

FINITE DIMENSIONAL INSEPARABLE ALGEBRAS

BY
SHUEN YUAN

Abstract. We determine the structure of finite dimensional algebras which are differentially simple with respect to a set of higher derivations.

Let C be a commutative ring of prime characteristic p , and let A be a subring of C both with the same identity. By a p -basis $\mathfrak{b}$ of C over A we mean a *finite* subset of C such that for each $t \in \mathfrak{b}$, $t^{p^{e(t)}} \in A$ for some positive integer $e(t)$ and the set of all monomials $\prod_{t \in \mathfrak{b}} t^{i(t)}$, $0 \leq i(t) < p^{e(t)}$, form an A -module basis for C . In this note we show that if A is the kernel of a set $\mathfrak{g}$ of higher derivations of C such that C is finitely generated as A -module and no ideal in C , except 0 and 1, is stable under $\mathfrak{g}$, then C admits a p -basis over A which must be a field with $\text{Hom}_A(C, C) = C[\mathfrak{g}]$. Conversely if C admits a p -basis over a field A , we show that there is a higher derivation D on C with $\text{Hom}_A(C, C) = C[D]$. So no nontrivial ideal can be stable under D . When $\mathfrak{g}$ is a set of ordinary derivations, the first statement is given in [4] and is essentially due to Harper [0]. When C is a field, these reduce to results of Sweedler [2] and Weisfeld [3]. We begin this paper with a construction of p -basis for local algebras of finite type.

All rings in the following are assumed to be commutative with 1 and of prime characteristic p . All modules and ring-homomorphisms are unitary. If C is an A -algebra, the structural map $A \rightarrow C$ is assumed to be one-to-one.

1. *p -generators.* For simplicity of notations, given a subset X of a ring Y we denote by $\mathfrak{F}^i(X)$ the subset $\{x^{p^i} \mid x \in X\}$ of Y .

Now let C be a local ring with Q as its maximal ideal. Let E be a C -algebra such that for some finitely generated nilpotent ideal J in E , $E = C + J$ as a C -module direct sum. Let $e = e(J)$ be the least integer such that $\mathfrak{F}^{e+1}(J) = 0$. Let $\mathfrak{b}_e$ be a subset of $\mathfrak{F}^e(J)$ such that $\{t + \mathfrak{F}^e((J + Q)J) \mid t \in \mathfrak{b}_e\}$ form a basis for $\mathfrak{F}^e(J)/\mathfrak{F}^e((J + Q)J)$ over the field $\mathfrak{F}^e(C)/\mathfrak{F}^e(Q) \cong \mathfrak{F}^e(C/Q)$. For each i , we are going to construct a subset $\mathfrak{b}_i$ of $\mathfrak{F}^i(J)$ with the property that

- (i) $\{t + \mathfrak{F}^i((J + Q)J) \mid t \in \mathfrak{b}_i\}$ form a basis for $\mathfrak{F}^i(J)/\mathfrak{F}^i((J + Q)J)$ over $\mathfrak{F}^i(C)/\mathfrak{F}^i(Q)$;
- (ii) $\mathfrak{b}_{i+1} = \{t^{p^i} \mid t \in \mathfrak{b}_i \text{ and } t^{p^i} \neq 0\}$, $0 \leq i < e$.

Assume we have already constructed $\mathfrak{b}_{i+1}$. Let $\mathfrak{b}'_i$ be a subset of $\mathfrak{F}^i(J)$ such that for all $t \in \mathfrak{b}_{i+1}$, $\mathfrak{b}'_i$ and $\{x \in \mathfrak{F}^i(J) \mid x^{p^i} = t\}$ has exactly one element in common.

Received by the editors September 16, 1968.

AMS Subject Classifications. Primary 13S0, 13G0.

Key Words and Phrases. Inseparable algebra, higher derivation, p -generators, p -basis.

Copyright © 1970, American Mathematical Society

Let b_i'' be a subset of $\{x \in \mathfrak{F}^i(J) \mid x^p = 0\}$ such that the residue classes $t + \mathfrak{F}^i((J+Q)J)$, $t \in b_i''$, form a basis for $\{x + \mathfrak{F}^i((J+Q)J) \mid x \in \mathfrak{F}^i(J) \text{ and } x^p = 0\}$ over $\mathfrak{F}^i(C)/\mathfrak{F}^i(Q)$. Since the monomials in b_{i+1} form a set of generators for the $\mathfrak{F}^{i+1}(C)$ -module $\mathfrak{F}^{i+1}(J)$, given $u \in \mathfrak{F}^i(J)$ there is a polynomial $\varphi = \varphi(b_i', C_i)$ in b_i' with coefficients in C_i , φ having no constant term, such that $(u - \varphi)^p = 0$. It follows from $u = (u - \varphi) + \varphi$ that the set $b_i = b_i' \cup b_i''$ meets all our requirements.

Hereafter $b = b_0$ will be called a set of p -generators for the decomposition $E = C + J$.

