Can. J. Math., Vol. XXX, No. 2, 1978, pp. 401–418

HIGHER DERIVATIONS AND TENSOR PRODUCTS OF COMMUTATIVE RINGS

W. C. BROWN

1. Introduction. The genesis of this paper is the following well known result in field theory: Let R denote a field of characteristic $p \neq 0$, and let k denote a subfield of R such that $R^{p^e} \subset k$ for some e sufficiently large. Then R is isomorphic to the tensor product (over k) of primitive extensions of k if and only if there exists a finite set Γ of k-higher derivations on R such that k is the field of constants of Γ. A proof of this theorem can be found in [**6**].

In this paper, we explore how much of this theorem remains true if R and k are arbitrary commutative rings. In other words, we are interested in the following conjecture: Let R/k be an extension of commutative rings. Suppose the characteristic of k is either zero or a prime p. Then $R \cong \otimes\, k[x_i]$ (the tensor product over k) if and only if there exists a finite set Γ of k-higher derivations on R such that k is the ring of constants of Γ.

This conjecture is, of course, a bit too optimistic. In fact, both directions in the conjecture are false. For instance, if k is a ring of prime characteristic, and $R = k[X_1, \ldots, X_n]$ is a polynomial ring in n-indeterminates over k, then $R \cong \otimes\, k[X_i]$. But, k is never the ring of constants of any finite set Γ of k-higher derivations on R. This fact follows from elementary considerations concerning higher derivations. We shall discuss this point more carefully in the next section of this paper. Conversely, we can easily construct examples R/k and Γ such that k is the ring of constants of Γ, but R fails to be a tensor product of primitive extensions of k. A specific case is Example 1 in this paper.

Thus, a more encouraging problem is the following: Let R/k be an extension of commutative rings with the characteristic of k being zero or a prime p. Let $\Gamma = \{D_1, \ldots, D_n\}$ be a finite set of k-higher derivations of R, and let R_Γ be the ring of constants of Γ. What further conditions on Γ will allow us to conclude that there exist elements $x_1, \ldots, x_n \in R - R_\Gamma$ such that $R \cong \otimes\, R_\Gamma[x_i]$?

The theorems in this paper together with the examples will give a fairly complete answer to this question.

2. Preliminaries. Throughout this entire paper, R and k will denote commutative, associative rings with identity. We shall always assume that the characteristic of k is either zero or a prime p. We say that R is an *extension* of k if $R \supset k$, and the identity of k is the same as the identity of R. If R is an extension of k, then we shall indicate this fact by writing R/k.

Received February 8, 1977.

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

Let R/k be an extension. A *k-higher derivation* D on R/k is a finite sequence $D = \{d_0, d_1, \ldots, d_m\}$ of k-endomorphisms of R such that $d_0 = I$, the identity map on R, and

$$(1) \quad d_r(xy) = \sum \{d_{r-j}(x)d_j(y)\,|\,0 \leqq j \leqq r\}.$$

Here, of course, equation (1) is to hold for all $x, y \in R$ and for all $r \leqq m$. By the rank (rk D) of D, we shall mean the largest integer $l \leqq m$ such that $d_l \neq 0$. We shall refer to $d_1, \ldots, d_l$ as the *components* of D. If $\Gamma = \{D_1, \ldots, D_n\}$ is any finite set of k-higher derivations, then we shall refer to the components of D_i as D_{ij} $(1 \leqq j \leqq \text{rk } D_i)$.

We shall also need the notion of a k-higher derivation E of infinite rank on R/k. E is just an infinite sequence $E = \{e_0, e_1, \ldots\}$ of k-endomorphisms of R such that for every m, $E^{(m)} = \{e_0, e_1, \ldots, e_m\}$ is a k-higher derivation on R/k. $E^{(m)}$ is called the mth *section* of E.

Now suppose $\Gamma = \{D_1, \ldots, D_n\}$ is any finite set of k-higher derivations on R/k. By the *ring of constants* R_Γ of Γ, we shall mean the set of all $x \in R$ such that $D_{ij}(x) = 0$ for all $1 \leqq i \leqq n$ and $1 \leqq j \leqq \text{rk } D_i$. One can easily verify that R_Γ is a subring of R containing k.

Let R/k be an extension and let S be a subring of R. If $x_1, \ldots, x_n$ are any elements of R, then we have a natural mapping $\varphi : \otimes_S S[x_i] \rightarrow R$ given by

$$\varphi\left(\sum s_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \otimes \ldots \otimes x_n^{\alpha_n}\right) = \sum s_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

In particular, if Γ is a set of k-higher derivations on R, and $x_1, \ldots, x_n \in R - R_\Gamma$, then we have a natural mapping φ: $\otimes_{R_\Gamma} R_\Gamma[x_i] \rightarrow R$. Throughout this paper, all tensor products will be over some ring of constants R_Γ. We shall therefore drop the R_Γ symbol on the tensor product and merely write $\otimes R_\Gamma[x_i]$. When we write $R \cong \otimes R_\Gamma[x_i]$, we mean that the natural mapping φ: $\otimes R_\Gamma[x_i] \rightarrow R$ is an isomorphism (onto).

We complete our preliminary remarks with an important identity that higher derivations satisfy if the characteristic of k is a prime p. Let R/k be an extension of characteristic p, and let $D = \{d_0, d_1, \ldots, d_m\}$ be a k-higher derivation on R. Then equation (1) implies that D induces a k-algebra homomorphism ψ_D: $R \rightarrow R[T]/(T^{m+1})$, T an indeterminate, given by

$$(2) \quad \psi_D(x) = x + d_1(x)T + \ldots + d_m(x)T^m.$$

Since the characteristic of k is $p \neq 0$, the map sending x to x^{p^e} is also a ring homomorphism of R. Thus, $\psi_D(x^{p^e}) = \{\psi_D(x)\}^{p^e}$. Using the fact that $R[T]/(T^{m+1})$ is a free R-module with basis $\{1, T, \ldots, T^m\}$, the identity $\psi_D(x^{p^e}) = \{\psi_D(x)\}^{p^e}$ gives us the following relationships:

$$(3) \quad d_j(x^{p^e}) = \begin{cases} 0 & \text{if } p^e \nmid j \\ \{d_r(x)\}^{p^e} & \text{if } j = rp^e \end{cases}$$

for $1 \leqq j \leqq m$.

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

Now suppose R_D denotes the ring of constants of D in the above discussion. Then equation (3) implies that there exists an e sufficiently large such that $R^{p^e} \subset R_D$. Thus, if $\Gamma = \{D_1, \ldots, D_n\}$ is any finite set of k-higher derivations on R, then there exists an e sufficiently large such that $R^{p^e} \subset R_\Gamma$. This fact explains the remark made in the example in the introduction. In that example, $k \neq R_\Gamma$ for any Γ because $R_\Gamma \supset k[X_1^{p^e}, \ldots, X_n^{p^e}]$ for some e sufficiently large.

If the characteristic of k is a prime p, we have seen that $R^{p^e} \subset R_\Gamma$ for some e sufficiently large. In particular, if $x \in R$, then some power of x lies in R_Γ. We define the integer $\mu_\Gamma(x)$ to be the smallest positive integer q such that $x^q \in R_\Gamma$. If R and k are both fields, then $\mu_\Gamma(x)$ is always a power of p. This result continues to hold for arbitrary rings of characteristic p under suitable conditions. We discuss this in the next section.

3. Main results. We return now to the main problem. Let R/k be an extension, and suppose that $\Gamma = \{D_1, \ldots, D_n\}$ is a finite set of k-higher derivations on R/k. Suppose that there exist elements $x_1, \ldots, x_n \in R$ such that

$$(4) \qquad D_{ij}(x_k) = \begin{cases} 0 & \text{if } k \neq i,\ 1 \leqq j \leqq \operatorname{rk} D_i \\ 1 & \text{if } k = i, \text{ and } j = 1. \end{cases}$$

If such elements $x_1, \ldots, x_n$ exist in R, we shall indicate this fact by saying $(D_1, \ldots, D_n | x_1, \ldots, x_n)$ satisfy (4).

Our first goal is to prove the following theorem:

THEOREM 1. *Suppose R/k is an extension of prime characteristic p, or R/k is an extension of characteristic zero in which no nonzero integer is a zero-divisor in R. Let $\Gamma = \{D_1, \ldots, D_n\}$ be a set of k-higher derivations on R/k, and suppose there exist elements $x_1, \ldots, x_n \in R - R_\Gamma$ such that $(D_1, \ldots, D_n | x_1, \ldots, x_n)$ satisfy (4). Then $R_\Gamma[x_1, \ldots, x_n] \cong \otimes R_\Gamma[x_i]$.*

To prove Theorem 1, we divide it into two cases (characteristic p or zero) and proceed by a series of lemmas which are of interest in their own right.

