if $a_0, a_1, \dots, a_{p^{\ell-1}}$ 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 $\exists 0 \neq a \in D_i b$ such that $\dim_D \left[f^j(a) \left[\begin{array}{c} j-1 \\ \cap \\ k=0 \end{array} \text{Ker}(f^k(a)) \right] \right] = 0$ or 1 for $j = 1, 2, \dots, n$ and $\dim_D(aV) = 0$ or 1 also. Now define $L_0 = 0$ and for $j \in \mathbb{Z}^+$, $L_j = D_i a + D_i f(a) + \dots + D_i f^{j-1}(a)$. Therefore $L_0 \subseteq L_1 \subseteq \dots$ and $f(L_0) \subseteq L_1$, $f(L_1) \subseteq L_2$, $f(L_2) \subseteq L_3, \dots$. Now if $N = jp^{\ell+k}$ with $j \in \{0, 1, 2, \dots\}$ and $k \in \{0, 1, \dots, p^{\ell-1}\}$ 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 $R = Ra + Rd(a) + \dots + Rd^n(a)$.

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 $1 \leq i \leq n+1$,

or

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

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

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

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

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

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

Note that $\mathcal{L}[0] \subseteq \mathcal{L}[1] \subseteq \dots \subseteq \mathcal{L}[n]$ and for $N \in \{0, 1, 2, \dots\}$, $d^N(\mathcal{L}[0]) \subseteq \mathcal{L}[N]$. But $a\theta(p^\ell - 1) \in \mathcal{L}[0]$ so $R \subseteq R\mathcal{L}[0] + R\mathcal{L}[1] + \dots + R\mathcal{L}[n] = R\mathcal{L}[n] \subseteq (D_i + I)(L_j + I) \subseteq L_j + I \subseteq R$ so $R = L_j + I$. Now choose j, k with $0 \leq k \leq p^\ell - 1$ with $n + 1 = jp^\ell + k$ and 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 $D_i = L_j = D_i a + D_i f(a) + \dots + f^{j-1}(a)$ so by the same reasoning as in lemmas 2 and 4, $j \geq \dim_D(V) = i$ but $n+1 = jp^\ell + k$ and $0 \leq k$ so $j \leq \frac{n+1}{p^\ell}$ so $ip^\ell \leq n + 1$.

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

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 $d(\mathcal{L}[N]) \subseteq I_{p^{\ell-2}}L_1 + \text{Id}(L_1) = \text{RL}_0 + I_{p^{\ell-1-1}}L_1 = \mathcal{L}[1]$ using 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 $1 \leq k < p^{\ell-1}$.

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

Case II: $N + 1 = jp^{\ell+k}$ with $k = p^{\ell-1}$.

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

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

Then $\mathcal{L}[N+1] = \text{RL}_j + I_{p^{\ell-1}}L_{j+1} = \text{RL}_{j-1} + I_0L_j + I_{p^{\ell-1}}L_{j+1} = \mathcal{L}[N] + I_{p^{\ell-1}}L_{j+1}$. Therefore $d(\mathcal{L}[N+1]) \subseteq \mathcal{L}[N+1] + I_{p^{\ell-2}}L_{j+1} = \text{RL}_j + I_{p^{\ell-2}}L_{j+1} = \mathcal{L}(j,1) = \mathcal{L}[N+2]$. ■

REFERENCES

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