We recall that given an algebra X over a ring Y , for any x in X , the exponent of x is the least nonnegative integer $e(x)$ such that $x^{p^{e(x)}}$ is in Y . The exponent of X over Y is the maximum of $\{e(x) \mid x \in X\}$.

EXAMPLE. Let C be a local A -algebra of finite exponent e such that the A -module C is finitely generated and flat. Put $E = C \otimes_A C$. Then $E = C \otimes 1 + J$ where $J = (C \otimes 1) \cdot \{1 \otimes x - x \otimes 1 \mid x \in C\}$. We may assume that the elements of b are of the form $1 \otimes t - t \otimes 1$. From $E = (C \otimes 1)[b]$ it follows that the inclusion map $C \otimes_A A[\{t \mid 1 \otimes t - t \otimes 1 \in b\}] \rightarrow E$ is onto. And so the inclusion map $A[\{t \mid 1 \otimes t - t \otimes 1 \in b\}] \rightarrow C$ is onto because C over A is actually faithfully flat. In other words, the monomials $\prod t^i$, $1 \otimes t - t \otimes 1 \in b$, $0 \leq i < p^{e(t)}$, form a set of generators for the A -module C .

2. Higher derivations. By a higher derivation D of rank ρ , $0 < \rho < \infty$, on a ring C we mean a sequence of maps

$$D^{(i)}: C \rightarrow C, \quad 1 \leq i \leq \rho,$$

making the map

$$\begin{aligned} \varphi_D: C &\rightarrow C[t]/(t^{\rho+1}), \\ x &\rightarrow x + (D^{(1)}x)t + \cdots + (D^{(\rho)}x)t^\rho \end{aligned}$$

a ring-homomorphism. The kernel of D is the set

$$\{x \in C \mid \varphi_D(x) = x\} = \bigcap \{\text{kernel } D^{(i)} \mid 1 \leq i \leq \rho\}.$$

Given a set g of higher derivations on C , we shall denote by $m(g)$ the set of all monomials μ of the form $D_1^{(i_1)} \cdots D_s^{(i_s)}$, $D_i \in g$, $0 \leq i_i \leq \text{rank } D_i$, where $D_i^{(0)}$ as usual is understood to be the identity map on C . The degree of μ is the sum $i_1 + \cdots + i_s$. The kernel of g is the set $\bigcap \{\text{kernel } D \mid D \in g\}$. An ideal a in C is said to be stable under g if $\mu(a) \subset a$ for all μ in $m(g)$.

LEMMA 2.1. Let g be a set of higher derivations on a ring C . Write $A = \text{kernel } g$.

- A is a subring of C and any idempotent element in C belongs to A .
- If C has no ideal, except 0 and 1, stable under g , then A is a field.
- If A is a field and if the vector space dimension of C over A is finite, so is the exponent of C over A .
- If there is a positive integer α such that $p^\alpha > \max \{\text{rank } D \mid D \in g\}$, then the exponent of C over A is not greater than α .

(e) If A is a field and the exponent of C over A is $\alpha < \infty$, then $x^{p^\alpha} = 0$ for all nonunit x in C .

Proof. (a) Given a pair of ring-homomorphisms

$$R \begin{array}{c} \xrightarrow{u} \\ \xrightarrow{v} \end{array} S,$$

it is clear that $\{x \in R \mid u(x) = v(x)\}$ form a subring of R . In particular for any higher derivation D on C , kernel $D = \{x \in C \mid \varphi_D x = x\}$ form a subring of C . So A is a subring of C .

Let $D = (D^{(1)}, D^{(2)}, \dots, D^{(l)}, \dots)$ be a higher derivation on C . From

$$\sum_i (D^{(i)} x^p) t^i = \varphi_D(x^p) = \varphi_D(x)^p = \sum_i (D^{(i)} x)^p t^{pi}$$

we get

$$\begin{aligned} D^{(l)}(x^p) &= 0, \quad \text{if } l \neq 0(p), \\ D^{(lp)}(x^p) &= D^{(l)}(x)^p. \end{aligned}$$

Now given a positive integer l , we may write $l = qp^r$ with q relatively prime to p . If ε is any idempotent in C , then

$$D^{(l)}(\varepsilon) = D^{(qp^r)}(\varepsilon^{p^r+1}) = (D^{(q)}(\varepsilon^p))^{p^r} = 0.$$

So ε belongs to A .

(b) For any $x \neq 0$ in A and any y in C we have $\varphi_D(xy) = x\varphi_D(y)$, $D \in \mathfrak{g}$. So the ideal xC is stable under $\mathfrak{g}$ because $D^{(l)}(xy) = x(D^{(l)}y)$. So $xC = C$ and x is a unit in C . From $\varphi_D(x^{-1}) = \varphi_D(x)^{-1} = x^{-1}$ it follows that x^{-1} is also in A . Hence A must be a field.