3A. The characteristic p case.

LEMMA 1. *Suppose R/k is an extension of prime characteristic p. Let $D = \{d_0, d_1, \ldots, d_m\}$ be a k-higher derivation on R. Set $R_D = \{z \in R | d_j(z) = 0, j \geqq 1\}$. Suppose there exists an element $x \in R$ such that $d_1(x) = 1$. Then*

(α) *$\mu_{R_D}(x) = p^f$ for some $f \geqq 1$,*

(β) *$p^{f-1} \leqq \operatorname{rk} D < p^f$, and*

(γ) *if $c\, x^i = 0$ for some $c \in R_D$ and some $i < \mu_{R_D}(x)$, then $c = 0$.*

Proof. From the remarks in the preliminaries, we know that $R^{p^e} \subset R_D$ for some e sufficiently large. Thus, $\mu_{R_D}(z)$ is a well defined function on R. Since $d_1(x) = 1$, we see $x \notin R_D$. Thus, $\mu_{R_D}(x) > 1$. Let us set $q = \mu_{R_D}(x)$. Then $x^q \in R_D$. So $0 = d_1(x^q) = q\ x^{q-1}$. If $p \nmid q$, then $x^{q-1} = 0$. In particular,

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

$x^{q-1} \in R_D$. This contradicts the definition of q. Thus, $p|q$. Now write $q = np^f$, for some $f \geqq 1$ and n relatively prime to p.

Now if $p^f > \operatorname{rk} D$, then equation (3) implies that $d_j(x^{p^f}) = 0$ for all $j = 1, \ldots, m$. Thus, $x^{p^f} \in R_D$. Since $p^f \leqq n\, p^f$, we conclude that $n = 1$. So, $\mu_{R_D}(x) = p^f$ in this case.

If $p^f \leqq \operatorname{rk} D$, then d_{p^f} is well defined. Using (3), we have:

$$(5) \qquad 0 = d_{p^f}(x^{np^f}) = \{d_1(x^n)\}^{p^f} = \{n\, x^{n-1}\}^{p^f}.$$

Since n is a unit in R, we conclude from (5) that $x^{(n-1)p^f} \in R_D$. Again since $(n-1)p^f < n\, p^f$, we must have $(n-1)p^f = 0$, i.e. $n = 1$. Thus, the proof of (α) is complete.

As for (β), we have already noted that $\operatorname{rk} D < p^f$. For if $\operatorname{rk} D \geqq p^f$ then d_{p^f} is defined and we would have $0 = d_{p^f}(x^{p^f}) = \{d_1(x)\}^{p^f} = 1$. On the other hand, if $\operatorname{rk} D < p^{f-1}$, then (3) implies $x^{p^{f-1}} \in R_D$ (a contradiction since $p^{f-1} < p^f$). Thus, $\operatorname{rk} D \geqq p^{f-1}$, and (β) is established.

For the proof of (γ), we proceed via induction on i. Suppose $cx = 0$ for some $c \in R_D$. Applying d_1 to this equation gives $c = 0$. Thus, (γ) is established if $i = 1$. So, assume $cx^l = 0$ some $1 < l < p^f = \mu_{R_D}(x)$. If $(p, l) = 1$, then applying d_1 to $cx^l = 0$ gives $clx^{l-1} = 0$. Since l is a unit in R, we conclude $cx^{l-1} = 0$. Thus, by induction, $c = 0$. Therefore, we can assume $p|l$. Since $p \leqq l < p^f$, the p-adic expansion of l has the following form:

$$(6) \qquad l = a_i p^i + \ldots + a_{f-1}p^{f-1}.$$

Here $1 \leqq i \leqq f - 1$, and $0 < a_i < p$. Now $p^i \leqq p^{f-1} \leqq \operatorname{rk} D$ by (β). So, $d_{,}$ is well defined. We need the following fact: For any $y, z \in R$, we have

$$(7) \qquad d_{p^i}(zy^{p^N}) = y^{p^N} d_{p^i}(z) \quad \text{whenever } N > i.$$

Equation (7) follows easily from equations (1) and (3). If we now apply d_{p^i} to the equation $cz^l = 0$ and use (6) and (7), we get

$$(8) \qquad c\, a_i^{pl}\, x^{(a_i-1)p^i + a_{i+1}p^{i+1} + \ldots + a_{f-1}p^{f-1}} = 0.$$

Since $a_i^{p^i}$ is a unit in k and the exponent in (8) is smaller than l, we conclude by induction that $c = 0$. This completes the proof of Lemma 1.

We can now give a proof of Theorem 1 if the characteristic of k is a prime p.

Proof of Theorem 1 (char $k = p$). Choose any i such that $1 \leqq i \leqq n$. Then by equation (4), $x_i \in \bigcap_{l \neq i} R_{D_l}$ (R_{D_l} being, of course, the ring of constants of D_l.) Since $R_\Gamma = R_{D_i} \cap (\bigcap_{l \neq i} R_{D_l})$, we conclude that $\mu_\Gamma(x_i) = \mu_{R_{D_i}}(x_i)$. Thus, by Lemma 1, $\mu_\Gamma(x_i) = p^{f_i}$ for some $f_i \geqq 1$. Further, $p^{f_i - 1} \leqq \operatorname{rk} D_i < p^{f_i}$, and property (γ) holds for any $c \in R_{D_i}$.

We now claim that $R_{D_i}[x_i]$ is a free R_{D_i}-module with basis $S_i = \{x_i^\alpha | 0 \leqq \alpha < \mu_\Gamma(x_i)\}$. Since $x_i^{pf_i} \in R_{D_i}$, we see that the elements of S_i generate the R_{D_i}-module $R_{D_i}[x_i]$. So, it remains to argue that the elements of S_i are linearly independent over R_{D_i}. Suppose we have some non-trivial relation among the

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

elements of S_i, say,

$$(9)\quad c_t x_i^t + \ldots + c_1 x_i + c_0 = 0.$$

Here the c_j are in R_{D_i} $(0 \leqq j \leqq t)$ and are not all zero. Further $t \leqq p^{f_i} - 1$. Among all such non-trivial relations as in (9), we can pick one in which t is as small as possible. Say this relation is

$$(10)\quad c_m x_i^m + \ldots + c_1 x_i + c_0 = 0.$$

Here $c_j \in R_{D_i}$ for $0 \leqq j \leqq m$, $c_m \neq 0$, and $1 \leqq m \leqq p^{f_i} - 1$. If some exponent present in (10) is not divisible by p, say l, then applying D_{i1} to (10) gives

$$(11)\quad mc_m x_i^{m-1} + \ldots + lc_l x^{l-1} + \ldots + c_1 = 0.$$

Since this is a relation among the elements of S_i of smaller degree than m, we conclude that every coefficient in (11) is zero. But then $c_l = 0$. This is a contradiction, since we are assuming $c_l x^l$ is present in (10). Thus, we can assume the exponents present in (10) are all divisible by p. Set $f(T) = c_m T^m + \ldots + c_0 \in R_{D_i}[T]$ (T an indeterminant). Then we can find an $e \geqq 1$ and sufficiently large such that $f(T) \in R_{D_i}[T^{p^e}] - R_{D_i}[T^{p^{e+1}}]$. Thus, $f(x_i) = 0$ can be written as

$$(12)\quad \sum_{l=0}^{K} c_{lp^e} x_i^{lp^e} = 0.$$

Here $Kp^e = m$. Now $\mu_\Gamma(x_i) = p^{f_i} > m \geqq p^e$. Thus, $e \leqq f_i - 1$. Consequently, D_{ip^e} is well defined. We now apply D_{ip^e} to (12). Using (3), we get

$$(13)\quad \sum_{l=1}^{K} c_{lp^e} l^{p^e} x_i^{(l-1)p^e} = 0.$$

Equation (13) is a relation among the elements of S_i of degree less than m. Consequently, the coefficients $l^{p^e} c_{lp^e}$ in (13) are zero. But this implies $p|l$ for all l appearing in (12). So, $f(T) \in R_{D_i}[T^{p^{e+1}}]$. This is a contradiction. Thus, we have shown that $R_{D_i}[x_i]$ is a free R_{D_i}-module with basis S_i.

Now the same proof shows that $R_\Gamma[x_i]$ is a free R_Γ-module with basis S_i. Thus, $\otimes R_\Gamma[x_i]$ is a free R_Γ-module with basis $\{x_1^{\alpha_1} \otimes \ldots \otimes x_n^{\alpha_n} | 0 \leqq \alpha_i < \mu_\Gamma(x_i)\}$. Now let $\varphi: \otimes R_\Gamma[x_i] \rightarrow R_\Gamma[x_1, \ldots, x_n]$ be the natural mapping, i.e. φ is given by

$$(14)\quad \varphi\left(\sum c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \otimes \ldots \otimes x_n^{\alpha_n}\right) = \sum c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Clearly φ is onto. The fact that φ is one-to-one follows easily from the fact that

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

$R_{D_i}[x_i]$ is a free R_{D_i}-module with basis S_i. For suppose $\sum c_{\alpha_1\ldots\alpha_n}x_1^{\alpha_1}\ldots x_n^{\alpha_n} = 0$ for some $c_{\alpha_1\ldots\alpha_n} \in R_\Gamma$, and $0 \leqq \alpha_i < \mu_\Gamma(x_i)$. Then we can rewrite $\sum c_{\alpha_1\ldots\alpha_n}x_1^{\alpha_1}\ldots x_n^{\alpha_n} = 0$ in the form:

$$(15)\quad \sum_{\alpha_1}\left(\sum c_{\alpha_1\ldots\alpha_n}x_2^{\alpha_2}\ldots x_n^{\alpha_n}\right)x_1^{\alpha_1} = 0.$$

The terms in parentheses in (15) lie in R_{D_i} and so are all zero. Induction now gives us every $c_{\alpha_1\ldots\alpha_n} = 0$. Thus, φ is an isomorphism and the proof of Theorem 1 in the characteristic p case is complete.

Before proceeding with the proof of Theorem 1 in the characteristic zero case, we give an example in characteristic p which shows that we cannot omit the hypothesis that $(D_1, \ldots, D_n|x_1, \ldots, x_n)$ satisfy equation (4).

Example 1. Let k be a field of characteristic two and set $S = k[X_1, X_2]$, a polynomial ring in two variables X_1 and X_2 over k. We define two first order k-derivations D_1 and D_2 on S by the formulas:

$$(16)\quad D_1(X_1) = 0 = D_2(X_2),\quad D_1(X_2) = X_2,\quad D_2(X_1) = X_1.$$

One can easily check that $S_{D_1} = k[X_1, X_2^2]$, and $S_{D_2} = k[X_1^2, X_2]$. We further note that $I = (X_1X_2)$, the principal ideal in S generated by X_1X_2, is differential under both D_1 and D_2. Thus, D_1 and D_2 induce first order k-derivations (which we continue to denote by D_1 and D_2) on $R = S/I$.

If we set x_i equal to the residue class of X_i in R, then $R = k[x_1, x_2]$. One easily checks that $R_{D_1} = k[x_1, x_2^2]$, and $R_{D_2} = k[x_1^2, x_2]$. Thus, if we set $\Gamma = \{D_1, D_2\}$, then $R_\Gamma = k[x_1^2, x_2^2]$. We note that R is generated as an R_Γ-module by $\{1, x_1, x_2\}$.

We now claim that for no elements $f, g \in R - R_\Gamma$ is φ: $R_\Gamma[f] \otimes R_\Gamma[g] \rightarrow R_\Gamma[f, g]$ an isomorphism. Suppose the claim is false. Then there exist $f, g \in R - R_\Gamma$ such that φ is an isomorphism. Now we can write $f = a + bx_1 + cx_2$ with $a, b, c \in R_\Gamma$. Since $x_1x_2 = 0$, we can further assume that $b \in k[x_1^2]$, $c \in k[x_2^2]$. Since $f \notin R_\Gamma$, either $b \neq 0$ or $c \neq 0$. We can assume $b \neq 0$ without any loss in generality. We also note that since $f^2 \in R_\Gamma$, $R_\Gamma[f]$ is generated as an R_Γ-module by $\{1, f\}$. Similar remarks can be made about g. That is, we can write $g = a' + b'x_1 + c'x_2$ with $b' \in k[x_1^2]$, and $c' \in k[x_2^2]$. $R_\Gamma[g]$ is an R_Γ-module with generators $\{1, g\}$, and either $b' \neq 0$, or $c' \neq 0$.

Now an easy computation shows that $f \otimes (g + a') + 1 \otimes (A + ag) \in \ker \varphi$. Here $A = aa' + bb'x_1^2 + cc'x_2^2$. Thus, since φ is an isomorphism, we have

$$(17)\quad f \otimes (g + a') + 1 \otimes (A + ag) = 0.$$

Since $\{1, f\}$ is a set of generators of $R_\Gamma[f]$, we conclude from (17) and [**1**, Lemma 10, p. 41] that there exist elements $z_1, \ldots, z_n \in R_\Gamma[g]$ and elements

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

$a_{j\lambda} \in R_\Gamma (j = 1, \ldots, n, \lambda = 1, 2)$ such that

$$(18)\quad \begin{aligned} &\text{(i) } a_{j1}f + a_{j2} = 0 \quad \text{for } j = 1, \ldots, n \\ &\text{(ii) } g + a' = \sum_{j=1}^{n} z_j a_{j1} \\ &\text{(iii) } A + ag = \sum_{j=1}^{n} z_j a_{j2}. \end{aligned}$$

We now argue that the equations in (18) imply a contradiction. There are two cases to consider:

Case 1. Suppose $f = a + bx_1 + cx_2$ with $b \neq 0$, $c \neq 0$.

In this case, (18*i*) implies that $a_{j1}(bx_1 + cx_2) \in R_\Gamma$. Now write a_{j1}, b and c as follows:

$$(19)\quad \begin{aligned} a_{j1} &= \sum_{l=0}^{N} (\alpha_{j1l}(x_1^2)^l + \beta_{j1l}(x_2^2)^l) \\ b &= \sum_{l=0}^{N} \gamma_l (x_1^2)^l, \quad c = \sum_{l=0}^{N} \delta_l (x_2^2)^l \end{aligned}$$

with $\alpha_{j1l}, \beta_{j1l}, \gamma_l, \delta_l \in k$. If we substitute the expressions from (19) into the relation $a_{j1}(bx_1 + cx_2) \in k[x_1^2, x_2^2]$, we easily see that $\alpha_{j1l} = \beta_{j1l} = 0$ for all l. Thus, $a_{j1} = 0$ for all $j = 1, \ldots, n$. But then (18 ii) implies that $g = a' \in R_\Gamma$, a contradiction.

Case 2. Suppose $f = a + bx_1$ with $b \neq 0$.

We begin as in Case 1. Equation (18 i) implies that $a_{j1}bx_1 \in k[x_1^2, x_2^2]$. Writing a_{j1} and b as in (19) and substituting into the relation $a_{j1}bx_1 \in k[x_1^2, x_2^2]$ gives $\alpha_{j1l} = 0$ for all l. We conclude that each a_{j1} is a polynomial in x_2^2 without constant term. Thus, we can write

$$a_{j1} = \sum_{l=1}^{N} \beta_{j1l}(x_2^2)^l \quad (j = 1, \ldots, n)$$

with $\beta_{j1l} \in k$. So equation (18 ii) now takes the form

$$(20)\quad g + a' = \sum_{j=1}^{n} z_j \left(\sum_{l=1}^{N} \beta_{j1l}(x_2^2)^l \right).$$

Now recall that $b' \in k[x_1^2]$, $c' \in k[x_2^2]$ and that $g + a' = b'x_1 + c'x_2$. Since $x_2^2 R \subset k[x_2]$, equation (20) implies $b' = 0$. Thus, equation (20) has the form

$$(21)\quad \left\{ \sum_{i=0}^{r} \gamma_i (x_2^2)^i \right\} x_2 = \sum_{j=1}^{n} z_j \left(\sum_{l=1}^{N} \beta_{j1l}(x_2^2)^l \right)$$

for some $\gamma_i \in k$. Now each $z_j = \alpha_j + \beta_j g$ with α_j and β_j in R_Γ. If we write α_j and β_j as in equation (19) and substitute into (21), we easily see that (21) is impossible. Thus, in either case, (18) is impossible. Therefore, φ is never an isomorphism, and Example 1 is complete.