(c) Let C_i denote the A -subalgebra of C generated by x^{p^i} , $x \in C$. We have $C_{i+1} \subset C_i \subset \text{kernel } D^{(i)}$ for all $i \neq 0(p)$. In particular the intersection of all C_i , $i = 0, 1, 2, \dots$, is contained in A . Since C is finite dimensional over A , there exists a positive integer α such that $C_\alpha = C_{\alpha+1} = C_{\alpha+2} = \dots$. The exponent of C over A is therefore at most α because C_α is contained in A .

(d) For any x in C , $D^{(l)}(x^{p^\alpha})$ is zero for all D in $\mathfrak{g}$. So the exponent is at most α .

(e) For any nonunit x in C , x^{p^α} as a nonunit in the field A must be zero.

LEMMA 2.2. Let $\mathfrak{g}$ be a set of higher derivations on a local ring C . Then the following two statements are equivalent.

(i) No ideal in C , except 0 and 1, is stable under $\mathfrak{g}$.

(ii) Given any nonunit $x \neq 0$ in C there is some $\mu \in \mathfrak{m}(\mathfrak{g})$ such that $\mu(x)$ is a unit in C .

Proof. (i) $\rightarrow$ (ii). Let $\mathfrak{a}$ be the nonzero ideal in C generated by $\{\mu(x) \mid \mu \in \mathfrak{m}(\mathfrak{g})\}$ which is clearly stable under $\mathfrak{g}$. So $\mathfrak{a} = C$ and one of the $\mu(x)$'s must be a unit because C is a local ring. (ii) $\rightarrow$ (i) is trivial.

If g is a set of higher derivations on a ring C with $A = \text{kernel } g$, then for any $D = \{D^{(1)}, \dots, D^{(n)}\}$ in g , both $1 \otimes D = \{1 \otimes D^{(1)}, \dots, 1 \otimes D^{(n)}\}$ and $D \otimes 1 = \{D^{(1)} \otimes 1, \dots, D^{(n)} \otimes 1\}$ are higher derivations on $C \otimes_A C$. Let $g \otimes g$ denote the set of all $1 \otimes D, D \otimes 1$ with $D \in g$. We have the following.

LEMMA 2.3. *Let g be a set of higher derivations on a ring C with kernel $g = A$. Assume no ideal in C , except 0 and 1, is stable under g . Then no ideal in $E = C \otimes_A C$, except 0 and 1, is stable under $g \otimes g$. The kernel of $g \otimes g$ is equal to A .*

Proof. We have an exact sequence

$$0 \longrightarrow A \longrightarrow C \xrightarrow{(D^{(i)})} \prod C.$$

Tensoring over A with C we get the exactness of

$$0 \longrightarrow A \otimes_A C \longrightarrow E \xrightarrow{(D^{(i)} \otimes 1)} \prod E.$$

This shows $\text{kernel } g \otimes g = (A \otimes_A C) \cap (C \otimes_A A) = A$.

Now assume α is a nonzero ideal in E which is stable under $g \otimes g$ and $\alpha \not\subseteq A$. Let $\sigma = x_1 \otimes y_1 + \dots + x_r \otimes y_r \neq 0$ be an element of α with r minimal. Clearly $r > 1$. Let $\mu \in m(g)$ such that $\mu(x_1)$ is a unit in C . The element

$$(\mu \otimes 1)\sigma = \mu(x_1) \otimes y_1 + \dots + \mu(x_r) \otimes y_r$$

cannot be zero because $y_1, \dots, y_r$ are linearly independent over the field A . Put $\sigma' = 1 \otimes y_1 + x'_2 \otimes y_2 + \dots + x'_r \otimes y_r$ where $x'_i = \mu(x_1)^{-1} \mu(x_i)$. Since $\sigma' \in \alpha$, it cannot belong to $A \otimes_A C$ otherwise r would be equal to 1 and we would get a contradiction. So $(D^{(i)} \otimes 1)\sigma' = (D^{(i)}x'_2) \otimes y_2 + \dots + (D^{(i)}x'_r) \otimes y_r$ is nonzero for some $D^{(i)}, D \in g$. We therefore get a contradiction to the minimality of r because $0 \neq (D^{(i)} \otimes 1)\sigma' \in \alpha$. So no nontrivial ideal in E is stable under g . This completes the proof of the lemma.