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

We note that Example 1 also gives an example of the remarks made in the introduction of this paper. If $R = k[x_1, x_2]$, and $\Gamma = \{D_1, D_2\}$, as in Example 1, then R/R_Γ is an extension of characteristic two such that R_Γ is the ring of constants of Γ. But, R fails to be a tensor product over R_Γ of primitive extensions of R_Γ.

In view of Example 1, the hypotheses appearing in Theorem 1 are reasonable.

3B. The characteristic zero case.

LEMMA 2. *Let R/k be an extension of characteristic zero such that no nonzero integer is a zero-divisor in R. Let $D = \{d_0, d_1, \ldots, d_m\}$ be a k-higher derivation on R, and let R_D be the ring of constants of D. Suppose there exists an element x in R such that $d_1x = 1$. Then x is transcendental over R_D.*

Proof. By x being transcendental over R_D, we, of course, mean that x satisfies no algebraic equation of the form:

$$(22) \quad c_nx^n + c_{n-1}x^{n-1} + \ldots + c_0 = 0$$

where the c_j's are in R_D and are not all zero. The proof of Lemma 2 is by contradiction. Suppose x satisfies such an equation (22). Among all such equations that x satisfies, we can pick one for which n is minimal. Say equation (22) is one such equation. Then applying d_1 to (22) gives

$$(23) \quad n\, c_nx^{n-1} + \ldots + c_1 = 0.$$

By the minimality of n, the coefficients of the expression in (23) are all zero. Since no nonzero integer is a zero-divisor in R, we conclude that $c_n = \ldots = c_1 = 0$. But, then every coefficient in (22) is zero. This is a contradiction, and the proof of Lemma 2 is complete.

Before we give the proof of Theorem 1 in the characteristic zero case, we give an easy example which shows that the hypothesis "no nonzero integer is a zero-divisor in R" cannot be omitted from Lemma 2.

Example 2. Let $\mathbf{Z}$ denote the integers, and let X be an indeterminate. Set $k = \mathbf{Z}[X]/(2X)$. Then k has characteristic zero, and 2 is a zero-divisor in k. Let x denote the image of X in k. Then $k = \mathbf{Z}[x]$. Now let Y be an indeterminate over k and set $R = k[Y]/(xY^2)$. Let y be the image of Y in R. Then $R = k[y]$ is an extension of k of characteristic zero, and 2 is a zero-divisor in R.

Now we can define a first order k-derivation D on $k[Y]$ by letting $D(Y) = 1$. Since $D(xY^2) = 2xY = 0$, we see (xY^2) is a differential ideal under D. So, D induces on R a first order k-derivation (which we shall also call D) such that $D(y) = 1$.

Thus, R/k has a first order k-derivation D, and an element $y \in R$ such that $D(y) = 1$. But y is algebraic over R_D since $x \in R_D$ and $xy^2 = 0$. Thus, the conclusion of Lemma 2 can fail if we allow nonzero integers to be zero-divisors.

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

We now prove Theorem 1 in the characteristic zero case.

Proof of Theorem 1 (char = 0). Since $(D_1, \ldots, D_n | x_1, \ldots, x_n)$ satisfy equation (4), we have $R_{D_i} \supset R_\Gamma[x_1, \ldots, \hat{x}_i, \ldots, x_n]$. Thus, by Lemma 2, x_i is transcendental over $R_\Gamma[x_1, \ldots, \hat{x}_i, \ldots, x_n]$. Now consider $\varphi: \otimes R_\Gamma[x_i] \rightarrow R_\Gamma[x_1, \ldots, x_n]$. If $\sum c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha_1} \otimes \ldots \otimes x_n^{\alpha_n} \in \ker \varphi$, $(c_{\alpha_1 \ldots \alpha_n} \in R_\Gamma)$, then in R, we have

$$(24) \quad \sum_{\alpha_1} \left(\sum c_{\alpha_1 \ldots \alpha_n} x_2^{\alpha_2} \ldots x_n^{\alpha_n} \right) x_1^{\alpha_1} = 0.$$

Since x_1 is transcendental over $R_\Gamma[x_2, \ldots, x_n]$, we conclude that each expression in parentheses in (24) is zero. Thus, we conclude by induction that every $c_{\alpha_1 \ldots \alpha_n}$ is zero.

The proof of Theorem 1 is now complete in all cases. We give two examples concerning the hypotheses of Theorem 1 in the characteristic zero case. The first example shows that the hypotheses $(D_1, \ldots, D_n | x_1, \ldots, x_n)$ satisfy (4) cannot be omitted from Theorem 1. The second example shows that the hypothesis "no nonzero integer is a zero-divisor in R" cannot be omitted either.

Example 3. Let k be any field of characteristic zero and let X_1 and X_2 be indeterminates over k. Set $R = k[X_1, X_2]$. We define two first order k-derivations D_1 and D_2 on R by the formulas:

$$(25) \quad D_1(X_1) = X_1, \quad D_1(X_2) = D_2(X_2) = 0, \quad D_2(X_1) = X_2.$$

Then one can easily check that $R_{D_1} = R_{D_2} = k[X_2]$. Thus, $R_\Gamma = k[X_2]$ when $\Gamma = \{D_1, D_2\}$.

Now if $f \in R - R_\Gamma$, then clearly f is transcendental over R_Γ. Thus, if f, $g \in R - R_\Gamma$, and $\varphi: R_\Gamma[f] \otimes R_\Gamma[g] \rightarrow R_\Gamma[f, g]$ is the natural map, then simple dimension theoretic considerations imply that φ cannot be an isomorphism.

In Example 1, $R_{D_1} \neq R_{D_2}$. In Example 3, $R_{D_1} = R_{D_2}$. In either example, $R_\Gamma[f, g]$ fails to be isomorphic to $R_\Gamma[f] \otimes R_\Gamma[g]$. Thus, the order relationships between the rings R_{D_i} are not enough to decide if any finitely generated R_Γ-algebra contained in R is a tensor product.

Example 4. Again, let $\mathbf{Z}$ denote the integers. Let X denote an indeterminate over $\mathbf{Z}$ and set $k = \mathbf{Z}[X]/(4X)$. We shall let x denote the image of X in k. Therefore, $k = \mathbf{Z}[x]$. Now let Y_1 and Y_2 be indeterminates over k, and set $S = k[Y_1, Y_2]$. We define two first order k-derivatives D_1 and D_2 on S by $D_1(Y_1) = 1 = D_2(Y_2)$, and $D_1(Y_2) = D_2(Y_1) = 0$. So, $(D_1, D_2 | Y_1, Y_2)$ satisfy equation (4). Now let $\mathfrak{A}$ be the following homogeneous ideal in S:

$$(26) \quad \mathfrak{A} = (x\, Y_1^2 Y_2^2, 2x\, Y_1 Y_2^2, 2x\, Y_1^2 Y_2, 2x\, Y_1^2, 2x\, Y_2^2).$$

One can easily check that $\mathfrak{A}$ is differential under D_1 or D_2. Thus, D_1 and D_2 induce first order k-derivations (which we shall continue to call D_1 and D_2)

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

on $R = S/\mathfrak{A}$. If we let y_i denote the image of Y_i in R, then $R = k[y_1, y_2]$, R/k is an extension of characteristic zero, 2 is a zero-divisor in R and $(D_1, D_2|y_1, y_2)$ satisfy equation (4).

Now set $\Gamma = \{D_1, D_2\}$, and let R_Γ denote the ring of constants of Γ as usual. Consider φ: $R_\Gamma[y_1] \otimes R_\Gamma[y_2] \rightarrow R_\Gamma[y_1, y_2]$. An easy computation shows that $x\, y_1^2$ and y_2^2 are not elements of R_Γ, but $x\, y_1^2 \otimes y_2^2 \in \ker \varphi$. We shall now show that $x\, y_1^2 \otimes y_2^2 \neq 0$, and, consequently, φ is not an isomorphism.

The argument is similar to that in Example 1. We assume $x\, y_1^2 \otimes y_2^2 = 0$. Then by [**1**, Lemma 10, p. 40], there exist elements $a_{j\lambda} \in R_\Gamma (j = 1, \ldots, n, \lambda = 0, 1, \ldots)$, and $\omega_j \in R_\Gamma[y_1]$ such that

$$\text{(i)} \sum_{\lambda=0}^{\infty} a_{j\lambda} y_2^{\lambda} = 0, \quad j = 1, \ldots, n$$

$$(27) \qquad \text{(ii)}\ xy_1^2 = \sum_{j=1}^{n} \omega_j a_{j2}$$

$$\text{(iii)}\ 0 = \sum_{j=1}^{n} \omega_j a_{j\lambda}, \quad \lambda \neq 2.$$

Here we note that the family $\{a_{j\lambda}|\lambda = 0, 1, \ldots\}$ has finite support, and, thus, (27 i) is a finite sum. We wish to argue that the equations in (27) are impossible. The computations are tedious but not difficult. We sketch the main ideas and leave the details to the interested reader.

We first note that any element $z \in R_\Gamma$ can be written in the following form:

$$(28) \qquad z = \alpha + g_3 + \ldots + g_m.$$

Here $\alpha \in k$, and g_i is a homogeneous polynomial in y_1 and y_2 (coefficients in k) of degree i. Since only finitely many $a_{j\lambda}$ appear in (27 i), we can write each $a_{j\lambda}$ as

$$(29) \qquad a_{j\lambda} = \alpha^{j,\lambda} + g_3^{j,\lambda} + \ldots + g_m^{j,\lambda}$$

for some m sufficiently large. Here $\alpha^{j,\lambda}$ and $g_i^{j,\lambda}$ are as in equation (28). If we now substitute (29) into equation (27 i) and apply D_2^2, we conclude that a_{j2} has the following form:

$$(30) \qquad a_{j2} = 2x\, \beta^{j,2} + g_3^{j,2} + \ldots + g_m^{j,2}.$$

Here $\beta^{j,2} \in k$, and $g_i^{j,2}$ are homogeneous polynomials of degree i in y_1 and y_2. We now substitute (30) into (27 ii) getting

$$(31) \qquad xy_1^2 = \sum_{j=1}^{n} \omega_j(2x\beta^{j,2} + g_3^{j,2} + \ldots + g_m^{j,2}).$$

Now each ω_j lies in $R_\Gamma[y_1]$. Thus, each ω_j can be written as $\omega_j = \sum_{t=0}^{N} c_{jt} y_1^t$. Here $c_{jt} \in R_\Gamma$. If we write each c_{jt} as in (28) and substitute into equation (31), we easily see that equation (31) is impossible. Thus, $x\, y_1^2 \otimes y_2^2 \neq 0$, and φ fails to be an isomorphism.

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

Thus, even if $(D_1, \ldots, D_n|x_1, \ldots, x_n)$ satisfy equation (4), the conclusion of Theorem 1 may fail if some nonzero integer is a zero-divisor in R.

One last comment about Theorem 1 seems appropriate here. We can state a slightly more general version of Theorem 1 as follows:

THEOREM 1′. *Suppose R/k is an extension of prime characteristic p or an extension of characteristic zero in which no nonzero integer is a zero-divisor. Let $\Gamma = \{D_1, \ldots, D_n\}$ be a set of k-higher derivations on R, and suppose there exists elements $x_1, \ldots, x_n \in R - R_\Gamma$ such that the following system of equations is satisfied;*

$$(32)\quad \begin{aligned} &D_{ij}(x_k) = 0 \quad \text{if } k \neq i,\ 1 \leqq j \leqq \operatorname{rk} D_i \\ &D_{i1}(x_i) \text{ is a unit in } R,\ 1 \leqq i \leqq n. \end{aligned}$$

Then $R_\Gamma[x_1, \ldots, x_n] \cong \otimes R_\Gamma[x_i]$.

Proof. Set $D_{i1}(x_i) = \epsilon_i$, a unit in R. Let the multiplicative inverse of ϵ_i be α_i. If $D_i = \{D_{i0}, D_{i1}, \ldots, D_{im(i)}\}$, then clearly $D_i' = \{D_{i0}, \alpha_i D_{i1}, \ldots, \alpha_i^{m(i)} D_{im(i)}\}$ is another k-higher derivation on R such that $\operatorname{rk} D_i' = \operatorname{rk} D_i$. Since α_i is a unit, $R_{D_i} = R_{D_i'}$. Thus, $R_\Gamma = \bigcap R_{D_i'}$, and equation (32) implies $(D_1', \ldots, D_n'|x_1, \ldots, x_n)$ satisfy equation (4). Thus, the result follows from Theorem 1.

To complete our study of the main problem in this paper, we now investigate when $R = R_\Gamma[x_1, \ldots, x_n]$. In the first place, if the conditions of Theorem 1 are satisfied, we cannot conclude that $R = R_\Gamma[x_1, \ldots, x_n]$. A simple example will illustrate this point.

Example 5. Let k be any field and let X_1, X_2, X_3 be indeterminates over k. Set $R = k[X_1, X_2, X_3]$. We define two first order k-derivations D_1 and D_2 on R by the following formulas:

$$(33)\quad \begin{aligned} D_1(X_1) &= D_2(X_2) = 1 \\ D_1(X_2) &= D_2(X_1) = 0 \\ D_1(X_3) &= D_2(X_3) = X_3. \end{aligned}$$

Then $(D_1, D_2|X_1, X_2)$ satisfy equation (4). But if $\Gamma = \{D_1, D_2\}$, then $X_3 \notin R_\Gamma[X_1, X_2]$. To prove this fact, we merely have to note that given any $f \in R_\Gamma[X_1, X_2]$, there exists an n sufficiently large such that $D_1^n(f) = 0$. Since $D_1^n(X_3) = X_3$ for all n, we conclude that $X_3 \notin R_\Gamma[X_1, X_2]$.

Thus, more conditions on Γ are needed in order to ensure that R is a tensor product over R_Γ. We shall state exactly what is necessary when R is an integral domain.

Let R/k be an integral domain, and let S be a subring of R. We shall denote by $Q(S)$ the quotient field of S. If D is a k-higher derivation on S, then D has a natural extension to $Q(S)$. A proof of this fact can be found in [**4**, Theorem 15]. In particular, if $\Gamma = \{D_1, \ldots, D_n\}$ is a set of k-higher derivations on R/k,

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

then Γ can be viewed as a set of k-higher derivations on $Q(R)$. It also follows from [**4**, Theorem 15], that $Q(R_\Gamma)$ is a subfield of the field of constants of Γ on $Q(R)$.

We need the following lemma.

LEMMA 3. *Let R/k be a domain of prime characteristic p. Let $\Gamma = \{D_1, \ldots, D_n\}$ be a set of k-higher derivations on R. Suppose there exist elements $x_1, \ldots, x_n \in R - R_\Gamma$ such that $(D_1, \ldots, D_n|x_1, \ldots, x_n)$ satisfy equation* (4). *Then for every polynomial*

$$f = \sum \{c_{\alpha_1\ldots\alpha_n}x_1^{\alpha_1} \ldots x_n^{\alpha_n} |0 \leqq \alpha_i < \mu_\Gamma(x_i)\},$$

with coefficients $c_{\alpha_1\ldots\alpha_n} \in Q(R_\Gamma)$, there exists a composite $E_1 \circ \ldots \circ E_r$ of components of $D_1, \ldots, D_n$ such that $E_1 \circ \ldots \circ E_r(f) = l\, c_{\gamma_1\ldots\gamma_n}$. Here l is a nonzero integer (*in* $\mathbf{Z}/p\mathbf{Z}$), *and $c_{\gamma_1\ldots\gamma_n}$ is one of the* (*nonzero*) *coefficients appearing in f.*

Proof. The proof of Lemma 3 is easy, and we shall only sketch the main ideas. Since $(D_1, \ldots, D_n|x_1, \ldots, x_n)$ satisfy equation (4), Lemma 3 is easily seen to be true if f has degree less than or equal to one. Thus, we can proceed by induction on the degree of f. If f has degree bigger than one, we can assume without loss of generality that x_1 is present in a term of highest possible degree in f. Then we can write f in the following form:

$$(34)\quad f = A_0 + A_1x_1 + \ldots + A_mx_1^m.$$

Here $A_i \in Q(R_\Gamma)[x_2, \ldots, x_n] \subset Q(R)_{D_1}$. Further, $A_m \neq 0$, and $m \deg A_m = \deg f$. We note that $m < \mu_\Gamma(x_1)$. Thus, by techniques similar to those used in Theorem 1, we can show that there exists a component D_{1i} of D_1 such that $D_{1i}(f) \neq 0$, $D_{1i}(f) = B_1 + B_2x_1 + \ldots + B_mx_1^{m-1}$ and each B_i is just A_i multiplied by some element l_i of $\mathbf{Z}/p\mathbf{Z}$. Since the degree of $D_{1i}(f)$ is less than f, there exists a composite of components $E_1 \circ \ldots \circ E_r$ of $D_1, \ldots, D_n$ such that $E_1 \circ \ldots \circ E_r(D_{1i}(f))$ is a nonzero multiple of one of the nonzero coefficients of $D_{1i}(f)$. Thus, $E_1 \circ \ldots \circ E_r \circ D_{1i}$ is the required composite for f.