THEOREM 2.4. *Let g be a set of higher derivations on a ring C with $A = \text{kernel } g$. Assume C is finitely generated as an A -module and no ideal in C , except 0 and 1, is stable under g . Then C admits a p -basis over A .*

Proof. Since A is a field and C is finite dimensional over A , by Lemma 2.1, C is a local ring with nilpotent maximal ideal Q . Put

$$E = C \otimes_A C, \quad J = \{1 \otimes x - x \otimes 1 \mid x \in C\}E.$$

Let $\{1 \otimes x_1 - x_1 \otimes 1, \dots, 1 \otimes x_n - x_n \otimes 1\}$ be a set of p -generators for $E = C \otimes 1 + J$. We claim that $x_1, \dots, x_n$ form a p -basis for C over A . Let F be a subfield of C such that $C = F + Q$. Let $\{y_1, \dots, y_m\}$ be a set of p -generators for $C = F + Q$. It is clear that $\{y_1 \otimes 1, \dots, y_m \otimes 1, 1 \otimes x_1 - x_1 \otimes 1, \dots, 1 \otimes x_n - x_n \otimes 1\}$ form a set of p -generators for $E = F \otimes 1 + (Q \otimes 1 + J)$. Moreover, by a lemma to be established later,

$$\prod_{i=1}^m (y_i^{p^{e_i}-1} \otimes 1) \cdot \prod_{i=1}^n (1 \otimes x_i - x_i \otimes 1)^{p^{e_i}-1} \neq 0$$

where e_i (respectively f_i) is the exponent of $1 \otimes x_i - x_i \otimes 1$ (respectively y_i). It follows that for any $y \in C$,

$$(y \otimes 1) \prod_{i=1}^n (1 \otimes x_i - x_i \otimes 1)^{p^{e_i}-1} = 0$$

implies $y=0$. So $\{1 \otimes x_1 - x_1 \otimes 1, \dots, 1 \otimes x_n - x_n \otimes 1\}$ form a p -basis for E over $C \otimes 1$. Now from the binomial expansion of

$$((1 \otimes x_i - x_i \otimes 1) + x_i \otimes 1)^{d_i} = 1 \otimes x_i^{d_i},$$

it follows that $1 \otimes \prod_{i=1}^n x_i^{d_i}$ can be expressed as a polynomial in

$$\{1 \otimes x_i - x_i \otimes 1 \mid 1 \leq i \leq n\}$$

with coefficients in $C \otimes 1$ and with $\prod_{i=1}^n (1 \otimes x_i - x_i \otimes 1)^{d_i}$ as its highest degree term. This implies that $\{\prod_{i=1}^n x_i^{d_i} \mid 0 \leq d_i < p^{e_i}\}$ is linearly independent over A . Since the dimension of C over A is equal to the dimension of E over $C \otimes 1$, $\{x_1, \dots, x_n\}$ must be a p -basis for C over A .

COROLLARY 2.5. *Let C be a finite dimensional purely inseparable field extension over A . If A is the kernel of a set of higher derivations of C , then C admits a p -basis over A .*

Now let $x_1, \dots, x_m$ be elements of C . It follows from

$$\varphi_D\left(\prod_{i=1}^m x_i\right) = \prod_{i=1}^m \varphi_D(x_i)$$

that

$$D^{(l)}(x_1 \cdots x_m) = \sum \prod_{i=1}^m D^{(\alpha_i)} x_i$$

where the summation runs through all $(\alpha_1, \dots, \alpha_m)$, α_i nonnegative integers with $\sum_{i=1}^m \alpha_i = l$. Let $(l:m)$ denote the set of all these m -tuples and assume we are given $D_1^{(l_1)}, \dots, D_s^{(l_s)}$ where D_i are higher derivations on C . For any $(a_1, \dots, a_s)$, $a_i = (\alpha(i, 1), \dots, \alpha(i, m)) \in (l_i:m)$, set

$$(a_1, \dots, a_s)^*(x_1, \dots, x_m) = \prod_{j=1}^m \left(\prod_{i=1}^s D_i^{\alpha(i,j)} \right) x_j.$$

An induction on s gives the following formula.

$$D_1^{(l_1)} \cdots D_s^{(l_s)}(x_1 \cdots x_m) = \sum (a_1, \dots, a_s)^*(x_1, \dots, x_m), \quad a_i \in (l_i:m).$$

LEMMA 2.6. *Let C be a local ring with Q as its maximal ideal. Let E be a C -algebra such that $E = C + J$ as a C -module direct sum for some finitely generated nilpotent ideal J in E . Let $\pi: E = C + J \rightarrow J$ denote the second coordinate projection. Let $\mathfrak{g}$ be a set of higher derivations on E . Put $I = \{x \in J \mid \mu(x) \in Q + J \text{ for all } \mu \in \mathfrak{m}(\mathfrak{g})\}$.*

Assume $\pi\mu(I) \subset I$ for all $\mu \in \mathfrak{m}(\mathfrak{g})$. If $I \cap \mathfrak{F}^i(J) \subset \mathfrak{F}^i(QJ)$ for all i , then the product

$$t_1^{q_1} \cdots t_n^{q_n} \neq 0 \quad (I)$$

where $\{t_1, \dots, t_n\} = \mathfrak{b}$ is a set of p -generators for $E = C + J$, $q_i = p^{e_i} - 1$, $e_i = e(t_i)$ is the exponent of t_i with respect to C .