We can now state the main result in characteristic p. Let $\mathrm{Der}_{R_\Gamma}{}^1(R)$ denote the R-module of first order R_Γ-derivations of R.

THEOREM 2. *Let R/k be a domain of prime characteristic p. Let $\Gamma = \{D_1, \ldots, D_n\}$ be a set of k-higher derivations on R. Suppose there exist elements $x_1, \ldots, x_n \in R - R_\Gamma$ such that $(D_1, \ldots, D_n|x_1, \ldots, x_n)$ satisfy equation* (4). *Then $R \cong \bigotimes R_\Gamma[x_i]$ if and only if $\{D_{11}, \ldots, D_{n1}\}$ span $\mathrm{Der}_{R_\Gamma}{}^1(R)$.*

Proof. Suppose φ: $\bigotimes R_\Gamma[x_i] \rightarrow R$ is an isomorphism. Since the image of φ is $R_\Gamma[x_1, \ldots, x_n]$, we conclude that $R = R_\Gamma[x_1, \ldots, x_n]$. Now if D is any first order R_Γ-derivation of R, then D is uniquely determined by its values on the x_i. Thus, it is clear that $D = \sum_{i=1}^n D(x_i)D_{i1}$. Therefore, $D_{11}, \ldots, D_{n1}$ span $\mathrm{Der}_{R_\Gamma}{}^1(R)$.

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

Suppose we now assume $D_{11}, \ldots, D_{n1}$ span $\mathrm{Der}_{R_\Gamma}{}^1(R)$. We easily see that $\mathrm{Der}_{R_\Gamma}{}^1(Q(R)) = \mathrm{Der}_{Q(R_\Gamma)}{}^1(Q(R)) = \mathrm{Der}_K{}^1(Q(R))$ where K is the subfield of $Q(R)$ generated by $Q(R_\Gamma)$ and $Q(R)^p$. Since $\mathrm{Der}_{R_\Gamma}{}^1(Q(R)) \cong Q(R) \otimes_R \mathrm{Der}_{R_\Gamma}{}^1(R)$, we conclude that $\{D_{11}, \ldots, D_{n1}\}$ is a basis for the $Q(R)$-module $\mathrm{Der}_K{}^1(Q(R))$.

We next show that $\{x_1, \ldots, x_n\}$ is a p-basis of $Q(R)/K$. Since $(D_1, \ldots, D_n|x_1, \ldots, x_n)$ satisfy (4), we easily see that $\{x_1, \ldots, x_n\}$ is a p-independent subset of $Q(R)/K$. Thus, there exists a p-basis B of $Q(R)/K$ such that $\{x_1, \ldots, x_n\} \subset B$. Suppose there exists a $y \in B - \{x_1, \ldots, x_n\}$. Then by [**3**, Theorem 17, p. 181], there exists a first order K-derivation D on $Q(R)$ such that $D(x_i) = 0, i = 1, \ldots, n$, and $D(y) = 1$. But, $\{D_{11}, \ldots, D_{n1}\}$ is a basis for $\mathrm{Der}_K{}^1(Q(R))$. Consequently, there exist constants $\alpha_1, \ldots, \alpha_n \in Q(R)$ such that

$$(35) \quad D = \alpha_1 D_{11} + \ldots + \alpha_n D_{n1}.$$

If we now evaluate (35) at each x_i, we get $\alpha_i = 0, i = 1, \ldots, n$. Thus, $D = 0$. But this is impossible since $D(y) = 1$. We conclude that $B - \{x_1, \ldots, x_n\} = \emptyset$, and, consequently, $\{x_1, \ldots, x_n\}$ is a p-basis of $Q(R)/K$.

Since $\{x_1, \ldots, x_n\}$ is a p-basis of $Q(R)/K$, we have $Q(R) = K(x_1, \ldots, x_n)$. In other words, $Q(R) = Q(R_\Gamma)(Q(R)^p)(x_1, \ldots, x_n)$. Iterating this relationship and using the fact that $R^{p^e} \subset R_\Gamma$ for some e sufficiently large, we get $Q(R) = Q(R_\Gamma)(x_1, \ldots, x_n)$.

Now let $z \in R$. Since $Q(R) = Q(R_\Gamma)(x_1, \ldots, x_n) = Q(R_\Gamma)[x_1, \ldots, x_n]$, there exist elements $c_{\alpha_1 \ldots \alpha_n} \in Q(R_\Gamma)$ such that

$$(36) \quad z = \sum c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha 1} \ldots x_n^{\alpha n}.$$

Here $0 \leqq \alpha_i < \mu_\Gamma(x_i)$. We conclude the proof of Theorem 2 by showing that equation (36) implies every $c_{\alpha_1 \ldots \alpha_n}$ lies in R_Γ.

We proceed by induction on the number of monomials present on the right hand side of (36). If only one monomial is present, then equation (36) has the form

$$(37) \quad z = c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha 1} \ldots x_n^{\alpha n}.$$

We now apply Lemma 3 to equation (37). Hence there exists a composite of components $E_1 \circ \ldots \circ E_r$ of $D_1, \ldots, D_n$ such that $E_1 \circ \ldots \circ E_r(z) = lc_{\alpha_1 \ldots \alpha_n}$. Here l is some nonzero element in $\mathbf{Z}/p\mathbf{Z}$. Since $E_1 \circ \ldots \circ E_r(z) \in R$, we conclude $c_{\alpha_1 \ldots \alpha_n} \in Q(R_\Gamma) \cap R$. But again by [**4**, Theorem 15], $Q(R_\Gamma) \cap R = R_\Gamma$. Thus, $c_{\alpha_1 \ldots \alpha_n} \in R_\Gamma$. So, the result is established if only one monomial appears on the right in equation (36).

Now suppose more than one monomial appears on the right in (36). Use Lemma 3 again. We can find a composite of components $E_1 \circ \ldots \circ E_r$ of $D_1, \ldots, D_n$ such that $E_1 \circ \ldots \circ E_r(z) = l\, c_{\gamma_1 \ldots \gamma_n}$. Here $c_{\gamma_1 \ldots \gamma_n}$ is one of the coefficients appearing in (36). Thus, $c_{\gamma_1 \ldots \gamma_n} \in R_\Gamma$. Now (36) can be rewritten as

$$(38) \quad z - c_{\gamma_1 \ldots \gamma_n} x_1^{\gamma 1} \ldots x_n^{\gamma_n} = \sum c_{\alpha_1 \ldots \alpha_n} x_1^{\alpha 1} \ldots x_n^{\alpha n}.$$

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

The sum on the right is now taken over all n-tuples $(\alpha_1, \ldots \alpha_n) \neq (\gamma_1, \ldots, \gamma_n)$. Since there are fewer monomials now appearing on the right in (38) than in (36), we conclude by induction that every $c_{\alpha_1 \ldots \alpha_n}$ lies in R_Γ.

Thus, we have proven that $R_\Gamma[x_1, \ldots, x_n] = R$. By Theorem 1, $\varphi: \otimes R_\Gamma[x_i] \rightarrow R_\Gamma[x_1, \ldots, x_n]$ is an isomorphism. Therefore, $\otimes R_\Gamma[x_i] \cong R$, and the proof of Theorem 2 is complete.

We note that the two main hypotheses in Theorem 2 are independent of each other. Example 5 provides an example in which $(D_1, D_2 | X_1, X_2)$ satisfy equation (4), but the set $\{D_1, D_2\}$ does not span $\mathrm{Der}_{R_\Gamma}{}^1(R)$. For example, if the characteristic of k is two, then $R_\Gamma = k[X_1^2, X_2^2, X_3^2]$. So, D_3 defined by $D_3(X_1) = D_3(X_2) = 0$, and $D_3(X_3) = 1$ is a well defined first order R_Γ-derivation on R. But, D_3 is not an R-linear combination of D_1 and D_2.

On the other hand, if a set $\Gamma = \{D_1, \ldots, D_n\}$ of k-higher derivations on R/k is such that the set $\{D_{11}, \ldots, D_{n1}\}$ spans $\mathrm{Der}_{R_\Gamma}{}^1(R)$, then it need not follow that there exist elements $x_1, \ldots, x_n$ in R such that equation (4) is satisfied. Consider the following example:

Example 6. Let k be any field of characteristic not equal to two or three. Let X and Y be indeterminates over k, and set $R = k[X, Y]/(X^2 - Y^3)$. Then R is an integral domain. Since R is a homomorphic image of $k[X, Y]$, $\mathrm{Der}_k{}^1(R)$ is a finitely generated R-module. Let x and y denote the images of X and Y in R. Then $R = k[x, y]$. Set $m = (x, y)$, the maximal ideal in R generated by x and y.