Proof by contradiction. Let m be the minimal integer such that for some integers m_i , $0 \leq m_i \leq p^{e_i} - 1$ and $\sum m_i = m$, we have

$$z = t_1^{m_1} \cdots t_n^{m_n} = 0 \quad (I).$$

We have $m > 1$ because $I \subset QJ$. We claim that $m_i = 0 \ (p)$ for all $i = 1, \dots, n$. Assume this is not the case. Let $m_1, \dots, m_r$ be nonzero modulo p while $m_i = 0 \ (p)$ for all $i > r$. Write

$$z_i = t_i^{m_i-1} \prod_{k \neq i} t_k^{m_k}, \quad i = 1, \dots, r.$$

The minimality of m asserts that z_i is nonzero modulo I . Let l be the least integer such that for some i , $1 \leq i \leq r$, $\mu(z_i)$ is a unit in E for some $\mu \in \mathfrak{m}(\mathfrak{g})$ with degree $\mu = l$. By a change of indices we may assume $i = 1$. Now $\mu(z) = \mu(t_1^{m_1} \cdots t_r^{m_r} \tau)$, $\tau = \prod_{k > r} t_k^{m_k}$, can be expressed as a polynomial in $\mathfrak{b}$ with coefficients in C . We are going to show that the coefficient of t_1 in $\mu(z)$, which modulo Q is unique, is a unit in C . This is not possible because $\pi\mu(z) \in I \subset QJ$. So m_i must be zero modulo p for all $i = 1, \dots, n$.

Put $\sigma = m_1 + \cdots + m_r$, $\mu = D_1^{(l_1)} \cdots D_s^{(l_s)}$ and let

$$a_i = (\alpha(i, 1, 1), \dots, \alpha(i, 1, m_1), \dots, \alpha(i, r, 1), \dots, \alpha(i, r, m_r), \alpha_i)$$

be a general element of $(l_i : \sigma + 1)$. Write

$$a = (a_1, \dots, a_s),$$

$$L(a, u, v) = \text{the coefficient of } t_1 \text{ in } E_{u,v} = \left(\prod_{i=1}^s D_i^{(\alpha(i,u,v))} \right) t_u,$$

$$C(a, u, v) = \text{the constant term of } \left(\prod_{(i,j) \neq (u,v)} E_{i,j} \right) \left(\prod_{i=1}^s D_i^{(\alpha_i)} \right) \tau.$$

Given an s -tuple $b = (\beta_1, \dots, \beta_s)$, $0 \leq \beta_i \leq l_i$, of integers, we denote by

$$A(b, u, v) \quad \text{the set } \{a \mid a_i \in (l_i : \sigma + 1) \text{ with } \alpha(i, u, v) = \beta_i\}.$$

Since the coefficient of t_1 in $(\prod_{i=1}^s D_i^{(\alpha_i)}) \tau$ is zero modulo Q , the modulo Q coefficient of t_1 in $\mu(z) = (D_1^{(l_1)} \cdots D_s^{(l_s)})(t_1^{m_1} \cdots t_r^{m_r} \tau)$ is

$$\sum_{u=1}^r \sum_{v=1}^{m_u} \sum_a C(a, u, v) L(a, u, v) = \sum_{u=1}^r \sum_{v=1}^{m_u} \sum_b \sum_{a \in A(b, u, v)} C(a, u, v) L(a, u, v).$$

We have the following cases

(i) Not all of β_i are zero. By the minimality of l , $\sum_{a \in A(b, u, v)} C(a, u, v)$ as the constant term of $(D_1^{(l_1 - \beta_1)} \cdots D_s^{(l_s - \beta_s)})z_u$ is zero modulo Q . Hence

$$\sum_{a \in A(b, u, v)} C(a, u, v)L(a, u, v)$$

is zero modulo Q .

(ii) $\beta_i = 0$ for all $i = 1, \dots, s$ but $u \neq 1$. $\sum_{a \in A(b, u, v)} C(a, u, v)L(a, u, v)$ is zero modulo Q because $L(a, u, v)$ is.

(iii) $\beta_i = 0$ for all $i = 1, \dots, s$ and $u = 1$. Let $\mu(z_1) = \gamma + \nu$ with $\gamma \in C$ and $\nu \in J$. So

$$\sum_{a \in A(b, 1, v)} C(a, 1, v)L(a, 1, v) = \gamma.$$

This shows $\pi\mu(z) = 0$ modulo I has a modulo Q nonzero linear term $m_1\gamma t_1$ which is the desired contradiction.

Recall that the integer $e = e(J)$ is the least integer such that $\mathfrak{F}^{e+1}(J) = 0$. From what we have shown we see that the lemma is true for $e = 0$. Moreover, if the lemma is incorrect for some $e > 0$, then it is also incorrect for $\mathfrak{F}(E) = \mathfrak{F}(C) + \mathfrak{F}(J)$ with $e(\mathfrak{F}(J)) = e(J) - 1$. An induction on e completes the proof of the lemma.

3. The endomorphism ring. We begin with a slight rewording of the Jacobson-Bourbaki theorem. The proofs are adapted from Hochschild [1, Lemma 2.1 and Theorem 2.1].

LEMMA 3.1. *Let C be a local ring with nilpotent maximal ideal Q . Let Ω be an $n < \infty$ dimensional free C -submodule of $\text{Hom}_Z(C, C)$ where Z is the ring of all integers. Then there exist $c_1, \dots, c_n$ in C and a C -module basis $\omega_1, \dots, \omega_n$ for Ω such that $\omega_i(c_j) = \delta_{ij}$.*

Proof. Let $T_{0,1}, \dots, T_{0,n}$ be any C -module basis for Ω . We first observe that $T_{0,i}(C) \not\subset Q$ for all $i = 1, \dots, n$. For if e is the least integer such that $Q^e = 0$, then from $T_{0,i}(C) \subset Q$ we get $uT_{0,i} = 0$ and hence $u = 0$ for any u in Q^{e-1} which is absurd.

Now suppose we have already found $c_1, \dots, c_l$ in C and a C -module basis $T_{1,1}, \dots, T_{l,n}$ of Ω such that $T_{l,i}(c_j) = \delta_{ij}$, for $1 \leq i \leq n$ and $1 \leq j \leq l$. If $l < n$, there is an element $c_{l+1} \in C$ such that $T_{l,l+1}(c_{l+1})$ is a unit in C . We set $T_{l+1,l+1} = T_{l,l+1}(c_{l+1})^{-1}T_{l,l+1}$, so that $T_{l+1,l+1}(c_{l+1}) = 1$. For every $i \neq l+1$, we set $T_{l+1,i} = T_{l,i} - T_{l,i}(c_{l+1})T_{l+1,l+1}$. Then we have $T_{l+1,i}(c_j) = \delta_{ij}$, for $1 \leq i \leq n$ and $1 \leq j \leq l+1$, and that $T_{l+1,i}$ are still a C -module basis for Ω . Proceeding in this fashion, starting from the case $l = 0$, we finally obtain $c_1, \dots, c_n$ in C and $\omega_i = T_{n,i}$ which satisfy the requirements of the lemma.

LEMMA 3.2. *Let C be a ring and Ω a (not necessarily commutative) subring of $\text{Hom}_Z(C, C)$. Assume that Ω is a free C -module based on $\omega_1, \dots, \omega_n$ ($n < \infty$) such that for some $c_1, \dots, c_n$ in C , $\omega_i(c_j) = \delta_{ij}$. Let A denote the subring $\{c \in C \mid \omega(cx) = c\omega(x) \text{ for all } x \in C \text{ and all } \omega \text{ in } \Omega\}$ of C . Then C is a free A -module based on $c_1, \dots, c_n$ and $\Omega = \text{Hom}_A(C, C)$.*

Proof. Given ω in Ω , if we write $\omega = \sum_{i=1}^n x_i \omega_i$, $x_i \in C$, then $x_i = (\sum_{j=1}^n x_j \omega_j)(c_i) = \omega(c_i)$. In particular,

$$\omega_i(x\omega_j) = \sum_{i=1}^n (\omega_i(x\omega_j))(c_i) \omega_i = \omega_i(x) \omega_j \quad (x \in C).$$

So for any c in C , $\omega_i(x)\omega_j(c) = \omega_i(x\omega_j(c))$. It follows that $\omega_j(c) \in A$ for all $c \in C$ and $j=1, \dots, n$. Now let $c \in C$ and write $c' = c - \sum_{i=1}^n \omega_i(c)c_i$. We have $\omega_j(c')=0$ for all $j=1, \dots, n$. So $c'=0$ because ω_j form a basis for Ω which as a subring of $\text{Hom}_Z(C, C)$ contains the identity map on C . This shows $c = \sum_{i=1}^n \omega_i(c)c_i$ for all c in C . If $\sum_{i=1}^n \alpha_i c_i = 0$, $\alpha_i \in A$, then $\alpha_i = \omega_i(\sum_{j=1}^n \alpha_j c_j) = 0$. Hence $c_1, \dots, c_n$ form a basis for C over A . Given any f in $\text{Hom}_A(C, C)$, we have $f = \sum_{i=1}^n f(c_i)\omega_i$. So $\Omega = \text{Hom}_A(C, C)$. This completes the proof of the lemma.