Now if $D \in \mathrm{Der}_k{}^1(R)$, then $2x\, D(x) = 3y^2 D(y)$. It now easily follows from this equation that $D(R) \subset m$. Thus, no first order k-derivation on R can take any element of R to a unit. In particular, if $\Gamma = \{D_1, \ldots, D_n\}$, where $\{D_1, \ldots, D_n\}$ span $\mathrm{Der}_k{}^1(R)$, then Γ spans $\mathrm{Der}_{R_\Gamma}{}^1(R)$. But, no elements $x_1, \ldots, x_n$ can be found in R such that $(D_1, \ldots, D_n | x_1, \ldots, x_n)$ satisfy equation (4).

We now turn our attention to the analog of Theorem 2 when R/k is a domain of characteristic zero. We first note that the two main hypotheses in Theorem 2 are not strong enough to imply the result in characteristic zero. Consider the following example:

Example 7. Let k be a field of characteristic zero, and suppose X_1 and X_2 are indeterminates over k. Set $R = k[X_1, X_2, Z, 1/Z]$ where $Z^2 = X_1$. We can define two first order k-derivations D_1 and D_2 on $k[X_1, X_2]$ by setting $D_1(X_1) = D_2(X_2) = 1$, $D_1(X_2) = D_2(X_1) = 0$. Since Z is separable over $k[X_1, X_2]$, each D_i has a unique extension to R. We easily check that R/k is a domain of characteristic zero in which $(D_1, D_2 | X_1, X_2)$ satisfy equation (4). Further, $\Gamma = \{D_1, D_2\}$ spans $\mathrm{Der}_k{}^1(R)$, and, thus, $\mathrm{Der}_{R_\Gamma}{}^1(R)$ also.

Consequently, R/k satisfies the two main hypotheses of Theorem 2, but $R_\Gamma[X_1, X_2] \neq R$. For $Z \notin R_\Gamma[X_1, X_2]$. To see this, we merely have to note that some high power of D_1 kills any given element of $R_\Gamma[X_1, X_2]$. Since $D_1{}^n(Z) \neq 0$ for any n, we conclude that $Z \notin R_\Gamma[X_1, X_2]$.

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

When we study Example 7, we come to the conclusion that a necessary condition for $R_\Gamma[x_1, \ldots, x_n] = R$ in the presence of equation (4) is that large composites of $D_{11}, \ldots, D_{n1}$ should kill any given element of R. If $\{D_{11}, \ldots, D_{n1}\}$ span $\mathrm{Der}_{R_\Gamma}{}^1(R)$, then this condition is sufficient also.

THEOREM 3. *Let R/k be an integral domain such that k contains the rationals. Let $\Gamma = \{D_1, \ldots, D_n\}$ be a set of k-higher derivations on R, and suppose there exist elements $x_1, \ldots, x_n \in R - R_\Gamma$ such that $(D_1, \ldots, D_n|x_1, \ldots, x_n)$ satisfy equation* (4). *Then $R \cong \otimes R_\Gamma[x_i]$ if and only if the following two conditions are satisfied*:

(α) $\{D_{11}, \ldots, D_{n1}\}$ *span* $\mathrm{Der}_{R_\Gamma}{}^1(R)$.

(β) *For every $z \in R$, there exists a nonnegative integer $N(z)$ such that if $m > N(z)$, then $E_1 \circ \ldots \circ E_m(z) = 0$. Here $E_i \in \{D_{11}, \ldots, D_{n1}\}$.*

Proof. If $R \cong \otimes R_\Gamma[x_i]$, then $R = R_\Gamma[x_1, \ldots, x_n]$. In this case, condition (β) follows trivially from equation (4). The proof of (α) is the same as in Theorem 2.

So, let us assume conditions (α) and (β) are satisfied. By Theorem 1, $\varphi: \otimes R_\Gamma[x_i] \rightarrow R_\Gamma[x_1, \ldots, x_n]$ is an isomorphism. Thus, we need to show that conditions (α) and (β) imply $R_\Gamma[x_1, \ldots, x_n] = R$.

Let $R_{D_{i1}}$ denote the ring of constants of D_{i1}, $(1 \leqq i \leqq n)$. We first argue that $R_\Gamma = \bigcap_{i=1}^n R_{D_{i1}}$. Clearly, $R_\Gamma \subset \bigcap_{i=1}^n R_{D_{i1}}$. Let $z \in \bigcap_{i=1}^n R_{D_{i1}}$. It is well known that each D_i can be embedded as a section in some R_Γ-higher derivation E_i of infinite rank on R. A proof of this fact can be found in [**5**, (q) p. 33]. We can regard E_i as a $Q(R_\Gamma)$-derivation of infinite rank on $Q(R)$. By [**2**, (5)], each component of E_i is just a sum of composites of first order $Q(R_\Gamma)$-derivations on $Q(R)$. Now condition (α) implies that $\{D_{11}, \ldots, D_{n1}\}$ is a $Q(R)$-basis of $\mathrm{Der}_{Q(R_\Gamma)}{}^1(Q(R))$. Thus, any first order $Q(R_\Gamma)$-derivation on $Q(R)$ vanishes on z. Therefore, any component of E_i vanishes on z. In particular, $D_{ij}(z) = 0$ for every $j = 1, \ldots, \mathrm{rk}\, D_i$. Thus, $z \in R_\Gamma$.

It is now clear that the components of rank greater than one (if present) in D_i play no role in this theorem. Thus, without loss of generality, we can assume that each D_i is just a first order k-derivation on R.

We next claim that $Q(R)$ is an algebraic extension of $Q(R_\Gamma)(x_1, \ldots, x_n)$. We proceed by contradiction. Suppose $Q(R)$ contains an element z such that z is transcendental over $Q(R_\Gamma)(x_1, \ldots, x_n)$. Set $K = Q(R_\Gamma)(x_1, \ldots, x_n, z)$. By the proof of Theorem 1, $\{x_1, \ldots, x_n\}$ is a transcendence set over $Q(R_\Gamma)$. Since z is transcendental over $Q(R_\Gamma)(x_1, \ldots, x_n)$, $\{x_1, \ldots, x_n, z\}$ is also a transcendence set over $Q(R_\Gamma)$. Thus, we can define a $Q(R_\Gamma)$-derivation D on K by $D(x_i) = 0$ $(1 \leqq i \leqq n)$, and $D(z) = 1$. Since the characteristic of K is zero, D can be extended to a $Q(R_\Gamma)$-derivation on $Q(R)$. Since $\{D_1, \ldots, D_n\}$ is a basis for $\mathrm{Der}_{Q(R_\Gamma)}{}^1(Q(R))$, there exist elements $\alpha_1, \ldots, \alpha_n \in Q(R)$ such that

$$(39) \quad D = \alpha_1 D_1 + \ldots + \alpha_n D_n.$$

If we evaluate equation (39) at each x_i, we get $\alpha_i = 0$ for all $i = 1, \ldots, n$. Thus, $D = 0$. But, this is a contradiction since $D(z) = 1$. Therefore, $Q(R)$ is an

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

algebraic extension of $Q(R_\Gamma)(x_1, \ldots, x_n)$. In particular, each element $z \in R$ satisfies some algebraic equation over $R_\Gamma[x_1, \ldots, x_n]$.

Now let $z \in R$. Then there exists a nonnegative integer $N(z)$ such that condition (β) holds. We shall show that $z \in R_\Gamma[x_1, \ldots, x_n]$ by proceeding by induction on the integer $N(z)$.

If $N(z) = 0$, then condition (β) implies that $D_i(z) = 0$ for every $i = 1, \ldots .n$ Thus, $z \in R_\Gamma$. In particular, $z \in R_\Gamma[x_1, \ldots, x_n]$, and the proof is complete in this case. Thus, we can assume that if $N(z) < M$ $(M > 0)$, then $z \in R_\Gamma[x_1, \ldots, x_n]$. Let $z \in R$ such that $N(z) = M$. We note then that $N(D_i(z)) < M$ for any $i = 1, \ldots, n$. Thus, $D_i(z) \in R_\Gamma[x_1, \ldots x_n]$ for all i.