THEOREM 3.3. *Let C be a local ring with nilpotent maximal ideal Q . Let $\mathfrak{g}$ be a set of higher derivations on C such that no ideal in C , except 0 and 1, is stable under $\mathfrak{g}$. Let A denote the kernel of $\mathfrak{g}$ and write $\Omega = C[\mathfrak{g}]$. If Ω is finitely generated as a C -module, then $\Omega = \text{Hom}_A(C, C)$.*

Proof. In view of Lemmas 3.1 and 3.2 above, it suffices to show that Ω is a finite dimensional free C -module. Let $\omega_1, \dots, \omega_n$ be elements in $\mathfrak{m}(\mathfrak{g}) \subset \Omega$ such that the $\omega_i + Q\Omega$ form a basis for $\Omega/Q\Omega$ over C/Q . It follows from [5, p. 105, Corollaire 2] that $\omega_1, \dots, \omega_n$ generate Ω as a C -module. If $\sum_{i=1}^n x_i \omega_i = 0$ ($x_i \in C$), then $x_i \in Q$. Assume that not all the x_i are zero. Let μ be an element in $\mathfrak{m}(\mathfrak{g})$ with minimal degree such that $\mu(x_i)$ is a unit in C for some i (Lemma 2.2). We have

$$0 = \mu\left(\sum_{j=1}^n x_j \omega_j\right) \equiv \sum_{j=1}^n \mu(x_j) \omega_j \text{ modulo } Q\Omega$$

which is a contradiction to the choice of ω_j . This shows that Ω is a free C -module based on $\omega_1, \dots, \omega_n$ as desired.

4. One derivation. Let C be an algebra over a field A . Assume C over A admits a p -basis $\{t_1, \dots, t_r\}$. We may assume the t_i 's are units. For if t_i is not a unit, it must be a nilpotent so can be replaced by $1+t_i$. Let e_i be the exponent of t_i . By a change of indices we may assume $e_1 \geq \dots \geq e_r$. Let $D = \{D^{(1)}, \dots, D^{(p-1)}\}$, $\rho = p^{e_1}$, be the higher derivation on C corresponding to the A -algebra homomorphism

$$\begin{aligned} \varphi_D: C &\rightarrow C[z]/(z^\rho), \\ t_1 &\rightarrow t_1 + z, \\ t_{i+1} &\rightarrow t_{i+1} + \gamma_{i+1} z^{q_i+1}, \end{aligned}$$

where $\gamma_{i+1} = \prod_{l \leq i} t_l^{-1}$, $q_{i+1} = p^{e_1 - e_{i+1}}$. We have the following

THEOREM 4.1. *With notations as above,*

$$(E) \quad C[D] = \text{Hom}_A(C, C).$$

Proof. The assertion is obviously true for $r=1$. When $r=1$ the following statement (H) is also true.

(H) Given a_λ in A , $0 < \lambda < p^{e_r}$, if there exists $x \in C$ such that

$$\begin{aligned} D^{(\lambda q_r)} x &= a_\lambda \gamma_{r+1}^\lambda, & 0 < \lambda < p^{e_r}, \\ D^{(l)} x &= 0, & l \neq 0 \ (q_r), \end{aligned}$$

then $x \in A[t_r]$ and $a_\lambda = 0$ for all λ .

We are going to establish the following chain of implications:

(E) and (H) for all $r < s \Rightarrow$ (H) for $r = s \Rightarrow$ (E) for $r = s$.

Write

$$x = \sum_{i=0}^{n-1} x_i t_s^i, \quad (n = p^{e_s}, x_i \in A[t_1, \dots, t_{s-1}]).$$

We have, for all $l > 0$,

$$\begin{aligned} (1) \quad D^{(l)} x &= \sum_{i=0}^{n-1} D^{(l)}(x_i t_s^i) \\ &= \sum_{i=0}^{n-1} \sum_{\lambda} (D^{(l-\lambda q_s)} x_i) D^{(\lambda q_s)} t_s^i \\ &= \sum_{i=0}^{n-1} \sum_{\lambda} \binom{i}{\lambda} \gamma_s^\lambda t_s^{i-\lambda} (D^{(l-\lambda q_s)} x_i) \\ &= \sum_{j=0}^{n-1} t_s^j \sum_{i \geq j} \binom{i}{i-j} \gamma_s^{i-j} (D^{(l-(i-j)q_s)} x_i). \end{aligned}$$

Taking into account the assumption placed on x in the statement (H), we get for $l \neq 0 \ (q_s)$,

$$(2) \quad \sum_{i \geq j} \binom{i}{i-j} \gamma_s^{i-j} D^{(l-(i-j)q_s)} x_i = 0, \quad 0 \leq j \leq n-1.$$

In particular for $j=n-1$, we get

$$(3) \quad D^{(l)} x_{n-1} = 0$$

for all $l \neq 0 \ (q_s)$. Putting $j=n-2$ in (2) and taking into account (3) we get $D^{(l)} x_{n-2} = 0$ for all $l \neq 0 \ (q_s)$. Hence

$$(4) \quad D^{(l)} x_i = 0$$

for all i and all $l \neq 0 \ (q_s)$. Now put $l = \lambda q_s$ ($\lambda \neq 0$) in (1). From (H) we get

$$a_\lambda \gamma_{s+1}^\lambda = \sum_{j=0}^{n-1} t_s^j \sum_{i \geq j} \binom{i}{i-j} \gamma_s^{i-j} D^{(\lambda - i + j q_s)} x_i.$$

So

$$\sum_{i \geq j} \binom{i}{i-j} \gamma_s^{i-j} D^{(i-j)q_s} x_i = a_\lambda \theta_s \gamma_s^\lambda, \quad j = n-\lambda,$$

$$= 0, \quad j \neq n-\lambda,$$

where $\theta_s = (t_s^{p^e s})^{-1}$. In particular

$$D^{(q_s)} x_{n-1} = a_1 \theta_s \gamma_s; \quad D^{(\lambda q_s)} x_{n-1} = 0 \quad (\lambda \neq 1).$$

By induction hypothesis we get $a_1 = 0$. So $D^{(l)} x_{n-1} = 0$ for all $l \neq 0$. Applying the induction hypothesis again, we get $x_{n-1} \in A$.

Now assume $a_i = 0$, $x_{n-i} \in A$ for all $1 \leq i < k$. So

$$D^{(\lambda q_s)} x_{n-k} = 0 \quad \text{for } \lambda > k$$

$$D^{(k q_s)} x_{n-k} = a_k \theta_s \gamma_s^k$$

$$D^{(\lambda q_s)} x_{n-k} = -\binom{n-k+\lambda}{\lambda} \gamma_s^\lambda x_{n-k+\lambda} \quad \text{for } 1 \leq \lambda < k.$$

The induction hypothesis asserts that $a_k = 0$, $D^{(l)} x_{n-k} = 0$ for all $l > 0$. So x_{n-k} is also in A . This shows (H) is correct for $r = s$. In particular the kernel of D is contained in $A[t_s]$. We claim that kernel D is exactly A .

Let $x = \sum_{i=0}^l x_i t_s^i$, $x_i \in A$, $x_i \neq 0$, be an element of kernel D with l minimal. If l is greater than zero, then

$$D^{(l q_s)} x = \sum_{i=0}^l x_i D^{(l q_s)} t_s^i = x_l D^{(l q_s)} t_s^l = x_l \gamma_s^l$$

is not zero because γ_s^l is a unit; hence a contradiction.

We now contend that kernel $D = A$ implies $\text{Hom}_A(C, C) = C[D]$. Let M be the set of all monomials $t_1^{u_1} \cdots t_s^{u_s}$, $0 \leq u_i < p^{e_i}$. A lexicographic order may be imposed on M as follows: $t_1^{u_1} \cdots t_s^{u_s} < t_1^{v_1} \cdots t_s^{v_s}$ if there is a k such that $u_k < v_k$ and $u_i = v_i$ for all $l > k$. Given $f = \sum_{u_1, \dots, u_s} f_{u_1, \dots, u_s} t_1^{u_1} \cdots t_s^{u_s}$, $f_{u_1, \dots, u_s} \in A$, we denote by $0(f)$ the smallest element of M such that $t_1^{u_1} \cdots t_s^{u_s} \leq 0(f)$ whenever $f_{u_1, \dots, u_s}$ is not zero. We would like to show that given $x \neq 0$ in C there is some $\mu \in \mathfrak{m}(D)$ such that $\mu(x)$ is a unit in C . Assume this is not the case. Let $f = \sum_{u_1, \dots, u_s} f_{u_1, \dots, u_s} t_1^{u_1} \cdots t_s^{u_s}$, $f_{u_1, \dots, u_s} \in A$, be a nonzero element in C with the least $0(f)$ such that $\mu(f)$ is not a unit for any $\mu \in \mathfrak{m}(D)$. Since $0(D^{(l)} \zeta) < \zeta$ for all $l > 0$ and $\zeta \neq 1$ in M , f must belong to kernel D which is the field A . But f is not a unit so must be zero, hence a contradiction. This shows that no ideal in C , except 0 and 1, is stable under D (Lemma 2.2). It follows from Theorem 3.3 that $C[D] = \text{Hom}_A(C, C)$.

REFERENCES

0. L. R. Harper, *On differentially simple algebras*, Trans. Amer. Math. Soc. **100** (1961), 63-72. MR **24** #A116.
1. G. Hochschild, *Double vector spaces over division rings*, Amer. J. Math. **71** (1949), 443-460. MR **10**, 676.

2. M. Sweedler, *Structure of inseparable extensions*, Ann. of Math. (2) **87** (1968), 401–410. MR **36** #6391.
3. M. Weisfeld, *Purely inseparable extensions and higher derivations*, Trans. Amer. Math. Soc. **116** (1965), 435–449. MR **33** #122.
4. Shuen Yuan, *Differentiably simple rings of prime characteristic*, Duke Math. J. **31** (1964), 623–630. MR **29** #4772.
5. N. Bourbaki, *Algèbre commutative*. Chapitres I, II, Actualités Sci. Indust., no. 1290, Hermann, Paris, 1961. MR **36** #146.

STATE UNIVERSITY OF NEW YORK AT BUFFALO,
AMHERST, NEW YORK 14226