Now we know z satisfies some algebraic equation over $R_\Gamma[x_1, \ldots, x_n]$. Thus, we have

$$(40) \quad a_m z^m + a_{m-1}z^{m-1} + \ldots + a_0 = 0.$$

Here the a_j's are all elements of $R_\Gamma[x_1, \ldots, x_n]$ and not all zero. We can assume that m in (40) is as small as possible among all such relations on z.

We now claim that our induction hypothesis implies that $m = 1$. If $m = 1$ in equation (40), then there is nothing to prove. Suppose $m \geqq 2$. We need at this point the analog of Lemma 3. We claim that for any non-zero $f \in R_\Gamma[x_1, \ldots, x_n]$, there exists a composite $D_1^{l_1} \circ \ldots \circ D_n^{l_n}$ such that $D_1^{l_1} \circ \ldots \circ D_n^{l_n}(f)$ is a non-zero constant of R_Γ. A proof of this fact follows easily from equation (4) and induction on the degree of f. Now, we apply this remark to the leading coefficient a_m in (40). Thus, there exists a composite $D_1^{l_1} \circ \ldots \circ D_n^{l_n}$ such that $D_1^{l_1} \circ \ldots \circ D_n^{l_n}(a_m) = c_m$ where c_m is a non-zero element in R_Γ. If we apply D_n to equation (40), we get

$$(41) \quad D_n(a_m)z^m + (ma_mD_n(z) + D_n(a_{m-1}))z^{m-1} + \ldots = 0.$$

By our induction assumption, the coefficients of z^i in (41) lie in $R_\Gamma[x_1, \ldots, x_n]$. It is now clear that $D_1^{l_1} \circ \ldots \circ D_n^{l_n}$ when applied to (40) gives an equation of the form:

$$(42) \quad c_m z^m + b_{m-1}z^{m-1} + \ldots + b_1 z + b_0 = 0.$$

Here c_m is a non-zero element in R_Γ, and $b_{m-1}, \ldots, b_0$ lie in $R_\Gamma[x_1, \ldots, x_n]$.

Now apply D_i to equation (42). We get

$$(43) \quad (mc_mD_i(z) + D_i(b_{m-1}))z^{m-1} + \ldots = 0.$$

Now the minimality of m implies that $mc_mD_i(z) + D_i(b_{m-1}) = 0$ for every $i = 1, \ldots, n$. Therefore, $mc_mz + b_{m-1} \in R_\Gamma$. But this relation implies that z satisfies an algebraic relationship of the type in equation (40) with $m = 1$. This is a contradiction since we are assuming that the minimum m possible in (40) is bigger than or equal to two. Thus, we conclude that $m = 1$ in equation (40).

We now claim that $z \in Q(R_\Gamma)[x_1, \ldots, x_n]$. Our induction hypothesis shows that z satisfies an equation of type (42) with $m = 1$. Dividing by c_1, gives us that $z \in Q(R_\Gamma)[x_1, \ldots, x_n]$. To summarize, we have now shown that $N(z) = M$

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

implies that there exist elements $c_{\alpha_1\ldots\alpha_n} \in Q(R_\Gamma)$ such that

$$(44) \quad z = \sum c_{\alpha_1\ldots\alpha_n} x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

We now proceed exactly as in the proof of Theorem 2. We can easily argue by induction on the number of monomials present on the right side of equation (44) that each $c_{\alpha_1\ldots\alpha_n}$ lies in R. But then each $c_{\alpha_1\ldots\alpha_n} \in R_\Gamma$, and, hence, $z \in R_\Gamma[x_1, \ldots, x_n]$. This completes the induction step and consequently the proof of Theorem 3.

We conclude this paper with a few remarks concerning the independence of conditions (α) and (β) in Theorem 3. We have already noted in Example 7 that (α) does not imply (β). We give a final example which shows that (β) does not imply (α).

Example 8. Let k be any field of characteristic zero and suppose X_1, X_2, X_3 are indeterminates over k. Set $R = k[X_1, X_2, X_3]$. We define two k-higher derivations D_1 and D_2 on R by the following equations:

$$(45) \quad \begin{array}{lll} D_{11}(X_1) = 1, & D_{12}(X_1) = 0, & D_2(X_1) = 0 \\ D_{11}(X_2) = 0, & D_{12}(X_2) = 0, & D_2(X_2) = 1 \\ D_{11}(X_3) = X_1, & D_{12}(X_3) = X_3, & D_2(X_3) = X_2. \end{array}$$

Note that D_1 is a k-higher derivation of rank two, while D_2 is a k-higher derivation of rank one on R. Clearly, $(D_1, D_2|X_1, X_2)$ satisfy equation (4).

We first show that $\{D_{11}, D_2\}$ satisfy condition (β) of Theorem 3. An easy computation shows that $D_{11}D_2 = D_2D_{11}$ Thus, it suffices to show that for each $z \in R$ there exist integers N and M sufficiently large such that $D_{11}^N(z) = D_2^M(z) = 0$. Since D_{11} and D_2 are symmetric, it suffices to prove this statement for D_{11} only. We need the following lemma.

LEMMA 4. $D_{11}^s(X_1^n X_3^l) = g(X_1, X_3) + \alpha X_1^{n+s}X_3^{l-s}$.

Here g is a polynomial in X_1 and X_3 with coefficients in k such that the degree of g is less than $n + l$. $\alpha \in k$.

The proof of this lemma is an easy induction argument on s. We omit it.

Now suppose $z \in R$. Since D_{11}^N is a k-endomorphism of R, we can assume z is a monomial. Suppose $z = X_1^nX_2^mX_3^l$. We proceed by induction on $L = n + l$. If $L = 0$, then $z = X_2^m$, and (45) implies $D_{11}(z) = 0$. In general, apply D_{11}^l to z first. By Lemma 4, we get

$$(46) \quad D_{11}^l(z) = X_2^m(g(X_1, X_3) + \alpha X_1^{n+1}).$$

Here deg $g < n + l = L$. Thus, by our induction assumption, there exists an N_1 such that $D_{11}^{N_1}(g) = 0$. Let $N > \max\{N_1, n + l\}$. Then clearly $D_{11}^{N+l}(z) = 0$.

Thus, $\{D_{11}, D_2\}$ satisfy condition (β) in Theorem 3. We next note that $\{D_{11}, D_2\}$ do not span $\mathrm{Der}_{R_\Gamma}{}^1(R)$ where $\Gamma = \{D_1, D_2\}$. To show this, we make

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press

use of Theorem 3 itself. If $\{D_{11}, D_2\}$ did span $\mathrm{Der}_{R_\Gamma}{}^1(R)$, then by Theorem 3, $R = R_\Gamma[X_1, X_2]$. But in this example, $R \neq R_\Gamma[X_1, X_2]$. We shall prove this last inequality by showing $X_3 \notin R_\Gamma[X_1, X_2]$.

Suppose $X_3 \in R_\Gamma[X_1, X_2]$. Then there exist elements $c_{ij} \in R_\Gamma$ such that

$$(47)\quad X_3 = \sum c_{ij} X_1{}^i X_2{}^j.$$

Now $D_{12}{}^N$ is a linear transformation with respect to R_Γ. Thus, applying $D_{12}{}^N$ to (47) and using equation (45), we get

$$(48)\quad X_3 = \sum c_{ij} X_2{}^j D_{12}{}^N (X_1{}^i).$$

Now we can easily argue that for N sufficiently large, the right hand side of (48) is zero. Thus, $X_3 = 0$. This is a contradiction. Therefore, $R \neq R_\Gamma[X_1, X_2]$ and Example 8 is complete.

Theorems 2 and 3 together with the examples given in this paper give a fairly complete answer to the final question in the introduction.

References

1. N. Bourbaki, *Algebre commutative* (Hermann, Paris).

2. N. Heerema, *Higher derivations and automorphisms of complete local rings*, Bull. Amer. Math. Soc. *76* (1970), 1212–1225.

3. N. Jacobson, *Lectures in abstract algebra, III* (D. Van Nostrand Co., Princeton, New Jersey).

4. Y. Nakai, *High order derivations I*, Osaka J. Math. *7* (1970), 1–27.

5. P. Ribenboim, *Higher derivations of rings I*, Rev. Roum. Math Pures et Appl. *16* (1971), 77–110.

6. M. Weisfeld, *Purely inseparable extensions and higher derivations*, Trans-Amer. Math. Soc. *116* (1965), 435–450.

Michigan State University,
East Lansing, Michigan

https://doi.org/10.4153/CJM-1978-035-9 Published online by Cambridge University Press